Audit Management mit DBMS_AUDIT_MGMT

Oehrli Stefan . Senior Consultant . 29. September 2010

Mit Oracle 11g R2 führte Oracle im Sicherheitsbereich das neue PL/SQL Package DBMS_AUDIT_MGMT ein. Wie man aus dem Namen bereits vermuten kann, dient dieses Package der Verwaltung von Audit Informationen. Die Tage, wo DBAs eigene Scripts und Jobs für die Organisation von Audit-Daten entwickeln müssen, scheinen gezählt zu sein. Ob dies wirklich zutrifft, ist Thema dieses Artikels. Neben einer kurzen Einführung in die Funktionalität, sollen auch die Problem und Einschränkungen bei den aktuellen Versionen aufgezeigt werden.

1. Allgemeines zu Datenbank Audit

1.1 Übersicht

Je nach Sicherheitsanforderungen an eine Oracle Datenbank ist es erforderlich, gewisse Datenbankaktivitäten mit Auditing zu überwachen. Das Standardauditing lässt sich dabei einfach mit dem init.ora Parameter AUDIT_TRAIL einschalten. Dieser Parameter legt auch gleich fest, wo die Audit-Daten gespeichert werden. Die Tabelle 1 fasst die möglichen Werte für AUDIT_TRAIL kurz zusammen:

Wert	Beschreibung
NONE	Auditing ist ausgeschaltet. Dies ist der Standardwert, wenn die Datenbank nicht mit dem DBCA erstellt wurde. Wird die Datenbank mit dem DBCA erstellt, so werden „Enhanced default security settings“ gesetzt. Diese liessen sich vor 11g R2 noch explizit ausschalten.
OS	Audit-Daten werden als Text Dateien (*.aud) auf dem Betriebssystem unter AUDIT_FILE_DEST abgespeichert.
DB	Audit Datensätze werden direkt in der Datenbank Tabelle AUD$ bzw. FGA_LOG$ abgespeichert.
XML	Audit-Daten werden als XML Dateien (*.xml) auf dem Betriebssystem unter AUDIT_FILE_DEST abgespeichert.
XML, EXTENDED DB, EXTENDED	Speicherort analog DB bzw. XML mit erweiterten Audit Informationen.

Tabelle 1 AUDIT_TRAIL Parameter Werte

Im Weiteren lassen sich die Audit-Informationen unter Unix im SYSLOG bzw. unter Windows im Event Log abspeichern. DBMS_AUDIT_MGMT bietet in diesen Fällen keine Möglichkeit, die Audit-Daten zu verwalten.

Im Anschluss an die Einstellungen des AUDIT_TRAIL ist noch die Definition der zu überwachenden Statements, Privilegien und Objekte zu erstellen, damit Audit-Daten effektiv gesammelt werden.

1.2 Problematik des Audit Datenmanagement

Werden die Audit-Daten als .xml oder .aud Dateien auf dem Betriebssystem im Verzeichnis AUDIT_FILE_DEST abgelegt, lassen sich diese bei allen Oracle Versionen manuell mit OS Kommandos, sowie mithilfe von Shell Scripten einfach archivieren oder löschen. Dies funktioniert grundsätzlich unabhängig von der Datenbank. Beim Löschen ist lediglich darauf zu achten, dass die entsprechende Datei aktuell nicht in Verwendung ist, d.h. dass keine Audit-Informationen geschrieben werden.

Werden die Audit-Daten dagegen in der Datenbank abgelegt (AUDIT_TRAIL auf DB oder DB, EXTENDED), werden die Daten in der Tabelle AUD$ bzw. FGA_LOG$ gespeichert. Standardmässig liegen diese Tabellen im SYSTEM Tablespace. Solange diese Tabellen nur eine handvoll Datensätze enthält, ist dies unproblematisch. Je nachdem welche Statements, Privilegien und Objekte überwacht werden, entsteht bald einmal eine umfangreiche Ansammlung von Audit-Daten. Werden die AUDIT_TRAIL Tabellen grösser, wächst zwangsläufig auch der SYSTEM Tablespace. Wenn viele Audit-Daten gesammelt, nie oder selten gelöscht werden, können diese im Extremfall den Grossteil der effektiven Daten im SYSTEM Tablespace ausmachen. Neben negativen Einflüssen bei der Handhabung des SYSTEM Tablespaces, kann sich dies auch auf die Performance auswirken.

Bis einschliesslich Oracle 10g ist der einzige offizielle Ausweg die Daten in den Griff zu bekommen, diese regelmässig zu löschen. Dazu wird die Rolle DELETE_CATALOG_ROLE benötigt. Alternativ besteht auch die Möglichkeit, die AUDIT_TRAIL Tabellen in ein anderes Tablespace zu verschieben. Auf My Oracle Support findet man eine entsprechende Metalink Note[1], welche beschreibt wie die AUDIT_TRAIL Tabellen verschoben werden können. Gleichzeitig wird in dieser Note darauf hingewiesen, dass das manuelle Verschieben der Tabellen nicht unterstützt ist und man das neue Feature DBMS_AUDIT_MGMT verwenden soll.

2. DBMS_AUDIT_MGMT Package

2.1 Verfügbarkeit von DBMS_AUDIT_MGMT

DBMS_AUDIT_MGMT ist ab der Oracle Version 11.2.0.1 enthalten und kann ohne weiteres eingesetzt werden. Um DBMS_AUDIT_MGMT bei ältere Versionen zu verwenden, ist das Patchset 10.2.0.5 bzw. 11.1.0.7 einzuspielen. Für Oracle 10.2.0.3 und 10.2.0.4.x gibt es jeweils separate Patch's. Versionen vor Oracle 10.2.0.3 werden nicht mehr unterstützt. Mehr Informationen zu den Patchs findet man unter anderem in der Metalink Note "*New Feature DBMS_AUDIT_MGMT To Manage And Purge Audit Information [ID 731908.1]*". Entsprechend dieser Note benötigt man für die Verwendung von DBMS_AUDIT_MGMT in 10g R2 und 11g R1 zwingend eine Oracle Audit Vault Lizenz. Bei Oracle 11g R2 ist DBMS_AUDIT_MGMT Teil des Releases, so dass keine zusätzliche Oracle Audit Vault Lizenz benötig wird. Bei einem produktiven Einsatz ist es gegebenenfalls sinnvoll, die effektive Lizenz Situation mit Ihrem Oracle Software Lieferant abzuklären.

2.2 Funktionalitäten von DBMS_AUDIT_MGMT

Ist das Auditing einmal eingeschaltet, ist es Zeit eine vorgängig geplante Strategie für das Aufbewahren von Audit-Daten um zusetzten. Bei dieser Tätigkeit lässt sich die Arbeit bei folgenden Punkten mit DBMS_AUDIT_MGMT vereinfachen:

- AUDIT_TRAIL initialisieren
- AUDIT_TRAIL verschieben d.h. AUD$ bzw. FGA_LOG$ Tabelle mit den entsprechenden Abhängigkeiten in ein anderes Tablespace verschieben
- Löschen der archivierten Audit Datensätze
- Erstellen, ändern und löschen eines Purge Job's
- Setzen verschiedenen Parameter

[1] Moving AUD$ to Another Tablespace and Adding Triggers to AUD$ [ID 72460.1]

Die Tabelle 2 enthält einen Auszug der Prozeduren und Funktionen von DBMS_AUDIT_MGMT. Eine komplette Liste kann der Oracle Dokumentation[2] entnommen werden.

Prozedur / Funktion	Typ	Beschreibung
CLEAN_AUDIT_TRAIL	Prozedur	Löschen der archivierten AUDIT_TRAIL Datensätze
CREATE_PURGE_JOB	Prozedur	Erstellen eines Jobs zum Löschen der AUDIT_TRAIL Datensätze
DEINIT_CLEANUP	Prozedur	Rückgängig machen des Audit Setup's durch INIT_CLEANUP Prozedur
DROP_PURGE_JOB	Prozedur	Löschen eines Jobs zum Löschen der AUDIT_TRAIL Datensätze
INIT_CLEANUP	Prozedur	Initialisierung der Audit Management Infrastruktur und festlegen eines Standardintervall für das Aufräumen der AUDIT_TRAIL Datensätze
IS_CLEANUP_INITIALIZED	Funktion	Prüfen ob die INIT_CLEANUP Prozedur ausgeführt wurde
SET_AUDIT_TRAIL_LOCATION	Prozedur	Verschieben der AUDIT_TRAIL Tabellen (AUD$) in ein Benutzerdefiniertes Tablespace
SET_AUDIT_TRAIL_PROPERTY	Prozedur	Setzen der Eigenschaften von AUDIT_TRAIL
SET_LAST_ARCHIVE_TIMESTAMP	Prozedur	Setzen des Zeitpunktes, wann die Audit Datensätze letztmals archiviert wurden
SET_PURGE_JOB_INTERVAL	Prozedur	Intervall für den Löschjob festlegen
SET_PURGE_JOB_STATUS	Prozedur	Ein- und Ausschalten des Löschjobs

Tabelle 2 Auszug der DBMS_AUDIT_MGMT Prozeduren und Funktionen

Damit die Prozeduren und Funktionen von DBMS_AUDIT_MGMT verwendet werden können, benötigt man ein explizites EXECUTE Recht auf dem Package. Die Rolle SYSDBA besitzt dieses Recht ebenfalls. Es wird empfohlen, dieses Recht nur bewusst dem Audit Administrator zu vergeben, da sonst ungewollt Audit-Daten manipuliert bzw. gelöscht werden könnten.

Neben den Prozeduren und Funktionen gibt es zusätzlich 4 neue Data Dictionary Views. Anhand dieser Views können vorwiegend Informationen zur aktuellen AUDIT_TRAIL Konfiguration, den automatischen Lösch-Jobs sowie ausgeführten Aufräumarbeiten abgefragt werden. Die Namen der Views sowie eine kurze Beschreibung, kann der Tabelle 3 entnommen werden.

View	Beschreibung
DBA_AUDIT_MGMT_CLEANUP_JOBS	Konfigurierte AUDIT_TRAIL Lösch-Jobs
DBA_AUDIT_MGMT_CLEAN_EVENTS	Protokoll der Aufräumarbeiten
DBA_AUDIT_MGMT_CONFIG_PARAMS	Eigenschaften der AUDIT_TRAIL Typen
DBA_AUDIT_MGMT_LAST_ARCH_TS	Letzter Zeitstempel für das Löschen der AUDIT_TRAIL Datensätze

Tabelle 3 Audit Management Views

[2] Oracle Database PL/SQL Packages and Reference 11g Release 2, Kapitel 27 DBMS_AUDIT_MGMT

3. Management der Audit-Daten

3.1 Initialisierung des Audit-Managements

Um mit DBMS_AUDIT_MGMT arbeiten zu können, muss die Audit Management Infrastruktur als erstes mit *INIT_CLEANUP* initialisiert werden. Dabei werden neben einem Standard Cleanup Intervall, auch die AUDIT_TRAIL Tabellen vom SYSTEM Tablespace in das SYSAUX Tablespace verschoben. Will man das nicht, müssen die Tabellen vorgängig mit *SET_AUDIT_TRAIL_LOCATION* in ein entsprechendes Tablespace verschoben werden. Je nach Oracle Version muss man immer zuerst einmal *INIT_CLEANUP* ausführen, bevor man mit *SET_AUDIT_TRAIL_LOCATION* die Tabellen in das eigentliche Tablespace verschieben kann.

Situation vor der Initialisierung:

```
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
```

Initialisieren der Audit Management Infrastruktur:

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

Situation nach der Initialisierung:

```
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
```

In diesem Beispiel wurde jeweils mit dem AUDIT_TRAIL des Standardauditing gearbeitet. Weiter werden bei AUDIT_TRAIL_TYPE folgende Typen unterschieden:

- AUDIT_TRAIL_ALL, alle Typen d.h. die Datenbank Audit Tabellen (AUD$ und FGA_LOG$) sowie die Audit-Daten auf dem Betriebssystem (OS und XML)
- AUDIT_TRAIL_AUD_STD, nur die Standardauditing Tabelle
- AUDIT_TRAIL_DB_STD, die Tabelle für das Standardauditing (AUD$) und das Fine Grained Audit (FGA_LOG$)
- AUDIT_TRAIL_FGA_STD, nur die Tabelle für das Fine Grained Audit
  AUDIT_TRAIL_FILES, Audit-Daten auf dem Betriebssystem (OS und XML)
- AUDIT_TRAIL_OS, Audit-Daten auf dem Betriebssystem als Text Dateien
- AUDIT_TRAIL_XML Audit-Daten auf dem Betriebssystem als XML Dateien

Die verschieden AUDIT_TRAIL Typen besitzen jeweils unterschiedliche Eigenschaften. So lässt sich beispielsweise bei den Datei Typen die maximale Grösse einer Audit-Datei, oder die Zeitdauer wie lange eine Audit-Datei geöffnet ist, festlegen. Beide Tabellen AUD$ und FGA_LOG$ können dagegen, je nach Bedürfnis, in unterschiedliche Tablespaces verschoben werden.

3.2 Verschieben der Audit-Daten

Sollen die Audit-Daten in ein benutzerspezifischen Tablespace verschoben werden, erfolgt dies mit der Prozedur *SET_AUDIT_TRAIL_LOCATION*. Je nach dem wie gross die Audit Tabellen bereits sind, kann dies einen Moment in Anspruch nehmen, da die Daten effektiv physisch verschoben werden. Beim Aufruf dieser Prozedur ist wichtig vorgängig sicher zu stellen, dass im Ziel Tablespace entsprechend genügend Platz vorhanden ist. Das folgende Beispiel zeigt, wie beide Audit Tabellen (AUD$ und FGA_LOG$) verschoben werden.

```
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;
/
```

Die Prozedur für das Verschieben der Audit-Daten kann nicht auf die AUDIT_TRAIL Typen AUDIT_TRAIL_FILES, AUDIT_TRAIL_OS und AUDIT_TRAIL_XML angewendet werden. Bei diesen Typen wird die Ablage der Audit-Daten weiterhin mit dem Parameter AUDIT_FILE_DEST festgelegt.

3.3 Löschen der Audit-Daten

Das Löschen der Audit-Daten erfolgt entweder manuell mit *CLEAN_AUDIT_TRAIL* oder mit einem regelmässigen Lösch-Job. Unabhängig davon, ob das Löschen manuell oder mit einem Job erfolgt, gibt es zwei unterschiedliche Arten wie die Audit-Daten gelöscht werden. Entweder werden alle Audit-Datensätze gelöscht oder nur die archivierten Datensätze. Damit bekannt ist, welche Datensätze archiviert wurden, ist beim Archivieren mit *SET_LAST_ARCHIVE_TIMESTAMP* explizit ein Zeitstempel zu setzten. Dass heisst die Archivierung ist weiterhin Aufgabe des Audit oder Datenbank Administrators und muss mit Hilfe eigener Scripte oder Tools wie Audit Vault, etc. sichergestellt werden.

Ein solcher Archivierungs-Zeitstempel kann wie folgt definiert werden:

```
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;
/
```

Mit *CLEAR_LAST_ARCHIVE_TIMESTAMP* kann ein zuvor gesetzter Archivierungs-Zeitstempel wieder gelöscht werden.

```
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
SYSTEM    LOGON        27-SEP-10 11.28.39.565309 PM +00:00             0
SYSTEM    LOGOFF       27-SEP-10 11.28.46.299682 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.
```

Ist der Archivierungs-Zeitstempel gesetzt, lassen sich alle Audit-Datensätze, welche älter sind, löschen:

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

select USERNAME,ACTION_NAME,EXTENDED_TIMESTAMP ,RETURNCODE
from DBA_AUDIT_SESSION order by 3;



USERNAME  ACTION_NAME  EXTENDED_TIMESTAMP                          RETURNCODE
--------- ------------ ----------------------------------- ----------
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

3 rows selected.
```

Wird USE_LAST_ARCH_TIMESTAMP auf FALSE gesetzt, werden alle Audit-Datensätze gelöscht. Der Standard Wert von USE_LAST_ARCH_TIMESTAMP ist TRUE.

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

select USERNAME,ACTION_NAME,EXTENDED_TIMESTAMP ,RETURNCODE
from DBA_AUDIT_SESSION order by 3;

no rows selected
```

3.4 Definition automatischer Lösch Jobs

Mit der Prozedur *CREATE_PURGE_JOB* lässt sich ein regelmässiger Job für das Löschen der Audit-Daten erstellen. Auch hier kann man wiederum mit dem Archivierungs-Zeitstempel arbeiten. Auf diese Weise wird sichergestellt, dass noch nicht archivierte Daten nicht gelöscht werden. Der Job wird wie folgt erstellt:

```
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;
/
```

Je nach Anforderung können verschiede Jobs erstellt werden. Z.B. für das tägliche Bereinigen des AUDIT_TRAIL, sowie ein monatlicher Job der alles löscht. Informationen zu den Jobs können in der View DBA_AUDIT_MGMT_CLEANUP_JOBS oder in der View DBA_SCHEDULER_JOBS abgefragt werden.

```
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
```

Mit *SET_PURGE_JOB_INTERVAL* kann der Job Intervall angepasst werden. Bestehende Jobs können mit *SET_PURGE_JOB_STATUS* zeitweilig ausgeschaltet oder mit *DROP_PURGE_JOB* gelöscht werden.

4. Einschränkungen

4.1 Fehlende Funktionalität und Einschränkungen

DBMS_AUDIT_MGMT hat zwei grundlegende Einschränkungen, welche auf den ersten Blick als fehlende Funktionen aufgefasst werden könnten, bei genauer Betrachtung aber durchwegs Sinn machen. So ist es z.B. nicht möglich die AUDIT Informationen vom SYS zu löschen. Dass heisst wird in der Datenbank AUDIT_SYS_OPERATIONS eingeschaltet, so werden entsprechende .aud Text Dateien im AUDIT_FILE_DEST abgelegt. Ähnlich wie dies auch der Fall ist, wenn AUDIT_TRAIL = OS ist. Diese Dateien müssen wie bis anhin mit entsprechenden Scripten bzw. Betriebssystem-Kommandos weiterverarbeitet werden. Sollen die SYS Tätigkeiten überwacht werden, ist es grundsätzlich sinnvoll, wenn SYS nicht seine eigenen Audit-Daten „verwalten" kann. Diese Daten könnten zum Beispiel durch einen Audit Administrator weiterverarbeitet werden.
Die zweite Einschränkung betrifft den Fall, wenn die Audit-Daten an syslog auf Unix bzw. an das Event Log auf Windows geschickt werden. In beiden Fällen verlassen die Daten die Oracle Datenbank und können bzw. müssen aus der Sicht der Datenbank nicht mehr weiterverarbeitet werden.
Neben den Einschränkungen, gibt es auch Funktionen, die man vermisst. So wäre hilfreich, wenn es weitere Prozeduren im Zusammenhang mit dem Archivieren der Audit-Daten geben würde. Hier ist man bis auf weiteres auf eigene Scripte und Lösungen angewiesen, wenn man nicht Tools wie Oracle Audit Vault einsetzen kann.

4.2 Probleme und Known Issues

DBMS_AUDIT_MGMT weist in den Versionen bis 11.1.0.7 diverse Bug's auf, welche einen produktiven Einsatz z.T. stark einschränken. So besteht z.B. ein Problem beim Löschen der Audit-Dateien, wenn die ORACLE_SID in Grossbuchstaben ist. Die Dateien können in dem Fall gar nicht gelöscht werden. Ähnliche Bugs gibt es auch im Zusammenhang mit den Audit Tabellen. Anbei eine kurze Zusammenstellung einiger Bugs:

- *Bug 8421069* DBMS_AUDIT_MGMT.SET_AUDIT_TRAIL_LOCATION does not move the lob segments
- *Bug 7427320* Audit file switches before it reaches 1k (FILE_MAXSIZE not set)
- *Bug 8598843* DBMS_AUDIT_MGMT.CLEAN_AUDIT_TRAIL should clean up entries in adx_sid.txt
- *Bug 9164488* CLEAN_AUDIT_TRAIL doesn't delete SYS.AUD$ and SYS.FGA_LOG$ tables
- *Bug 9438890* CLEAN_AUDIT_TRAIL does not work for AUDIT_TRAIL = OS with uppercase ORACLE_SID

Die meisten Bug's werden mit 11.2.0.2 behoben. Aus diesem Grund empfehlen wir den Einsatz von DBMS_AUDIT_MGMT ausschliesslich ab Oracle 11.2.0.2. Weitere Informationen zu den Known Issues findet man auch in der Metalink Note *„Known Issues When Using: DBMS_AUDIT_MGMT [ID 804624.1]"*.

5. Fazit

Mit DBMS_AUDIT_MGMT werden dem DBA verschiedene Verwaltungs- und Administrations-Arbeiten erleichtert. Oracle bietet zudem erstmals eine offizielle Möglichkeit, die AUDIT_TRAIL Tabellen in ein anderes Tablespace zu verschieben. Leider gibt es noch den einen oder anderen Bug, welcher die Funktionalität von DBMS_AUDIT_MGMT teilweise stark einschränkt. Viele der Bugs werden bereits mit dem Patchset 11.2.0.2 behoben. Nichts desto trotz empfehlen wir vor einem produktiven Einsatz von DBMS_AUDIT_MGMT entsprechende Tests durchzuführen sowie das aktuellste Patchset einzuspielen.
Auch wenn mit dem DBMS_AUDIT_MGMT die Verwaltung der Audit-Daten vereinfacht wird, bleibt aber weiterhin die Frage: „Was soll überwacht werden?“, „Wie lange werden die Daten aufbewahrt?“ und „Wie können die Daten ausgewertet werden?“. Als Antwort auf die erste Frage liefert Oracle mit den „Enhanced default security settings“ ein erstes Set von entsprechenden Audit-Einstellungen, welche aber sicher an die eigenen Anforderungen und Bedürfnisse anzupassen sind.
Bei der Frage der Aufbewahrung und Auswertung bietet Oracle lediglich Oracle Audit Vault als Lösung an. Je nach Infrastruktur und Umgebung, für welche Audit-Informationen gesammelt werden sollen, können hohe Lizenz- und Projektkosten entstehen. Als Alternative bleiben nur Produkte wie Sentrigo Hedgehog oder die Entwicklung einer eigenen Lösung für die Auswertung der AUDIT_TRAIL Informationen. Die Definition und Umsetzung eines Audit Konzeptes ist nicht trivial und beinhaltet einige Herausforderungen.

Wir unterstützen und beraten Sie bei diesem Thema aber gerne.

Stefan Oehrli
Trivadis AG
Europa-Strasse 5 Tel: +41-44-808 70 20
CH-8152 Glattbrugg Fax: +41-44-808 70 21
Internet: www.trivadis.com Mail: info@trivadis.com

Literatur und Links

- Metalink Note [ID 72460.1] : Moving AUD$ to Another Tablespace and Adding Triggers to AUD$
- Metalink Note [ID 731908.1] : New Feature DBMS_AUDIT_MGMT To Manage And Purge Audit Information
- Metalink Note [ID 804624.1] : Known Issues When Using: DBMS_AUDIT_MGMT
- Oracle® Database PL/SQL Packages and Types Reference, 11g Release 2 (11.2), Part Number E16760-04
- www.trivadis.com