Audit Management mit DBMS_AUDIT_MGMT

Stefan Oehrli, Senior Consultant, Trivadis AG, Glattbrugg, Schweiz

Mit der Datenbank 11*g* 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, in denen DBAs eigene Scripts und Jobs für die Organisation von Audit-Daten entwickeln müssen, scheinen gezählt zu sein. Der Artikel zeigt, ob dies tatsächlich zutrifft. Neben einer kurzen Einführung in die Funktionalität sind auch die Probleme und Einschränkungen bei den aktuellen Versionen aufgezeigt.

Bei bestimmten Sicherheitsanforderungen ist es erforderlich, gewisse Datenbank-Aktivitäten mit Auditing zu überwachen. Das Standard-Auditing lässt sich dazu einfach mit dem „init.ora"-Parameter „AUDIT_TRAIL" einschalten. Dieser legt auch gleich fest, wo die Audit-Daten gespeichert sind. Tabelle 1 fasst die möglichen Werte zusammen.

Die Audit-Informationen lassen sich außerdem unter Unix im SYSLOG beziehungsweise unter Windows im Event-Log abspeichern. DBMS_AUDIT_MGMT bietet in diesen beiden Fällen keine Möglichkeit, die Audit-Daten zu verwalten. Im Anschluss an die Einstellungen des „AUDIT_TRAIL"-Parameters ist noch die Definition der zu überwachenden Statements, Privilegien und Objekte zu erstellen, damit die Audit-Daten effektiv gesammelt werden.

Problematik des Audit-Datenmanagements

Sind die Audit-Daten als „.xml"- oder „.aud"-Dateien auf dem Betriebssystem im Verzeichnis „AUDIT_FILE_DEST" abgelegt, kann man diese bei allen Oracle-Versionen manuell mit OS-Kommandos sowie mithilfe von Shell-Skripten 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, das heißt, dass gerade keine Audit-Informationen geschrieben werden.

Sind die Audit-Daten dagegen in der Datenbank abgelegt (AUDIT_TRAIL auf DB oder DB EXTENDED), werden sie in der Tabelle „AUD$" beziehungsweise „FGA_LOG$" gespeichert. Standardmäßig liegen diese Tabellen im SYSTEM-Tablespace. Solange diese Tabelle nur wenige Datensätze enthält, ist dies unproblematisch. Je nachdem, welche Statements, Privilegien und Objekte überwacht werden, entsteht jedoch bald eine umfangreiche Ansammlung von Audit-Daten. Wachsen die AUDIT_TRAIL-Tabellen an, vergrößert sich zwangsläufig auch der SYSTEM-Tablespace. Wenn man viele Audit-Daten sammelt und nie oder nur selten löscht, können diese im Extremfall den Großteil der effektiven Daten im SYSTEM-Tablespace ausmachen. Neben negativen Einflüssen bei der Handhabung des SYSTEM-Tablespace kann sich dies auch auf die Performance auswirken.

Bis einschließlich der Datenbank 10*g* ist der einzige offizielle Ausweg, um die Daten in den Griff zu bekommen, diese regelmäßig zu löschen. Dazu ist die Rolle „DELETE_CATALOG_ROLE" erforderlich. 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 (Moving AUD$ to Another Tablespace and Adding Triggers to AUD$ [ID 72460.1]), welche beschreibt, wie die AUDIT_TRAIL-Tabellen verschoben werden können. Gleichzeitig weist diese Note darauf hin, dass das manuelle Verschieben der Tabellen nicht unterstützt ist und man das neue Feature „DBMS_AUDIT_MGMT" verwenden soll.

Verfügbarkeit von DBMS_AUDIT_MGMT

DBMS_AUDIT_MGMT ist ab der Version 11.2.0.1 enthalten und kann ohne Weiteres eingesetzt werden. Um die Funktion auch bei älteren Versionen verwenden zu können, ist das Patchset 10.2.0.5 beziehungsweise 11.1.0.7 einzuspielen. Für Oracle 10.2.0.3 und 10.2.0.4.x existieren jeweils separate Patches. Versionen vor 10.2.0.3 sind nicht mehr unterstützt. Weitere Informationen zu den Patches findet man

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 11*g* 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$ beziehungsweise 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 beziehungsweise XML mit erweiterten Audit-Informationen.

Tabelle 1: Werte des „AUDIT_TRAIL"-Parameters

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	Rückgängigmachen des Audit Setups durch die 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 Standardintervalls 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 Zeitpunkts, an dem die Audit-Datensätze letztmals archiviert wurden
SET_PURGE_JOB_INTERVAL	Prozedur	Intervall für den Lösch-Job festlegen
SET_PURGE_JOB_STATUS	Prozedur	Ein- und Ausschalten des Lösch-Jobs

Tabelle 2: Auszug der DBMS_AUDIT_MGMT-Prozeduren und -Funktionen

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

unter anderem in einer Metalink Note (New Feature DBMS_AUDIT_MGMT To Manage And Purge Audit Information [ID 731908.1]). Entsprechend dieser benötigt man für die Verwendung von DBMS_AUDIT_MGMT in 10*g* R2 und 11*g* R1 zwingend eine Audit-Vault-Lizenz. Bei Oracle 11*g* R2 ist DBMS_AUDIT_MGMT Teil des Release, sodass diese nicht mehr erforderlich ist. Bei einem produktiven Einsatz ist es gegebenenfalls sinnvoll, die effektive Lizenz-Situation mit dem Software-Lieferanten abzuklären.

Funktionalitäten von DBMS_AUDIT_MGMT

Ist das Auditing einmal eingeschaltet, ist es an der Zeit, eine zuvor geplante Strategie für das Aufbewahren von Audit-Daten umzusetzen. Dabei vereinfacht DBMS_AUDIT_MGMT die Arbeit in folgenden Punkten:

- AUDIT_TRAIL initialisieren
- AUDIT_TRAIL verschieben, das heißt, AUD$- beziehungsweise FGA_LOG$-Tabelle mit den entsprechenden Abhängigkeiten in ein anderes Tablespace verschieben
- Löschen der archivierten Audit-Datensätze
- Erstellen, Ändern und Löschen eines Purge-Jobs
- Setzen verschiedener Parameter

Tabelle 2 zeigt einen Auszug der Prozeduren und Funktionen von DBMS_AUDIT_MGMT. Die komplette Liste steht in der Oracle-Dokumentation (Oracle Database PL/SQL Packages and Reference 11g Release 2, Kapitel 27 DBMS_AUDIT_MGMT).

Um die Prozeduren und Funktionen von DBMS_AUDIT_MGMT verwenden zu können, ist ein explizites EXECUTE-Recht auf dem Package erforderlich. Die Rolle „SYSDBA“ besitzt dieses Recht ebenfalls. Es wird empfohlen, dieses Recht bewusst nur dem Audit-Administrator zu geben, da sonst ungewollt Audit-Daten manipuliert beziehungsweise gelöscht werden könnten.

Neben den Prozeduren und Funktionen gibt es zusätzlich vier neue Data-Dictionary-Views. Diese zeigen vorwiegend Informationen zur aktuellen AUDIT_TRAIL-Konfiguration, den automatischen Lösch-Jobs sowie ausgeführten Aufräumarbeiten (siehe Tabelle 3).

Initialisierung des Audit-Managements

Um mit DBMS_AUDIT_MGMT arbeiten zu können, ist als Erstes die Audit-Management-Infrastruktur mit „INIT_CLEANUP“ zu initialisieren. Dabei werden neben einem Standard-Cleanup-Intervall, auch die AUDIT_TRAIL-Tabellen vom SYSTEM-Tablespace in das SYSAUX-Tablespace verschoben. Will man das nicht, sind die Tabellen zuvor mit „SET_AUDIT_TRAIL_LOCATION“ in ein entsprechendes Tablespace zu verschieben; je nach Oracle-Version ist zuerst „INIT_CLEANUP“ auszuführen. Das Beispiel zeigt die 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
```

Dann folgt das 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;
/
```

Jetzt die 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 Standard-Auditing gearbeitet. Bei AUDIT_TRAIL_TYPE unterscheidet man folgende Typen:

- AUDIT_TRAIL_ALL: Alle Typen, das heißt, die Datenbank-Audit-Tabellen (AUD$ und FGA_LOG$) sowie die Audit-Daten auf dem Betriebssystem (OS und XML)
- AUDIT_TRAIL_AUD_STD: Nur die Standard-Auditing-Tabelle
- AUDIT_TRAIL_DB_STD: Die Tabelle für das Standard-Auditing (AUD$) 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 verschiedenen Typen besitzen jeweils eigene Eigenschaften. So lassen 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.

Verschieben der Audit-Daten

Die Prozedur „SET_AUDIT_TRAIL_LOCATION“ verschiebt die Audit-Daten in ein benutzerspezifisches Tablespace. Je nachdem, wie groß die Audit-Tabellen bereits sind, kann dies entsprechend dauern, da die Daten physisch verschoben werden. Vor dem Aufruf dieser Prozedur ist sicherzustellen, dass im Ziel-Tablespace genügend Platz vorhanden ist. Das folgende Beispiel zeigt das Verschieben der beiden Audit-Tabellen (AUD$ und FGA_LOG$):

```
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;
/
```

Diese Prozedur ist auf die AUDIT_TRAIL-Typen „AUDIT_TRAIL_FILES“, „AUDIT_TRAIL_OS“ und „AUDIT_TRAIL_XML“ nicht anwendbar. Hier wird die Ablage der Audit-Daten weiterhin mit dem Parameter „AUDIT_FILE_DEST“ festgelegt.

Löschen der Audit-Daten

Das Löschen der Audit-Daten erfolgt entweder manuell über „CLEAN_AUDIT_TRAIL“ oder mit einem regelmäßigen Lösch-Job. Unabhängig davon gibt es zwei unterschiedliche Arten des Löschens – entweder werden alle Audit-Datensätze oder nur die archivierten Datensätze entfernt. Damit bekannt ist, welche Datensätze archiviert sind, wird beim Archivieren mit „SET_LAST_ARCHIVE_TIMESTAMP“ explizit ein Zeitstempel gesetzt. Das bedeutet, die Archivierung ist weiterhin Aufgabe des Audit- oder Datenbank-Administrators und muss mithilfe eigener Skripte oder Tools wie Audit Vault sichergestellt sein. Das Beispiel zeigt die Definition eines solchen Archivierungs-Zeitstempels:

```
BEGIN
  DBMS_AUDIT_MGMT. SET_LAST_AR-
CHIVE_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;
/
```

„CLEAR_LAST_ARCHIVE_TIMESTAMP“ löscht einen zuvor gesetzten Archivierungs-Zeitstempel wieder (siehe Listing, nächste Seite oben).

Wussten Sie schon?

Über Ihr Profil wählen Sie, welche Informationen Sie von der DOAG per E-Mail erhalten.
www.doag.org/go/profil

```
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.
```

Danach lassen sich alle älteren Audit-Datensätze 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.
```

Ist „USE_LAST_ARCH_TIMESTAMP“ auf „FALSE“ gesetzt, werden alle Audit-Datensätze gelöscht. Der Standard-Wert 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
```

Automatische Lösch-Jobs

Die Prozedur „CREATE_PURGE_JOB“ erstellt einen regelmäßigen Job für das Löschen der Audit-Daten. Auch hier kann man mit dem Archivierungs-Zeitstempel arbeiten. Auf diese Weise ist sichergestellt, dass noch nicht archivierte Daten nicht gelöscht werden. Der Job wird wie folgt erstellt:

```
BEGIN
  DBMS_AUDIT_MGMT.CREATE_PUR-
GE_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;
```

Einschränkungen

DBMS_AUDIT_MGMT besitzt zwei grundlegende Einschränkungen, die auf den ersten Blick als fehlende Funktionen aufgefasst werden könnten, bei genauer Betrachtung aber einen Sinn ergeben. So ist es nicht möglich, die AUDIT-Informationen vom SYS zu löschen. Dass heißt, beim Aktivieren von „AUDIT_SYS_OPERATIONS“ werden entsprechende „.aud“-Textdateien im „AUDIT_FILE_DEST“ abgelegt. Ähnlich ist auch der Fall bei „AUDIT_TRAIL=OS“. Diese Dateien müssen mit entsprechenden Skripten beziehungsweise Betriebssystem-Kommandos weiterverarbeitet werden. Zum Überwachen der SYS-Tätigkeiten ist es grundsätzlich sinnvoll, wenn SYS nicht seine eigenen Audit-Daten verwalten kann. Diese könnten zum Beispiel durch einen Audit-Administrator weiterverarbeitet werden.

Die zweite Einschränkung betrifft den Fall, dass die Audit-Daten an „syslog“ auf Unix beziehungsweise an das Event-Log auf Windows geschickt werden. In beiden Fällen verlassen die Daten die Oracle-Datenbank und können beziehungsweise müssen aus Sicht der Datenbank nicht mehr weiterverarbeitet werden.

Neben diesen Einschränkungen gibt es auch Funktionen, die man vermisst. So wären weitere Prozeduren im Zusammenhang mit dem Archivieren der Audit-Daten hilfreich. Hier ist man bis auf Weiteres auf eigene Skripte und Lösungen angewiesen, wenn man nicht Tools wie Audit Vault einsetzen kann.

Probleme bekannte Fehler

DBMS_AUDIT_MGMT weist in den Versionen bis 11.1.0.7 diverse Bugs auf, die einen produktiven Einsatz teilweise stark einschränken. So besteht ein Problem beim Löschen der Audit-Dateien, wenn die „ORACLE_SID“ in Großbuchstaben geschrieben ist. Die Dateien lassen sich dann nicht löschen. Ähnliche Bugs gibt es auch im Zusammenhang mit den Audit-Tabellen. Nachfolgend einige 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 davon sind mit 11.2.0.2 behoben. Aus diesem Grund ist der Einsatz von DBMS_AUDIT_MGMT erst ab 11.2.0.2 empfohlen. Weitere Informationen dazu auch in einer Metalink Note (Known Issues When Using: DBMS_AUDIT_MGMT [ID 804624.1]).

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 bis zum Patchset 11.2.0.2 noch den einen oder anderen Bug, der die Funktionalität von DBMS_AUDIT_MGMT teilweise stark einschränkt. Vor einem produktiven Einsatz von DBMS_AUDIT_MGMT sind entsprechende Tests des aktuellsten Patchsets dringend empfohlen.

Auch wenn mit dem DBMS_AUDIT_MGMT die Verwaltung der Audit-Daten vereinfacht wird, bleiben weiterhin die Fragen „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, die aber 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 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-Konzepts ist nicht trivial und beinhaltet einige Herausforderungen.

Kontakt:
Stefan Oehrli
stefan.oehrli@trivadis.com