Audit Vault – Erfahrungen aus der ersten deutschen Produktivumgebung

Volker Mach
MT AG
40882 Ratingen

Schlüsselworte:

Datenbanksicherheit, Überwachung

Einleitung

„Audit; von lateinisch audit: „er/sie hört"; sinngemäß: „er/sie überprüft"; werden in der Informationstechnik (IT) Maßnahmen zur Risiko- und Schwachstellenanalyse (engl. Vulnerability Scan) eines IT-Systems oder Computerprogramms bezeichnet. (Quelle: http://de.wikipedia.org/wiki/IT-Sicherheitsaudit)“

Die Frage, wer hat wann auf meine Daten zugegriffen und sie eventuell verändert, wird immer häufiger gestellt. Wie aber baut man ein vernünftiges Audit-System auf?

Dieser Frage sind wir im Rahmen eines Audit-Projekts für Oracle Datenbanken bei einem Kunden im Bankenumfeld nachgegangen und mussten feststellen, dass nicht das Produzieren der Audit-Daten schwierig ist, sondern die sinnvolle Auswertung der Daten und der Schutz vor Manipulation an diesen. Wir haben uns für das Produkt Audit Vault entschieden, da dieses den Anforderungen am besten gerecht wurde. Natürlich musste auch hier eine vernünftige Basis der Datenbankadministration geschaffen werden, wie zum Beispiel personalisierte Benutzer auf Betriebssystemebene, um beim Auditieren auch den Betriebssystem-Benutzer erkennen zu können.

Nachdem schon einige Erfahrungen mit Testinstallationen des Produktes Audit Vault gesammelt wurden, haben wir beim ersten produktiven Einsatz von Audit Vault in Deutschland auch viele neue Hürden und Überraschungen erlebt. In diesem Beitrag wird die notwendige Basis für den Einsatz dieses Produktes erläutert und wie man ein optimales Regelwerk für das Auditieren von Datenbankobjekten erstellen kann.

Wie funktioniert Audit Vault?

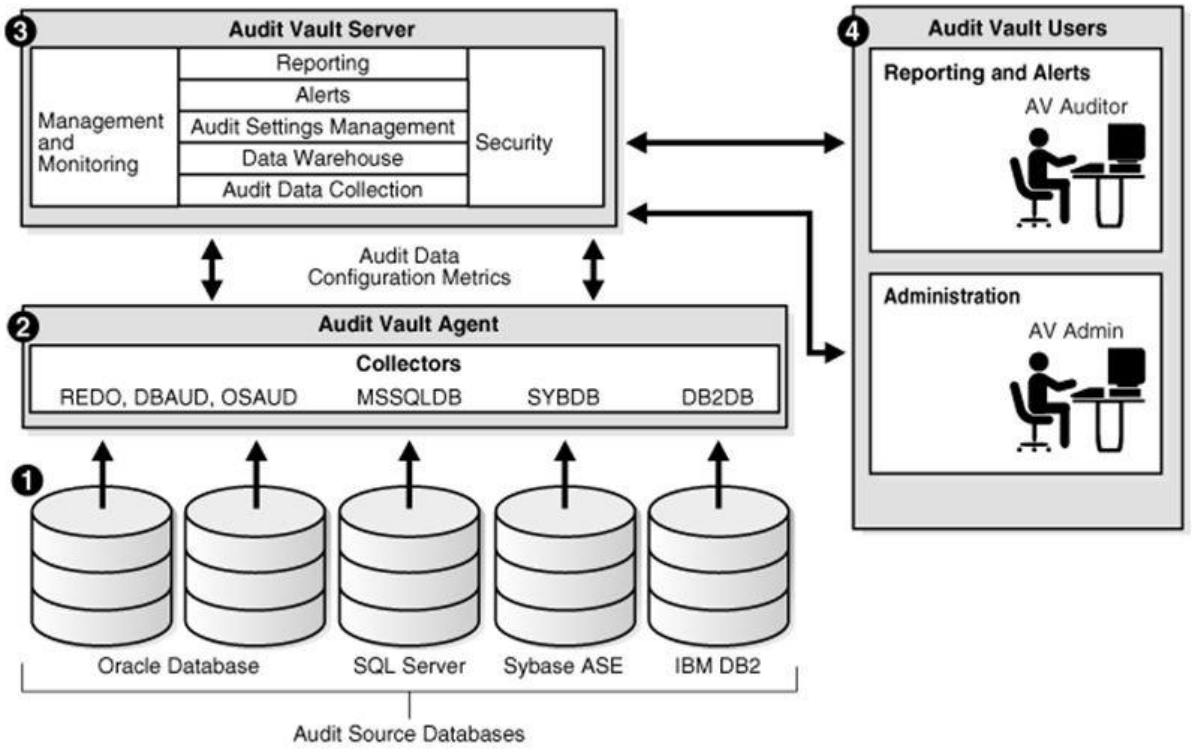

Abb. 1: Schematische Darstellung Audit Vault

Sogenannte „Kollektoren“ sammeln auf den einzelnen Datenbankservern die Auditereignisse und transportieren diese auf den Audit Vault Server.

Die „Kollektoren“ werden als Audit Vault Agenten in einem serperaten Verzeichnis auf den zu auditierenden Server installiert. Auf dem Audit Vault Server werden die gesammelten Auditereignisse dann in eine Oracle Datenbank geschrieben und mit der Datenbankfunktion „Database Vault“ direkt vor Manipulation geschützt. Standardmäßig werden die Auditereignisse für 10 Jahre vorgehalten.

Für die Auswertung dieser Auditereignisse bietet Oracle Audit Vault ein webbasiertes Auswertungstool inklusive eines Dashboards für den schnellen Überblick . Zusätzlich besteht aber auch die Möglichkeit mit dem Oracle BI oder dem Oracle BAM Active Viewer individuelle Reports für die Auswertung zu bauen. In unserem Projekt wurden die Reports mit dem Oralce BI nach Vorlage der Revision erstellt und bei Bedarf angepasst.

Abb. 2: Dashboard Audit Vault

Bevor es in unserem Projekt an die Erstellung der einzelnen Auditregeln ging, mussten organisatorische Rollen für das Auditkonzept festgelegt werden.

Auf der reinen Monitoringebene wurden folgende Rollen Personen zugeordnet:

<u>Auditor</u>

Verantwortlich für die Auswertung der erstellten Auditreports

<u>Audit Administrator</u>

Verantwortlich Erstellung der Regeln nach Vorgabe der Revision

Auf der Ebene der Administration war folgende Rolle zu vergeben:

<u>Audit Vault Administrator</u>

Verantwortlich für die Konfiguration, Pflege (Patches und Updates) und Sicherheit (Sicherheitsupdates)

Die einzelen Rollen wurden hierbei nach dem „Vier-Augen“-Prinzip eingerichtet, so dass immer eine Person aus der Monitoringebene mit einem Mitarbeiter auf der administrativen Ebene zusammen gelegt wurde.

Nachdem die Verteilung der Rollen abgeschlossen war, wurden in Abstimmung der Revision Regeln für das eigentliche Auditing erstellt .

Als Vorgabe sollten alle „Rating“-relevanten Tabellen des Kunden bei DML und DDL Operationen auditiert werden. Da der Eigentümer der „Rating“-relevanten Tabellen in der Datenbank die DBA-Rolle hatte, haben wir uns für das „Fine Grained Auditing“ entschieden.

Beispiel „Fine Grained Auditing“ :

```
DBMS_FGA.ADD_POLICY (
object_schema => 'RATING',
object_name => 'RATING_TAB',
policy_name => 'FGA_RATING_TAB',
audit_condition => 'USER="RATING‘‘‘',
audit_column => NULL,
handler_schema => NULL,
handler_module => NULL,
enable => TRUE,
statement_types => 'UPDATE, DELETE, SELECT',
audit_trail => DBMS_FGA.XML + DBMS_FGA.EXTENDED);
```

Weitere Themen im Vortrag:

-Personalisierung der Datenbankadministratoren
-SYSDBA Auditing
-Verwendung des “XML, EXTENDED”
-Package DBMS_AUDIT_MGMT

Kontaktadresse:

Volker Mach
MT AG
Balcke-Dürr-Allee 9
D-40882 Ratingen

Telefon: +49 (0) 2102 309 6140
Fax: +49 (0) 2102 309 6150
E-Mail volker.mach@mt-ag.com
Internet: www.mt-ag.com