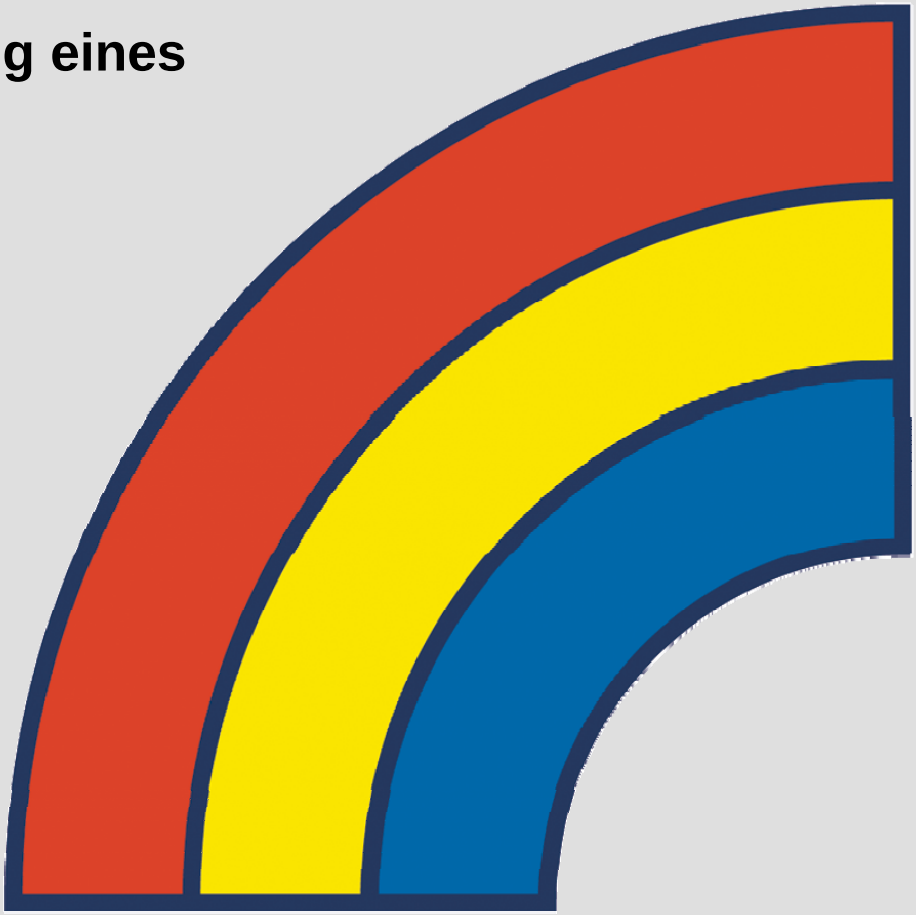
# Projekterfahrungen mit Oracle Audit Vault -

## Möglichkeit und Herausforderung eines zentralen Auditings



Jan-Peter Timmermann
Bereichsleiter

- **Betrieben werden ca. 145 Oracle Datenbanken**
  - Produktionssysteme, Pre-Produktionssysteme, Entwicklungssystem sowie Sicherungssysteme
- **Eigenentwicklungen**
  - Entwickler sitzen im Unternehmen und brauchen Zugriffe
- **Es werden 10 DBA‘s beschäftigt**
  - 24 mal 7 Stunden Betrieb muss abgedeckt sein
- **Ca. 6000 Benutzer greifen auf die selbst entwickelte Anwendung zu**
  - Teilweise mit „Power Usern“

- **Anforderung**
  - Im Rahmen von „Revisionen“ wird eine nachvollziehbare Protokollierung der Datenbank Zugriffen verlangt
    - Administratoren
    - Entwickler
    - „Power User“
  - Ebenso müssen Fehlgeschlagene Anmeldeversuche erkennbar sein

- **Nachvollziehbare Protokollierung**
  - Administrativen Benutzern
    - Connect sys as sysdba
    - Connect sys as sysoper
    - Tätigkeiten des Benutzers SYSTEM
  - Entwicklern
    - Greifen auf das Produktive System zu
  - Fehlerhaften Anmelde Versuchen
    - Gibt es Anmelde Versuche
  - Was sieht der „Power User“

- **Welche Möglichkeiten bietet Oracle für die Protokollierung von Benutzerzugriffen**
  - Alert.log
  - Logon Trigger
  - Selbst entwickelte Datenbank Trigger
  - Virtuell Private Database (unter vorbehalt )
  - Datenbank Audit

## Was kann auditiert werden

- **Per Default werden folgende Aktionen auditiert**
  - Verbindungen mit administrativen Rechten
    - Sysdba / sysoper
  - Starten und stoppen der Datenbank
  - Auditing administrativer User
  - Auditing weiterer User durch gezieltes einschalten

- **Was soll wie wohin protokolliert werden**
  - Auditing in das Dateisystem
    - Alle Zugriffe werden in das Dateisystem protokolliert
      - Alle Informationen des Auditings werden in definiertes Verzeichnis des Servers gelegt
  - Auditing in die Datenbank
    - Zugriffe werden innerhalb der Datenbank gesammelt
      - System Tabellen die per SQL ausgewertet werden können

- **Anhand eines Beispieles soll erläutert werden wie sich die Einträge für das Audit darstellen**
  - Erfolgreiches Anmelden eines Benutzers

Mon Jan 7 16:25:02 2008
SESSIONID: "110026" ENTRYID: "1" STATEMENT: "1" USERID: “DBUser" USERHOST: "IN\OC7675JPT" TERMINAL: “LAPHH80“
ACTION: "100" RETURNCODE: "0" COMMENT$TEXT: "Authenticated by: DATABASE; Client address: ADDRESS=(PROTOCOL=tcp)(HOST=192.168.30.64)(PORT=1522))“ OS$USERID: “jpt345se" PRIV$USED: 5

  - Die zunächst relevanten Einträge sind “USERID”, “USERHOST“, „ACTION“, „PRIV$USED“. Hiermit lässt sich sofort darstellen, wer von welchem Client aus welchen Befehl benutzt hat. Ein User „DBUser“ vom Client „N\OC7675JPT “ hat sich eingloggt (Action=100) und dazu das Privileg „create session“ (PRIV$USED=5) benutzt.

- **Sehr viel Informationen**
  - Sehr viel Informationen in der Datenbank oder im Dateisystem
  - Immer nur direkt in einer Datenbank oder einem Dateisystem
- **Zentrales sammeln der Daten**
  - Kopieren der Informationen auf einen Zentralen Server
  - Regelmäßiges Archivieren der Datenbank Informationen

- **Zentrale Ablage der Auditdaten**
  - Da die Audit Daten in einem definierten Verzeichnis auf den einzelnen Servern liegen, können diese in zyklischen Abständen auf einen Logserver kopiert werden
- **Anwachsen des System Tablespaces**
  - Bei einem Auditing über die Datenbank muss darauf geachtet werden, das die System Tabellen in regelmäßigen Abständen Archiviert werden.

- **Verwertung der Daten**
  - Aus diesem Vorgehen ergibt sich, dass eine ganze Reihe an strukturierten Informationen vorliegen, diese müssen gesammelt und ausgewertet werden
- **Fragen die sich in diesem Zusammenhang ergeben haben**
  - Wo werden die Daten gesammelt
  - Wie kann man sie gegen Veränderungen schützen
  - Wie kann man sie sinnvoll auswerten

- **Verfeinern der Audit Informationen**

  - Fine-Grained Auditing dient zur spezifischeren Definition der Protokollierung von Zugriffen auf bestimmte – zu definierende - Daten einer Datenbank. Welche Datenbereiche dabei in Betracht kommen, hängt im Wesentlichen von den festgelegten Sicherheitsrichtlinien und der Datensensibilität ab.

  - Sogenannte Audit-Policies sind mit Tabellen verknüpft und werden aufgerufen, wenn auf die entsprechende Tabelle zugegriffen (bei SELECT, INSERT, UPDATE und DELETE) wird.

## Probleme

- **Datenschwemme**
  - Durch das erweitern der Audit Informationen werden noch mehr Daten gesammelt
- **Manipulation**
  - Die Anforderung der Datensicherheit wächst
- **Einrichten der Richtlinien**
  - Jede Richtline muss auf den einzelnen Servern umgesetzt werden

- **Vorteile von Database Vault**

  - Mit Database Vault lässt sich stärker kontrollieren, wann welcher Nutzer auf welche Applikationsdaten zugreifen darf
  - Wenn sogenannten REALMS und Regeln eingerichtet sind, wird es diesen Nutzern nicht mehr erlaubt sein auf die Daten zuzugreifen.
  - Um diese kostenpflichtige Option zu nutzen, müssen die Applikationen nicht angepasst werden.
  - Es gibt eine neue administrative Ebene, die die Regeln und Realms einrichten und überwachen muß.
  - Diese sollte nicht im Bereich der Datenbankadministration angesiedelt sein

  - Es werden hiermit Regeln erstellt und eingerichtet

- **Oracle Audit Vault**

  - konsolidierte Möglichkeit, sowohl das Standard-Auditing als auch das Fine Grained Auditing für verschiedene Datenbanken zu administrieren und auszuwerten

  - Agenten installiert sein, die die Audit-Daten direkt an den zentralen Audit-Vault-Server schicken

  - Ebenso können mit Hilfe des Audit-Vault-Servers zentral die Auditeinstellungen der zu überwachenden Datenbanken administriert werden

- **Transaktionen**
  - Jede Transaktion, die mit einem Datenbankbenutzer durchgeführt wird, der auditiert wird, wird in eine Datei geschrieben oder Datenbank geschrieben
- **Speicherbedarf**
  - Dadurch entsteht zusätzlicher Schreibbedarf, der sich in der Gesamtperformance des Systems niederschlagen wird.
- **Tests laufen zur Zeit**

- **Installation der aktuellen Version**
  - Release Note 10.2.3 unbedingt lesen
    - Connect as sysdba innerhalb der Installation
  - Server nicht für Windows Verfügbar
  - Empfehlung von „Metalink“ Installation 10.2.2 dann upgrade
  - Collektoren auch für nicht Oracle Datenbanken
  - Agent Installation Fehlerfrei

## Fazit

- **Database Audit**
  - Einfache Möglichkeit des auditings
  - Ohne zentrale Sammlung der Informationen
  - „Aufwendiges“ Einrichten der Richtlinenen
- **Database Vault**
  - Vereinfachtes erstellen der Richtlinen
- **Database Audit Vault**
  - Zentraler Server indem Richtlinien verwaltet werden
  - Zentraler Server der Auffälligkeiten bereit stellt
  - Zentraler Server der das Reporting bereit stellt
- **Kostenpflichtig aber Sinnvoll**

# Fragen ? ? ? und Antworten

**Kontakt:**

**Jan-Peter Timmermann**

Tel: 040 / 74 11 22 -1325

Mobil: 0172 / 215 10 43

Email: Jan.Timmermann@opitz-consulting.de