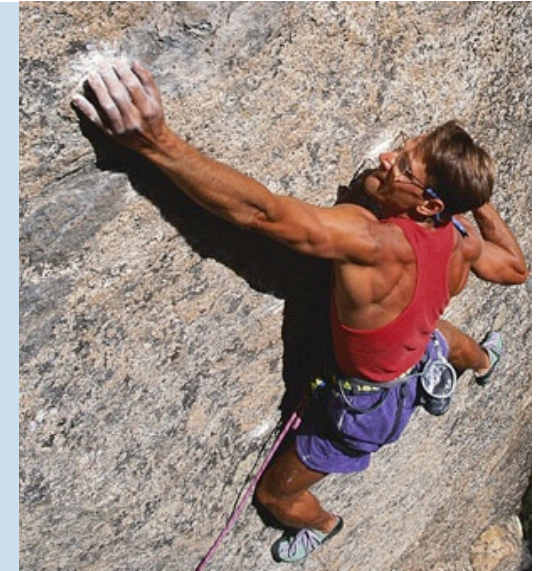


# Praxiserfahrungen mit Database Vault 10g

Dr. Peter Alteheld, Systemberater, MT AG

DOAG NRW, 13.12.07



- n DBA soll Daten aus einzelnen Schemata nicht auslesen können.
  - à Database Vault, nur Realms
- n Daten aus Datenbankdateien sollen nicht auslesbar sein.
  - à Verschlüsselung der Daten in den Dateien
  - à Transparent Data Encryption (TDE)
- n SQL-Befehle aus der SQLNET-Kommunikation (TCP/IP-Pakete) sollen nicht ausgelesen werden können.
  - à Verschlüsselung der Kommunikation
  - à Advanced Security Option (ASO)

- n Voraussetzung: Oracle DB-Software installiert und Datenbank erstellt – Version 10.2.0.3 oder ...
- n Installationsvorgang: eigener runInstaller
- n Installation zweiter Datenbank mit Database Vault-Schutz
  - n dvca, Passwörter in Kommandozeile
- n Einrichtung RMAN-Sicherungen:
  - n orapwd mit Option nosysdba=n aufrufen
  - n SYS-Passwort per mkstore in Passwort-Wallet ablegen

- n Umfangreich – Metalink-Note 445092.1:
  - n Database Vault deaktivieren per make und relinken
  - n DVSYS freischalten, DVSYS-Trigger deaktivieren
  - n Patchen und relinken
  - n catmac.sql – läuft über eine Stunde
  - n DVSYS-Trigger aktivieren, DVSYS sperren
  - n Database Vault aktivieren per make
  - n dabei: Datenbank(en) mehrfach runter- und wieder hochfahren

- n Webanwendung DVA – Database Vault Administrator:
  - n <http://xxx:1156/dva> (wird per emctl mitgestartet/beendet)
  - n Anmeldung durch DVOWNER
- n Nur begrenzt intuitiv bedienbar

à für Anwender Schulung erforderlich

Oder: Einrichtung des Realms durch DBA nach Datenübernahme und anschliessend DVOWNER-Passwortänderung durch den Verantwortlichen

- n Die Kernfrage: Kann der DBA, also SYS oder SYSTEM, Daten in per Realm geschützten Schemata einsehen?
  - n Bei select gibt es die Meldung: insufficient privileges
  - n Andere Zugriffsarten:
    - Datendateien auslesen: durch TDE vermieden
    - Recovery in ein Oracle-Home ohne Database Vault erfolgreich. Zugriff auf TDE-geschützte Daten, wenn Walletpasswort bekannt.
    - Export
    - SQL Trace
    - Histogramme

- n Kein Eingriff in Applikationen
  - à Keine funktionale Veränderung in den Anwendungen
- n Transparent Data Encryption
  - à Datenübernahme und Full table scans sind langsamer aufgrund der Ver- und Entschlüsselung

- n expdp als SYS war erfolgreich – Workaround Directory-Objekte ggf. löschen
- n NLS-Einstellungen beeinflussen Wirksamkeit von DBVault
- n Für Tabellentrigger-Erstellung müssen DVSYS-Trigger disabled werden.

- n Objekte mit Objektnamen in Hochkommata, z.B. `CREATE TABLE "Meine Tabelle"...`, können nicht geschützt werden
- n Fehlermeldungen von `GATHER_STATS_JOB` (Patch verfügbar)

- n Database Vault ist die Lösung, die es ermöglicht, auch Administratoren den Lesezugriff auf Daten in der Oracle-Datenbank zu entziehen, ohne in die Applikation eingreifen zu müssen.
- n Oracle-Sicherheitsupdates schließen vorhandene Lücken.

**Vielen Dank für Ihre Aufmerksamkeit!**

Dr. Peter Alteheld · Systemberater

MT AG · Balcke-Dürr-Allee 9 · 40882 Ratingen

Tel. 02102 309 61-0 · Fax 02102 309 61-10

[www.mt-ag.com](http://www.mt-ag.com) · [Peter.Alteheld@mt-ag.com](mailto:Peter.Alteheld@mt-ag.com)

