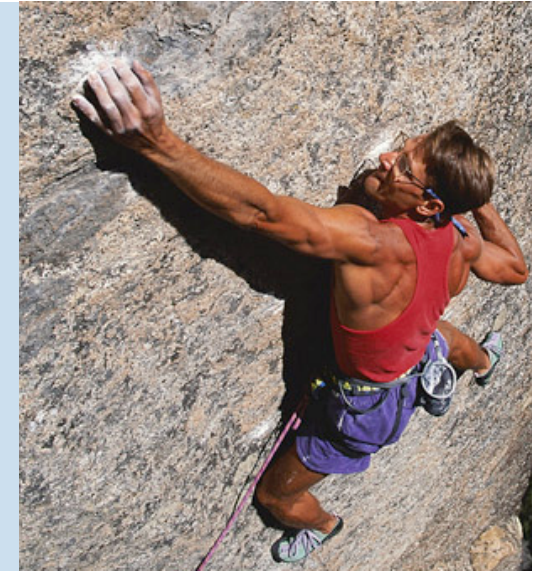


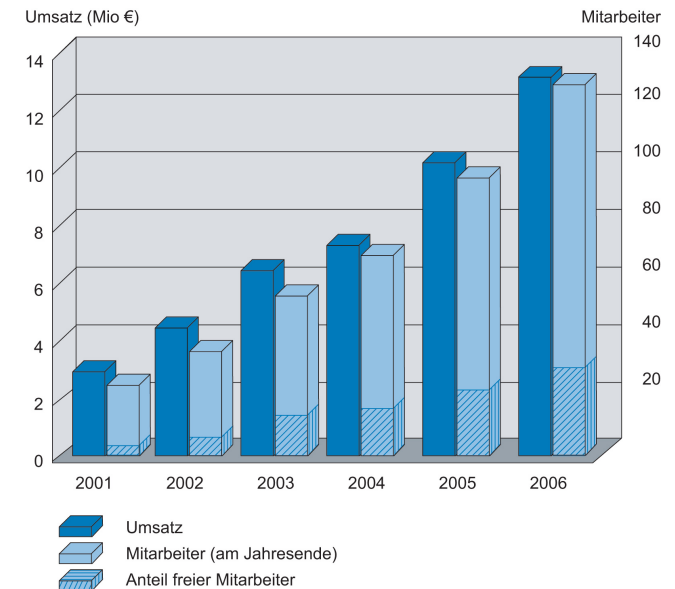
Praxisbericht: Database Vault 10.2.0.3 in der Personalabteilung

Volker Mach, Senior Systemberater, MT AG



Key-facts:

- n 1994: Gründung als MT Software GmbH
- n 2000: Umwandlung zur MT AG, Aktienkapital: 1,5 Mio. €
- n Anteile: In der Hand von Management und Aufsichtsrat
- n Zurzeit: ca. 145 Festangestellte
ca. 60 freie Mitarbeiter



Die MT AG ist langjähriger **IT-Beratungspartner** von Großunternehmen und Mittelstand.

Sie steht für **Technologie-Know-how** und **praxisnahe, effiziente IT-Dienstleistung**: von Strategie und Beratung über Entwicklung und Integration bis hin zu Wartung und Administration von IT-Infrastrukturen.

- n Anfrage der Personalabteilung
- n Anforderungen der Personalabteilungen
- n Auszug internationale Bestimmungen
- n Was ist Database Vault?
- n Was kommt mit der Installation von Database Vault?
- n Wie wird Database Vault verwaltet?
- n Wie erstelle ich Realms und Rule Sets?
- n Wie kann man die Sicherheit noch erhöhen?
- n Erfahrungen während der Implementation
- n Fragen und Antworten

Dialog Personalabteilung à Systemadministration

PA: Könnt ihr die Personaldaten lesen oder ändern?

SA: Theoretisch: JA

PA: Gibt es Möglichkeiten, dies zu unterbinden?

SA: Oracle Database Vault

PA: Was kann Oracle Database Vault und ist das nun sicher?

n Gesetzliche Anforderungen

- n EU Privacy Directives
- n BSI
- n Basel II
- n PCIDSS
- n J-SOX (Asien)

n Firmeninterne Anforderungen

- n Sicherheitsbestimmungen
- n Datenschutz
- n Schutz vor Industriespionage

Oracle Database Vault (DBV) and Regulations		
Regulation	Requirement	Does DBV Mitigate This Risk?
Sarbanes-Oxley Section 302	Unauthorized changes to data	Yes
Sarbanes-Oxley Section 404	Modification to data, Unauthorized access	Yes
Sarbanes-Oxley Section 409	Denial of service, Unauthorized access	Yes
Gramm-Leach-Bliley	Unauthorized access, modification and/or disclosure	Yes
HIPAA 164.306	Unauthorized access to data	Yes
HIPAA 164.312	Unauthorized access to data	Yes
Basel II – Internal Risk Management	Unauthorized access to data	Yes
CFR Part 11	Unauthorized access to data	Yes
Japan Privacy Law	Unauthorized access to data	Yes
PCI – Requirement 7	Restrict access to cardholder data by business need-to-know	Yes
PCI – Requirement 8.5.6	Enable accounts used by vendors for remote maintenance only during the time period needed	Yes
PCI – Compensating Controls for Requirement 3.4	Provide ability to restrict access to cardholder data or databases based on the following criteria: <ul style="list-style-type: none"> • IP address/Mac address • Application/service • User accounts/groups 	Yes
PCI - Requirement A.1: Hosting providers protect cardholder data environment	Ensure that each entity only has access to own cardholder data environment	Yes

- n Database Vault ist eine Datenbank Option, die Sie einsetzen können um:
 - n Datenzugriff durch den DBA zu vermeiden
 - n Strukturänderungen zu verhindern
 - n Kontrollen zur Umsetzung des Zugangs durch dynamische und flexible Sicherheit
 - n gesetzliche Bestimmungen einzuhalten
 - n interne Kontrollen durchzuführen



n Oracle Database 9i (9.2.0.8) Enterprise Edition

- n Solaris Operating System (SPARC) (32-bit)
- n Solaris Operating System (SPARC) (64-bit)
- n Linux x86-64
- n AIX 5L Based Systems (64-Bit)
- n HP-UX PA-RISC (64-Bit)

n Oracle Database 10g Release 2 (10.2.0.3) Enterprise Edition

- n Windows (32-bit)
- n Linux x86
- n Linux Itanium
- n Linux x86-64
- n Solaris Operating System (SPARC) (64-bit)
- n Windows Itanium
- n Windows (x64)
- n HP-UX PA-RISC (64-Bit)
- n AIX 5L Based Systems (64-Bit)
- n HP-UX Itanium

Für 11g noch nicht zertifiziert
Lizenzierung:
Named-User: 296,00 €/zzgl. MwSt
CPU Lizenz: 14.806,00 €/zzgl. MwSt

n Folgende Realms (Bereiche) werden bei der Installation schon erzeugt

n Oracle Database Vault

- DV Schemas : DVSYS, DVF und LBACSYS

n Database Vault Account Management

- Usermanagement und Erstellung von Profilen

n Oracle Data Dictionary

- SYSMAN, SYSTEM, SYS, MDSYS usw.

n Neue Rollen

n DV_OWNER à DV Owner Role

n DV_ADMIN à DV Konfigurations Manager

n DV_SECANALYST à DV Security Analyst

n DV_ACCTMGR à DV Account Manager

Wie wird Database Vault verwaltet?

ORACLE Data Vault

Login

Login to Database: orcl

★ User Name

★ Password

ORACLE Data Vault

[Help](#) [Logout](#)

Database

Logged in as DVOWNER

Database Instance: orcl

Administration

[Data Vault Reports](#)

[General Security Reports](#)

[Monitor](#)

The links below allow you to protect applications and data using Oracle Data Vault features that include: Realms, Command Rules, Rule Sets, Factors, and Secure Application Roles.

Data Vault Feature Administration

[Realms](#)

[Command Rules](#)

[Factors](#)

[Rule Sets](#)

[Secure Application Roles](#)

[Label Security Integration](#)

Erstellen eines Realms



ORACLE Data Vault

[Help](#) [Logout](#)
Database

[Database Instance: orcl](#) > [Realm](#) > Create Realm

Logged in as DVOWNER

Create Realm

Enable or disable the enforcements for objects protected by the realm and to control the auditing that occurs during this enforcement.

General

* Name

Description

Status Enabled
 Disabled

Audit Options

Audit Disabled
 Audit On Failure
 Audit On Success or Failure

Erstellen eines Realms



ORACLE Database Vault [Help](#) [Logout](#)
Database

Database Instance: orcl > Realm > Create Realm Logged in as DBV_OWNER

Create Realm

[Cancel](#) [OK](#)

Enable or disable the enforcements for objects protected by the realm and to control the auditing that occurs during this enforcement.

General

* Name	HR Realm
Description	This realm protects the HR data from DBA access
Status	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

Audit Options

- Audit Disabled
- Audit On Failure
- Audit On Success or Failure

Erstellen eines Realms (2)

ORACLE Data Vault

[Help](#) [Logout](#)

Database

Database Instance: orcl > Realms

Logged in as DVOWNER

Realms

Data Vault realms provide a capability to classify database schemas and database roles into functional groups in order to provide fine-grained access control of the ability to use system level privileges against these types of database objects.

Create

Edit

Remove

Select	Name 	Audit Options	Oracle Defined Realm?	Objects Protected?	Users Authorized?	Status
<input type="radio"/>	Data Vault Account Management	Audit On Failure	✓	✓	✓	✓
<input checked="" type="checkbox"/>	HR Protect	Audit On Failure		✗	✗	✓
<input type="radio"/>	Oracle Data Dictionary	Audit On Failure	✓	✓	✓	✓
<input type="radio"/>	Oracle Data Vault	Audit On Failure	✓	✓	✓	✓

Edit

Remove

Erstellen eines Realms (3)

ORACLE Data Vault Help Logout Database

Database Instance: orcl > Realm > Edit Realm: HR Protect Logged in as DVOWNER

Edit Realm: HR Protect

Cancel OK

Enable or disable the enforcements for objects protected by the realm and to control the auditing that occurs during this enforcement.

General

*Name

Description

Status Enabled
 Disabled

Audit Options

Audit Disabled
 Audit On Failure
 Audit On Success or Failure

Realm Secured Objects

Create

Select	Owner	Object Type	Object Name
No Items Found			

Erstellen eines Realms (4)



ORACLE Data Vault [Help](#) [Logout](#)

Database

Database Instance: orcl > [Realms](#) > [Edit Realm: HR Protect](#) > [Create Realm Secured Object](#) by [Gerd Laatz](#) as [SYSDBA](#)

Create Realm Secured Object

Define a database schema or database role that is protected by the realm.

Object Owner

Object Type

Object Name

Erstellen eines Realms (5)

ORACLE Data Vault

Help Logout
Database

Database Instance: orcl > Realm > Edit Realm: HR Protect

Logged in as: DVOWNER

Edit Realm: HR Protect

Cancel OK

Enable or disable the enforcements for objects protected by the realm and to control the auditing that occurs during this enforcement.

General

* Name

Description

Status Enabled
 Disabled

Audit Options

Audit Disabled
 Audit On Failure
 Audit On Success or Failure

Realm Secured Objects

Create

Edit Remove

Select	Owner	Object Type	Object Name
<input checked="" type="radio"/>	HR	%	%

ORACLE Data Vault

[Help](#) [Logout](#)
Database

Logged in as DVOWNER

Database Instance: orcl

Administration [Data Vault Reports](#) [General Security Reports](#) [Monitor](#)

The links below allow you to protect applications and data using Oracle Data Vault features that include: Realms, Command Rules, Rule Sets, Factors, and Secure Application Roles.

Data Vault Feature Administration

[Realms](#)

[Command Rules](#)

[Factors](#)

[Rule Sets](#)

[Secure Application Roles](#)

[Label Security Integration](#)

Administration [Data Vault Reports](#) [General Security Reports](#) [Monitor](#)

Audit des Realms (2)

ORACLE Data Vault [Help](#) [Logout](#)

Database

Logged in as DVOWNER

Database Instance: orcl

[Administration](#) | **Data Vault Reports** | [General Security Reports](#) | [Monitor](#)

Use this screen to run reports about potential Data Vault configuration issues and Data Vault audit events.

[Run Report](#)

[Expand All](#) | [Collapse All](#)

⊕ Reports

Select Focus	Report Title
<input type="radio"/>	▼ Reports
<input type="radio"/>	⊕ ▼ Data Vault Configuration Issues Reports
<input type="radio"/>	Command Rule Configuration Issues
<input type="radio"/>	Factor Configuration Issues
<input type="radio"/>	Factors Without Identities
<input type="radio"/>	Identity Configuration Issues
<input type="radio"/>	Realm Authorization Configuration Issues
<input type="radio"/>	Rule Set Configuration Issues
<input type="radio"/>	Secure Application Configuration Issues
<input type="radio"/>	⊕ ▼ Data Vault Auditing
<input checked="" type="radio"/>	Realm Audit
<input type="radio"/>	Command Rule Audit
<input type="radio"/>	Factor Audit

Audit des Realms (3)



ORACLE Data Vault

[Help](#) [Logout](#)

Database

Database Instance: orcl > Report Results: Realm Audit

Logged in as DVOWNER

Report Results: Realm Audit

Page Refreshed **Apr 13, 2006**
12:42:09 AM

[Return To Re](#)

Previous 1-25 of 66

Violation Attempt	Timestamp	Return Code	Account	User Host	Instance Number	Realm Name	Rule Set
Realm Violation Audit	APR 12, 2006 11:37:30 P.M.	-47401	SYSTEM	OUSER-US	1	HR Protect	
Realm Violation Audit	APR 12, 2006 11:21:29 P.M.	-47401	SYSTEM	MYOUNG-LAP	1	HR Protect	
Realm Violation Audit	APR 12, 2006 11:21:29 P.M.	-47401	SYSTEM	MYOUNG-LAP	1	HR Protect	
Realm Violation Audit	APR 12, 2006 11:21:14 P.M.	-47401	SYSTEM	MYOUNG-LAP	1	HR Protect	

Erstellen eines Rule Sets



ORACLE Data Vault

[Help](#) [Logout](#)

Database

Logged in as DVOWNER

Database Instance: orcl

Administration

[Data Vault Reports](#) [General Security Reports](#) [Monitor](#)

The links below allow you to protect applications and data using Oracle Data Vault features that include: Realms, Command Rules, Rule Sets, Factors, and Secure Application Roles.

Data Vault Feature Administration

[Realms](#)

[Command Rules](#)

[Factors](#)

[Rule Sets](#)

[Secure Application Roles](#)

[Label Security Integration](#)

Administration

[Data Vault Reports](#) [General Security Reports](#) [Monitor](#)

Erstellen eines Rule Sets (2)

ORACLE Data Vault [Help](#) [Logout](#)

Database

Database Instance: orcl > Rule Sets Logged in as DVOWNER

Rule Sets

Data Vault provides a rules engine that can be used in the security policy decisions of factors, realms, command rules, and secure application roles.

[Create](#)

[Edit](#) [Remove](#)

Select	Name ▲	Evaluation Options	Error Handling	Audit Options	Rules Defined?	Status
<input type="radio"/>	Allow Sessions	All True	Show Error Message	Audit On Failure	✗	✓
<input type="radio"/>	Can Grant VPD Administration	All True	Show Error Message	Audit On Failure	✓	✓
<input type="radio"/>	Can Maintain Accounts/Profiles	Any True	Show Error Message	Audit On Failure	✓	✓
<input type="radio"/>	Can Maintain Own Account	Any True	Show Error Message	Audit On Failure	✓	✓
<input type="radio"/>	Disabled	All True	Show Error Message	Audit Disabled	✓	✓
<input type="radio"/>	Enabled	All True	Show Error Message	Audit Disabled	✓	✓
<input checked="" type="radio"/>	Enforce Local Access	All True	Show Error Message	Audit On Failure	✗	✗
<input type="radio"/>	test rule	All True	Show Error Message	Audit On Failure	✓	✓

Erstellen eines Rule Sets (3)

ORACLE Data Vault Help Logout

Database

Database Instance: orcl > Rule Set > Edit Rule Set: Enforce Local Access Accessed in as DVOWNER

Edit Rule Set: Enforce Local Access

A rule set is a collection of one or more rules that evaluates to true or false based on the evaluation of each rule it contains and the evaluation type (All True or Any True).

General

* Name	<input type="text" value="Enforce Local Access"/>
Description	<input type="text" value="Enforce Local Access"/>
Status	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Evaluation Options	<input checked="" type="radio"/> All True <input type="radio"/> Any True

Audit Options

Audit Disabled
 Audit On Failure
 Audit On Success or Failure

Erstellen eines Rule Sets (4)



Fail Message
The failure message is a custom text error message displayed to the database session when the rule set fails. The message can be up to 80 characters in length.

Custom Event Handler Option
 Handler Disabled
 Execute On Failure
 Execute On Success or Failure

Custom Event Handler Logic
The rule set custom event handler is called depending on the custom event handler option chosen and may include any value PL/SQL package procedure or standalone procedure. Make sure to use a fully qualified procedure, such as schema.procedure_name, and be sure to GRANT EXECUTE privilege on the procedure to the DVSYS account. The procedure's signature should be one of the following forms:
PROCEDURE my_ruleset_handler(p_ruleset_name IN VARCHAR2, p_ruleset_rules IN BOOLEAN) - This form is used when the name of the rule set that is executed and the return value of the rule set are required in the handler processing.
PROCEDURE my_ruleset_handler - This form is used when the name of the rule set that is executed and the return value of the rule set are not required in the handler processing.

Rules Associated To The Rule Set

[Create](#) [Add Existing Rules](#)

Select	Rule Name	Rule Expression
	No Items Found	

Erstellen eines Rule Sets (5)

ORACLE Data Vault Help Logout

Database

Database Instance: orcl > Rule Set > Edit Rule Set: Enforce Local Access Log Cancel Create Rule

Create Rule

Cancel OK

A rule is a SQL WHERE clause expression that evaluates to true or false.

General

* Name

* Rule Expression

A rule expression may be any valid SQL WHERE clause expression. The value returned by this expression must return a boolean value (TRUE or FALSE). When using PL/SQL functions, make sure to use the full name of the function, such as schema.function_name, and make sure to GRANT EXECUTE privilege on the function to the user account.

Cancel OK

Rules Associated To The Rule Set

Create

Add Existing Rules

Edit

Remove

Select	Rule Name 	Rule Expression
<input checked="" type="radio"/>	Local Access	sys_context('userenv','ip_address')='130.35.46.19'

Edit

Remove

Erstellen eines Rule Sets (7)

ORACLE Data Vault [Help](#) [Logout](#)

Database

[Database Instance: orcl](#) > [Rule Set](#) > [Edit Rule Set: Enforce Local Access](#) Accessed in as DVOWNER

Edit Rule Set: Enforce Local Access

A rule set is a collection of one or more rules that evaluates to true or false based on the evaluation of each rule it contains and the evaluation type (All True or Any True).

General

* Name	<input type="text" value="Enforce Local Access"/>
Description	<input type="text" value="Enforce Local Access"/>
Status	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Evaluation Options	<input checked="" type="radio"/> All True <input type="radio"/> Any True

Audit Options

- Audit Disabled
- Audit On Failure
- Audit On Success or Failure

Erstellen eines Rule Sets (8)

ORACLE Data Vault

[Help](#) [Logout](#)

Database

Database Instance: orcl > Rule Sets

Logged in as DVOWNER

Rule Sets

Data Vault provides a rules engine that can be used in the security policy decisions of factors, realms, command rules, and secure application roles.

[Create](#)

[Edit](#)

[Remove](#)

Select	Name ▲	Evaluation Options	Error Handling	Audit Options	Rules Defined?	Status
<input checked="" type="radio"/>	Allow Sessions	All True	Show Error Message	Audit On Failure	✗	✓
<input type="radio"/>	Can Grant VPD Administration	All True	Show Error Message	Audit On Failure	✓	✓
<input type="radio"/>	Can Maintain Accounts/Profiles	Any True	Show Error Message	Audit On Failure	✓	✓
<input type="radio"/>	Can Maintain Own Account	Any True	Show Error Message	Audit On Failure	✓	✓
<input type="radio"/>	Disabled	All True	Show Error Message	Audit Disabled	✓	✓
<input type="radio"/>	Enabled	All True	Show Error Message	Audit Disabled	✓	✓
<input type="radio"/>	Enforce Local Access	All True	Show Error Message	Audit On Failure	✓	✓
<input type="radio"/>	test rule	All True	Show Error Message	Audit On Failure	✓	✓

Einer Command Rule ein Rule Set zuweisen



ORACLE Data Vault

[Help](#) [Logout](#)
Database

Logged in as DVOWNER

Database Instance: orcl

Administration [Data Vault Reports](#) [General Security Reports](#) [Monitor](#)

The links below allow you to protect applications and data using Oracle Data Vault features that include: Realms, Command Rules, Rule Sets, Factors, and Secure Application Roles.

Data Vault Feature Administration

[Realms](#)

[Command Rules](#)

[Factors](#)

[Rule Sets](#)

[Secure Application Roles](#)

[Label Security Integration](#)

Administration [Data Vault Reports](#) [General Security Reports](#) [Monitor](#)

Einer Command Rule ein Rule Set zuweisen (2)

ORACLE Data Vault

[Help](#) [Logout](#)

Database

Database Instance: orcl > Command Rules

Logged in as DVOWNER


Command Rules

Command rules control the ability to process Data Definition Language (DDL) commands and special database operations. Command rules determine whether or not to allow the command to succeed based on the evaluation of a Data Vault rule set.

Create

Edit

Remove

Select	Command 	Object Owner	Object Name	Rule Set Name	Status
<input type="radio"/>	ALTER PROFILE	%	%	Can Maintain Accounts/Profiles	✓
<input checked="" type="radio"/>	ALTER SYSTEM	%	%	Allow Sessions	✗
<input type="radio"/>	ALTER USER	%	%	Can Maintain Own Account	✓
<input type="radio"/>	CONNECT	%	%	Enforce Local Access	✗
<input type="radio"/>	CREATE PROFILE	%	%	Can Maintain Accounts/Profiles	✓
<input type="radio"/>	CREATE USER	%	%	Can Maintain Accounts/Profiles	✓
<input type="radio"/>	DROP PROFILE	%	%	Can Maintain Accounts/Profiles	✓
<input type="radio"/>	DROP USER	%	%	Can Maintain Accounts/Profiles	✓
<input type="radio"/>	GRANT	SYS	DBMS_RLS	Can Grant VPD Administration	✓
<input type="radio"/>	REVOKE	SYS	DBMS_RLS	Can Grant VPD Administration	✓

Edit

Remove

Einer Command Rule ein Rule Set zuweisen (3)



ORACLE Data Vault [Help](#) [Logout](#)
Database

Database Instance: orcl > Command > Edit Command Rule: ALTER SYSTEM
Edit Command Rule: ALTER SYSTEM

This page allows you to create or edit a command that can be authorized based on the evaluation of a Data Vault rule set.

General

* Command

Status Enabled
 Disabled

Applicability

Object Owner

Object Name

Rule Set

Command Rule Audit



ORACLE Data Vault

[Help](#) [Logout](#)

Database

Database Instance: orcl > Report Results: Command Rule Audit

Logged in as DVOWNER

Report Results: Command Rule Audit

Page Refreshed Apr 13, 2006 12:43:24 AM

[Return To Reports Menu](#)

Violation Attempt ▲	Timestamp	Return Code	Account	User Host	Instance Number	Command Rule	Rule Set	Command
Command Authorization Audit	APR 13, 2006 12:38:09 A.M.	0	SYSTEM	MYOUNG-LAP	1	ALTER SYSTEM	Enforce Local Access	alter system switch logfile
Command Authorization Audit	APR 12, 2006 11:56:02 P.M.	0	SYSTEM	MYOUNG-LAP	1	ALTER SYSTEM	Enforce Local Access	alter system switch logfile

- n Einsatz von Transparent Data Encryption um auch den Zugriff durch Verschlüsselung auf die Datendateien zu erschweren
- n Nutzen von Oracle Label Security
 - n Oracle Label Security ist eine Virtual Private Database-(VPD)Anwendung
 - n Oracle Label Security bietet “out-of-the-box” VPD Funktionalität
 - n Programmierung ist nicht notwendig
 - n Oracle Policy Manager (GUI) zur Administration von ‘Labels’ und Authorisierung

```
n [oracle@dbva~] $ . Oraenv
```

```
ORACLE_SID=dbva
```

```
[oracle@dbva~]$ sqlplus / as sysdba
```

```
SQL*Plus: Release 10.2.0.3.0 –Production on Mon 23 14:31:22 2007
```

```
Copyright © 1982, 2006, Oracle. All Rights Reserved.
```

```
Error:
```

```
ORA-01031: insufficient privileges
```

```
Enter username:
```

Ich kann mich nicht mehr als SYSDBA anmelden!!

Starten und Stoppen der Datenbank nur als SYSOPER

Scheitert ein SELECT auf einen geschützten Bereich durch SYS?

- n Bei den Testumstellungen wurde festgestellt, dass Database Vault nicht auf Objekte wirkt, deren Namen in Hochkommata stehen, d.h. wurde eine Tabelle mit dem Befehl `CREATE TABLE SALARIES ...` in dem per Realm geschützten Bereich erstellt, so lieferte ein SELECT auf die Tabelle als SYS einen Fehler. Wurde die Tabelle dagegen per `CREATE TABLE "SALARIES" ...` erstellt, so war ein SELECT als SYS erfolgreich.
- n Im konkreten Fall wurden als Workaround die Hochkommata aus den Create-Skripten herausgenommen.

∅ Dies wurde mit dem CPU 2007 Oktober behoben

- Metalink **Note:432865.1**

n Was ändert sich mit Database Vault?

n Login als SYSDBA nötig

- lt. White Paper sollte man 2 Passwordfiles anlegen

```
§ $orapw file=orapw<sid>.sysdba_closed password=<enter sys password here> nosysdba=y
```

```
§ $orapw file=orapw<sid>.sysdba_open password=<enter sys password here> nosysdba=n
```

```
§ $cp -p orapw<sid>.sysdba_open orapw<sid>
```

Das „switchen“ des Passwordfiles sollte nach jedem Backup erfolgen!

Oracle empfiehlt, das Backup über den bekannten Enterprise Manager vorzunehmen oder die

Dateiberechtigungen der eigenen Backup Scripte zu verschärfen:

z.B. `$chmod 700 rman_scripts`

- n Minimale Änderungen am Trigger-Quellcode verursachen beim Kompilieren mögliche Fehler
- n Bekannter Bug : 5630439
 - Ø *Unpublished bug which is still worked on by Development.*
- n ORA-47999: compiling a trigger after Database Vault installation

n Den Schemanamen als Präfix vor den Tabellennamen setzen

Ø z.B. AFTER INSERT OR UPDATE OF update_date ON
schema_name.TBS_STATUS

Eine andere, etwas unkonventionelle Methode wäre, sich als DV_OWNER anzumelden und folgenden Trigger zu „disablen“

```
alter trigger dvsys.DV_BEFORE_DDL_TRG disable
```

Nun kann man den Trigger in gewohnter Art und Weise erstellen.

- n Database Vault hilft durch eine einfache administrative Oberfläche bei der Umsetzung der internen und externen Sicherheitsbestimmungen
- n Database Vault zeigt durch sein Reportwesen die Sicherheitslücken in der Datenbank auf
- n Kann als Sicherungsnachweis gegen Datenspionage wirken
- n Database Vault bietet dem DBA Selbstschutz, da ein Zugriff auf Anwendungsdaten durch Database Vault technologisch ausgeschlossen wird
- n Database Vault ist das einzige Tool, das diese Anforderungen für Oracle Datenbanken erfüllt
- n Getrennte Sicherheit von Betriebssystem und Datenbank notwendig
- n Zusätzlicher administrativer Aufwand für Database Vault

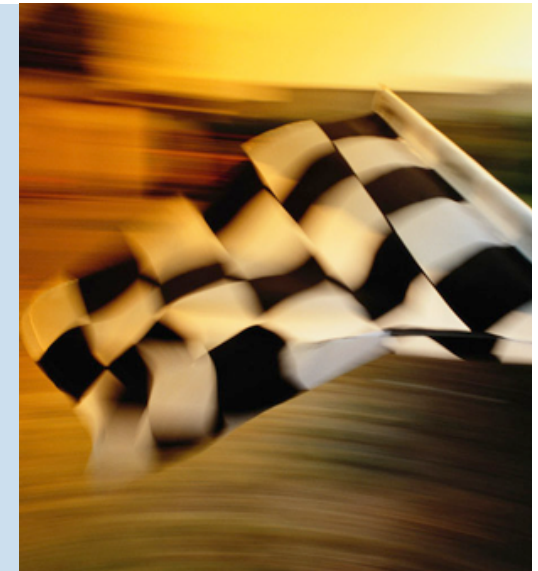
Fragen und Antworten

Volker Mach, Senior Systemberater

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

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

www.mt-ag.com · volker.mach@mt-ag.com



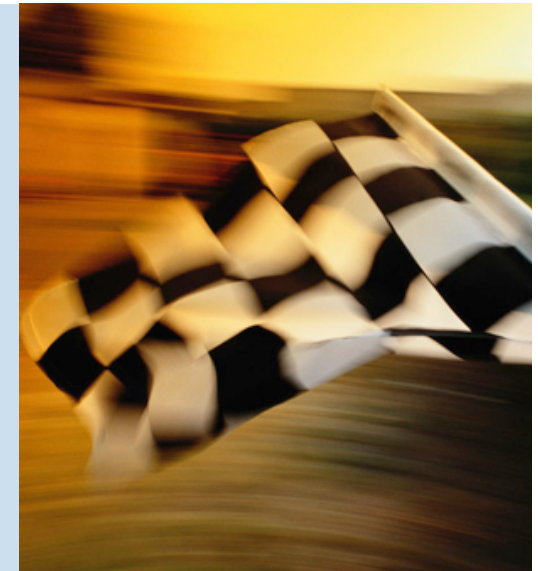
Vielen Dank für Ihre Aufmerksamkeit!

Volker Mach, Senior Systemberater

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

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

www.mt-ag.com · volker.mach@mt-ag.com



Wann	Thema	Referent MT AG
Di., 20.11.	ETL Monitoring & Tuning durch Auswertung der OWB Laufzeit-Metadaten	Lutz Bauer
Di., 20.11.	Erfahrungsbericht Einführung ARIS beim Kaufhof	Hildgund von Alten-Krämer
Mi., 21.11. 11:00 – 11:45h	Oracle Warehouse Builder: Automatisierung von Designschritten bei der Bayer HealthCare AG	Lutz Bauer
Mi., 21.11. 12:00 – 12:45h	So profitieren Unternehmen von Oracle Web-Center Suite: Wie sich Web 2.0-Features bewähren	Niels de Bruijn Detlef Müller/Oracle
Do., 22.11. 11:00 – 11:45h	Praxisbericht: Database Vault 10.2.0.3 in der Personalabteilung	Volker Mach
Do., 22.11. 12:00 – 12:45h	Beschleunigte Oracle-ADF-Entwicklung von Rich Client-Anwendungen im Bankenwesen	Tobias Otto
Do., 22.11. 13:00 – 13:45h	Risikominimierung bei der Migration von Datenbank und Application Server nach 10gR2	Dr. Peter Alteheld
Do., 22.11. 14:00 – 14:45h	Best Practices: Entwicklung komplexer APEX-Applikationen	Niels de Bruijn, Anja Wiegele
Standby	Best Practices im Business-Reporting: So kombiniert man Hyperion Intelligence mit dem OWB	Jens Wiesner