Oracle Database Vault

beperken van toegang tot bedrijfskritische en privacy-gevoelige data

Spreker(s) : Ruud de Gunst

Datum: 15 september 2015

E-mail : rgunst@transfer-solutions.com

TRANSFER

Wat kun je met ODV?

- gebieden in de database beschermen tegen toegang van super-privileged users
- beperken van toegang tot de database a.d.h.v. condities
- beperken van toegang tot SQL commando's a.d.h.v. condities
- implementeren van "separation of duties" binnen de organisatie

TRANSFER

Installatie van ODV

- tweetrapsraket: library & dbca
- twee nieuwe users:
  - ODV Owner
  - ODV Account Manager
- drie nieuwe rollen:
  - DV_OWNER & DV_ADMIN
  - DV_ACCTMGR

TRANSFER

Wat merk je na installatie van ODV?

- DBA kan geen database accounts meer creëeren
- de ANY privileges geven geen toegang meer tot objecten die binnen een realm zijn geregistreerd

TRANSFER

ODV aangepaste initiële parameters

parameter	standaard waarde	nieuwe ODV waarde
AUDIT_SYS_OPERATIONS	*FALSE*	*TRUE*
OS_ROLES	*-*	*FALSE*
RECYCLEBIN	*ON*	*OFF*
REMOTE_LOGIN_PASSWORDFILE	*EXCLUSIVE*	*EXCLUSIVE*
SQL92_SECURITY	*FALSE*	*TRUE*

TRANSFER

ODV revoked privileges

user or role	revoked privilege
DBA	*BECOME USER* *SELECT ANY TRANSACTION* *CREATE ANY JOB* *CREATE EXTERNAL JOB* *EXECUTE ANY PROGRAM* *EXECUTE ANY CLASS* *MANAGE SCHEDULER* *DEQUEUE ANY QUEUE* *ENQUEUE ANY QUEUE* *MANAGE ANY QUEUE*
IMP_FULL_DATABASE	*BECOME USER* *MANAGE ANY QUEUE*

TRANSFER

ODV revoked privileges

user or role	revoked privilege
EXECUTE_CATALOG_ROLE	*EXECUTE on DBMS_LOGMNR* *EXECUTE on DBMS_LOGMNR_D* *EXECUTE on DBMS_LOGMNR_LOGREP_DICT* *EXECUTE on DBMS_LOGMNR_SESSION* *EXECUTE on DBMS_FILE_TRANSFER*
SCHEDULER_ADMIN_ROLE	*CREATE ANY JOB* *CREATE EXTERNAL JOB* *EXECUTE ANY PROGRAM* *EXECUTE ANY CLASS* *MANAGE SCHEDULER*
PUBLIC (user)	*EXECUTE on UTL_FILE*

TRANSFER

ODV geblokkeerde privileges

privilege
CREATE PROFILE
CREATE USER
ALTER PROFILE
ALTER USER (uitzondering: eigen wachtwoord aanpassen)
DROP PROFILE
DROP USER

TRANSFER

ODV componenten

- realms
- rules & rule sets
- command rules
- factors
- secure application roles

TRANSFER

Realms

- logische groepering van schema's, objecten en database rollen
- toegang tot objecten
  1. reguliere security model
  2. realm autorisatie

TRANSFER

Rules & rule sets

- een rule is een PL/SQL expressie die als uitkomst TRUE of FALSE heeft
- een rule set is een verzameling rules die als uitkomst TRUE of FALSE heeft
  - afhankelijk van het evaluatietype
    - all TRUE
    - any TRUE
- rule set kan worden geassocieerd met realm authorisatie, command rules en secure application roles.

TRANSFER

Command rule

- uitvoeren van SQL statements reguleren
  - DDL, SELECT, DML, ALTER SYSTEM
- toestemming op basis van evaluatie van een rule set

TRANSFER

Factors

- binnen een sessie bekende variabelen
  - session user, session IP-address, etc.
- waarde ervan kan worden geëvalueerd in een rule

TRANSFER

Secure application roles

- uitbreiding op application roles
- al dan niet activeren van een application role wordt bepaald door evaluatie van een rule set

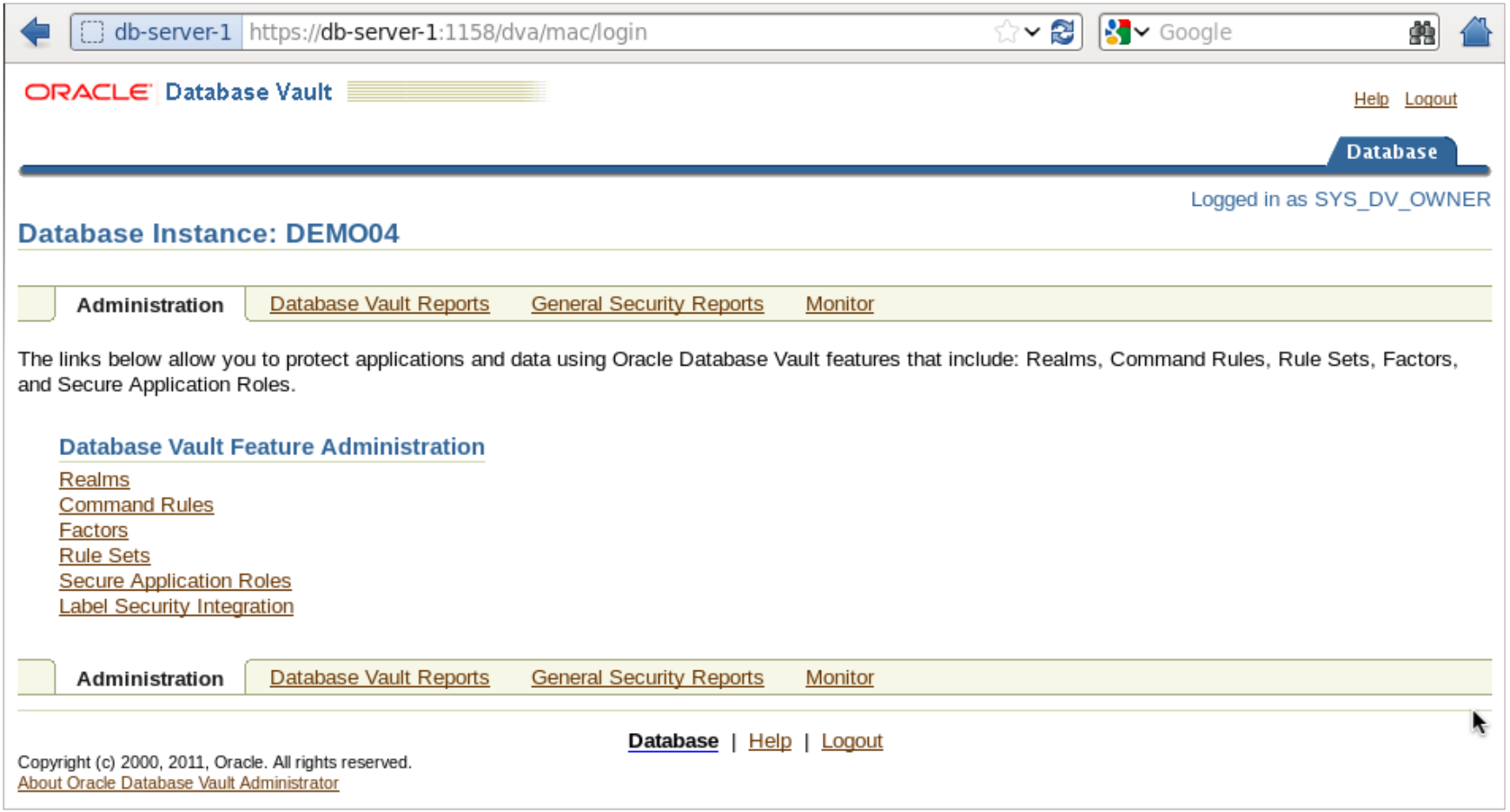
TRANSFER

Realm

- logische groepering van schema's en/of losse objecten en/of rollen
- beheren als gebruiker met DV_OWNER rol
  - vanuit SQL*Plus met DBMS_MACADM package
  - OEM Grid Control, dbconsole
  - DV Administration console

TRANSFER

Realm

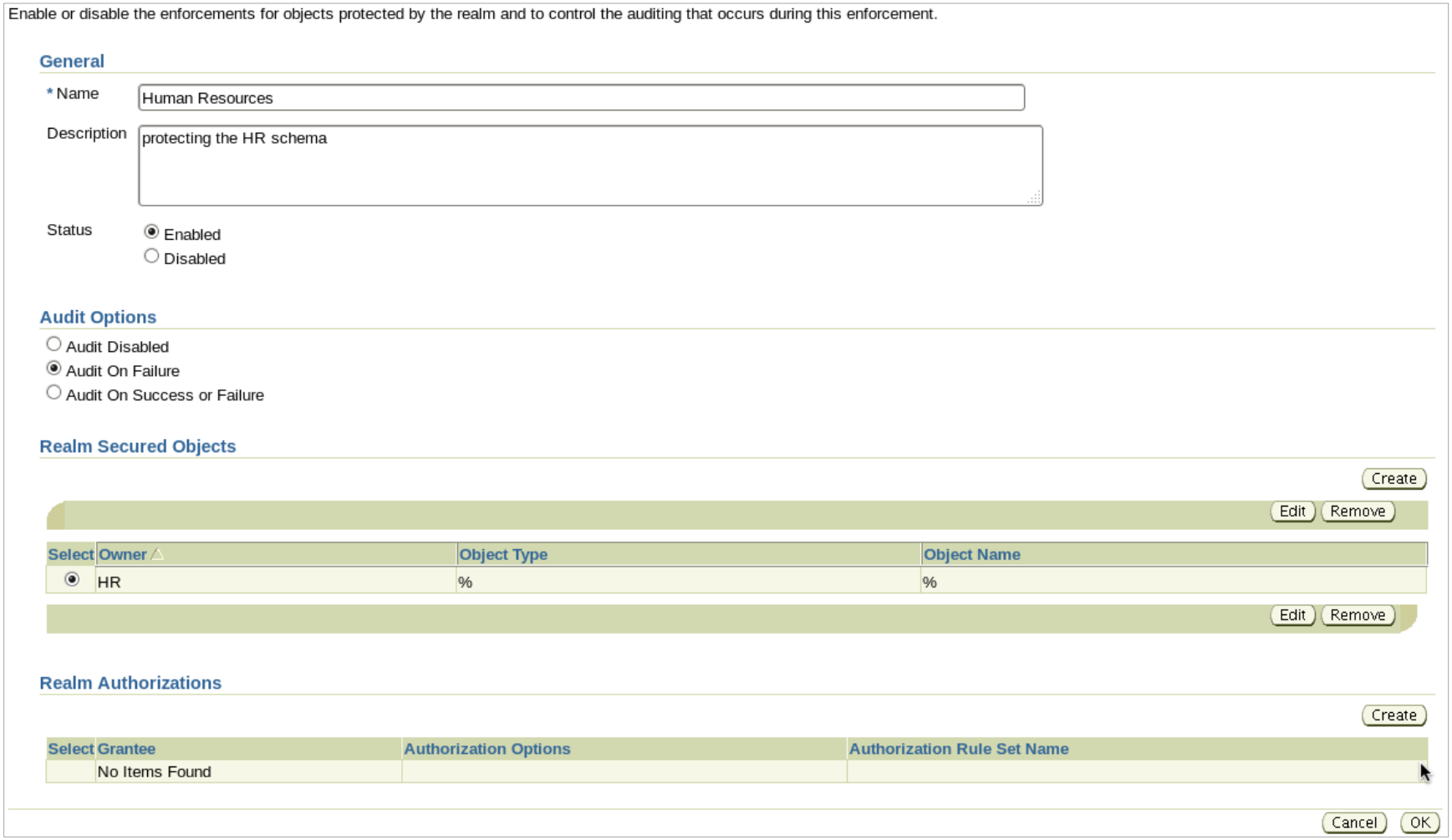


Realm

- 4 standaard realms
  - Oracle Database Vault
    - DVSYS & DVF schema's & rollen
  - Database Vault Account Management
    - DV_ACCTMGR & CONNECT rollen
  - Oracle Data Dictionary
    - oracle catalog schema's & administratie rollen
  - Oracle Enterprise Manager
    - SYSMAN & DBSNMP schema's

TRANSFER

Realm: voorbeeld



Realm: voorbeeld

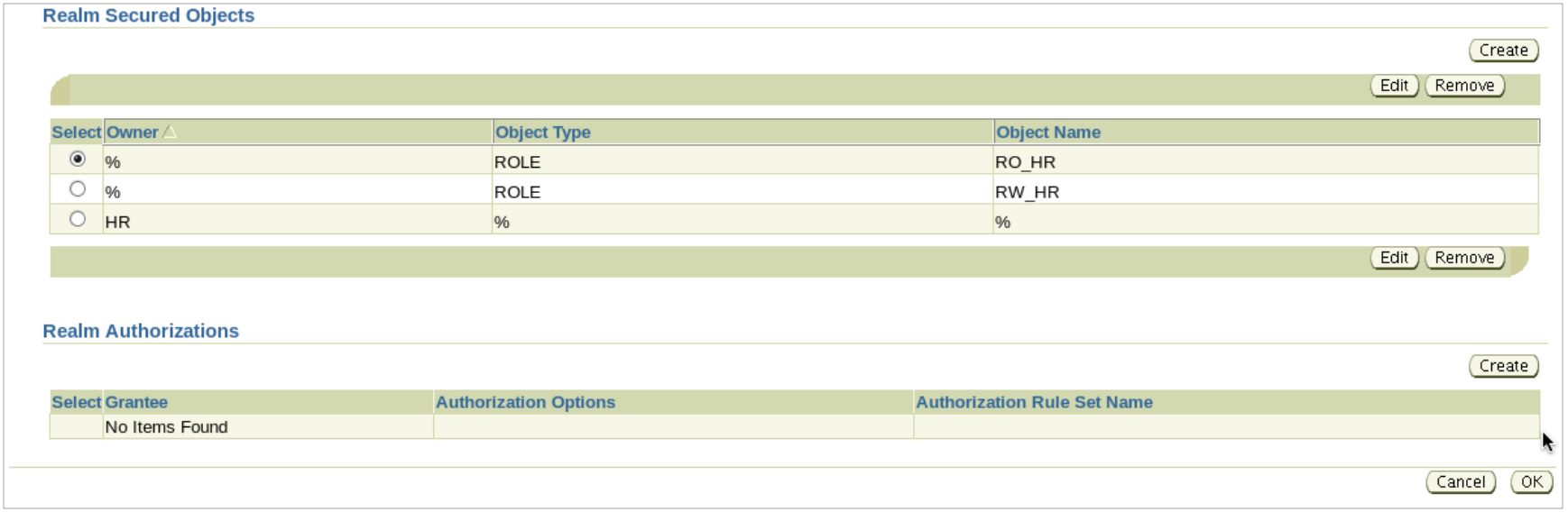
```
[oracle@db-server-1 ~]$ sqlplus

SQL*Plus: Release 11.2.0.3.0 Production on Sun Sep 6 15:56:33 2015

Copyright (c) 1982, 2011, Oracle.  All rights reserved.

Enter user-name: / as sysdba

Connected to:
Oracle Database 11g Enterprise Edition Release 11.2.0.3.0 - 64bit Production
With the Oracle Label Security, OLAP, Data Mining and Oracle Database Vault options

SQL> select * from hr.employees;
select * from hr.employees
              *
ERROR at line 1:
ORA-01031: insufficient privileges
```

TRANSFER

Realm: voorbeeld

```
SQL> r
  1* select * from hr.employees


EMPLOYEE_ID FIRST_NAME           LAST_NAME
----------- -------------------- -------------------------
EMAIL                     PHONE_NUMBER         HIRE_DATE JOB_ID         SALARY
------------------------- -------------------- --------- ---------- ----------
COMMISSION_PCT MANAGER_ID DEPARTMENT_ID
-------------- ---------- -------------
        100 Steven                King
SKING                     515.123.4567         17-JUN-03 AD_PRES         24000
                                    90

        101 Neena                 Kochhar
NKOCHHAR                  515.123.4568         21-SEP-05 AD_VP           17000
                     100            90
```

Realm: voorbeeld




```
SQL> show user
USER is "SYS"
SQL> grant RO_HR to ruud;
grant RO_HR to ruud
*
ERROR at line 1:
ORA-47410: Realm violation for GRANT on RO_HR
```

TRANSFER

Realm authorization

- de DV_OWNER kan users en roles autoriseren om op basis van hun *system privileges* objecten in een realm te mogen benaderen
- 2 niveaus van realm authorization
  - owner
    - objecten & toekennen realm rollen
  - participant
    - objecten

TRANSFER

Realm authorization: voorbeeld

```
SQL> connect sys_dv_admin/DV%sys02
Connected.
SQL> create user HR_DBA identified by "HR%dba01";

User created.

SQL> grant CONNECT to HR_DBA;

Grant succeeded.

SQL> connect / as sysdba
Connected.
SQL> create role HR_ADMIN;

Role created.

SQL> grant SELECT ANY TABLE to HR_ADMIN;

Grant succeeded.

SQL> grant GRANT ANY ROLE to HR_ADMIN;

Grant succeeded.

SQL> grant HR_ADMIN to HR_DBA;

Grant succeeded.
```

TRANSFER

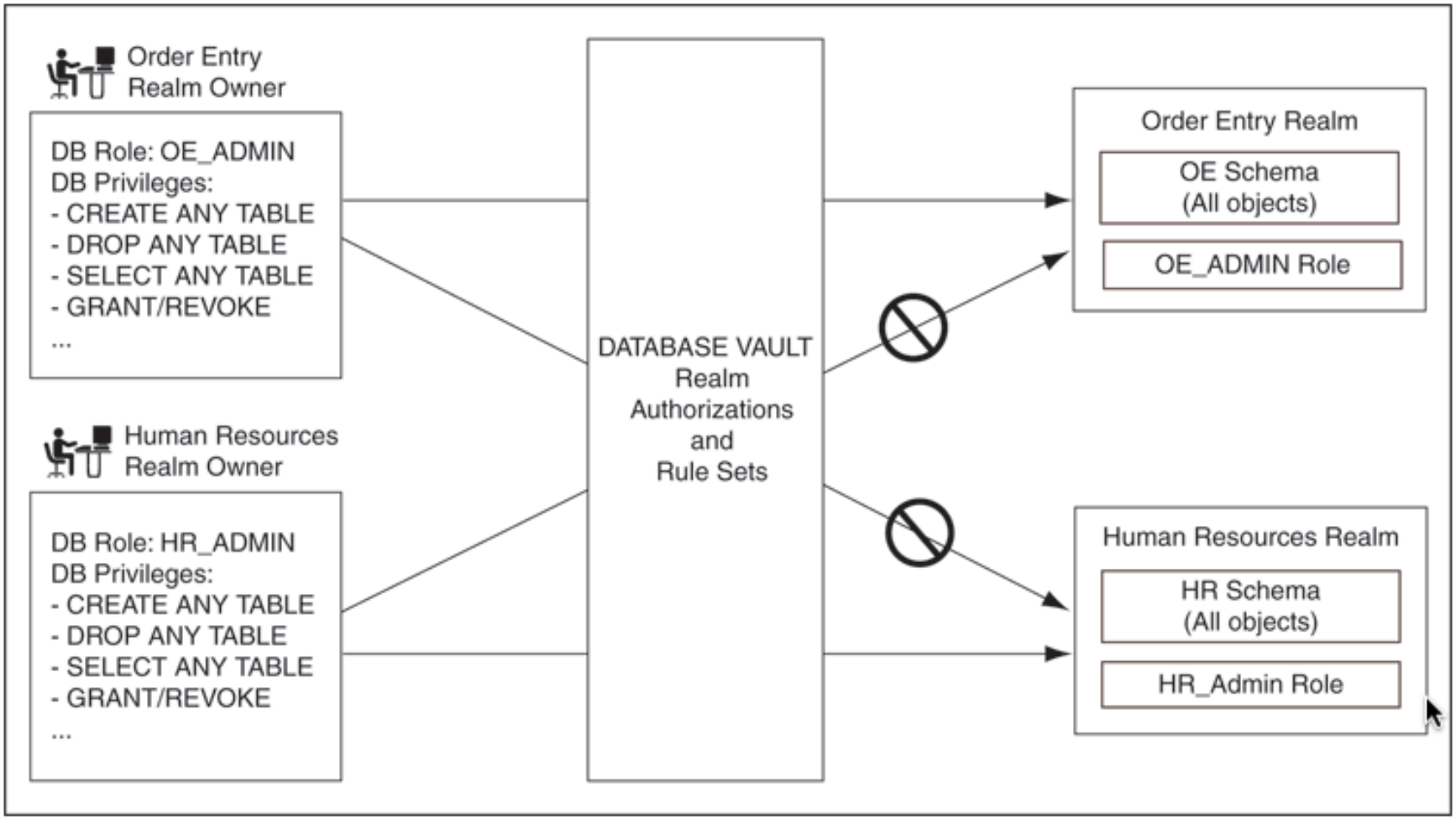
Realm authorization: voorbeeld

```
SQL> connect HR_DBA/HR%dba01
Connected.
SQL> grant RO_HR to RUUD;
grant RO_HR to RUUD
*
ERROR at line 1:
ORA-47410: Realm violation for GRANT on RO_HR


SQL> select count(*) from HR.EMPLOYEES;
select count(*) from HR.EMPLOYEES
                        *
ERROR at line 1:
ORA-01031: insufficient privileges


SQL> grant RO_HR to RUUD;

Grant succeeded.

SQL> select count(*) from HR.EMPLOYEES;


  COUNT(*)
----------
       107
```

TRANSFER

Realm authorization: voorbeeld

Realm authorization



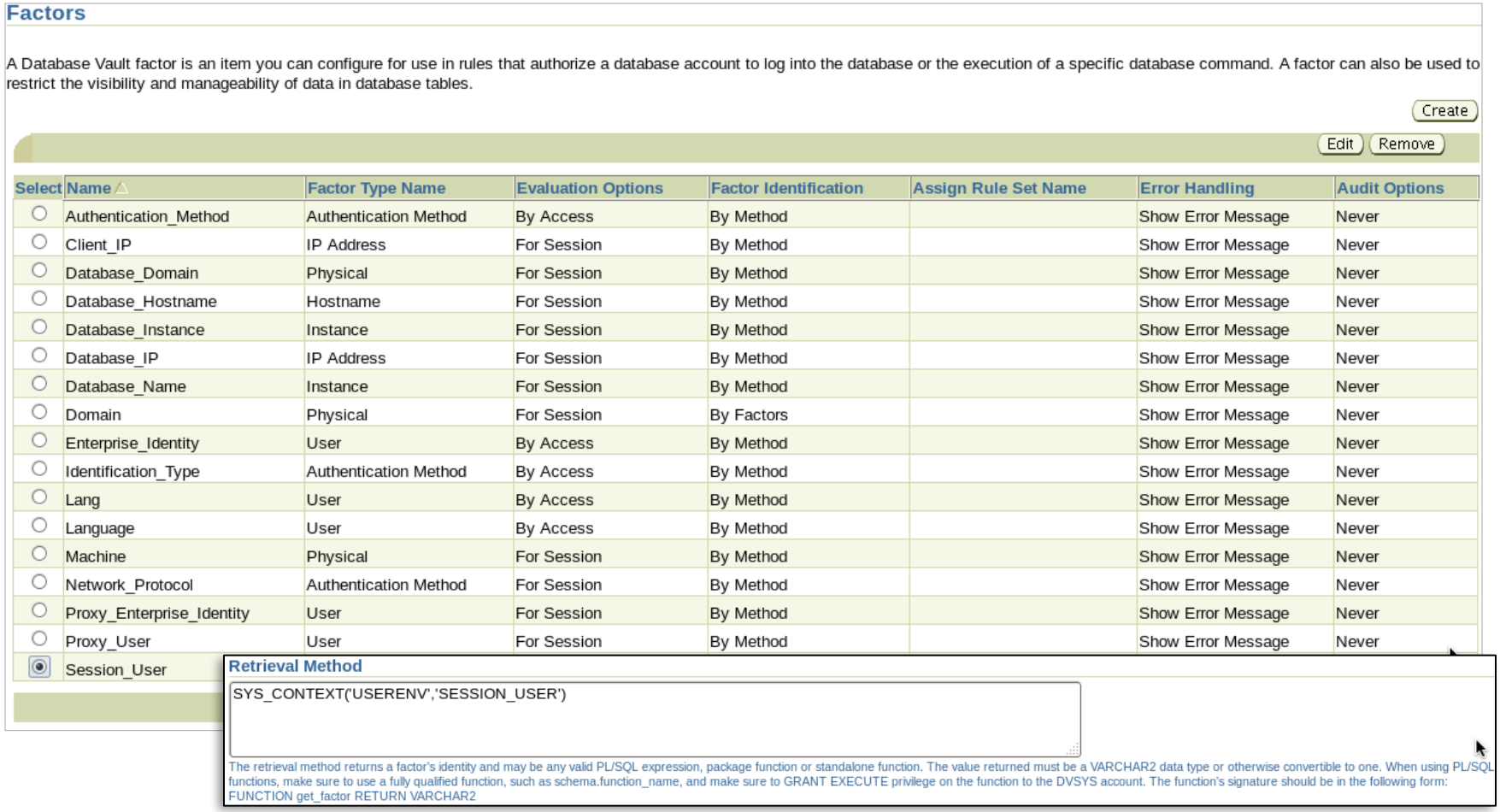
TRANSFER

Factors, rules & rulesets

- factor
  - variabele waarvan de waarde kan worden bepaald en geëvalueerd in een rule
- rule
  - PL/SQL expressie die evalueert als TRUE of FALSE
- ruleset
  - combinatie van één of meerdere rule
  - evaluatie type "All TRUE" of "Any TRUE"

TRANSFER

Factors



Factors

A Database Vault factor is an item you can configure for use in rules that authorize a database account to log into the database or the execution of a specific database command. A factor can also be used to restrict the visibility and manageability of data in database tables.

Create

Edit Remove

Select	Name	Factor Type Name	Evaluation Options	Factor Identification	Assign Rule Set Name	Error Handling	Audit Options
○	Authentication_Method	Authentication Method	By Access	By Method		Show Error Message	Never
○	Client_IP	IP Address	For Session	By Method		Show Error Message	Never
○	Database_Domain	Physical	For Session	By Method		Show Error Message	Never
○	Database_Hostname	Hostname	For Session	By Method		Show Error Message	Never
○	Database_Instance	Instance	For Session	By Method		Show Error Message	Never
○	Database_IP	IP Address	For Session	By Method		Show Error Message	Never
○	Database_Name	Instance	For Session	By Method		Show Error Message	Never
○	Domain	Physical	For Session	By Factors		Show Error Message	Never
○	Enterprise_Identity	User	By Access	By Method		Show Error Message	Never
○	Identification_Type	Authentication Method	By Access	By Method		Show Error Message	Never
○	Lang	User	By Access	By Method		Show Error Message	Never
○	Language	User	By Access	By Method		Show Error Message	Never
○	Machine	Physical	For Session	By Method		Show Error Message	Never
○	Network_Protocol	Authentication Method	For Session	By Method		Show Error Message	Never
○	Proxy_Enterprise_Identity	User	For Session	By Method		Show Error Message	Never
○	Proxy_User	User	For Session	By Method		Show Error Message	Never
◉	Session_User						

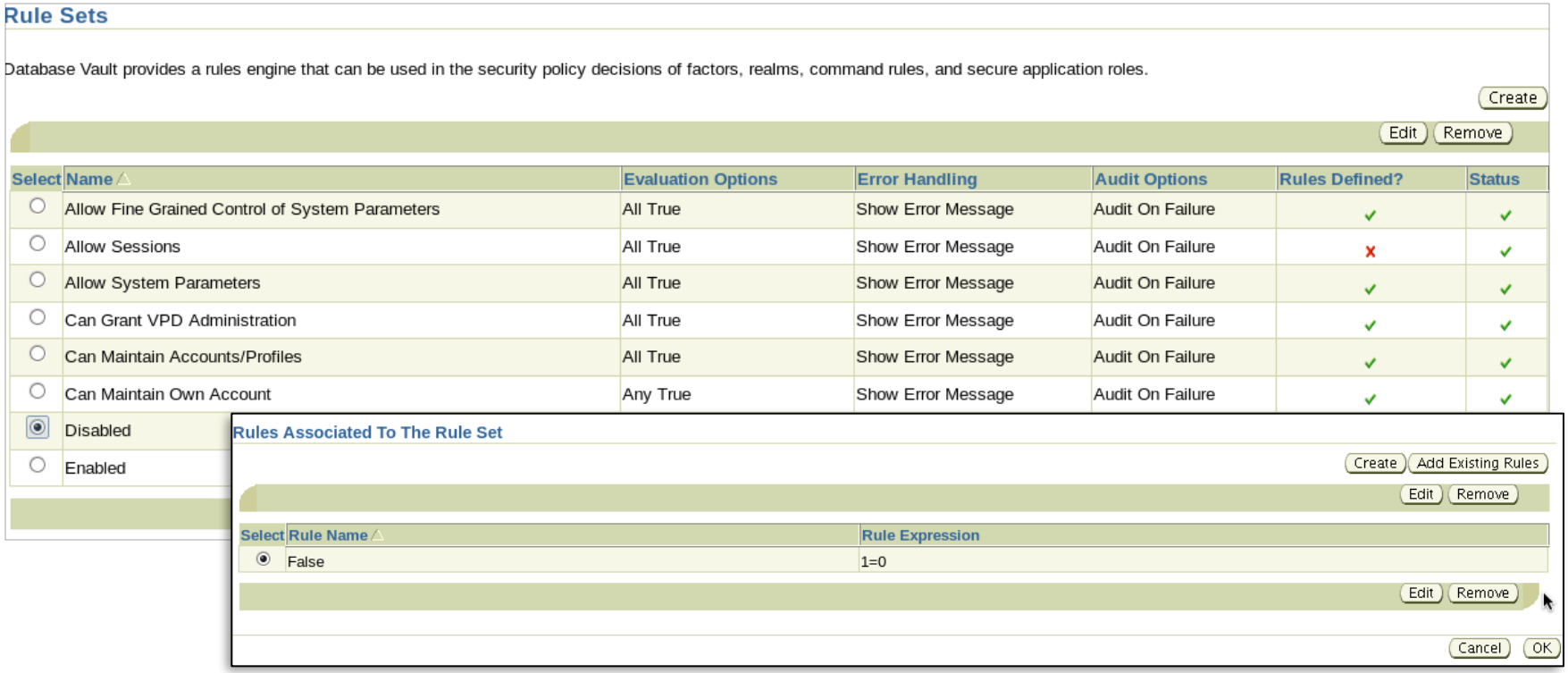
Retrieval Method

SYS_CONTEXT('USERENV','SESSION_USER')

The retrieval method returns a factor's identity and may be any valid PL/SQL expression, package function or standalone function. The value returned must be a VARCHAR2 data type or otherwise convertible to one. When using PL/SQL functions, make sure to use a fully qualified function, such as schema.function_name, and make sure to GRANT EXECUTE privilege on the function to the DVSYS account. The function's signature should be in the following form: FUNCTION get_factor RETURN VARCHAR2

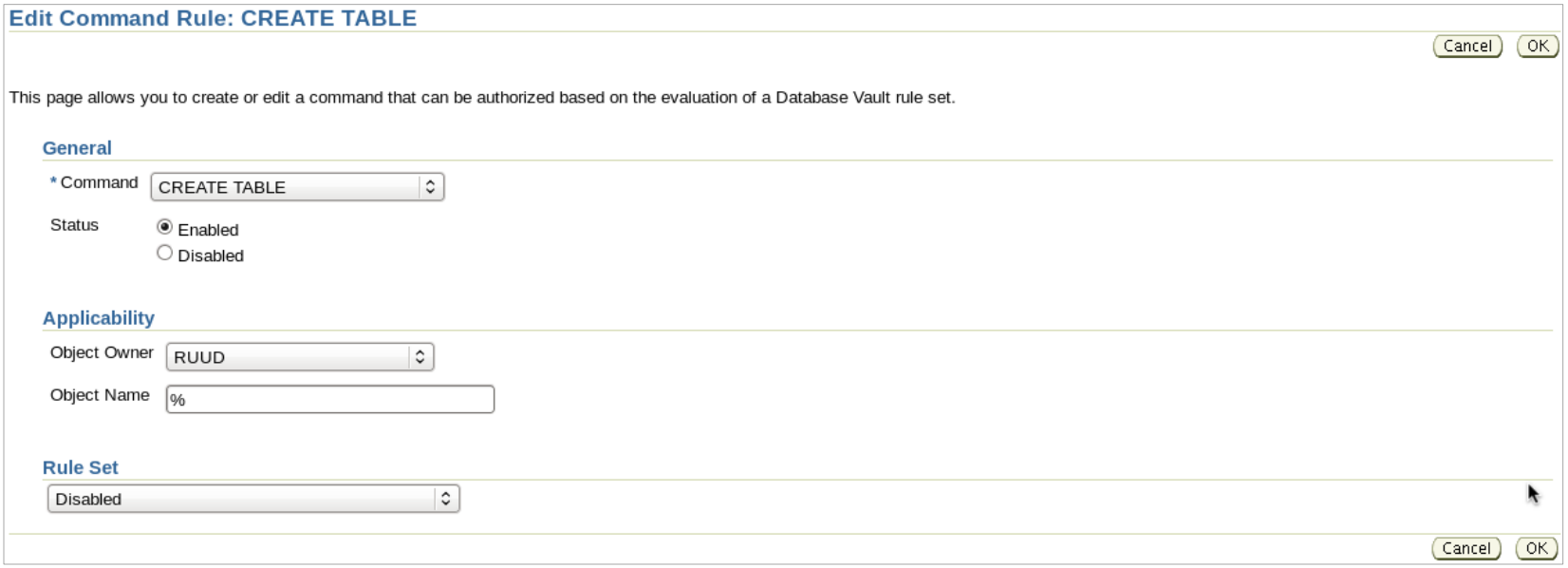
TRANSFER

Rules & rulesets

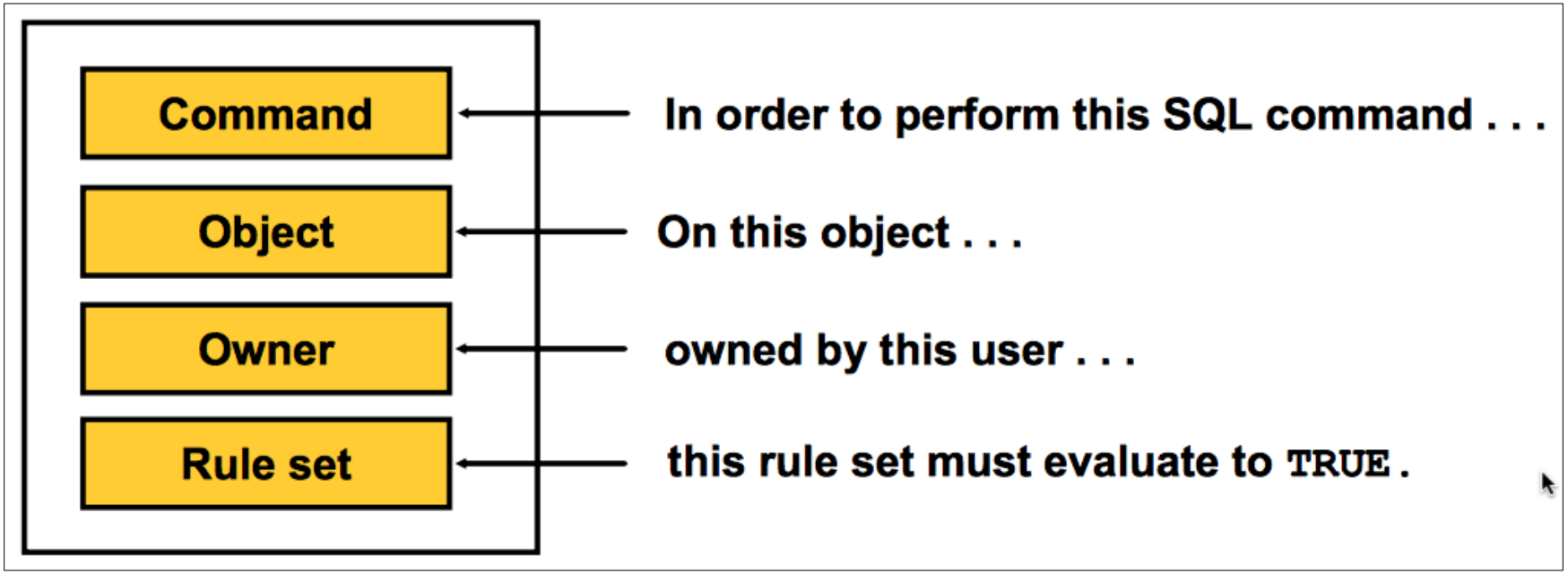


Command rules

- fijnmazige regulering van de toestemming of een SQL commando mag worden uitgevoerd op basis van evaluatie van een ruleset

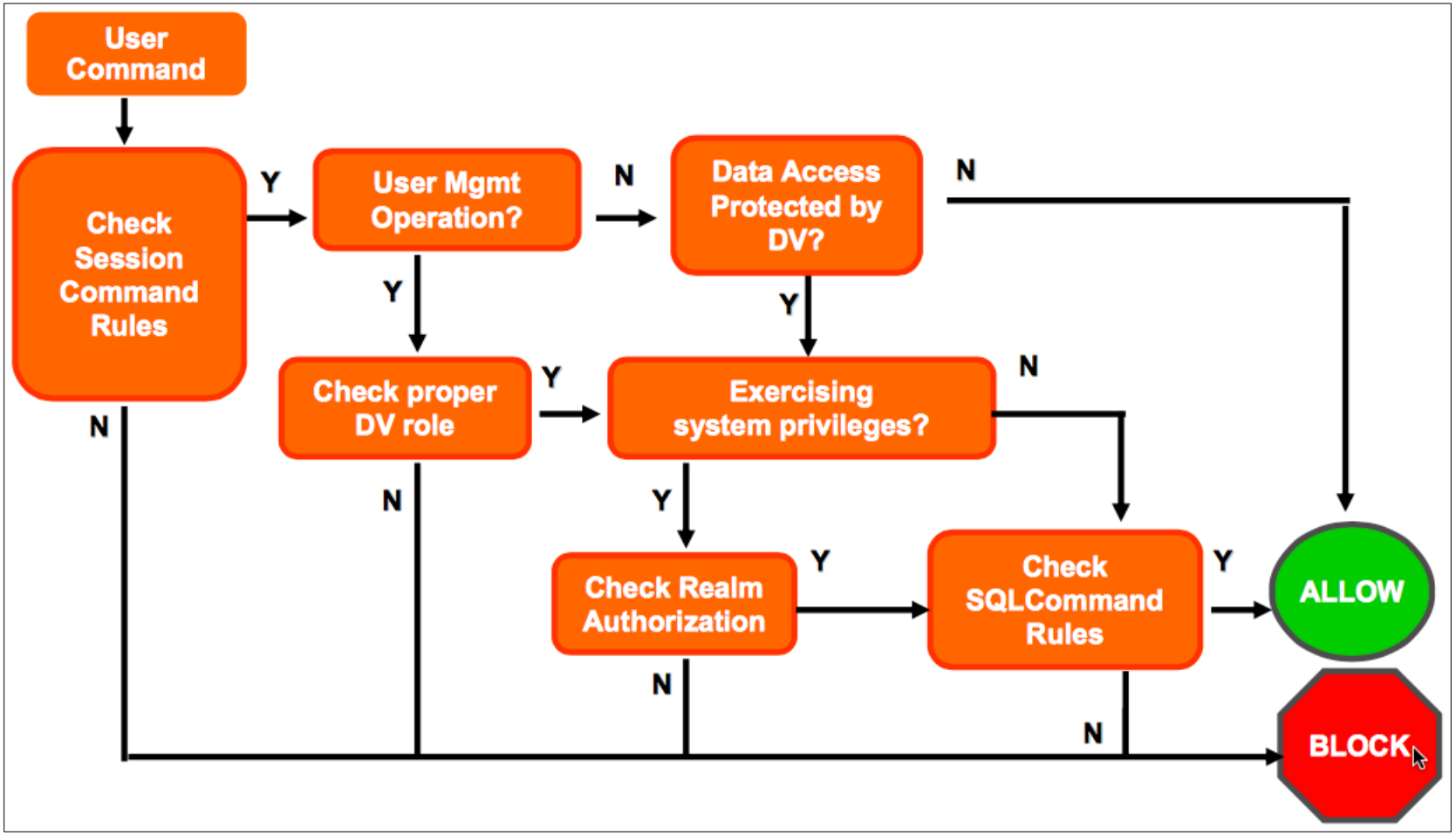


Command rules



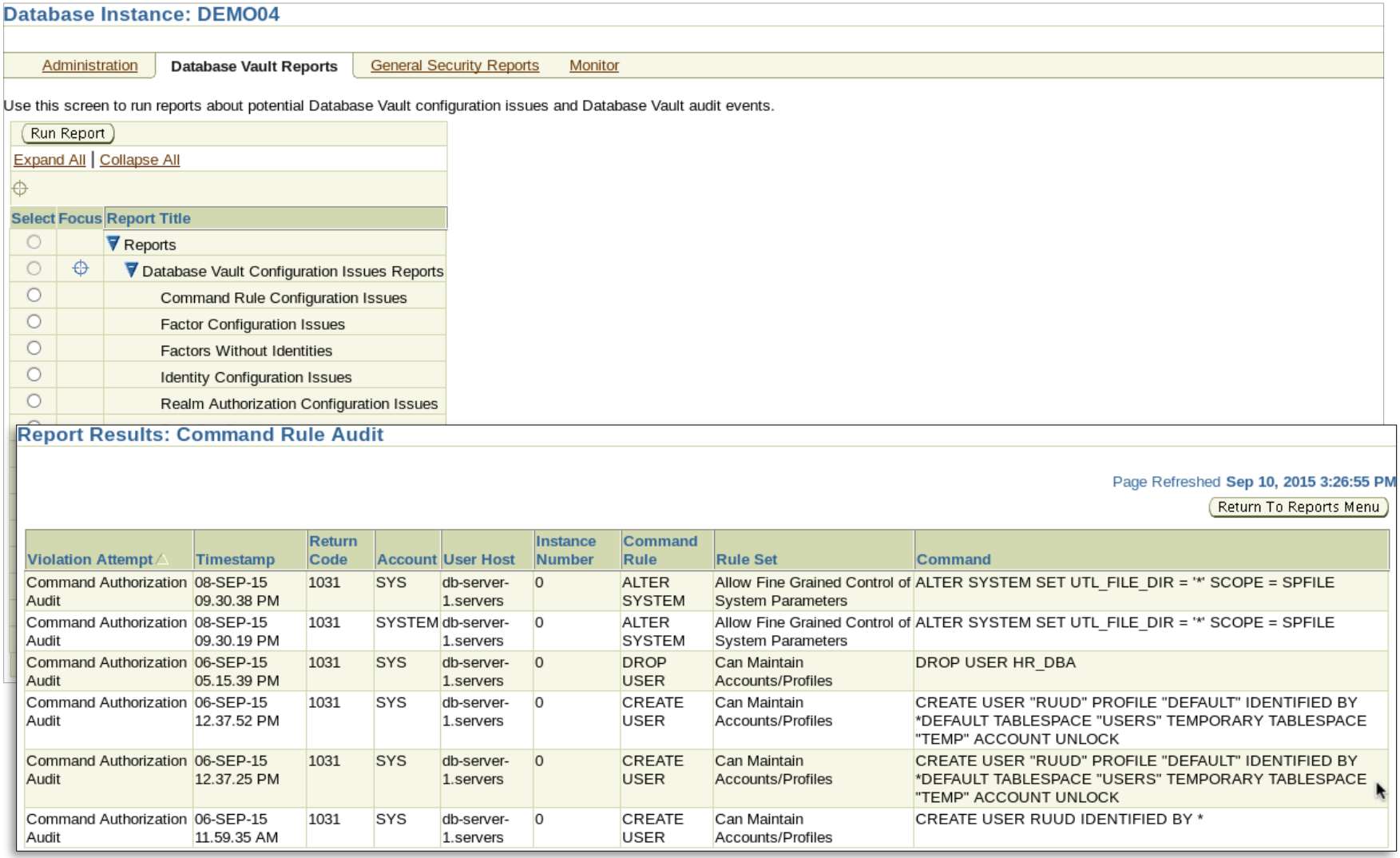
TRANSFER

Database Vault beslissings algoritme



TRANSFER

Audit & reporting



Database Instance: DEMO04

Administration | Database Vault Reports | General Security Reports | Monitor

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

Run Report

Expand All | Collapse All

Select	Focus	Report Title
		Reports
		Database Vault Configuration Issues Reports
		Command Rule Configuration Issues
		Factor Configuration Issues
		Factors Without Identities
		Identity Configuration Issues
		Realm Authorization Configuration Issues

Report Results: Command Rule Audit

Page Refreshed **Sep 10, 2015 3:26:55 PM**

Return To Reports Menu

Violation Attempt	Timestamp	Return Code	Account	User Host	Instance Number	Command Rule	Rule Set	Command
Command Authorization Audit	08-SEP-15 09.30.38 PM	1031	SYS	db-server-1.servers	0	ALTER SYSTEM	Allow Fine Grained Control of System Parameters	ALTER SYSTEM SET UTL_FILE_DIR = '*' SCOPE = SPFILE
Command Authorization Audit	08-SEP-15 09.30.19 PM	1031	SYSTEM	db-server-1.servers	0	ALTER SYSTEM	Allow Fine Grained Control of System Parameters	ALTER SYSTEM SET UTL_FILE_DIR = '*' SCOPE = SPFILE
Command Authorization Audit	06-SEP-15 05.15.39 PM	1031	SYS	db-server-1.servers	0	DROP USER	Can Maintain Accounts/Profiles	DROP USER HR_DBA
Command Authorization Audit	06-SEP-15 12.37.52 PM	1031	SYS	db-server-1.servers	0	CREATE USER	Can Maintain Accounts/Profiles	CREATE USER "RUUD" PROFILE "DEFAULT" IDENTIFIED BY *DEFAULT TABLESPACE "USERS" TEMPORARY TABLESPACE "TEMP" ACCOUNT UNLOCK
Command Authorization Audit	06-SEP-15 12.37.25 PM	1031	SYS	db-server-1.servers	0	CREATE USER	Can Maintain Accounts/Profiles	CREATE USER "RUUD" PROFILE "DEFAULT" IDENTIFIED BY *DEFAULT TABLESPACE "USERS" TEMPORARY TABLESPACE "TEMP" ACCOUNT UNLOCK
Command Authorization Audit	06-SEP-15 11.59.35 AM	1031	SYS	db-server-1.servers	0	CREATE USER	Can Maintain Accounts/Profiles	CREATE USER RUUD IDENTIFIED BY *

TRANSFER

Samenvatting

- Oracle Database Vault
  - security framework, toevoeging aan het standaard security model
  - beschermt database & schema objecten tegen ongeautoriseerde aanpassingen
  - geeft de mogelijkheid te bepalen wie, wat, waar & wanneer m.b.t. aanpassingen
  - dwingt "separation of duty" af
  - uitgebreide auditing & rapportage

TRANSFER

CONSULTING | MANAGED SERVICES | EDUCATION

WWW.TRANSFER-SOLUTIONS.COM