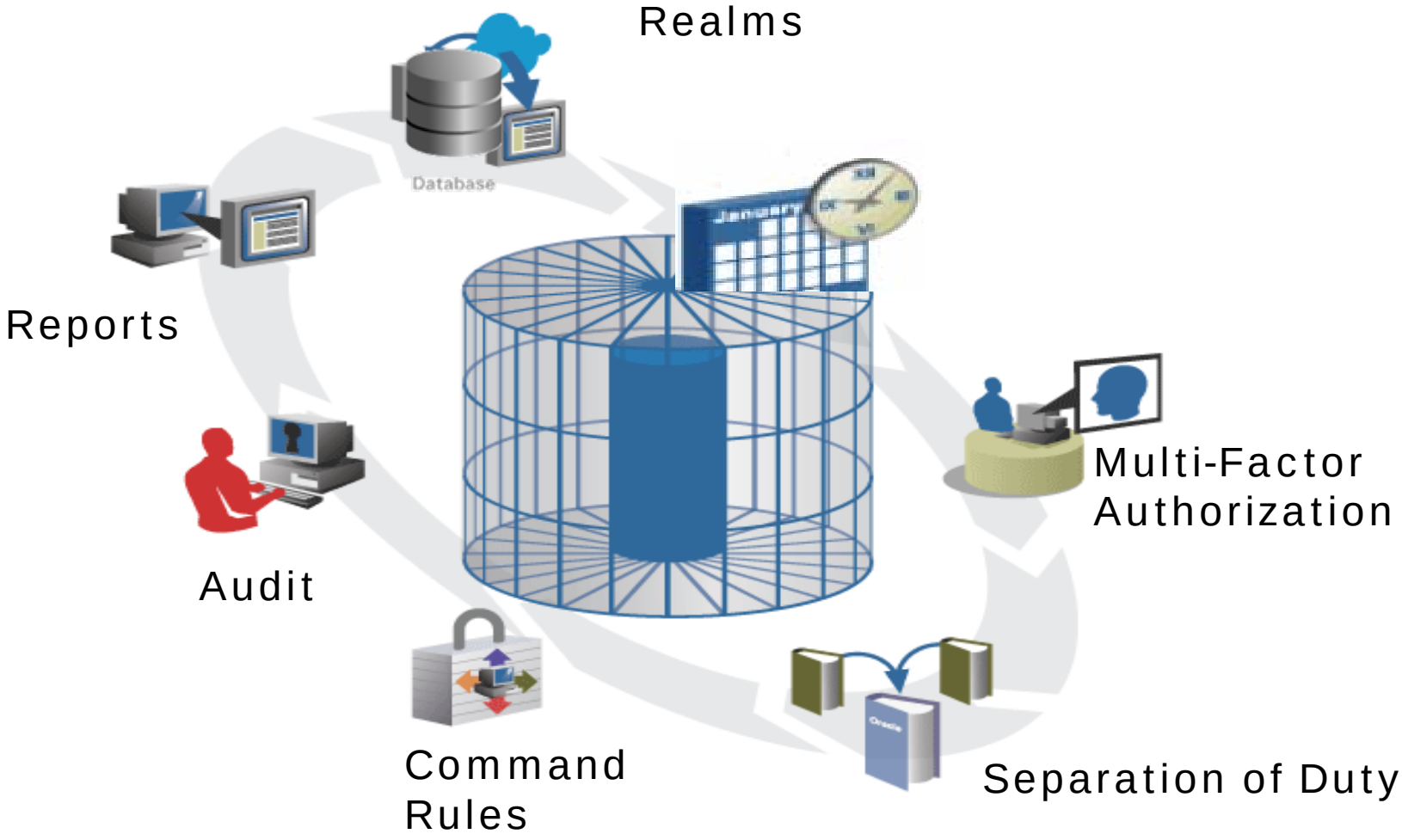
Oracle Database Vault

Zaštita podataka i aplikacija

Zašto Oracle Database Vault

- Nepovjerenje u privilegirane korisnike (DBA,SA)
- Poslovne regulative (npr. Sarbanes Oxley)
- Podjela administrativnih poslova
- Hostanje aplikacija
- Konsolidacija baza podataka


Realms
Database
Reports
Audit
Multi-Factor
Authorization
Command
Rules
Separation of Duty

Sigurnosne mogućnosti i opcije

Enteprise Edition

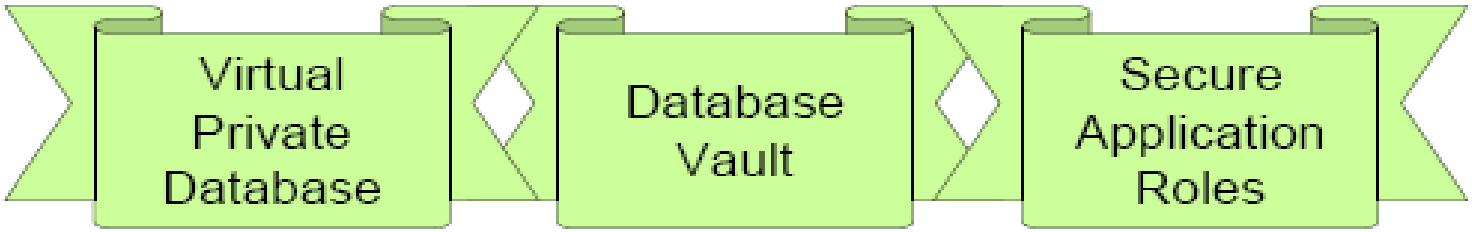
- Virtual Private Database
- RMAN Backup Encryption
- Secure Application Roles

Dodatno licenciranje na EE

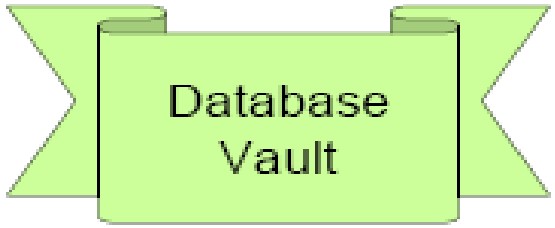
- Advanced Security
- Transparent Data Encryption
- Database Vault
- Label Security
- Secure Backup

Sigurnosni rizici

- Kako da autoriziramo korisnike preko kriterija kao što su npr. vrijeme, mrežni protokol ili IP adresa



- Kako da se zaštitimo od korisnika koji imaju sistemske privilegije kao npr. “SELECT ANY TABLE”



Dostupnost i Uvjeti

- Dostupno za Oracle Database 10g Release 2

Samo verzija 10.2.0.3 za:

- Linux (x86,x86-64, Itanium)
- Windows (32bit, 64bit, Itanium)
- Solaris SPARC 64bit
- HP-UX PA-RISC 64bit
- AIX 5L (64bit)
- Label Security (nije potrebna licenca)
- Enterprise Manager Database Control (ako koristimo GUI)
- Bez ASM instance u istom ORACLE_HOME-u

Zaštita od SYSDBA

- SYSDBA je najmoćnija privilegija, korisnik spojen kao SYSDBA može vidjeti sve podatke u bazi podataka i njima manipulirati čak i ako je baza zaštićena sa Virtual Private Database ili Label Security
- OS korisnik koji pripada DBA grupi (na OS nivou) se može spojiti na bazu podataka sa SYSDBA privilegijom bez lozinke
- Pošto je takva autentifikacija od OS-a, SA može iskoristiti takvo stanje
- Nakon što se instalira ODV ukida se takav nači autentifikacije
- Onemogućava se spajanje kao SYSDBA
- Za većinu operacija treba koristiti SYSOPER

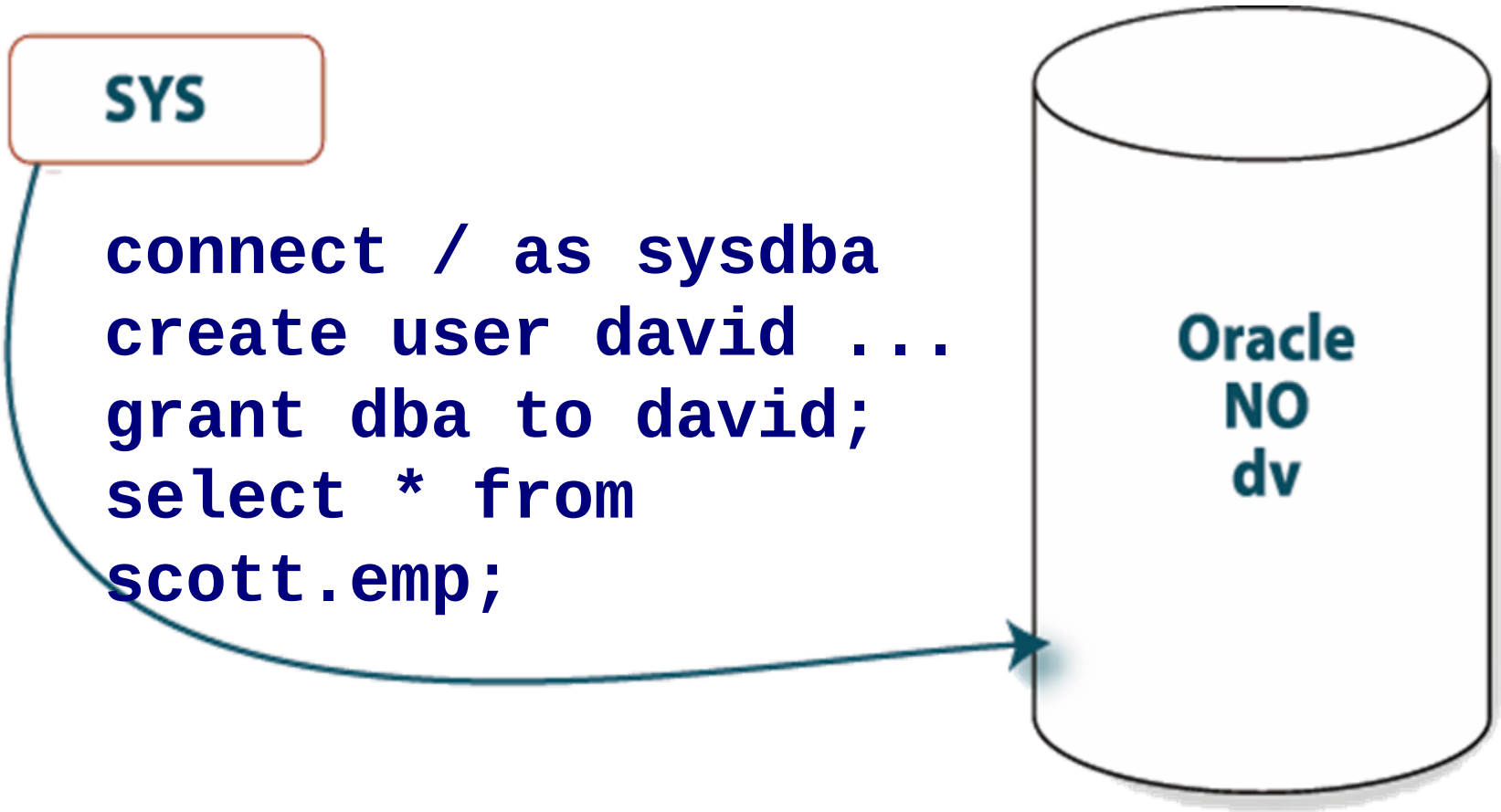
Ipak SYSDBA?

- Data Guard
- RMAN
- Real Application Clusters
- Automatic Storage Management

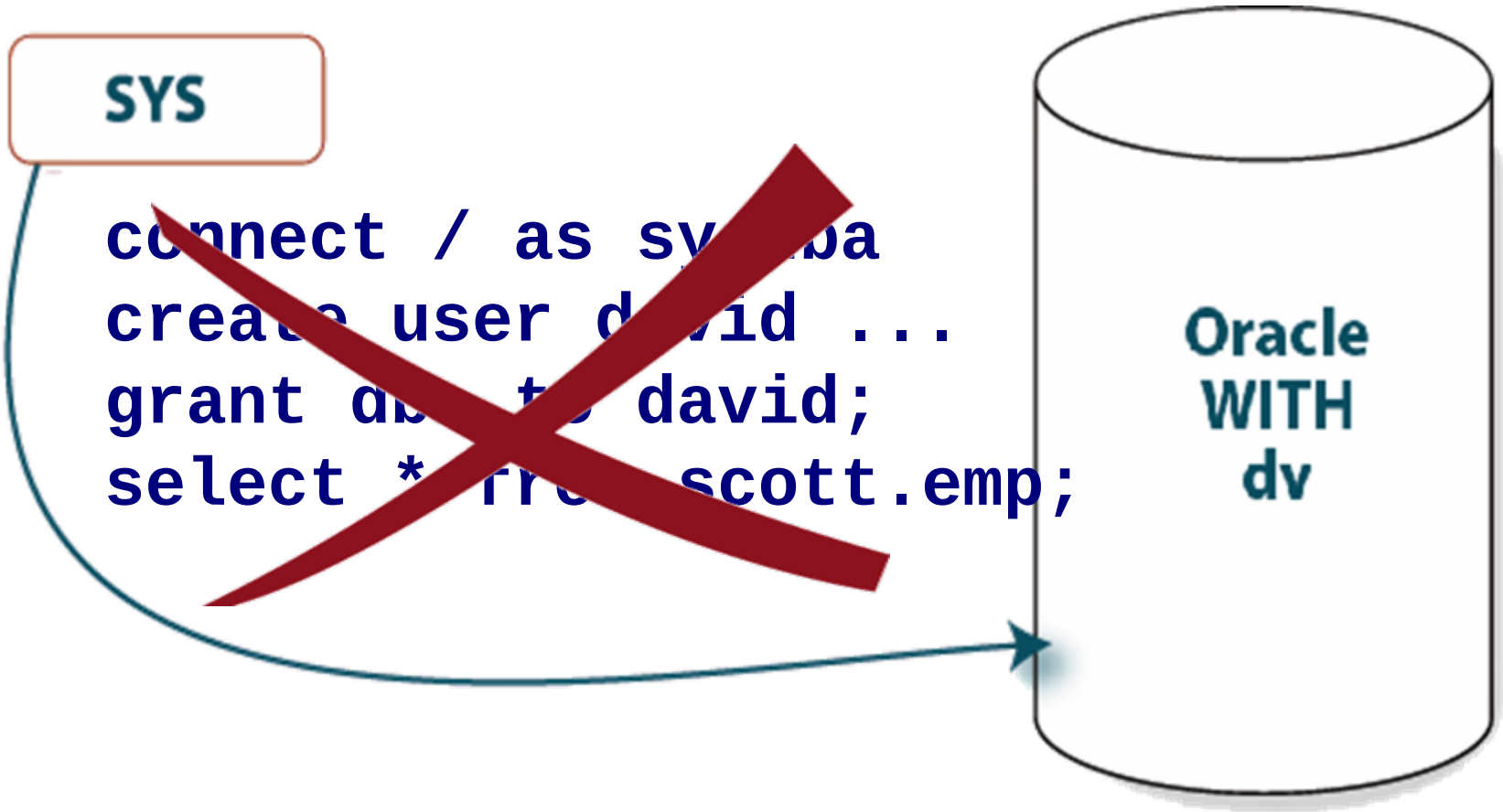
Za omogućiti SYSDBA nakon instalacije ODV-a trebamo rekreirati password datoteku, i pnovno imamo omogućeno spajanje kao SYSDBA,

orapwd file=<File> password=<PW> nosysdba=n

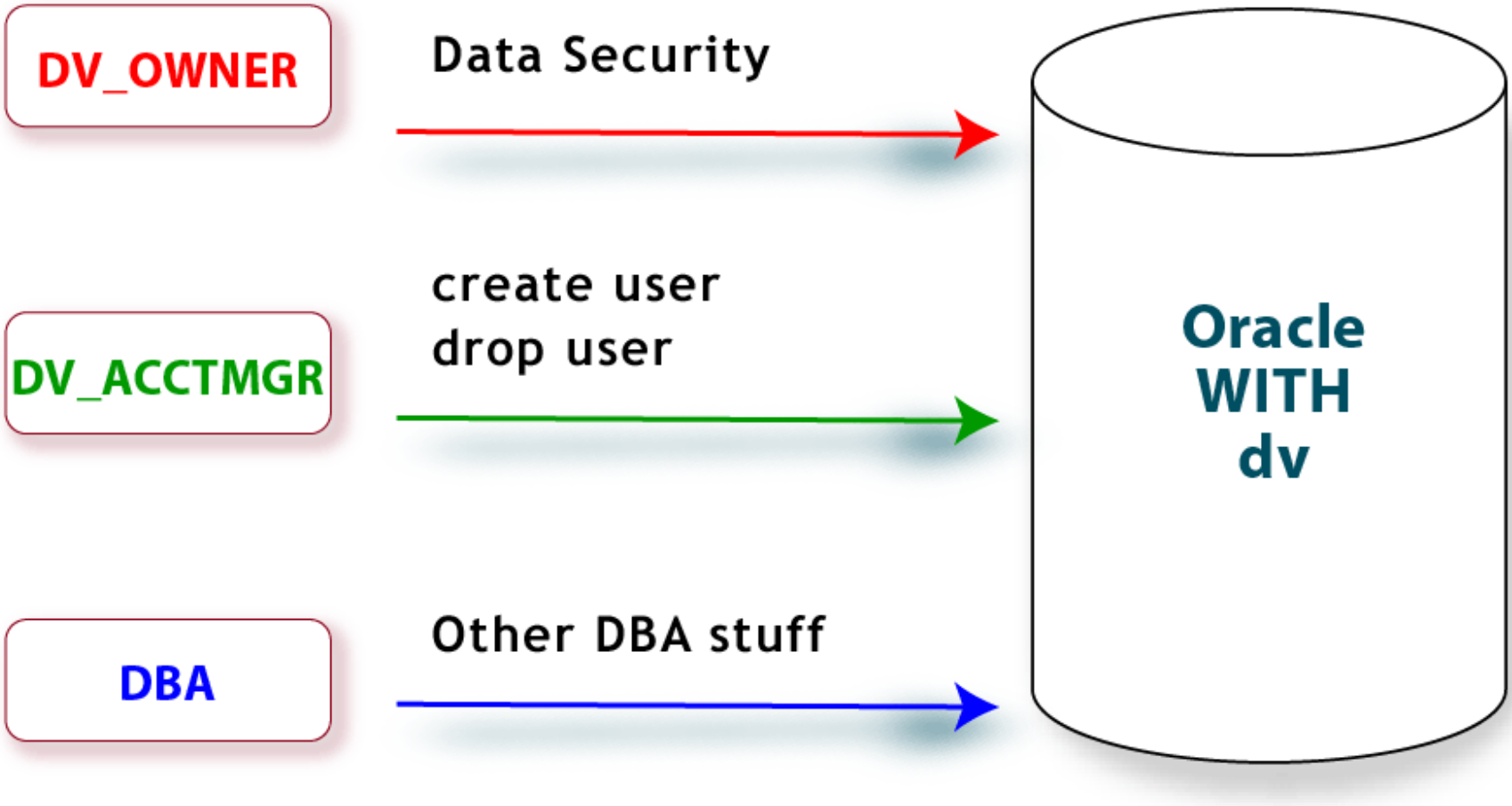
Podjela uloga



Podjela uloga



Podjela uloga



Podjela uloga

Uloga:	DBA	DV_OWNER	DV_ACCTMGR
Korisničko ime:	system	dbv	dbu
Zadaće:	backup/recovery, rad sa tablespace-ovima itd ..	održavanje database vaulta	kreiranje i dropa nje korisnika

Podjela uloga

- DV_OWNER (Database Vault Owner Role) sve privilegije na DVSYS shemi
- DV_ADMIN (Database Vault Configuration Administrator) Izvršna privilegija na DVSYS.DBMS_MACADM
- DV_SECANALYST (Database Vault Security Analyst) Select privilegija na objekte DVSYS sheme

Podjela uloga

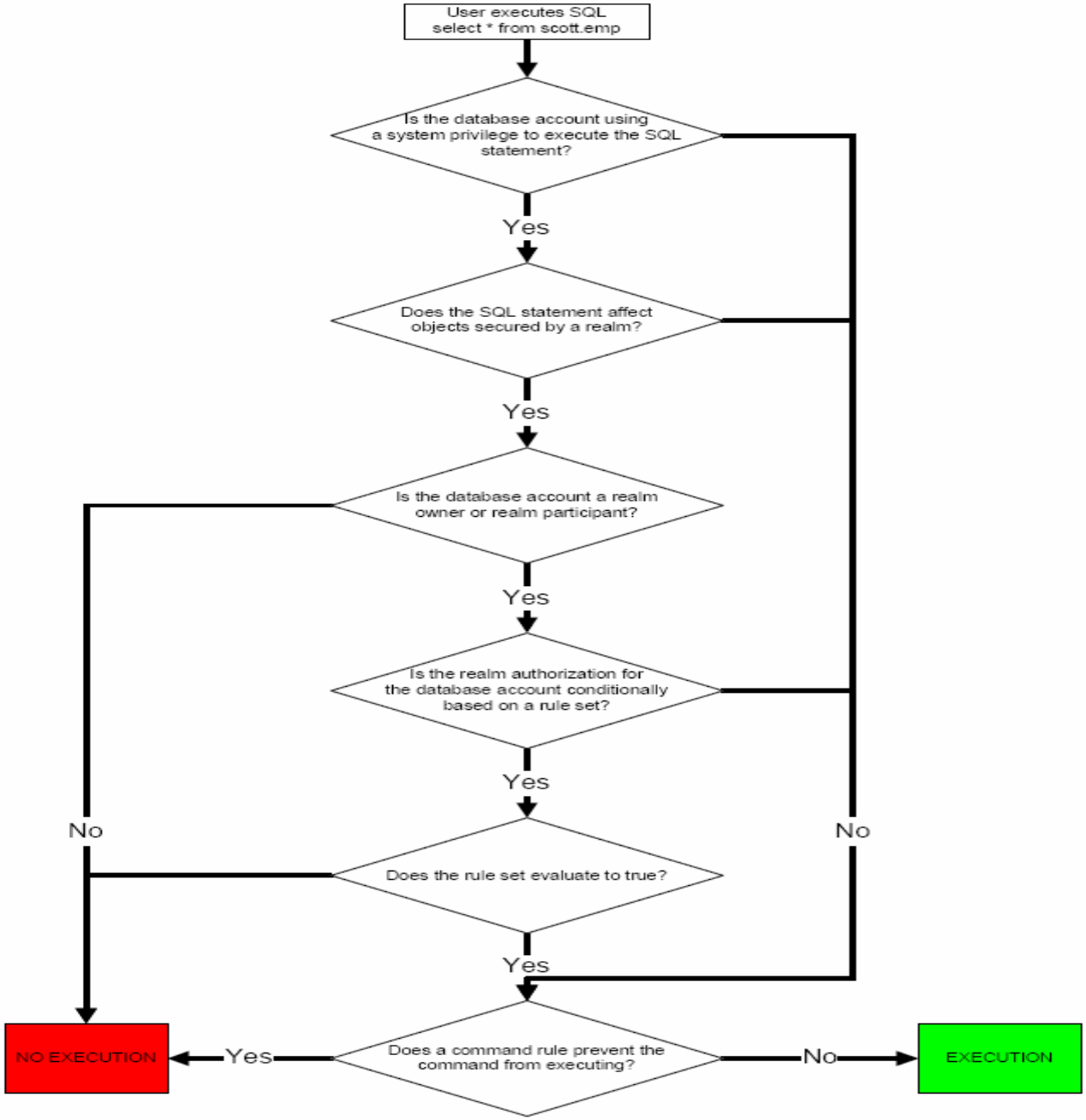
- DV_ACCTMGR

Može manipulirati userima i profilima
CREATE | DROP | ALTER USER
CREATE | DROP | ALTER PROFILE

Nemože dropati ili alterirati DVSYS account

Struktura ODV-a

- Realms
- Command Rules
- Factors
- Rule Sets
- Secure Application Roles


User executes SQL
select * from scott.emp
Is the database account using a system privilege to execute the SQL statement?
Yes
Does the SQL statement affect objects secured by a realm?
Yes
Is the database account a realm owner or realm participant?
Yes
Is the realm authorization for the database account conditionally based on a rule set?
Yes
No
No
Does the rule set evaluate to true?
Yes
NO EXECUTION
Yes
Does a command rule prevent the command from executing?
No
EXECUTION

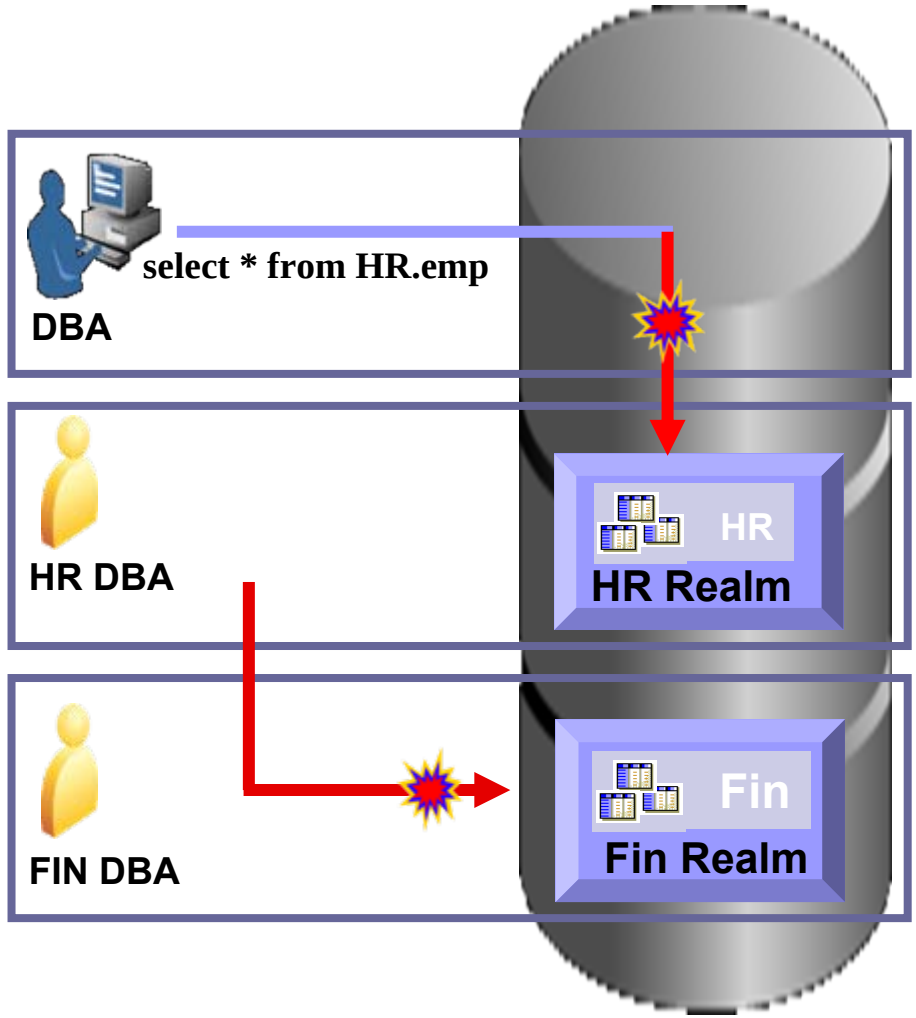
RELM

- **DBA gleda HR podatke**

  Zaštita od insajdera

- **HR DBA gleda Fin.**

  Eliminira sigurnosne rizike kod konsolidacije



Relm

- RELM je funkcionalno grupiranje shema i rola koje moraju biti osigurane za danu aplikaciju
- Imamo nekoliko predefiniranih relmova (Oracle Data Dictionary, Oracle Database Vault, Database Vault Account Management)

-- Create Realm / Role: DV_OWNER or DV_ADMIN

DBMS_MACADM.CREATE_REALM(realm_name => 'Scott Schema Realm', description => 'Realm for all SCOTT Objects', enabled => 'YES', audit_options => 1);

-- Add Objects

DBMS_MACADM.ADD_OBJECT_TO_REALM(realm_name => 'Scott Schema Realm', object_owner => 'SCOTT', object_name => '%', object_type => '%');

Relm vlasnik i participant

- Vlasnik relma

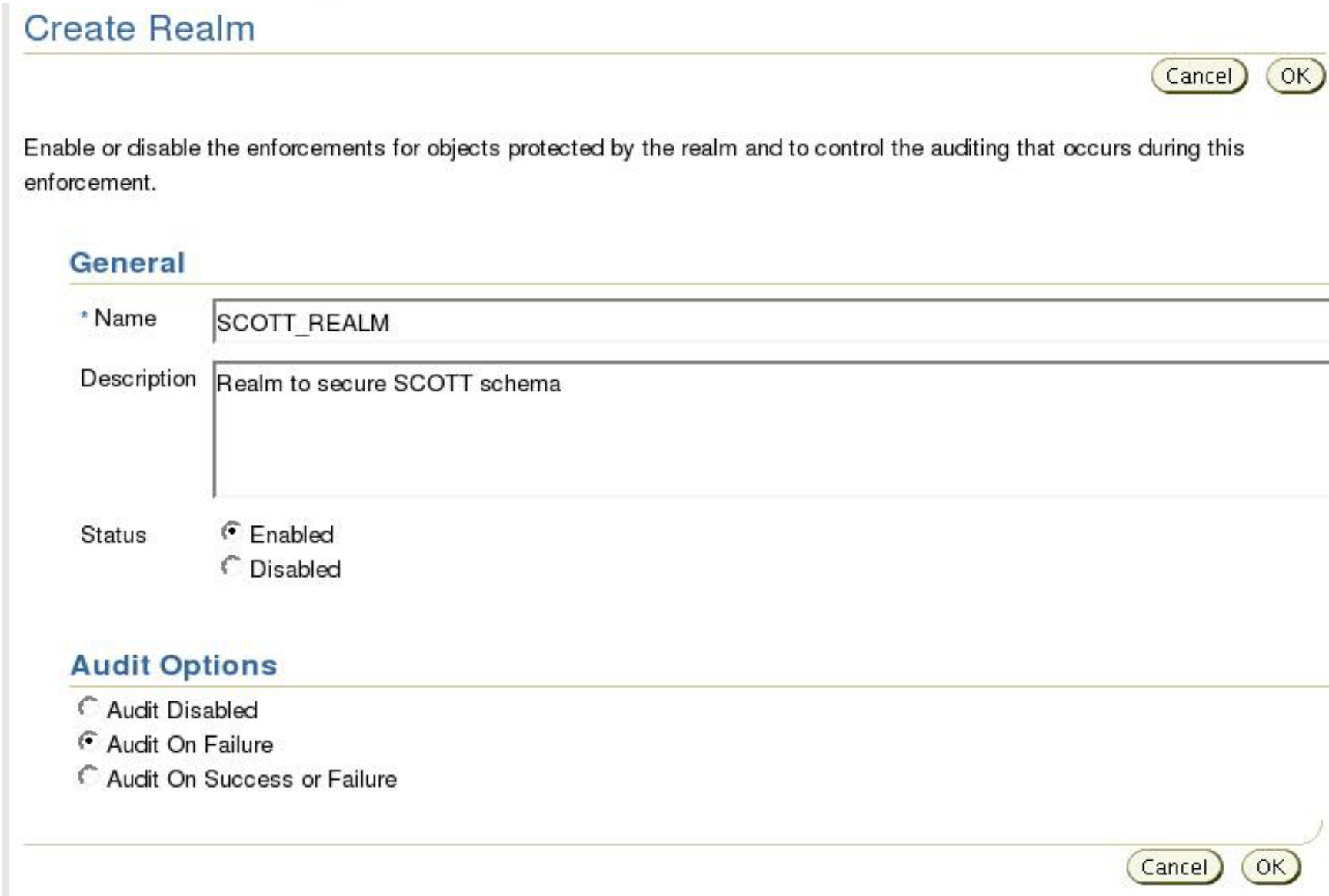
Može svakom dati ili uzeti sigurnosne relm role baze podataka

- Relm participant

Realm participant, može pristupiti objektima u relmu sa standardnom Oracel autentifikacijom.

DBMS_MACADM.ADD_AUTH_TO_REALM(realm_name => 'Scott Schema Realm', grantee => 'SYSTEM', auth_options => 0); -- 0 Participan / 1 Owner

Kreiranje Relm-a kroz GUI



Osiguravanje objekata

Database 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
○	Database Vault Account Management	Audit On Failure	✓	✓	✓	✓
○	Oracle Data Dictionary	Audit On Failure	✓	✓	✓	✓
○	Oracle Database Vault	Audit On Failure	✓	✓	✓	✓
○	Oracle Enterprise Manager	Audit On Failure	✓	✓	✓	✓
◉	SCOTT_REALM	Audit On Failure		✗	✗	✓

Edit Remove

Osiguravanje objekata

Realm Secured Objects

Create

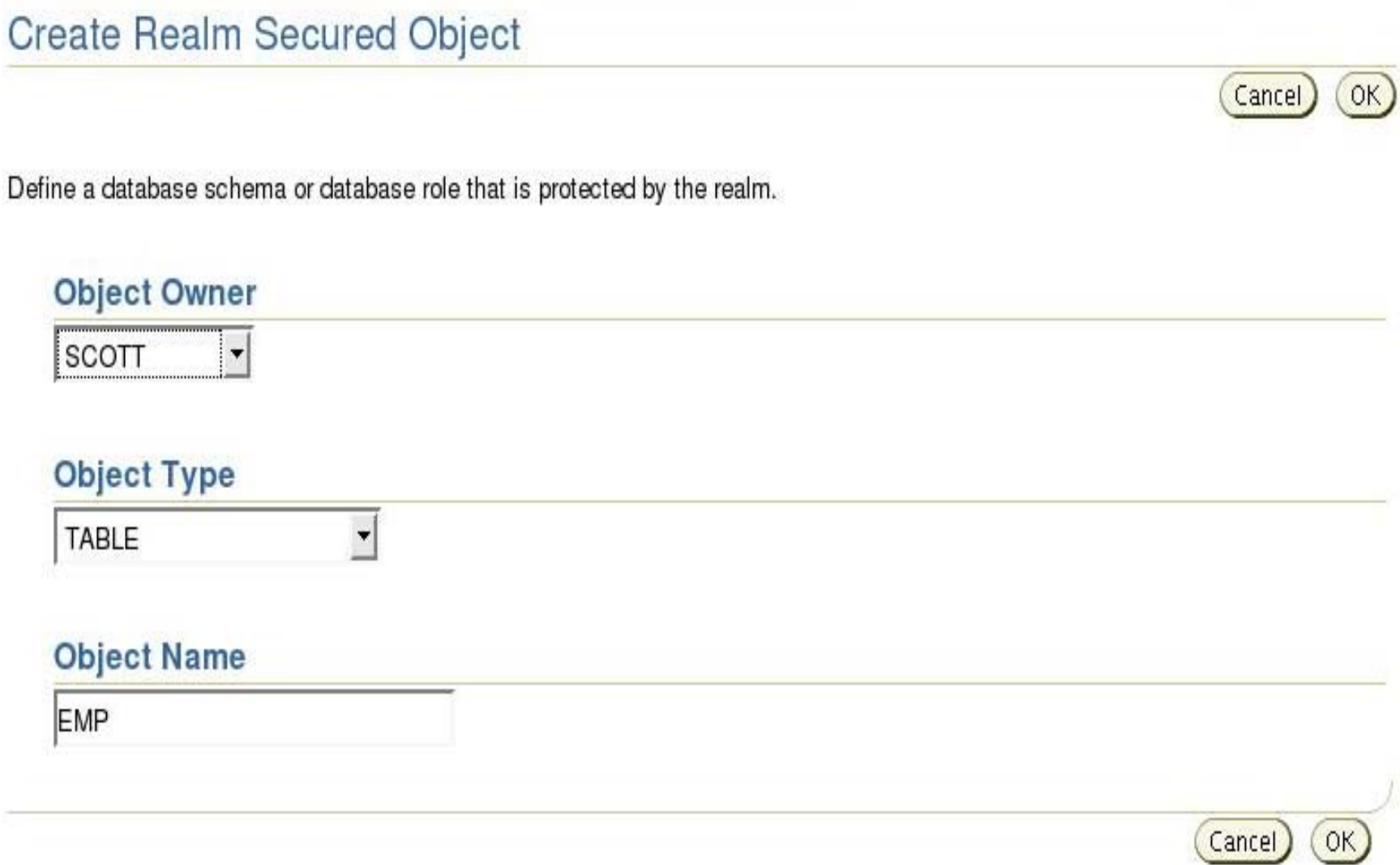
Select	Owner	Object Type	Object Name
	No Items Found		

Realm Authorizations

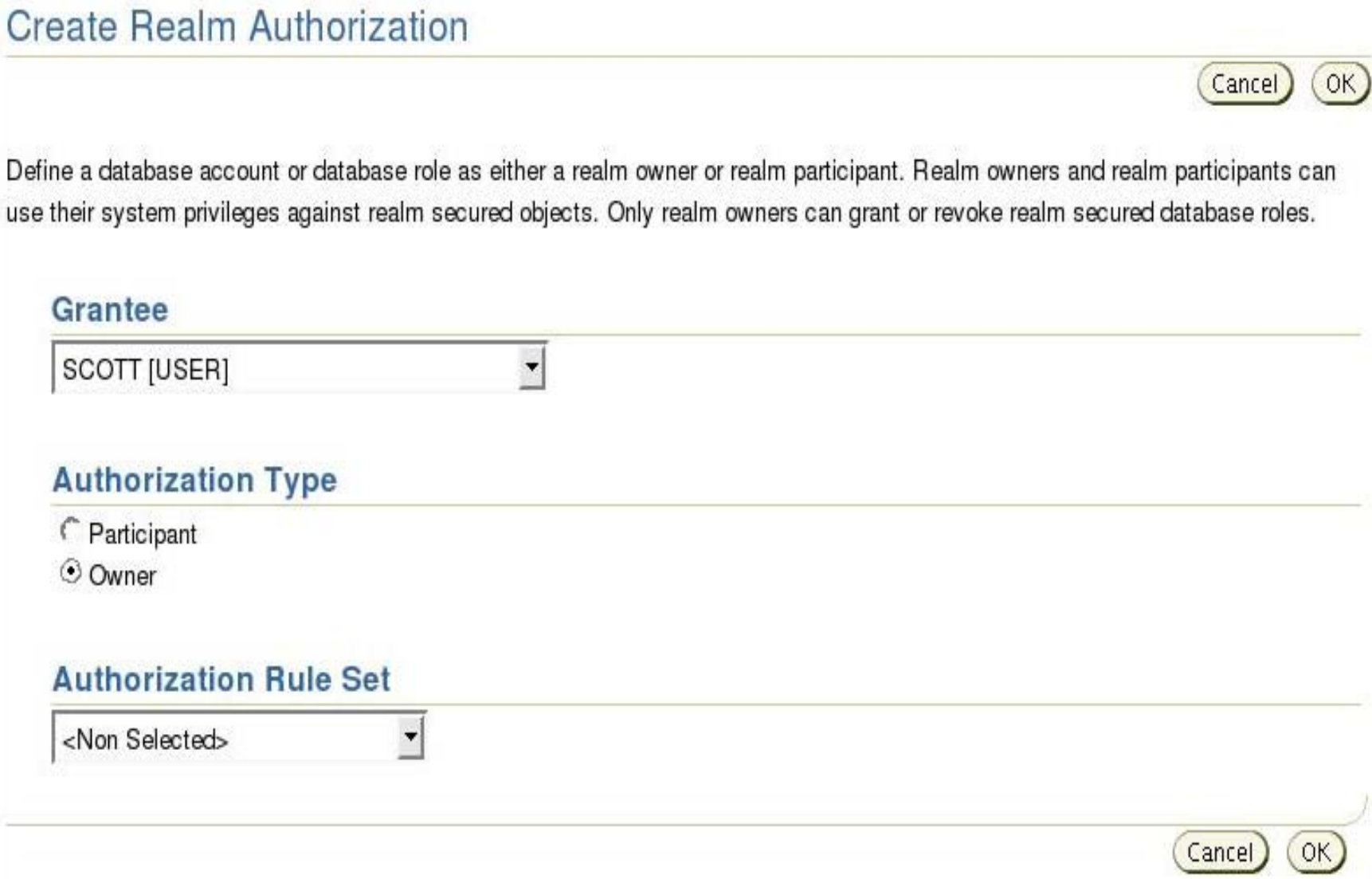
Create

Select	Grantee	Authorization Options	Authorization Rule Set Name
	No Items Found		

Osiguravanje objekata



Kreiranje vlasnika relma



Osiguravanje objekata

Osiguravanje objekata

Realms

Database 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
◉	Database Vault Account Management	Audit On Failure	✓	✓	✓	✓
○	Oracle Data Dictionary	Audit On Failure	✓	✓	✓	✓
○	Oracle Database Vault	Audit On Failure	✓	✓	✓	✓
○	Oracle Enterprise Manager	Audit On Failure	✓	✓	✓	✓
○	SCOTT_REALM	Audit On Failure		✓	✓	✓

Edit Remove

Osiguravanje objekata

```
SQL> select * from scott.emp;
select * from scott.emp
              *
ERROR at line 1:
ORA-01031: Insufficient Privileges
```

```
SQL> select * from scott.dept;
    DEPTNO DNAME          LOC
---------- -------------- --------
        10 ACCOUNTING     NEW YORK
        20 RESEARCH       DALLAS
        30 SALES          CHICAGO
        40 OPERATIONS     BOSTON
SQL>
```

Rule Sets (skupovi pravila)

Rule Set je skup jednog ili više pravila koja povezujemo sa autorizacijom na realm, raspodjelom faktora, komandnih pravila ili zaštićenih aplikacijskih rola.Rule Set može biti *true* ili *false* s obzirom na procjenu svakog pravila koje i evaluacijski tip (Svi *True* ili bilo koji *True*). Rule (pravilo) u rule setu je PL/SQL izraz koji evaluira u T ili F. Jedno pravili može pripadati u više skupova pravila.

Rule Sets

```
DBMS_MACADM.CREATE_RULE_SET(
rule_set_name => 'ScottSecure',
description => 'Only SSL Connection allowed',
enabled => 'YES',
eval_options => 1, --ALL
audit_options => POWER(2,1), --Audits whenever the
rule set is used
fail_options => 1,
fail_message => NULL,
fail_code => NULL,
handler_options => NULL,
handler => NULL);
```

Rules (pravila)

Rule (pravilo) u rule setu je PL/SQL izraz koji evaluira u T ili F. Jedno pravilo može pripadati u više skupova pravila.

Rules (pravila)

```
DBMS_MACADM.CREATE_RULE(
rule_name => 'SecureClientConnection',
rule_expr =>
'GET_FACTOR(''Network_Protocol'') =
''tcps''');

-- Add Rule to the Ruleset
DBMS_MACADM.ADD_RULE_TO_RULE
_SET(
rule_set_name => 'ScottSecure',
rule_name => 'SecureClientConnection',
rule_order => 2,
enabled => 'YES');
```

Faktori

- *Faktori* su varijable ili atributi prepoznati od Oracle Data Vaulta poput korisnikove lokacije, IP adrese ili sesije. *Faktori* se mogu koristiti za aktivnosti poput autorizacije korisnika na bazu podatakaili kreiranje filtrirajuće logike da onemogućimo vidljivost ili upravljivost podacima.
- *Faktori* se mogu koristiti u kombinaciji sa *Rulovima i Rule Set-ima*.
- ODV pruža skup zadanih faktora ,mogu se kreirati vlastiti faktori bazirani na ovim zadanim koristeći svoje PL/SQL pristupne metode. Zadani faktori su:
  - Način autorizacije (Password- lokalni korisnik baze podataka ili SYSDBA/SYSOPER korisnik koji korisit password file, Kerberose, SSL, SYSDBA/SYSOPER OS,)
  - IP adresa korisnika
  - Domena baze podataka
  - Ime servera na kojem je baza podataka
  - Ime instance
  - IP adresa baze podataka
  - Ime baze podataka

Faktori

```
DBMS_MACADM.CREATE_FACTOR(
factor_name => 'Network_Protocol',
factor_type_name => 'Authentication Method',
description => 'Network protocol begin used for
communication',
rule_set_name => NULL,
get_expr => NULL,
validate_expr =>
'UPPER(SYS_CONTEXT(''USERENV'',''IP_ADDRESS'
'))',
identify_by => 1, --By Method
labeled_by => 0, --By Self
eval_options => 0, --By Session
audit_options => POWER(2,0), --Always audits
fail_options => POWER(2,0)); --Shows an error
message.
```

Command Rules (komandna pravila)

Command rule su pravila koja štite jedan ili više objekata baze podataka od SELECT, DDL i DML naredbi. *command rules* se grupiraju u *rule set-ovima*. *Command rule* djeluju na svakog tko koristi SQL izraze na objektima koje on štiti bez obzira na *Realm* u kojem se objekti nalaze.

Command rule ima sljedeće atribute:

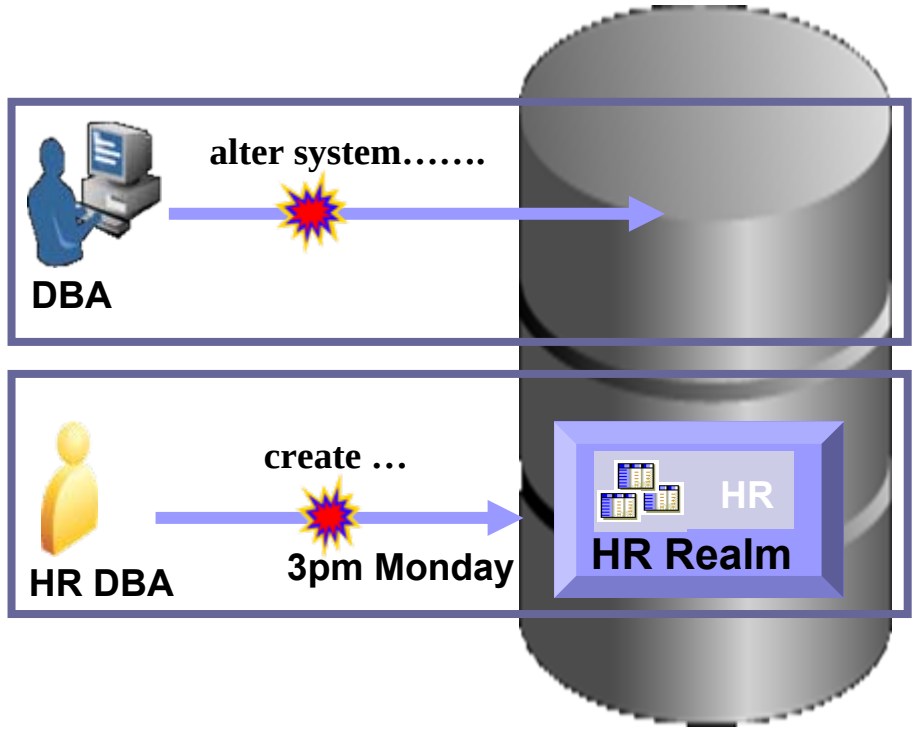
- SQL izraz od kojeg CR štiti
- Vlasništvo objekta na koji se primjenjuje CR
- Objekt bazr podataka na koji se CR odnosi
- Dali je CR aktiviran ili ne
- Odgovarajući *rule set* CR-a

Command Rules (komandna pravila)

```
DBMS_MACADM.CREATE_COMMAND_RULE(
command => 'CREATE USER',
rule_set_name => 'Can Maintain Accounts/Profiles',
object_owner => '%',
object_name => '%',
enabled => 'YES');
```

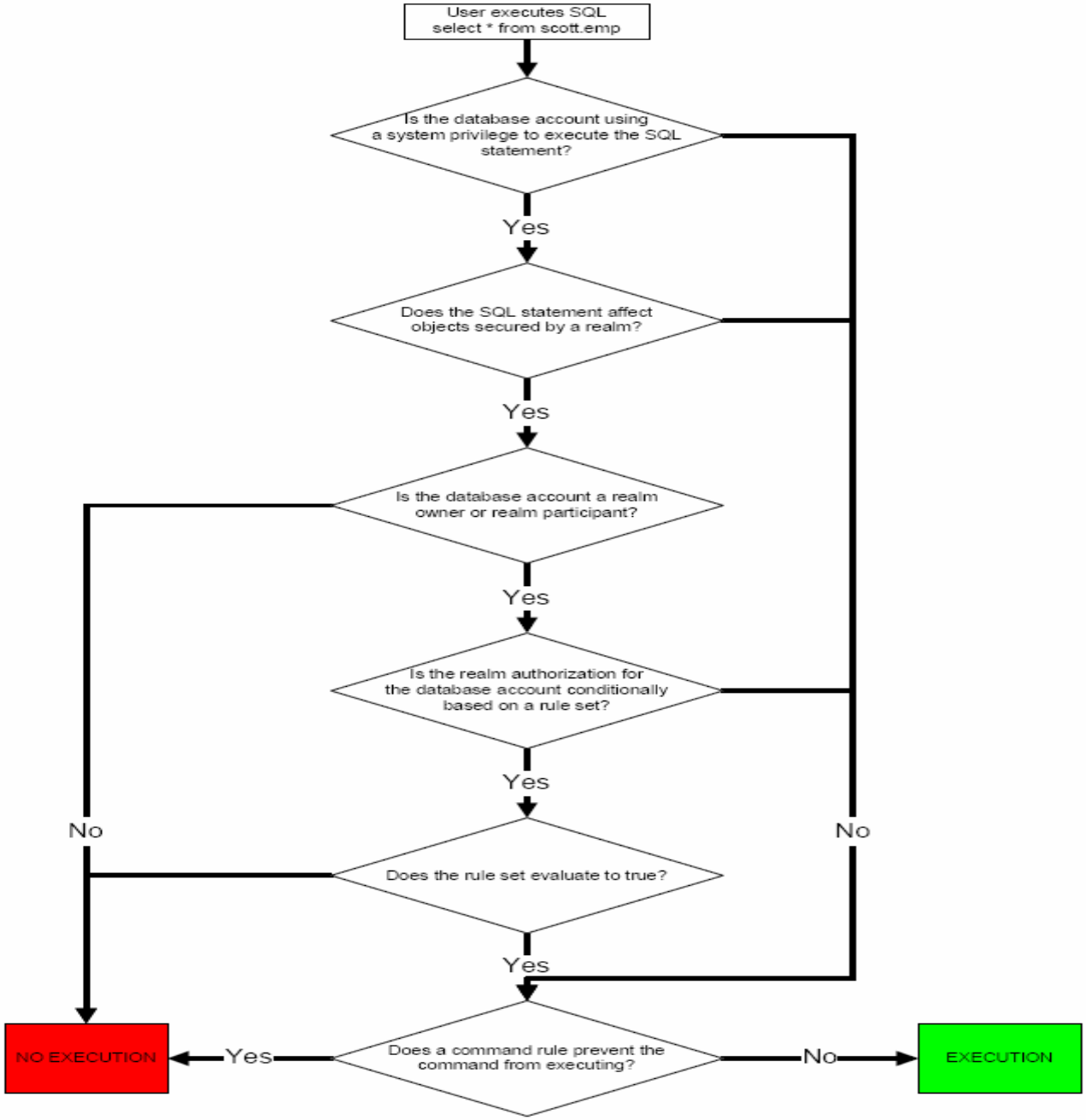
ODV Pravila i Faktori

- **DBA sa udaljenog računala**
  - Pravilo bazirano na IP adresi blokira akciju
- **HR DBA pokušava napraviti neautoriziranu akciju tijekom produkcije**
  - Pravilo bazirano na datumu i vremenu blokira akciju

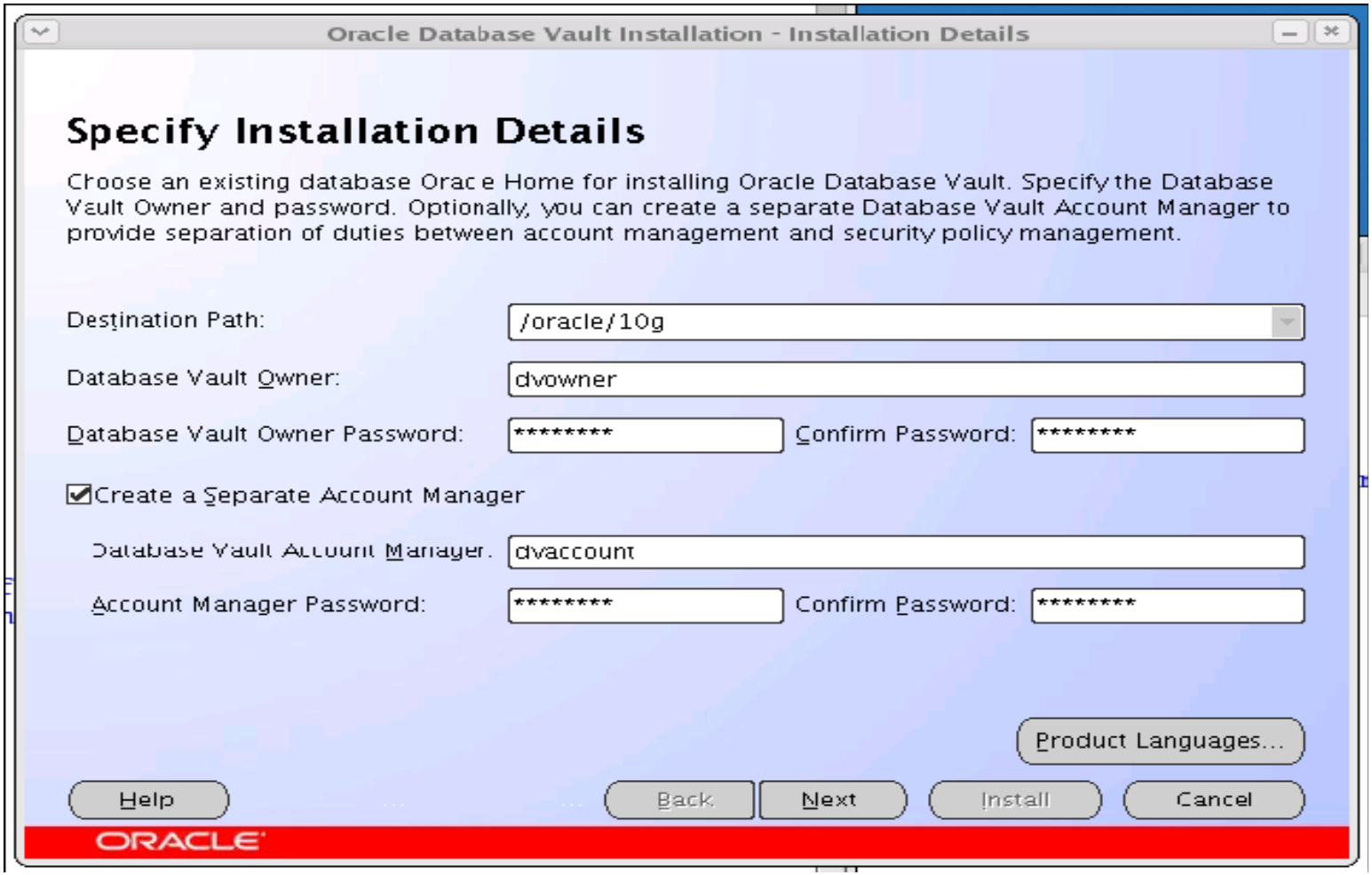


SIGURNOSNE APLIKACIJSKE ROLE

U Oracle Database Vault-u, mogu se kreirati sigurnosne aplikacijske role koje se aktiviraju sa Oracle Database Vault skupom pravila. Svrha korištenja sigurnosnih aplikacijskih rola je onemogućavanje korisnicima pristupanje podacima van aplikacije. One prisiljavaju korisnika da radi u aplikacijskom sučelju sa aplikacijskim privilegijama koje su mu grantane rolama. Prednost baze podataka koja sigurnost temelji na rolama u skupovima pravila je to da tako imamo sigurnosnu politiku baze podataka na jednom centralnom mjestu, nasuprot držanju aplikacijskih rola u svakoj pojedinoj aplikaciji.

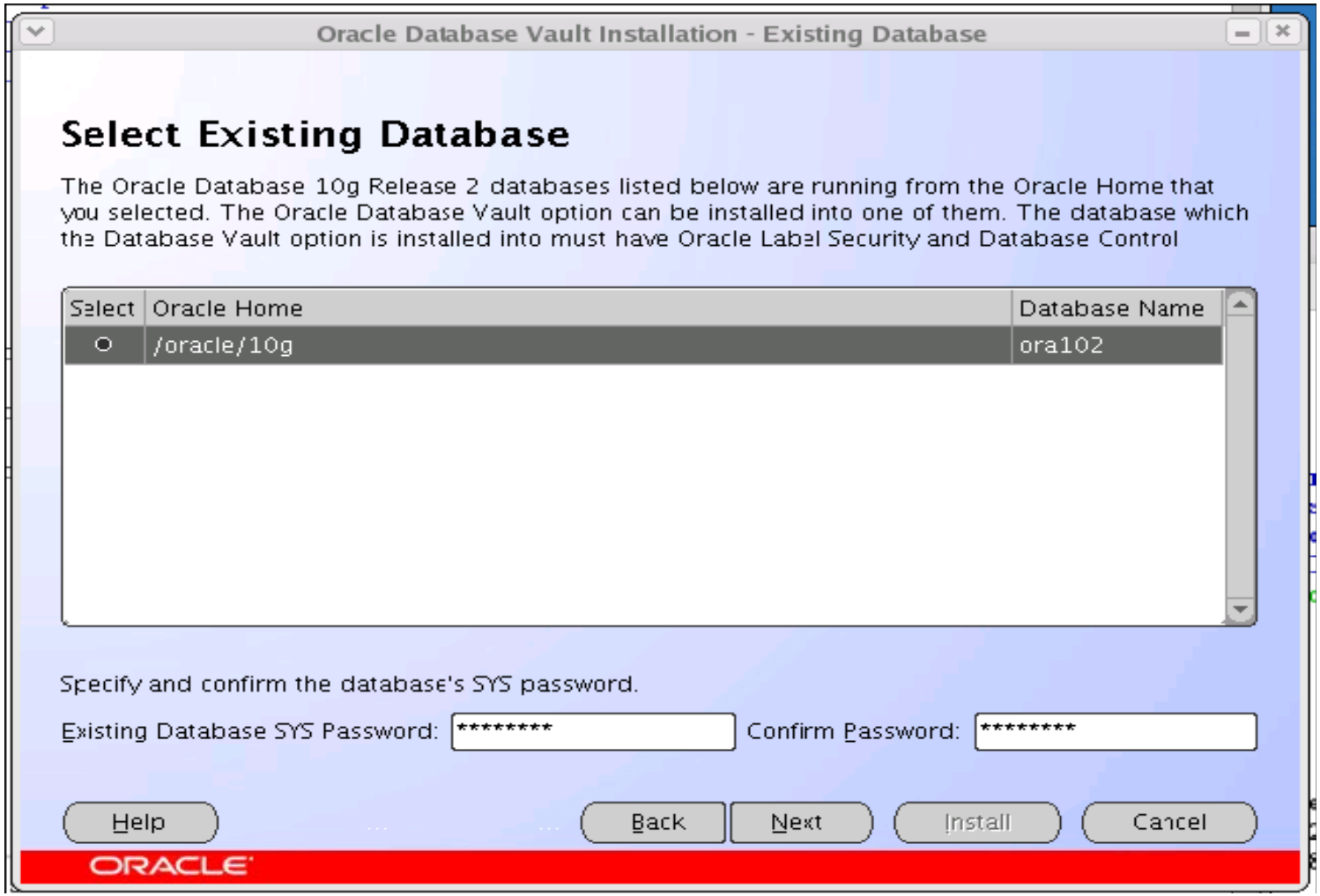

User executes SQL
select * from scott.emp
Is the database account using a system privilege to execute the SQL statement?
Yes
Does the SQL statement affect objects secured by a realm?
Yes
Is the database account a realm owner or realm participant?
Yes
Is the realm authorization for the database account conditionally based on a rule set?
Yes
No
No
Does the rule set evaluate to true?
Yes
NO EXECUTION
Yes
Does a command rule prevent the command from executing?
No
EXECUTION

ODV Instalacija

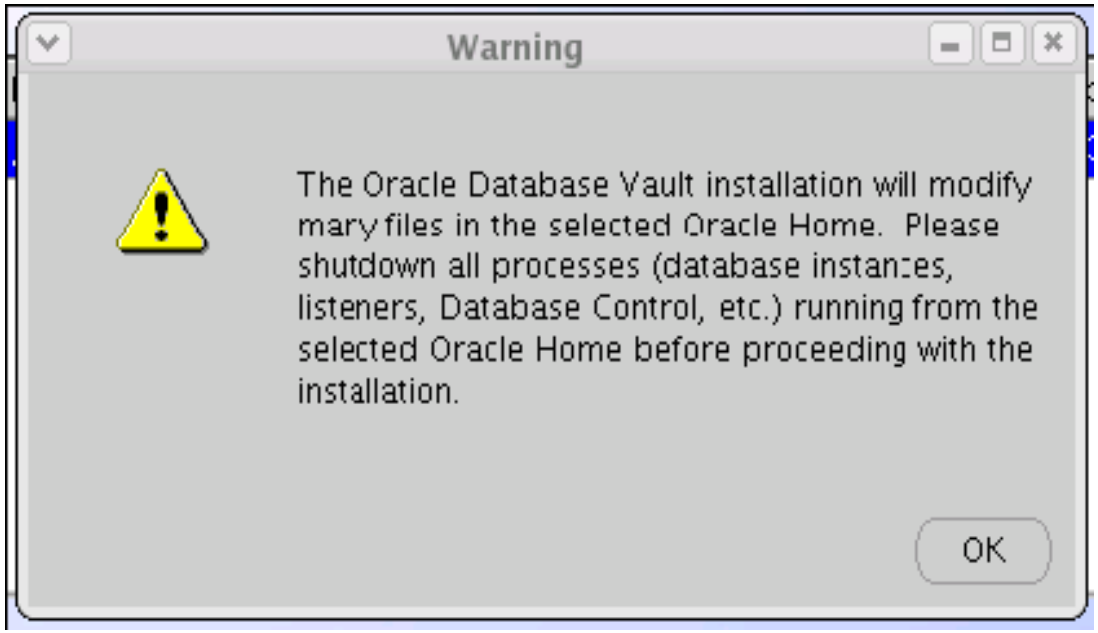


ODV Instalacija

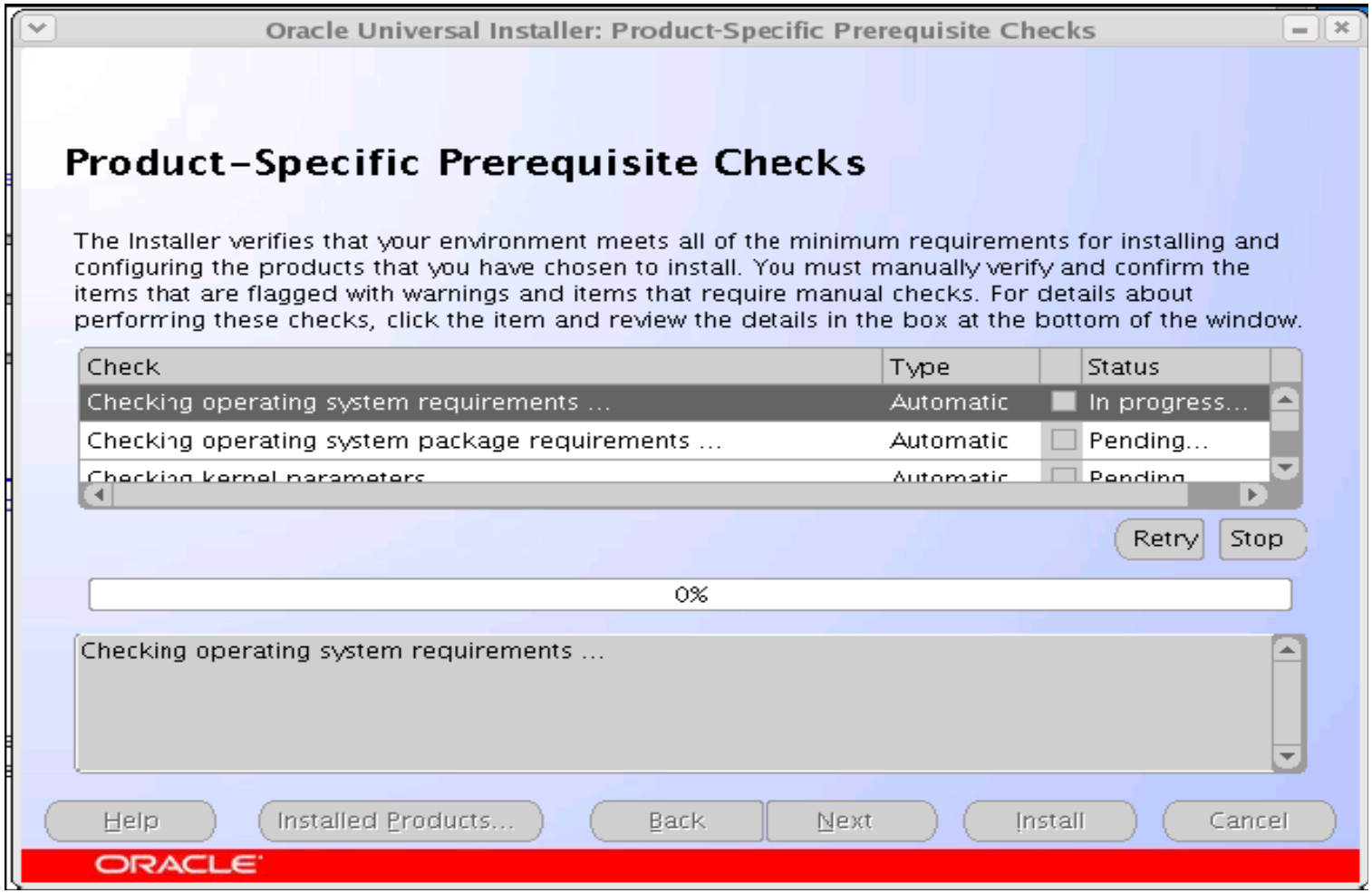
ODV Instalacija



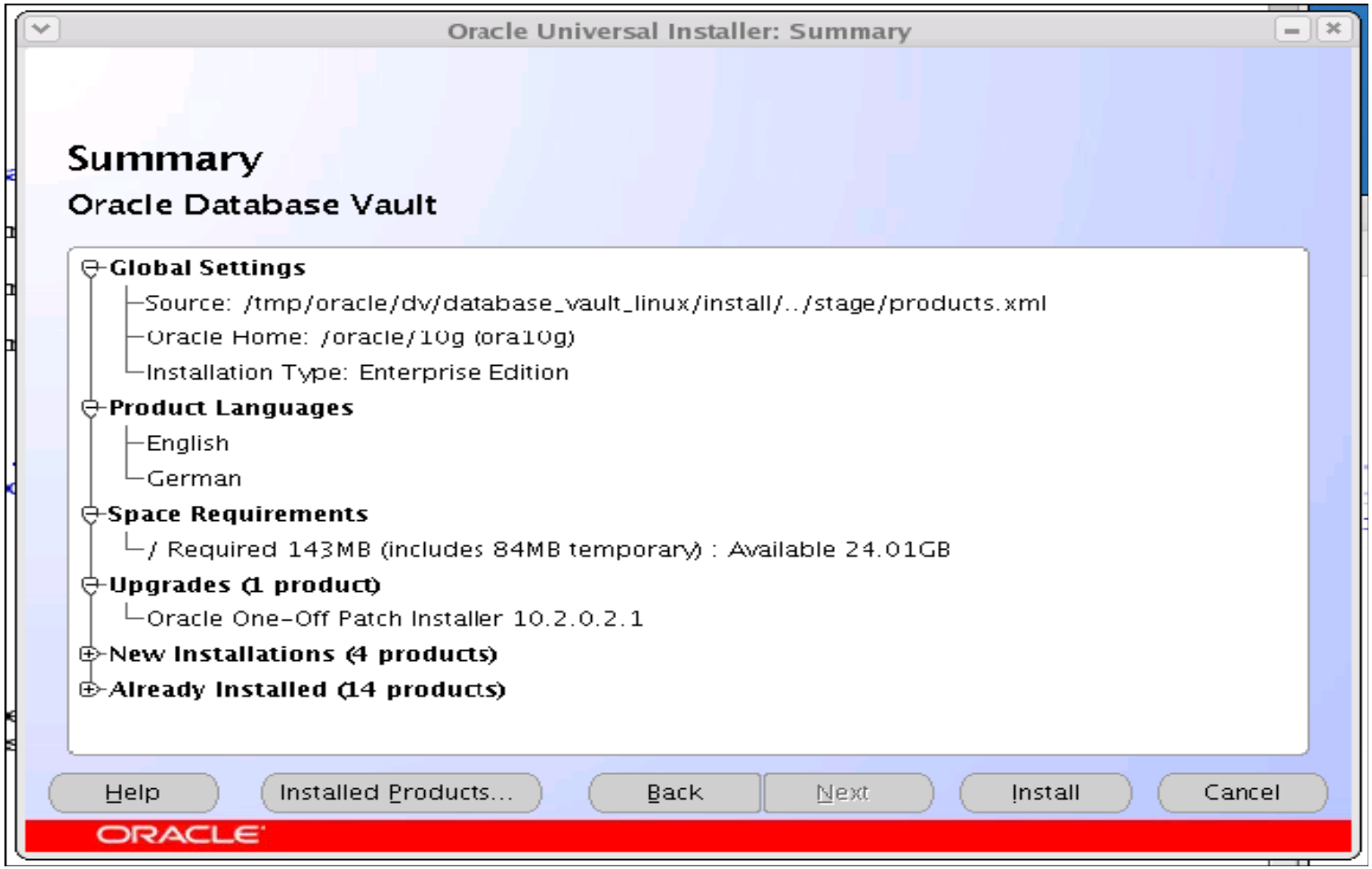
ODV Instalacija



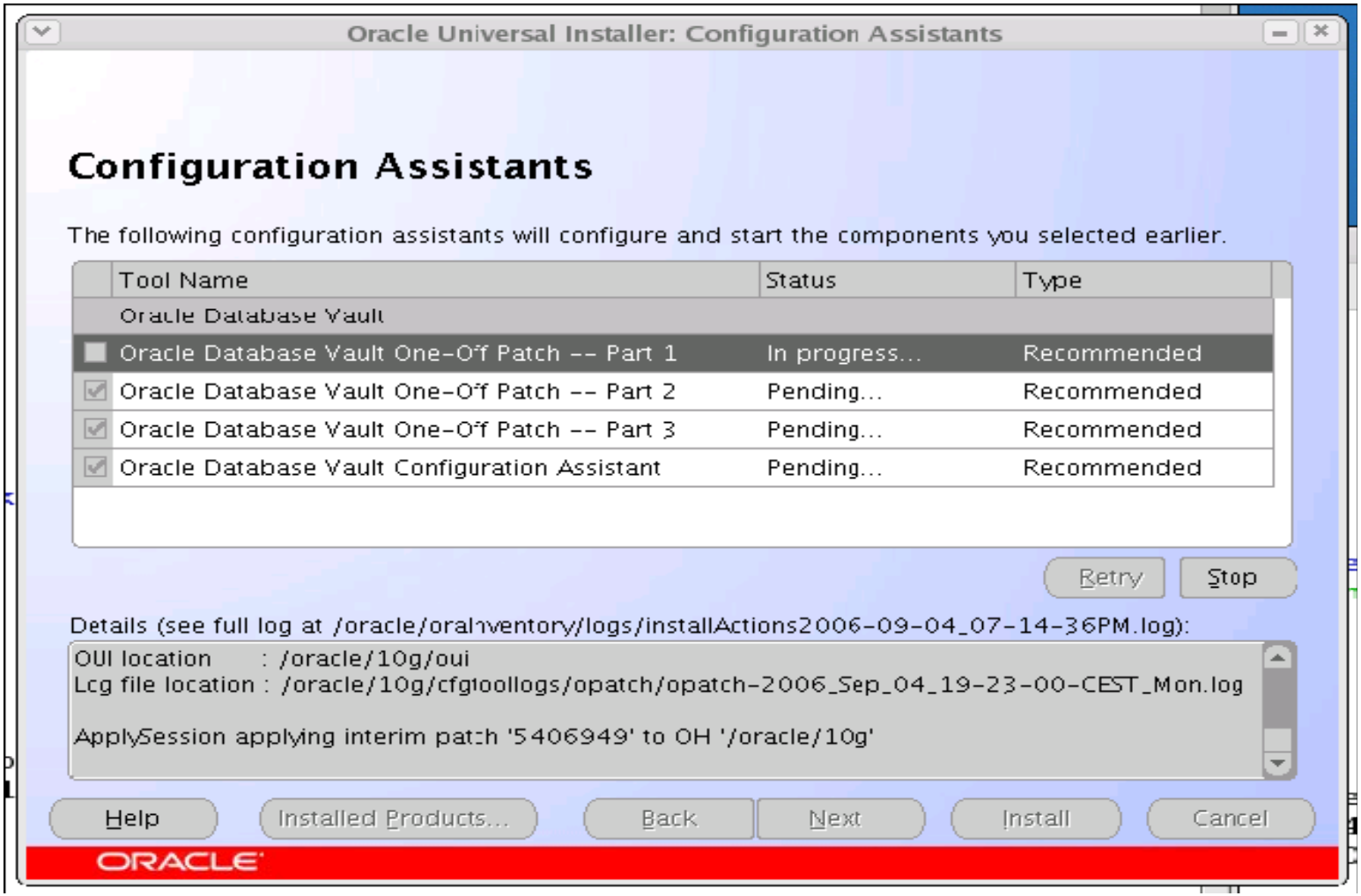
ODV Instalacija



ODV Instalacija



ODV Instalacija



ODV Instalacija

Nakon Instalacije

```
SQL> SELECT comp_name FROM dba_registry;
COMP_NAME
----------------------------------------------
Oracle Label Security
Oracle Workspace Manager
Oracle Enterprise Manager
Oracle Database Catalog Views
Oracle Database Packages and Types
SQL> SELECT value
2 FROM v$option
3 WHERE parameter = 'Oracle Database Vault';
VALUE
----------------------------------------------------------------
TRUE
SQL> SELECT owner, tablespace_name, sum(bytes)
2 FROM dba_segments
3 WHERE owner IN ('DVF','DVSYS','VAULTOWN','VAULTMGR')
4 GROUP BY owner, tablespace_name
5 ORDER BY owner, tablespace_name;
OWNER TABLESPACE_NAME SUM(BYTES)
------------------------------ ------------------------------ ----------
DVSYS SYSTEM 6881280
```

Nakon Instalacije

```
SQL> SELECT owner, object_type, count(*)
2 FROM dba_objects
3 WHERE owner IN
('DVF','DVSYS','VAULTOWN','VAULTMGR')
4 GROUP BY owner, object_type
5 ORDER BY owner, object_type;
OWNER OBJECT_TYPE COUNT(*)
------------------------------ ------------------ ----------
DVF FUNCTION 17
DVF PACKAGE 1
DVF PACKAGE BODY 1
DVSYS EVALUATION CONTEXT 1
DVSYS FUNCTION 16
DVSYS INDEX 74
DVSYS LIBRARY 4
DVSYS LOB 1
DVSYS PACKAGE 35
DVSYS PACKAGE BODY 35
DVSYS PROCEDURE 6
DVSYS RULE 17
DVSYS RULE SET 7
DVSYS SEQUENCE 22
DVSYS SYNONYM 1
DVSYS TABLE 30
DVSYS TRIGGER 2
DVSYS VIEW 54
```

Zaključak

+ Dobra GUI implementacija ukoliko je Database Control instaliran
(http://<host>:<port>/dva)
+ Moguća integracija u postojeće aplikacijske sheme
- Još nema dovoljno dokumentacije (posebno za bagove)
- Otežano je patchiranje (treba onemogućiti ODV prije primjene patcha)

Zaključak

- Database vault donosi sa sobom nekoliko potpuno novih mogućnosti koje se tiču sigurnosti u Oracle bazi podataka
- Ne smije se zaboraviti da nakon instalacije ODV-a ni jedna sistemska ANY privilegija nije ono što je prije bila (ANY != ANY)
- Potrebna je striktna podjela zadataka unutar administracije baze podataka jer ako toga nema ODV je bespotreban

Pitanja?