parallel
oracle expert team

Tehnički aspekti Database Vault-a

Autori:
Maja Veselica, Security Consultant
Zoran Pavlović, Security Manager

ORACLE Certified Expert

ORACLE Certified Specialist

Agenda

1. Šta je Database Vault, njegov značaj i prednosti
2. Standardi
3. Implementacija Database Vault-a
4. Segregacija dužnosti
5. Komponente Database Vault-a
6. Database Vault u praksi
7. Zaključak
8. Kontakt informacije

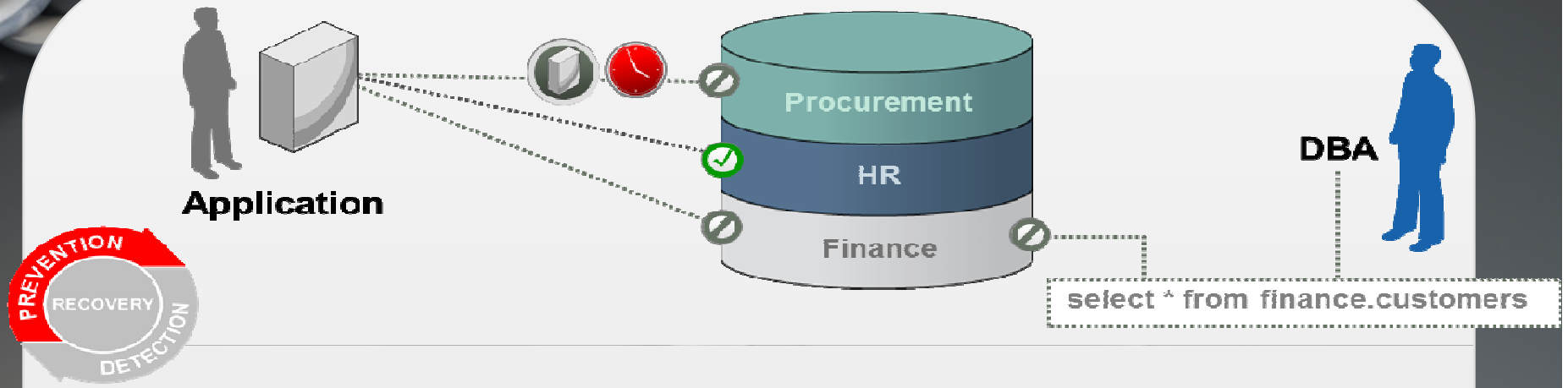
Database Vault (DBV)

- U verziji 11g je ugrađen u kernel baze
- Spada u rešenja za kontrolu pristupa
- U velikoj meri pruža zaštitu od unutrašnjih pretnji
- Podržava rad sa Real Application Cluster (RAC) okruženjem

Unutrašnje pretnje

- Najveću pretnju predstavljaju:
  - Korisnici koji imaju :
    - DBA rolu
    - Jake sistemske privilegije
- DBAs mogu čitati osetljive podatke u bazi
- Narušeni:
  - Business need to know
  - Least privilege principle
- Bolje sprečiti, nego lečiti!

Prednosti DBV

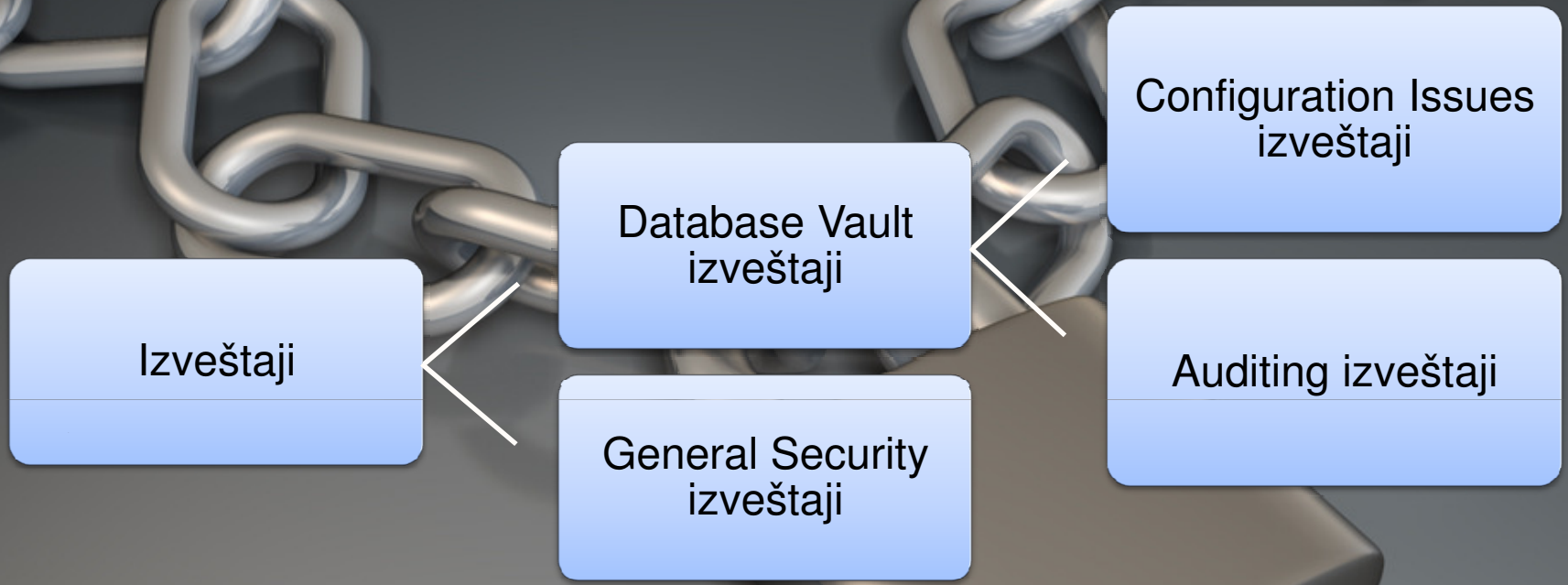


- Separacija dužnosti odnosno ukidanje “superusera”
- DBAs ne mogu čitati podatke!
- Sprečava “hakere” da pristupe podacima iako su uspeli da zaobiđu aplikaciju

Prednosti DBV

- **Dopunjuje DAC (Discretionary Access Control)**
- **Kompleksna kontrola pristupa podacima**
- **Definisanje uslova *samo* pod kojima je moguće izvršiti neku komandu**
- **Može da radi sa Label Security**
- **Monitoring**

Prednosti DBV



- **Ukupno 53 ugrađena izveštaja**
  - **9 grupa General Security izveštaja**

parallel
oracle expert team

Standardi

- **PCI DSS**
  - **Restrict access to cardholder data**

    by business need-to-know (Req 7)
  - **Enable accounts used by vendors**

    for remote maintenance

    only during the time period needed (Req 8.5.6)
  - **Compensating Controls for Req 3.4**
  - **Requirement A.1**
- **Basel II**
- **SOX**

Implementacija DBV

- **Pre implementacije je potrebno definisati:**
  - **Politiku bezbednosti**
  - **Sigurnosne procedure**

Segregacija dužnosti

- **Implementacijom Database Vault-a uvedene su funkcije:**
  - **Security administrator**
  - **Account manager**
  - **Database administrator – sada ima:**
    - **Ograničenu moć**
    - **Adekvatno usklađene privilegije i radne zadatke**

parallel
oracle expert team

Komponente DBV

- Realms
- Rule sets
- Factors
- Command rules
- Secure application roles

parallel
oracle expert team

Realms (domeni)

16 hroug

- *Domeni* **štite objekte baze**

koji su u njima sadržani od korisnika

koji upotrebljavaju sistemske privilegije.

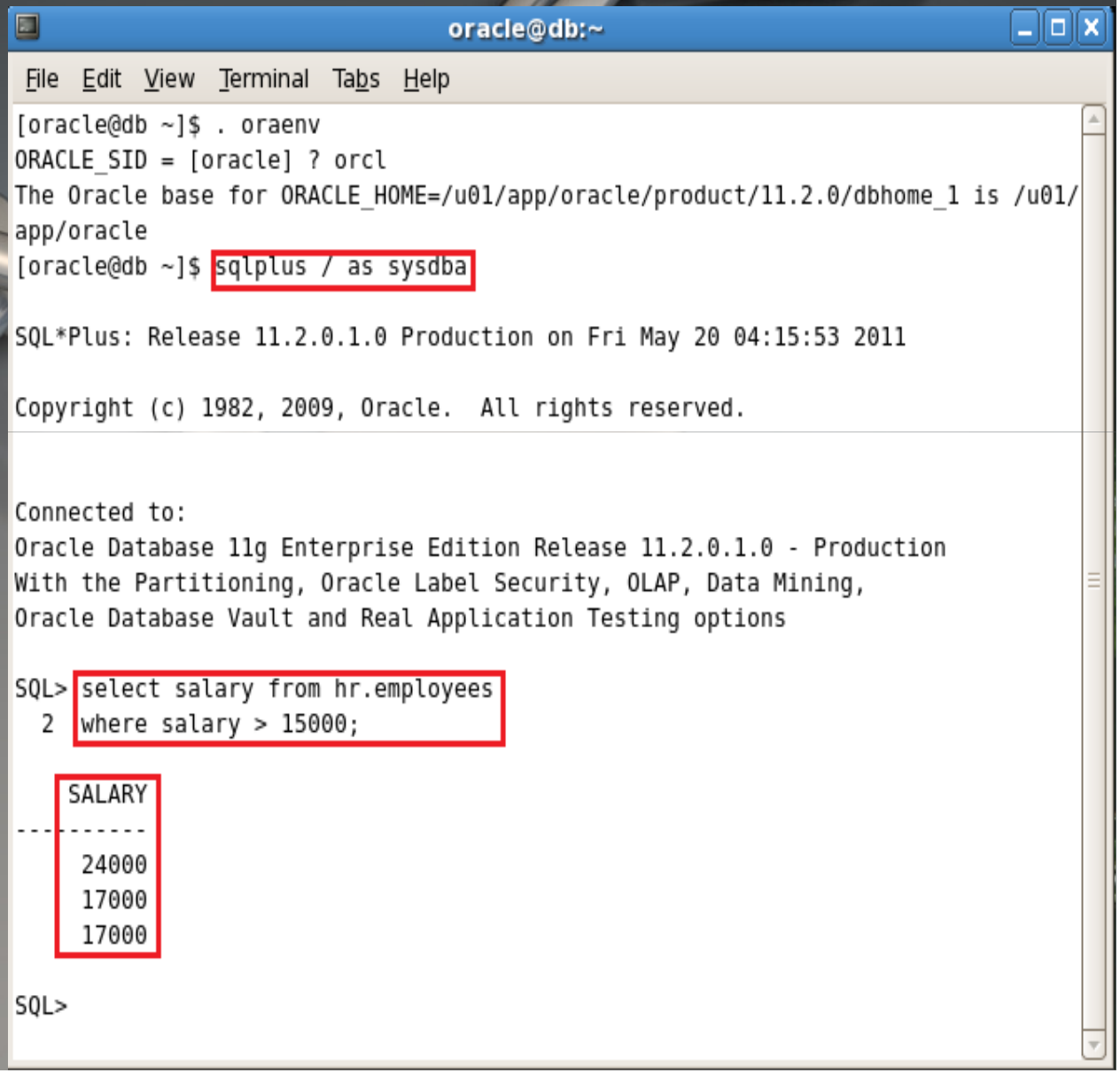
- **Definišu koji korisnici mogu da**

koriste sistemske privilegije

nad zaštićenim objektima

Realms – Primer 1

Pre postavljanja *realm*-a, SYS može da pristupi podacima o platama



Realms – Primer 1

Posle kreiranja i konfiguracije *realm*-a, SYS ne može da pristupi podacima o platama, a direktor može.

```
oracle@db:~
File  Edit  View  Terminal  Tabs  Help
[oracle@db ~]$ . oraenv
ORACLE_SID = [oracle] ? orcl
The Oracle base for ORACLE_HOME=/u01/app/oracle/product/11.2.0/dbhome_1 is /u01/
app/oracle
[oracle@db ~]$ sqlplus / as sysdba

SQL*Plus: Release 11.2.0.1.0 Production on Fri May 20 16:25:23 2011

Copyright (c) 1982, 2009, Oracle.  All rights reserved.


Connected to:
Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 - Production
With the Partitioning, Oracle Label Security, OLAP, Data Mining,
Oracle Database Vault and Real Application Testing options

SQL> select salary from hr.employees
  2  where salary > 15000;
select salary from hr.employees
                     *
ERROR at line 1:
ORA-01031: insufficient privileges


SQL> connect direktor
Enter password:
Connected.
SQL> select salary from hr.employees
  2  where salary > 15000;

    SALARY
---------
     24000
     17000
     17000

SQL>
```

Realms – Primer 2

Ako vlasnik šeme (schema owner) nije autorizovan u domenu, ne može izvršiti DDL naredbe.

```
oracle@db:~
File  Edit  View  Terminal  Tabs  Help
[oracle@db ~]$ . oraenv
ORACLE_SID = [oracle] ? orcl
The Oracle base for ORACLE_HOME=/u01/app/oracle/product/11.2.0/dbhome_1 is /u01/
app/oracle
[oracle@db ~]$ sqlplus hr

SQL*Plus: Release 11.2.0.1.0 Production on Mon Jun 6 20:22:06 2011

Copyright (c) 1982, 2009, Oracle.  All rights reserved.

Enter password:

Connected to:
Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 - Production
With the Partitioning, Oracle Label Security, OLAP, Data Mining,
Oracle Database Vault and Real Application Testing options

SQL> select last_name from hr.employees
  2  where salary > 15000;

LAST_NAME
--------------------
King
Kochhar
De Haan

SQL> drop table hr.employees;
drop table hr.employees
*
ERROR at line 1:
ORA-47401: Realm violation for DROP TABLE on HR.EMPLOYEES


SQL>
```

parallel
oracle expert team

Rule sets

Rule set

$$\tau(P_1 \wedge P_2 \wedge \ldots \wedge P_n) \in \{True, False\}$$

$$\tau(P_1 \vee P_2 \vee \ldots \vee P_n) \in \{True, False\}$$

$$P_i - Pravilo, \tau(P_i) \in \{True, False\}$$

- ***Rule set*** **predstavlja skup pravila**

  čijom evaluacijom se utvrđuje

  pravo pristupa

parallel
oracle expert team

Rule sets

- ***Rule set*** **može da koristi faktore**
- **Samo definisanje *Rule set*-a**

nema nikakav uticaj na zaštitu

- **Potrebno ga je primeniti u**

okviru neke od komponenti:

  - ***Realm***
  - ***Command rule***
  - ***Secure application role***

Rule sets – Tekst primera

- **Moguće je kreirati *Rule set Radno vreme*,**

čija je svrha da utvrdi

da li korisnik pokušava da

pristupi van radnog vremena

(od pon do petka; 9h - 17h)

Moguće rešenje primera

- **Sastavljen je od 2 pravila:**
  - **Da li je dan OK?**

```
SQL> show parameter nls_territory;

NAME                                 TYPE        VALUE
------------------------------------ ----------- ---------
nls_territory                        string      AMERICA
```

// to_char (sysdate,'d') between '2' and '6'

  - **Da li je vreme OK?**

// to_char (sysdate,'hh24') between '09' and '17'

- **Potrebno odabrati opciju da su**

oba pravila zadovoljena (tačna) tj. All True

Factors (faktori)

- *Faktor* je imenovana promenjiva

  (npr. IP adresa)

- Vrednost faktora se naziva *Identity*

  (npr. 127.0.0.1)

- Postoji veliki broj ugrađenih faktora
- Security administator može

  definisati nove *faktore*

- Kombinacijom *faktora* je moguće

  implementirati multifaktorsku autorizaciju

parallel
oracle expert team

Command rules

16 hroug

- **Koriste *rule set* za definisanje pravila koja moraju biti zadovoljena da bi se izvršila SQL naredba nad objektom**

- ***Command rule* nema ime**

Command rules

- **Jednoznačno je određeno trojkom:**
  - **SQL komandom (npr. UPDATE)**
  - **Imenom vlasnika objekta (object owner) (npr. HR)**
  - **Nazivom objekta (npr. EMPLOYEES);**

% označava sve objekte

Command rules – Tekst primera

- **Napravljen je *command rule*,**

  koji omogućava izvršenje

  UPDATE naredbe nad HR.EMPLOYEES

  samo radnim danima od 9h do 17h

  (*Rule set* Radno vreme)

parallel
oracle expert team

Rezultat primera

oracle@db:~

File Edit View Terminal Tabs Help

```
The Oracle base for ORACLE_HOME=/u01/app/oracle/product/11.2.0/dbhome_1 is /u01/
app/oracle
[oracle@db ~]$ sqlplus direktor

SQL*Plus: Release 11.2.0.1.0 Production on Fri May 20 22:31:26 2011

Copyright (c) 1982, 2009, Oracle.  All rights reserved.

Enter password:

Connected to:
Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 - Production
With the Partitioning, Oracle Label Security, OLAP, Data Mining,
Oracle Database Vault and Real Application Testing options

SQL> update hr.employees
  2  set salary = 30000
  3  where salary = 24000;
update hr.employees
           *
ERROR at line 1:
ORA-01031: insufficient privileges


SQL> select salary from hr.employees
  2  where salary > 15000;

    SALARY
----------
     24000
     17000
     17000

SQL>
```

Command rules – Primer

Security Violation Attempts

May 19, 2011 11:18:14 PM - May 20, 2011 11:18:14 PM

Previous 1-10 of 11 Next 1

Timestamp	User Name	User Host	Action Name	Return Code	Action Object Name	Rule Set Name	Action Command
May 20, 2011 10:33:10 PM	DIREKTOR	db.zoracle.com	Command Authorization Audit	1031	UPDATE	Radno vreme	UPDATE HR.EMPLOYEES SET SALARY = 30000 WHERE SALARY = 24000

- **Na slici je prikazan**

deo strane Monitor iz

Database Vault Administrator alata,

gde se vidi da je direktor pokušao

da poveća platu van radnog vremena

Secure application roles (SARs)

- ***SAR*** **se sastoji isključivo od *naziva***

  i pridruženog *rule set*-a

- **Specifični uslovi moraju biti**

  zadovoljeni da bi rola

  mogla biti dodeljena korisniku

- **Uslovi su definisani u okviru**

  jednog (pridruženog) *rule set*-a

Secure application roles (SARs)

- **Rolu “aktivira” PL/SQL procedura koja se nalazi u zaštićenom paketu, koji DBV pruža**

- **Više nije potrebno pisanje PL/SQL procedure**

- ***SARs* onemogućavaju zaobilaženje aplikacije**

parallel
oracle expert team

DBV u praksi

- **Kako se DBV pokazao u praksi?**
- **Koja je procedura za vršenje**

FULL EXPORT-a, FULL IMPORT-a i

rad sa Scheduler-om kada

u sistemu postoji DBV?

- **Često postavljana pitanja**

parallel
oracle expert team

Zaključak

- **Primenom Database Vault-a**

se prave značajni koraci u pravcu

poboljšanja zaštite i ispunjenju

zahteva postojećih standarda

(PCI DSS, SOX, itd.)

Kontakt

- **Autori:**
  - **Maja Veselica, *Security Consultant***
    maja.veselica@parallel.rs
  - **Zoran Pavlović, *Security Manager***
    zoran.pavlovic@parallel.rs

- **Parallel d.o.o:**
  - **e-mail: info@parallel.rs**
  - **adresa: Pariske komune 24, Novi Beograd**
  - **telefon: +381 11 260 74 84**

parallel
oracle expert team

Prilog

16 hroug

- **Obezbeđen je disk,**

kao prilog prezentaciji,

na kojem se nalaze

video materijali.

parallel
oracle expert team

16
hroug

Hvala na pažnji!


parallel
oracle expert team
16
hroug