Privacy
Insider Threats
Compliance

ORACLE

Sigurnosni koncept baze

Dražen Pataric
Senior Sales Consultant
Oracle Hrvatska

HrOUG – 12. Konferencija

Rovinj, 16. – 20. listopada 2007.

Sigurnost - zašto, kako?

razlozi …

1. Volja uprave

2. Zakoni, propisi

i rješenje …

1. Pravila

2. Procedure

Sigurnost - razine

- Disk
- Baza podataka
- Mreža
- Aplikacija

Sigurnost – 1. problem

- **CJELOVITOST, POTPUNOST**

Informacija ne smije NIGDJE “curiti”

Cijev za protok tekucine s rupama

Sigurnost – 2. problem

PROTURJECNOST

- **Aplikacija – omogucava da se nešto može**
- **Sigurnost – osigurava da se nešto NE može**

Oracle sigurnosna rješenja

Bazu podataka

Aplikacijsku infrastrukturu

Auditing

Drugi sustavi (non Oracle)

Razjasnimo

Što cemu služi ?

OAS - Oracle Advanced Security Option
OLS - Oracle Label Security
- Zoran Jovanovic, IN2
Oracle Data Vault – Alan Bubic, Comping

Audit Vault - Dražen Pataric, Oracle

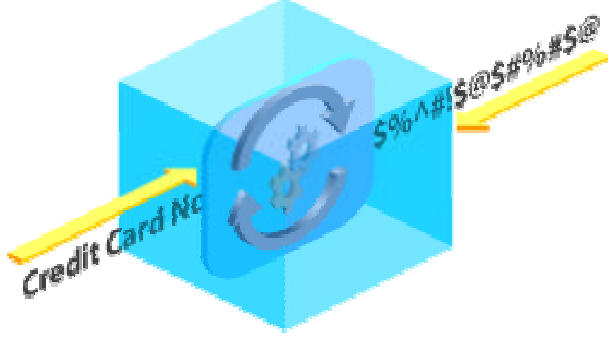
Trenutno stanje u kompanijama Konsolidacija

- Nekompletno
  - Mnogobrojna rješenja više dobavljaca
  - Nekompatibilne tehnologije – ne rade skupa
- Kompleksno
  - Djelomicne integracije – u koracima
  - Jako puno manualnog posla
- Ne zadovoljava regulative
  - Teško uspostavljanje skupova pravila zaštite
  - Teška procjena zadovoljejna regulativa

TDE - Transparent Data Encryption

- Dio OAS (Oracle Advanced Security)

- Zaštita nekih podataka na disku (na nivou kolone)
- Zaštita na BACKUP mediju integracija s RMAN-om
- Zaštita na redo nivou redo-a

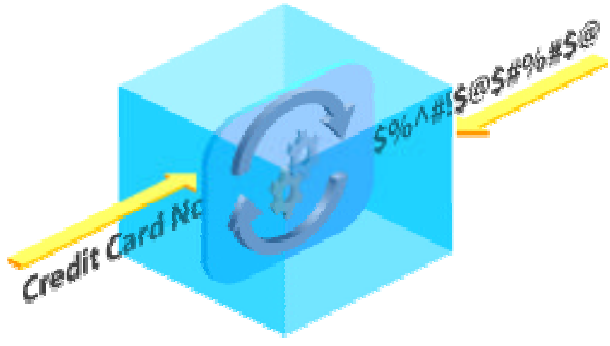


- Koji je sadržaj na odbacenim trakama i diskovima ?

TDE - protokoli zaštite

Package Feature	DBMS_OBFUSCATION_TOOLKIT (Oracle8*i* and Oracle9*i*)	DBMS_CRYPTO (Oracle 10g and 10g R2)	Transparent Data Encryption (Oracle 10g R2 Adv. Sec. Option)
Cryptographic algorithms	DES, 3DES	DES, 3DES, AES, RC4, 3DES_2KEY(1)	3DES, AES (128, 192, and 256 bit)
Padding forms	none supported	PKCS5, zeroes	PKCS5(2)
Block cipher chaining modes	CBC	CBC, CFB, ECB, OFB	CBC(2)
Cryptographic hash algorithms	MD5	SHA-1, MD4(1), MD5(1)	SHA-1(2)
Keyed hash (MAC) algorithms	none supported	HMAC_MD5, HMAC_SH1	n/a
Cryptographic pseudo-random number generator	RAW, VARCHAR2	RAW, NUMBER, BINARY_INTEGER	n/a
Database types	RAW, VARCHAR2	RAW, CLOB, BLOB	All but: OBJ., ADT, LOB

TDE - ogranicenja



- Kolone stranog kljuca
- Indeksno pretraživanje – samo jednakost
- Zahtijeva planiranje u modelu podataka
  - pomocno polje i tablica
- Data Guard – samo PHYS standby
- Dodatna opcija na EE
- Oracle 11g – tablespace, securefiles

TDE – od koga štiti

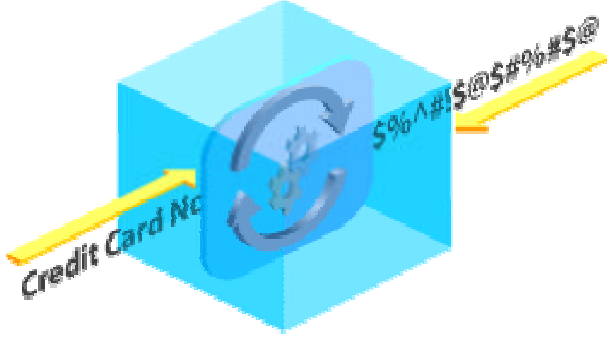
- Pristup datotekama na disku
  datafile, redo log, arch log, backup set
  (sistem administrator, backup administrator)

- Pristup datotekama na traci
  backup set
  (sistem administrator, backup administrator, kurir)

- **Prijetnje i izvana i iznutra**

Network Encryption (with Data Integrity)

- Dio OAS opcije (Oracle Advanced Security)
- Zaštita mrežnog prometa (izmedu BAZE i aplikacije)



- Osigurava zaštitu i nepromjenjivost podatka u transferu mrežom (bilo tko tko može promatrati mrežni promet)

Network Encryption (kripto standardi)

- Protokoli za mrežnu zaštitu

  RC4 (40, 56, 128, i 256 bita)

  DES (40 and 56 bita)

  3DES (2 i 3 kljuca)

  AES (128, 192, i 256 bita)

- Data Integrity protokoli

  MD5

  SHA-1

Strong Authentication

(tko je zapravo tamo)

- Dio OAS (Oracle Advanced Security)
- **Autentikacija** višeg nivoa sigurnosti (PIN , Token kartice, biometrija, itd.)
- Integracija s vanjskim paketima
- Smanjuje vjerojatnost korisnicke greške
- Elektronicki token

Strong Authentication protokoli

Kerberos

RADIUS (Remote Authentication Dial-In User Service)

Secure Sockets Layer (s digitalnim certifikatom)

PKI (Public Key Infrastructure)

OLS - Oracle Label Security

- Dodatna opcija na EE

- Zaštita pristupa na nivou RETKA
  osigurana i sprovedena od strane BAZE
- Bazirano na OZNACI (engl Label)

- 3 dimenzije oznake (2 opcionalne)
  1. LEVEL (nivo) – obavezan atribut
  2. COMPARTMENT (odjeljak)
  3. GROUP (grupa)

OLS - kada i kome

- Zajednicki podaci za razne odvojene PS
  3 dimenzije – jako fina podjela prava

- Primjer:
  1 tablica placa za više poslovnih subjekata
  Select count(*) from table1 – razliciti brojevi

- Ciljane grupe korisnika
  Vojska, Policija, Financijske aplikacije, Javni sektor

OLS - od koga štiti

- Osigurava da svaki korisnik može vidjeti samo onaj dio cjeline koji mu pripada (i koji smije)
- Osigurava regulative (Data Privacy)

Data Vault

- Dodatna opcija na EE
- Ultimativna metoda zaštite baze
  zaštita i od korisnika s DBA privilegijom
- REALM
  (firewall zatvoren sa svih strana)
  strogo kontrolirana interakcija
- Pravila

Data Vault – 2 glavne funkcije

- REALM prostor
  razlicite App imaju odvojene REALM-ove
  - podaci drugih app kao da su u posve drugoj bazi
  - niti jedan privilegirani korisnik ne može vidjeti podatke unutar REALM-a za koji nema ovlasti

- Pravila (Cak i ako korisnik ima prava u REALM-u)
  Nitko ne može napraviti DROP ili TRUNC TABLE
  Alter table je moguc samo u vremenu od 20 do 04
  Pristup je moguc samo s adrese ...
  itd ...

Data Vault

ORACLE DATABASE VAULT 10g

Od koga štiti ?

- Od privilegiranih korisnika
  Od pokušaja proboja iznutra
  (REALM)
- Nesmotrena ili kriva manipulacija data modelom
  (implementacija pravila)
- Regulative i podjela uloga

Audit Vault

- Aplikacija (kao i EM) - neovisna
- Prvenstveno audit namjena
- Audit kompleksnog okruženja (mnoštvo baza)
  - vlastiti repozitorij aud dogadaja
  - mogucnost reakcije (dogadaj)
  - mogucnost koreliranog izvještavanja
  - preko politika (skupova pravila)

Audit Vault - zašto je važan?

- **Osigurava neporecivost**
- Od koga štiti
  od **privilegiranih korisnika**
  regulative
  podjela uloga
- Oslobada od lažne optužbe
  (sve se vidi iz i postavki sustava i auditing-a)

I za kraj ...

- Uloga u sigurnosnom smislu
  Zajedno se nadopunjavaju
- Transparentnost
  (Netw encr, Strong Auth, Audit Vault)
- Model podataka, procesni model
  (TDE, Data Vault, OLS)
- “Out of box ?”

I još malo za kraj ...

- Nema apsolutne sigurnosti
  (skupa je)

- Kada imamo ipak nekakvu sigurnost ?

Koji je cilj svega?

- Ukupno sigurnosno stanje i miran san vlasnika
- Zadovoljenje sigurnosnih propisa i regulativa

- Lakša revizija sigurnosnog sustava

ORACLE

Information Company

Oracle – 25 Plus Years of Security Leadership

Audit Vault
Database Vault
Content DB, Records DB
Secure Enterprise Search
Thor & Octet String (IdM Acquisitions)
Phaos, Oblix, (IdM Acquisitions)
Database CC Security Eval #18 (10g R1)
Transparent Data Encryption
VPD Column Sec Policies
Fine Grained Auditing (9i)
1st Database Common Criteria (EAL4)
Oracle Label Security (2000 8.1.7)
Virtual Private Database (1998)
Enterprise User Security (8i)
Database Encryption API
Kerberos Support (8i)
Support for PKI
Radius Authentication
Network Encryption (Oracle7)
Oracle Advanced Security introduced
First Orange Book B1 evaluation (1993)
Trusted Oracle7 MLS DB
Government customer (CIA – Project Oracle)

ORACLE

Security Company

Pitanja ?

Demonstracija

- Primjer TDE
- Primjer OLS - Zoran Jovanovic, IN2
- Primjer Data Vault - Alan Bubic, Comping