GDPR I BAZE PODATAKA - sigurnost Oracle DBMS-a

Zlatko Sirotić, univ.spec.inf.
ISTRA TECH d.o.o.
Pula

GDPR i baze podataka

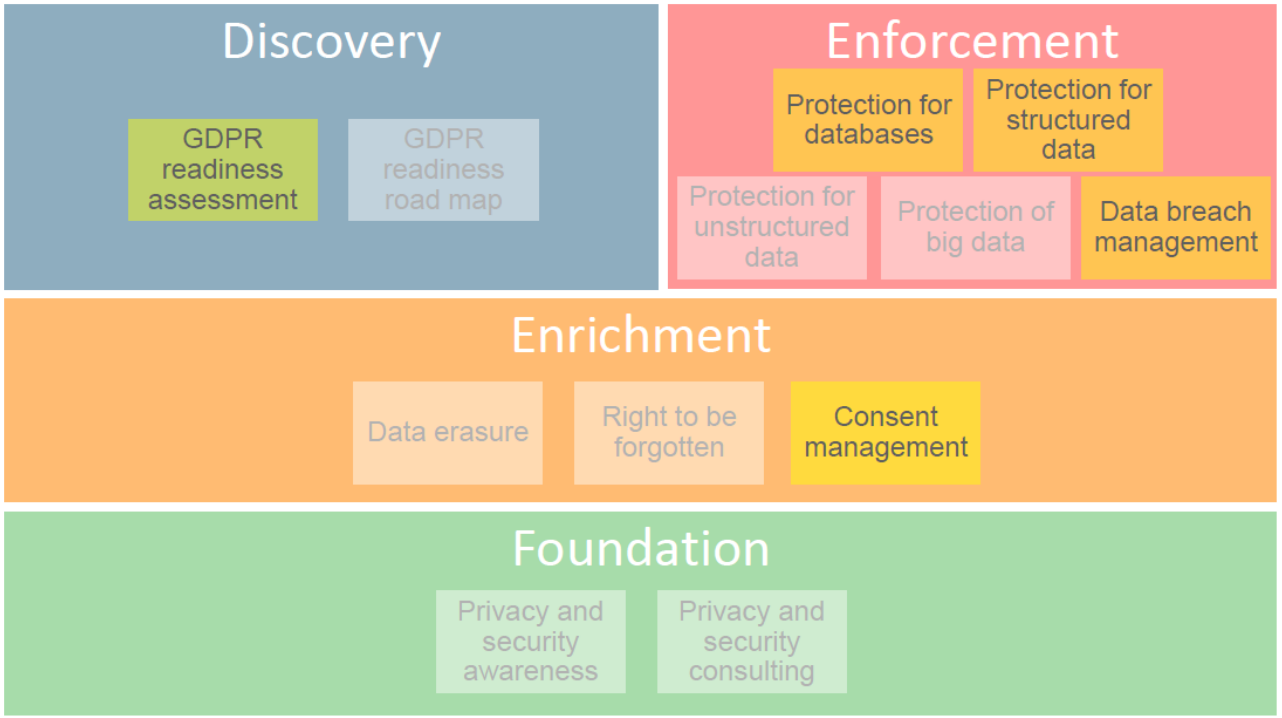
- Kod primjene GDPR uredbe, baze podataka (BP) imaju vrlo veliku važnost, jer se u njima nalazi velika količina podataka, od kojih su neki obuhvaćeni tom uredbom.
- Podatke treba primjereno zaštiti, primjenom poznatih metoda identifikacije, autenti(fi)kacije i autorizacije korisnika, te kriptiranjem osjetljivih podataka.
- Nadalje, svakako trebamo pratiti promjene nad podacima (audit podataka), kako bismo znali tko je mijenjao (a možda i gledao) podatke.
- U slučaju pada servera BP, potrebno je brzo podignuti drugi server BP, a najbolje je da to bude (skoro) trenutačno, korištenjem sekundarnog servera BP za disaster recovery, koji se ažurira (skoro) trenutačno na temelju podataka iz primarnog servera BP.

GDPR i baze podataka

- Kod primjene prethodnih metoda, postavljaju se barem dva pitanja.
- Jedno pitanje nije vezano isključivo za GDPR:
  možemo (ili želimo) li platiti sva ona rješenja koja proizvođač softverske opreme (u ovom slučaju Oracle) nudi?
  Ta su rješenja (vjerojatno) obuhvatnija i kvalitetnija od vlastitih, ali ponekad je cijena neprihvatljiva za korisnika i prisiljeni smo naći (ili napraviti) jeftinija rješenja.
- Drugo je pitanje: da li neke metode imaju, sa stanovišta GDPR zahtjeva, uz dobre strane i one loše?
  Npr. ako moramo raditi (značajan) audit podataka, **time se opet stvaraju novi podaci koje isto moramo voditi u skladu s GDPR zahtjevima**.
  Slično je i sa stvaranjem replika podataka.

GDPR i sigurnost u Oracle bazi – prezentacija s konferencije OOW 2017

EU GDPR and Database Security



Securing data in your Oracle Databases is a fundamental component of GDPR compliance.

Database Security is also one of the more simple GDPR tasks – an easy way to demonstrate progress in your compliance project!

ORACLE Capgemini CONSULTING.TECHNOLOGY.OUTSOURCING

GDPR i sigurnost u Oracle bazi – prezentacija s konferencije OOW 2017

A view on Database Compliance

Oracle is the leader in DBMS

- Discovery
  - Configuration Analysis
  - Sensitive Data Discovery
- Enforcement
  - Encryption and Key Management (Advanced Security, Key Vault)
  - Access Controls (Database Vault, Real Application Security)
  - Anonymization (Data Masking & Subsetting, Data Security Cloud Services)
  - Activity Monitoring (Audit Vault & Database Firewall, Data Security Cloud Services)
- Enrichment
  - Enforcement of consent and restriction of processing (Label Security)

ORACLE

 25

GDPR i sigurnost u Oracle bazi – prezentacija s konferencije OOW 2017

GDPR Articles and Mapping to Oracle Database Security

GDPR Article	Protection Mechanism	Oracle Mapping
Article 35	**Data Protection Impact Assessment**	Configuration & Compliance Cloud Service Database Security Assessment Tool NEW
Article 32	**Pseudonymization and encryption of personal data**	Advanced Security, Key Vault
Article 25, 29	**Data protection by design and by default** **Processing under the authority**	Database Vault
Article 30, 33	**Notification of a personal data breach**	Audit Vault and Database Firewall Security Monitoring and Analytics Cloud Service
Article 18, 25, 32	**Right to restriction of processing** **Data protection by design and by default**	Label Security
Articles 25, 32	**Pseudonymisation and encryption of personal data** **Data Minimization**	Data Masking and Subsetting
Article 25	**Data Protection by Design and Default**	All of the above

ORACLE

Accelerate Your Response to the EU GDPR Using Oracle DB Security Products (w.paper)

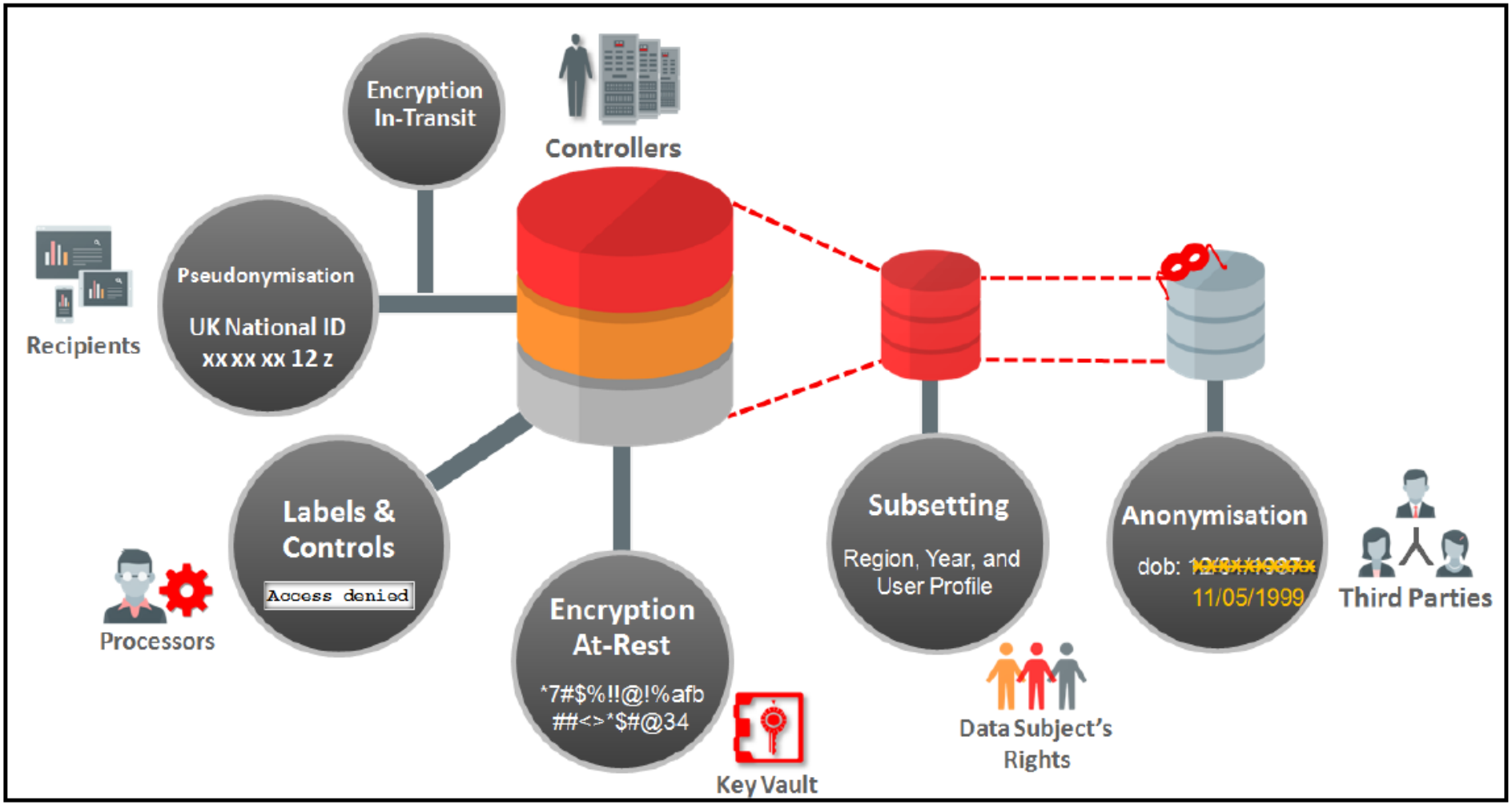


Figure 6: Oracle Database Security Preventive Controls

Accelerate Your Response to the EU GDPR Using Oracle DB Security Products (w.paper)

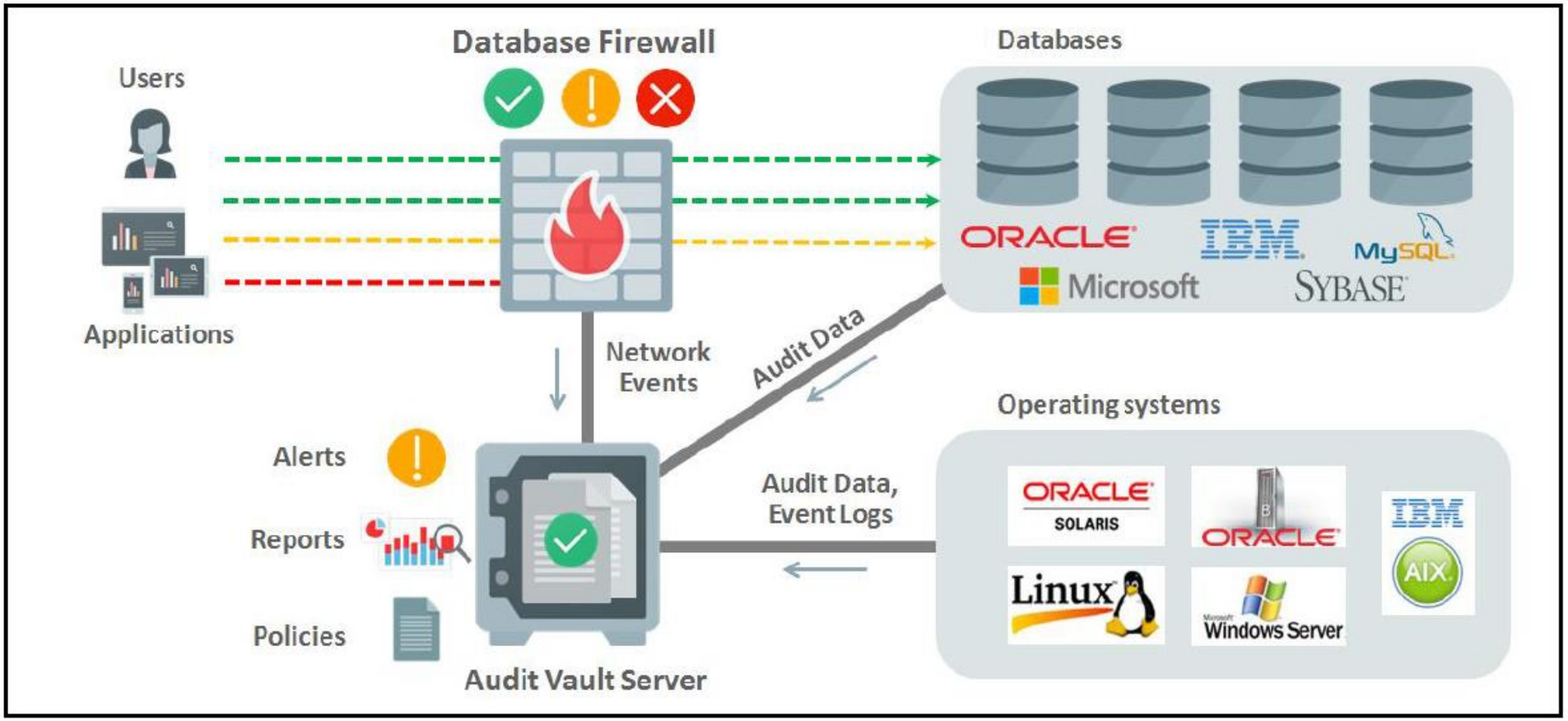


Figure 7: Oracle Database Security Monitoring Controls

Accelerate Your Response to the EU GDPR Using Oracle DB Security Products (w.paper)

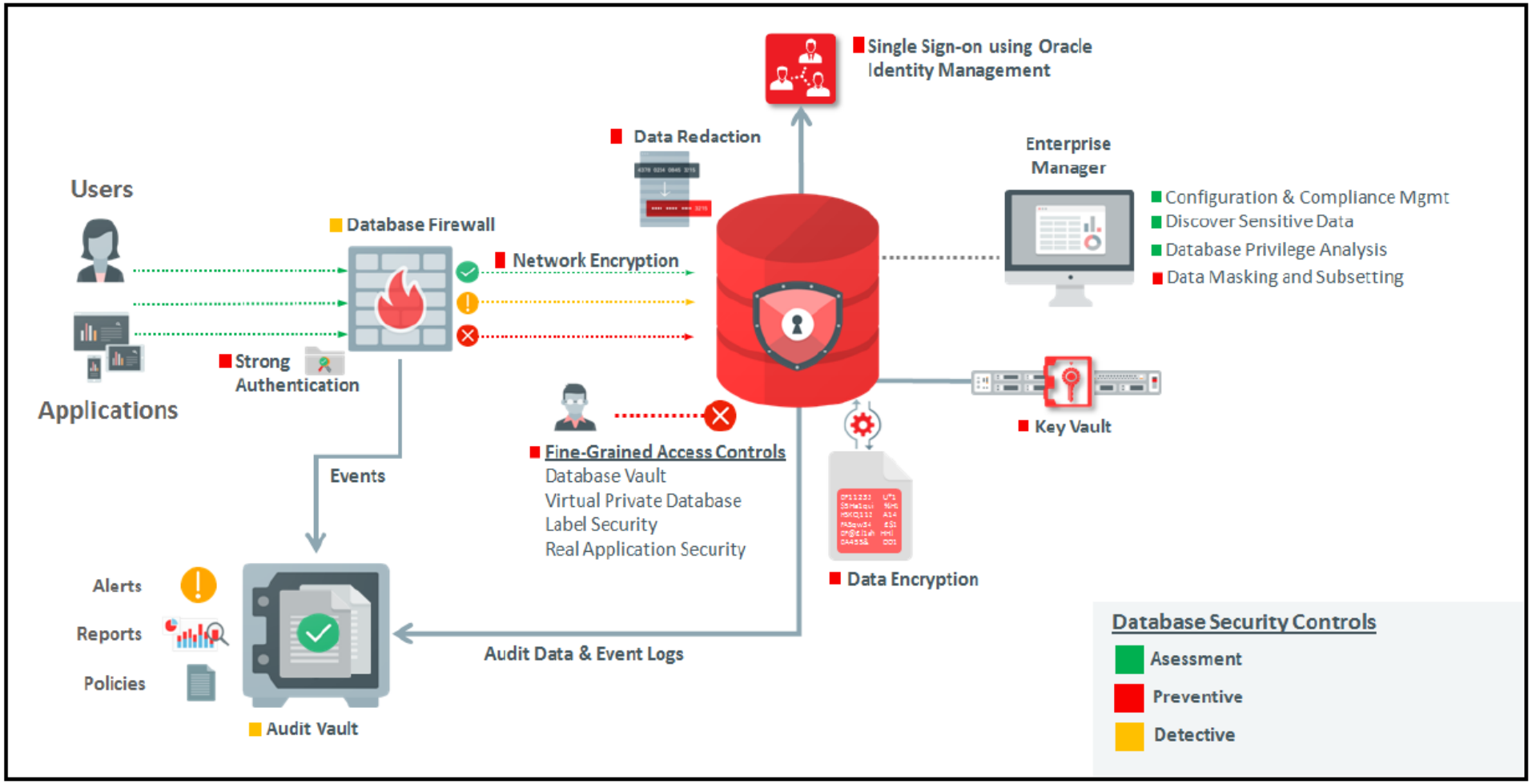


Figure 8: Oracle Maximum Data Security Architecture

Rekapitulacija sigurnosnih mogućnosti Oracle DBMS-a

- Identifikacija i autenti(fi)kacija
- Autorizacija (standardna)
- Fina autorizacija: Virtual Private Database (VPD) i Label Security (LS) tehnologije
- Standardno auditiranje
- Fino auditiranje: Fine-Grained Auditing (FGA) i Audit Vault (AV)
- Kriptiranje podataka
- Replikacija i Disaster Recovery

Identifikacija i autenti(fi)kacija

- Kreiranje korisnika (sheme) radi se naredbom:

CREATE USER korisnik IDENTIFIED BY zaporka;

- Oracle baza ne drži kriptiranu vrijednost lozinke, jer bi onda negdje morao biti zapisan i ključ za dekriptiranje, već drži **hash vrijednost** lozinke.
- Identifikacija i autentikacija u distribuiranoj bazi podataka je složenija. Oracle ima rješenje – tzv. Enterprise User Security (u Enterprise ediciji).
- EUS se temelji na Oracle Identity management infrastrukturi, koja koristi LDAP-suglasan direktorij za centralnu pohranu i održavanje korisnika.

Autorizacija – prava i role

- U Oracle bazi mogu se dati tri vrste prava:

1. na određenu radnju nad **određenim objektom** baze:

```
GRANT SELECT ON razvoj.m_dobavljaci
    TO neki_korisnik;
```

2. na određenu radnju nad **bilo kojim objektom određene vrste na bazi** (tzv. System Privileges):

```
GRANT SELECT ANY TABLE TO neki_korisnik;
```

3. indirektno pravo, dodijeljeno **preko rola** (uloga) :

```
CREATE ROLE rola1;
GRANT SELECT ON razvoj.m_dobavljaci TO rola1;
GRANT rola1 TO neki_korisnik;
```

Autorizacija – korisnički profili

- Osim autorizacije preko privilegija i rola, Oracle ima i dodjelu prava preko **profila**:

CREATE PROFILE profile
LIMIT resource / password_parameters;

Nakon kreiranja, profil se dodjeljuje korisniku u CREATE USER ili ALTER USER naredbi.

- Parametri koji se mogu postaviti kod profila dijele se na resursne parametre i parametre lozinki.

Resursni parametri, npr. SESSIONS_PER_USER, CPU_PER_SESSION, CPU_PER_CALL, CONNECT_TIME i dr.

Parametri lozinki, npr. FAILED_LOGIN_ATTEMPTS, PASSWORD_LIFE_TIME i dr.

Fina autorizacija - Virtual Private Database

- Virtualna privatna baza podataka (**Virtual Private Database**) je tehnologija koja omogućava veću sigurnost kod pristupa podacima.
- Omogućava da određeni korisnici gledaju samo određene redove ili / i određene stupce tablice.
- VPD tehnologija temelji se na mogućnosti dinamičke modifikacije upita. Server baze podataka automatski modificira naredbu koju je korisnik poslao bazi i dodaje u WHERE klauzulu dodatne uvjete (poznate kao predikati). Za primjenu VPD tehnologije koristi se Oracle paket DBMS_RLS.
- VPD tehnologiju ima samo Enterprise edicija baze (EE).

Fina autorizacija - Label Security

- **Label Security** (LS) tehnologija je dodatna opcija Enterprise edicije. Namijenjena je prije svega vojsci, policiji, državnoj upravi, financijskim institucijama i sl.
- Omogućava da se podaci klasificiraju u određene klase i da određena klasa korisnika može mijenjati i i gledati samo određene klase podataka.
- Funkcionalnost koju ima LS može se postići i sa VPD tehnologijom, pa čak i sa vlastitim rješenjem, ali LS tehnologija omogućava da se željena funkcionalnost postigne bez programiranja.
- No, niti VPD i LS tehnologije **ne štiti podatke od privilegiranih korisnika.**
- Oracle ima posebnu opciju, **Data Vault**, za tu namjenu.

Auditiranje – standardno auditiranje

- Auditiranje podataka ne povećava privatnost, integritet ili raspoloživost podataka, ali zato omogućava neporecivost.
- Nije preporučljivo uvijek auditirati sve radnje / događaje, jer bi takvo auditiranje moglo značajno smanjiti performanse sustava i zauzelo bi značajne količine diskovnog prostora.
- Standardno auditiranje ima i Standard edicija baze. Njega prvo treba parametarski dozvoliti. Nakon toga možemo pokrenuti npr. ovakav selektivni audit:

```
AUDIT INSERT, UPDATE, DELETE ON komitenti
      WHENEVER NOT SUCCESSFUL;
```

čime smo rekli da želimo auditirati tablicu KOMITENTI za sve DML radnje, ali samo kod neuspjeha tih radnji.

Auditiranje – Fine-Grained Auditing (FGA) i Audit Vault

- Ponekad nam je potrebno fino auditiranje, npr. na razini pojedinog stupca, a ne cijelog retka tablice. To je moguće izvesti i vlastitim programiranjem, uz pomoć okidača baze i paketa.
- U Enterprise ediciji baze moguće ga je dobiti bez programiranja, korištenjem paketa DBMS_FGA – tzv. **Fine-Grained Auditing**.
- Problem i sa standardnim i sa FGA auditiranjem je da ga **privilegirani korisnici mogu isključiti ili zaobići**. Oracle nudi posebnu opciju na Enterprise ediciji baze, koja se zove **Audit Vault** i koja omogućava neporecivost od strane privilegiranih korisnika.

Kriptiranje podataka u tranzitu

- Kriptiranje podataka koji su u tranzitu nije vezano samo za baze podataka i takvo se kriptiranje uglavnom koristilo i prije kriptiranja podataka koji stoje u bazi.
- Kada je riječ o Oracle bazi, postoje rješenja kriptiranja podataka u tranzitu koja su vezana uz Oracle bazu, ali postoje i rješenja nezavisna od Oracle baze.
- Obje varijante kriptiranja podataka u tranzitu imaju isti cilj, zaštiti tri vrste paketa koji se prenose mrežom:

1. **paketi koji služe za inicijaciju sesije** između klijenta i servera baze podataka;
2. **paketi koje klijent šalje bazi**, uključujući SQL naredbe;
3. **paketi koje baza šalje klijentu** (kao odgovore).

Kriptiranje podataka u tranzitu

- Zašto je važno zaštiti i 1.vrstu paketa, iako Oracle baza tokom logon procesa **uvijek prenosi lozinku u kriptiranom obliku** (bez obzira da li je promet mrežom kriptiran ili nije)?
- Ako promet mrežom nije kriptiran, tokom postupka identifikacije/autentikacije na Oracle bazu može se pojaviti jedna **potencijalna ranjivost – ako napadač zna hash lozinke i prisluškuje mrežu**.
- Proces kriptiranja podataka u tranzitu može se raditi pomoću dva Oracle rješenja (uz Advanced Security Options): **Network Data Encryption** (NDE) i sa **Secure Socket Layer** (SSL).
- Moguće je koristiti i nezavisna softverska ili hardverska rješenja, npr. **Secure Shell** (SSH), **Internet Security Protocol** (IPSec), **hardverske akceleratore**.

Kriptiranju podataka na diskovima može se pristupiti na tri načina

- **„Ručno" kriptiranje kroz aplikaciju, programiranjem**; dobra strana je da je to vrlo fleksibilno; no, ne može se izvesti na brzinu, jer su aplikacije kompleksne; kriptiranje uvijek pogoršava performanse, a kriptiranje vlastitim programiranjem najčešće je najsporije; najveća mana je da se ne može na adekvatan način zaštiti ključeve za kriptiranje;
- **„Automatsko" kriptiranje kroz sustav za upravljanje bazom podataka**; bolje je od prethodne varijante; no, za razliku od programiranja kroz aplikaciju, "transparentno" kriptiranje ne pomaže kod sakrivanja podataka od onih koji imaju pristup bazi;
- **"Automatsko" kriptiranje na razini diskovnog sustava**; isto ne može sakriti podatke od onih koji imaju pristup bazi.

Kriptiranje podataka pomoću paketa DBMS_CRYPTO

- „Ručno" kriptiranje podataka u bazi vrlo je zahtjevno. Traži puno vremena za izvedbu, ima najlošije performanse, omogućuje ostavljanje "rupa" u kriptiranju, a najveći je problem kod njega - kako upravljati ključevima za kriptiranje.
- No, ponekad se mora koristiti "ručno" kriptiranje, npr.:

- **na raspolaganju je samo Standard edicija baze**, koja nema mogućnosti za "transparentno" kriptiranje (koje je dodatna opcija u Enterprise ediciji);
- **želi se kriptirati (neke) podatke i korisnicima baze** - "transparentno" kriptiranje ne može sakriti podatke korisnicima baze.

- Za "ručno" kriptiranje koristi se paket (na bazi) DBMS_CRYPTO.

Kriptiranje podataka pomoću paketa DBMS_CRYPTO (sve edicije)

- podržava kriptografske algoritme: DES, 3DES, 3DES_2KEY, AES, RC4; preporučljivo je koristiti algoritam AES, koji omogućava kriptiranje sa 128, 192 ili 256-bitnim ključevima;
- kriptografski hash algoritmi: MD5, MD4, SH512 / 384 / 256, SHA-1;
- MAC algoritmi (algoritmi za autentikaciju poruka) HMAC_MD5, HMAC_SH512 / 384 / 256; HMAC_SH1;
- kriptografski generatori pseudoslučajnih brojeva u formatu RAW, NUMBER, BINARY_INTEGER;
- kriptiranje blokova podataka: CBC (Cipher Block Chaining, CBC), CFB (Cipher Feedback Chaining) i OFB (Output Feedback Chaining), ECB (Electronic Codebook).
- ispunjavanje (padding) podataka (npr.) nulama ili pomoću metode PBCS5 (preporučljivo).

Kriptiranje podataka pomoću TDE Column Encryption (EE edicija)

- Kao i Oracle Wallet, i TDE CS se može koristiti samo u EE ediciji baze, pri čemu je (isto) potrebna i ASO opcija.
- TDE CS služi **za zaštitu određenih stupaca tablica podataka na disku**, u slučaju da netko neovlašteno dođe do tih podataka izvan baze.
- No, ti stupci **za korisnike baze uvijek transparentno dekriptirani**. Treba napomenuti da stupci nisu kriptirani samo u tablicama, već i REDO, UNDO i TEMP strukturama.
- Može se kreirati novi kriptirani stupac postojeće tablice, ili kriptirati postojeći stupac, ili kreirati potpuno nova tablica:

```
CREATE TABLE t (
        c1 varchar2(30),
        c2 varchar2(30) ENCRYPT);
```

Kriptiranje podataka pomoću TDE Tablespace Encryption (EE)

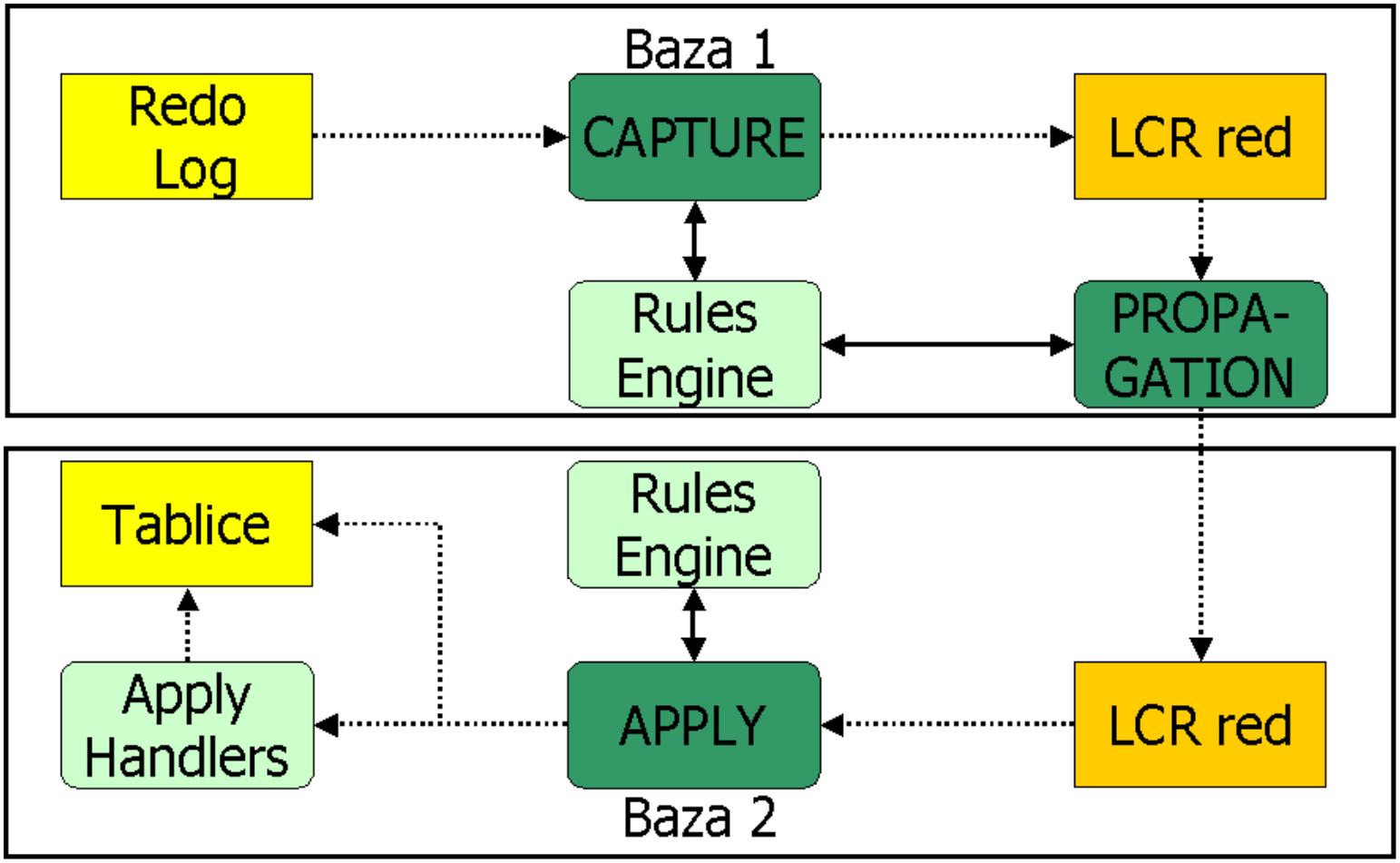
- TDE Tablespace Security (kao i TDE CS) može se koristiti samo u EE ediciji baze, pri čemu je potrebna i ASO opcija.
- Kako samo ime kaže, ovdje se **ne kriptira samo određeni stupac, već cijeli tablespace**.
- Za razliku od TDE CS, kod TDE TS nije moguće kriptirati postojeću tablicu ili postojeći tablespace, već je **potrebno kreirati novi kriptirani tablespace** i onda u njega kopirati postojeće tablice koje želimo kriptirati.
- Kreiranje kriptiranog tablespace-a radi se sa:

```
CREATE TABLESPACE kriptirani_tablespace
        DATAFILE ...
        ENCRYPTION DEFAULT STORAGE (ENCRYPT);
```

Kriptiranje podataka pomoću TDE Tablespace Encryption (EE)

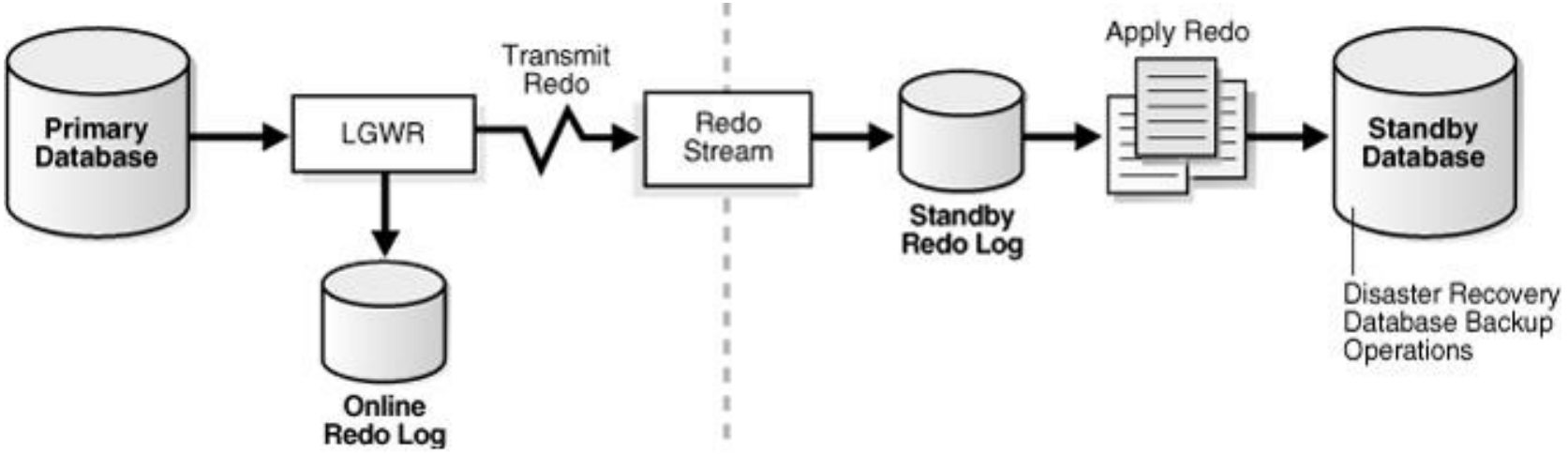
- **TDE TS kriptira podatke prije slanja podataka iz SGA na disk**, odnosno dekriptira ih u obrnutom smjeru.
- To znači da su **podaci u SGA u nekriptiranom obliku**, što predstavlja malu potencijalnu ranjivost u slučaju da netko neovlašten može
- Prednost je u tome da se **čitanje/upis u SGA radi brzo**.
- Podaci u REDO, UNDO i TEMP pomoćnim strukturama na disku su kriptirani, isto kao i kod TDE CS.
- Nakon kopiranja nekriptirane tablice iz nekriptiranog tablespace-a u kriptirani tablespace, te brisanja nekriptirane tablice, nije sigurno da više nema nekriptiranih podataka. Naime, **ti podaci ostaju određeno vrijeme** u REDO, UNDO i TEMP pomoćnim strukturama.

Replikacija podataka pomoću Oracle Streams procesa (EE edicija)



- Vlastito rješenje replikacije može se zasnivati npr. na database triggerima.

Oracle Data Guard za povećavanje raspoloživosti i Disaster Recovery (opcija nad EE)



- Vlastito rješenje može se zasnivati na sličnoj tehnici, pri čemu sami rješavamo slanje arhivskih redo logova na sekundarnu (udaljenu) lokaciju, te njihovu primjenu na sekundarnu bazu podataka.

Zaključak

- Oracle DBMS ima puno rješenja za sigurnost BP, koja su važna i kod podrške GDPR regulativi.
- Neka od tih rješenja imaju i jeftinija SE edicija baze (pa čak i besplatna XE edicija baze.
- Neka rješenja ima samo značajno skuplja EE edicija, npr. Virtual Private Database, Fine-Grained Auditing.
- Neka rješenja su opcije (koje se dodatno plaćaju) nad EE edicijom, npr. Data Vault, Audit Vault, Label Security, Transparenet Data Encryption, Network Data Encryption
- Kod auditiranja podataka, moramo paziti da sada uz izvorne podatke i audit podaci moraju biti u skladu s GDPR regulativom.
- Isto vrijedi i za replikaciju i Disaster Recovery rješenja, pa čak i najobičniji backup podataka.