Oracle EUS / SSO arhitektura u Croatia osiguranju

Nenad Dragojlović
Tihomir Bošnjak

Sadržaj

1. Problem (zahtijev, motivacija)
2. Analiza mogućih rješenja
3. Instalacija i konfiguracija EUS rješenja
4. Konfiguracija SSO rješenja za Forms&Reports middletier
5. Topologija Oracle aplikacijskih servera u CO
6. Zaključak
7. Referentni materijali

Problem

Problem : Slabe bazne lozinke korisnika

- sigurnosni problem + zahtijev revizije

Rješenja :

a) uvesti “password policy” na korisničkim računima u bazi

- pravila kompleksnosti

- periodika promjene

=> dodatno opterećenje na korisnike

b) korištenje windows lozinke za autentikaciju na bazi

=> uložiti napor u integraciju

Odlučili smo se omogućiti korištenje windows lozinki za prijavu na bazu.

Analiza mogućih rješenja

Kako bi bila moguća autentikacija korisnika sa lozinkom pohranjenom u korporativnom AD-u, slijedeći uvjeti moraju biti zadovoljeni :

1) Baza mora biti konfigurirana za Enterprise User Security (EUS)

- **EUS može koristiti isključivo Oracle-ovu implementaciju LDAP direktorija : Oracle Internet Directory (OID)**
- **OID je obavezna komponenta.**
  - **Pohranjuje kompatibilne password verifier-e (SHA1, MD5)**
  - **Služi za definiranje korporativnih (globalnih) korisnika i mapiranje na zajedničke bazne scheme**

2) Mora postojati integracija između AD-a i OID-a.

Analiza mogućih rješenja

Integracija AD-a i OID-a moguća je na 2 načina :

1) **Sinhronizacija korisničkih zapisa korištenjem Oracle Directory Integration Platform tehnologije (DIP)**
   - Zapisi se fizički prebacuju (sinhroniziraju) iz AD-a u OID
   - Zbog nekompatibilnosti password verifier-a, lozinke se prebacuju korištenjem Oracle Active Directory Password filtera na DC-u
2) **Ulančavanje direktorija korištenjem OID server chaining tehnologije**
   - Svaki upit na OID proslijeđuje se i na AD
   - Nema fizičkog prebacivanja (sinhronizacije) korisnika i njihovih lozinki
   - OID ostaje kao mapping direktorij
   - Postojanje kompatibilnog password verifiera osigurava se instalacijom Active Directory Notification Plug-in-a na svaki DC
   - Rješenje dostupno od verzije IDM-a 10.1.4.2

Analiza mogućih rješenja

Oba riješenja kompatibilna su sa password authenticated EUS tehnologijom jer mogu osigurati provjeru kompatibilnih password verifier-a.

Sinhronizacija korisničkih zapisa (DIP) + provjera AD lozinke korištenjem External Authentication Plug-in-a nije kompatibilna sa EUS tehnologijom, pa smo je isključili iz razmatranja.

OID server chaining je puno jednostavniji za konfiguraciju.

Međutim, OID server chaining nije kompatibilan sa Forms aplikacijama u single sign-on modu rada pa smo se odlučili za Directory Integration Platform rješenje !

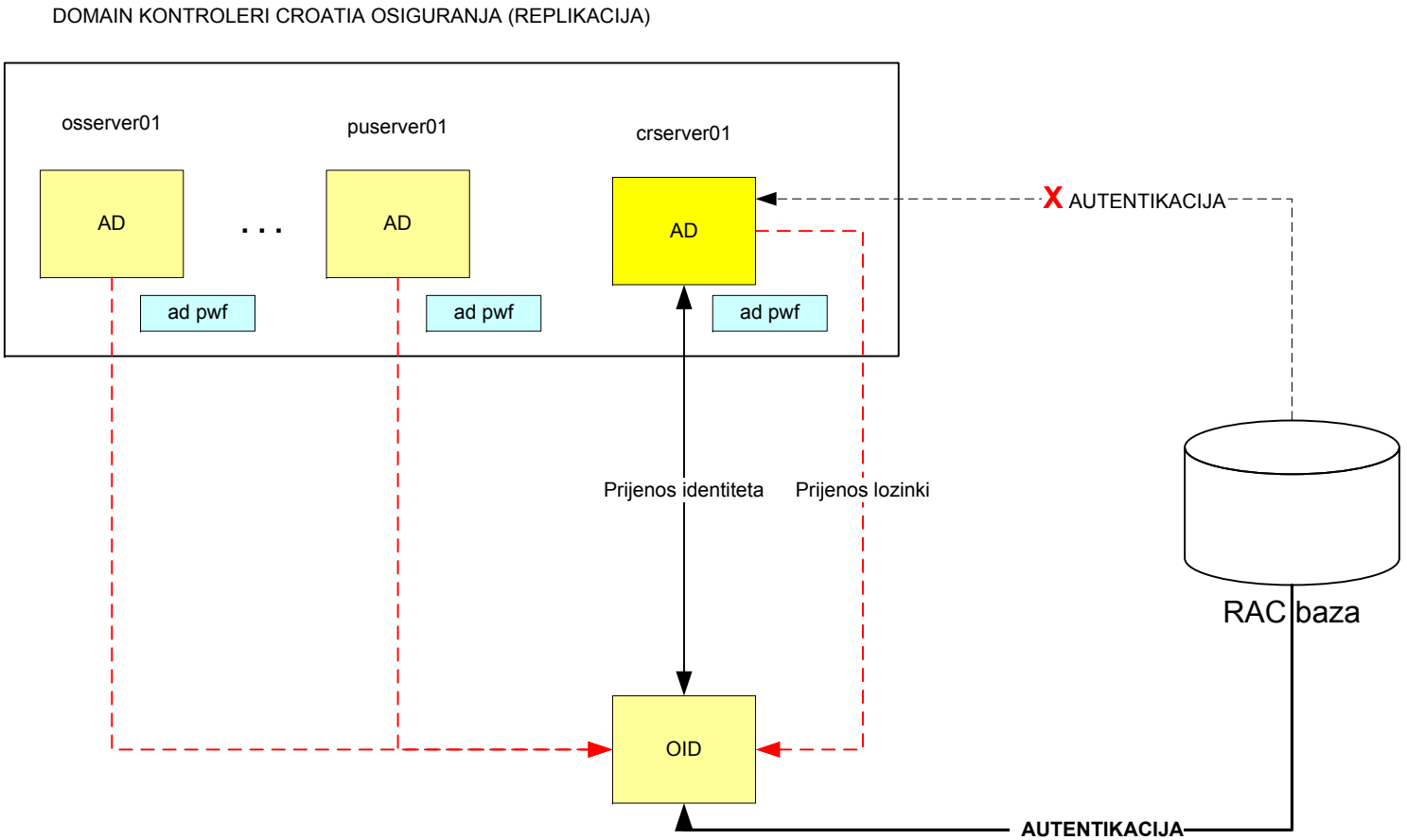
Instalacija i konfiguracija EUS rješenja

1. **Instalacija OID-a**

2. **Integracija AD-a i OID-a**
   - **2.1. Prijenos korisnika iz AD-a u OID**
     - **konfiguracija DIP-a**
   - **2.2. Prijenos lozinki iz AD-a u OID**
     - **Oracle Active Directory Password Filter**

3. **Konfiguracija baze za password authenticated EUS**

Instalacija i konfiguracija EUS rješenja

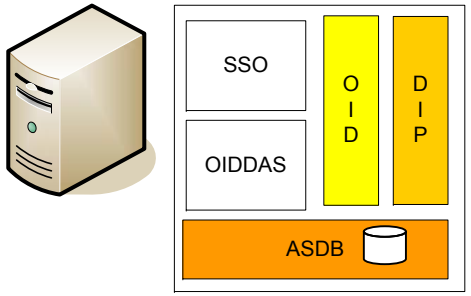


1. Instalacija OID-a

OID dolazi kao sastavna komponenta Oracle Identity Management 10.1.4. instalacije.

Integralne komponente u Oracle Identity Management 10.1.4. su :

Oracle Internet Directory (OID)
Directory Integration Server (DIP)
Single sign-on server (SSO)
Delegated Administration Services (DAS)
Metadata Repository (ASDB)

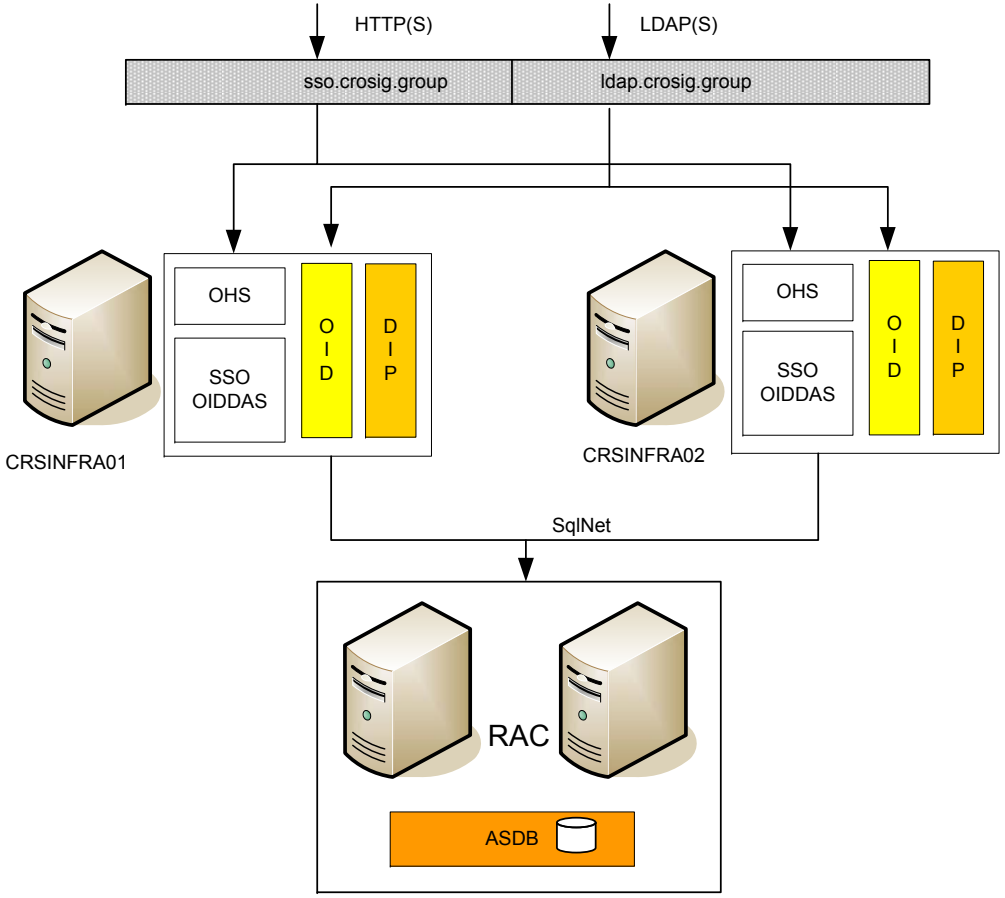


OID i DIP sadržani su i kao identity managent komponetne u FM 11g

1. Instalacija OID-a

Mission critical sustav => želimo visoko raspoloživo rješenje.

Oracle je predvidio **OracleAS Cluster (Identity Management) konfiguraciju** :



1. Instalacija OID-a

Instalacija OracleAS Cluster (Identity Management) arhitekture :

1. **Konfiguracija load balancer-a**
2. **Instalacija metadata repository-a u RAC bazu**
3. **Instalacija prvog noda infrastrukture**
4. **Instalacija drugog noda infrastrukture**

1. Instalacija OID-a

1. **Konfiguracija load balancera**

Definirati virtualne adrese, odnosno “content rule-ove” za sve servise u clusteru

1) HTTP : Infra.crosig.group:7778 : crsinfra01:7778, crsinfra02:7778
2) LDAP : Infra.crosig.group:389 : crsinfra01:389, crsinfra02:389
3) SLDAP : Infra.crosig.group:636 : crsinfra01:636, crsinfra02:636

Dodatno, zbog potrebe postojanja sekundarne instance ldap servera s kojom preko ssl protola (sa serverskom autentikacijom) komunicira AD password filter pri slanju lozinki (objašnjeno dalje u prezentaciji)

4) SLDAP : Infra.crosig.group:1636 : crsinfra01:1636, crsinfra02:1636

VAŽNO : deifinirati NAT koji source IP noda translatira virtualni IP.

2.1. Prijenos korisnika iz AD u OID

1. **Konfiguriranje DIP-a**
   - **1.1. Definiranje mapping file-a**
   - **1.2. Konfiguriranje connector profila**

2. **Uspostavljanje sinhronizacije**
   - **2.1 priprema OID-a**
   - **2.2. izvođenje bootstrapa korisnika**
   - **2.3 pokretanje odisrv-a za kontinuiranu sinhronizaciju**

2.2. Prijenos lozinki iz AD-a u OID

1. **Priprema dodatne OID instance**
2. **Podešavanje Oracle Password filtera**

3. Konfiguracija baze za password authenticated EUS

1. Konfigurirati ORACLE_HOME za uporabu OID-a

- Za konfiguraciju koristimo Oracle Net Configuration Assistant (**netca**)
- Odaberemo OID za tip direktorija i zadamo hostname, port i ssl port
- U ORACLE_HOME/network/admin folderu nastat će **ldap.ora** datoteka

```
# ldap.ora Network Configuration File: /u02/TNS_ADMIN/ldap.ora
# Generated by Oracle configuration tools.

DIRECTORY_SERVERS= (infra.crosig.group:389)

DEFAULT_ADMIN_CONTEXT = "dc=crosig,dc=group"

DIRECTORY_SERVER_TYPE = OID
```

3. Konfiguracija baze za password authenticated EUS (2)

2. Registrirati bazu u OID-u

- Za registraciju baze koristimo Database Configuration Assistant (**dbca**)
- DBCA koristi LDAP.ora kako bi locirao OID
- Odabrati Configure Database Options / ime baze / opciju da želimo registrirati bazu za korištenja sa direktorijem
- Unijeti podatke o super korisniku OID-a

```
User DN: cn = orcladmin
Password = ******
```

- Unijeti lozinku za wallet
  - wallet je potreban iako ne koristimo SSL za osiguranje komunikacije
  - wallet sadrži random generiranu lozinku koju baza koristi za spajanje na OID
  - ukoliko do sada ne postoji, wallet će biti kreiran

3. Konfiguracija baze za password authenticated EUS (3)

Napomene uz registraciju RAC baze :

Na prvom nodu :

- **Napraviti LDAP.ora datoteku**
- **Registrirati bazu u OID**
  -> Prije pokretanja DBCA osigurati da u oratab file-u stoji zapis za lokalnu instancu.

Na ostalim nodovima :

- **Iskorpirati LDAP.ora file na istu lokaciju ($ORACLE_HOME/network/admin/ldap.ora)**
- **Kopirati wallet na istu lokaciju ($ORACLE_BASE/admin/[database]/wallet/ewallet.p12)**
- **Kroz OWM omogućiti auto-login opciju na iskopiranim walletima => mora nastati i datoteka cwallet.sso**
- **Dodati LDAP_DIRECTORY_ACCESS=PASSWORD u spfile.ora ili init.ora datoteku na ostalim RAC instancama**

3. Konfiguracija baze za password authenticated EUS (4)

3. Migrirati bazne korisnike u korporativne korisnike

a) Manualno

```
ALTER USER mperic IDENTIFIED GLOBALLY AS
'cn=mperic,cn=users,dc=crosig,dc=group';
```

b) Koristeći komandno linijski utiliy : UMU (User Migration Utility)

Konfiguracija SSO-a za Forms&Reports middletier

Razmjerno jednostavna !

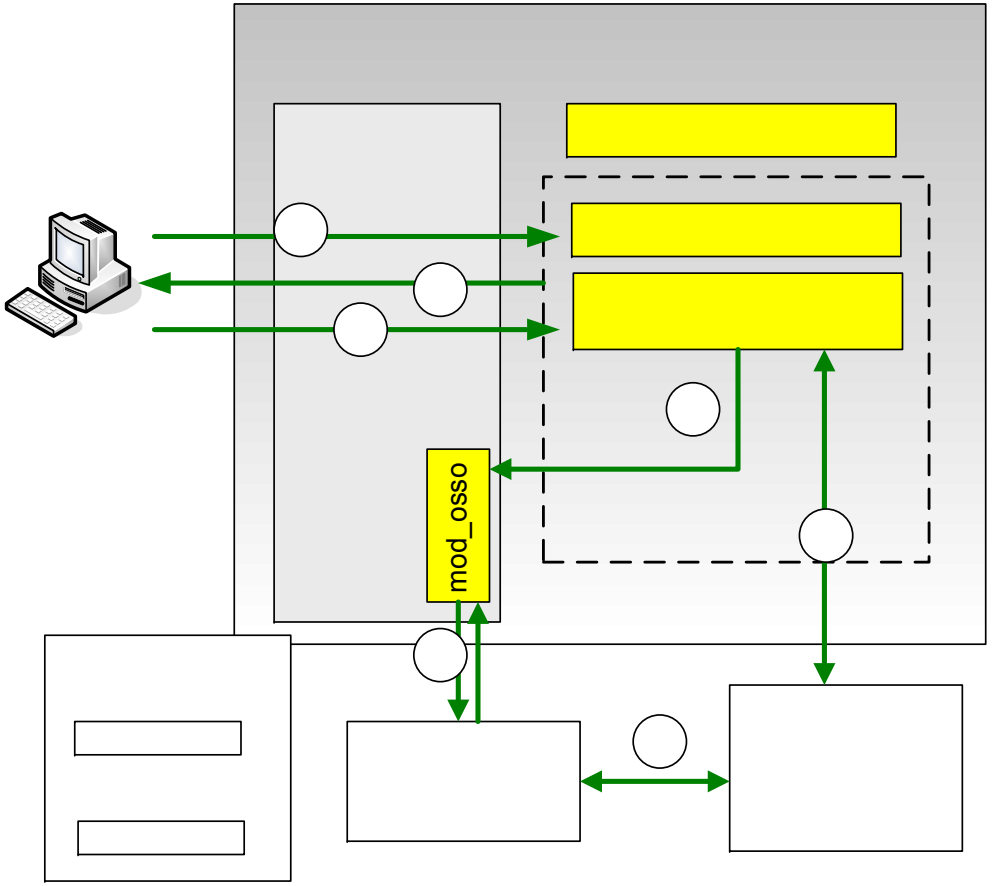
- **registrirati middletier instancu sa OID-om i metadata repositorijem (MR)**
- **omogućiti sso funkcionalnost u formsweb.cfg datoteci**

Konfiguracija SSO-a za Forms&Reports middletier

```
<formsweb.cfg>

[default]

# Single Sign-On OID configuration parametri :

ssoEnabled=false
oid_formsid=formsApp_crsias01.crosig.group_928E57C15EC311DF9F1EFF7D
formsid_group_dn=cn=Logical Application Group,
      orclApplicationCommonName=formsApp_crsias01.crosig.group_928E57C15EC311DF9F1
      EFF7D22AF6C6F, cn=forms, cn=Products, cn=OracleContext
ssoDynamicResourceCreate=true
ssoErrorUrl=
ssoCancelUrl=
(…)

[app1]
ssoEnabled=true
form=start_form.fmx
(…)

[app2]
(…)
```

Konfiguracija SSO-a za Forms&Reports middletier

Kako radi SSO ?



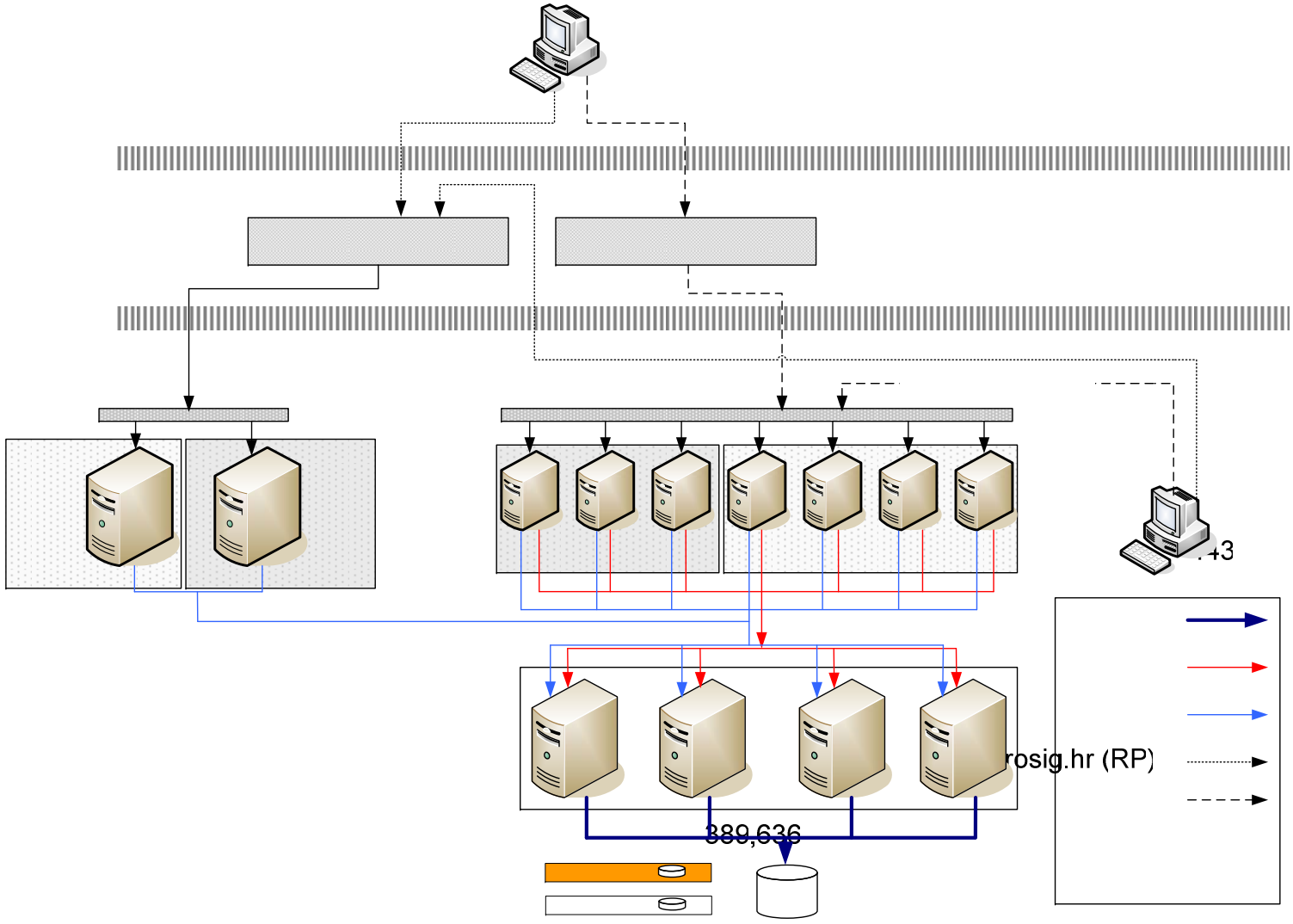
Oracle Appli

Oracle HT
Server

Konfiguracija SSO-a za Forms&Reports middletier

- **Problemi sa RAD-ovima i EUS-om**
- **Mogućnost integracije sa WNA rješenjem**

CO topologija (logički pogled)



CO topologija

Visoka raspoloživost baze osigurana je ORACLE RAC 10gRel2 tehnologijom

- **4 noda Bull (IA64)**
- **Red Hat Enterprise Linux 4**
- **Dvije baze :**
  - **Transakcijska produkcijska baza (CODB)**
  - **Metadata repository baza (ASDB)**

Visoka raspoloživost Forms&Reports middletier-a osigurana je farmom ias-a

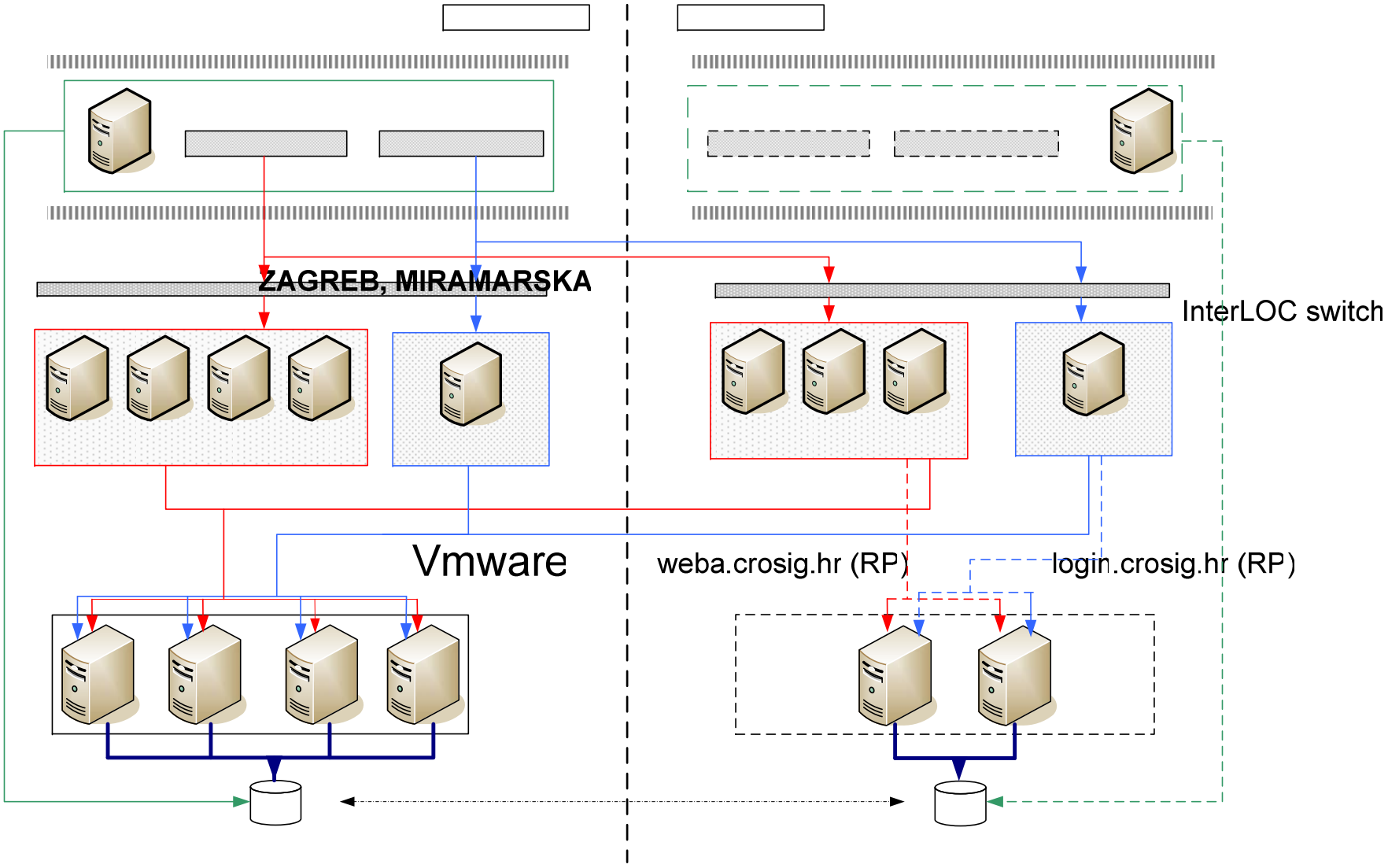
- **7 nodova, verzija OAS 10.1.2.2**
- **CISCO CSS 11500 (load balancer)**
- **Svi nodovi registrirani u SSO infrastrukturu**

CO topologija (2)

Pristup s Interneta osiguran je tehnologijom reverznog proxy-ja

- **Kao reverzni proxy koristi se Oracle Web Cache**
- **Koristimo 2 reverzna proxy-a**
  - **weba.crosig.hr**
    - **Redirekcija na forms&reports farmu**
    - **Nužnost konfiguriranja “sticky” load balancinga na temelju http cookie-a (JSESSIONID)**
    - **Nužnost definiranja novog virtualnog hosta (weba.crosig.hr) na svakom od nodova**
    - **Nužnost registracije novog virtualnog hosta na SSO server-u (ssoconf)**
  - **login.crosig.hr**
    - **Redirekcija na infrastrukturni cluster**
    - **I Internet i intanet korisnici su preusmjereni za login.crosig.hr jer se SSO može konfigurirati samo na jednoj adresi**
      - **Korištenje isključivo https protokola za pristup do login stranice**
    - **Nužnost prekonfiguracije sso servera na url reverznog proxy-a**
    - **Nužnost definiranja novog virtualnog hosta (login.crosig.hr) na svakom od nodova**

CO topologija (disaster recovery pogled)



CO topologija (disaster recovery pogled)

- **Temelj disaster recovery rješenja su 2 EMC Symmetrix storage-a,**
- **Na storage-u se nalaze :**
  - **data file-ovi baze**
  - **Image-i operacijskih sustava**
    - **Linux nodovi (RAC instance)**
    - **Windows serveri u disaster recovery rješenju**
      - **Exchange**
      - **Revezni proxy (login.crosig.hr i weba.crosig.hr)**
      - **(…)**
- **Dva storage-a su u sinhronoj replikaciji !**
  - **> Sadržaj na prvom storage-u se ne može pohraniti dok se ne pohrani i na drugom storage-u.**
- **CSS-ovi su povezani kroz interlokacijske switcheve**
  - **Portovi su u istom VLAN-u**

CO topologija (disaster recovery pogled)

Kada je primarna lokacija aktivna :

- **Bazne instance na sekundarnoj lokaciji su ugašene**
- **Forms&Reports instance su aktivne na obje lokacije**
- **Infrastrukturne intance su aktivne na obje lokacije**
- **Reverzni proxy je ugašen na sekundarnoj lokaciji**

Kada sekundarna lokacija postaje aktivna :

- **Sekundarne bazne instance se pale**
  - **Identična mrežna i os konfiguracija kao i prva dva noda na primarnoj lok.**
- **Forms&Reports zahtijeve preuzimaju 3 instance na sekundarnoj lok.**
- **Infrastrukturne zahtijeve (SSO,EUS) preuzima 1 instanca na sek. lok.**
- **Pali se sekundarni reverzni proxy**

Zaključak

- **Rješenje zadovoljava početne zahtijeve.**
- **Korisnici pamte i mijenjaju samo jednu lozinku za pristup svim aplikacijama.**
- **Korisnici se održavaju na jednom mjestu. Deaktivacija računa na AD-u onemogućuje pristup bazi.**
- **Pristup login infrastrukturi moguć je iz intraneta, ali i sa interneta.**
- **Rješenje nudi HA na lokaciji , ali i geografski distribuiran disaster recovery**
- **Ostvareno bez nabavke dodatnih licenci.**

Referentni materijali

- **Enterprise User Administration Guide 10gRel2**
- **Can EUS Users Authenticate With Passwords Stored in AD ? (Note 344432.1)**
- **How To Configure Enterprise User Security In An Oracle 10g RAC Environment (Note 316360.1)**
- **Oracle Identity Management Integration Guide 10.1.4.2**