Kako promijeniti LDAP domenu ustanove

LDAP domena ustanove u pravilu mora odgovarati DNS domeni. Ako ustanova mijenja svoju DNS domenu, potrebno je promjeniti i LDAP domenu ustanove. Promjenom LDAP domene mijenjaju se i korisničke oznake svih korisnika iz te ustanove (jedna ustanova ne može istodobno imati dvije različite LDAP domene) na sljedeći način:

nesto@stara_domena.hr -> nesto@nova_domena.hr

Postupak promjene domene

1. Željenu promjenu najaviti timu sustava AAI@EduHr na adresu aai@srce.hr te s timom dogovoriti točan termin promjene.
2. Podnijeti zahtjev kroz web-sučelje AAI@EduHr administracija. Zahtjev je dostupan u izborniku web-sučelja:

    - Novi zahtjev vezan uz status
        - Promjena domene matične ustanove“
            - Zahtjev za promjenom domene matične ustanove.

    U zahtjev je potrebno upisati novi naziv domene i željeni datum promjene. Ispuniti „checkbox“ ukoliko su ispunjeni svi uvjeti iz „checkbox-a“. Ako uvjeti iz „checkbox-a“ nisu ispunjeni, zahtjev možete spremiti za kasnije i podnijeti ga kada ispunite sve navedene uvjete. Kada su svi traženi podaci ispunjeni, podnosi se zahtjev. Kada zahtjev prijeđe u stanje 'podneseno' bit će omogućen dohvat PDF verzije obrasca zahtjeva koju je potrebno ovjeriti potpisom čelnika i pečatom ustanove te poslati na adresu navedenu na obrascu.
3. Svim korisnicima koji se nalaze u LDAP imeniku ustanove **obavezno i na vrijeme** treba najaviti točan datum promjene korisničkih oznaka jer nakon što prebacite LDAP imenik na novu domenu, autentikacija sa starim korisničkim oznakama više neće biti moguća. Korisnicima objasniti da će se promijeniti domena u njihovoj korisničkoj oznaci, a da će im zaporka ostati ista.
4. Voditi računa o tome da će neke aplikacije promjenom korisničke oznake korisnika izgubiti povijest korištenja za korisnike kojima se promijenila korisnička oznaka (ako je aplikacija tako dizajnirana da osobu pamti po korisničkoj oznaci, promjenom korisničke oznake aplikacija će misliti da je to novi korisnik). Upozoriti korisnike na tu činjenicu. U slučaju da ustanova koristi neki sustav za e-učenje, svakako obavjestiti održavatelje sustava o nadolazećim promjenama.
5. U dogovorenom terminu u koordinaciji s timom sustava AAI@EduHr na poslužitelju ustanove napraviti promjene opisane u nastavku.
    - ako koristite uslugu ugošćavanja primarnih AAI@EduHr servisa na računalu hosting.aaiedu.hr, promjene će za vas napraviti tim sustava AAI@EduHr
    - ako koristite uslugu ugošćavanja sekundarnih AAI@EduHr servisa, svakako to napomenuti u postupku dogovoranja.

Procedura promjene LDAP domene na lokalnom poslužitelju ustanove opisana je u nastavku.

Promjena kofiguracije LDAP poslužitelja

1. Spustite LDAP, RADIUS i AOSI poslužitelj izvršavanjem naredbi:

    ```
    /etc/init.d/aosi stop
    /etc/init.d/freeradius stop
    /etc/init.d/slapd stop
    ```

2. Eksportirajte podatke iz LDAP imenika u .ldif datoteku:

    ```
    # slapcat -l /var/backups/openldap-backup.ldif
    ```

3. Za svaki slučaj, napravite backup direktorija **/var/lib/ldap/**:

    ```
    # tar cfvz /var/backups/ldap.tar.gz /var/lib/ldap/
    ```

4. Zamjenite staru domenu novom uporabom naredbe:

    ```
    # sed s/stara_domena/nova_domena/g /var/backups/openldap-backup.ldif > /var/backups/openldap-new.ldif
    ```

    (sve u jednom retku) i pritom pripazite da se možda string **stara_domena** ne poklapa s nečim što se ne bi smjelo promijeniti. Takve stvari ručno popravite editirajući datoteku **/var/backups/openldap-new.ldif**

5. Zatim prekonfigurirajte LDAP:

    ```
    # dpkg-reconfigure slapd
    ```

    (u postupku rekonfiguracije potrebno je upisati novu domenu):

```
# dpkg-reconfigure openldap-aai
```

6. Obrišite LDAP bazu s diska:

   ```
   # rm -f /var/lib/ldap/*
   ```

   te pokrenite LDAP poslužitelj kako bi se kreirala nova baza pa zatim spustite LDAP poslužitelj:

   ```
   /etc/init.d/slapd start
   /etc/init.d/slapd stop
   ```

7. U novi LDAP imenik unesite korisnike iz **openldap-new.ldif** datoteke koju ste kreirali u 4. koraku:

   ```
   # slapadd -l /var/backups/openldap-new.ldif
   ```

Postavite odgovarajuće ovlasti nad datotekama u **/var/lib/ldap/** direktoriju. Ovisno o distribuciji, sve datoteke trebaju biti u vlasništvu korisnika *ldap* ili *openldap* tj. potrebno je izvršiti jednu od sljedećih naredbi:

```
# chown -R ldap:ldap /var/lib/ldap/
```

ili

```
# chown -R openldap:openldap /var/lib/ldap/
```

Promjena konfiguracije RADIUS poslužitelja

1. U datoteci **/etc/freeradius/modules/ldap-aai** liniju:

   ```
   basedn = "dc=stara_domena,dc=hr"
   ```

   zamijenite linijom:

   ```
   basedn = "dc=nova_domena,dc=hr"
   ```

   Prema potrebi, u istoj datoteci promjenite i naziv poslužitelja u liniji:

   ```
   server = "naziv_posluzitelja"
   ```

2. U datotekama **/etc/freeradius/proxy-eduroam.conf** i **/etc/freeradius/sites-available/aai** liniju:

   ```
   realm stara_domena.hr {
   ```

   zamijenite linijom:

   ```
   realm nova_domena.hr {
   ```

3. Prema uputama za upravljanje certifikatom (FreeRADIUS) generirati novi rootCA i poslužiteljski certifikat koji će imati ispravnu vrijednost nove domene;

4. Prema uputama kako korisnicima omogućiti spajanje na eduroam predati novi rootCA i novi logo institucije u installer uslugu;

5. Ako institucija ima uvedenu eduroam uslugu, zatražite novu vrijednost atributa Operator-Name slanjem elektroničke pošte na adresu admin@eduroam.hr. Novu vrijednost unesite u konfiguraciju RADIUS poslužitelja prema uputama datim u e-mailu s novom vrijednošću;

6. Obavijestite sve korisnike da je zbog promjene domene potrebno ponovno konfigurirati uređaje za spajanje na eduroam uslugu. Najjednostavniji način za rekonfiguraciju je korištenjem eduroam installer alata;

Promjena konfiguracije AOSI poslužitelja

1. U datoteci **/etc/aosi/config.pm** redak

   ```
   $base_dn='dc=stara_domena,dc=hr';
   ```

   zamijenite s:

```
$base_dn='dc=nova_domena,dc=hr';
```

2. U datoteci **/etc/aosi-www/config.php** u retcima:

```
define ('REALM', 'stara_domena.hr');
define ('BASE_DN', 'dc=stara_domena,dc=hr');
```

potrebno je umjesto stare domene upisati novu LDAP domenu ustanove:

```
define ('REALM', 'nova_domena.hr');
define ('BASE_DN', 'dc=nova_domena,dc=hr');
```

3. Ako je potrebno, u datoteci **/var/lib/aosi/www/aosi.wsdl** pri dnu datoteke u retku koji počinje s **<wsdlsoap:address location="...** promjenite adresu poslužitelja.

I na kraju...

1. Ako to još niste napravili u nekom od prethodnih koraka, pokrenite LDAP, AOSI i RADIUS poslužitelje naredbama:

```
/etc/init.d/slapd start
/etc/init.d/aosi start
/etc/init.d/freeradius start
```

2. Obavezno na aai@srce.hr pošaljite obavijest da ste izvršili promjenu domene kako bismo mogli ažurirati odgovarajuće parametre u središnjem dijelu AAI@EduHr sustava.