Instalacija i konfiguracija LDAP aplikacije

---

1. Prekopirajte *ldap-admin.war*, *ldap-korisnik.war* i *configurator.jar* u */root* folder na serveru
2. Potrebno je raspakovati preuzete aplikacije:

```
cd /root
mkdir ldap-admin
unzip ldap-admin.war -d ldap-admin
mkdir ldap-korisnik
unzip ldap-korisnik.war -d ldap-korisnik
```

Nakon ovoga će biti kreirani folderi *ldap-admin* i *ldap-korisnik* što ce ujedno biti i imena aplikacija.

Napomena: ukoliko želite da promenite imena ovim aplikacijama, potrebno je da umesto *ldap-admin* odnosno *ldap-korisnik* u prethodnim komandama unesete imena koja želite. Ova nova imena ćete morati da unesete i pri konfiguraciji aplikacije u sledećem koraku.

3. Za konfigurisanje aplikacije potrebno je pokrenuti *configurator.jar* fajl:

```
java -jar configurator.jar
```

U komandnoj liniji unesite potrebne informacije koje će se tražiti od vas.

4. Zaštita pristupa aplikacijama

Predviđeno je da korisnička aplikacija bude javno dostupna, dok je pristup administratorskoj aplikaciji treba biti dostupan samo sa IP adresa računara u instituciji sa kojih se otvaraju korisnički nalozi.

Ukoliko su administratorska i korisnička aplikacija instalirane na različitim serverima, onda se pristup administratorskoj aplikaciji treba ograničiti na odgovarajućim pristupnim listama mrežnih uređaja i/ili u *iptables* samog servera.

Međutim, ukoliko su obe aplikacije instalirane na istom serveru, onda je prethodno navedeno filtriranje nemoguće konfigurisati, obzirom da se obema aplikacijama pristupa po istoj IP adresi i portu. U tom slučaju je neophodno u samoj aplikaciji definisati sa kojih IP adresa je omogućen pristup administratorskoj aplikaciji.

U okviru Tomcata web servera, moguće je definisati sa kojih IP adresa je moguć pristup pojedinačnim aplikacijama http://tomcat.apache.org/tomcat-7.0-doc/config/valve.html#Remote Address Filter. Potrebno je da odkomentarišete i izmenite deo koji se odnosi na prava pristupa u */root/ldap-*

admin/META-INF/context.xml fajlu, tako što ćete dozvoliti pristup IP adresama administratora aplikacije. U *allow* atribut treba da navedete IP adrese koje imaju pristup aplikaciji, razdvojene uspravnom crtom (|) , npr:

```
<Valve className="org.apache.catalina.valves.RemoteAddrValve" allow="192.16.1.1|192.16.1.9" />
```

U okviru *allow* atributa se mogu koristiti i regularni izrazi kojima se mogu opisati opsezi adresa. Sintaksa za regularne izraze koja se koristi je opisana u okviru *java.util.regex* paketa, a za detalje o implementaciji konsultujte java dokumentaciju. Jedan primer korišćenja regularnih izraza bi bio:

```
<Valve className="org.apache.catalina.valves.RemoteAddrValve" allow="192.16.1.[1-5]|192.16.1.9" />
```

Ovakvom konfiguracijom, eksplicitno se dozvoljava pristup sa navedenih IP adresa, dok je sa sa svih ostalih IP adresa pristup implicitno zabranjen.

5. Potom aplikacije treba da zapakujete u *.war* fajlove komandama:

```
cd ldap-admin
zip -9 -rD ldap-admin.war *
cd ..
cd ldap-korisnik
zip -9 -rD ldap-korisnik.war *
cd ..
```

Napomena: ukoliko ste menjali naziv aplikacijama, potrebno je da u ovim komandama unesete odgovarajuće nove nazive

6. Sada treba prebaciti aplikacije u tomcat-ov *webapps* folder:

```
mv ldap-admin/ldap-admin.war /usr/local/tomcat/webapps/ldap-admin.war
mv ldap-korisnik/ldap-korisnik.war /usr/local/tomcat/webapps/ldap-korisnik.war
```

Napomena: ukoliko ste menjali naziv aplikacijama, potrebno je da u ovim komandama unesete odgovarajuce nove nazive

Ukoliko se korisnička i administratorska aplikacija ne nalaze na istom serveru, odgovarajući *.war* fajl prebacite na u *../tomcat/webapps* folder na drugom serveru.

7. Nakon ovoga možete ukloniti *ldap-admin* i *ldap-korisnik* direktorijume:

```
rm -rf ldap-admin
rm -rf ldap-korisnik
```

8. Kako bi bila moguća TLS komunikacija korisničke i administratorske aplikacije sa LDAP direktorijumom, potrebno je u *trusted certificate* Java-in *keystore* na serveru gde se nalaze korisnička i administratorska aplikacija uvesti sertifikat koji koristi LDAP direktorijum.

Komanda za uvoz *trusted* sertifikata u Java *keystore*, npr:

```
cd /usr/java/jdkX.X/jre/lib/security
keytool -import -alias aai -file sertifikat.crt -keystore cacerts
```

gde je X.X verzija Java-e koja se koristi, a *sertifikat.crt* sertifikat koji koristi LDAP server. Ukoliko pri ovome morate da unesete lozinku, njena default vrednost je “changeit”

9. Aplikacija koristi port 587 za slanje mail-ova putem TLS-a. Pošto koristi TLS, sertifikat SMTP servera takođe mora biti ubačen u Java-in keystore, na opisan način.

10. Aplikacije su spremne za korišćenje i možete im pristupiti na sledeći način:

```
https://ime-servera/ldap-admin
https://ime-servera/ldap-korisnik
```

Napomena: Ukoliko ste menjali imena aplikacijama, potrebno je da umesto *ldap-korisnik* odnosno *ldap-admin* unesete nova imena

Napomena: Da biste mogli da koristite aplikacije LDAP server mora da bude startovan.

11. log fajl aplikacije se nalazi u tomcat-ovom fajlu */usr/local/tomcat/logs/catalina.out*.

Posle uspešne instalacije potrebno je isključiti debug level logovanje, kako log fajlovi ne bi opterećivali sistem. Isključivanje se obavlja tako što se u fajlovima *ldap-korisnik/WEB-INF/classes/log4j.properties* i *ldap-admin/WEB-INF/classes/log4j.properties* na mestima gde piše DEBUG, navede INFO.

12. Da bi korisnik imao privilegije administratora na ldap-admin aplikaciji potrebno je da ima postavljen atribut sa vrednošću

    eduPersonEntitlement = urn:mace:amres.ac.rs:rcub.bg:entitlement:ldap:SuperAdmin

    Ili

    eduPersonEntitlement = urn:mace:amres.ac.rs:rcub.bg:entitlement:ldap:Admin