ownCloud i AAI@EduHR

Kao nastavak serije članaka o vlastitom oblaku fokusirat ćemo se na aplikaciju ownCloud uz prijavu korisnika pomoću podataka iz sustava AAI@EduHR.

ownCloud [1]je rješenje otvorenog koda vrlo slično popularnom Dropboxu. Uz sinkronizaciju datoteka na računalima i mobilnim uređajima, moguće je i dijeliti datoteke među korisnicima (javnim ili privatnim poveznicama), postavljati lozinke za pristup datotekama, kao i zadavanje datuma isteka dijeljenja.

Instalacija se na Debianu se obavlja standardnim načinom, uz napomenu da paket nije dostupan na službenom Debianovom repozitoriju nego na SUSEovom. Zato je potrebno dodati taj repozitorij naredbom:

```
echo 'deb http://download.opensuse.org/repositories/isv:/ownCloud:/community/Debian_7
.0/ /' >> \
/etc/apt/sources.list.d/owncloud.list
```

Nakon ovog ide standardni dio, *apt-get update* i *apt-get install owncloud*.

Također je potrebno pripremiti bazu podataka (podržane su MySQL, SQLite, MariaDB i PostreSQL) i korisnika koji će pristupati samoj bazi, te kreirati novo web sjedište unutar konfiguracije Apache-ja. Odmah ću napomenuti da ownCloud ima (preporučenu) opciju koja forsira sve konekcije preko *https-a,* pa se može iskoristiti suradnja CARNeta i TERENA-e i kreirati odgovarajući certifikat. To će produžiti postupak konfiguracije za nekoliko dana, koliko je potrebno za dobivanje certifikata, ali na ovaj se način dobiva siguran i pouzdan prijenos datoteka preko mreže. Nakon podešavanja Apacha i baze podataka dovoljno je u internetski preglednik ukucati novu adresu i dovršiti instalaciju ownClouda.

Za korištenje LDAP autentikacije potrebno je unutar ownClouda uključiti odgovarajući plugin. LDAP poslužitelj podešen od AAI tima zbog sigurnosnih razloga ima definiranu vrijednost koja anonimnom korisniku ograničava dohvaćanje više od 10 rezultata. Time nije moguće dodati/kreirati više od 10 korisnika unutar ownClouda, barem ne onih koji će se na sustav prijavljivati el. identitetom. Zato treba u LDAP imeniku kreirati novi zapis, tj. dodati novog korisnika koji će imati isključivo prava čitanja, ali će moći dobiti više od 10 rezultata. S tim novim korisnikom ownCloud će se vezati na LDAP imenik i potražiti korisnika. Uz pomoć kolega sa SRCA uspio sam dobiti potrebne *ldif* datoteke kojima sam napravio navedene izmjene. Prva datoteka je *add_user.ldif* koja dodaje novog korisnika, a njen sadržaj je sljedeći:

```
dn: cn=owncloud,dc=ustanova,dc=hr
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
cn: owncloud
sn: owncloud
userPassword: {CRYPT}kriptirana_lozinka
```

Primijetit ćete da novi korisnik nema atribut *objectClass=hrEduPerson* jer ne pripada osobi. Također, nema ni atribut *uid*, čime se tom korisniku onemogućava prijava na AOSI web sučelje. Ovo je

Copyright ©2003.-2017. CARNet. Sva prava pridržana.
Mail to portal-team(at)CARNet.hr

preporučeni [2] način dodavanja zapisa u LDAP imenik za potrebe autentikacije aplikacija. Korisnika dodajemo naredbom:

```
ldapadd -f add_user.ldif -cvx -D cn=admin,dc=ustanova,dc=hr –W
```

Dalje, potrebno je podesiti prava tj. "access listu" za novog korisnika, a ona su navedena u datoteci */etc/ldap/slapd.d/cn\=config/olcDatabase={1}hdb.ldif*. Kako ni ovu datoteku nije preporučljivo mijenjati ručno, poslužit ćemo se naredbom *ldapmodify*. Pri njenom pokretanju pozvat ćemo drugu datoteku, *mod_user.ldif*, čiji je sadržaj sljedeći:

```
changetype: modify
replace: olcLimits
olcLimits: {0}dn.base="cn=hreduadmin,dc=ustanova,dc=hr" size=unlimited
olcLimits: {1}dn.base="cn=owncloud,dc=ustanova,dc=hr" size=unlimited
olcLimits: {2}users size=50
olcLimits: {3}anonymous size=10
```

Postojeće vrijednosti dozvoljavaju autenticiranim korisnicima čitanje potrebnih atributa tako da je jedina izmjena novi podatak pod brojem {1}. Sama naredba kojom mijenjamo prava je:

```
ldapmodify -Y EXTERNAL -H ldapi:/// -f mod_user.ldif
```

Rezultat je poprilično očit, korisnik cn=owncloud,dc=ustanova,dc=hr nema ograničenja broja dobivenih rezultata prilikom pretrage LDAP imenika.

Preostaje podesiti LDAP plugin unutar ownClouda upivanjem podataka o LDAP poslužitelju, podataka korisnika kojim ćemo pretraživati imenik (cn=owncloud,dc=ustanova,dc=hr) te atribut Base DN. Ako pristup aplikaciji želite dodijeliti samo određenim djelatnicima ustanove (primjerice studente izostavljamo), tada svakog korisnika trebate dodati u novu grupu proizvoljnog imena. To se obavlja preko AOSI web sučelja postavljanjem vrijednosti (tj. naziva grupe) na atribut *hrEduPersonGroupMember* za svakog korisnika. A te korisnike ćete u ownCloudu dobiti postavljanjem *raw filtera* na tabu *User Filter*:

```
(&(hrEduPersonAffiliation=djelatnik)(hrEduPersonGroupMember=ime_grupe))
```

Ovako možete podesiti različite filtere, ovisno o potrebama. Od ostalih vrijednosti plugina podesio sam autentikaciju korisnika atributom *hrEdupersonUniqueID* (tab *Login Filter*), a na *Expert* dijelu sam upisao *uid* kao interno korisničko ime. Ovako se korisnička imena unutar ownClouda prikazuju čitljivo.

ownCloud se pokazao kao solidna zamjena za, primjerice, Dropbox ili SkyDrive, s razlikom što su podaci na našem vlastitom poslužitelju. Te podatke svaki korisnik za sebe može posebnim pluginom čak i kriptirati. Još jedna zgodna mogućnost dostupna u ownCloudu jest povezivanje Dropboxa i Google Drive-a, tako da se podaci na tim sustavima prikazuju unutar ownClouda.

Je li to dovoljno da isprobate ownCloud? "Jedino" ulaganje su diskovi i malo sistemčeva vremena.

uto, 2014-03-25 22:44 - Mirko Lovričević**Kuharice:** Linux [3]
Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

Copyright ©2003.-2017. CARNet. Sva prava pridržana.
Mail to portal-team(at)CARNet.hr

Source URL: https://sysportal.carnet.hr/node/1372

Links
[1] http://owncloud.org
[2] http://developer.aaiedu.hr/faq/16.html
[3] https://sysportal.carnet.hr/taxonomy/term/17

Copyright ©2003.-2017. CARNet. Sva prava pridržana.
Mail to portal-team(at)CARNet.hr