Moodle i AAI@EduHr na siguran način

Mnoge visokoškolske ustanove koriste Moodle sustav kao ispomoć pri održavanju nastave. Na mojoj ustanovi Moodle se koristi 4 godine, a od samog početka implementirali smo prijavu na sustav pomoću podataka elektroničkog identiteta zajedno sa sigurnim prijenosom korisničkih podataka preko mreže.

Iako je dostupan Single-Sign-On plugin za Moodle (http://developer.aaiedu.hr/faq/12.html [1]), odabrali smo LDAP plugin koji je došao sa sustavom. Razlog je sljedeći: SSO plugin je predviđen za prijavu korisnika koji nisu iz vaše ustanove (imaju različiti *realm*), a kako naš sustav ne koriste osobe izvan ustanove, SSO plugin stvarno nije potreban.

Konfiguracija LDAP plugina se nalazi unutar S*ite administration -> Plugins -> Authentication -> LDAP server*, a potrebno je pripaziti na sljedeća polja (vrijedi za Moodle v2.2):

LDAP server settings
Host URL: *FQDN* ili *IP adresa* poslužitelja na kojem se nalazi LDAP imenik
Version: *3*
LDAP encoding: *utf-8*
Bind settings
Hide passwords: *Yes*
User lookup settings
Contexts: *dc=domena,dc=hr*
Search subcontexts: *Yes* - ako su korisnici razdijeljeni prema organizacijskim jedinicama (LDAP atribut *ou*)
User attribute: *hrEduPersonUniqueID*
LDAP password expiration settings - ove postavke trenutno rade samo sa Novellovim eDirectory serverom i MS-AD-om
Expiration: *No*
Cron synchronization script
Removed ext user: *Suspend internal*
Data mapping
First name: *givenName*
Surname: *sn*
Email address: *mail*

Ovime je Moodle spreman za prijavu korisnika s podacima elektroničkog identiteta. Prilikom prve prijave korisnika Moodle će kreirati interni korisnički račun, ali će svaka daljnja prijava biti moguća isključivo na taj isti način.
Preostalo je konfigurirati Apache da koristi ssl, što je već opisano u ovom članku [2].

Odlučio sam cijeli Moodle sustav prebaciti isključivo na *https*, ne samo prijavu, radi jednostavnije konfiguracije. Članci na Internetu govore da se time dobije pad performansi za 5 do 15%, što mi se ne čini pretjerano za današnje poslužitelje. Unutar Apache-ja trebalo je podesiti preusmjeravanje sa *http://moodle.ustanova.hr* na *https://moodle.ustanova.hr*. U konfiguracijskoj datoteci dotičnog web poslužitelja – nazovimo je *moodle.ustanova.hr*, a koja se nalazi unutar */etc/apache2/sites-available*, na početku direktive *<VirtualHost *:80>* treba dodati dva retka:

```
RewriteEngine on
RewriteRule ^(.*)$ https://moodle.ustanova.hr$1 [R,L]
```


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

Time je preusmjeravanje gotovo. Primijetite da je izostao restart Apache servisa - to ćemo napravit tek na kraju.

Slijedi podešavanje konfiguracije php-a unutar Moodlea. Naime, prilikom instalacije *https* nije bio konfiguriran, pa varijabla *wwwroot*, koja određuje putanju do sustava, ima vrijednost koja počinje s *http://* i nju treba pormijeniti u *https://*. Ta se varijabla nalazi u datoteci *config.php* u *root* direktoriju sustava Moodle.

Zadnji korak je uključivanje opcije "*HTTPS for logins*" unutar sustava Moodle (*Site administration -> Security -> HTTP security*) te opcije "*Secure cookies only*" (na istom mjestu). Ovim smo dovršili konfiguraciju i možemo napraviti restart Apache servisa.

Moram upozoriti da se, ako *https* nije ispravno konfiguriran, nećete moći prijaviti na sustav, čak ni kao administrator. Srećom, i tome ima lijeka. Uz brisanje redirekcije na *https* (ili, jednostavnije, komentiranjem tih linija), potrebno je na neki način pristupiti bazi podataka sustava Moodle (komandnom linijom ili nekim GUI sustavom), pronaći tablicu *mdl_config* te u njoj promijeniti sljedeće vrijednosti atributa:
- *loginhttps* iz 1 u 0
- *cookiesecure* iz 1 u 0

Jedina mana LDAP plugina jest ta što se pri prijavi na sustav provjeravaju samo korisničko ime i lozinka, a izostaje provjera ostalih atributa poput datuma isteka el. identiteta (*hrEduPersonExpireDate*) ili temeljna povezanost s ustanovom (*hrEduPersonPrimaryAffiliation*). Međutim, postoji skripta */putanja/do/moodlea/auth/ldap/cli/sync_users.php* koja radi sinhronizaciju korisnika LDAP-a i internih Moodle korisničkih računa. Pokretanjem ove skripte (ručno ili iz *crona*) iz Moodle sustava će biti obrisani ili zaključani svi korisnici koji više ne postoje u našem LDAP imeniku. Sama radnja ovisi o gore spomenutoj postavci *Removed ext user* pa je, ukoliko se odabere opcija *Full delete internal,* treba koristiti s oprezom.

pet, 2013-02-01 23:07 - Mirko Lovričević**Kuharice:** Linux [3]
Kategorije: Servisi [4]
Vote: 4.75

Vaša ocjena: Nema Average: 4.8 (4 votes)

Source URL: https://sysportal.carnet.hr/node/1196?page=0

Links
[1] http://developer.aaiedu.hr/faq/12.html
[2] https://sysportal.carnet.hr/node/315
[3] https://sysportal.carnet.hr/taxonomy/term/17
[4] https://sysportal.carnet.hr/taxonomy/term/28

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