

Apache2: autentikacija korisnika rabeći samo LDAP



U člancima <http://sistemac.carnet.hr/node/42> [1] (Autentikacija osnovnih servisa putem LDAP-a i RADIUS-a) i <http://sistemac.carnet.hr/node/41> [2] (Autorizacija Apache web poslužitelja putem LDAP-a i RADIUS-a) smo objasnili kako autentificirati mrežne servise, s naglaskom na RADIUS. No, njegova uporaba nije nužna jer se sve može napraviti direktno preko LDAP-a.

Prvo, trebate osigurati da su učitani odgovarajući moduli, **mod_auth_basic** i **mod_authnz_ldap**. Možda ste primjetili da se modul ne zove `mod_auth_ldap`, nego `mod_authnz_ldap`. Ova se promjena dogodila od inačice 2.1, jer su neki moduli podijeljeni na autentikacijske ("n") i autorizacijske ("z"). Kako LDAP modul nosi obje oznake, znači da obavlja obje funkcije, što je svojevrsan povratak na staro. No, nećemo razbijati glavu s tim, nego idemo dalje.

Obično su svi potrebni moduli već učitani, ali ukoliko nisu, poslužite se naredbom **a2enmod**:

```
# a2enmod authnz_ldap
Module authnz_ldap installed; run /etc/init.d/apache2 force-reload to enable.
```

Nakon što ste poslušali savjet i restartali Apache na način koji se preporuča u poruci, možete dalje pristupiti konfiguraciji. Ona je zapravo vrlo jednostavna, sve što trebate učiniti je kreirati datoteku **.htaccess** koju ćete staviti u **direktorij koji želite zaštititi**. Ona ima ovakav sadržaj:

```
AuthType basic
AuthName "Molimo unesite LDAP zaporku"
AuthBasicProvider ldap
AuthLDAPURL ldap://ldap.domena.hr/dc=domena,dc=hr?hrEduPersonUniqueID
AuthLDAPRemoteUserIsDN off
require ldap-filter &(hrEduPersonUniqueID=*)
```

Što govore ove direktive? Situacija je prilično jasna, ove direktive određuju da će se rabiti osnovna ("basic") autentikacija (dakle, preko osnovnog HTTP Basic mehanizma), te određuju LDAP poslužitelj koji će se rabiti. Najzanimljiviji je parametar **ldap-filter**. On određuje koji će se atribut iz LDAP-a provjeravati, a u ovom slučaju je **hrEduPersonUniqueID** upravo ono što nam treba, a to je AAI@EduHr korisnička oznaka.

Naravno, mogli ste staviti i samo "uid" umjesto "hrEduPersonUniqueID", što je skraćena inačica (umjesto "korisnik@domena.hr" pisat ćete samo "korisnik" u formu za prijavu).

Ovo može zbuniti korisnike, pa je možda bolje da ostavite "hrEduPersonUniqueID". Ne zaboravite isti atribut postaviti i u direktivi `AuthLDAPURL`. U ovom trenutku nećemo ulaziti u sve mogućnosti ovog modula, a za više informacija provjerite dokumentaciju na adresi:

http://httpd.apache.org/docs/2.2/mod/mod_authnz_ldap.html

- [Logirajte](#) [3] se za dodavanje komentara

čet, 2009-06-18 08:28 - Željko BorošKuharice: [Linux](#) [4]

Kategorije: [Servisi](#) [5]

Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

Source URL: <https://sysportal.carnet.hr/node/600>

Links

[1] <https://sysportal.carnet.hr/node/42>

[2] <https://sysportal.carnet.hr/node/41>

[3] <https://sysportal.carnet.hr/sysportallogin>

[4] <https://sysportal.carnet.hr/taxonomy/term/17>

[5] <https://sysportal.carnet.hr/taxonomy/term/28>