Šta je LDAP direktorijum

LDAP (*Lightweight Directory Access Protocol*) direktorijum predstavlja standard za ?uvanje podataka o identitetima korisnika i njihovu autentifikaciju. Direktorijumi su hijerarhijske baze podataka i sa stanivišta fleksibilnosti i jednostavnosti za ove svrhe imaju brojne prednosti u odnosu na tradicinalne relacione baze. Tako?e veliki broj gotovih softverskih rešenja ima ugra?enu podršku za autentifikaciju i ?itanje podataka o korisnicima iz LDAPa (npr. dokuWiki na ?ijim stranicama se upravo nalazite :), freeRadius itd.).

OpenLDAP je besplatna, *open source* implementacija LDAP protokola, objavljena pod OpenLDAP *Public Licence* licencom.

Instalacija OpenLDAP direktorijuma

Uputstvo za instalaciju OpenLDAP softvera možete pogledati na http://www.eduroam.amres.ac.rs/rs/institucije-uputstva.html, u okviru uputstva za instalaciju FreeRADIUS softvera.

Konfigurisanje OpenLDAP direktorijuma

Nakon instalacije OpenLDAP softvera potrebno je izvršiti inicijalnu konfiguraciju u okviru ***../openldap/slapd.conf*** konfiguracionog fajla. Primer konfiguracionog fajla, sa objašnjenjima razli?itih opcija možete preuzeti primer.slapd.rar.

U datom primeru koristi se rsEdu, eduPerson, eduOrg, eduMember i schac šeme, te ih je prethodno neophodno kopirati na server. Linkove za njihovo preuzimanje pogledajte na stranici https://bpd.amres.ac.rs/doku.php?id=amres_aai_wiki:rsedu_sema.

Osim osnovnih podešavanja, u ***slapd.conf*** fajlu mogu se konfigurisati liste za kontrolu pristupa *Access Control List* ACL kojima se definišu privilegije razli?itih korisnika nad LDAP direktorijumom. ACL konfiguracija je jako mo?na ali zahteva razumevanje. Uputstvo za konfiguraciju osnovnih ACL preuzmite ovde Upustvo za konfiguraciju ACL.

Unos inicijalnog LDAP stabla

Kada je OpenLDAP instaliran i servis pokrenut, pre unošenja korisni?kih identiteta neophodno je

napraviti incijalno LDAP stablo. Postoje razli?ita mogu?a rešenja za dizajn LDAP stabla. Naša preporuka je da se koristi takozvano “flat” ldap stablo u kome se korisni?ki nalozi nalaze u jednoj grani.

AMRES tim je spremio skriptu kojom se može generisati ldif stablo za vašu instituciju. Potrebno je da preuzmete:

- skriptu za generisanje .ldif fajla napravildif.rar
- po?etno .ldif stablo original.rar

Po preuzimanju, ova dva fajla otpakujte i smestite na proizvoljnu lokaciju na serveru gde je instaliran LDAP direktorijum. Skriptu napraviLdif.sh pokrenite komandom:

./napraviLdif.sh

Napomena: napravildif.sh mora imati dovoljne privilegije tako da je dozvoljeno pokretanje ovog fajla. Ukoliko to nije slu?aj, privilegije možete promeniti komandom:

chmod o+x napraviLdif.sh

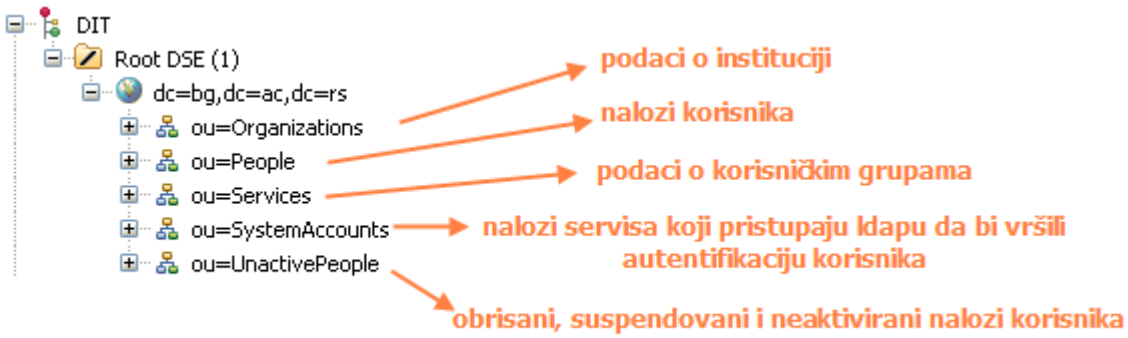
Po pokretanju skripte, na komandnoj liniji ?ete uneti potrebne informacije za generisanje .ldif stabla. Kada unesete sve potrebne informacije, generisa?e se fajl novo.ldif, koji predstavlja inicijalno ldap stablo.

Preostalo je još da ovo stablo uvezete u vaš direktorijum što možete uraditi pokretanjem komande:

ldapadd -f novo.ldif -D *korisnicko-ime* -w *lozinka*

gde su ***korisnicko-ime*** i ***lozinka*** parametri ldap administratorskog naloga koji ste uneli u slapd.conf.

Po uvozu stabla, vaš LDAP direktorijum ?e izgledati okvirno ovako:



Pristup LDAP direktorijumu

Podacima u LDAP direktorijumu možete pristupiti na nekoliko na?ina:

1. Iz komandne linije, koriš?enjem OpenLDAP komandi:

- ***ldapsearch*** - prikaz podataka
- ***ldapadd*** - dodavanje podataka
- ***ldapmodify*** - dodavanje i menjanje podataka
- ***ldapdelete*** - brisanje podataka

Uputstva za koriš?enje ovih komandi možete pogledati na http://www.zytrax.com/books/ldap/ch14/#openldap.

2. Koriš?enjem nekog LDAP *browser* softvera poput *Apache Directory Studio*, koji možete preuzeti na http://directory.apache.org/studio/.

3. Koriš?enjem aplikacije za administriranje LDAPa koju je spremio AMRES/RCUB tim. Uputstva za preuzimanje i instalaciju aplikacije pogledajte na stranici.

Naša preporuka je da za pregled, unos i brisanje korisni?kih identiteta koristite AMRES/RCUB aplikaciju za administriranje LDAPa obzirom da je jednostavna za koriš?enje i ne zahteva poznavanje LDAP direktorijuma. Ukoliko ste glavni administrator LDAP direktorijuma, savetujemo da tako?e korisitite i *Apache Directory Studio* koji omogu?ava kompletan uvid u podatke u LDAP direktorijumu i manipulaciju sa njima.

Unos ve? postoje?ih naloga u LDAP direktorijum

AMRES/RCUB tim je obezbedio alat kojim u LDAP direktorijum možete pebaciti ve? postoje?e naloge korisnika iz neke druge baze.

1. Priprema CSV fajla za uvoz

Potrebno je da pripremite fajl sa nalozima korisnika koje želite da uvezete u LDAP direktorijum. Fajl treba da bude u CSV formatu (*Comma Separated Values*), tako da su:

- u prvom redu kompletan naziv institucije (opciono) i domen institucije razdvojeni zarezima. Ukoliko ne navedete naziv institucije, onda se u osobi mora nalaziti atribut o.

- u drugom redu nazivi atributa podataka koje želite da uvezete (po rsEdu šemi) razdvojeni zarezima
- svaki naredni red predstavlja jednu osobu sa odgovaraju?im vrednostima atributa tako?e razdvojeni zarezima

Naziv CSV fajla treba da bude: **original.csv**

Primer jednog fajla bi bio:

Ra?unarski Centar Univerziteta u Beogradu, rcub.bg.ac.rs
sn, givenName, mail, uid, userPassword, rsEduPersonUniqueNumber, rsEduPersonAffiliation
Markovic, Ivan, ivanm@gmail.com, ivke, cve33!tic, 1244145124514, zaposleni

– **navo?enje lozinki** –

Lozinke mogu biti u *cleartext-u, hash-irane* ili *crypt-ovane*.

Ukoliko lozinka ostane u *cleartext* formatu, bi?e kreiran ldif fajl za *hash-iranom* lozinkom pomo?u SHA algoritma. CSV fajl pri tome treba da izgleda kao na prethodnom primeru.

Ukoliko želite da uvezete lozinke koje su *hash-irane* MD5, SHA ili NT *hash-om*, potrebno je da ispred naziva atributa *userPassword*, u prvoj koloni, u viti?astim zagradama navedete naziv hash-a koji je koriš?en za hash-iranje lozinki, npr. za SHA **{SHA}userPassword**. Ukoliko je lozinka *crypt-ovana* potrebno je na isti na?in navesti **{CRYPT}userPassword**. Za vrednost lozinke je potrebno staviti hash-iranu odnosno *crypt-ovanu* vrednost, npr:

*sn, givenName, mail, uid, **{SHA}userPassword**, rsEduPersonUniqueNumber, rsEduPersonAffiliation*
*Markovic, Ivan, ivanm@gmail.com, ivke, **a655ad068ba9eb1fdb57bcc5a898d18775163178**, 1244145124, zaposleni*

– **minimalan set atributa** –

U prethodnim primerima je ujedno naveden i minimalni set atributa koji mora postojati za svakog korisnika. Ukoliko nisu navedeni,na osnovu postoje?ih vrednosti, bi?e kreirani i slede?i atributi:

- *o* - preuzimanjem imena institucije navedenog u prvom redu csv fajla
- *cn* - spajanjem vrednosti *givenName* i *sn* atributa navedenim u osobi
- *eduPersonPrincipalName* - spajanjem *uid* atributa navedenog u osobi i domena institucije navedenog u prvom redu csv fajla
- *rsEduPersonScopedAffiliation* - spajanjem *rsEduPersonAffiliation* atributa navedenog u osobi i domena institucije navedenog u prvom redu csv fajla

Ukoliko odre?eni korisnik nema neki od atributa, za taj atribut treba ostaviti prazno polje, tj. dva

zareza jedan do drugog.

– **višestruki atributi** –

Ukoliko odre?eni korisnik ima više vrednosti za jedan atribut naziv tog atributa se pojavljuje više puta u drugom redu, npr:

Ra?unarski Centar Univerziteta u Beogradu,rcub.bg.ac.rs
sn, givenName, mail, mail, uid, userPassword, rsEduPersonUniqueNumber, rsEduPersonAffiliation
Markovic, Ivan, ivanm@gmail.com, ivanm@yahoo.com, ivke, cve33!t, 1244145124, zaposleni
Petrovic, Marko, p.marko@gmail.com,,markop, lap22top@, 2245825014203, student

2. Kreiranje ldif fajla

Ukoliko imate podatke o korisnicima smeštene u neki .csv fajl, imate dostupnu aplikaciju pomo?u koje te podatke možete prebaciti u LDAP direktorijum.

Po preuzimanju, fajl otpakujte i smestite na proizvoljnu lokaciju na serveru gde je instaliran LDAP direktorijum. Na istoj lokaciji treba da se nalazi i CSV fajl koji ste prethodno pripremili. Neophodno je da je na serveru instalirana Java.

Program pokrenite komandom:

java -jar csvparser-2.0.0.jar

Nakon izvršavanja kreira?e se slede?i faljovi:

- ***users.ldif*** - idenititeti osoba ispravno konvertovani u ldif fajl
- ***inactive.ldif*** - identiteti osoba koji nemaju mail adresu. Ovi identiteti su odvojeni u poseban fajl jer se ovaj atribut zahteva za optimalno koriš?enje ldap korisni?ke aplikacije. Ovi identiteti su u inactive.ldif fajlu pripremljeni tako da se uvoz radi u UnactivePeople granu, sa idejom da se posle dodavanja email adrese korisnika koriš?enjem administratorske ldap aplikacije identitet može aktivirati i prebaciti u People granu. Ukoliko ne želite da koristite AMRES/RCUB ldap aplikaciju i želite da identitete bez mailova uvezete kao aktivne u People granu, pre uvoza inactive.ldif fajla u ldap string “ou=UnactivePeople” zameniti sa stringom “ou=People” što možete jednostavno uraditi u bilo kom tekstualnom editoru.
- ***error.log*** - sadrži spisak osoba ?iji identiteti nisu kreirani zato što ne postoje svi obavezne atributi, kao i listu atributa koji nedostaju

Nakon ovoga, dobijeni ldif fajl možete uvesti u LDAP direktorijum pokretanjem komande:

ldapadd -f users.ldif -D *korisnicko-ime* -w *lozinka*

gde su ***korisnicko-ime*** i ***lozinka*** parametri ldap administratorskog naloga koji ste uneli u slapd.conf.

Važno: neki od ldap browsera poput Apache Directory Studio nepravilno unose specijalna slova srpskog alfabeta, pa je neophodno uvoz uraditi iz komandne linije na na?in opisan iznad

From:
http://www.bpd.amres.ac.rs/ - **AMRES wiki**

Permanent link:
http://www.bpd.amres.ac.rs/doku.php?id=amres_aai_wiki:ldap_direktorijum

Last update: **2013/10/29 11:43**