AMPEC
Академска мрежа Србије

LDAP директоријум

Историја верзија документа

Верзија	Датум	Иницијали аутора	Опис промене
1.0			Прва верзија овог документа

Садржај

LDAP директоријум

1 LDAP директоријум

LDAP (Lightweight Directory Access Protocol) директоријум представља стандард за чување података о идентитетима корисника и аутентификацију. Директоријуми су хијерархијске базе података и са становишта флексибилности и једноставности за ове сврхе имају бројне погодности у односу на традиционалне релационе базе. Такође, велики број софтверских решења има уграђену подршку за аутентификацију и читање података о корисницима из LDAP-а.

OpenLDAP је бесплатна имплементација LDAP протокола са отвореним кодом, објављена под *OpenLDAP Public Licence* лиценцом.

2 Инсталација LDAP директоријма

Упутство за инсталацију OpenLDAP софтвера можете погледати на званичним страницама AMPEC eduroam услуге, у оквиру упутства за инсталацију FreeRADIUS софтвера.

3 Конфигурисање OpenLDAP директоријума

Након инсталације OpenLDAP софтвера, потребно је извршити иницијалну конфигурацију у оквиру `/usr/local/etc/openldap/slapd.conf` конфигурационог фајла. Пример конфигурационог фајла, са објашњењима различитих опција можете преузети са AMPEC веб странице [1].

У датом примеру се користе *rsEdu*, *eduPerson*, *eduOrg*, *eduMember* и *schac* шеме, те их је потербно претходно копирати на сервер. Линкове за њихово преузимање погледајте у документу rsEdu шема на страници Даваоци идентитета на AMPEC веб-сајту [2].

Осим основних подешавања, у `slapd.conf` фајлу се могу конфигурисати и листе за контролу приступа (Access Control List - ACL), којима се дефинишу привилегије различитих корисника над LDAP директоријумом. Конфигурисањем ACL можете постићи много, али ове листе захтевају основни ниво разумевања. Да бисте лакше разумели како ACL функционишу, наша препорука је да прочитате упутство за конфигурисање основних ACL [3].

4 Унос почетног LDAP стабла

Када је OpenLDAP инсталиран и сервис покренут, пре уношења корисничких идентитета неопходно је направити иницијално LDAP стабло. Постоје различита могућа решења за дизајн LDAP стабла. Препорука AMPEC-а је да се користи тзв. „flat" LDAP стабло у коме се кориснички налози смештају у једну грану.

Да бисте једноставно генерисали почетно *ldif* стабло за вашу институцију, потребно је да преузмете:

- скрипту за генерисање *ldif* фајла, napraviLdif.zip [4]
- почетно *ldif* стабло, original.zip [5]

По преузимању, ова два фајла је потребно отпаковати и сместити у директоријум на серверу где је инсталиран LDAP директоријум (нпр. `/usr/local/etc/openldap/`). Скрипта се покреће командом:

```
./napraviLdif.sh
```

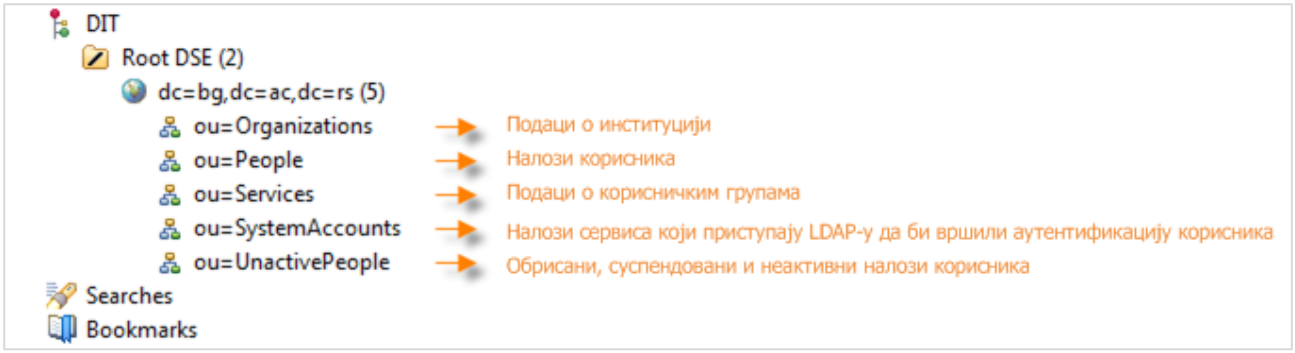
Напомена: Да би се скрипта за креирање почетног *ldif* фајла покренула, мора имати правилно подешене пермисије, односно скрипта мора имати могућност извршавања. Уколико то није случај, пермисије се могу променити следећом командом:

```
chmod o+x napraviLdif.sh
```

По успешном покретању скрипте, у комадној линији је потребно одговорити на сва питања. На овај начин се омогућава креирање почетног *ldif* стабла. Резултат извршавања скрипте је фајл `novo.ldif`, који представља иницијално стабло. Потребно је да ово стабло увезете у ваш директоријум командом:

```
ldapadd -f novo.ldif -D rootdn -w rootpw
```

где "`rootdn`" представља администраторски налог који сте дефинисали у `slapd.conf` конфигурационом фајлу. Параметар "`rootpw`" је одговарајућа лозинка за "`rootdn`" налог. Након што се почетно стабло успешно увезе, LDAP директоријум за вашу институцију би требало да изгледа као на слици испод.



Слика 1. Изглед почетног LDAP стабла

5 Приступ LDAP директоријуму

Подацима који се налазе у LDAP директоријуму се може приступати на неколико начина:

1. Из командне линије, коришћењем предефинисаних команди:
   - `ldapsearch` - приказ података,
   - `ldapadd` - додавање података,
   - `ldapmodify` - додавање и мењање података,
   - `ldapdelete` - брисање података.

   Упутства за коришћење ових команди можете погледати у онлајн књизи за коришћење OpenLDAP софтвера [6].
2. Коришћењем LDAP *browser* софтвера, као што је нпр. *Apache Directory Studio* [7].

Уколико сте главни администратор LDAP директоријума, препорука је да користите и *Apache Directory Studio*. Овај LDAP *browser* омогућава увид у податке из LDAP директоријума и манипулацију њима.

6 Унос постојећих налога у LDAP директоријум

AMPEC/РЦУБ тим је обезбедио алат којим се у LDAP директоријум могу пребацити постојећи налози из неке друге базе.

Постоје две фазе у пребацивању налога:

1. Припрема CSV фајла за увоз у LDAP директоријум

Потребно је да припремите фајл са налозима корисника који желите да увезете у LDAP директоријум. Фајл мора бити у CSV (Comma Separated Values) формату, тако да:

- у првом реду буде комплетан назив институције и домен институције, раздвојени зарезима. Уколико не наведете назив институције, онда се за сваки кориснички налог мора додати атрибут "o".
- у другом реду буду називи атрибута за податке које желите да увезете (према rsEdu шеми), раздвојени зарезима.
- сваки наредни ред представља једну особу са одговарајућим вредностима атрибута, раздвојених зарезима.

Назив CSV фајла мора бити **original.csv**. Пример једног фајла који је спреман за увоз у LDAP директоријум можете преузети са AMPEC веб-страница [8].

2. Навођење лозинки

Приликом увоза лозинки, прихватљиви формати су: *cleartext*, *hash* и *crypt*. Уколико се у CSV фајлу налазе лозинке у cleartext формату, биће креиран *ldif* фајл у коме ће та иста лозинка бити *hash*-ована *SHA1* алгоритмом. У случају да лозинка треба да задржи свој формат (*MD5*, *SHA* или *NT*), потребно је да испред назива атрибута *userPassword*, у другом реду, у витичастим заградама наведете назив *hash* алгоритма који се користи. Ако се користи нпр. *SHA* алгоритам, онда је потребно урадити следеће: *{SHA}userPassword*. Исти принцип важи и за остале типове *hash* алгоритама који су прихватљиви. Пример CSV фајла који користи *hash*-ован вредности за лозинке можете преузети са AMPEC веб-страница [9].

3. Минималан скуп атрибута

У претходним примерима је уједно наведен и минималан скуп атрибута који мора постојати за сваког корисника. Уколико нису наведени, или не постоје у башој бази, на основу вредности из CSV фајла биће креирани и следећи атрибути:

- **o** - на основу имена институције из првог реда,
- **cn** - спајањем вредности *givenName* и *sn* атрибута који су наведени за корисника,
- **eduPersonPrincipalName** - спајањем *uid* атрибута који је наведен за корисника и домена институције наведеног у првом реду, формат је *uid@domen*,
- **rsEduPersonScopedAffiliation** - спајањем *rsEduAffiliation* атрибута наведеног за корисника и домена институције наведеног у првом реду.

Уколико за неког корисника не постоји вредност одређеног атрибута, оставља се празно поље, тј. два зареза један до другог.

4. Вишеструки атрибути

У случају да неки корисник има више од једне вредности за исти атрибут, потребно је да се назив тог атрибута појављује онолики број пута у првом реду колико вредности има. Пример оваквог CSV фајла можете преузети са AMPEC веб-страница [10].

7 Креирање ldif фајла

Уколико су подаци о корисницима смештени у CSV фајл, AMPEC/РЦУБ је развио апликацију помоћу које можете те податке пребацити у *ldif* формат. Апликацију можете преузети преузети са AMPEC веб-страница [11]. По преузимању, фајл је потребно отпаковати и сместити у исти директоријум где је инсталиран LDAP директоријум. CSV фајл се мора налазити на истој локацији. На серверу мора бити инсталирана Java. Програм се покреће командом:

```
java -jar csvparser-2.0.0.jar
```

Уколико је обрада CSV фајла успешно завршена, у посматраном директоријуму се налазе следећи фајлови:

- *users.ldif* - садржи идентитете корисника за које су налози успешно креирани.
- *inactive.ldif* - садржи идентитете корисника који немају мејл адресу. Ови идентитети су одвојени у посебан фајл јер овај атрибут омогућава оптимално коришћење LDAP апликације за кориснике. Ови идентитети су тако креирани да се омогућава увоз кроз UnactivePeople грану. После додавања мејл адресе за корисника, уз помоћ LDAP администраторске апликације, идентитет се може активирати и пребацити у People грану. Уколико користите Apache Directory Studio, идентитети се могу увести као активни у People грану. Пре увоза корисника из овог фајла, потребно је само стринг "ou=UnactivePeople" заменити стрингом "ou=People".
- *error.log* - садржи списак особа чији идентитети нису креирани зато што не постоје сви обавезни атрибути. Такође садржи и списак атрибута који недостају.

Добијени ldif фајл можете увести у LDAP директоријум покретањем команде:

```
ldapadd -f novo.ldif -D rootdn -w rootpw
```

где "rootdn" представља администраторски налог који сте дефинисали у slapd.conf конфигурационом фајлу. Параметар "rootpw" је одговарајућа лозинка за тај налог.

Напомена: Apache Directory Studio неправилно уноси специјална слова српског алфабета, па је неопходно увоз урадити из командне линије, као што је описано изнад.

Референце

[1] http://www.amres.ac.rs/dokumenti/institucije/iamres-federacija-identiteta/davaoci-identiteta/primer.zip

[2] http://www.amres.ac.rs/institucije/iamres-federacija-identiteta/davaoci-identiteta

[3] http://www.amres.ac.rs/dokumenti/institucije/iamres-federacija-identiteta/davaoci-identiteta/konfiguracija_acl_openldap.pdf

[4] http://www.amres.ac.rs/dokumenti/institucije/iamres-federacija-identiteta/davaoci-identiteta/napraviLdif.zip

[5] http://www.amres.ac.rs/dokumenti/institucije/iamres-federacija-identiteta/davaoci-identiteta/original.zip

[6] http://www.zytrax.com/books/ldap/ch14/#openldap

[7] http://directory.apache.org/studio/

[8] http://www.amres.ac.rs/dokumenti/institucije/iamres-federacija-identiteta/davaoci-identiteta/original.csv

[9] http://www.amres.ac.rs/dokumenti/institucije/iamres-federacija-identiteta/davaoci-identiteta/original1.csv

[10] http://www.amres.ac.rs/dokumenti/institucije/iamres-federacija-identiteta/davaoci-identiteta/original2.csv

[11] http://www.amres.ac.rs/dokumenti/institucije/iamres-federacija-identiteta/davaoci-identiteta/csvparser-2.0.0.jar