LDAP

sistemsko i administrativno održavanje

Dubravko Penezić, Srce
Dubravko.Penezic@Srce.hr

Sadržaj

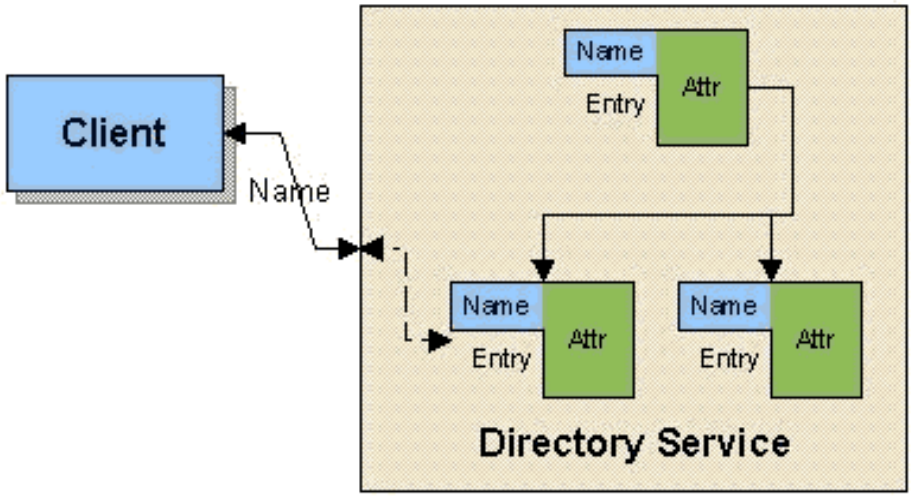
- Osnove LDAP-a
- OpenLdap i preporučene postavke
- Sistemske postavke
- Sistemsko održavanje LDAP imenika
- Administrativno održavanje LDAP imenika
- LDAP u aplikacijama (AAI)

Osnove LDAP-a

- Imenički servisi
- LDAP
- Programska riješenja po LDAP-u
  - Netscape LDAP (Sun one)
  - OpenLDAP
  - NovelNetware
  - Microsoft AD

Imenički servisi

- način distribucije, održavanja i pohranjivanja djeljenih informacija
- osnovna jedinica informacije je entry
- entry se sastoji od jednog ili više atributa
- svaki entry ima svoju jedinstvenu oznaku (DN)



LDAP

- **L**ightweight **D**irectory **A**ccess **P**rotocol
- pojednostavljeni X.500 protokol
- standard za imeničke servise
- verzija v2 i v3
- uz osnovne funkcionalnosti imeničkgo servisa dodane su neke druge (strukturno pretraživanje, sigurnost, PKI)
- http://www.comptechdoc.org/independent/directory/begin/dirldap.html

LDAP schema

- popis tipova varijabli
- opis atributa
- OID – jedinstveni broj za sve objekte u schemi
- nasljedna svojstva
- atributi mogu biti MAY i MUST
- s pojedinačnom ili višestrukom vrijednošću

LDAP - RFC

- RFC1777 - Lightweight Directory Access Protocol. (Obsoletes RFC1487)
- RFC1778 - The String Representation of Standard Attribute Syntaxes
- RFC1779 - A String Representation of Distinguished Names.(Obsoletes RFC1485)
- RFC1823 - The LDAP Application Program Interface
- RFC1960 - A String Representation of LDAP Search Filters (Obsoletes RFC1558)
- RFC 2251 - Lightweight Directory Access Protocol (v3)
- RFC 2252 - LDAPv3 Attribute Syntax Definitions
- RFC 2253 - UTF-8 String Representation of Distinguished Names
- RFC 2254 - The String Representation of LDAP Search Filters
- RFC 2255 - The LDAP URL Format
- RFC 2256 - A Summary of the X.500(96) User Schema for use with LDAPv3
- RFC 2829 - Authentication Methods for LDAP.
- RFC 2830 - Lightweight Directory Access Protocol (v3): Extension for Transport Layer Security.

LDAP – dodatni RFC

- RFC1274 - The COSINE and Internet X.500 Schema
- RFC1279 - X.500 and Domains
- RFC1308 - Executive Introduction to Directory Services Using the X.500 Protocol
- RFC1309 - Technical Overview of Directory Services Using the X.500 Protocol
- RFC1617 - Naming and Structuring Guidelines for X.500 Directory Pilots (Obsoletes RFC1384)
- RFC1684 - Introduction to White Pages services based on X.500
- RFC2079 - Definition of an X.500 Attribute Type and an Object Class to Hold Uniform Resource Identifiers (URIs)

Programska rješenja

- Sun[tm] ONE Directory Server 5.2
- http://docs.sun.com/db/coll/S1_DirectoryServer_52
- Komercijalna verzija, izuzetak visokoobrazovne institucije

Programska rješenja

- OpenLDAP
- http://www.openldap.org
- Verzija 2.2.14
- Open Source

  *"OpenLDAP Software is an open source implementation of the **L**ightweight **D**irectory **A**ccess **P**rotocol. "*

Programska rješenja

- Novell eDirectory
- http://www.novell.com/products/edirectory/
- Komercijalno riješenje, jedan od najvećih donatora Open Source podrške za LDAP imenike

Programska rješenja

- Microsoft Active Directory
- http://www.microsoft.com/windowsserver2003/technologies/directory/activedirectory/default.mspx
- Sastavni autentikacijski dio MS Windows Server aplikacije

OpenLdap i preporučene postavke

- BDB
- slapd.conf
- schema
- password
- Dostupnost informacija
  - Annonymous
  - User
  - Administrator

Instaliranje

- CARNet paketi (apt-get install)
  - Debian *openldap-cn*
  - Sparc *openldap*
- Source
  http://www.openldap.org/software/download/

BDB

- Berkeley DB
- Sleepycat Software
  http://www.sleepycat.com/products/db.shtml
- DB engine, koristi ga većina Open Source programa
- malen i brzi kod za rad s bazama podataka
- transakcijski model

slapd.conf

- konfiguracijask datoteka
- http://www.openldap.org/software/man.cgi?query=slapd.conf&section=5&apropos=0&manpath=OpenLDAP+2.2-Release
- opći dio, dio o DB-u, te dio o pristupu podacima
- dozvole na datoteci **600**
- čuvati sigurnosnu kopiju

slapd.conf – opći dio

```
include         /etc/ldap/schema/core.schema
include         /etc/ldap/schema/cosine.schema
include         /etc/ldap/schema/nis.schema
include         /etc/ldap/schema/inetorgperson.schema
include         /etc/ldap/schema/carnetperson.schema
include         /etc/ldap/schema/carnetcmuperson.schema

allow bind_v2

modulepath      /usr/lib/ldap
moduleload      back_bdb
```

slapd.conf – DB dio

```
database        bdb

suffix          "dc=domena,dc=hr"

directory       "/var/lib/ldap“

rootdn  "cn=admin,dc=domena,dc=hr"
rootpw  1Astr0z

index           objectClass eq
index   cn              eq,sub
index   sn              eq,sub
index   mail             eq,sub
index   uid             eq,sub
index   CARNetuniqueName        eq,sub
index   CARNetuniqueID          eq,sub
```

slapd.conf – pristup podacima

```
access to dn.subtree="dc=srce,dc=hr"
attr=CARNetPersonID,CARNetuserGroup,CMUquotaType,
CMUauthMetod,CMUexpireDate
  by dn="cn=cmuadmin,dc=srce,dc=hr" read
  by self read
  by anonymous auth

access to dn.subtree="dc=srce,dc=hr" attr=userPassword
  by dn="cn=cmuadmin,dc=srce,dc=hr" read
  by self write
  by anonymous auth

access to dn.subtree="dc=srce,dc=hr"
attr=uid,CARNetuniqueName,CARNetuniqueID,CM
UstatID,CMUenable
  by self read
  by * read
```

slapd.conf – pristup podacima

```
access to dn.subtree="dc=domena,dc=hr"
  by self write
  by * read

access to * by * read

limits dn="cn=cmuadmin,dc=srce,dc=hr" size.hard="none"
limits user size=100
limits anonymous size.hard=50
```

password encription

- rootpw – može biti *plain text* ili **{CRYPT}**, **{MD5}**, **{SMD5}**, **{SSHA} ili {SHA}**
- preporuka je da uz dozvolu 600 na slapd.conf, rootpw bude kriptiran nekim od gore navedenih standarada
- preporuka je korištenje **{SSHA} ili {SHA}**

Dostupnost do informacija (user)

- tri skupine korisnika
  - anonymous
  - user
  - administrator
    - admin
    - cmuadmin

limits dn="cn=cmuadmin,dc=srce,dc=hr“ size.hard="none"

limits user size=100

limits anonymous size.hard=50

Dostupnost do informacija (network)

- javni servis (kao HTTP server)
- sustav autentikacije
- ograničen dohvat informacija sustavom limita
- ograničen dohvat informacija sustavom pristupa *access to*

Sistemsko održavanje LDAP imenika

- Backup procedura
- Restore procedura
- Recover procedura
- Brisanje binarnih logova transakcija
- Promjena administracijskog passworda
- Testiranje rada LDAP imenika

Backup procedura

- ldapsearch – prijenos podataka u LDIF formatu
- http://www.openldap.org/software/man.cgi?query=ldapsearch&apropos=0&sektion=0&manpath=OpenLDAP+2.2-Release&format=html

Paket OpenLDAP 2.1.12-x -:

```
/usr/local/bin/ldapsearch -LLL -H ldap://server_host_name:389/ \
-b "dc=domena,dc=hr" -x -D "cn=root,dc=domena,dc=hr" \
-s sub -W "objectClass=*" > backup_file.ldif
```

Paket OpenLDAP 2.1.17-x +:

```
ldapsearch -LLL -H ldap://server_host_name:389/ \
-b "dc=domena,dc=hr" -x -D "cn=admin,dc=domena,dc=hr" \
-s sub -W objectClass=* > backup_file.ldif
```

Restor procedura

- ldapmodify – unos podataka iz LDIF formata u bazu podataka (imenik)
- http://www.openldap.org/software/man.cgi?query=ldapmodify&apropos=0&sektion=0&manpath=OpenLDAP+2.2-Release&format=html

Paket OpenLDAP 2.1.12-x -:

```
/usr/local/bin/ldapmodify -H
ldap://server_host_name:389/ \
-a -c -x -D "cn=root,dc=domena,dc=hr" -W -f
backup_file.ldif
```

Paket OpenLDAP 2.1.17-x +:

```
ldapmodify -H ldap://server_host_name:389/ \
-a -c -x -D "cn=admin,dc=domena,dc=hr" -W -f
backup_file.ldif
```

Restore procedura

- zaustavljanje *slapd* procesa
- brisanje svih podataka iz direktorija gdje se nalaze podaci imenika
- pokretanje *slapd* procesa
- punjenje podataka *ldamodify* naredbom

Recover procedura

- *db_recover, db4.1_recover* naredba
- paket db4.1-util sadrži potrebne programe
- zaustavimo *slapd* proces
- pozicioniramo se u direktorij gdje se nalaze podaci o imeniku
- pokrenemo naredbu db_recover ili db4.1_recover s opcijom –c
- ponovno pokrenemo *slapd* proces

Brisanje binarnih logova transakcija

- transakcijska baza podataka
- transakcije se bilježe u binarne logove
- logove treba pobrisati ako se ne koriste (zauzimaju nepotrebno prostor na disku)
- koristiti set db_ odnosno db4.1_ skripti za rad s dbd bazom podataka

Skripta za brisanje binarnih logova

```
#!/usr/bin/bash
/etc/init.d/ldapd stop
sleep 5
cd /serv/ldap-data
/usr/local/openldap/db/bin/db_recover -c
sleep 5
/etc/init.d/ldapd start
for red in `/usr/local/openldap/db/bin/db_archive -a`; do (echo $red; rm $red;);
 done
#
```

Promjena administracijskog passworda

- u slapd.conf datoteci zamjeniti vrijednosta atributa rootpw
- zaustaviti slapd proces i ponovno ga pokrenuti

```
slappasswd -h {SHA}
New password:
Re-enter new password:
{SHA}kMnXvfudDF5mr5eAWjfjRNse0Dg=
```

Testiranje rada LDAP imenika

- ldapsearch -x -h <ip_adresa> -s base -b "" +

```
# extended LDIF
#
# LDAPv3
# base <> with scope base
# filter: (objectclass=*)
# requesting: +
#

#
dn:
structuralObjectClass: OpenLDAProotDSE
namingContexts: dc=publiczg,dc=hr
supportedControl: 2.16.840.1.113730.3.4.18
supportedControl: 2.16.840.1.113730.3.4.2
...
```

Testiranje rada LDAP imenika

- ldapsearch -x -H ldap://<ip_adresa>/ -b "dc=<domena>,dc=hr"

```
# extended LDIF
#
# LDAPv3
# base <dc=publiczg,dc=hr> with scope sub
# filter: (objectclass=*)
# requesting: ALL
#

# publiczg.hr
dn: dc=publiczg,dc=hr
objectClass: organization
objectClass: dcObject
dc:: UFVCTElDWkcg
o:: SmF2bm8gcmFjdW5hbG8gQ0FSTmV0YSB1IFphZ3JlYnUg
postalAddress:: Q0FSTmV0JEouTWFyb2huaWNhIGIuYi4kSFItMTAwMDAkSHJ2YXRza2Eg
postalCode: HR-10000
```

Testiranje rada LDAP imenika

- ldapsearch -x -H ldap://<ip_adresa>/ -b "dc=<domena>,dc=hr“ cn=cmuadmin

```
# extended LDIF
#
# LDAPv3
# base <dc=publiczg,dc=hr> with scope sub
# filter: cn=cmuadmin
# requesting: ALL
#

# cmuadmin, publiczg.hr
dn: cn=cmuadmin,dc=publiczg,dc=hr
CMUstatID: A
CMUenable: D
sn: CMUADMIN
mail: cmu-admin@CARNet.hr
objectClass: person
objectClass: organizationalPerson
# numEntries: 1
```

Administrativno održavanje LDAP imenika

- LDIF datoteka
- Dodavanje novih zapisa
- Ažuriranje zapisa
- Brisanje zapisa
- Pretraživanje zapisa

LDIF datoteka

- tekstualna datoteka za pohranu podataka iz LDAP imenika
- pojedinačni zapis završava praznim redom
- zadnji redak u LDIF datoteci mora biti prazni redak
- : označava tekstualnu vrijednost
- :: označava MIME 64 kodiranu vrijednost (naši znakovi)

Struktura LDIF datoteka

- počinje navođenjem jedinstvene oznake za svaki zapis (dn:)
- sljedi popis shema koje se koriste za zapisivanje podataka unutar zapisa (objectclass:)
- završava popisom atributa i njihovih vrijednosti
- zadnji red zapisa je uvijek prazni red
- izuzetak je LDAP browser (java) koji završava s dva prazna reda

Primjer LDIF datoteke

dn: uid=shucika,dc=publicst,dc=hr

objectClass: CarnetCmuPerson

objectClass: CarnetPerson

objectClass: inetOrgPerson

objectClass: organizationalPerson

objectClass: person

CARNetuniqueID: shucika.publicst.20040122100157

CARNetuniqueName: shucika.publicst

CMUenable: E

CMUstatID: D

cn:: U2luacWhYSBIdWNpa2E=

sn: Hucika

userPassword:: e1NIQX1mTGc5YWZhNWI5KzRDTastronedi0RMc1dhSU09

Dodavanje novih zapisa

- kreirati LDIF datoteku s podacima
- *ldapmodify* s opcijom –a (add)
- http://www.openldap.org/software/man.cgi?query=ldapmodify&apropos=0&sektion=0&manpath=OpenLDAP+2.2-Release&format=html
- koristiti predstavljanje kao administrator imenika

```
ldapmodify -H ldap://server_host_name:389/ \
-a  -x -D "cn=admin,dc=domena,dc=hr" -W -f backup_file.ldif
```

Ažuriranje zapisa

- kreirati LDIF datoteku s podacima
  - dn: zapisa
  - objectclass: shema koje se koriste za atribute koji se koriste u LDIF zapisu
  - popis atributa čije vrijednosti se mjenjaju
- *ldapmodify*
- http://www.openldap.org/software/man.cgi?query=ldapmodify&apropos=0&sektion=0&manpath=OpenLDAP+2.2-Release&format=html
- koristiti predstavljanje kao administrator imenika

Ažuriranje zapisa

```
ldapmodify -H ldap://server_host_name:389/ \
-x -D "cn=admin,dc=domena,dc=hr" -W -f file.ldif
```

Brisanje zapisa

- kreirati LDIF datoteku samo s dn: podatkom zapisa koji želimo obrisati
- pravilo završetka zapisa s praznim redom je obavezno
- ldapdelete
- http://www.openldap.org/software/man.cgi?query=ldapdelete&apropos=0&sektion=0&manpath=OpenLDAP+2.2-Release&format=html

Brisanje zapisa

```
ldapdelete -H ldap://server_host_name:389/ \
-x -D "cn=admin,dc=domena,dc=hr" -W -f file.ldif
```

Pretraživanje zapisa

- ldapsearch
- http://www.openldap.org/software/man.cgi?query=ldapsearch&apropos=0&sektion=0&manpath=OpenLDAP+2.2-Release&format=html
- dobiveni rezultat ovis o tipu autentikacije
- osnovni dio komande se sastoji od uvijeta traženja i popisa atributa koji se traže od imenika za svaki zapis koji zadovoljava upit

Uvijeti traženja

attribute **OPERATOR** *value*

Operators:

=	jednako
>=	veće od
<=	manje od
=*	svi zapisi koji sadrže ovaj atribut
~=	približna pretraga
&	i , zapisi moraju zadovoljiti oba uvijeta
|	ili, zapisi moraju zadovoljiti jedan od uvijeta
!	negacija

Uvijeti traženja

Primjer:

(| (sn=roiron) (&ou=tecfa) (sn=muller))

.. vraća sve zapise u kojima je ili sn jednako roiron ili muller, a članovi su organizacije tecfa

Uvijeti traženja

 # ldapsearch -x -H ldap://161.53.2.130/ -b "dc=publiczg,dc=hr" cn=admin

extended LDIF

#

LDAPv3

base <dc=publiczg,dc=hr> with scope sub

filter: cn=admin

requesting: ALL

#

search result

search: 2

result: 0 Success

numResponses: 1

LDAP u aplikacijama (AAI)

- PHP
- PAM
- SAMBA
- CMU
- AAI – StuDom
- AAI@EDU.HR

Osnove LDAP autentikacija

- bind – korištenje autentikacijskih parametara lozinke i DN-a pristupamo LDAP imeniku
- anonymous pristup podacima koji su javno dostupni
- administrativni pristup podacima dohvačaju se svi podaci pa se uspoređuju s dobivenim podacima od korisnika

PHP

- http://hr2.php.net/manual/en/ref.ldap.php
- osnova se svodi na
  - spajanje na server
  - bind – predstavljanje korisnik, anonymous, administrator
  - dohvat informacija, promjena, dodavanje ili brisanje podataka

PHP

- obratiti pažnju na tip protokola (v2 ili v3)
- vrijeme odziva LDAP servera može biti jako, jako, jako dugo (normalna situacia, a ne greška)
- podaci izvan ASCII-a se zapisuju u UTF-8 standardu (potrebnom MIME 64 kodiranje)
- password se pohranjuje kao plain text ako drugačije nije kreirano u PHP-u

PAM

- pam_ldap
- http://www.padl.com/OSS/pam_ldap.html
- nedostak jer se traži potpuni prijenos podataka o autentikaciji i autorizaciji u LDAP imenik
- postoji rješenje za samu autentikaciju (Dinko Korunić)
- pam_radius_auth – praktičnije riješenje

pam_radius_auth

- http://www.freeradius.org/pam_radius_auth/
- višestruki backup pristup
- mogućnost dodatne autentikacije/autorizacije/auditinga
- vremenski precizan sustav
- robustnost i jednostavnost

SAMBA

- http://us1.samba.org/samba/samba.html
- zamjena za Microsoft Active Directory
- postoji SAM modul za LDAP AA
- kao i PAM modul, a sukladno s Microsoft politikom fizički usporedjuje dobivene podatke a ne koristi bind mogućnost LDAP-a
- ne skalabilan pristup

SAMBA

- Srce projekt – Uporaba SAMB-a za autentikaciju korisnika u Microsoft okruženju – suživot dva svijeta
- iskorištena mogučnost Microsoft Windows 2000+ servera o prosljedjivanju sustava autentikacije
- patch za SAMB-u u obliku pravih PAM modula (Dinko Korunić)
- očekivani rezultati 2004/4

CMU

- http://www.cmu.carnet.hr/
- http://cmung.cmu.carnet.hr/
- LDAP kao autentikacijski i autorizacijski izvor podataka (CMUperson shema)
- Radius kao autentikacijsko-autorizacijsko-auditivni mehanizam
- centralizirani pristup i autentikacija CMU sustava

CMU

- centralni backup sustav bilježi samo podatke potrebne za autentikaciju korisnika na modemskim ulazima
- dostupnost LDAP-a za cmuadmin korisnika s mreža 161.53.114.0/24, 161.53.1.0/24, 161.53.2.0/24, 161.53.254.0/24
- moguć ograničen povrat podataka ustanovama (najbolje je redovito raditi lokalni full backup)

AAI - StuDum

- http://www.srce.hr/StuDOM/
- pristup Internetu za studente smještene u stunskim domovima
- autenticirani pristup putema 802.1x seta protokola (EAP-TTLS)
- omogućena autentikacija i stranim studentima ustanova uključenih u sustav TERENA TF-Mobility projekta

AAI@EDU.HR

- http://www.srce.hr/aai/
- projekt MZOŠa, Srca i CARNeta
- osigurati jedinstvenu, opće prihvaćenu hrvatsku LDAP shemu, kompatibilnu s medjunarodno prihvaćenim standardima
- osigurati AAI infrstrukturu na što široj osnovi
- sudjelovati u radu GEANT 2 projekta (JRA5)