

LDAP - osnove

- LDAP (*engl. Lightweight Directory Access Protocol*) → mrežni standard
- Direktorij – baza podataka
(četiri skupine)
- povijesni razvoj:
X.500, DAP, LDAP

LDAP - osnove

- Tim Howes, Steve Kille i Wengyik Yeong – tvorci LDAP protokola



Organizacija LDAP -a

- Podaci na LDAP poslužitelju organizirani su u hijerarhijsko-relacijskom formatu
- LDAP se zasniva na četiri modela:

informacijski model
model imenovanja
model funkcionalnosti
sigurnosni model

Informacijski model

- razred
- atributi
- sintaksa atributa
- zapisi
- shema

Model imenovanja

- organizacija i referenciranje podataka
- informacijsko stablo direktorija

Model funkcionalnosti

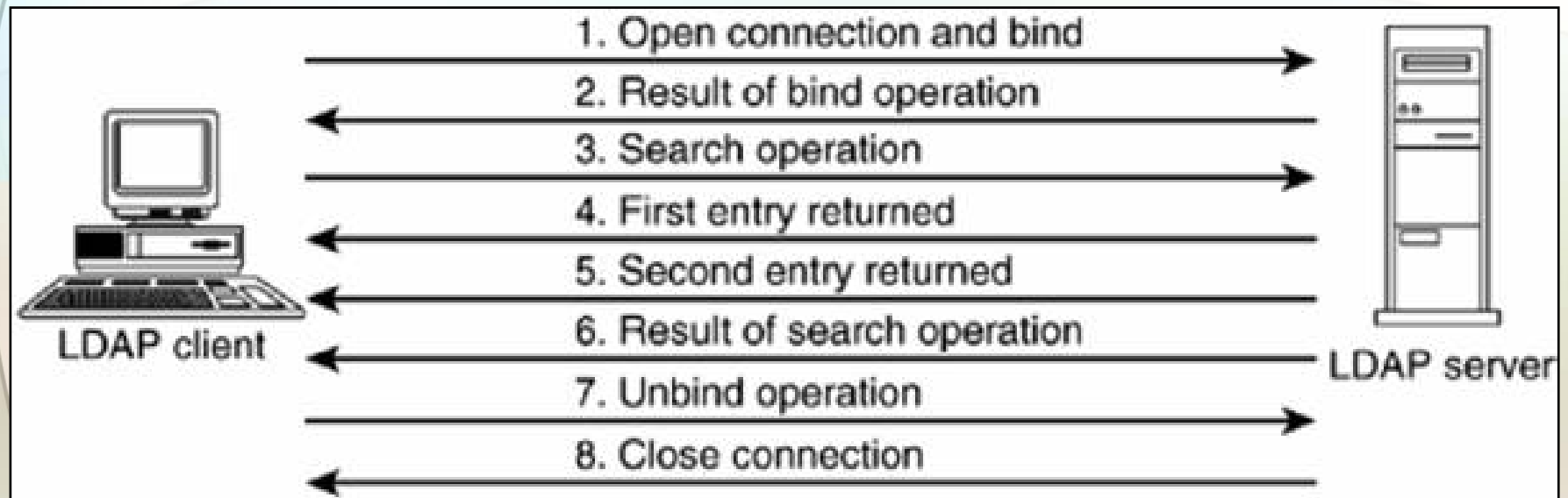
- autentikacija
Open, Bind, Unbind
- pretraživanje
Search, Compare
- izmjena
Add, Modify, Modify RDN, Delete

Sigurnosni model

- siguran pristup podacima
- SASL (*Simple Authentication and Security Layer*) mehanizama

LDAP komunikacija

- komunikacija u 8 koraka:



LDAP IMPLEMENTACIJE

OpenLDAP

Apple Open Directory

Novell eDirectory

IBM Tivoli Directory Server

Microsoft Active Directory

Apache Directory Server

Fedora Directory Server

Oracle Internet Directory

SIDVault (Simple Integration Database)

OpenLDAP

- besplatna, *opensource* implementacija LDAP-a
- OpenLDAP projekt je započeo razvijati 1998. Kurt Zeileng



OpenLDAP

- OpenLDAP softver uključuje:

samostalni LDAP server (slapd)

samostalni LDAP replikacijski server
(slurpd)

set razvojnih alata (ldap)

razni drugi alati

Glavne verzije OpenLDAP-a

- OpenLDAPv1 – *“pročišćavanje”*
- OpenLDAPv2.0 – *LDAPv3, IPv6*
- OpenLDAPv2.1 – *SASL podrška*
- OpenLDAPv2.2 – *LDAP sync engine*
- OpenLDAPv2.3 – *Password Policy*

Novell eDirectory

- prije poznat kao Novell Directory Service
- koristi se u više od 80% *Fortune 1000* kompanija
- objektno-orijentirana baza podataka

Novell eDirectory

The screenshot displays the phpLDAPadmin web interface within a Mozilla browser window. The browser title is "phpLDAPadmin - CVS - Mozilla" and the address bar shows "http://raider/phpldapadmin/". The interface is divided into a left sidebar and a main content area.

Left Sidebar (Directory Tree):

- cn=DEVNET-PUBLIC
 - cn=DEVNET-PUBLIC Backup Queue
 - cn=DEVNET-PUBLIC SMS RPC
 - cn=DEVNET-PUBLIC_SP
 - cn=DEVNET-PUBLIC_SYS
 - cn=DEVNET-PUBLIC_VOL1
 - cn=dmitryugov
 - cn=File
 - cn=FZhao
 - cn=gcamaszotisz
 - cn=jcox
 - cn=JLOVE
 - cn=LDAP Catalog - DEVSUP-FTP
 - cn=ldap certificate - DEVNET-PUBLIC**
 - cn=LDAP Group - DEVNET-PUBLIC
 - cn=LDAP Group - DEVSUP-FTP
 - cn=LDAP Server - DEVNET-PUBLIC
 - cn=LDAP Server - DEVSUP-FTP
 - cn=lkpodo
 - cn=misch
 - cn=NAASKMO - DEVNET-PUBLIC
 - cn=NFAUUser
 - cn=NISSERV_DEVNET-PUBLIC
 - cn=NLSP_DEVNET-PRIVATE

Main Content Area (Entry Details):

cn=ldap certificate - DEVNET-PUBLIC
Server: IILDAP Distinguished Name: cn=ldap certificate - DEVNET-PUBLIC,o=NOVELL

Actions: Refresh, Export, Copy this entry, Show internal attributes, Delete this entry, Rename, Create a child entry, Add new attribute.

Hint: To delete an attribute, empty the text field and click save.
Hint: To view the schema for an attribute, click the attribute name.

ACL

- 2#entry#[Public]#hostServer
- 2#subtree#cn=SAS Service - DEVNET-PUBLIC,o=NOVELL
- (add value)

cn

- ldap certificate - DEVNET-PUBLIC
- (add value)

hostServer

- cn=DEVNET-PUBLIC,o=NOVELL

nDSPKICertificateChain

- Binary value
- download value
- delete attribute

nDSPKIGivenName

The browser's status bar at the bottom shows the URL: "http://raider/phpldapadmin/edit.php?server_id=1&dn=cn=ldap certificate - DEVNET-PUBLIC,o=NOVELL".

Microsoft Active Directory

- Prvi prikaz bio je 1996. sa Windowsima 2000
- centralna baza podataka
- veličina instalacije varira (10^2 – 10^6 objekata)



Struktura Microsoft Active Directory-ja

- objekti
- stabla, šume, domene
- povjerenje (trust):

one way, two way, trusting domain, trusted domain, transitive trust, intransitive trust, explicit trust, cross-link trust

Fedora Directory Server

- LDAP server razvijen od strane Red Hat-a
- bivši *slapd* projekt Sveučilišta Michigan
- Netscape Communications Corp. preuzima
- Red Hat – 1.lipanj 2005.
→opensource
- multi-master ability

Fedora Directory Server

The screenshot displays the Fedora Directory Server console interface. The window title is "localhost:localhost: Fedora Directory Server - localhost". The interface includes a menu bar (Console, Edit, View, Object, Help) and a toolbar with tabs for Tasks, Configuration, Directory, and Status. A left-hand navigation tree shows the directory structure for "localhost:localhost:10000", including Performance Counters, userRoot, roles, NetScapeRoot, MVRDN, example, directory, dirius.com, Logs (Access Log, Error Log, Audit Log), and Replication Status.

The main content area is titled "Directory Server" and contains several sections:

- General Information:**
 - Server version: Fedora-Directory/1.0.82005.325.2143
 - Startup time on server: 12/1/05 11:43 AM
 - Current time on server: 12/1/05 12:11 PM
 - Buttons: Refresh, Continuous refresh
- Resource Summary:**

Resource	Usage Since Startup	Average Per Minute
Connections	38	0.6
Operations Initiated	546	19.5
Operations Completed	545	19.5
Entries Sent To Clients	1982	70.8
Bytes Sent To Clients	1556482	55588.6
- Current Resource Usage:**

Resource	Current Total
Active Threads	30
Open Connections	8
Remaining Available Connections	952
Threads Waiting To Read From Client	1
Databases In Use	7
- Connection Status:**

Time Opened	Started	Completed	Bound As	Read/Writes
Thu Dec 01 11:49:34 MST 2...	5		uid=admin,ou=administrat...	Not blocked
Thu Dec 01 11:43:43 MST 2...	1	1	cn=admin-srv-localhost.c...	Not blocked
Thu Dec 01 11:43:44 MST 2...	1	1	cn=admin-srv-localhost.c...	Not blocked
Thu Dec 01 11:43:43 MST 2...	2	2	cn=admin-srv-localhost.c...	Not blocked
Thu Dec 01 11:43:44 MST 2...	2	2	cn=admin-srv-localhost.c...	Not blocked
Thu Dec 01 11:49:34 MST 2...	86	86	uid=admin,ou=administrat...	Not blocked
Thu Dec 01 11:54:05 MST 2...	192	191	cn=directory manager	r
Thu Dec 01 12:03:15 MST 2...	225	223	cn=directory manager	Not blocked
- Global Database Cache Information:**

Performance Metric	Current Total
Hits	115345
Misses	115598
Hit Ratio	99
Pages read in	213
Pages written out	446
Read-only page evicts	0
Read-write page evicts	0

A "Help" button is located in the bottom right corner of the console window.

Oracle Internet Directory

- integracija sa Oracle bazama podataka
- više-platfomska struktura
- integracija certifikata o postojećim javnim ključevima
- suživot sa ostalim LDAP implementacijama

SIDVault (Simple Integration Database)

- trenutno najbrži, potpuni LDAP server na tržištu (tvrde u kompaniji)
- Podupire sve relevantne RFC protokole: LDAPv2, LDAPv3, HTTP, ILS
- lagana integracija sa sadašnjim LDAP sistemima
- Podržava *Microsoft NetMeeting Client* i *Microsoft Portrait*

SIDVault (Simple Integration Database)

SIDVault
Alpha Centauri Software Ltd

- Intro Page
- Registration Info
- Accounts / Users
- Site Stats
- Setup
 - Security
 - IP Details
 - Modules
 - Base DN's
 - Socking
 - From LDIF
 - From LDAP Server
- Advance Setup
 - Schema's
 - Backup Database
 - Replicate
 - Replicate Stats
 - Replicate Grab
 - Directories
 - HTTP Settings
 - DataBase
 - Referrals
- Manuals
- User Interface
- Shutdown

- Logs
- Debug
 - Memory Allocation
 - Mutex Allocation
 - Database CRC's
 - Thread List

Site Stats

Started	Type (ID)	IP/Port	Conn.	Cur/Max
11/07/05 12:15am	ldap (main)	all:389	0	0/50
11/07/05 12:15am	http (web)	all:6680	10	1/50
11/07/05 12:15am	replicate (rep)	all:6680	0	0/10

Backup Database
Thread List

Failed Modules

IP Limiting

ID	Max Conn	Conn/Rate	Pass/Rate
main	10	50 / 30sec (30sec block)	3 / 30sec (60sec block)
web	100		3 / 60sec (60sec block)

IP Details

Current Connections

TID	Type	From IP	In	Out	Started
2216	http	[REDACTED]	749	0	11/07/05 12:19am close

Past Connections

Type	From IP	In	Out	Conn.	Last Touched
http	[REDACTED]	14857	82694	9	11/07/05 12:17am

Literatura

- <http://en.wikipedia.org/wiki/Ldap>
- <http://ipv6.carnet.hr/paketi/dokumentacija/CAR6Net-ldap-utils.pdf>
- http://jagor.srce.hr/~ivelimir/docs/case2004_velimirovic_paper.pdf
- <http://www.openldap.org/>
- http://os2.zemris.fer.hr/protokoli/2005_nejasmic/index.htm
- <http://osnove.tel.fer.hr/nastavnici/randic/oum/Seminar0405/LDAP.pdf>
- <http://directory.apache.org/>
- <http://alphacentauri.co.nz/sidvault/index.htm>
- http://en.wikipedia.org/wiki/Fedora_Directory_Server
- http://en.wikipedia.org/wiki/IBM_SecureWay_Directory
- http://en.wikipedia.org/wiki/Oracle_Internet_Directory
- <http://www.kerio.com/manual/kms/en/ch29s02.html>
- http://en.wikipedia.org/wiki/Active_Directory
- <http://www.apple.com/server/macosx/features/opendirectory.html>
- <http://www.novell.com/products/edirectory/>
- <http://www-03.ibm.com/servers/eserver/series/ldap/schema/>
- <http://www.redbooks.ibm.com/redbooks/pdfs/sg244986.pdf>