

Configuring LDAP on z/VM and Linux

Rich Smrcina
VM Assist

Session 9156
August 26, 2009



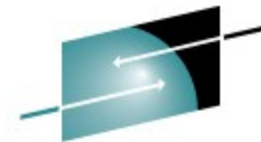
Presentation Materials



- SHARE Proceedings
- <http://linuxvm.org>
- <http://sites.google.com/site/rsmrcina/presentations>

This presentation is generally a follow-on to 'Securing Linux with RACF on z/VM' by Alan Altmark. Provides additional detail about configuring LDAP on z/VM

Agenda



S H A R E

Technology • Connections • Results

- What is LDAP?
- Background
- General Configuration
- LDAP Startup
- LDAP Checkout
- Setting up Linux on System z to work/play in this environment
 - Load Schemas
 - Setup Admin Access
 - Using z/VM LDAP with Linux
 - Browsing the LDAP Directory
- Other software
 - Apache
 - Browsing/Editing Tools
 - Monitoring
- References

What is LDAP?

- Stands for **L**ightweight **D**irectory **A**ccess **P**rotocol
- A standard method for accessing and updating information in a directory
 - Defined in RFC 1777 and others¹
- Widely used across all major operating systems and platforms
- The 'directory' can contain almost anything
 - Generally it is data that is read much more than updated
 - Name and address book
 - Organization chart
 - Hardware and/or Software information
- LDAP is optimized for lookup operations

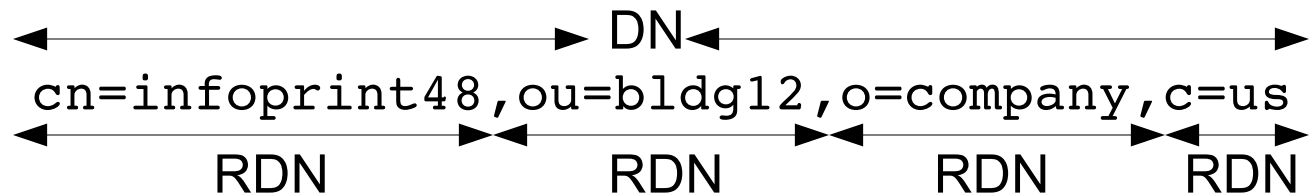
¹RFCs 1777, 1778, 1779, 1959, 1960, 2251, 2252, 2253, 2254, 2255, 2256, 2829, 2830, 3377

What is LDAP?

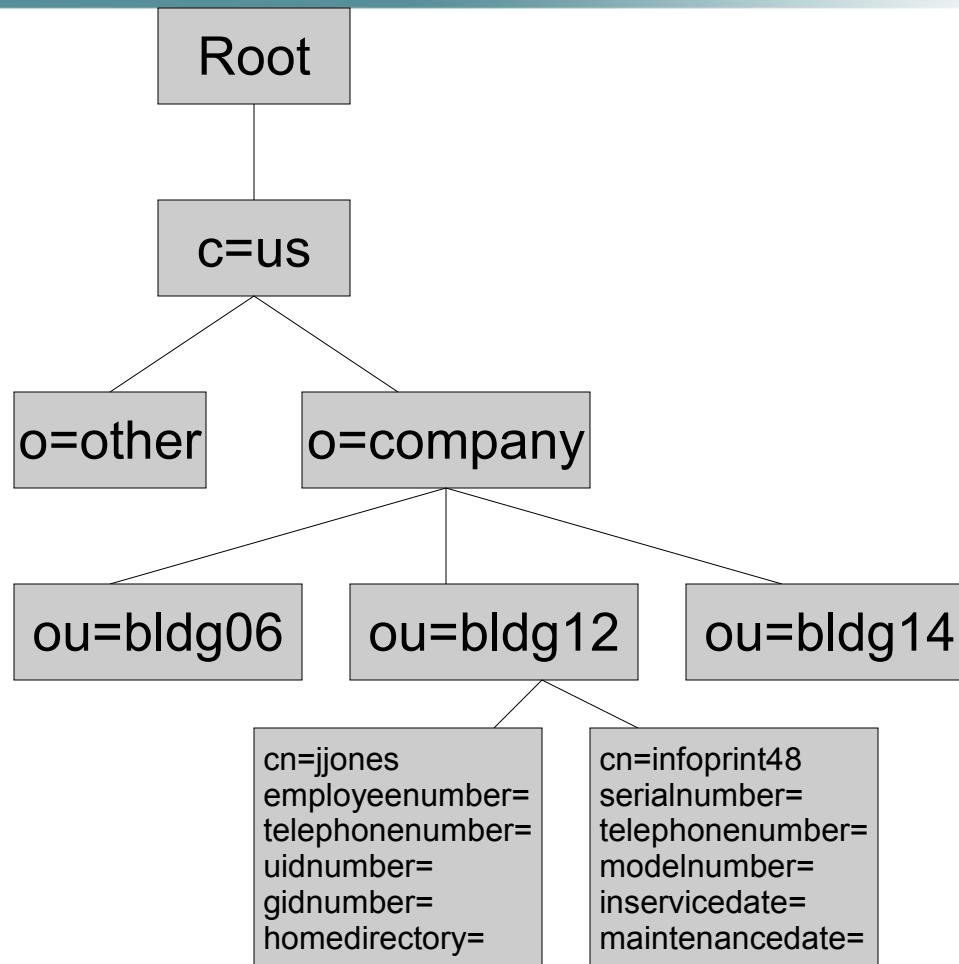
- Consider the phone book approach
- LDAP can search on any object in the directory
- Updating the directory can be limited to administrators
 - And/or controlled via ACLs so that certain people can update specific parts of the directory
- LDAP is the messaging protocol for communicating between clients and servers
 - Defines the API for accessing the directory
 - Does not define the mechanism to be used for backend storage

What is LDAP?

- The directory is made up of objects organized in a tree
 - Called the Directory Information Tree (DIT)
- Similar to DNS, the tree starts at a root and branches out
- Each entry is arranged on the tree via a unique identifier called the distinguished name or DN
- Each component of the DN is called the relative distinguished name or RDN



What is LDAP?



What is LDAP?

- More commonly LDAP is used to store and manage security related information
- Available across the network by any machine that needs it
 - Subject, of course, to it's own security controls
- Can be part of an enterprise-wide identity management infrastructure
 - A single point of control for user profile management

Background

- The LDAP Server on z/VM 5.4
 - Ported from IBM Tivoli Directory Server for z/OS V1.10
- Provides
 - Multiple database backends
 - Version 2 and 3 client capability
 - CRAM-MD5, DIGEST-MD5 authentication, Simple authentication
 - Referrals, aliases, directory information access controls
 - Change Logging
 - Client and Server authentication using SSL (V3) and TLS (V1)

Background

- **LDBM Backend (Lightweight Database Manager)**
 - Simplest setup
 - Performs authentication and password modification with the z/VM RACF Security Server
 - Stores directory information in the Byte File System
 - Keeps it in memory while the LDAP server is running
- **SDBM Backend (Secure Database Manager)**
 - Provides more comprehensive interface to the z/VM RACF Security Server
 - Allows password phrases up to 100 characters
- **GDBM Backend (GNU Database Manager)**
 - Used for auditing changes to LDAP server

General Configuration

- Uses TCP ports 389 and 636
 - As coded in the default profile that comes with the TCP/IP stack
- DTCPARMS values can default
 - If using the SDBM backend or the LDBM backend with RACF, set ESM_Enable to YES
- The sample file(s) provided with z/VM contain these statements

General Configuration

- The mount tag is used to set up the ROOT file space for the LDAP server in the BFS
- Use the Parns tag to pass any additional parameters to the LDAP server
 - A different configuration file (the default is DS CONF)
 - Debugging options
 - Listening URL
 - Maintenance mode

General Configuration

- Default values from 'IBM DTCPARMS'

```
:nick.ldap      :type.class
                 :name.LDAP daemon
                 :command.LDAPSRV
                 :runtime.C
                 :memory.128M
                 :mixedcaseparms.YES
                 :mount. /../VMBFS:VMSYS:ROOT/ / ,
                       /../VMBFS:VMSYS: /var/ldap
                 :ESM_Enable.NO
                 :ESM_Racroute.LDAPESM
```

General Configuration



- The LDAP server runs in the LDAPSrv virtual machine by default
- A different machine or additional machine(s) can be used
- A few caveats...
 - Directory Entry
 - BFS File Space creation and proper BFS permissions
 - Mount entry for additional server
 - Parns value to indicate a new listening port

General Configuration

- The LDAP Server uses the Byte File System to store
 - Message catalog files
 - Schema databases and other files for the LDBM and GDBM backends
 - Locations are tailorable
- ! Tip: Make sure the SFS file servers come up before TCP/IP
- Two Configuration files
 - DS CONF – Primary Operational Parameters
 - DS ENVVARS – Environment Variables
- Copy samples from TCPMAINTs 591 disk to the 198 disk
 - LDAP-DS SCONFIG ----- > DS CONF
 - LDAP-DS SAMPENVR -----> DS ENVVARS

General Configuration

- Tailoring the configuration files
- DS CONF on TCPMAINTs 198
- A different name can be used
 - Indicate this with the -f flag on the LDAPSRV startup PARMS
- Contains four sections
 - Global section
 - LDBM section
 - SDBM section
 - GDBM section

General Configuration

- In the Global Section

- Set `adminDN` to the Distinguished Name of the administrator

```
adminDN "cn=Admin"
```

- Set the `adminPW`

- In the LDBM Section

- Uncomment the `database` keyword

```
database LDBM GLDBLD31
```

- Uncomment the `suffix` keyword and change the Distinguished Name

```
suffix "o=VMAssist,c=US"
```

General Configuration

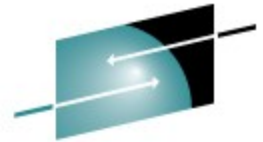
- Tailoring the Environment Variables
- DS ENVVARS on TCPMAINTs 198 disk
- Read only at LDAP server startup time
- The following can be customized
 - Message logging options
 - Severity
 - End of an operation
 - Microseconds on timestamp
 - Summary records
 - Timezone
 - Debugging options
 - Trace output file
 - Error messages output
 - Environment variables filename

LDAP Startup

- Log on to LDAPSRV
- Starts up like any other TCP/IP service on z/VM

```
DTCRUN1011I Server started at 10:00:37 on 17 Jun 2008 (Tuesday)
DTCRUN1011I Running "LDAPSRV"
DTCLDP2106I Debug setting: 0
DTCLDP2107I Using server configuration file: DS CONF D1
DTCLDP2107I Using environment variable file: DS ENVVARS D1
DTCLDP2107I Using server module: GLDSRV31 MODULE E2
080617 15:00:41.662708 GLD1003I LDAP server is starting.
080617 15:00:41.667573 GLD1001I LDAP server version 3.18, Service level
OA19849, Build date Mar 22 2007, Time 22:58:27.
080617 15:00:41.671714 GLD1002I LDAP runtime version 3.18, Service
level OA19849, Build date Mar 22 2007, Time 23:25:52.
080617 15:00:42.123599 GLD1023I Processing configuration file
//DD:CONFIG.
080617 15:00:42.186911 GLD1024I Configuration file //DD:CONFIG
processed.
Server Configuration
adminDN: cn=Admin
adminPW: *configured*
allowAnonymousBinds: on
```

LDAP Startup



S H A R E

Technology • Connections • Results

```
armName: GLDSRVR
audit 1: off
commThreads: 10
db2Terminate: recover
dnCacheSize: 1000
idleConnectionTimeout: 0
listen 1: ldap://:389
logfile: /etc/ldap/gldlog.output
maxConnections: 65535
pcIdleConnectionTimeout: 0
pcThreads: 10
schemaPath: /var/ldap/schema
schemaReplaceByValue: on
securityLabel: off
sendV3StringsOverV2As: UTF-8
serverEtherAddr: 402094000001
serverSysplexGroup: undefined
sizeLimit: 500
srvStartUpError: terminate
supportKrb5: off
```

```
tcpTerminate: recover
timeLimit: 3600
validateIncomingV2Strings: on
database LDBM GLDBLD31 LDBM-0001
changeLoggingParticipant: on
commitCheckpointEntries: 10000
commitCheckpointTOD: 00:00
databaseDirectory: /var/ldap/ldbm
extendedGroupSearching: off
fileTerminate: recover
filterCacheBypassLimit: 100
filterCacheSize: 5000
krbIdentityMap: off
multiServer: off
nativeAuthSubtree: all
nativeUpdateAllowed: on
persistentSearch: off
pwEncryption: none
pwCryptCompat: on
readOnly: off
secretEncryption: none
```

LDAP Startup

```
sizeLimit: 500
suffix 1: o=VMAssist, c=US
timeLimit: 3600
useNativeAuth: off
080617 15:00:58.233324 GLD1191I LDAP server auditing is not available.
080617 15:01:02.186225 GLD1074W Maximum client connections changed from
65535 to 65523.
080617 15:01:02.229484 GLD1004I LDAP server is ready for requests.
080617 15:01:03.491447 GLD1059I Listening for requests on 192.168.1.50
port 389.
080617 15:01:03.552522 GLD1059I Listening for requests on 192.168.240.1
port 389.
080617 15:01:03.564893 GLD1059I Listening for requests on 127.0.0.1
port 389.
```

LDAP Checkout

- Netstat output

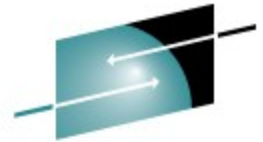
VM TCP/IP Netstat Level 540

TCP/IP Server Name: TCPIP

Active IPv4 Transmission Blocks:

User Id	Conn	Local Socket	Foreign Socket	State
----	--	-----	-----	-----
FTPSERVE	1004	*..FTP-C	*..*	Listen
INTCLIEN	1003	*..TELNET	*..*	Listen
INTCLIEN	1011	192.168.1.50..TELNET	10.1.0.2..41112	Established
INTCLIEN	1012	192.168.1.50..TELNET	10.1.0.2..41113	Established
SSLSERV	1000	127.0.0.1..1024	*..*	Listen
SSLSERV	1001	127.0.0.1..1024	127.0.0.1..1025	Established
SSLSERV	1002	*..1026	*..*	Listen
LDAPSRV	1007	192.168.1.50..389	*..*	Listen
LDAPSRV	1006	192.168.240.1..389	*..*	Listen
LDAPSRV	1008	127.0.0.1..389	*..*	Listen

LDAP Checkout



SHARE

Technology • Connections • Results

```
pwd
/var/ldap
$
ls -l
total 0
drwxr----- 1 ldapsrv system          0 Jun 17 15:04 ldbm
drwxr----- 1 ldapsrv system          0 Jun 17 15:00 schema
$
ls -l ldbm
total 16
-rw-r----- 1 ldapsrv system        32 Jun 17 15:00 LDBM-1.db
-rw-r----- 1 ldapsrv system        24 Jun 17 15:04 LDBM.ckpt
$
ls -l schema
total 56
-rw-r----- 1 ldapsrv system    25832 Jun 17 15:00 schema.db
$
```

LDAP Checkout

- Issuing LDAP Commands from CMS requires the use of characters that CP will remove from the command
 - eg: “”, @
- We need to tell CP to not perform line editing when we issue LDAP commands

```
CP SET LINEDIT OFF
```

...OR...

```
CP TERMINAL ESCAPE OFF (for the double quotes)  
CP TERMINAL CHARDEL OFF (for the at sign)
```


LDAP Checkout

- Test access to the server
- LDAP utilities are provided for use in CMS
 - ldapsearch (LDAPSrch), ldapadd (LDAPADD), ldapmodify (LDAPMODIFY), ldapcompare (LDAPCOMPARE), ldapdelete (LDAPDELETE), ldapmodrdn (LDAPMRDN)
- We will use the LDAPSrch command

```
ldapsrch -h 127.0.0.1 -w secret -s base -b "o=VMAssist,c=US" "objectclass=*"
ldap_search: No such object
ldap_search: additional info: R004071 DN 'o=VMAssist,c=US' does not exist
(ldbm_process_request)
```

- ...the database is empty

Load schema

- Schema is the definition of objects and their characteristics
 - eg: the rules that must be followed to form a telephone number
- Required for LDBM backend only
- Link and access TCPMAINTs 591 and 592 disks

```
ldapmdfy -h 127.0.0.1 -D "cn=Admin" -w ***** -f //USRSCHM.LDIF -u on
```

```
ldapmdfy -h 127.0.0.1 -D "cn=Admin" -w ***** -f //IBMSCHM.LDIF -u on
```

- A single line of output while the command is running
modifying entry cn=schema
- No error messages indicate a successful execution

Additional Schema

- Provides the LDAP posixAccount object class
 - Allows the use of uidnumber, gidnumber, homedirectory, etc
- Described in *Security on z/VM* redbook
- Download the schema from
 - <ftp://www.redbooks.ibm.com/redbooks/REDP0221/nisSchema.2.ldif>
- Upload file to z/VM (as NISSCHEM.LDIF)
- Modify line 5
 - From “dn:cn=schema, <suffix>” to “dn:cn=schema”
- Update schema on the LDAP Server

```
ldapmodify -h 127.0.0.1 -w secret -D "cn=Admin" -f //nisschem.ldif -u on  
modifying entry cn=schema
```

Native Authentication

- LDAP Server can authenticate to the Security Server through the LDBM backend
 - By providing Security Server password or pass phrase on a simple bind to the backend
- Information gathered by LDAP server based on DN that performed the bind
- LDAP server configuration options and specific attributes on LDAP user definition
 - useNativeAuth
 - nativeAuthSubtree
 - nativeUpdateAllowed
 - ibm-nativeID or uid

Setup Native Authentication and Admin access

- The LDAP Server virtual machine (LDAPSRV) will be set up as the administrator
 - The user exists on the z/VM system
- In DS CONF – LDBM section
 - Set the following options
 - `nativeUpdateAllowed on`
 - `useNativeAuth All`
 - `pwEncryption SHA`
- On user entries
 - `ibm-nativeID` or `uid`
- Create an **LDAP Data Interchange Format file (LDIF)**
 - A sample exists as SAMPSEV LDIF on TCPMAINTs 591 disk
 - The first two entries of the file were used as examples in the following scenario

Allow password or pass phrase updates in the Security Server via a modify command through the backend.

All or Selected, based on setting of `nativeAuthSubtree` option

Setup admin access

- In a file called ADMIN LDIF

```
dn: o=VMAssist,c=US
objectclass: top
objectclass: organization
o: VMAssist,c=US
```

```
dn: cn=LDAPSRV,o=VMAssist,c=US
objectclass: top
objectclass: person
objectclass: ibm-nativeAuthentication
description: Administrator
cn: LDAPSRV
sn: Administrator
ibm-nativeID: LDAPSRV
```

- File actually contains two entries
 - One to add the organization (o=VMAssist,c=US)
 - The other to add the 'user' (cn=LDAPSRV)

Setup admin access

- Use `ldapadd` to insert the entries into the LDBM database

```
ldapadd -h 127.0.0.1 -w secret -D "cn=Admin" -f //admin.ldif  
adding new entry o=VMAssist,c=US
```

```
adding new entry cn=LDAPSRV,o=VMAssist,c=US  
Ready; T=0.22/0.30 10:43:06
```

- Edit DS CONF to change the adminDN and remove the adminPW

```
adminDN "cn=LDAPSRV,o=VMAssist,c=US"  
#adminPW *****
```

Setup admin access

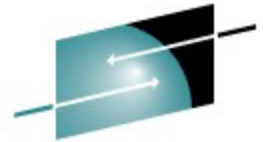
- Make sure LDAPSRV can properly access RACF
- In DTCPARMS
 - :ESM_Enable.YES
- Issue the following RACF commands

```
rdefine facility ichconn uacc(none)
permit ichconn class(facility) id(ldapsrv) access(update)
setropts raclist(facility) refresh
```

- Restart the LDAP Server

```
RPICMS016I USER/RACF VM Racroute communication path is established.
```


Setup admin access

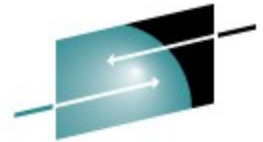


- Use `ldapsrch` to verify the entry just added

```
ldapsrch -h 127.0.0.1 -w vmpass -D "cn=LDAPSRV,o=VMAssist,c=US"  
-b "o=VMAssist,c=US" "(cn=LDAPSRV)"
```

```
cn=LDAPSRV,o=VMAssist,c=US  
objectclass=top  
objectclass=person  
objectclass=ibm-nativeAuthentication  
description=Administrator  
cn=LDAPSRV  
sn=Administrator  
ibm-nativeid=LDAPSRV
```

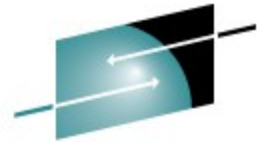
Using z/VM LDAP with Linux



SHARE
Technology • Connections • Results

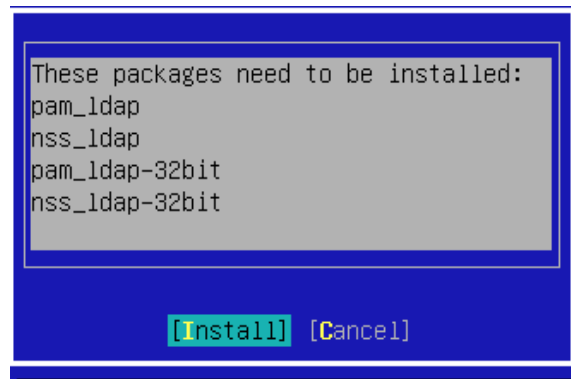
- LDAP provides a way to keep a repository of security information in a centralized place
 - Previously this could have been done with NIS
- The LDAP Server running on z/VM
 - Brings the power and capabilities of RACF to security management on Linux
 - LDAP clients (virtual machines or real machines) can authenticate with RACF
 - Passwords can be synchronized with z/VM

Using z/VM LDAP with Linux



SHARE
Technology • Connections • Results

- Prerequisite software
 - openldap2-client, pam-ldap, nss-ldap, +32-bit versions and yast2-ldap
- While configuring the LDAP client, if the prereq software is not installed, YaST will perform the install automatically



Using z/VM LDAP with Linux

- Configure LDAP client with YaST

```
rks0 : telnet
File Edit View Scrollback Bookmarks Settings Help
YaST2 - ldap @ ldap11

LDAP Client Configuration

User Authentication
( ) Do Not Use LDAP
(x) Use LDAP
( ) Use LDAP but Disable Logins

LDAP Client
Addresses of LDAP Servers
192.168.1.50
LDAP Base DN
o=VMAssist,c=US
[ ] LDAP TLS/SSL
[ ] LDAP Version 2

[ ] Start Automounter
[x] Create Home Directory on Login
[Advanced Configuration...]

[ Help ]          [Cancel]
F1 Help  F8 Cancel  F10 OK
```

```
rks0 : telnet
File Edit View Scrollback Bookmarks Settings Help
YaST2 - ldap @ ldap11

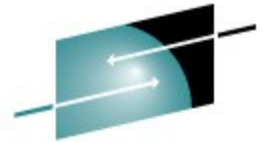
Advanced Configuration
Client Settings—Administration Settings—
Naming Contexts
User Map
o=VMAssist,c=US [Browse]
Password Map
o=VMAssist,c=US [e]
Group Map
o=VMAssist,c=US [use]

Password Change Protocol
racf

Group Member Attribute
member

[ Help ]          [Cancel]          [ OK ]
F1 Help  F8 Cancel  F10 OK
```

Using z/VM LDAP with Linux



SHARE
Technology • Connections • Results

- Review `/etc/ldap.conf`

```
Host                192.168.1.50
base                o=VMAssist,c=US
bind_policy         soft
pam_lookup_policy   yes
pam_password        racf
nss_initgroups_ignoreusers  root,ldap
nss_schema          rfc2307bis
nss_map_attribute   uniqueMember member
ssl                 no
ldap_version        3
pam_filter          objectClass=posixAccount
tls_checkpeer       no
```

Using z/VM LDAP with Linux

- YaST did not add the following to ldap.conf

```
binddn cn=LDAPSRV,o=VMAssist,c=US
bindpw vmpass
nss_base_passwd o=VMAssist,c=US
nss_base_shadow o=VMAssist,c=US
nss_base_group o=VMAssist,c=US
```

- These entries are very critical to the operation of the LDAP client
- No other LDAP client config changes required
 - ...on SLES 11
 - SLES 10 SP2 required additional changes
 - SHARE 111 or 112 presentations
 - zJournal article “Configuring Linux to Authenticate to the z/VM LDAP Server” April/May, 2009

Using z/VM LDAP with Linux

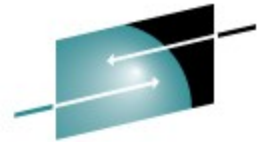
- Add Linux user to RACF

```
RAC ADDUSER RKS1 PASSWORD(PWORD)
```

- Create LDIF file to add Linux user to LDBM database

```
dn: cn=RKS1,o=VMAssist,c=US
objectclass: person
objectclass: ibm-nativeAuthentication
objectclass: posixAccount
description: Rich Smrcina
telephoneNumber: 414-491-6001
uidnumber: 2000
gidnumber: 100
uid: rks1
homedirectory: /home/rks1
loginshell: /bin/bash
cn: Rich
sn: Smrcina
ibm-nativeId: RKS1
```

Using z/VM LDAP with Linux



SHARE
Technology • Connections • Results

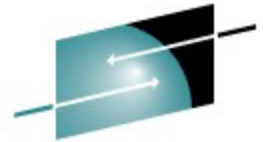
- Add the entry

```
ldapadd -h 127.0.0.1 -w vmpass -D "cn=LDAPSRV,o=VMAssist,c=US"  
-f //rks1.ldif  
adding new entry cn=RKS1,o=VMAssist,c=US
```

- Check it...

```
ldapsrch -h 127.0.0.1 -w vmpass -D "cn=LDAPSRV,o=VMAssist,c=US"  
-b "o=VMAssist,c=US" "(cn=RKS1)"  
cn=RKS1,o=VMAssist,c=US  
objectclass=person  
objectclass=ibm-nativeAuthentication  
objectclass=posixAccount  
objectclass=top  
description=Rich Smrcina  
telephonenumber=414-491-6001  
uidnumber=2000  
gidnumber=100  
uid=rks1  
homedirectory=/home/rks1  
loginshell=/bin/bash  
...
```


Using z/VM LDAP with Linux



SHARE

Technology • Connections • Results

```
rks0@laptop:~> telnet 192.168.240.20
Trying 192.168.240.20...
Connected to 192.168.240.20.
Escape character is '^]'.
Welcome to SUSE Linux Enterprise Server 11 (s390x) - Kernel
2.6.27.19-5-default(2).
```

```
ldap11 login: rks1
Password:
Creating directory '/home/rks1'.
Creating directory '/home/rks1/bin'.
Creating directory '/home/rks1/.fonts'.
Creating directory '/home/rks1/.mozilla'.
Directory: /home/rks1
Wed Aug 19 11:07:14 CDT 2009
rks1@ldap11:~> id
uid=2000(rks1) gid=100(users) groups=100(users)
```

Using z/VM LDAP with Linux



```
rks0@laptop:~> ssh rks1@192.168.240.20
Password:
Last login: Wed Aug 19 11:07:03 2009 from 192.168.1.101
rks1@ldap11:~> id
uid=2000(rks1) gid=100(users) groups=100(users)
rks1@ldap11:~> ll
total 4
drwxr-xr-x 2 rks1 users 4096 2009-08-19 11:07 bin
```

Using z/VM LDAP with Linux



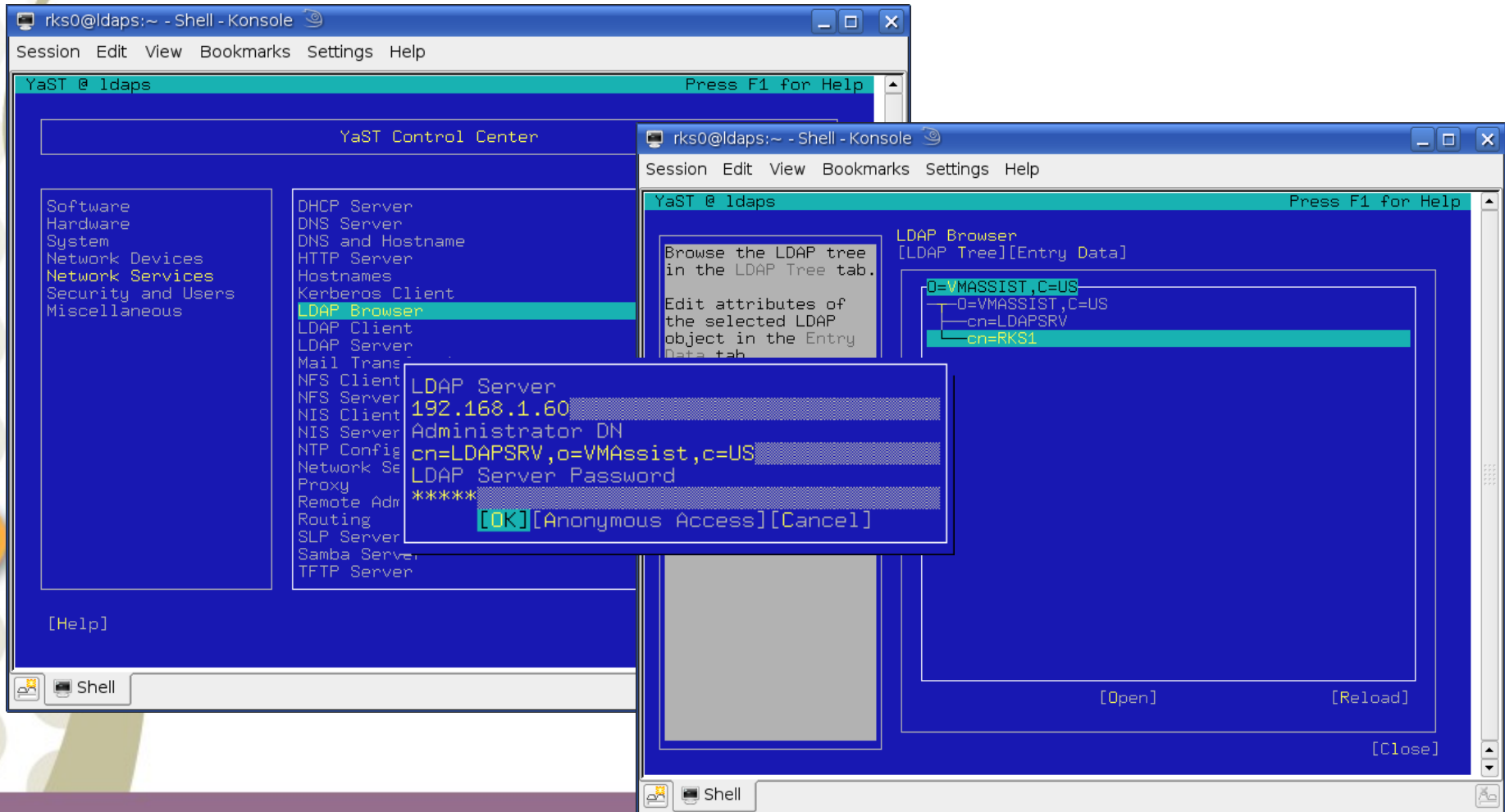
```
rks0@laptop:~> ftp 192.168.240.20
Connected to 192.168.240.20.
220 (vsFTPd 2.0.7)
Name (192.168.240.20:rks0): rks1
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
229 Entering Extended Passive Mode (|||30082|)
150 Here comes the directory listing.
drwxr-xr-x    2 2000      100          4096 Aug 19 16:07 bin
226 Directory send OK.
```

- **Log file entry from FTP login**

```
Aug 19 11:28:20 ldap11 vsftpd: Wed Aug 19 11:28:20 2009 [pid 22971]
[rks1] OK LOGIN: Client "192.168.1.101"
```

Browsing the LDAP Directory

- With YaST



The image shows a YaST Control Center window with the 'LDAP Browser' option selected. A dialog box is open for configuring LDAP server details. The dialog contains the following fields:

- LDAP Server: 192.168.1.60
- Administrator DN: cn=LDAPSrv,o=VMAssist,c=US
- LDAP Server Password: *****

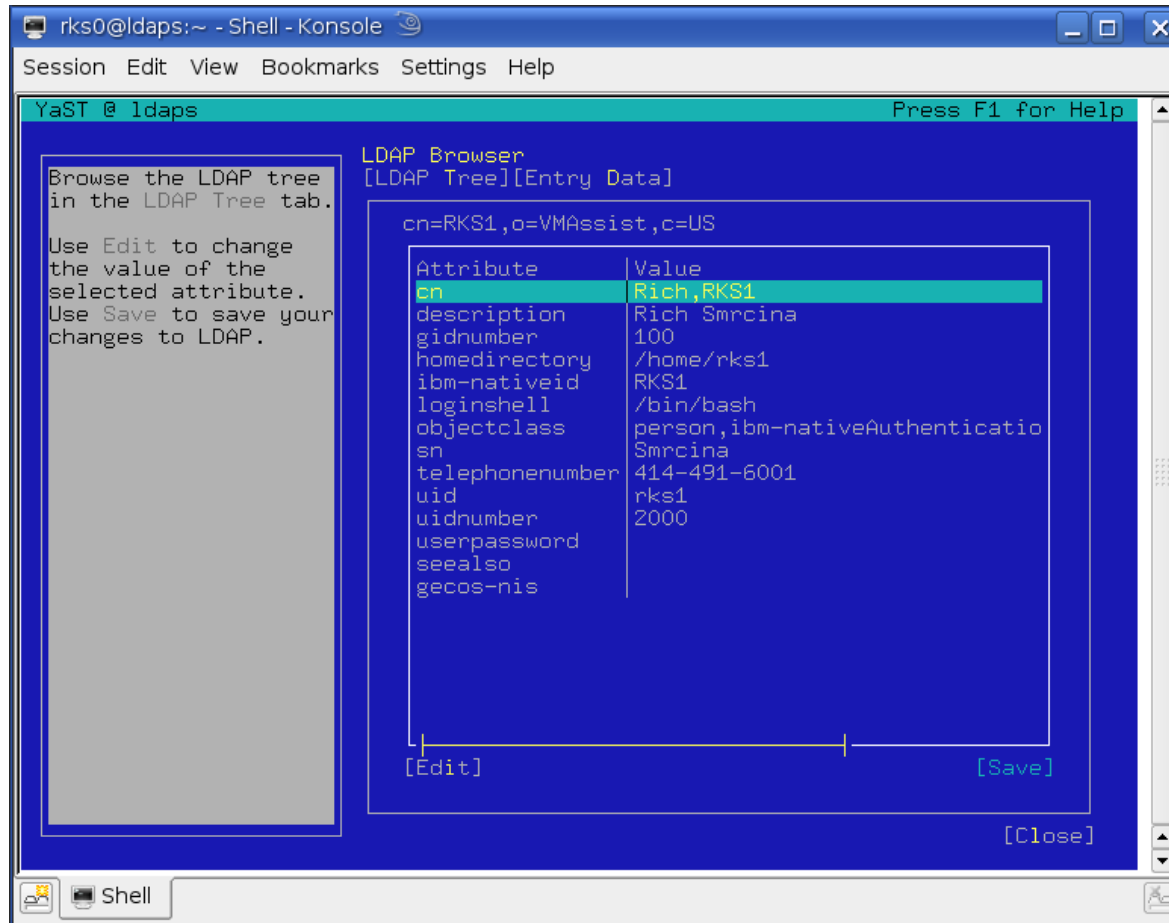
Buttons at the bottom of the dialog are [OK], [Anonymous Access], and [Cancel].

The background YaST window shows a tree view of the LDAP directory with the following structure:

- o=VMASSIST,C=US
 - o=VMASSIST,C=US
 - cn=LDAPSRV
 - cn=RKS1

Browsing the LDAP Directory

- With YaST



The screenshot shows a terminal window titled "rks0@ldaps:~ - Shell - Konsole". Inside the terminal, the YaST LDAP Browser is running. The window has a menu bar with "Session Edit View Bookmarks Settings Help" and a title bar "YaST @ ldaps" with "Press F1 for Help".

On the left side of the terminal, there is a grey box with the following text:

```
Browse the LDAP tree
in the LDAP Tree tab.

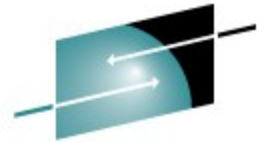
Use Edit to change
the value of the
selected attribute.
Use Save to save your
changes to LDAP.
```

The main area of the terminal displays the LDAP Browser interface. At the top, it says "LDAP Browser" and "[LDAP Tree][Entry Data]". Below this, the entry path is shown as "cn=RKS1,o=VMAssist,c=US".

Attribute	Value
cn	Rich,RKS1
description	Rich Smrcina
gidnumber	100
homedirectory	/home/rks1
ibm-nativeuid	RKS1
loginshell	/bin/bash
objectclass	person,ibm-nativeAuthenticatio
sn	Smrcina
telephonenumber	414-491-6001
uid	rks1
uidnumber	2000
userpassword	
seealso	
gecos-nis	

At the bottom of the terminal window, there are three buttons: "[Edit]", "[Save]", and "[Close]".

Browsing the LDAP Directory



SHARE
Technology • Connections • Results

- With YaST2

Browse the LDAP tree in the **LDAP Tree** tab.

Use **Edit** to change the value of the selected attribute. Use **Save** to save your changes to LDAP.

LDAP Browser

LDAP Tree | Entry Data

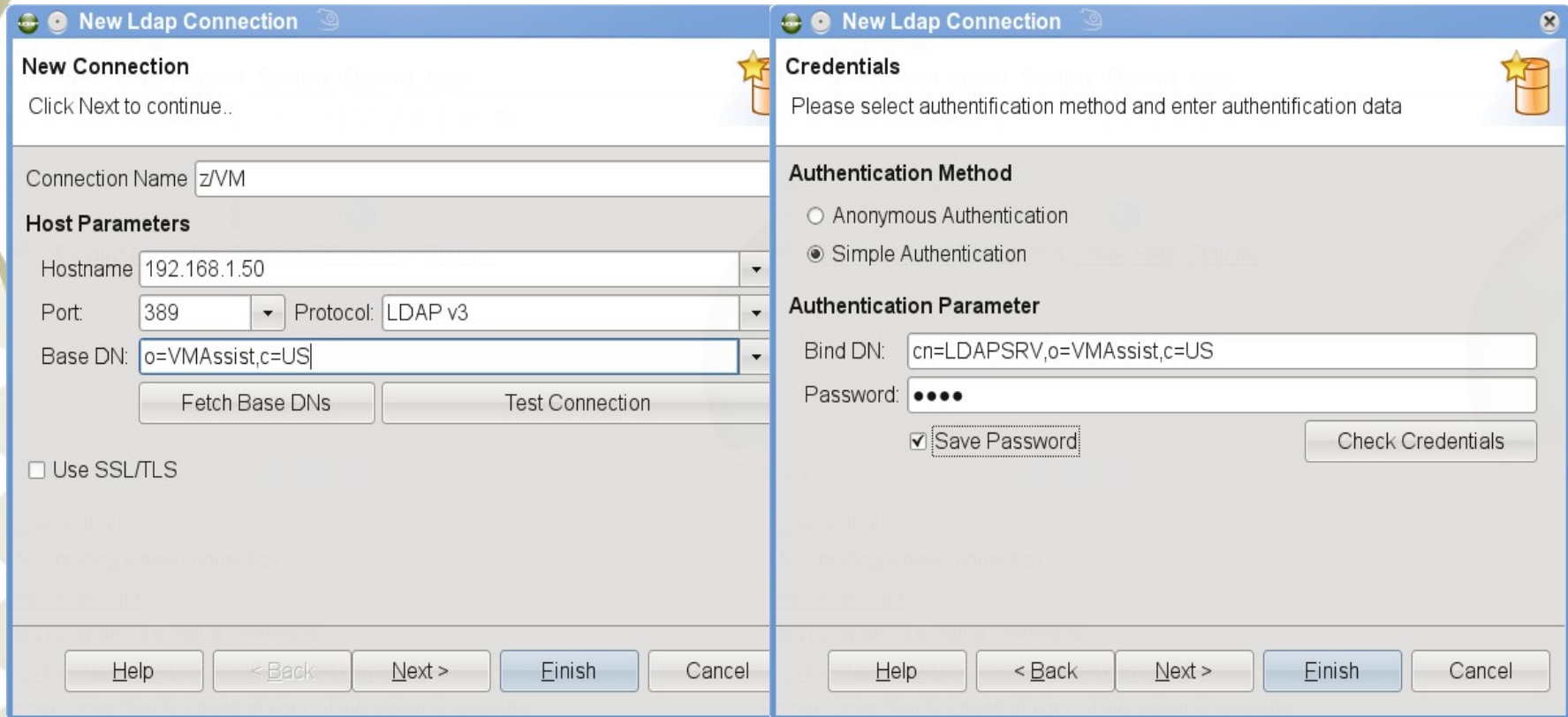
cn=RKS1,o=VMAssist,c=US

Attribute	Value
cn	Rich,RKS1
description	Rich Smrcina
gidnumber	100
homedirectory	/home/rks1
ibm-nativeid	RKS1
loginshell	/bin/bash
objectclass	person,ibm-nativeAuthentication,posixAccount,top
sn	Smrcina
telephonenumber	414-491-6001
uid	rks1
uidnumber	2000
userpassword	
seealso	
gecos-nis	

Edit Save Close

Browsing the LDAP Directory

- *LDAP Browser* from LDAPSoft (<http://www.ldapsoft.com>)



New Ldap Connection

New Connection
Click Next to continue..

Connection Name: z/VM

Host Parameters

Hostname: 192.168.1.50
Port: 389 Protocol: LDAP v3
Base DN: o=VMAssist,c=US

Fetch Base DNS Test Connection

Use SSL/TLS

Help < Back Next > Finish Cancel

New Ldap Connection

Credentials
Please select authentication method and enter authentication data

Authentication Method

Anonymous Authentication
 Simple Authentication

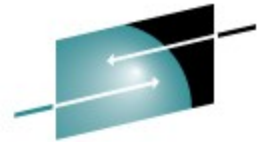
Authentication Parameter

Bind DN: cn=LDAPSRV,o=VMAssist,c=US
Password: ●●●●

Save Password Check Credentials

Help < Back Next > Finish Cancel

Browsing the LDAP Directory



SHARE

Technology • Connections • Results

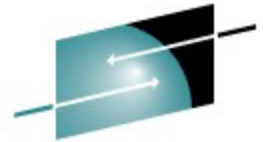
- Comes in Windows and Linux flavors
- Provides an SQL interface and LDIF import and export
- A commercial product is available that provides editing

The screenshot shows the LDAPSoft - LDAP Browser application. The search criteria are set to 'cn'. The left pane shows the directory tree with 'o=VMAssist,c=US' expanded to 'cn=LDAPSRV' and 'cn=RKS1' selected. The main pane displays a table of attributes for the selected entry.

Attribute Name	Value	Size	Type	Required
objectclass	person	6	ObjectClass	Y
objectclass	ibm-nativeAuthentication	24	ObjectClass	Y
objectclass	posixAccount	12	ObjectClass	Y
objectclass	top	3	ObjectClass	Y
cn	RichSmrcina	11	Text	Y
cn	rks1	4	Text	Y
gidnumber	100	3	Integer	Y
homedirectory	/home/rks1	10	Text	Y
ibm-nativeid	RKS1	4	Text	Y
sn	Smrcina	7	Text	Y
uid	rks1	4	Text	Y
uidnumber	2000	4	Integer	Y
<i>createtimestamp</i>	20090818161716.449545Z	22	Operational	N
<i>creatorsname</i>	cn=LDAPSRV,o=VMAssist,c=US	26	Operational	N
<i>description</i>	Rich Smrcina	12	Text	N
<i>loginshell</i>	/bin/bash	9	Text	N
<i>modifiersname</i>	cn=LDAPSRV,o=VMAssist,c=US	26	Operational	N
<i>modifytimestamp</i>	20090818161716.449545Z	22	Operational	N
<i>subschemasubentry</i>	cn=schema	9	Operational	N
<i>telephonenumber</i>	414-491-6001	12	Telephone N	N
<i>gecos-nis</i>		0	Text	N
<i>seeAlso</i>		0	Text	N
<i>userPassword</i>		0	userPasswo	N

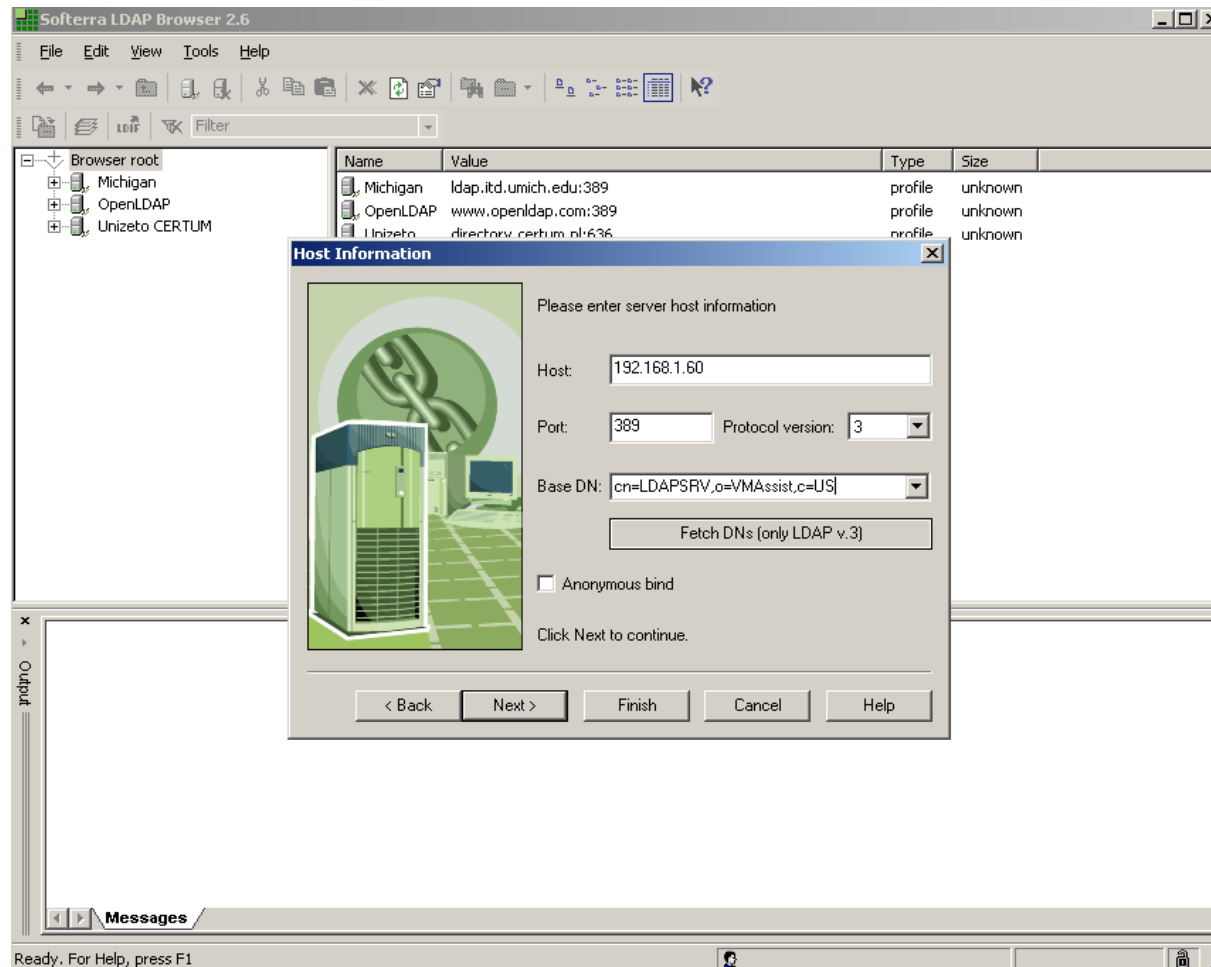
At the bottom of the window, it shows '1 items selected' and the entry path 'cn=LDAPSRV,o=VMAs: 8 : 6 : 23'.

Browsing the LDAP Directory

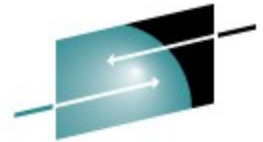


SHARE
Technology • Connections • Results

- Softerra LDAP Browser (<http://www.Idapbrowser.com>)



Browsing the LDAP Directory



SHARE
Technology • Connections • Results

- Softerra LDAP Browser (<http://www.ldapbrowser.com>)

The screenshot shows the Softerra LDAP Browser window. The title bar reads "cn=RK51,o=VMAssist,c=US". The interface includes a menu bar (File, Edit, View, Tools, Help), a toolbar with navigation icons, and a search filter set to "(objectClass=*)".

The left pane shows a tree view of the LDAP directory structure:

- Browser root
 - Michigan
 - OpenLDAP
 - Unizeto CERTUM
 - zvm
 - cn=LDAPSRV
 - ou=ldapconfig
 - cn=RK51

The right pane displays a table of attributes for the selected entry:

Name	Value	Type	Size
objectclass	person	text attribute	6
objectclass	ibm-nativeAuthentication	text attribute	24
objectclass	posixAccount	text attribute	12
objectclass	top	text attribute	3
description	Rich Smrcina	text attribute	12
telephonenumber	414-491-6001	text attribute	12
uidnumber	2000	text attribute	4
gidnumber	100	text attribute	3
uid	rks1	text attribute	4
homedirectory	/home/rks1	text attribute	10
loginshell	/bin/bash	text attribute	9
cn	Rich	text attribute	4
cn	RK51	text attribute	4
sn	Smrcina	text attribute	7
creatorsname	cn=LDAPSRV,o=VMAssist,c=US	operational attribute	26
createtimestamp	20080711155417.653630Z	operational attribute	22
modifiersname	cn=LDAPSRV,o=VMAssist,c=US	operational attribute	26
modifytimestamp	20080711155417.653630Z	operational attribute	22
subschemasubentry	cn=schema	operational attribute	9

The bottom pane shows a status message:

```
Successfully connected to 192.168.1.60
Schema has been cached. Using cache...
LDAP Syntaxes: Total: 22 Invalid: 0 Duplicated: 0
AttributeTypes: Total: 1228 Invalid: 0 Duplicated: 0
LDAPObjectClasses: Total: 321 Invalid: 0 Duplicated: 0
MatchingRules: Total: 22 Invalid: 0 Duplicated: 0
MatchingRulesUse: Total: 0 Invalid: 0 Duplicated: 0
```

The status bar at the bottom indicates "Ready. For Help, press F1", "Anonymous" user, and "Schema loaded".

Setting up other software - Apache

- In `/etc/sysconfig/apache2` add to `APACHE_MODULES=`
`ldap authnz_ldap`
- In the Apache configuration

```
ScriptAlias /hobbit-seccgi/ "/home/hobbit/cgi-secure/"
Directory "/home/hobbit/cgi-secure">
    AllowOverride None
    Options ExecCGI Includes
    Order allow,deny
    Allow from all

    AuthType Basic
    AuthName "Hobbit Administration"
    AuthBasicProvider ldap
    AuthzLDAPAuthoritative off
    AuthLDAPBindDN cn=LDAPSRV,o=VMAssist,c=US
    AuthLDAPBindPassword *****
    AuthLDAPURL ldap://192.168.1.60/o=VMAssist,c=US?uid?sub NONE

    Require valid-user
</Directory>
```



Setting up other software - SugarCRM

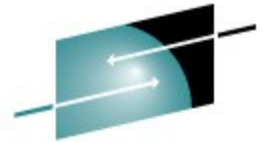
- SugarCRM is an open source customer resource management (CRM) package
- It uses the LAMP (Linux, Apache, MySQL, PHP) software stack
- Sugar offers an LDAP authentication option
 - In System Settings

LDAP Authentication Support

Enable LDAP	<input checked="" type="checkbox"/>	
Server:	<input type="text" value="192.168.1.50"/>	Example: ldap.example.com
Port Number:	<input type="text" value="389"/>	Example: 389
Base DN:	<input type="text" value="ou=vm,dc=vmassist,dc=com"/>	Example: DC=SugarCRM,DC=com
Bind Attribute:	<input type="text" value="dn"/>	For Binding the LDAP User Examples:[AD: userPrincipalName] [openLDAP: userPrincipalName] [Mac OS X: uid]
Login Attribute:	<input type="text" value="uid"/>	For searching for the LDAP User Examples:[AD: userPrincipalName] [openLDAP: dn] [Mac OS X: dn]
Authenticated User:	<input type="text" value="cn=admin,ou=vm,dc=vmassist,dc=com"/>	Used to search for the Sugar user. [May need to be fully qualified] It will bind anonymously if not provided.
Authenticated Password:	<input type="password" value="*****"/>	
Auto Create Users:	<input checked="" type="checkbox"/>	If an authenticated user does not exist one will be created in Sugar.
Encryption Key:	<input type="text"/>	For SOAP authentication when using LDAP.



Setting up other software - SugarCRM



SHARE

Technology • Connections • Results

SugarCRM - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://192.168.202.17/sugar/index.php?action=Login&r

SUGARCRM.
COMMERCIAL OPEN SOURCE

My Account | Employees | Training | About

Welcome to
SUGARCOMMUNITY EDITION.

Please enter your user name and password:

User Name:

Password:

[Options](#)

Login

Server response time: 38.87 seconds.
© 2004-2008 SugarCRM Inc. The Program is provided AS IS, without warranty. Licensed under [GPLv3](#).
This program is free software; you can redistribute it and/or modify it under the terms of the [GNU General Public License version 3](#) as published by the Free Software Foundation including the additional permission set forth in the

POWERED BY
SUGARCRM.

Done

SugarCRM - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://192.168.202.17/sugar/index.php?module=Home

SUGARCRM.
COMMERCIAL OPEN SOURCE

Welcome, rks1 [Logout] | My Account | Employees | Training | About

Home | Dashboard | Calendar | Activities | Emails | Documents | Contacts | Accounts | Campaigns | Leads | Opportunities | Projects

Last Viewed: none

Shortcuts

- Create Contact
- Enter Business Card
- Create Account
- Create Lead
- Create Opportunity
- Create Case
- Report Bug
- Schedule Meeting
- Schedule Call
- Create Task
- Compose Email

New Contact

First Name:

Last Name:

Office Phone:

Email:

Assigned to: [Select](#)

[Save](#)

My Calls (0 - 0 of 0)

Close	Subject	Duration	Start Date	Accept?
-------	---------	----------	------------	---------

My Meetings (0 - 0 of 0)

Close	Subject	Duration	Start Date	Accept?
-------	---------	----------	------------	---------

My Leads (0 - 0 of 0)

Name	Office Phone	Date Created
------	--------------	--------------

My Accounts (0 - 0 of 0)

Account Name	Phone	Date Entered
--------------	-------	--------------

Add Sugar Dashlets ? Help

JotPad Double click below to Edit.

Welcome to Sugar 5.1!

Click **My Account** to set your preferences.
Click the **Question Mark** icon to access the Help page for each module.

For assistance with getting started, click the **Training** link to find out about training offered through **Sugar University**.

My Open Cases (0 - 0 of 0)

Number	Subject	Priority	Status
--------	---------	----------	--------

My Top Open Opportunities (0 - 0 of 0)

Opportunity Name	Amount	Expected Close Date
------------------	--------	---------------------

Done

Monitoring

- LDAP Server keep statistics during it's operation
- An LDAP Search can be used to collect the statistics

```
ldapsrch -h 127.0.0.1 -s base -b cn=monitor "(objectclass=*)"
```

- Monitor stats can also be collected using SMSG

```
SMSG LDAPSRV DISPLAY MONITOR
```

- Stats can be reset via SMSG

```
SMSG LDAPSRV RESET MONITOR
```

- Statistics are not available over SNMP

- Format of the statistics

```
ldapsrch -h 127.0.0.1 -s base -b cn=monitor "(objectclass=*)"
```

```
cn=monitor
```

```
version=z/VM Version 5 Release 3 IBM LDAP Server
```

```
liveshreads=10
```

```
maxconnections=65523
```

```
sysmaxconnections=65535
```

```
totalconnections=29
```

```
currentconnections=2
```

```
maxreachedconnections=5
```

```
opsinitiated=81
```

```
opscompleted=80
```

```
abandonsrequested=4
```

```
abandonscompleted=4
```

```
addsrequested=0
```

```
addscompleted=0
```

```
bindsrequested=25
```

```
bindscompleted=25
```

```
comparesrequested=0
```

```
comparescompleted=0
```

```
deletesrequested=0
```

```
deletescompleted=0
```

```
extopsrequested=0
```

```
modifiesrequested=0
```

```
modifiescompleted=0
```

```
modifydnsrequested=0
```

```
modifydnscompleted=0
```

```
searchesrequested=31
```

```
searchescompleted=30
```

```
unbindsrequested=21
```

```
unbindscompleted=21
```

```
unknownopsrequested=0
```

```
unknownopscompleted=0
```

```
entriessent=17
```

```
bytessent=5992
```

```
searchreferencessent=0
```

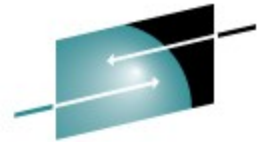
```
currenttime=Sat Jul 26 02:34:13.340516 2008
```

```
starttime=Sat Jul 26 01:15:05.412192 2008
```

```
resetttime=Sat Jul 26 01:15:05.412192 2008
```

```
resets=0
```

Monitoring



- Format of the statistics

```
smsg ldapsrv display monitor
```

```
Ready; T=0.01/0.01 21:45:22
```

```
Monitor Statistics
```

```
-----
```

```
Server Version:      z/VM Version 5 Release 3 IBM  
                    LDAP Server
```

```
Current Time:       Sat Jul 26 02:45:22.575461 2008
```

```
Start Time:         Sat Jul 26 01:15:05.412192 2008
```

```
Last Reset Time:   Sat Jul 26 01:15:05.412192 2008
```

```
Number of Resets:  0
```

```
Server Totals:
```

```
-----
```

```
Description          Count
```

```
-----
```

```
Config Max Connections 65523
```

```
System Max Connections 65535
```

```
Total Connections      31
```

```
Current Connections     1
```

```
MaxReached Connections  5
```


Operating the LDAP Server

- Startup
 - TCP/IP will start it
- Shutdown

MSG LDAPSRV SHUTDOWN

```
090822 13:16:35.083425 GLD1007I LDAP server is stopping.
```

```
090822 13:16:35.234857 GLD6051I No database changes to commit  
for LDBM backend named LDBM-0001.
```

```
Options Report for Enclave main 08/22/09 8:16:35 AM
```

```
Language Environment V01 R09.00
```

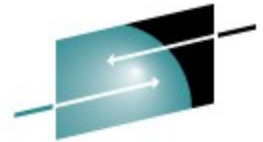
```
...
```

```
DTCRUN1014I Server ended normally at 08:16:35 on 22 Aug 2009  
(Saturday)
```

```
RPICMS017I USER/RACF VM Racroute communication path has been  
terminated.
```

- Does not listen to the shutdown signal

Operating the LDAP Server



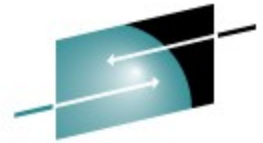
SHARE
Technology • Connections • Results

- The SMSG interface also provides the following
 - Auditing Controls
 - Setting the backends to read only or read-write
 - Commit changes
 - Set debugging levels
 - Display LDAP Server information
 - Logging control (on/off)
 - Set normal or maintenance mode
 - Initialize SSL environment
 - Reset counters

References

- z/VM V5R4.0 TCP/IP Planning and Customization - SC24-6125
- z/VM V5R4.0 TCP/IP LDAP Administration Guide - SC24-6140
- z/VM V5R4.0 TCP/IP User's Guide - SC24-6127
- Essential System Administration, Eelen Frisch
 - 3rd Edition, August 2002, Published by O'Reilly
- LDAP System Administration, Gerald Carter
 - March 2003, Published by O'Reilly
- Redbook: Security on z/VM - SG24-7471
- Redbook: Understanding LDAP - SG24-4986

Questions?



S H A R E

Technology • Connections • Results



Rich Smrcina
VM Assist, Inc.
<http://www.vmassist.com>
414-491-6001
rsmrcina@vmassist.com

Specializing in support of z/VM,
z/VSE and Linux on System z systems