Configuring LDAP on z/VM and Linux

Rich Smrcina
VM Assist

Session 9156
March 4, 2009
Presentation Materials

" SHARE Proceedings
" http://www.linuxvm.org
" http://sites.google.com/site/rsmrcina/presentations
Agenda

" 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
  " SugarCRM
  " z/VSE LDAP Client
  " Browsing/Editing Tools
  " Monitoring
Background

"This session is a companion to 9241 'Securing Linux with RACF on z/VM' by Alan Altmark

" We will get into more details about the configuration of LDAP
" But will not discuss/teach LDAP concepts

"Delivered with z/VM

" Currently based on IBM Tivoli Directory Server (ITDS) for z/OS 1.10
" ITDS 1.8 with z/VM 5.3
"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
  " Simplest setup
  " Can perform 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
  " Provides more comprehensive interface to the z/VM RACF Security Server
  " Allows password and password phrases verified by RACF

" GDBM Backend
  " Used for auditing changes to LDAP server
General Configuration

" TCP/IP Profile

PORT
  389 TCP LDAPSRV ; LDAP Server
  636 TCP LDAPSRV NOAUTOLOG ; LDAP Server (Secure)

AUTOLOG
  LDAPSRV 0

OBEY
  LDAPSRV
ENDOBEY

" The sample profile that comes with z/VM already provides these statements
General Configuration

" LDAP parameters in DTCPARMS

:nick.LDAPSRV :Type.server :Class.ldap
:nick.ldap     :Type.class
:ESM_Enable.
:ESM_Racroute.
:ESM_Validate.
:Mixedcaseparms.
:Mount.
:Parms.

" If using the SDBM backend
(or the LDBM backend with RACF), specify YES for
ESM_Enable

" Other ESM options can then default
General Configuration

" The mount tag is used to set up the ROOT file space for the LDAP server in the BFS

" Use the Parms 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
  " Parms 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 tailoroble

! Tip: Make sure the SFS file servers come up before
  TCP/IP

" The Message catalog files are stored in the ROOT file
  space

" The Schema databases are stored in the LDAP server
  users file space (default LDAPSRV)
General Configuration

" 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 administrator password
  adminPW secret

" In the LDBM Section
  " Uncomment the database keyword
  database LDBM GLDBLD31
  " Uncomment the suffix keyword and change the Distinguished Name
  suffix "ou=vm,dc=VMAssist,dc=com"
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 10:47:17 on 10 Dec 2008 (Wednesday)
DTCRUN1011I Running server command: LDAPSRV
DTCRUN1011I No parameters in use
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
081210 16:47:18.476413 GLD1003I LDAP server is starting.
081210 16:47:18.873245 GLD1023I Processing configuration file //DD:CONFIG.

Server Configuration
adminDN: cn=Admin
adminDN: cn=Admin
adminPW: *configured*
allowAnonymousBinds: on
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
tsrvStartUpError: 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: off
persistentSearch: off
pwEncryption: none
pwCryptCompat: on
readOnly: off
secretEncryption: none
sizeLimit: 500
suffix 1: ou=vm,dc=vmassist,dc=com
timeLimit: 3600
useNativeAuth: off
081210 16:47:24.252327 GLD1191I LDAP server auditing is not available.
081210 16:47:24.965361 GLD1074W Maximum client connections changed from 65535 to 65523.
081210 16:47:25.032070 GLD1004I LDAP server is ready for requests.


081210 16:47:26.177932 GLD1059I Listening for requests on 127.0.0.1 port 389.
LDAP Checkout

" Netstat output

VM TCP/IP Netstat Level 530

Active IPv4 Transmission Blocks:

<table>
<thead>
<tr>
<th>User Id</th>
<th>Conn</th>
<th>Local Socket</th>
<th>Foreign Socket</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTPSERVE</td>
<td>1003</td>
<td>*..FTP-C</td>
<td><em>..</em></td>
<td>Listen</td>
</tr>
<tr>
<td>INTCLIEN</td>
<td>1000</td>
<td>*..TELNET</td>
<td><em>..</em></td>
<td>Listen</td>
</tr>
<tr>
<td>INTCLIEN</td>
<td>1004</td>
<td>192.168.1.50..TELNET</td>
<td>192.168.1.102..53609</td>
<td>Established</td>
</tr>
<tr>
<td>INTCLIEN</td>
<td>1007</td>
<td>192.168.1.50..TELNET</td>
<td>192.168.1.102..44514</td>
<td>Established</td>
</tr>
<tr>
<td>INTCLIEN</td>
<td>1012</td>
<td>192.168.1.50..TELNET</td>
<td>192.168.1.102..50912</td>
<td>Established</td>
</tr>
<tr>
<td>PERFSVM</td>
<td>1005</td>
<td>*..81</td>
<td><em>..</em></td>
<td>Listen</td>
</tr>
<tr>
<td>PERFSVM</td>
<td>1002</td>
<td>192.168.1.50..81</td>
<td>192.168.1.102..44455</td>
<td>Established</td>
</tr>
<tr>
<td>PERFSVM</td>
<td>1006</td>
<td>192.168.1.50..81</td>
<td>192.168.1.102..44456</td>
<td>Established</td>
</tr>
<tr>
<td>SNMPD</td>
<td>UDP</td>
<td>192.168.1.50..161</td>
<td>192.168.1.102..44455</td>
<td>UDP</td>
</tr>
<tr>
<td>SNMPD</td>
<td>UDP</td>
<td>192.168.202.1..161</td>
<td>192.168.1.102..44456</td>
<td>UDP</td>
</tr>
<tr>
<td>SNMPD</td>
<td>1001</td>
<td>*..1024</td>
<td><em>..</em></td>
<td>Listen</td>
</tr>
<tr>
<td>LDAPSRV</td>
<td>1008</td>
<td>192.168.1.50..389</td>
<td><em>..</em></td>
<td>Listen</td>
</tr>
<tr>
<td>LDAPSRV</td>
<td>1009</td>
<td>192.168.202.1..389</td>
<td><em>..</em></td>
<td>Listen</td>
</tr>
<tr>
<td>LDAPSRV</td>
<td>1010</td>
<td>127.0.0.1..389</td>
<td><em>..</em></td>
<td>Listen</td>
</tr>
</tbody>
</table>
LDAP Checkout

```
pwd
/var/ldap
#
ls -lR

.:
total 0
drwxr----- 1 ldapsrv system 0 Dec 10 16:47 ldbm
drwxr----- 1 ldapsrv system 0 Dec 10 18:45 schema

./ldbm:
total 16
-rw-r----- 1 ldapsrv system 45 Dec 10 16:16 LDBM-1.db
-rw-r----- 1 ldapsrv system 37 Dec 10 16:47 LDBM.ckpt

./schema:
total 424
-rw-r----- 1 ldapsrv system 216015 Dec 10 18:45 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 (LDAPMDFY), ldapcompare (LDAPCMPR), ldapdelete (LDAPDLET), ldapmodrdn (LDAPMRDN)

" We will use the LDAPSrch command

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

" ...the database is empty
LDAP Checkout

" The same command from Linux

> ldapsearch -h 192.168.1.50 -x -w secret -s base -b "ou=vm,dc=VMAssist,dc=com" "objectclass=*"
# extended LDIF
#
# LDAPv3
# base <ou=vm,dc=vmassist,dc=com> with scope subtree
# filter: objectclass=*  
# requesting: ALL
#

# search result
search: 2
result: 32 No such object
text: R004071 DN 'ou=vm,dc=vmassist,dc=com' does not exist
(ldbms_process_request)

# numResponses: 1

" ... 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 secret -f //USRSCHEM.LDIF -u on
ldapmdfy -h 127.0.0.1 -D "cn=Admin" -w secret -f //IBMSCHEM.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
  "  SG24-7471

" Get the schema from
  "  ftp://www.redbooks.ibm.com/redbooks/REDP0221/nisSchema.2.ldif

" Upload file to z/VM

" Modify line 5
  "  From “dn:cn=schema, <suffix>” to “dn:cn=schema”

" Update schema on the LDAP Server

ldapmodify -h 127.0.0.1 -D cn=Admin -w secret -f //NISSCHEM.LDIF -u on
modifying entry cn=schema
" In this simple setup the administrator will be a user called 'Admin'

" Create an **LDAP Data Interchange Format** file (LDIF)
  " A sample exists as SAMPSERV LDIF on TCPMAINTs 591 disk
  " The first two entries of the file were used as examples in the following scenario
Setup admin access

" In a file called ADMIN LDIF

dn: ou=vm, dc=vmassist, dc=com
objectclass: top
objectclass: organizationalUnit
ou: vm

dn: cn=Admin, ou=vm, dc=vmassist, dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
cn: LDAP Administrator
sn: Administrator
userPassword: secret

File actually contains two entries

" One to add the organizational unit (ou=vm, dc=vmasssist,dc=com)
" The other to add the administrator (cn=Admin)
Setup admin access

" Use ldapadd to insert the entries into the LDBM database

```bash
ldapadd -h 127.0.0.1 -w secret -D "cn=Admin" -f //admin.ldif
adding new entry ou=vm, dc=vmassist, dc=com
adding new entry cn=Admin, ou=vm, dc=vmassist, dc=com
Ready; T=0.22/0.30 10:43:06
```

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

```bash
adminDN "cn=Admin, ou=vm, dc=VMAssist, dc=com"
#adminPW secret
```

" Turn off anonymous binds (optionally)

" Restart the LDAP Server

" The new adminDN comes out in the configuration summary
Setup admin access

" Use ldapsrch to check on the LDAPSRV entry just made

```
ldapsrch -h 127.0.0.1 -D "cn=Admin,ou=vm,dc=vmassist,dc=com" -w secret -b "ou=vm,dc=vmassist,dc=com" "(cn=Admin)"
cn=Admin, ou=vm, dc=vmassist, dc=com
objectclass=top
objectclass=person
objectclass=organizationalPerson
cn=LDAP Administrator
cn=Admin
sn=Administrator
userpassword=secret
```
Using z/VM LDAP with Linux

" 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

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
Using z/VM LDAP with Linux

Review /etc/ldap.conf

```
host    192.168.1.50
base    ou=vm,dc=vmassist,dc=com
ldap_version    3
bind_policy     soft
binddn    cn=LDAPSRV,o=VMAssist,c=US
bindpw    ********
pam_lookup_policy       yes
pam_password    crypt
ssl     no
nss_map_attribute       uniqueMember member
pam_filter   objectclass=posixAccount
tls_checkpeer    no
```
Using z/VM LDAP with Linux

" YaST should reconfigure several other files
  " /etc/nsswitch.conf, /etc/security/, /etc/pam.d/
  " YaST's modifications needed tweaking

" In /etc/nsswitch.conf
  " The following entries should be modified
    passwd: files ldap
group: files ldap
  " Remove the lines
    passwd_compat: ldap
group_compat: ldap

" In /etc/security/pam_unix2.conf
  " Remove the ldap values from
    auth:
    account:
    password:
  " Leave the lines in place
Using z/VM LDAP with Linux

" In /etc/pam.d/common-auth
   " Insert
   auth sufficient pam_ldap.so
   " Before
   auth required pam_unix2.so

" In /etc/pam.d/common-account
   " Insert
   account sufficient pam_ldap.so
   " Before
   account required pam_unix2.so
Using z/VM LDAP with Linux

" In /etc/pam.d/common-password
  " Insert
  password   sufficient     pam_ldap.so
  " Before
  password   required       pam_unix2.so

" In /etc/pam.d/common-session
  " Insert
  session    sufficient     pam_ldap.so
  " Before
  session    required       pam_unix2.so

" These files are included by PAM service configuration files in the same directory (login, ssh, passwd)
Using z/VM LDAP with Linux

" Create LDIF file to add Linux user to LDBM database

dn: cn=RKS1,ou=vm,dc=VMAssist,dc=US
objectclass: person
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
userPassword: secret

" Add the entry

ldapadd -h 127.0.0.1 -w secret -D "cn=admin,ou=vm,dc=VMAssist,dc=US" -f //rks1.ldif
adding new entry cn=RKS1, ou=vm, dc=VMAssist, dc=US
Using z/VM LDAP with Linux

rks0@laptop:~> telnet 192.168.202.17
Trying 192.168.202.17...
Escape character is '^]'.
Welcome to SUSE Linux Enterprise Server 10 SP2 (s390x) - Kernel 2.6.16.60-0.21-default (1).

sugar login: rks1
Password:
Creating directory '/home/rks1'.
Creating directory '/home/rks1/.fonts'.
Creating directory '/home/rks1/.mozilla'.
Creating directory '/home/rks1/.xemacs'.
Creating directory '/home/rks1/bin'.
Creating directory '/home/rks1/Documents'.
Creating directory '/home/rks1/public_html'.
rks1@sugar:~> pwd
/home/rks1
rks1@sugar:~> id
uid=2000(rks1) gid=100(users) groups=100(users)
Using z/VM LDAP with Linux

rks0@desktop:~> ssh rks1@192.168.202.17
Password:
rks1@sugar:~> id
uid=2000(rks1) gid=100(users) groups=100(users)
rks1@sugar:~> ll
total 12
drwxr-xr-x 2 rks1 users 4096 2009-01-05 11:43 bin
drwxr-xr-x 2 rks1 users 4096 2009-01-05 11:43 Documents
drwxr-xr-x 2 rks1 users 4096 2009-01-05 11:43 public_html
"The vsftpd pam configuration file does not participate in the 'common' configuration that is made available by SUSE

"It will need to be modified manually in order to authenticate with LDAP

"In /etc/pam.d/vsftpd

"Insert
auth sufficient pam_ldap.so
"Before
auth required pam_unix2.so

"Insert
account sufficient pam_ldap.so
"Before
account required pam_unix2.so
Using z/VM LDAP with Linux

rks0@laptop:~> ftp 192.168.202.17
220 (vsFTPD 2.0.4)
Name (192.168.202.17:rks0): rks1
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
257 "/home/rks1"

Log file entry from FTP login

Jan  5 12:05:33 sugar vsftpd: Mon Jan  5 12:05:33 2009 [pid 18459]
[rks1] OK LOGIN: Client "192.168.1.101"
Browsing the LDAP Directory

" With YaST
Browsing the LDAP Directory

"With YaST"
Browsing the LDAP Directory

With YaST2
Browsing the LDAP Directory

"LDAP Browser from LDAPSof (http://www.ldapsoft.com)"
Browsing the LDAP Directory

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

" Default configuration is to not encrypt the password

" To prevent the viewing of passwords while browsing the LDAP directory the server provides various ways to encrypt stored passwords
  " crypt, MD5, SHA, DES and AES

" In the LDBM section, the pwEncryption option determines the method used to encrypt the password

<table>
<thead>
<tr>
<th>pwEncryption SHA</th>
</tr>
</thead>
<tbody>
<tr>
<td>uid number</td>
</tr>
<tr>
<td>userpassword</td>
</tr>
<tr>
<td>seealso</td>
</tr>
<tr>
<td>rks1</td>
</tr>
<tr>
<td>2000</td>
</tr>
<tr>
<td>secret</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>LDAP Authentication Support</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable LDAP</td>
<td>☑</td>
</tr>
<tr>
<td>Server:</td>
<td>192.168.1.50</td>
</tr>
<tr>
<td>Port Number:</td>
<td>389</td>
</tr>
<tr>
<td>Base DN:</td>
<td>ou=vm,dc=vmassist,dc=com</td>
</tr>
<tr>
<td>Bind Attribute:</td>
<td>dn</td>
</tr>
<tr>
<td>Login Attribute:</td>
<td>uid</td>
</tr>
<tr>
<td>Authenticated User:</td>
<td>cn=admin,ou=vm,dc=vmassist,dc=com</td>
</tr>
<tr>
<td>Authenticated Password:</td>
<td></td>
</tr>
<tr>
<td>Auto Create Users:</td>
<td>☑</td>
</tr>
<tr>
<td>Encryption Key:</td>
<td></td>
</tr>
</tbody>
</table>

Example: ldap.example.com
Example: 389
Example: DC=SugarCRM,DC=com
For Binding the LDAP User Examples [AD: userPrincipalName] [openLDAP: userPrincipalName]
[Mac OS X: uid]
For searching for the LDAP User Examples [AD: userPrincipalName] [openLDAP: dn] [Mac OS X: dn]
Used to search for the Sugar user. [May need to be fully qualified]
It will bind anonymously if not provided.
If an authenticated user does not exist one will be created in Sugar.
Setting up other software - SugarCRM
Setting up other software - z/VSE LDAP Client

" An LDAP Client is delivered starting with z/VSE 4.2

" Provides an alternate signon program
  " Allows userids and passwords up to 64 characters
  " Lets the LDAP Server control identity management and security policies for z/VSE

" Sample provided as SKLDCFG

<table>
<thead>
<tr>
<th>LDAP_SERVERS</th>
<th>DC</th>
<th>CL256'192.168.202.1:389'</th>
</tr>
</thead>
<tbody>
<tr>
<td>BIND_DN</td>
<td>DC</td>
<td>CL64'cn=admin,ou=vm,dc=vmassist,dc=com'</td>
</tr>
<tr>
<td>BIND_PWD</td>
<td>DC</td>
<td>CL64'secret'</td>
</tr>
<tr>
<td>USER_ATTRIBUTE</td>
<td>DC</td>
<td>CL64'cn'</td>
</tr>
<tr>
<td>BASE_DN</td>
<td>DC</td>
<td>CL64'ou=vm,dc=vmassist,dc=com'</td>
</tr>
</tbody>
</table>
Setting up other software - z/VSE LDAP Client

A mapping file is used to map long userids to short userids

A utility is provided to populate the mapping file

```c
// EXEC IESLDUMA
ID USER='RKS0' PWD='PASS'
ADD LDAPUSER='rsmrcina' TYPE=LDAP DESC='Richard Smrcina'
    VSEUSER='RKS0' VSEPWD='PASS'
ADD LDAPUSER='richsmrcina' TYPE=LDAP DESC='Richard Smrcina'
    VSEUSER='RKS1' VSEPWD='PASS'
/*
```

Your terminal is G020 and its name in the network is V10620
Today is 01/29/2009  To sign on to CICSICCF -- enter your:

- USER-ID
- PASSWORD
- PF1=HELP
- 2=TUTORIAL
- 5=REMOTE APPLICATIONS
- 10=NEW PASSWORD
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
Monitoring

" 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
livethreads=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
resettime=Sat Jul 26 01:15:05.412192 2008
resets=0
```
"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:

<table>
<thead>
<tr>
<th>Description</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config Max Connections</td>
<td>65523</td>
</tr>
<tr>
<td>System Max Connections</td>
<td>65535</td>
</tr>
<tr>
<td>Total Connections</td>
<td>31</td>
</tr>
<tr>
<td>Current Connections</td>
<td>1</td>
</tr>
<tr>
<td>MaxReached Connections</td>
<td>5</td>
</tr>
</tbody>
</table>
Monitoring

" The Hobbit network services monitor can watch LDAP connections

" Must either
  " Build with the LDAP capabilities
  " Use the RPM

" In the hosts definition file

192.168.190.1 vma   # ldap://192.168.190.1/o=VMAssist,c=US?cn?sub?(cn=RKS1)
Monitoring

Sun Aug 3 21:29:08 2008

ldap://192.168.190.1/o=VMAsist,c=US?cn?sub?(cn=RKS1) - OK

Searching LDAP for ldap://192.168.190.1/o=VMAsist,c=US?cn?sub?(cn=RKS1) yields 1 results:

DN: cn=RKS1,o=VMAsist,c=US
    cn: RKS1

Seconds: 0.73

Status unchanged in 1 hours, 27 minutes
Status message received from 192.168.190.18
Operating the LDAP Server

"Startup
  " TCP/IP will start it

"Shutdown

SMG LDAPSrv SHUTDOWN
090109 04:13:33.833359 GLD1007I LDAP server is stopping.
090109 04:13:33.983744 GLD6051I No database changes to commit for LDBM backend named LDBM-0001.

Options Report for Enclave main 01/08/09 10:13:34 PM
Language Environment V01 R04.00

... (LE runtime messages) ...

DTCRUN1014I Server ended normally at 22:13:40 on 8 Jan 2009 (Thursday)

" Does not listen to the shutdown signal
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
RACF Integration

" LDBM backend also works with RACF
  " Integrate z/VM defined users into the LDAP concept
  " Password checking based in RACF

" Presented at SHARE 111 in same session
  " http://www.linuxvm.org/Present/SHARE111/S9156rs.pdf
References

" z/VM TCP/IP Planning and Customization
  " SC24-6125-03 (z/VM 5.3) SC24-6125-04 (z/VM 5.4)

" z/VM TCP/IP LDAP Administration Guide
  " SC24-6140-00 (z/VM 5.3) SC24-6140-01 (z/VM 5.4)

" z/VM TCP/IP User's Guide
  " SC24-6127-03 (z/VM 5.3) SC24-6127-04 (z/VM 5.4)

" Essential System Administration, Æleen 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
  " SG24-7471-00
Questions?

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