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

- 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 **Lightweight Directory Access Protocol**
- A standard method for accessing and updating information in a directory
  - Defined in RFC 1777 and others\(^1\)
- 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

\(^1\)RFCs 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

```plaintext
cn=infoprint48,ou=bldg12,o=company,c=us
```

- `RDN` - Relative Distinguished Name
- `DN` - Distinguished Name
What is LDAP?

LDAP is an internet standard which uses the TCP/IP protocol. It is used to communicate with a database of information, such as a directory service. LDAP stores data in a tree structure, with the root at the top, and branches down to the specific items of interest.

In the diagram above, the root is labeled as `c=us`. Underneath it, there are two branches labeled `o=other` and `o=company`. Under `o=other`, there is an `ou=bldg06` and under `o=company`, there are `ou=bldg12` and `ou=bldg14`.

Each of these branches contains information about specific items, such as `cn=jjones`, `employeenumber`, `telephonenumber`, `uidnumber`, `gidnumber`, `homedirectory`, `cn=infoprint48`, `serialnumber`, `telephonenumber`, `modelnumber`, `inservicedate`, and `maintenancedate`. This information is stored in a hierarchical manner, allowing for easy retrieval and organization.
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 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 tailororable

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 SAMPENVVR -----> 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

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/lodbm
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:

<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 1004</td>
<td>*..FTP-C</td>
<td><em>..</em></td>
<td><em>..</em></td>
<td>Listen</td>
</tr>
<tr>
<td>INTCLIE 1003</td>
<td>*..TELNET</td>
<td><em>..</em></td>
<td><em>..</em></td>
<td>Listen</td>
</tr>
<tr>
<td>INTCLIE 1011</td>
<td>192.168.1.50..TELNET</td>
<td>10.1.0.2..41112</td>
<td>Established</td>
<td></td>
</tr>
<tr>
<td>INTCLIE 1012</td>
<td>192.168.1.50..TELNET</td>
<td>10.1.0.2..41113</td>
<td>Established</td>
<td></td>
</tr>
<tr>
<td>SSLSERV 1000</td>
<td>127.0.0.1..1024</td>
<td><em>..</em></td>
<td><em>..</em></td>
<td>Listen</td>
</tr>
<tr>
<td>SSLSERV 1001</td>
<td>127.0.0.1..1024</td>
<td>127.0.0.1..1025</td>
<td>Established</td>
<td></td>
</tr>
<tr>
<td>SSLSERV 1002</td>
<td>*..1026</td>
<td><em>..</em></td>
<td><em>..</em></td>
<td>Listen</td>
</tr>
<tr>
<td>LDAPSRV 1007</td>
<td>192.168.1.50..389</td>
<td><em>..</em></td>
<td><em>..</em></td>
<td>Listen</td>
</tr>
<tr>
<td>LDAPSRV 1006</td>
<td>192.168.240.1..389</td>
<td><em>..</em></td>
<td><em>..</em></td>
<td>Listen</td>
</tr>
<tr>
<td>LDAPSRV 1008</td>
<td>127.0.0.1..389</td>
<td><em>..</em></td>
<td><em>..</em></td>
<td>Listen</td>
</tr>
</tbody>
</table>
## LDAP Checkout

```
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
  - ldapsrch (LDAPSRCCH), ldapadd (LDAPADD), ldapmodify (LDAPMDFY), ldapcompare (LDAPCMPR), ldapdelete (LDAPDLET), ldapmodrdn (LDAPMRDN)

- We will use the LDAPSRCCH command

```bash
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 //USRSCHEM.LDIF -u on`

  `ldapmdfy -h 127.0.0.1 -D "cn=Admin" -w ***** -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

• 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

```
ldapmdfy -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 SAMPserv 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

```bash
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

- 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`

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>192.168.1.50</td>
</tr>
<tr>
<td>base</td>
<td>o=VMAssist,c=US</td>
</tr>
<tr>
<td>bind_policy</td>
<td>soft</td>
</tr>
<tr>
<td>pam_lookup_policy</td>
<td>yes</td>
</tr>
<tr>
<td>pam_password</td>
<td>racf</td>
</tr>
<tr>
<td>nss_initgroups_ignoreusers</td>
<td>root,ldap</td>
</tr>
<tr>
<td>nss_schema</td>
<td>rfc2307bis</td>
</tr>
<tr>
<td>nss_map_attribute</td>
<td>uniqueMember member</td>
</tr>
<tr>
<td>ssl</td>
<td>no</td>
</tr>
<tr>
<td>ldap_version</td>
<td>3</td>
</tr>
<tr>
<td>pam_filter</td>
<td>objectClass=posixAccount</td>
</tr>
<tr>
<td>tls_checkpeer</td>
<td>no</td>
</tr>
</tbody>
</table>
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**
  
  \texttt{RAC ADDUSER RKS1 PASSWORD(PWORD)}

- **Create LDIF file to add Linux user to LDBM database**

  \begin{verbatim}
  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
  \end{verbatim}
Using z/VM LDAP with Linux

• Add the entry

```bash
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...

```bash
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

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:
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

[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

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.
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
Browsing the LDAP Directory

- Softerra LDAP Browser (http://www.ldapbrowser.com)
Browsing the LDAP Directory

• Softerra LDAP Browser (http://www.ldapbrowser.com)
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

<table>
<thead>
<tr>
<th>LDAP Authentication Support</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable LDAP</td>
<td>[ ]</td>
<td>Example: ldap.example.com</td>
</tr>
<tr>
<td>Server:</td>
<td>192.168.1.50</td>
<td>Example: 389</td>
</tr>
<tr>
<td>Port Number:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Base DN:</td>
<td>ou=vm,dc=vmassist,dc=com</td>
<td>Example: DC=SugarCRM,DC=com</td>
</tr>
<tr>
<td>Bind Attribute:</td>
<td>dn</td>
<td>For Binding the LDAP User Examples [AD: userPrincipalName] [openLDAP: userPrincipalName] [Mac OS X: uid]</td>
</tr>
<tr>
<td>Login Attribute:</td>
<td>uid</td>
<td>For searching for the LDAP User Examples [AD: userPrincipalName] [openLDAP: dn] [Mac OS X: dn]</td>
</tr>
</tbody>
</table>
| Authenticated User:         | cn=admin,ou=vm,dc=vmassist,dc=com | Used to search for the Sugar user. [May need to be fully qualified]
| Authenticated Password:     | ******** | It will bind anonymously if not provided. |
| Auto Create Users:          | [ ]      | If an authenticated user does not exist one will be created in Sugar. |
| Encryption Key:             |          | For SOAP authentication when using LDAP. |
Setting up other software - SugarCRM
Monitoring

- LDAP Server keep statistics during its 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

```bash
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
addsrerquested=0
addscopleted=0
bindsrerquested=25
bindscopleted=25
comparesrerquested=0
comparescopleted=0
deletesrerquested=0
deletescopleted=0
extopsrerquested=0
modifiesrerquested=0
modifiescopleted=0
modifydnsrerquested=0
modifydncopleted=0
searchsrerquested=31
searchscopleted=30
unbindsrerquested=21
unbindscopleted=21
unknownopsrerquested=0
unknownopscopleted=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
```
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**

  SMSG 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

• 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, 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
- Redbook: Understanding LDAP - SG24-4986
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