VM Assist
Providing quality systems
support since 1986

SHARE
Technology · Connections · Results

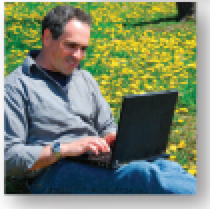
Configuring LDAP on z/VM and Linux

Rich Smrcina
VM Assist

Session 9156
August 13, 2008

IBM DESTINATION z

© Disney



Presentation Materials

- SHARE Proceedings
- http://www.vmassist.com/share111_9156.pdf

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
  - Apache
  - Browsing/Editing Tools
  - Monitoring
- References

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
- Starting with z/VM 5.3 an LDAP Server is delivered
  - Adapted from IBM Tivoli Directory Server for z/OS, on z/OS 1.8
- 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
  - 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
  - Provides more comprehensive interface to the z/VM RACF Security Server
  - Allows password phrases up to 100 characters
- 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 5.3 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, specify YES for ESM_Enable
  - Other ESM options can then default
- ESM_Racroute and ESM_Validate will need to be changed if using a different External Security Manager

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 tailorable
- 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 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/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 192.168.1.60
port 389.
080617 15:01:03.552522 GLD1059I Listening for requests on 192.168.190.1
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 530

Active IPv4 Transmission Blocks:

User Id  Conn    Local Socket            Foreign Socket          State
   ---- --  ----    ----- ------            ------- ------          -----
   FTPSERVE 1000    *..FTP-C                *..*                    Listen
   INTCLIEN 1003    *..TELNET               *..*                    Listen
   INTCLIEN 1004    192.168.1.60..TELNET    192.168.1.101..46604    Established
   INTCLIEN 1006    192.168.1.60..TELNET    192.168.1.101..46607    Established
   LDAPSRV  1001    192.168.1.60..389       *..*                    Listen
   LDAPSRV  1002    192.168.190.1..389      *..*                    Listen
   LDAPSRV  1005    127.0.0.1..389          *..*                    Listen


Active IPv6 Transmission Blocks: None
```

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
  - 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 ******* -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

LDAP Checkout

- The same command from Linux

```
dns:/etc # ldapsearch -h 192.168.1.60 -x -w ******** -s base -b
"o=VMAssist,c=US" "objectclass=*"
# extended LDIF
#
# LDAPv3
# base <o=VMAssist,c=US> with scope baseObject
# filter: objectclass=*
# requesting: ALL
#

# search result
search: 2
result: 32 No such object
text: R004071 DN 'o=VMAssist,c=US' does not exist (ldbm_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 ****** -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
- Update schema on the LDAP Server

```
ldapmdfy -h 127.0.0.1 -w ******** -D cn=LDAPSRV,o=VMAssist,c=US
-f //nisschem.ldif -u on
modifying entry cn=schema
modifying entry cn=schema
```

Setup admin access

- In this simple setup the administrator will be the LDAP server itself (LDAPSRV)
  - The user exists on the z/VM system
  - Set up for Native authentication
- In DS CONF
  - Set option `useNativeAuth` to `all`
- Create an **L**DAP **D**ata **I**nterchange **F**ormat 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: 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 person (cn=LDAPSRV)

Setup admin access

- Use ldapadd to insert the entries into the LDBM database

```
ldapadd -h 127.0.0.1 -w ******** -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 check on the LDAPSRV entry just made

```
ldapsrch -h 127.0.0.1 -w ******* -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

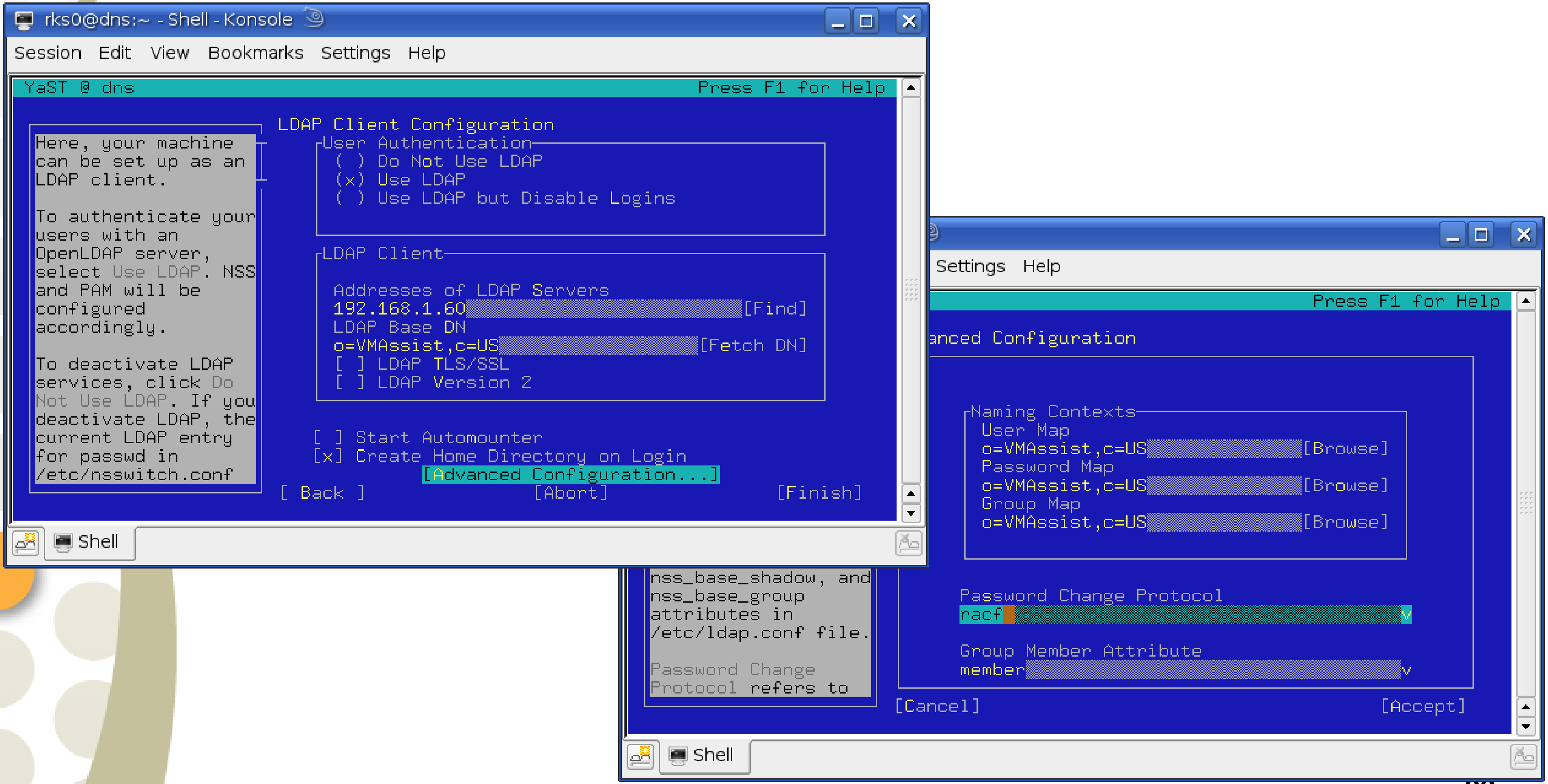
- LDAP provides a way to keep a repository of security information in a centralized place
  - Previously this could have been done with NIS
- The LDAP Server running on z/VM
  - Brings the power and capabilities of RACF to security management on Linux
  - LDAP clients (virtual machines or real machines)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



rks0@dns:~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
Shell

```
YaST @ dns                                                     Press F1 for Help

                         LDAP Client Configuration
Here, your machine      User Authentication
can be set up as an       ( ) Do Not Use LDAP
LDAP client.              (x) Use LDAP
                          ( ) Use LDAP but Disable Logins
To authenticate your
users with an           LDAP Client
OpenLDAP server,
select Use LDAP. NSS      Addresses of LDAP Servers
and PAM will be           192.168.1.60                          [Find]
configured                LDAP Base DN
accordingly.              o=VMAssist,c=US                       [Fetch DN]
                          [ ] LDAP TLS/SSL
To deactivate LDAP        [ ] LDAP Version 2
services, click Do
Not Use LDAP. If you
deactivate LDAP, the    [ ] Start Automounter
current LDAP entry      [x] Create Home Directory on Login
for passwd in                 [Advanced Configuration...]
/etc/nsswitch.conf      [ Back ]           [Abort]                [Finish]
```

```
                                                   Press F1 for Help
anced Configuration

      Naming Contexts
        User Map
        o=VMAssist,c=US                  [Browse]
        Password Map
        o=VMAssist,c=US                  [Browse]
        Group Map
        o=VMAssist,c=US                  [Browse]

nss_base_shadow, and
nss_base_group          Password Change Protocol
attributes in           racf                                  v
/etc/ldap.conf file.
                        Group Member Attribute
Password Change         member                                v
Protocol refers to
                    [Cancel]                                [Accept]
```

Using z/VM LDAP with Linux

- Review /etc/ldap.conf

```
host    192.168.1.60
base    o=VMAssist,c=US
ldap_version    3
bind_policy     soft
binddn  cn=LDAPSRV,o=VMAssist,c=US
bindpw  ********
pam_lookup_policy       yes
pam_password    racf
ssl     no
nss_map_attribute       uniqueMember member
pam_filter      objectclass=posixAccount
nss_base_passwd o=VMAssist,c=US
nss_base_shadow o=VMAssist,c=US
nss_base_group  o=VMAssist,c=US
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

- 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

- Add the entry

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

- Since the first logon will require a password change lets change the password now

```
ldapsrch -h 127.0.0.1 -w pword/newpass -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

```
telnet 192.168.190.12
Trying 192.168.190.12...
Connected to 192.168.190.12.
Escape character is '^]'.
Welcome to SUSE Linux Enterprise Server 10 SP1 (s390x) - Kernel
2.6.16.46-0.12-default (1).

dns 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@dns:~> pwd
/home/rks1
rks1@dns:~> id
uid=2000(rks1) gid=100(users) groups=100(users)
```

Using z/VM LDAP with Linux

```
rks0@laptop:~> ssh rks1@192.168.190.12
Password:
Last login: Mon Jul 14 15:29:23 2008 from 192.168.1.100
rks1@dns:~> id
uid=2000(rks1) gid=100(users) groups=100(users)
rks1@dns:~> ll
total 12
drwxr-xr-x 2 rks1 users 4096 2008-07-11 10:55 bin
drwxr-xr-x 2 rks1 users 4096 2008-07-11 10:55 Documents
drwxr-xr-x 2 rks1 users 4096 2008-07-11 10:55 public_html
```

Using z/VM LDAP with Linux

- 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

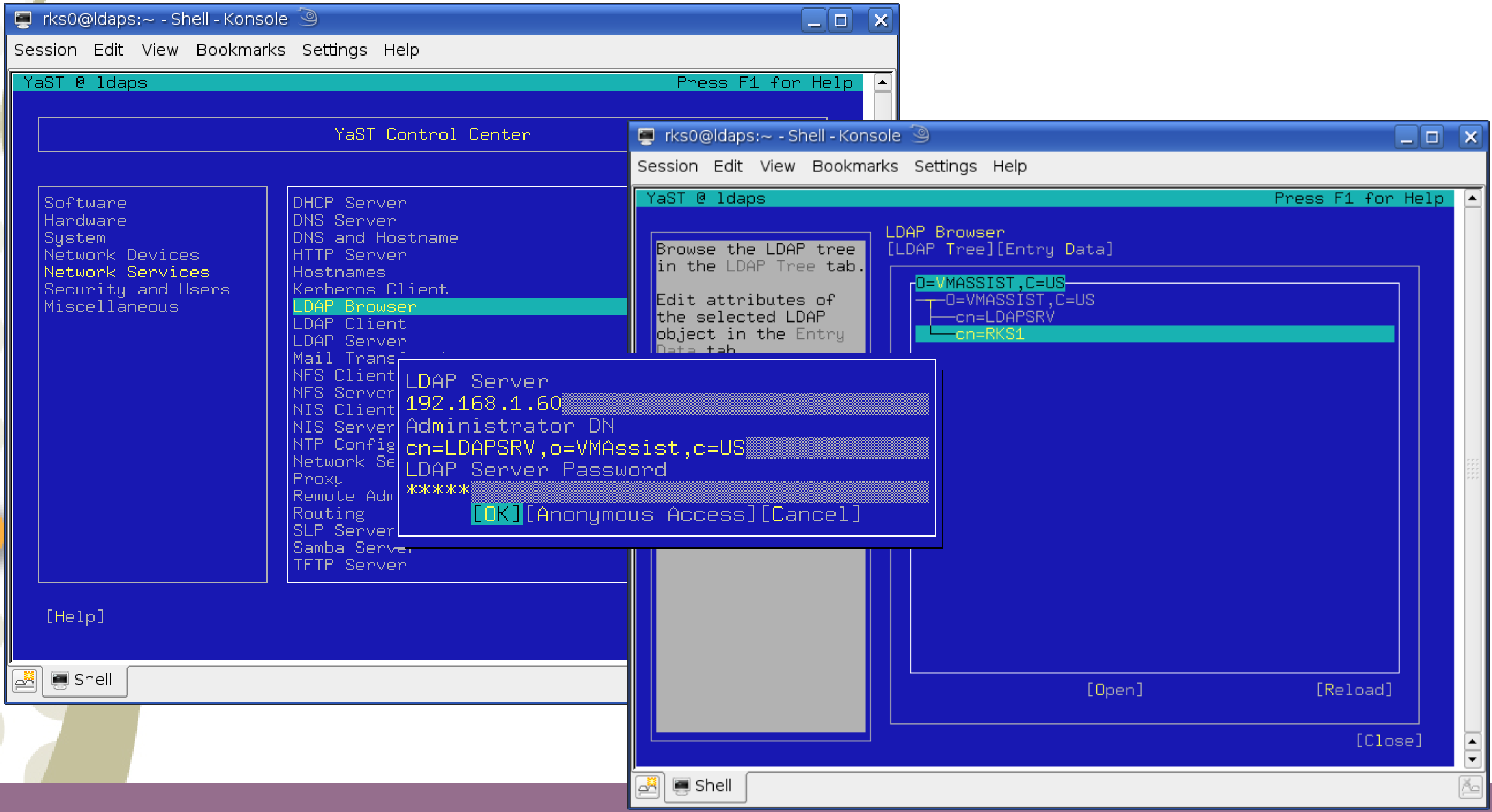
```
rks0@laptop:~> ftp 192.168.190.12
Connected to 192.168.190.12.
220 (vsFTPd 2.0.4)
Name (192.168.190.12:rks0): rks1
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
257 "/home/rks1"
ftp>
```

- Log file entry from FTP login

```
Jul 21 10:02:35 dns vsftpd: Mon Jul 21 10:02:35 2008 [pid 7894] [rks1]
OK LOGIN: Client "192.168.1.100"
```

Browsing the LDAP Directory

- With YaST



rks0@ldaps:~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
Shell

```
YaST @ ldaps                                             Press F1 for Help

                         YaST Control Center

Software                 DHCP Server
Hardware                 DNS Server
System                   DNS and Hostname
Network Devices          HTTP Server
Network Services         Hostnames
Security and Users       Kerberos Client
Miscellaneous            LDAP Browser
                         LDAP Client
                         LDAP Server
                         Mail Trans
                         NFS Client
                         NFS Server
                         NIS Client
                         NIS Server
                         NTP Config
                         Network Se
                         Proxy
                         Remote Adm
                         Routing
                         SLP Server
                         Samba Serv
                         TFTP Server

[Help]
```

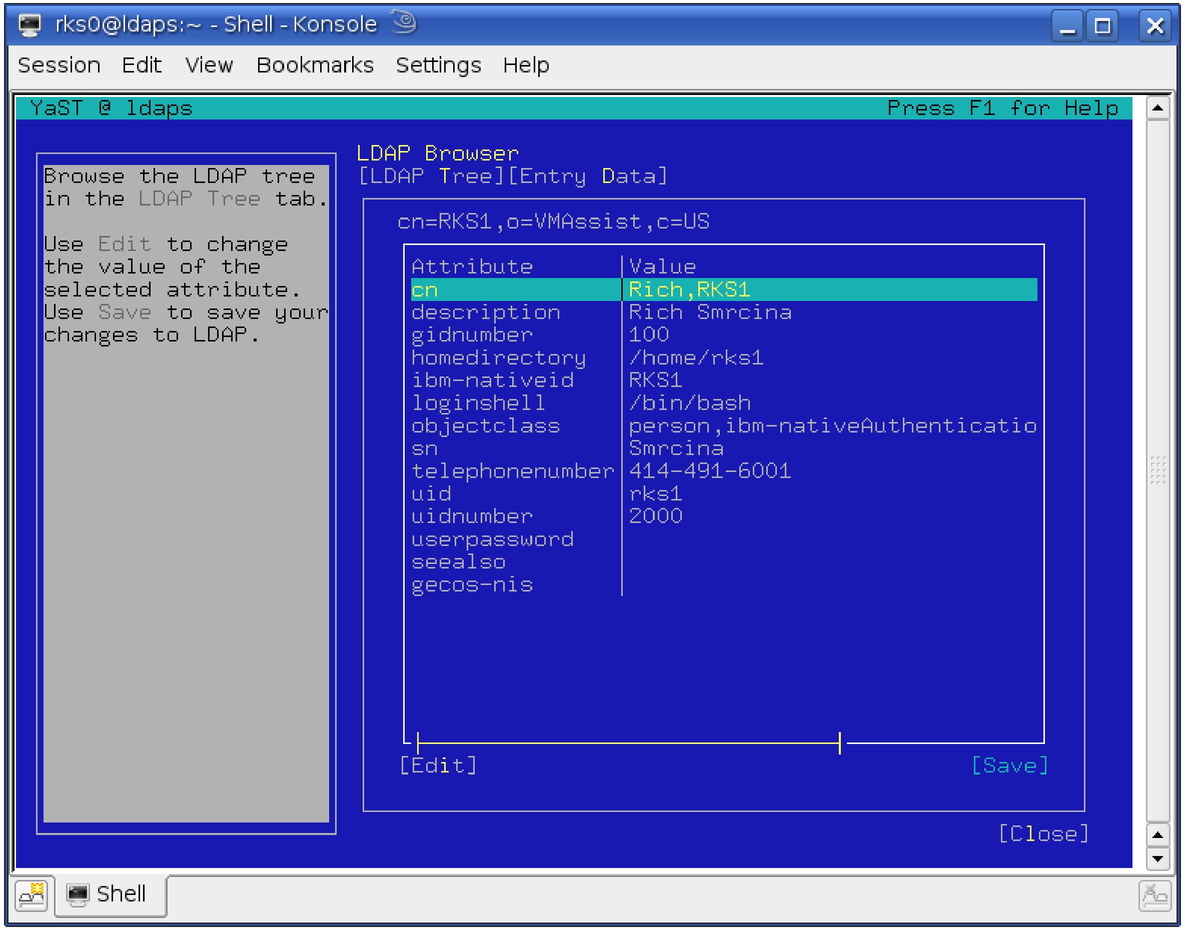
rks0@ldaps:~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
Shell

```
YaST @ ldaps                                             Press F1 for Help

                           LDAP Browser
Browse the LDAP tree       [LDAP Tree][Entry Data]
in the LDAP Tree tab.
                           O=VMASSIST,C=US
Edit attributes of         ┬─O=VMASSIST,C=US
the selected LDAP          ├──cn=LDAPSRV
object in the Entry        └──cn=RKS1
Data tab

                           [Open]                     [Reload]

                                                       [Close]
```

```
LDAP Server
192.168.1.60
Administrator DN
cn=LDAPSRV,o=VMAssist,c=US
LDAP Server Password
*****
   [OK][Anonymous Access][Cancel]
```

Browsing the LDAP Directory

" With YaST

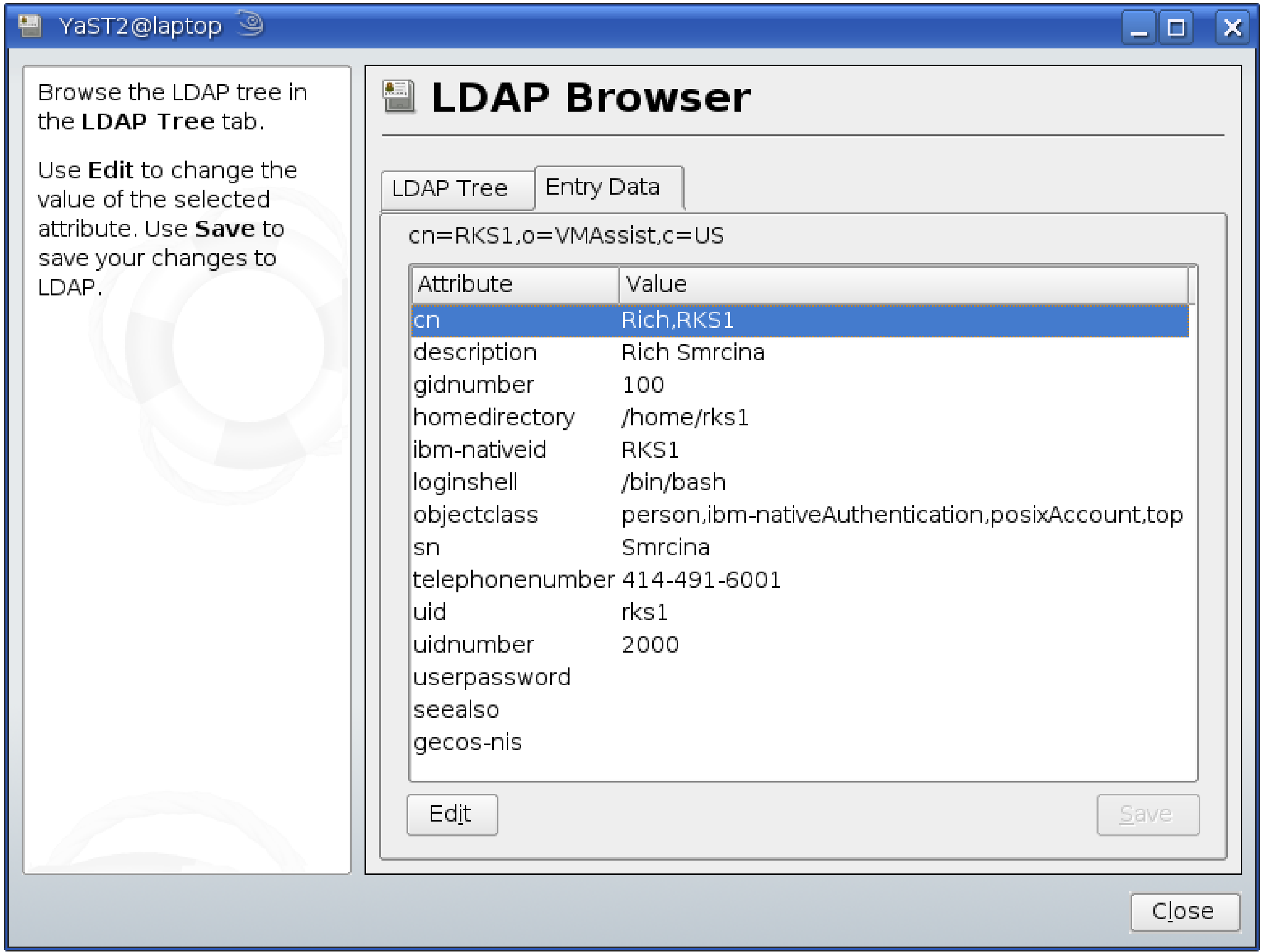


rks0@ldaps:~ - Shell - Konsole
Session Edit View Bookmarks Settings Help

```
YaST @ ldaps                                                    Press F1 for Help

                         LDAP Browser
 Browse the LDAP tree    [LDAP Tree][Entry Data]
 in the LDAP Tree tab.
                           cn=RKS1,o=VMAssist,c=US
 Use Edit to change
 the value of the           Attribute       │Value
 selected attribute.        cn              │Rich,RKS1
 Use Save to save your      description     │Rich Smrcina
 changes to LDAP.           gidnumber       │100
                            homedirectory   │/home/rks1
                            ibm-nativeid    │RKS1
                            loginshell      │/bin/bash
                            objectclass     │person,ibm-nativeAuthenticatio
                            sn              │Smrcina
                            telephonenumber │414-491-6001
                            uid             │rks1
                            uidnumber       │2000
                            userpassword    │
                            seealso         │
                            gecos-nis       │

                          [Edit]                                  [Save]

                                                                 [Close]
```

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.

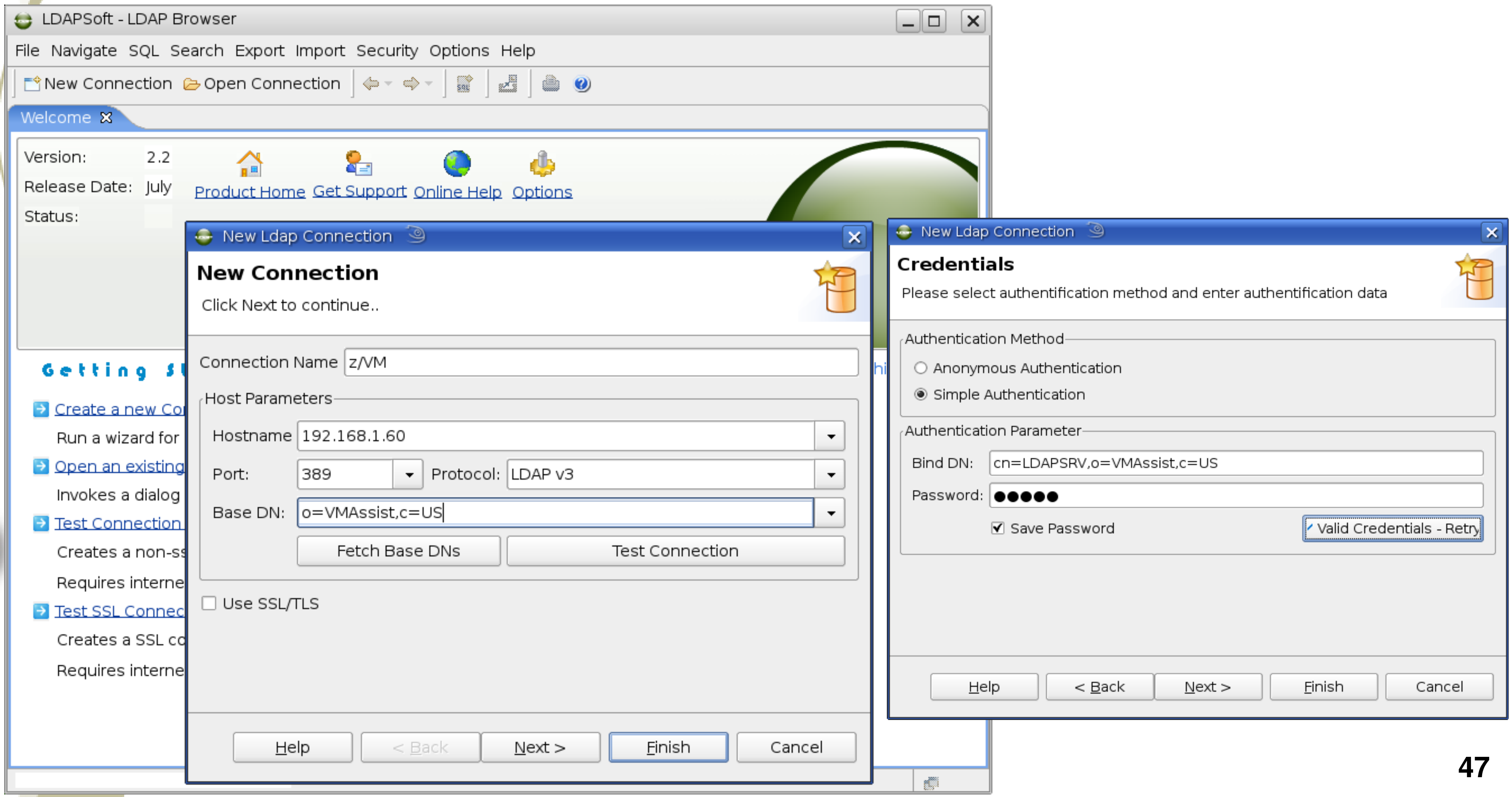
LDAP Browser

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	

Browsing the LDAP Directory

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



Version: 2.2

Release Date: July

Status:

New Connection

Click Next to continue..

Connection Name: z/VM

Host Parameters

Hostname: 192.168.1.60

Port: 389 Protocol: LDAP v3

Base DN: o=VMAssist,c=US

□ Use SSL/TLS

Credentials

Please select authentification method and enter authentification data

Authentication Method

○ Anonymous Authentication

● Simple Authentication

Authentication Parameter

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

Password: ●●●●●

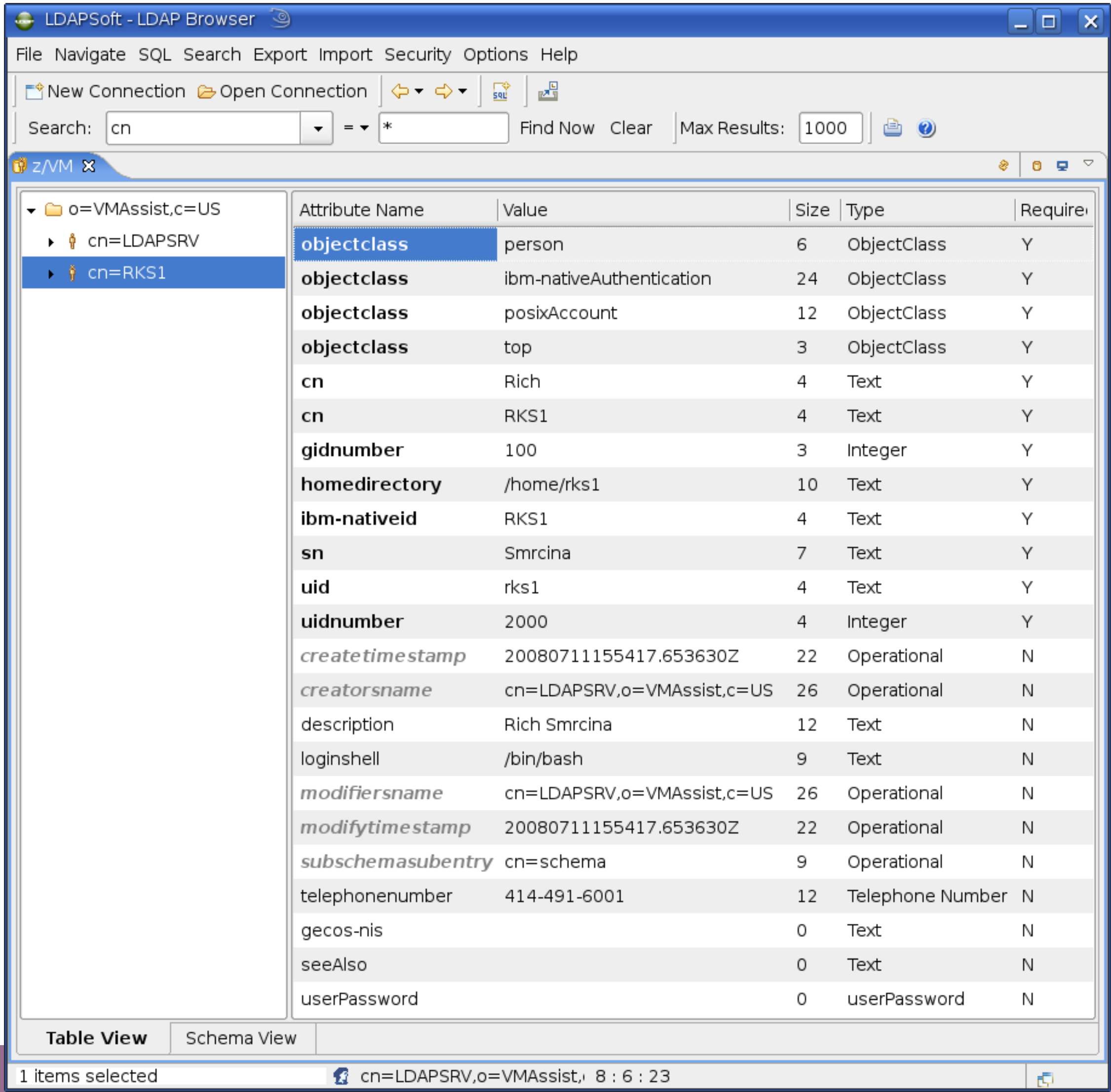
☑ Save Password

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

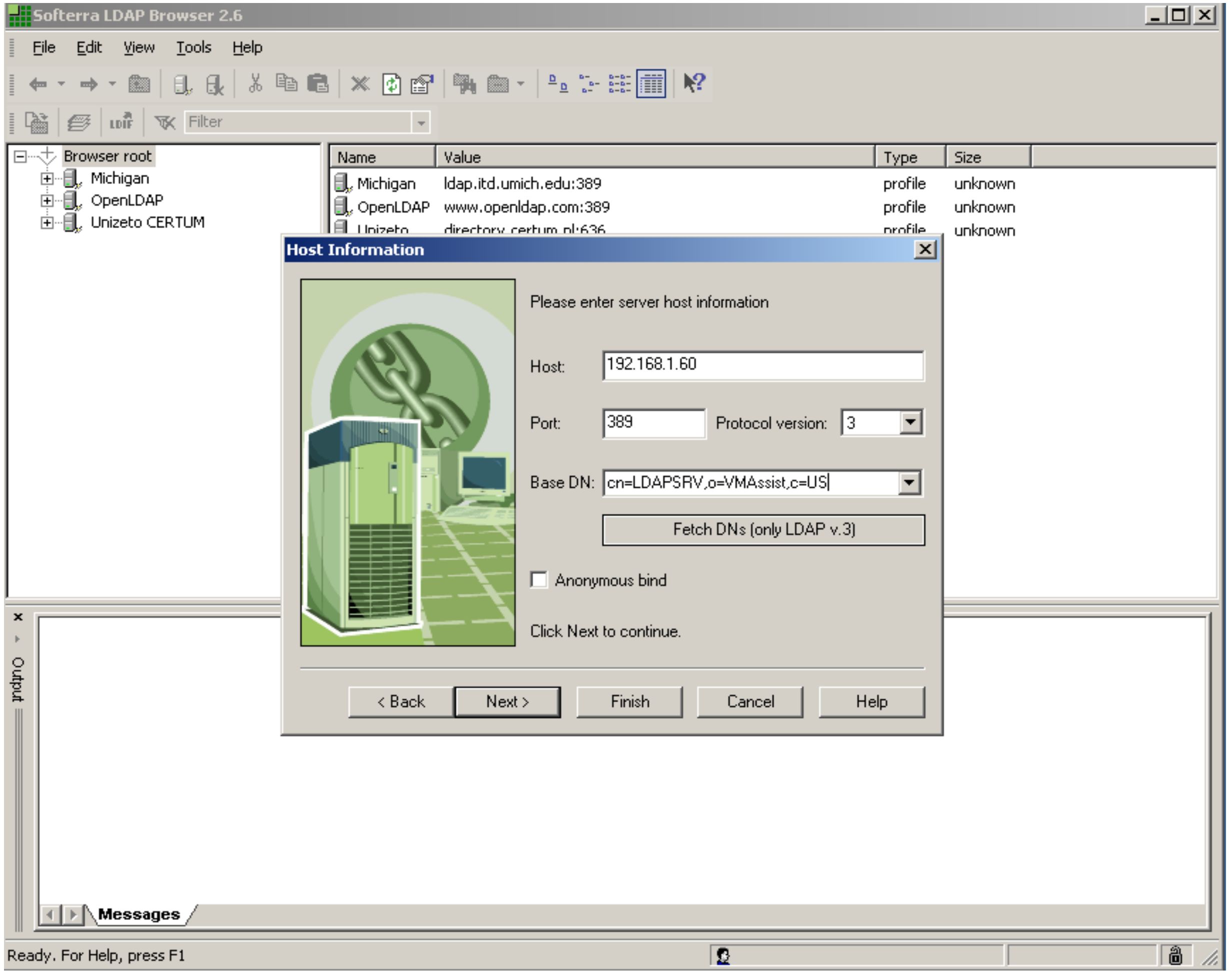


Attribute Name	Value	Size	Type	Require
objectclass	person	6	ObjectClass	Y
objectclass	ibm-nativeAuthentication	24	ObjectClass	Y
objectclass	posixAccount	12	ObjectClass	Y
objectclass	top	3	ObjectClass	Y
cn	Rich	4	Text	Y
cn	RKS1	4	Text	Y
gidnumber	100	3	Integer	Y
homedirectory	/home/rks1	10	Text	Y
ibm-nativeid	RKS1	4	Text	Y
sn	Smrcina	7	Text	Y
uid	rks1	4	Text	Y
uidnumber	2000	4	Integer	Y
createtimestamp	20080711155417.653630Z	22	Operational	N
creatorsname	cn=LDAPSRV,o=VMAssist,c=US	26	Operational	N
description	Rich Smrcina	12	Text	N
loginshell	/bin/bash	9	Text	N
modifiersname	cn=LDAPSRV,o=VMAssist,c=US	26	Operational	N
modifytimestamp	20080711155417.653630Z	22	Operational	N
subschemasubentry	cn=schema	9	Operational	N
telephonenumber	414-491-6001	12	Telephone Number	N
gecos-nis		0	Text	N
seeAlso		0	Text	N
userPassword		0	userPassword	N

1 items selected   cn=LDAPSRV,o=VMAssist, 8 : 6 : 23

Browsing the LDAP Directory

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



Softerra LDAP Browser 2.6
File Edit View Tools Help
Filter
Browser root
Michigan
OpenLDAP
Unizeto CERTUM
Output
Messages
Ready. For Help, press F1

Name	Value	Type	Size
Michigan	ldap.itd.umich.edu:389	profile	unknown
OpenLDAP	www.openldap.com:389	profile	unknown
Unizeto	directory.certum.pl:636	profile	unknown

Host Information

Please enter server host information

Host: 192.168.1.60

Port: 389 Protocol version: 3

Base DN: cn=LDAPSRV,o=VMAssist,c=US

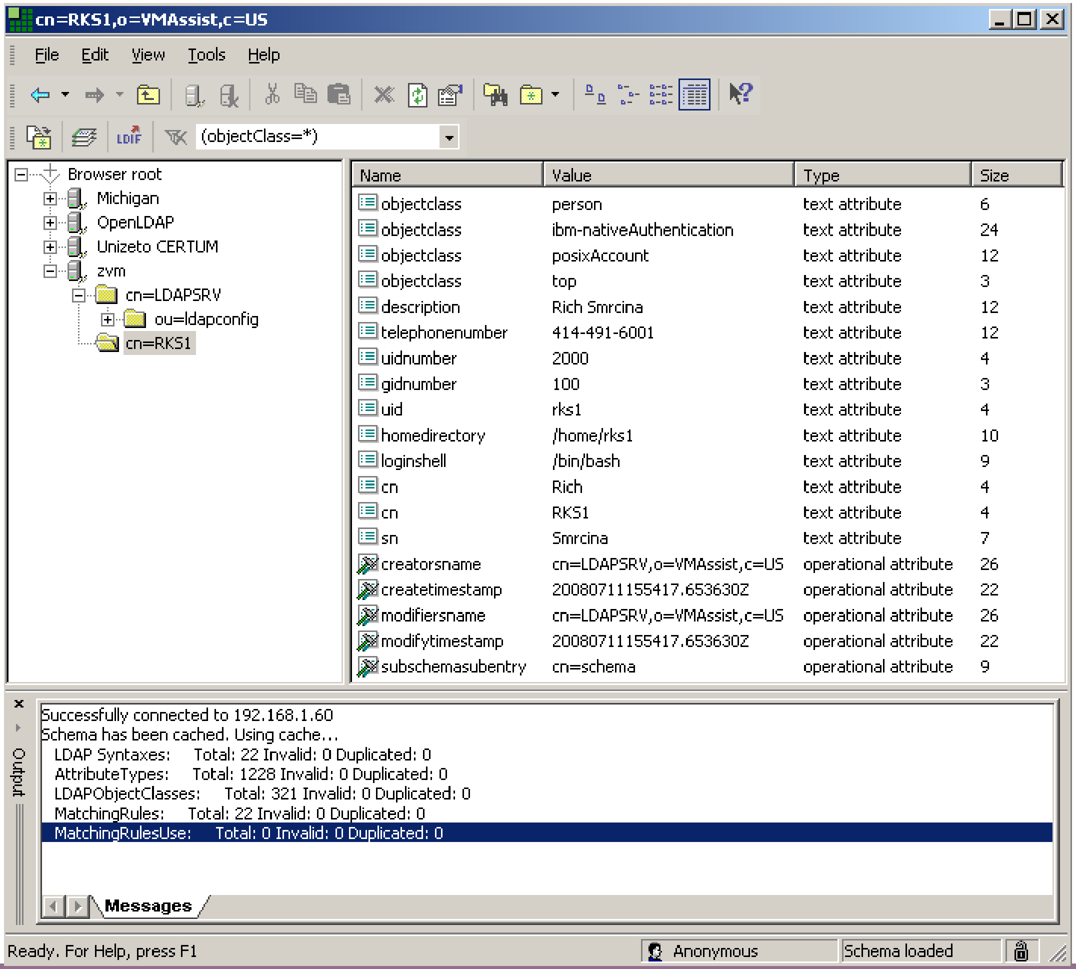
Fetch DNs (only LDAP v.3)

□ Anonymous bind

Click Next to continue.

Browsing the LDAP Directory

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



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	RKS1	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

```
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
```

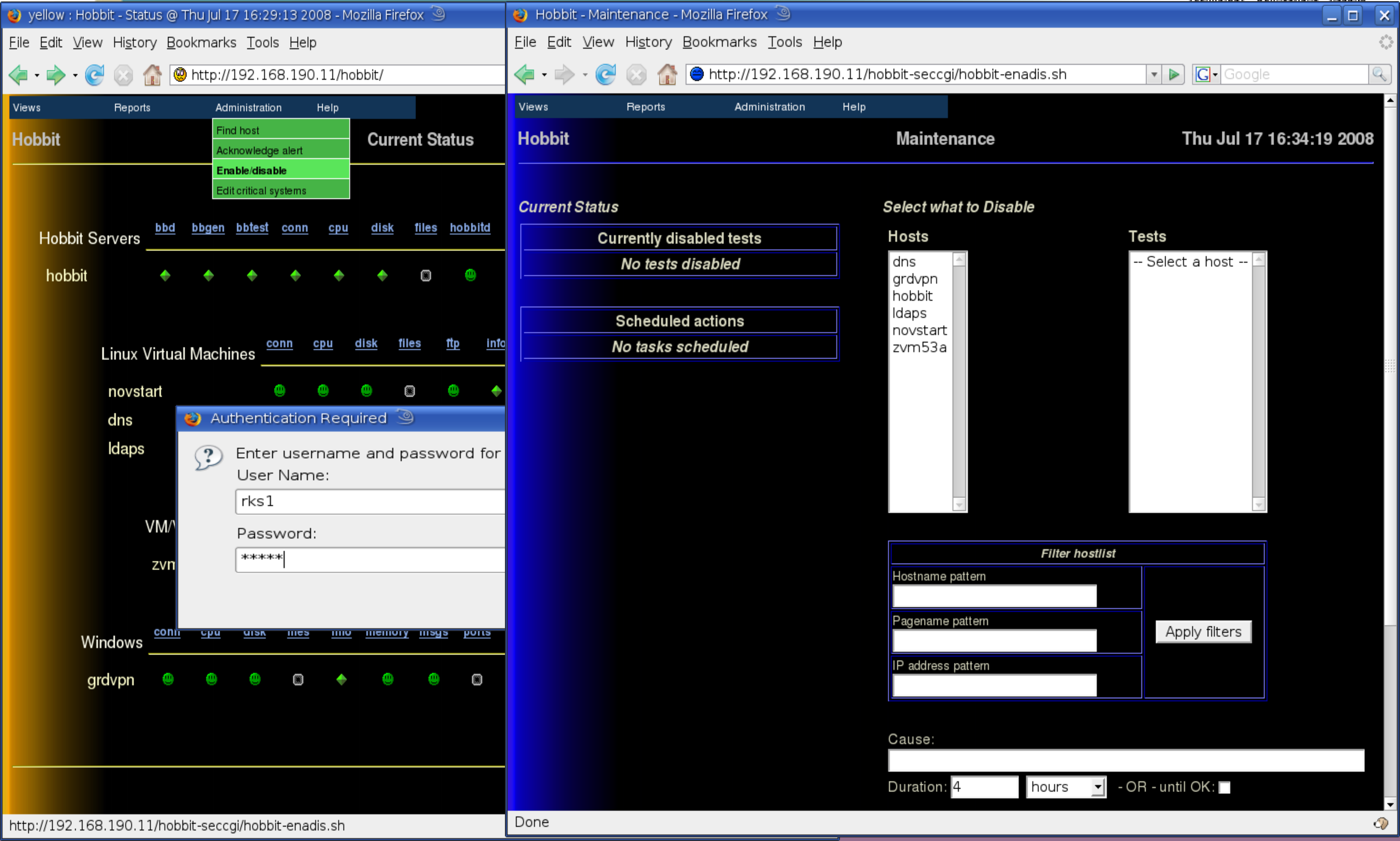
Setting up other software - Apache

- 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>
```

The Apache Software Foundation
http://www.apache.org/

Setting up other software - Apache



yellow : Hobbit - Status @ Thu Jul 17 16:29:13 2008 - Mozilla Firefox

http://192.168.190.11/hobbit/

Authentication Required

Enter username and password for

User Name: rks1

Password: *****

http://192.168.190.11/hobbit-seccgi/hobbit-enadis.sh

Hobbit - Maintenance - Mozilla Firefox

http://192.168.190.11/hobbit-seccgi/hobbit-enadis.sh

Current Status

Currently disabled tests
No tests disabled

Scheduled actions
No tasks scheduled

Select what to Disable

Hosts: dns, grdvpn, hobbit, ldaps, novstart, zvm53a

Tests: -- Select a host --

Filter hostlist

Hostname pattern:

Pagename pattern:

IP address pattern:

Cause:

Duration: 4 hours - OR - until OK: □

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

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
```

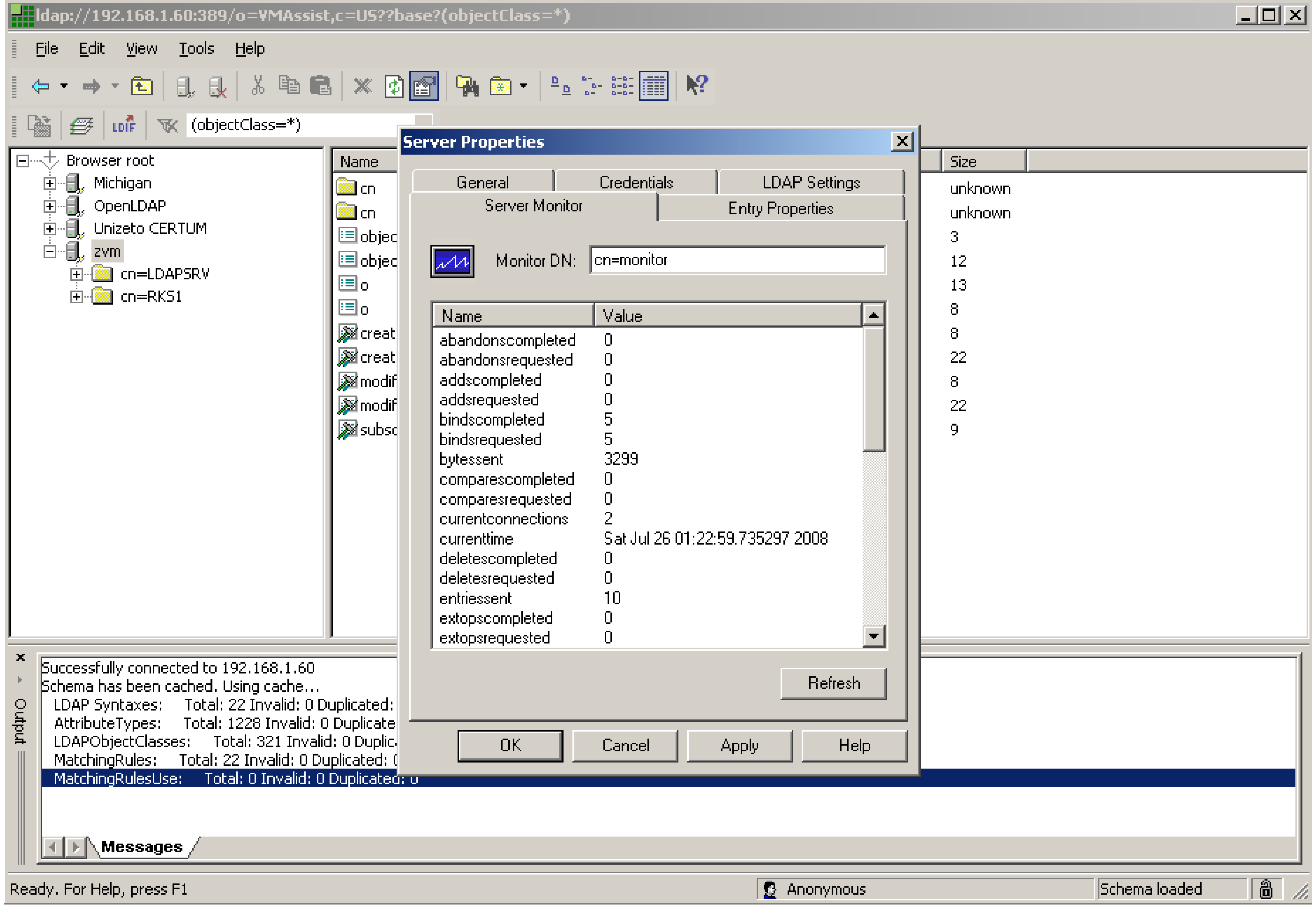
Monitoring

- 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
```

Monitoring

- Format of the statistics (Softerra LDAP Browser)



ldap://192.168.1.60:389/o=VMAssist,c=US??base?(objectClass=*)

Server Properties

Monitor DN: cn=monitor

Name	Value
abandonscompleted	0
abandonsrequested	0
addscompleted	0
addsrequested	0
bindscompleted	5
bindsrequested	5
bytessent	3299
comparescompleted	0
comparesrequested	0
currentconnections	2
currenttime	Sat Jul 26 01:22:59.735297 2008
deletescompleted	0
deletesrequested	0
entriessent	10
extopscompleted	0
extopsrequested	0

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

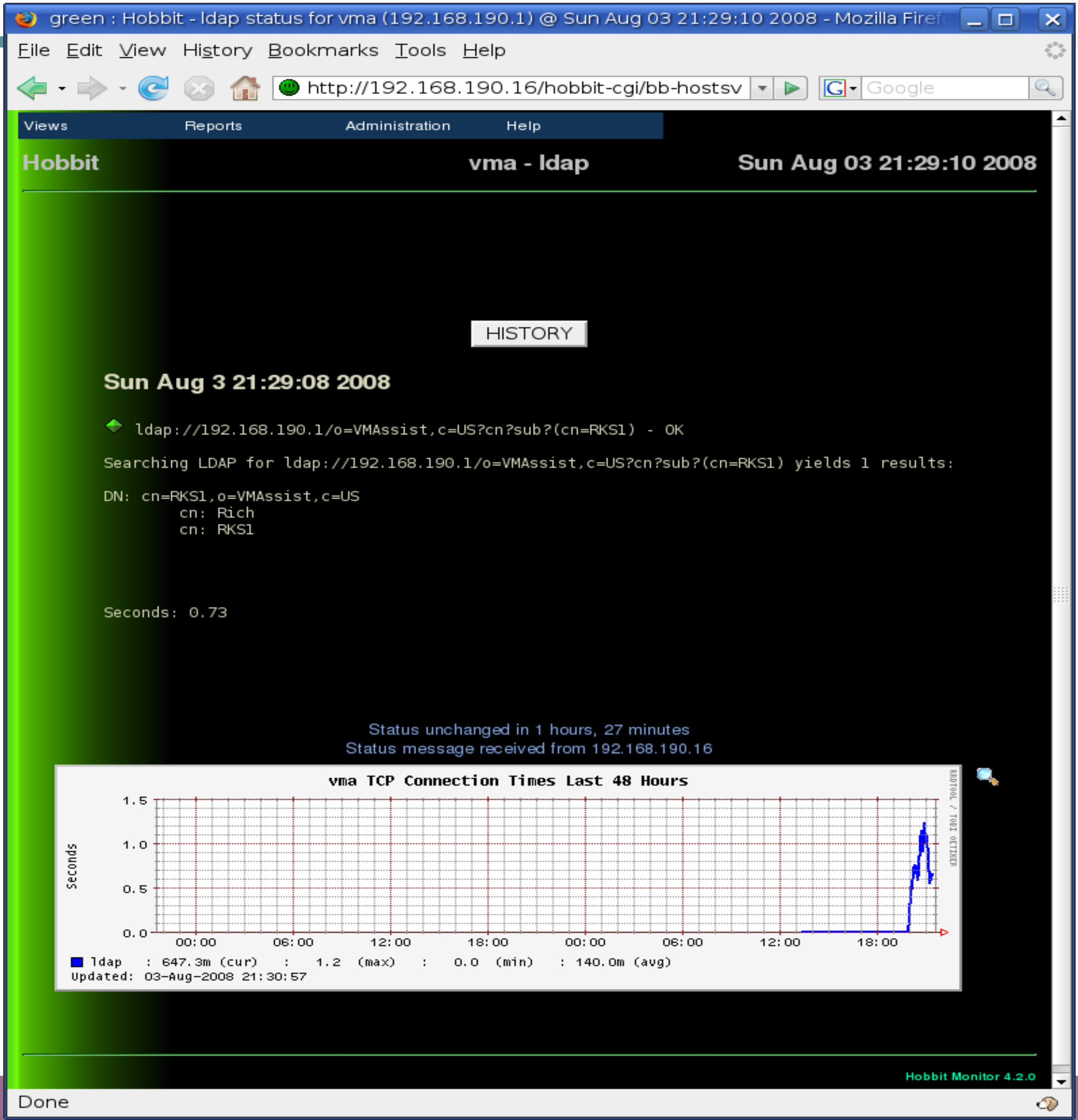
Ready. For Help, press F1

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


green : Hobbit - ldap status for vma (192.168.190.1) @ Sun Aug 03 21:29:10 2008 - Mozilla Firef
File Edit View History Bookmarks Tools Help
http://192.168.190.16/hobbit-cgi/bb-hostsv
Google
Views
Reports
Administration
Help
Hobbit
vma - ldap
Sun Aug 03 21:29:10 2008
HISTORY
vma TCP Connection Times Last 48 Hours
Seconds
1.5
1.0
0.5
0.0
00:00
06:00
12:00
18:00
00:00
06:00
12:00
18:00
RRDTOOL / TOBI OETIKER
Hobbit Monitor 4.2.0
Done

Sun Aug 3 21:29:08 2008

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

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

DN: cn=RKS1,o=VMAssist,c=US
        cn: Rich
        cn: RKS1


Seconds: 0.73
```

Status unchanged in 1 hours, 27 minutes
Status message received from 192.168.190.16

```
■ ldap   : 647.3m (cur)   :   1.2  (max)   :   0.0  (min)   : 140.0m (avg)
Updated: 03-Aug-2008 21:30:57
```

Operating the LDAP Server

- Startup
  - TCP/IP will start it
- Shutdown

```
SMSG LDAPSRV SHUTDOWN
080702 16:22:58.584170 GLD1007I LDAP server is stopping.
080702 16:22:59.368858 GLD6033I Committing changes to database
for LDBM backend named LDBM-0001.
080702 16:23:02.729066 GLD6034I Completed committing changes to
database for LDBM backend named LDBM-0001.

Options Report for Enclave main 07/02/08 11:23:03 AM
Language Environment V01 R04.00
... (LE runtime messages)
DTCRUN1014I Server ended normally at 11:23:14 on 2 Jul 2008
(Wednesday)
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 V5R3.0 TCP/IP Planning and Customization
  - SC24-6125-03
- z/VM V5R3.0 TCP/IP LDAP Administration Guide
  - SC24-6140-00
- z/VM V5R3.0 TCP/IP User's Guide
  - SC24-6127-03
- 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