File Solutions Using Samba

Michael MacIsaac - IBM - mikemac@us.ibm.com
Tuesday February 25th, 3:00 PM
SHARE Session 9325

Abstract

Many Samba presentations focus on Samba and the basics of file serving. This presentation focuses on solutions and assumes a working knowledge of Samba. Therefore some of the more advanced features and Samba can be addressed. The solutions described include enough examples so you should be able to go back home and try each one. The issues and solutions addressed are:

- Samba political boundaries - Will the Windows administrator reset my Samba trust?
- Samba installation (distributor/custom RPM, .tar.gz), start-up script and SWAT
- Using winbind for authentication
- Using LDAP for authentication - OpenLDAP, others
- Using [homes] and automatic user creation for low maintenance
- Sharing files in teams
- Permissions and ACLs
- Data migration issues - Windows workgroups, Windows domains, Novell Netware

Outline for this hour

- Introductions and overview of Samba
- Samba solutions!
  - Simple file serving
  - Set up SWAT
  - Set up a logical volume
  - Authenticate via winbind
  - Include an adduser script
  - Authenticate via OpenLDAP
  - Share files read/write in teams
  - Set up a z/VM front end
  - Set up a time server
- Migration and coexistence
- Performance
- Documentation and resources

Introductions - Who am I?

- Michael MacIsaac
  - 16 years with IBM
    - 10 years programmer (Fortran, C, C++)
    - 6 years with S/390
  - Led teams to produce redbooks in 2001:
    - Linux on zSeries and S/390: Distributions
    - Linux on zSeries and S/390: ISP/ASP solutions
  - zSeries Linux technical support
    - Talk to customers, client reps
    - Teach IBMers and Business Partners
  - Linux (open source/freeware) advocate
  - e-mail - mikemac@us.ibm.com

Introductions - Who are you?

- What is your professional area?
  - Marketing/sales
  - Technical
  - Management
- How is Linux in your enterprise?
  - None yet
  - Some in test only
  - Some in production
  - Majority of servers in production
- What is your IS background/where will you work with Linux?
  - S/390 (Debian, Marist, Red Hat, SuSE, others?)
  - PC
  - Other
- What is your desktop?
  - Windows
  - Linux
  - Other

Enterprise View

- It's a Windows desktop world, it's a UNIX server world
- Windows desktops rule 1 and rule 2:
  - Rule 1: Windows clients should not have to be modified.
  - Rule 2: When a change is needed to Windows client, see rule 1
- Samba crosses enterprise political boundaries
  - Samba works well in small groups and among friendly fiefdoms
  - Don't try to push Samba where walls are high
  - If the NT guys have the keys, invite them over for a Linux Lunch

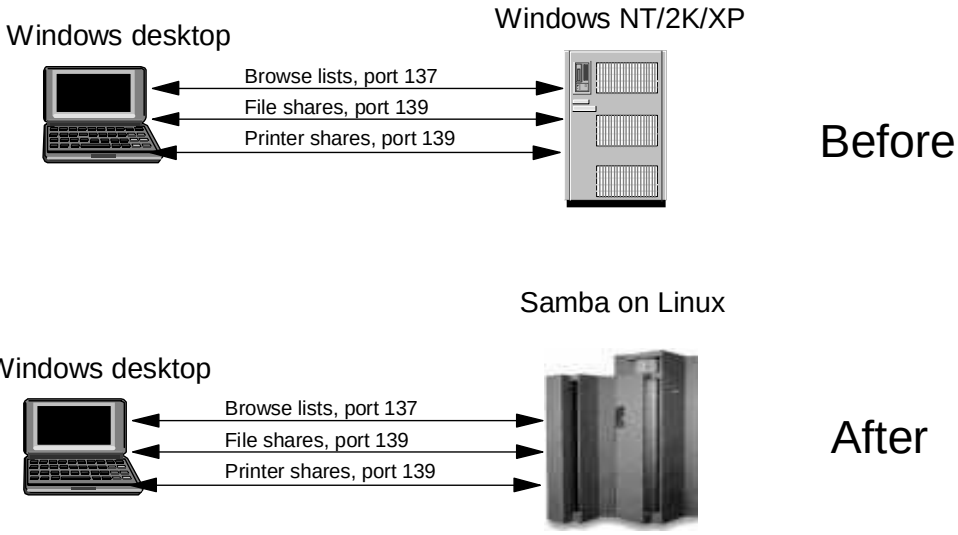
Samba background

- Samba Team
  - Has done an incredible job of "staying with" Microsoft
  - Founder Andrew Tridgell - founder:
    - Wrote Samba because it was more fun than his PhD dissertation
    - Had a Linux PC at home and wanted to share files with his wife's Windows PC
  - Some of the more prominent members:
    - Jeremy Allison
    - Gerald Carter
    - Chris Hertel
    - Richard Sharpe
    - Jim McDonough, Steve French - IBMers funded by the LTC
- License - GPL
- History - coincidentally shadows the history of Linux

Samba services

- File serving via **smbd**
  - Large file systems - LVM + journalled FS
  - Sharing files among teams
  - Using Access Control Lists
- Print serving via **smbd**
  - An existing print server must first exist - lpd, LPRng or CUPS
  - smbd acts as "middle-man" between print server and Windows clients
- Browse lists via **nmbd**
  - Viewable via "Network Neighborhood" or "My Network Places"
  - Not the UNIX model for file shares, however, useful for printers
- Time Serving via **smbd**
  - Again middleman between existing time server and Windows clients
- Domain login via **smbd**
- Authentication via **winbind** and administration via **swat**
  - Not really services, but important issues

Samba services



Samba administration

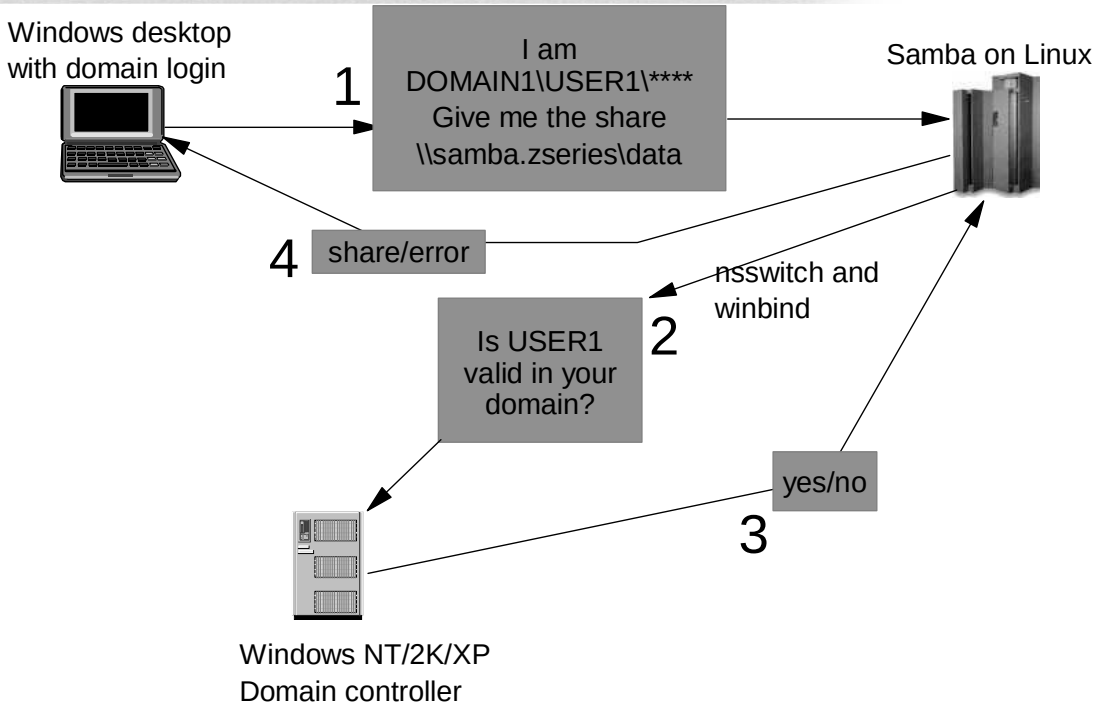
- Via the command line
  - vi, smb.conf, smbpasswd, smb startup script, log files, etc.
- SWAT - the Samba Web Administration Tool
  - Enable via inetd or xinetd
  - Sometimes using read/only is a compromise
- z/VM front end - EZLNXID
  - IBM-written freeware
  - Good for shops with better VM skills than Linux skills
  - See:

    `ftp://www.redbooks.ibm.com/redbooks/REDP3604/`

Authentication - can be done many ways

- Not at all (`guest = OK`)
- Traditional UNIX style:
  - On Linux with encrypted passwords /etc/passwd and /etc/smbpasswd
  - On Linux with unencrypted passwords - /etc/passwd - See Rule 1
- Windows NT style
  - With Samba acting as a PDC
  - On the Windows Domain Controller with winbind
  - On the Windows DC + auto home directories and /etc/passwd file
    - use the smb.conf parameter:
      `add user script = /usr/local/samba/bin/addSambauser`
    - this script is run *before* authentication is done and before a process is forked
- LDAP style
  - Allows an enterprise directory running on Linux
  - OpenLDAP seems to be getting "hot"

Solution - Authenticate via winbind



Samba installation options

- Samba Installation options
  - RPM with Linux distribution
  - Updated RPM from distributor or Web
  - Roll your own RPM
  - Build from source

Complexity ↓

Static nature of Samba version ↑

Linux for zSeries Distribution	Kernel level	Samba level
SuSE 7.0	2.2.16	2.0.7
SuSE SLES-7	2.4.7	2.2.0a
SuSE SLES-8	2.4.19	2.2.5
Red Hat 7.2	2.4.9	2.2.1a
Debian 3.0	2.4.17	2.2.3a

The smb.conf file

- The smb.conf file consists of:

```
[sections]
        parameters = values
```

- Default /etc/samba/smb.conf with SuSE SLES-8

```
[global]
        workgroup = TUX-NET
        os level = 2
        time server = yes
        unix extensions = yes
        encrypt passwords = yes
        log level = 1
        syslog = 0
        printing = CUPS
        printcap name = CUPS
        socket options = SO_KEEPALIVE IPTOS_LOWDELAY TCP_NODELAY
        wins support = no
        veto files = /*.eml/*.nws/riched20.dll/*.{*}/
```

- Other special sections

```
[homes]
[printers]
[print$]
[netlogon]
```

Solution - simple file serving

- Verify that Samba is installed

```
# rpm -q | grep samba
```

- Add some shares to smb.conf

```
# cd /etc/samba
# vi smb.conf  ...  add the following lines
        netbios name = mp3klnx3
        interfaces = 9.117.119.67/24    # needed with CTC interfaces
[sharedocs]
        path = /usr/share/doc/packages

[sambadocs]
        path = /usr/src/samba/docs
```

- Add a user

```
# useradd user01
# mkdir ~user01
# chown user01.users ~user01
# passwd user01
...
# smbpasswd -a user01
...
# cat /etc/samba/smbpasswd
...
user01:501:E77101BFD32FF9EBAAD3B435B51404EE:...:[UX   ]:LCT-3E26BAF1:
```

Solution - simple file serving

- Start Samba if not running

```
# ls -l `which rcsmb`
lrwxrwxrwx  1 root  20 Jan 14 /usr/sbin/rcsmb -> ../../etc/init.d/smb*
# rcnmb start          # needed with SLES-8, not SLES-7, Red Hat
Starting Samba ldap NMB daemon                                  done
# rcsmb start
Starting Samba ldap SMB daemon                                  done
```

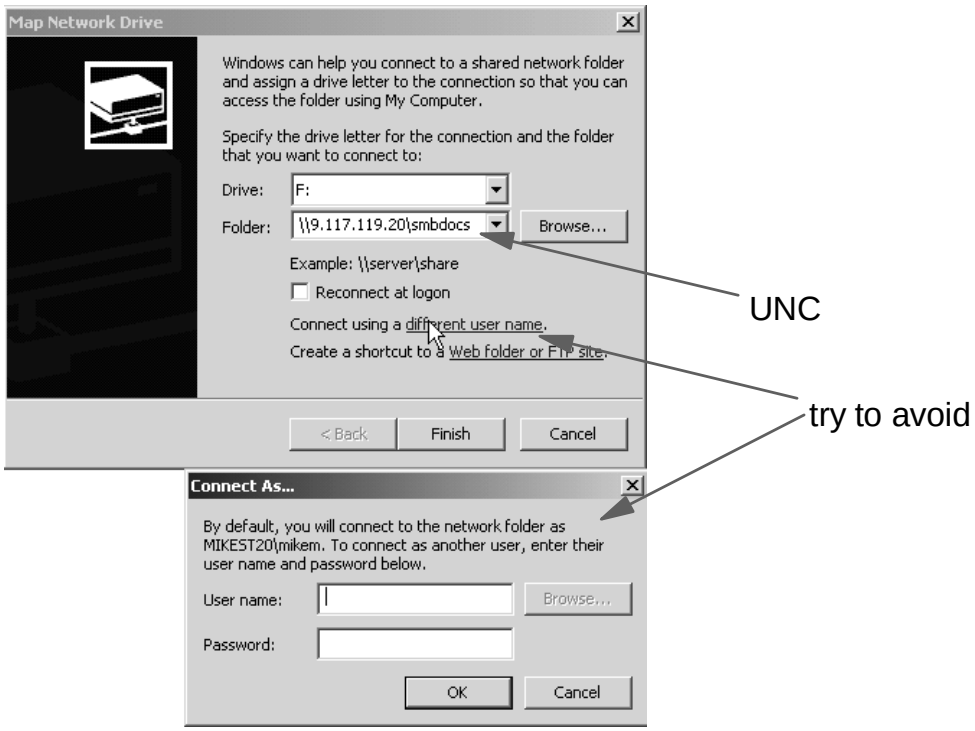
- Set Samba to start at boot time, if not set

```
# ls -l /etc/init.d/rc3.d/*[sn]mb
ls: /etc/init.d/rc3.d/*[sn]mb: No such file or directory
# chkconfig nmb on
# chkconfig smb on
# ls -l /etc/init.d/rc3.d/*[sn]mb
lrwxrwxrwx 1 root   6 Jan 17 07:46 /etc/init.d/rc3.d/K08smb -> ../smb*
lrwxrwxrwx 1 root   6 Jan 17 07:46 /etc/init.d/rc3.d/K14nmb -> ../nmb*
lrwxrwxrwx 1 root   6 Jan 17 07:46 /etc/init.d/rc3.d/S09nmb -> ../nmb*
lrwxrwxrwx 1 root   6 Jan 17 07:46 /etc/init.d/rc3.d/S15smb -> ../smb*
```

- Get a share from Windows
  - DOS prompt:

```
C:\>net use * \\9.117.99.215\smbdocs
Drive F: is now connected to \\9.117.99.215\smbdocs.
C:\> F:
```

Solutions - simple file serving: Map Network Drive



Solutions - set up SWAT

- SWAT is typically available but commented out in inetd.conf

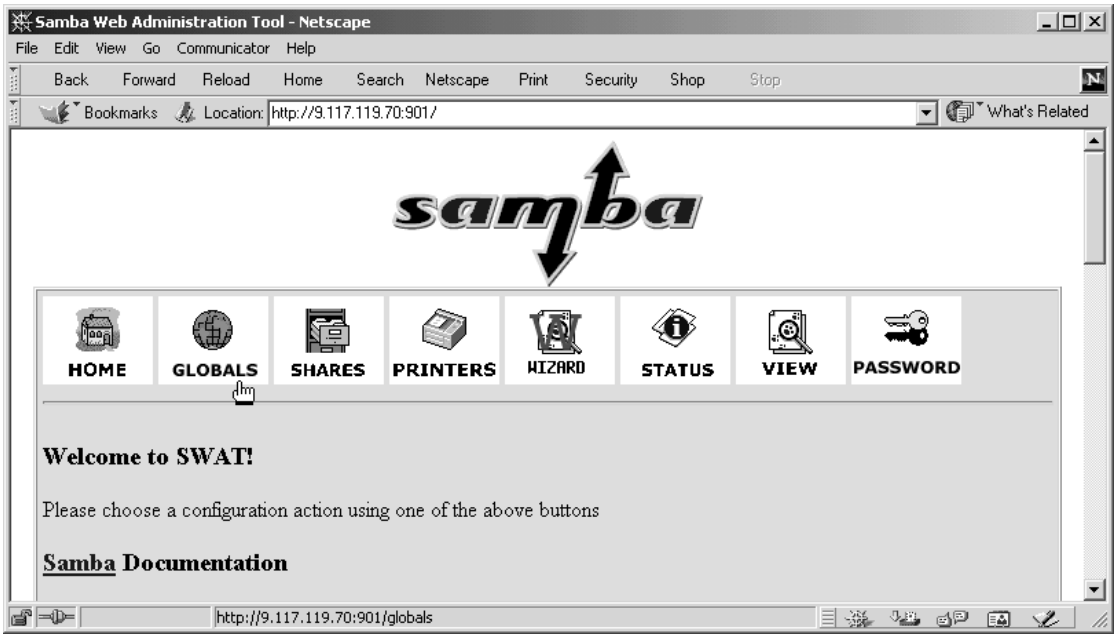
```
# which swat
/usr/sbin/swat
# cd /etc
# grep swat services inetd.conf
services:swat           901/tcp         # CONFLICT, not official
inetd.conf:# swat is the Samba Web Administration Tool
inetd.conf:# swat stream  tcp nowait.400  root    /usr/sbin/swat  swat
# vi inetd.conf               # just remove the pound sign (hash)
# rcinetd status
Checking for inetd:                                          unused
mp3klnx6:/etc # rcinetd start
Starting inetd                                               done
```

  - If your system uses xinetd, create a file /etc/xinetd/swat appropriately
- Enable inetd to start at IPL time (SLES-8)

```
# chkconfig inetd
inetd  off
# chkconfig inetd on
```

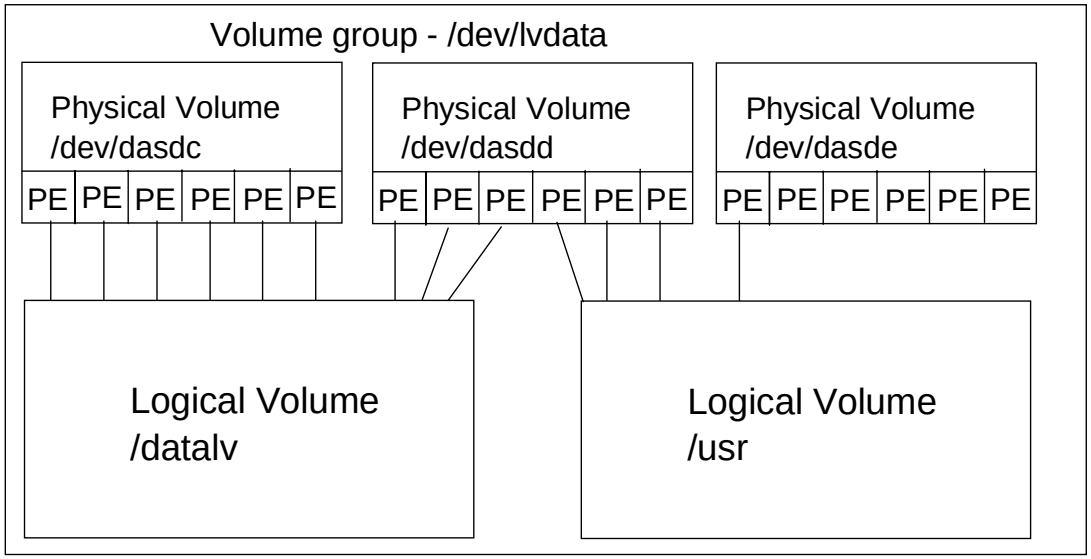
- Point browser to http://your.server.name:901

Solutions - SWAT main page



Solution - set up a logical volume

- LVM block diagram



Solution - Set up a logical volume (cont'd)

- Overall
  - Get some DASD defined to the VM user ID
  - Add the DASD in Linux
  - Format each DASD, carve into a single partition and verify
  - Create physical volumes for each DASD
  - Verify physical volumes
  - Create the volume group and verify
  - Create a striped logical volume using most of the volume group
  - Create a journalled file system and mount the logical volume
  - Give group write privileges and make a Samba share of the directory:
  - Set the LVM to come up at IPL (boot) time

Solution - Set up a logical volume (cont'd)

- Get some DASD defined to the VM user ID

```
USER MP3KLNX6 LNX6 128M 512M     G
 INCLUDE LNXDFLT
 MDISK 100 3390 0001 3338 VM20F  MR RPASS WPASS MPASS
 MDISK 101 3390 0751 0100 VM218  MR RPASS WPASS MPASS
 MDISK 200 3390 0001 3338 VM210  MR RPASS WPASS MPASS
 MDISK 201 3390 0001 3338 VM211  MR RPASS WPASS MPASS
 MDISK 202 3390 0001 3338 VM212  MR RPASS WPASS MPASS
 MDISK 203 3390 0001 3338 VM213  MR RPASS WPASS MPASS
 MDISK 204 3390 0001 3338 VM214  MR RPASS WPASS MPASS
 MDISK 191 3390 0851 0050 VM218  MR RPASS WPASS MPASS
```

- Add the DASD in Linux

```
# dasd add 200-204
# dasd list
0100(ECKD) at ( 94:  0) is dasda : active at blksz: 4096, 2347 MB
0101(ECKD) at ( 94:  4) is dasdb : active at blksz: 4096, 70 MB
0200(ECKD) at ( 94:  8) is dasdc : active n/f
0201(ECKD) at ( 94: 12) is dasdd : active n/f
0202(ECKD) at ( 94: 16) is dasde : active n/f
0203(ECKD) at ( 94: 20) is dasdf : active n/f
0204(ECKD) at ( 94: 24) is dasdg : active n/f
```

Sidebar - dasd script

- Sidebar - neat script (from "Large Scale Deployment" redbook)

```
# cat `which dasd`
#!/bin/sh
# dasd - simple utility for dynamic DASD management
if [ "$1" = "add" -a "$2" != "" ]; then
  echo "add range=$2" > /proc/dasd/devices
elif [ "$1" = "on" -a "$2" != "" ]; then
  echo "set device range=$2 on" > /proc/dasd/devices
elif [ "$1" = "off" -a "$2" != "" ]; then
  echo "set device range=$2 off" > /proc/dasd/devices
elif [ "$1" = "list" ]; then
  cat /proc/dasd/devices
else
  echo "Usage: dasd add|on|off vdev_or_range" 1>&2
  echo " dasd list" 1>&2
  exit 2
fi
```

Solution - Set up a logical volume (cont'd)

- Format each DASD, carve into a single partition and verify

```
# for i in c d e f g
> do
>  dasdfmt -b 4096 -y -f /dev/dasd$i
>  fdasd -a /dev/dasd$i
> done
Finished formatting the device.
Rereading the partition table... ok
...
# dasd list
0100(ECKD) at ( 94:  0) is dasda : active, 2347 MB
0101(ECKD) at ( 94:  4) is dasdb : active, 70 MB
0200(ECKD) at ( 94:  8) is dasdc : active, 2347 MB
...
0204(ECKD) at ( 94: 24) is dasdg : active, 2347 MB
```

- Initialize LVM

```
# vgscan
vgscan -- reading all physical volumes (this may take a while...)
vgscan -- "/etc/lvmtab" and "/etc/lvmtab.d" successfully created
vgscan -- This program does not do a VGDA backup of your volume group
```

Solution - Set up a logical volume (cont'd)

- Create physical volumes for each DASD

```
# pvcreate /dev/dasd[cdefg]1
pvcreate -- physical volume "dasdc1" successfully created
pvcreate -- physical volume "dasdd1" successfully created
pvcreate -- physical volume "dasde1" successfully created
pvcreate -- physical volume "dasdf1" successfully created
pvcreate -- physical volume "dasdg1" successfully created
```

- Verify physical volumes

```
# pvscan
pvscan -- reading all physical volumes (this may take a while...)
pvscan -- inactive PV "/dev/dasdc1" is in no VG  [2.29 GB]
pvscan -- inactive PV "/dev/dasdd1" is in no VG  [2.29 GB]
pvscan -- inactive PV "/dev/dasde1" is in no VG  [2.29 GB]
pvscan -- inactive PV "/dev/dasdf1" is in no VG  [2.29 GB]
pvscan -- inactive PV "/dev/dasdg1" is in no VG  [2.29 GB]
pvscan -- tot: 5 [11.46 GB] / in use: 0 [0] / in no VG: 5 [11.46 GB]
```

Solution - Set up a logical volume (cont'd)

- Create the volume group and verify:

```
# vgcreate datavg /dev/dasd[cdefg]1
vgcreate -- INFO: using default physical extent size 4 MB
vgcreate -- INFO: maximum logical volume size is 255.99 Gigabyte
vgcreate -- doing automatic backup of volume group "datavg"
vgcreate -- volume group "datavg" successfully created and activated
#  ls -ld /dev/datavg
dr-xr-xr-x    2 root     root     72 Jan 16 14:29 /dev/datavg/
# ls -l /dev/datavg
crw-r-----    1 root     disk     109,   0 Jan 16 14:06 group
# vgdisplay datavg | grep Size
MAX LV Size           255.99 GB
VG Size               11.43 GB
PE Size               4 MB
Alloc PE / Size       0 / 0
Free  PE / Size       2925 / 11.43 GB
```

Solution - Set up a logical volume (cont'd)

- Create a striped logical volume using most of the volume group

```
# lvcreate --stripes 5 --size 9G -n lv1 /dev/datavg
lvcreate -- INFO: using default stripe size 16 KB
lvcreate -- rounding to stripe boundary size
lvcreate -- doing automatic backup of "datavg"
lvcreate -- logical volume "/dev/datavg/lv1" successfully created
# lvdisplay /dev/datavg/lv1
--- Logical volume ---
LV Name                /dev/datavg/lv1
VG Name                datavg
LV Write Access        read/write
LV Status              available
LV #                   1
# open                 2
LV Size                9 GB
Current LE             2305
Allocated LE           2305
Stripes                5
...
# vgdisplay datavg | grep Size
MAX LV Size            255.99 GB
VG Size                11.43 GB
PE Size                4 MB
Alloc PE / Size        2305 / 9 GB
Free  PE / Size        620 / 2.42 GB
```

Solution - Set up a logical volume (cont'd)

- Create a journalled file system and mount the logical volume

```
# mkreiserfs /dev/datavg/lv1
...
# mkdir /data
# mount /dev/datavg/lv1 /data
# df -h
Filesystem            Size  Used Avail Use% Mounted on
/dev/dasda1           2.3G  1.3G  1.1G  55% /
shmfs                  62M     0   62M   0% /dev/shm
/dev/datavg/lv1       9.1G   33M  9.0G   1% /data
```

- Give group write privileges and make a Samba share of the directory:

```
# cd /
# chown root.users data
# chmod g+w data
# ls -ld data
drwxrwxr-x    3 root     users          48 Jan 16 14:44 data/
# cd /etc/samba
# vi smb.conf                          # add the entry
# cat smb.conf
...
[data]
        path = /data
        read only = no
```

Solution - Set up a logical volume (cont'd)

- Set the LVM to come up at IPL (boot) time

```
# cd /etc
# cp zipl.conf zipl.conf.orig
# vi zipl.conf                          # add DASD 200-204
# cat zipl.conf
...
[ipl]
target=/boot/zipl
image=/boot/kernel/image
ramdisk=/boot/initrd
parameters="dasd=100-101,200-204 root=/dev/dasda1"
...
# zipl
# cp fstab fstab.orig
# vi /etc/fstab                         # and add a line
# cat /etc/fstab
/dev/dasda1          /           reiserfs   defaults              1 1
/dev/datavg/lv1      /data       reiserfs   defaults              0 2
/dev/dasdb1          swap        swap       pri=42                0 0
devpts               /dev/pts    devpts     mode=0620,gid=5       0 0
proc                 /proc       proc       defaults              0 0
# shutdown -r now
...
```

Solution - Authenticate via winbind

- Overall steps:
  - Create an lmhosts file
  - winbind library in /lib
  - Modify nsswitch.conf to use winbind
  - Stop or restart nscd so it won't use its cache
  - Join the Windows domain
  - Start Samba and winbind
  - Test getting a share using domain credentials

Solution - Authenticate via winbind (cont'd)

- Create an lmhosts file with the assumptions
  - NT server IP = 7.117.119.70, NetBIOS name = LCCWIN2K
  - The server is Domain Controller for the domain POKLCC

```
# cd /etc/samba
# vi lmhosts                        #add two lines
# cat lmhosts
9.117.119.70 LCCWIN2K
9.117.119.70 POKLCC
```

- Verify or copy winbind library to /lib

```
# locate libnss | grep winbind
/lib/libnss_winbind.so
/lib/libnss_winbind.so.2
```

  - If building from source:

```
# cd /usr/src/samba/source/nsswitch/
# cp libnss_winbind.so /lib/libnss_winbind.so.2
```

- Modify the /etc/nsswitch.conf file to use the new library.

```
# cd /etc
# cp nsswitch.conf nsswitch.conf.orig
# vi nsswitch.conf     # add "winbind" to the passwd and group lines:
passwd: files winbind
group:  files winbind
```

Solution - Authenticate via winbind (cont'd)

- Make the libnss_winbind library available

```
# ldconfig -v | grep winbind
```

- Restart the name service caching daemon (if running) so it will not look for names in its cache.

```
# /etc/init.d/nscd restart
Shutting down Name Service Cache Daemon                    done
Starting Name Service Cache Daemon                         done
```

- Join the domain via the **smbpasswd** command with the -j and -r flags.

```
# smbpasswd -j POKLCC -r LCCWIN2K
2002/07/30 09:55:56 : change_trust_account_password: Changed \
password for domain POKLCC.
Joined domain POKLCC.
```

- Start Samba and verify it is running

```
# /etc/init.d/smb start
Starting SAMBA nmbd :                                      done
Starting SAMBA smbd :                                      done
Starting SAMBA winbindd :                                  done
```

  - **Note:** SuSE SLES-8 has split this into 3 scripts - smb, nmb and winbind

Solution - Authenticate via winbind (cont'd)

- List the users, groups and machine trust in the POKLCC domain

```
# wbinfo -u
POKLCC+Administrator
POKLCC+Guest
...
# wbinfo -g
POKLCC+Domain Admins
POKLCC+Domain Users
...
# wbinfo -t
Secret is good
```

- Try to identify the a specific domain user:

```
# id POKLCC+user1
uid=10008(POKLCC+user1) gid=10001(POKLCC+Domain Users) \
 groups=10001(POKLCC+Domain Users)
```

Solution - Include an adduser script

- When winbind is authenticating it is nice for all administration to be done on the Windows PDC
- Often a share for each user is desirable
  - The [homes] section allows for a no-maintenance smb.conf file
  - But [homes] goes to /etc/passwd for $HOME - so an automated /etc/passwd is needed
  - Samba has an smb.conf parm named **add user script** - desc from swat:

```
For sites that use Windows NT account databases as their primary
user database creating these users and keeping the user list in
sync with the Windows NT PDC is an onerous task. This option allows
smbd to create the required UNIX users ON DEMAND when a user
accesses the Samba server.
When the Windows user attempts to access the Samba server, at login
(session setup in the SMB protocol) time, smbd contacts the password
server and attempts to authenticate the given user with the given
password. If the authentication succeeds then smbd attempts to find
a UNIX user in the UNIX password database to map the Windows user
into. If this lookup fails, and add user script is set then smbd
will call the specified script AS ROOT, expanding any %u argument
to be the user name to create.
```

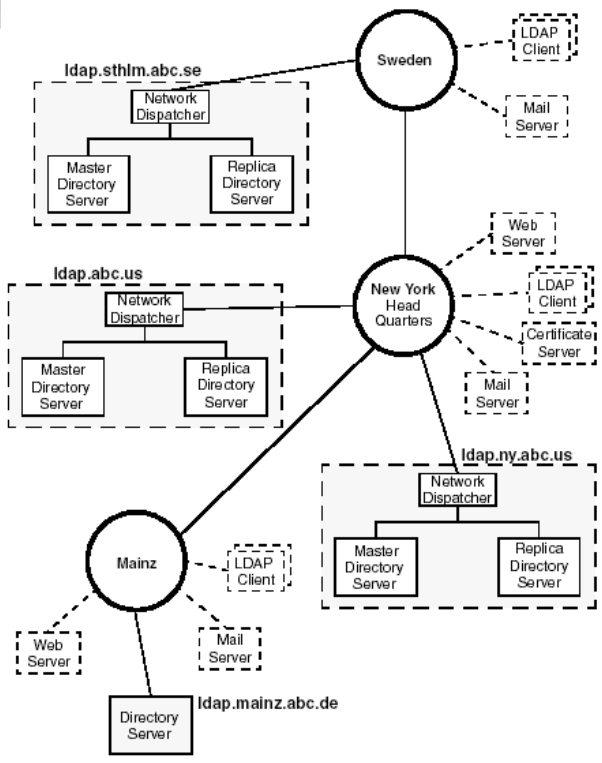
Solution - An add user script

```
#!/bin/sh
# add user and create home directory for the Samba [homes] share
# 1 arg = user name in form DOMAIN+userid - first set some variables
umask 077
dt=`date`
group="POKLCC+Domain Users"
userid=`echo $1 | sed s/poklcc+//`
logFile=/tmp/addSambaHomeLog.txt
# be sure the Windows user has a valid UID and the home directory doesn't exist
uid=`id -u $1`
rc=$?
if [ $rc != 0 ]; then
  echo "$dt: error in $0: id $1 returned $rc" >> $logFile
  exit 1
fi
if [ -d /home/$userid ]; then
  echo "$dt: error in $0: /home/$userid already exists" >> $logFile
  exit 2
fi
# append to /etc/passwd and create home directory
# we can't use the useradd command here because we want the Linux user name
# to be the Windows user name without the leading DOMAIN+
# useradd won't allow adding an ID with a duplicate UID
passwdEntry="$userid:x:$uid:ID for Samba homes:/home/$userid:/bin/false"
echo $passwdEntry >> /etc/passwd
mkdir /home/$userid
chown "$1.$group" /home/$userid
# log action
echo "$dt: added userid: $userid group: $group" >> $logFile
```

Solution - Authenticate via OpenLDAP

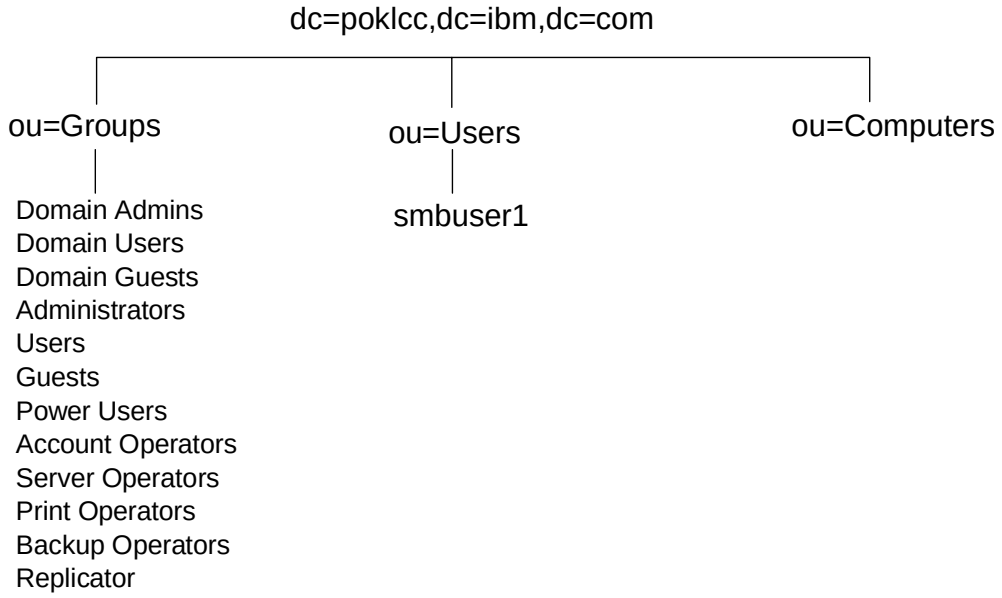
LDAP can become a complex solution:

Example of a more sophisticated LDAP architecture



Solution - Authenticate via OpenLDAP

Example Domain Information Tree (DIT)



Solution - Authenticate via OpenLDAP (cont'd)

- This is the Samba and LDAP LCD - Overall steps:
  1. Get OpenLDAP
  2. Get Samba binaries with LDAP support compiled in
  3. Configure the LDAP server (/etc/openldap/slapd.conf)
  4. Configure the LDAP client (/etc/openldap/ldap.conf)
  5. Start LDAP server and insert base objects
  6. Copy and configure smbldap tools
  7. Configure Linux to use LDAP
  8. Add a Samba user and password
- 1. Get OpenLDAP
  - SuSE SLES-8 in this example has OpenLDAP installed
  - Or go to:

    `http://www.openldap.org/`
  - Verify that you have OpenLDAP installed:

```
# rpm -qa | grep openldap
openldap2-client-2.1.4-26
openldap2-2.1.4-26
# rcldap status
Checking for service ldap:                    unused
```

Solution - Authenticate via OpenLDAP (cont'd)

- 2. Get Samba binaries with LDAP support compiled in
  - Samba has to be compiled with the configure option **--with-ldapsam**
  - SuSE SLES-8 has Samba built with both ldap and non-ldap (classic)

```
# tail -2 /etc/sysconfig/samba
#SAMBA_SAM="classic"
SAMBA_SAM="ldap"
# SuSEconfig --module samba
...             # symbolic links are reset to ldap binaries
# ls -l /usr/sbin/swat /var/lib/samba/bin/swat
lrwxrwxrwx    1 root     root           23 Feb  4 13:35
 /usr/sbin/swat -> /var/lib/samba/bin/swat*
lrwxrwxrwx    1 root     root           24 Feb  4 14:59
 /var/lib/samba/bin/swat -> /usr/lib/samba/ldap/swat*
```

  - Startup script /etc/init.d/smb uses this variable (no changes needed):

```
DAEMON_DIR="/usr/lib/samba/"
SMBD_BIN="smbd"
SYSCONFIG_FILE="/etc/sysconfig/samba"
. $SYSCONFIG_FILE
BIN_SUFFIX=$( echo ${SAMBA_SAM} | tr '[:upper:]' '[:lower:]')
startproc -p $SMBD_PID_FILE $DAEMON_DIR$BIN_SUFFIX/$SMBD_BIN -D
```

Solution - Authenticate via OpenLDAP (cont'd)

- 3. Configure the LDAP server (/etc/openldap/slapd.conf)

```
# cd /usr/share/doc/packages/samba/examples/LDAP
# cp samba.schema /etc/openldap/schema
# cat slapd.conf
# global directives
include         /etc/openldap/schema/core.schema
include         /etc/openldap/schema/cosine.schema
include         /etc/openldap/schema/inetorgperson.schema
include         /etc/openldap/schema/nis.schema
include         /etc/openldap/schema/samba.schema
pidfile         /var/run/slapd/slapd.pid
argsfile        /var/run/slapd/slapd.args

# database definition and configuration directives
database        bdb
suffix          "dc=poklcc,dc=ibm,dc=com"
rootdn          "cn=Manager,dc=poklcc,dc=ibm,dc=com"
rootpw          secret
directory       /var/lib/ldap
index   objectClass     eq
```

Solution - Authenticate via OpenLDAP (cont'd)

- 4. Configure the LDAP client (/etc/openldap/ldap.conf)

```
# cat ldap.conf
host    localhost
BASE    dc=poklcc,dc=ibm,dc=com

nss_base_passwd dc=poklcc,dc=ibm,dc=com?sub
nss_base_shadow dc=poklcc,dc=ibm,dc=com?sub
nss_base_group ou=Groups,dc=poklcc,dc=ibm,dc=com?one
ssl no
pam_password md5
```

Solution - Authenticate via OpenLDAP (cont'd)

- 5. Start LDAP server and insert base objects

```
# rcldap status
Checking for service ldap:                                  unused
# rcldap start
Starting ldap-server                                        done
```

- See http://www.idealx.org/

```
# ldapadd -x -h localhost -D "cn=manager,dc=poklcc,dc=ibm,dc=com"
  -f IDEALXbase.ldif -W
Enter LDAP Password:
adding new entry "dc=poklcc,dc=ibm,dc=com"

adding new entry "ou=Groups,dc=poklcc,dc=ibm,dc=com"
...
# ls -l /var/lib/ldap
total 176
-rw-------  ldap     8192 Jan 31 11:40 __db.001        <- The Schema
-rw-------  ldap   270336 Jan 31 11:40 __db.002
-rw-------  ldap    98304 Jan 31 11:40 __db.003
-rw-------  ldap   360448 Jan 31 11:40 __db.004
-rw-------  ldap    16384 Jan 31 11:40 __db.005
-rw-------  ldap     8192 Jan 31 11:40 dn2id.bdb
-rw-------  ldap    32768 Jan 31 11:40 id2entry.bdb
-rw-------  ldap    79663 Jan 31 11:42 log.0000000001
-rw-------  ldap    20480 Jan 31 11:42 objectClass.bdb  <- The DATA
```

Solution - Authenticate via OpenLDAP (cont'd)

- 6. Copy and configure smbldap tools (mkntpwd + smb Perl scripts):

```
# cd /usr/share/doc/packages/samba/examples/LDAP/smbldap-tools
# cp smb* /usr/local/sbin
# cd mkntpwd
# make
...
# cp mkntpwd /usr/local/sbin
# cd /usr/local/sbin
# chmod +x smb* mkntpwd
# vi smbldap_conf.pm           # change the following 8 lines:
$slaveLDAP = "127.0.0.1";
$masterLDAP = "127.0.0.1";
$suffix = "dc=poklcc,dc=ibm,dc=com";
$usersdn = "ou=Users,$suffix";
$computersdn = "ou=Computers,$suffix";
$groupsdn = "ou=Groups,$suffix";
$binddn = "cn=Manager,$suffix";
$bindpasswd = 'secret';
$_userLoginShell = q(/bin/bash);
$_userHomePrefix = q(/home/);
```

Solution - Authenticate via OpenLDAP (cont'd)

- 7. Configure Linux to use LDAP

Configure PAM

```
# cat /etc/pam.d/login
#%PAM-1.0
auth sufficient pam_unix2.so    nullok     #set_secrpc
auth sufficient pam_ldap.so     use_first_pass
auth required   pam_securetty.so
auth required   pam_nologin.so
auth required   pam_env.so
auth required   pam_mail.so
account required    pam_unix2.so
password required   pam_pwcheck.so  nullok
password sufficient pam_unix2.so    nullok use_first_pass use_authtok
password sufficient pam_ldap.so     use_authtok
session required    pam_unix2.so    none     # debug or trace
session required    pam_limits.so
```

Solution - Authenticate via OpenLDAP (cont'd)

7. Configure Linux to use LDAP (cont'd)

Configure the name service switch

```
# cat /etc/nsswitch.conf
passwd: compat ldap
group:  compat ldap
hosts:          files dns
networks:       files dns
services:       files ldap
protocols:      files ldap
rpc:            files ldap
ethers:         files ldap
netmasks:       files ldap
netgroup:       files ldap
publickey:      files ldap
bootparams:     files
automount:      files nis ldap
aliases:        files
```

Solution - Authenticate via OpenLDAP (cont'd)

- 8. Add a Samba user and password
  - First, leave your root session open and try to telnet/ssh in
  - Add a user:

```
# cd /usr/local/sbin
# smbldap-useradd.pl -m smbuser1
```

  - Set a password:

```
# ./smbldap-passwd.pl smbuser1
Changing password for smbuser1
New password :
Retype new password :
all authentication tokens updated successfully
```

  - See the user in the DIT:

```
# ldapsearch -x uid=smbuser1
```

Solution - Authenticate via OpenLDAP (cont'd)

- Good LDAP tool: web2ldap - mini Web server that runs on LDAP server

```
http://www.web2ldap.de/
```

- Download and FTP to your Linux LDAP server, then:

```
# tar xzf web2ldap-0.11.9.tar.gz
# cd web2ldap-0.11.9/
```

- This didn't work - drop it?
- How about diradmin - a GUI front end

```
http://diradmin.open-it.org/files.php
FTP it to Linux
Had to install gnome-libs-devel-1.4.1.7 and gtk2-devel-2.0.6 first
# tar xzf directory_administrator-1.3.4.tar.gz
# cd directory_administrator-1.3.4/
# ./configure
died on GTK error
```

- How about gq

```
http://biot.com/gq/
```

Solution - Share files read/write in teams

- UNIX (Linux) groups work well
  - Users can belong to multiple groups
  - Assumption: 1 Linux group = 1 team = 1 directory = 1 Samba share
  - Should work equally well from both Windows (SMB share) and Linux (telnet/ssh session) interfaces
  - The following things should be true:
    1. The group (team) must exist
    2. Users must be members of the goup
    3. Files and directories created by group members set the group owner correctly.
    4. Files and directories created have the group write permission bit set
  - To effect on Linux (assume **security = user** for now):
    1. **groupadd** <teamName> command
    2. **useradd -G** <teamName> <user> command with (supplemental groups)
    3. **chmod g+s** <sharePath> command - turns set group ID bit on
    4. **umask 002** - turns (default is usually umask 022)

Solution - Share files read/write in teams

- To effect on Windows
  - Set directory name = group name

```
 # ls -l /data
drwxrwsr-x    2 root     redp3604       48 Jan 20 09:02 redp3604/
drwxrwsr-x    2 root     redp3605       48 Jan 20 09:02 redp3605/
```

  - Example share definition

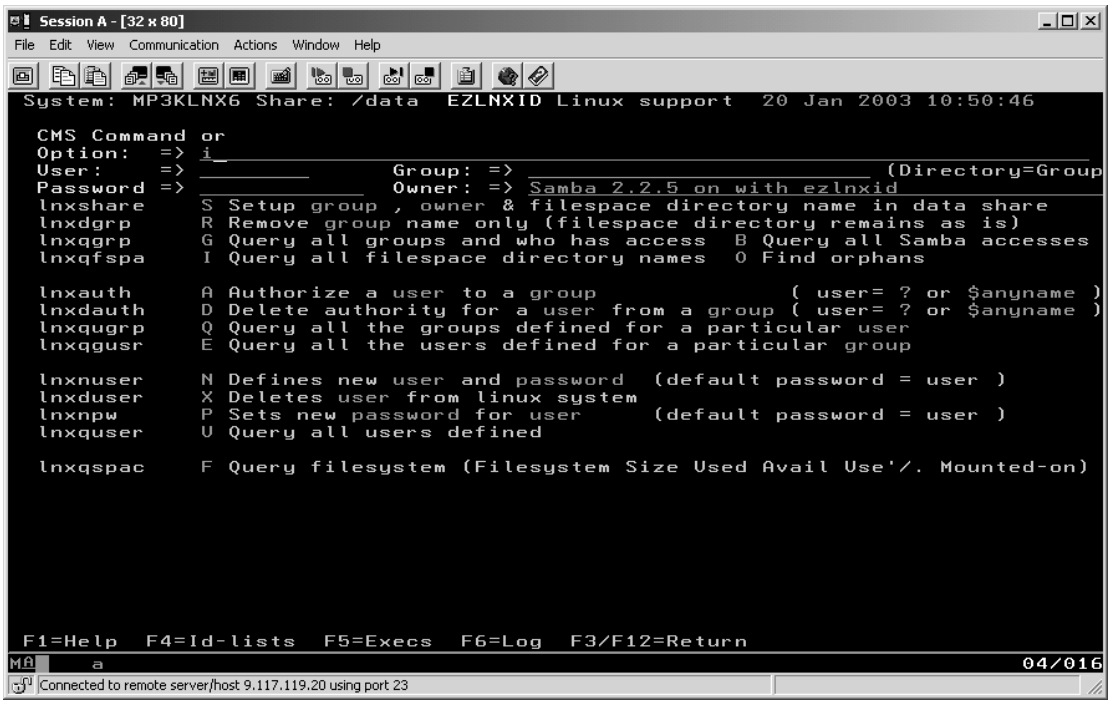
```
[redp3604]
       comment = new group redp3604
       path = /data/redp3604
       writeable = Yes
       force group = +redp3604
       create mask = 0775
       directory mask = 0775
       force directory mode = 2775
```

Solution - Set up a z/VM front end

- The tool EZLNXID was written at ITSO in Poughkeepsie, NY
- Gives a z/VM front-end with a Linux back-end via REXX/regina
- Allows users, groups, passwords and shares to be manipulated:
  - Define new users and sets Linux and Samba passwords
  - Define new groups for access to Samba file systems
  - Create new file system directories
  - Creates Samba share definitions for the Linux file system
  - Authorizes new and existing users to groups
  - Change passwords, both for Linux and Samba
  - Removes users from groups
  - Removes users from Linux system
  - List users, groups, Samba shares, and Linux file system usage
- Create a huge logical volume under /data, for example, and add shares beneath that
- Think of a SWAT for VM
- See the redpaper "*Linux on IBM zSeries and S/390: Managing a Samba Server From z/VM*", on the Web at:

  `http://publib-b.boulder.ibm.com/Redbooks.nsf/RedpaperAbstracts/redp3604.html`

Solution - Set up a z/VM front end (cont'd)



Solution - Migration and coexistense

- Migration and coexistence - no "best practices"
  - There are issues:
    - Winbind mapping of NT RID to Linux UID is dynamically allocated
    - How to backup/restore to same UID
    - POSIX ACLs are slightly different than Windows ACLs
  - There are a lot of tools to work around these issues
    - Winbind (today)
    - Active directory support (Samba 3.0)
    - tar/zip + FTP
    - Drag and drop
    - Scripts

Samba Performance

- Observations by the Linux Scalability Center:
  - With a single Gbe OSA card up to 25 guests with one concurrent request each and an aggregate throughput of 13.37 MB/second could be supported. Maximum OSA throughput was reached between 12-15 SMB processes.
  - With a single guest server and a single OSA card we were able to support up to 30 concurrent users at an aggregate throughput of 19.4 MB/second.
  - Summary of Native results vs. VM guest results. The cost in throughput between the 2.4.17 kernel in a native LPAR vs. running the timer change version of this kernel on z/VM is most significant with small numbers of Guests.
    - Cost for the first 1-10 guests was 20-26% total.
    - Cost for 15 - 35 guest was only 9.7-16% total.
  - SuSE SLES 7 throughput is not as good as new internal kernel. At 35 connections the 2.4.17 Timer kernel produced up to 125% improvement over SuSE SLES 7. It is likely that significant improvement would be seen in SuSE SLES 8 vs. SLES 7.

Samba Performance (cont'd)

- Recommendations by the IBM Linux Scalability Center
  - Network configuration for communications: Use direct connections from OSA gigabit or fast ethernet cards to each Samba server guest.
  - If the configuration must use connections to one or more Linux guests used as a router, the recommendations for routing are as follows:
    - Use VM guest LAN rather than VCTC to connect the guests to the Linux system that is providing routing capability, or
    - Use VM TCP/IP routing from the OSA card to the guest servers.
  - Recommended virtual memory size: 128 MB. If a large number of guests are to be implemented, the goal should be to keep the Samba server virtual memory size as small as possible while avoiding Linux guest paging.
  - Real memory: to avoid paging, 128 MB per guest is recommended.
  - Minidisk caching was of little value and used a large amount of VM storage.

Samba Performance (cont'd)

- Recommendations by the Linux Scalability Center (cont'd)
  - The SuSE SLES 7 (2.4.7 kernel) QDIO communications provided significantly less throughput than the 2.4.17 kernel. With the changes provided in the 2.4.17 kernel and device drivers, the internal throughput improved by up to 100% in a heavily loaded guest, and by approximately 15% in a lightly loaded multiple guest configuration.
  - Download the latest QETH and QDIO device drivers supported for your kernel from IBM developerWorks to ensure that the installation is running at peak
- Recommendations from unofficial testing
  - The following smb.conf settings may give you better performance.

```
max xmit = 8192
socket options = TCP_NODELAY IPTOS_LOWDELAY \
  SO_SNDBUF=14596 SO_RCVBUF=14596
dead time = 10
```

Documentation and resources

- Documentation
  - SuSE docs, including Samba docs

```
[sharedocs]
        path = /usr/share/doc/packages
```

  - *Using Samba*, Jay Ts, Robert Eckstein, David Collier-Brown (2nd ed)
  - SWAT - includes *Using Samba* (1st edition) on line
  - *SAMBA Essentials for Windows Administrators*, Gary Wilson
  - Redbooks
    - *Linux for S/390*
      `http://www.redbooks.ibm.com/abstracts/sg244987.html`
    - *Linux for zSeries and S/390: Distributions*
      `http://www.redbooks.ibm.com/abstracts/sg246264.html`
    - *Understanding LDAP* , SG24-4986
      `http://www.redbooks.ibm.com/abstracts/sg244986.html`

Documentation and resources (cont'd)

- Web sites
  - Linuxvm.org - the Linux on zSeries portal:
    `http://linuxvm.org`
  - DeveloperWorks - IBM Boeblingen
    `http://www10.software.ibm.com/developerworks/opensource/linux390/index.shtml`
  - ISV applications for Linux on zSeries:
    `http://www.ibm.com/servers/eserver/zseries/solutions/s390da/linuxproduct.html`
  - z/VM and Linux:
    `http://www.vm.ibm.com/linux`
  - linux-390 archives:
    `http://www.marist.edu/htbin/wlvindex?linux-390`
  - z/VM publications:
    `http://www.vm.ibm.com/pubs/`
- Mailing lists
  - linux-390 mailing list (subscribe at bottom of page)
    `http://www.marist.edu/htbin/wlvindex?linux-390`
  - Samba mailing list (this host or other mirror)
    `http://us2.samba.org/samba/archives.html`

Questions??