

# Samba 3 PDC for Windows Clients and Samba 3 Book Review

Michael Lueck, Lueck Data Systems  
Sr. Director of Technologies  
[mlueck@lueckdatasystems.com](mailto:mlueck@lueckdatasystems.com)

International Conference on Computing and Mission  
June 8 - June 12, 2007  
Taylor University

# Samba - Where and What?

Samba provide SMB style file and print sharing on top of GNU Linux and other operating systems...

Application:  
Samba

smbpasswd, netgroup

Computers / Workgroups

Share: Files and Printers

Operating System:  
GNU Linux

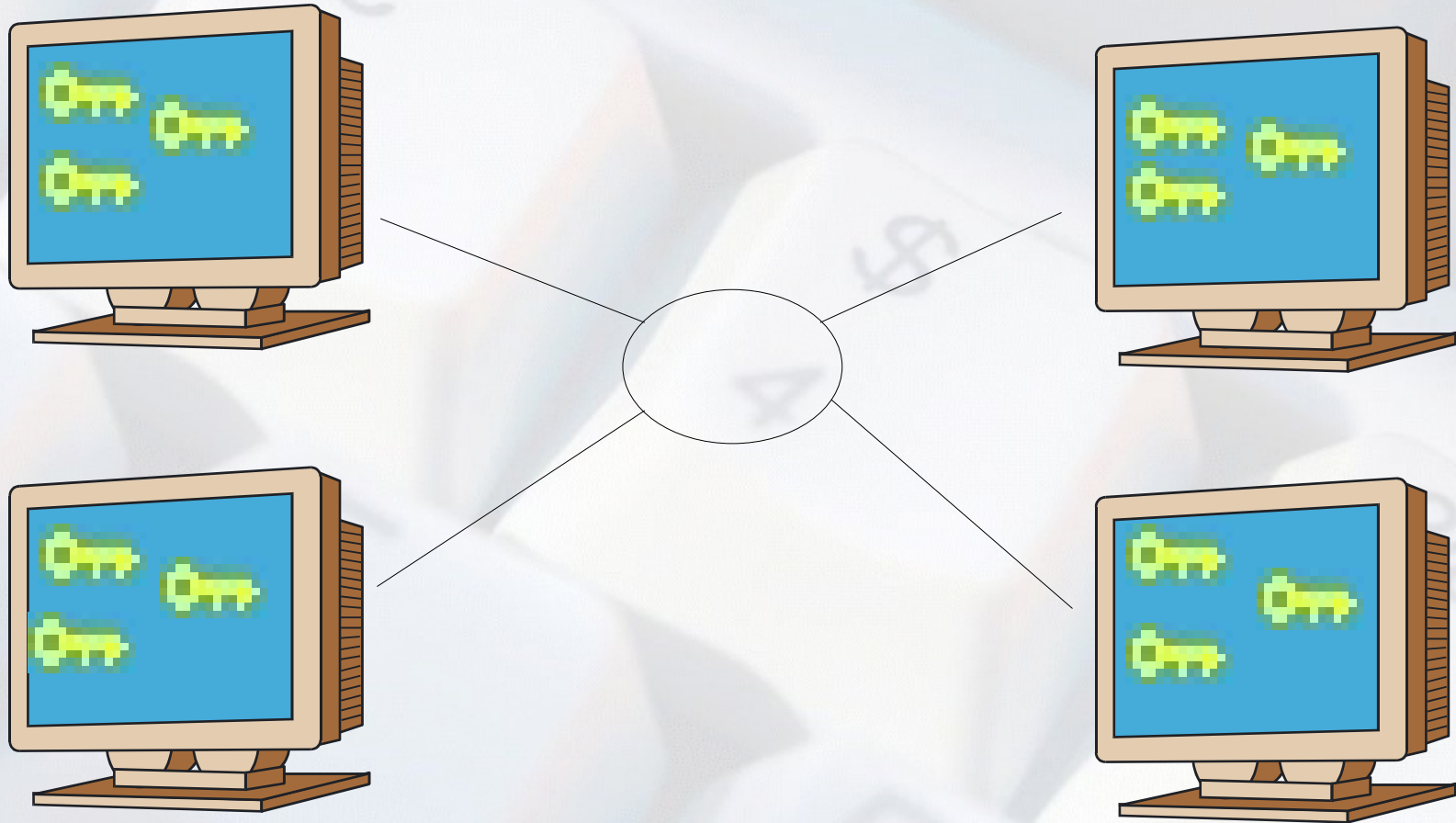
Security: passwd, group

LAN: TCP/IP, DNS, DHCP

File Systems: XFS

# Security Models

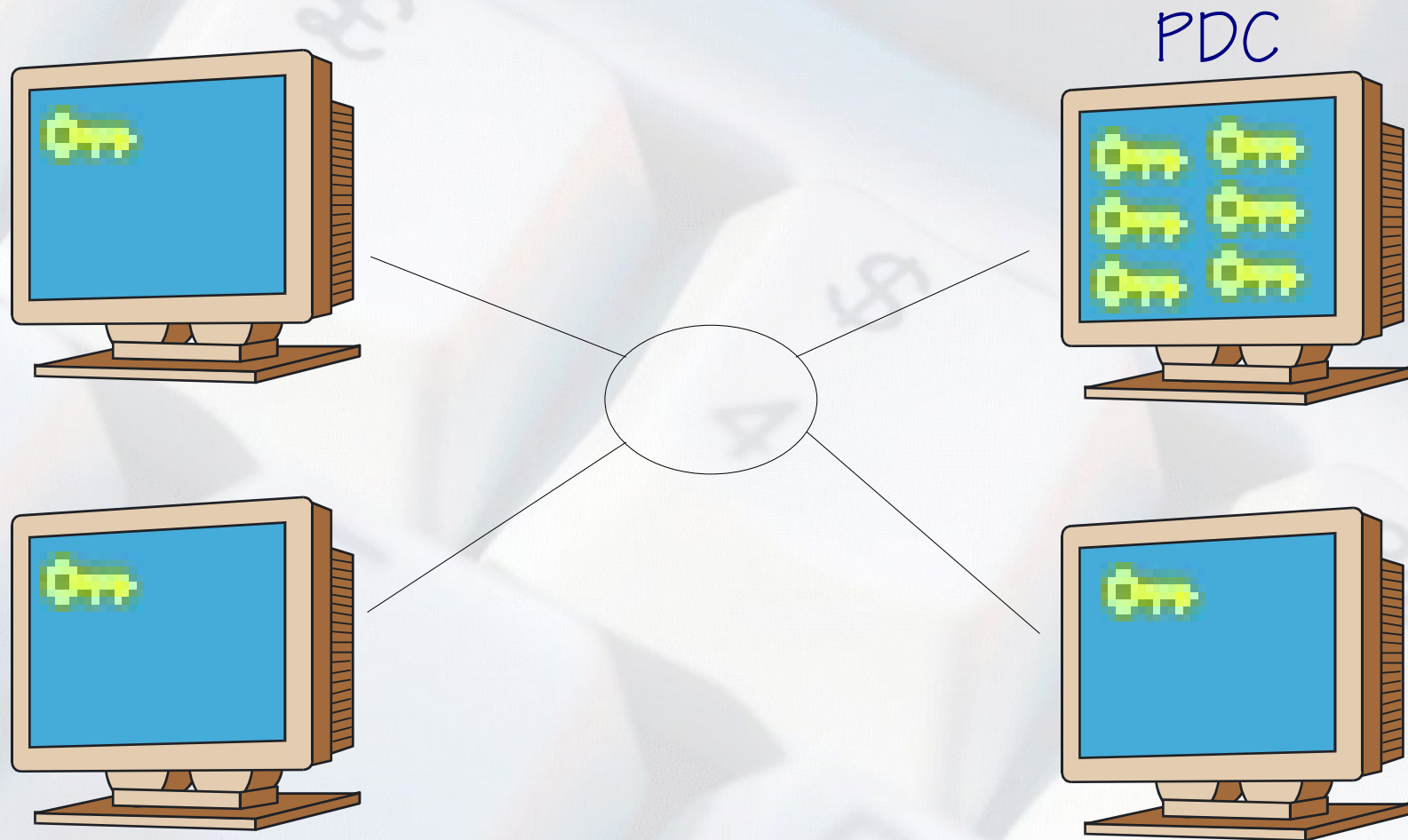
Peer-to-Peer





# Security Models

Domain - SMB Style



# Samba PDC Setup 101

```
# /etc/samba/smb.conf
[global]
    workgroup = LDS-DEMO
    netbios name = LDSSLNX03
    admin users = pianoman
    log file = /var/log/samba/log.%m
    log level = 1
    max log size = 1000

##### NT Domain Related #####
    security = user
    encrypt passwords = true
    passdb backend = smbpasswd
    domain logons = true
    time server = true
    add machine script = /usr/sbin/useradd -d /dev/null -g 100...
                        -s /bin/false %u
```

Restart Samba - exact syntax depends on OS

```
# sudo /etc/init.d/samba restart
```

Then add your first user to smbpasswd

```
# sudo smbpasswd -a pianoman
```

# By now you can...

Then run to a Windows box and join the Domain!

- ✓ Use the pianoman account to join Windows workstations to the domain. (Log in to local Administrator account, network identification dialog, use pianoman account to authenticate with the domain, reboot...)
- ✓ From Windows logon to the workstation using the domain account pianoman
- ✓ Gee, that was fun, wasn't it! ☺

# User Accounts / Permissions

Considering Samba using smbpasswd back end...

#1

Linux Users  
/etc/passwd  
/etc/group

#2

Samba Users  
/etc/samba/smbpasswd

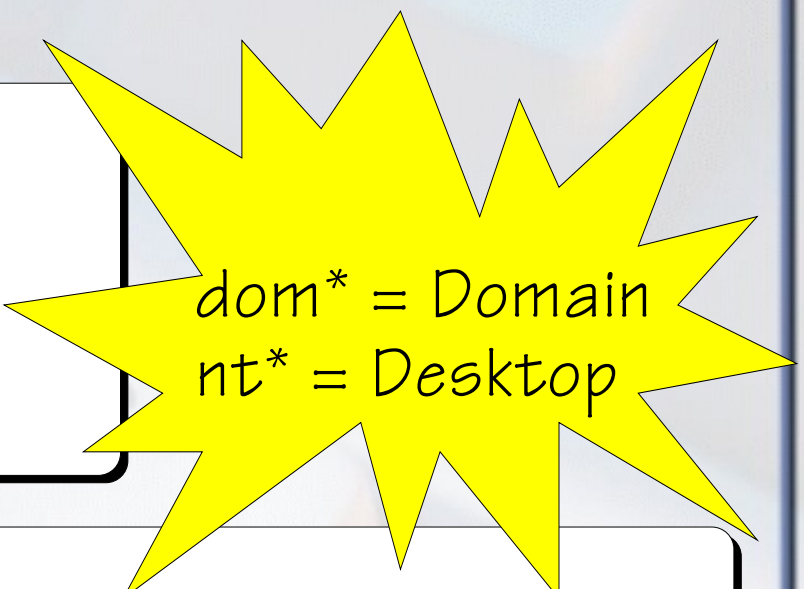
#3

Windows Desktop Permissions  
aka NET LOCALGROUP



# Group Topics

```
/etc/group
domadmin:x:2000:ldsinst,pianoman
domusers:x:2001:mdlueck
domguest:x:2002:
ntadmins:x:2010:pianoman
ntpwrusr:x:2011:mdlueck
ntusers:x:2012:ldsinst
ntguests:x:2013:
```



dom\* = Domain  
nt\* = Desktop

```
#!/bin/bash
# initGrps.sh
```

```
# Map Windows Domain Groups to UNIX groups
```

```
net groupmap add ntgroup="Domain Admins" unixgroup=domadmin rid=512 type=d
net groupmap add ntgroup="Domain Users"  unixgroup=domusers  rid=513 type=d
net groupmap add ntgroup="Domain Guests" unixgroup=domguest rid=514 type=d
```

```
# Create some Domain Groups to administer local security
```

```
net groupmap add ntgroup=ntadmins unixgroup=ntadmins type=d
net groupmap add ntgroup=ntpwrusr unixgroup=ntpwrusr type=d
net groupmap add ntgroup=ntusers  unixgroup=ntusers  type=d
net groupmap add ntgroup=ntguests unixgroup=ntguests type=d
```



# Group Topics

```
# /etc/samba/smb.conf
[global]
    domain admins = @domadmin
```

Add another user to Samba

```
# sudo smbpasswd -a ldsinst
```

Restart Samba - exact syntax depends on OS

```
# sudo /etc/init.d/samba restart
```

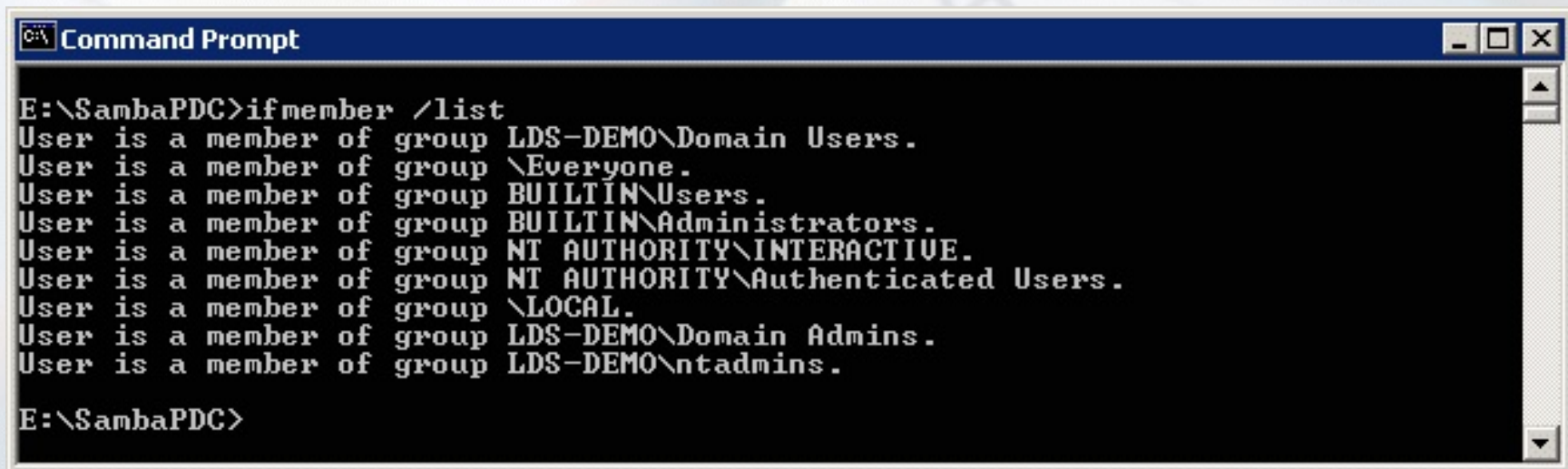
```
REM JoinDomain.cmd
NETDOM.EXE JOIN %ComputerName% /Domain:LDS-DEMO /UserD:ldsinst
/PasswordD:password
```

```
REM Remove domain to local group mapping done by NETDOM
NET LOCALGROUP "Users" "LDS-DEMO\Domain Users" /DEL
NET LOCALGROUP "Administrators" "LDS-DEMO\Domain Admins" /DEL
```

```
REM Add domain to local group mapping
NET LOCALGROUP "Administrators" "LDS-DEMO\ntadmins" /ADD
NET LOCALGROUP "Power Users" "LDS-DEMO\ntpwrusr" /ADD
NET LOCALGROUP "Users" "LDS-DEMO\ntusers" /ADD
NET LOCALGROUP "Guests" "LDS-DEMO\ntguests" /ADD
```

# Group Topics

So, after all that... log back into Windows, open a Command Prompt, and run the ifmember.exe command to have a look at the results of your hard work.



```
Command Prompt
E:\SambaPDC>ifmember /list
User is a member of group LDS-DEMO\Domain Users.
User is a member of group \Everyone.
User is a member of group BUILTIN\Users.
User is a member of group BUILTIN\Administrators.
User is a member of group NT AUTHORITY\INTERACTIVE.
User is a member of group NT AUTHORITY\Authenticated Users.
User is a member of group \LOCAL.
User is a member of group LDS-DEMO\Domain Admins.
User is a member of group LDS-DEMO\ntadmins.
E:\SambaPDC>
```

# By now you can...

- ✓ Add additional users to Linux / Samba and...
- ✓ Define what permissions they have in Linux...
- ✓ Define what permissions they have in the Domain...
- ✓ Define what permissions they have on their Windows workstation.
- ✓ Gee, this is way cool more fun! ☺

# Samba PDC Setup 102

Allow a special normal user account to join computers to the domain. Much safer than allowing a root-equiv account with static password to exist on the domain!

```
# /etc/samba/smb.conf
[global]
    #This is not the BEST way to do this...
    #admin users = @domadmin

##### NT Domain Related #####
    enable privileges = true
```

```
#!/bin/bash
# initLDSInst.sh
net rpc rights grant LDS-DEMO\\ldsinst SeMachineAccountPrivilege

pianoman# ./initLDSInst.sh
Password:
Successfully granted rights.
```



# User Profiles

Do not let them roam wild!

You are also getting an error message about being unable to create / store the user profile on the network...

```
# /etc/samba/smb.conf
[global]
##### NT Domain Related #####
    logon script = LOGON.BAT
    logon drive = I:
    logon path =

##### File Shares #####
[netlogon]
    comment = Network Logon Service
    browseable = no
    path = /shares/netlogon/%a
    locking = no
    guest ok = no
    read only = yes
    write list = @domadmin
```

✓ Tip: %a makes the directory client OS specific!

# User Profiles

## Windows Side

This registry update tells Windows not to even think about doing Roaming Profiles... Way Cool!

```
REGEDIT4
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System]  
"LocalProfile"=dword:00000001
```

Note: Always leave an extra blank line or two in your .REG files or RegEdit will not process the entire file.

# Logon Script

Map some Network Drives

Following is a very simple logon script...

```
REM LOGON.BAT
%SystemRoot%\System32\NET.EXE USE /PERSIST:NO
%SystemRoot%\System32\NET.EXE USE P: %LOGONSERVER%\PDOXDATA
%SystemRoot%\System32\NET.EXE USE Y: %LOGONSERVER%\APPS
%SystemRoot%\System32\NET.EXE USE Z: %LOGONSERVER%\DATA
```

- ✓ NET USE /PERSIST:NO means to make drive mappings which are not automatically remembered, a good thing...
- ✓ Full Path to NET.EXE or else it asks Samba for the file, you look in the samba log and see how much traffic for this little script... full path everything!
- ✓ locking = no for netlogon as it is read-only anyway



# User Home Directory

*“My Place for Stuff!”*

```
# /etc/samba/smb.conf
[homes]
    comment = %U's Home Directory
    volume = home
    path = %H/WinHome
    browseable = no
    read only = no
    create mask = 0600
    directory mask = 0700
```

- ✓ Tip: %H looks up the home directory from the /etc/passwd file. As suggested here, the user is locked into a subdirectory of that Linux home directory when using Windows... keeps the Linux settings files safe from Windows.



# Simple Group File Shares

*“Our Place for Stuff!”*

```
# /etc/samba/smb.conf
[pdoxdata]
    comment = Paradox Databases
    path = /shares/pdoxdata
    guest ok = no
    read only = no
    create mask = 0666
    directory mask = 0777

[data]
    comment = Shared Application Data Files
    path = /shares/data
    guest ok = no
    read only = no
    create mask = 0666
    directory mask = 0777
```

# File Locking Issues - Oplocks

```
# /etc/samba/smb.conf
[global]
##### File Sharing #####
    oplocks = no
    level2 oplocks = no
```

REGEDIT4

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MRxSmb\Parameters]
"OplocksDisabled"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters]
"CachedOpenLimit"=dword:00000000
"EnableOplocks"=dword:00000000
```

Many apps (especially desktop databases) have issues with files getting corrupted if Oplocks are enabled which is the default. Above is how to disable on Win2K or newer, NT4 and 9x are different.

# By now you can...

- ✓ Log in without error messages and without losing your Windows preferences between logins
- ✓ Receive drive mappings for personal (home) and shared data directories
- ✓ OK, time for a snack! Pizza anyone!? ☺



# A Touch of Class...

## Browsing around all of the Names

```
# /etc/samba/smb.conf
[global]
##### NT Domain Related - Master Browser #####
    browse list = true
    domain master = true
    local master = true
    os level = 33
    preferred master = true
    wins support = yes
    name resolve order = wins host bcast
```

These lines enable first the Master Browser and the last two lines handle name resolution and specifically running a WINS server within the nmbd task. Add the IP of this server to your DHCP configuration as a WINS server. Also, disable browser tasks on your workstation... if you never want them to be the Master Browser why run them?



# Time to Print!

First, set up CUPS for RAW per the documentation...

```
# /etc/samba/smb.conf
[global]
##### Printing #####
    load printers = yes
    printcap name = CUPS
    printing = CUPS
    use client driver = no

##### Print Shares #####
[printers]
    comment = SMB Print Spool
    path = /var/spool/samba
    browseable = no
    public = yes
    guest ok = yes
    read only = yes
    printable = yes
    create mode = 0600
[print$]
    comment = Printer Driver Download Area
    path = /shares/print
    browsable = yes
    guest ok = yes
    read only = yes
    write list = @domadmin
```

# Time to Print!

## Non smb.conf setup steps...

```
#!/bin/bash
# initPrint.sh
# No longer initPrint.sh seems to be needed, so one less step

mkdir /var/spool/samba
chmod 0777 /var/spool/samba
chmod o+t /var/spool/samba
```

```
#!/bin/bash
# initPrintOperator.sh

net rpc rights grant "LDS-DEMO\\Domain Admins" SePrintOperatorPrivilege
```

As usual, restart samba, and then log in to a Windows workstation with the domain pianoman account. Upload print drivers to the network printers per John Terpstra's HOWTO documentation, set defaults if you like.

# Printing - The Client Side

OK, printers should be ready for end users now...

```
RunDLL32 PrintUI.DLL,PrintUIEntry /dn /n \\LDSLNX03\HPLJ4000-PCL6  
RunDLL32 PrintUI.DLL,PrintUIEntry /in /n \\LDSLNX03\HPLJ4000-PCL6  
RunDLL32 PrintUI.DLL,PrintUIEntry /y /n \\LDSLNX03\HPLJ4000-PCL6
```

PrintUI.DLL is a handy way to script Add Printer Wizard (APW) related activities. The above creates SPOOLSS style printer connections for the user currently logged in. Other domain users will not see these printers when they log in. Thus, this could be part of the LOGON.BAT. Admin permissions are not required for the drivers to install on the workstation.



# By now you can...

- ✓ Have CUPS printers show up in Samba
- ✓ Use Samba to spool the RAW printer data as fast as the printer is able to print it
- ✓ Use MS Point-n-Print to download drivers for network printer queues
- ✓ OK, that be your basic Samba PDC!

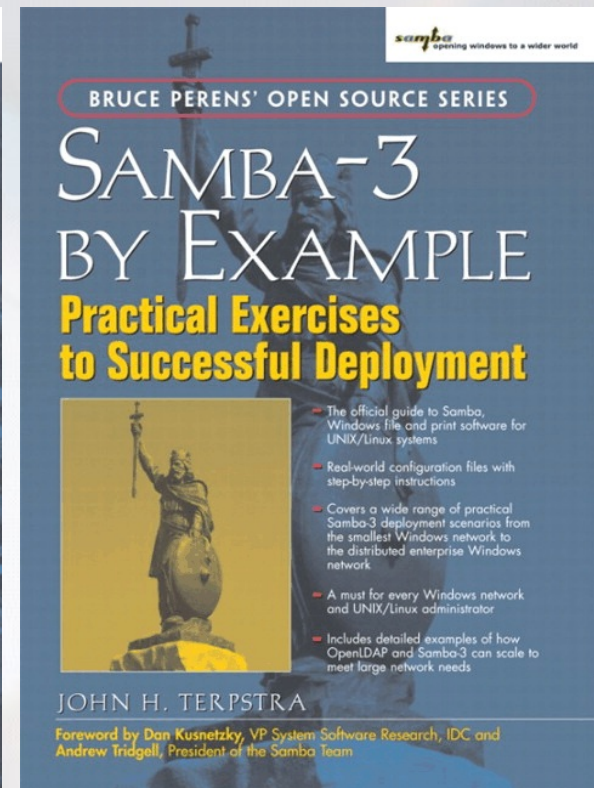
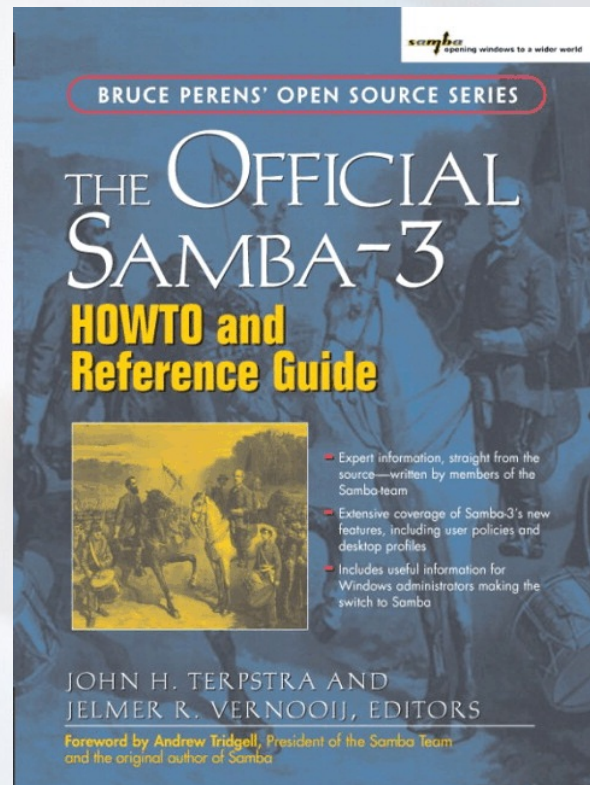
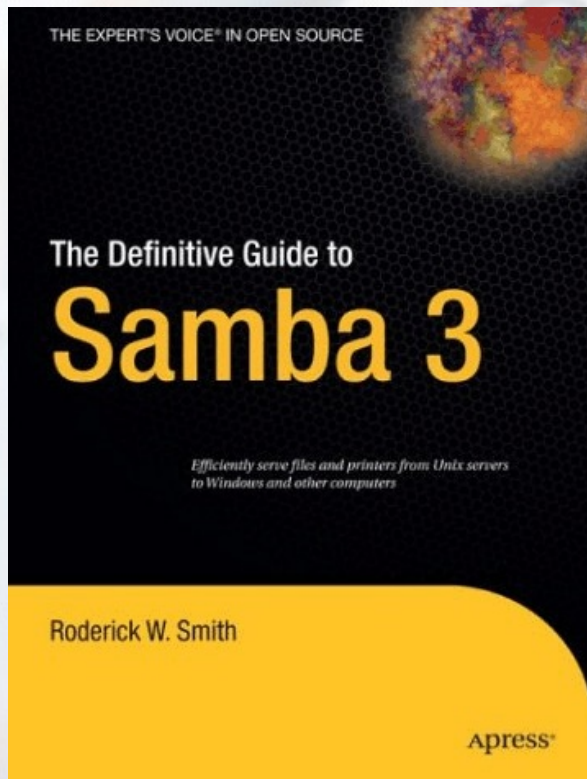


# Things you do not do...

Oh yes there are those!

- ✓ Do not set root as an invalid user in smb.conf... you break network printing, specifically your ability to be a print admin. It's all fine and dandy to say you will never log in as root, we all know that is a bad thing, but disabling root is bad too! Let's just be glad the Samba team can make a real OS do SMB, and live with what they deliver us!
- ✓ Do not set “duplicate” netgroup commands, only one of your group mappings will take affect! Mr. Terpstra says this will be much better in Samba 3.2... for now we exchanged some emails about one of his examples and I shared my solution (presented here) on how to actually make it do something useful (at least to me).

# Samba-3 Book Review





# The Definitive Guide to Samba 3

By Roderick W. Smith

- ✓ Good overview of the SMB/CIFS protocol, and the how's and why's behind what it is... how we got to where we are today. Good background, but not a doctoral thesis on the protocol.
- ✓ I read through chapters 1-4, 7, 10 and had the PDC up with a single one line change to smb.conf
- ✓ Chapter 8 quickly added a Master Browser to the configuration.
- ✓ Chapter 9 quickly added a NetBIOS Name Server
- ✓ Good examples of security settings, had an "add machine" script which worked flawlessly (Until Debian Etch that is!)
- ✓ The new NET command seems added as it is in an Appendix yet it is pretty important to Samba 3

# The Official Samba-3 HOWTO

By John H. Terpstra and Jelmer R. Vernooij

- ✓ Critical steps here for uploading printer drivers and setting default printer settings - found nowhere else
- ✓ Some advanced things covered which I have not needed such as AD integration
- ✓ In general LOTS of data which you just might need - file shares, printing both classic and CUPS, Winbind, upgrading Samba 2.x to 3.x, DHCP / DNS, on and on...



# Samba-3 By Example

By John H. Terpstra

- ✓ This is very much a technical cook-book. Starts out sniffing the SMB packets right on the wire!
- ✓ Various size networks are presented with the solutions to making Samba great in each of those environments
- ✓ Various technologies are explored and how Samba interacts with them such as AD, DNS, NT4 to Samba PDC migrations, etc...

# So which one, Michael?

All Three!

- ✓ Rod's book did arrive first, so that is what I started with. As important as 'net' has become, it by no means belongs in an Appendix... aka "after thought?"
- ✓ The Official HOWTO has over the years proven to be the book of these three that ends up containing the answer I was looking for.
- ✓ But then I still like to push technology as hard as possible, so various examples in the "By Example" will come in handy as well. Thus, buy all three! Hey, it is one way to "send pizza" to say thanks to these kind authors!



# Steps to Setting up Samba

Add Ubuntu Server 7.04 packages: acl, attr, xfsdump (among others...)

Create initial Linux accounts: pianoman, ldsinst

Make staging directory and place scripts / config files there: /srv/samba/

Make directory for Samba packages: /srv/samba/3024/

Download Samba packages:

/srv/samba/3024/ # sudo wget http://security.ubuntu.com/ubuntu/pool/main/s/samba/samba\_3.0.24-2ubuntu1.2\_i386.deb

# sudo wget http://security.ubuntu.com/ubuntu/pool/main/s/samba/samba-common\_3.0.24-2ubuntu1.2\_i386.deb

Install Samba packages: /srv/samba/3024/ # sudo dpkg -i samba\_3.0.24-6etch2\_i386.deb samba-common\_3.0.24-6etch2\_i386.deb

Stop Samba: # sudo /etc/init.d/samba stop

Backup the smb.conf as smb.conf.ubuntu: /etc/samba/ # sudo cp smb.conf smb.conf.ubuntu

Copy in the prepared smb.conf customized for this server /etc/samba/ # sudo cp /srv/samba/smb.conf smb.conf

Update initShares.sh for the shares for this server and run it.: # sudo /srv/samba/initShares.sh

Populate the NetLogon share with the logon script(s)

Append provided group entries to /etc/group

Run initPrint.sh: # sudo /srv/samba/initPrint.sh

Start Samba: # sudo /etc/init.d/samba start

Add users to Samba # sudo smbpasswd -a [userid]

Run initGrps.sh script: # sudo /srv/samba/initGrps.sh

Update initLDSInst.sh for the domain name for this server and run it AS A MEMBER OF DOMADMIN, NOT ROOT!!! pianoman# /srv/samba/initLDSInst.sh and you will be prompted for the password of the account you use.

Update initPrintOperator.sh for the domain name for this server and run it. pianoman# /srv/samba/initPrintOperator.sh

# LDS's smb.conf

```
[global]
  workgroup = LDS-DEMO
  netbios name = LDSLNX03
  server string = %h server
  log file = /var/log/samba/log.%m
  log level = 1
  max log size = 1000
  syslog = 0
  panic action = /usr/share/samba/panic-action %d
  passwd program = /usr/bin/passwd %u
  passwd chat = *Enter\snew\sUNIX\spassword:* %n\n *Retype\snew\sUNIX\spassword:* %n\n .

##### NT Domain Related #####
  security = user
  encrypt passwords = true
  passdb backend = smbpasswd
  domain logons = true
  time server = true
  enable privileges = true
  add machine script = /usr/sbin/useradd -d /dev/null -g 100 -s /bin/false %u
  logon script = LOGON.BAT
  logon drive = I:
  logon path =

##### NT Domain Related - Master Browser #####
  browse list = true
  domain master = true
  local master = true
  os level = 33
  preferred master = true
  wins support = yes
  name resolve order = wins host bcst

##### Printing #####
  load printers = yes
  printcap name = CUPS
  printcap cache time = 180
  printing = CUPS
  use client driver = no

##### File Sharing #####
  oplocks = no
  level2 oplocks = no
  socket options = TCP_NODELAY
```



# LDS's smb.conf continued...

```
##### File Shares #####  
[netlogon]  
    comment = Network Logon Service  
    browseable = no  
    path = /srv/shares/netlogon/%a  
    locking = no  
    guest ok = no  
    read only = yes  
    create mask = 0666  
    directory mask = 0777  
    write list = @domadmin  
  
[homes]  
    comment = %U's Home Directory  
    volume = home  
    path = %H/WinHome  
    browseable = no  
    read only = no  
    directory mask = 0700  
  
[pdoxdata]  
    comment = Paradox Databases  
    path = /srv/shares/pdoxdata  
    guest ok = no  
    read only = no  
    create mask = 0666  
    directory mask = 0777  
  
[stage]  
    comment = MichaelDist Opus 3 Stager  
    browseable = no  
    path = /srv/shares/stage  
    guest ok = no  
    read only = yes  
    create mask = 0666  
    directory mask = 0777  
    write list = @mdldistadmin
```

# LDS's smb.conf the end...

```
[mldlist]
comment = MichaelDist Opus 3.5 Stager
browseable = no
path = /srv/shares/mldlist
guest ok = no
read only = yes
create mask = 0666
directory mask = 0777
writelist = @mldlistadmin

[apps]
comment = Shared Application Program Files
path = /srv/shares/apps
guest ok = no
read only = no
create mask = 0666
directory mask = 0777

[data]
comment = Shared Application Data Files
path = /srv/shares/data
guest ok = no
read only = no
create mask = 0666
directory mask = 0777

##### Print Shares #####
[printers]
comment = SMB Print Spool
path = /var/spool/samba
browseable = no
public = yes
guest ok = yes
read only = yes
printable = yes
create mode = 0600

[print$]
comment = Printer Driver Download Area
path = /shares/print
browsable = yes
guest ok = yes
read only = yes
write list = @domadmin
```

# LDS's initShares.sh

```
#!/bin/bash
#
# initShares.sh
#

mkdir /srv/shares
mkdir /srv/shares/apps
mkdir /srv/shares/data
mkdir /srv/shares/mdldist
mkdir /srv/shares/netlogon
mkdir /srv/shares/pdoxdata
mkdir /srv/shares/print
mkdir /srv/shares/stage

chmod 0777 /srv/shares/apps
chmod 0777 /srv/shares/data
chmod 0777 /srv/shares/mdldist
chmod 0777 /srv/shares/netlogon
chmod 0777 /srv/shares/pdoxdata
chmod 0777 /srv/shares/print
chmod 0777 /srv/shares/stage
```

# LDS's /etc/group

```
domadmin:x:2000:pianoman  
domusers:x:2001:ldsinst,mdlueck  
domguest:x:2002:  
ntadmins:x:2010:pianoman  
ntpwrusr:x:2011:mdlueck  
ntusers:x:2012:ldsinst  
ntguests:x:2013:
```



# LDS's initPrint.sh

```
#!/bin/bash
#
# initPrint.sh
# No longer initPrint.sh seems to be needed, so one less step

mkdir /var/spool/samba
chmod 0777 /var/spool/samba
chmod o+t /var/spool/samba
```

# LDS's initGrps.sh

```
#!/bin/bash
#
# initGrps.sh
#

# Map Windows Domain Groups to UNIX groups
net groupmap add ntgroup="Domain Admins" unixgroup=domadmin rid=512 type=d
net groupmap add ntgroup="Domain Users"  unixgroup=domusers rid=513 type=d
net groupmap add ntgroup="Domain Guests" unixgroup=domquest rid=514 type=d

# Create some Domain Groups to administer local security
net groupmap add ntgroup=ntadmins unixgroup=ntadmins type=d
net groupmap add ntgroup=ntpwrusr unixgroup=ntpwrusr type=d
net groupmap add ntgroup=ntusers  unixgroup=ntusers  type=d
net groupmap add ntgroup=ntquests unixgroup=ntquests type=d
```

# LDS's initLDSInst.sh

```
#!/bin/bash
#
# initLDSInst.sh
#
net rpc rights grant LDS-DEMO\\ldsinst SeMachineAccountPrivilege
```

# LDS's initPrintOperator.sh

```
#!/bin/bash
#
# initPrintOperator.sh
#
net rpc rights grant "LDS-DEMO\\Domain Admins" SePrintOperatorPrivilege
```