Samba-3 by Example

Practical Exercises in Successful Samba Deployment

5 Making Happy Users **85**

5.1 Regarding LDAP Directories and Windows Computer Accounts 86

5.7.2 Configuration of MS Outlook to Relocate PST File . . . 128
5.7.3 Configure Delete Cached Profiles on Logout . . . 129
5.7.4 Uploading Printer Drivers to Samba Servers . . . 130
5.7.5 Software Installation . . . 130
5.7.6 Roll-out Image Creation . . . 131
5.8 Key Points Learned . . . 131
5.9 Questions and Answers . . . 132

6 A Distributed 2000-User Network 134
6.1 Introduction . . . 134
6.1.1 Assignment Tasks . . . 134
6.2 Dissection and Discussion . . . 135
6.2.1 Technical Issues . . . 135
6.2.1.1 User Needs . . . 136
6.2.1.2 The Nature of Windows Networking Protocols.6 A Distributed 2000-User Network

7.3.5 UNIX/Linux Client Domain Member 180 UN8 8(NT4Domain)-250(Member)80 0 1457o. 1817.3.5 UN8 8(ADS

List of Figures

List of Tables

1 Samba Changes — 3.0.2 to 3.0.20 xix

1.1 Accounting Office Network Information 13

3.1 Abmas.US ISP Information 32

3.2 DNS (named) Resource Files 32

About the Cover Artwork

Part I

Example Network Configurations

9. Configure the printers with the IP address as shown in . Follow the instructions in the manufacturer's manual to permit printing to port 9100 so that the CUPS spooler can print using raw mode protocols.

10. Configure the CUPS Print Queues:

```
root#  lpadmin -p PRINTQ -v socket://192.168.1.20:9100 -E
root#  lpadmin -p hplj5 -v socket://192.168.1.30:9100 -E
```

    This creates the necessary print queues with no assigned print filter.

11. Edit the file `/etc/cups/mime.convs` to uncomment the line:

```
application/octet-stream     application/vnd.cups-raw      0     -
```

12. Edit the file `/etc/cups/mime.types` to uncomment the line:

```
application/octet-stream
```

13. Use the standard system tool to start Samba and CUPS to configure them to restart automatically at every system reboot. For example,

```
root#  chkconfig smb on
root#  chkconfig cups on
root#  /etc/rc.d/init.d/smb restart
root#  /etc/rc.d/init.d/cups restart
```

Example 1.2

Example 1.3 Charity Administration Office smb.conf Old-style File

Example 1.4

1.2.3 Accounting Office

Abmas Accounting is a 40-year-old family-run business. There are nine permanent computer users. The network clients were upgraded two years ago. All computers run Windows 2000 Professional. This year the server will be upgraded from an old Windows NT4 server (actually running Windows NT4 Workstation, which worked fine for fewer than 10 users) that has run in workgroup (standalone) mode, to a new Linux server running Samba.

The office does not want a Domain Server. Mr. Alan Meany wants to keep the Windows 2000 Professional clients running as workgroup machines so that any staff member can take a

12. Create the directory mount point for the disk subsystem that is mounted to provide data storage for company files. In this case the mount point is indicated in the `smb.conf` file is `/dataG`

2.4 Questions and Answers

Your new Domain Controller is ready to serve you. What does it mean? Here are some questions and answers that may help.

1.

Example 3.4 130 User Network with tdbsam [globals] Section

```
# Global parameters
[global]
```

Example 3.8 DHCP Server Configuration File /etc/dhcpd.conf

```
# Abmas Accounting Inc.
default-lease-time 86400;
max-lease-time 172800;
default-lease-time 86400;
option ntp-servers 192.168.1.1;
option domain-name "abmas.biz";
option domain-name-servers 192.168.1.1, 192.168.2.1;
```

Example 4.2 Server: MASSIVE (PDC), File: /etc/samba/dc-common.conf

Example 4.8 Server: BLDG1, File: dhcpd.conf

Example 4.12 Server: MASSIVE, File: named.conf, Part: C

Example 4.17 Initialize Groups Script, File: /etc/samba/initGrps.sh

```
#!/bin/bash

# Create UNIX groups
groupadd acctsdep
groupadd finsrvcs
groupadd piops

# Map Windows Domain Groups to UNIX groups
```

2. Join the Windows domain MEGANET. Use the domain administrator username `root` and the SMB password you assigned to this account. A detailed step-by-step procedure for joining a Windows 200x/XP Professional client to a Windows domain is g 0 G3 0 Td [(root)]TJ/F52 9.9626 Tf 26.262 0 Td [(and)-236(theignede2 0 Td [f 41. 0 l Srg 0 l SRGmain)]TJ/F68 Td

Chapter 5

Making Happy Users

It is said that ‘a day that is without troubles is not fulfilling. Rather, give me a day of troubles well handled so that I can be content with my achievements.’

- Defective networking hardware. Over the past few years, we have seen on the Samba mailing list a significant increase in the number of problems that were traced to a defective network interface controller, a defective HUB or Ethernet switch,

You configure a new MS Windows XP Professional workstation disk image that you roll out to all desktop users. The instructions you have created are followed on a staging machine from which all changes can be carefully tested before inflicting them on your network users.

This is the last network example in which specific mention of printing is made. The example again makes use of the CUPS printing system.

5.3 Dissection and Discussion

The implementation of Samba BDCs necessitates the installation and configuration of LDAP. For this site, you use OpenLDAP, the open source software LDAP server platform. Commercial LDAP servers in current use with Samba-3 include:

- Novell eDirectory is being successfully used by some sites. Information on how to use eDirectory can be obtained from the Samba mailing lists or from Novell.
- IBM Tivoli Directory Server

5.3.1.2 Roaming Profile Background

As XP roaming profiles grow, so does the amount of time it takes to log in and out.

An XP roaming profile consists of the HKEY_CURRENT_USER hive file

```
auth      required   pam_nologin.so
#auth     required   pam_homecheck.so
auth      required   pam_env.so
auth      required   pam_mail.so
account   required   pam_unix2.so   use_ldap
password  required   pam_pwcheck.s  nullok
password  required   pam_unix2.so   nullok use_first_pass \
                                    06cmefRG[-1800(pam_pwcheck)]TJ0g0G[(.)]TJ000rg000RG[(s)]TJ0g
```

The expected output from this is:

Example 5.10 LDAP Based smb.conf File, Shares Section Part A

Samba uses a well-known public algorithm for assigning RIDs from UIDs and GIDs. This algorithm ought to ensure that there

Chapter 6

A Distributed 2000-User Network

There is something indeed mystical about things that are big. Large networks exhibit a certain magnetism and exude a sense of importance that obscures reality. You and I know that it is no more difficult to secure a large network than it is a small one. We all know that over and above a particular number of network clients, the rules no longer change; the only real dynamic is the size of the domain (much like a kingdom) over which the network ruler (oops, administrator) has control. The real dynamic then transforms from the technical to the political. Then again, that point is often reached well before the kingdom (or queendom) grows large.

following information pertains exclusively to the interaction between a Windows XP Professional workstation and a Samba-3.0.20 server. In the discussion that follows, use is made of DHCP and WINS.

As soon as the Windows workstation starts up, it obtains an IP address. This is immediately followed by registration of its name both by broadcast and Unicast registration that is directed at the WINS server.

Given that the client is already a domain member, it then sends a directed (Unicast) request to the WINS server seeking the list of IP addresses for domain controllesua15(tz8bBIO0(WINS)-251(0(at)-yp1(0(at)0x1Cicas.(0(at)T250(the)-250(WINS)-250(serv)1cast)

In , you implemented a single LDAP server for the entire network. This may work for smaller networks, but almost certainly fails

Example 6.3 Primary Domain Controller smb.conf File Part A

```
#
```

Example 6.6 Backup Domain Controller smb.conf File Part A

```
# \# Global
```

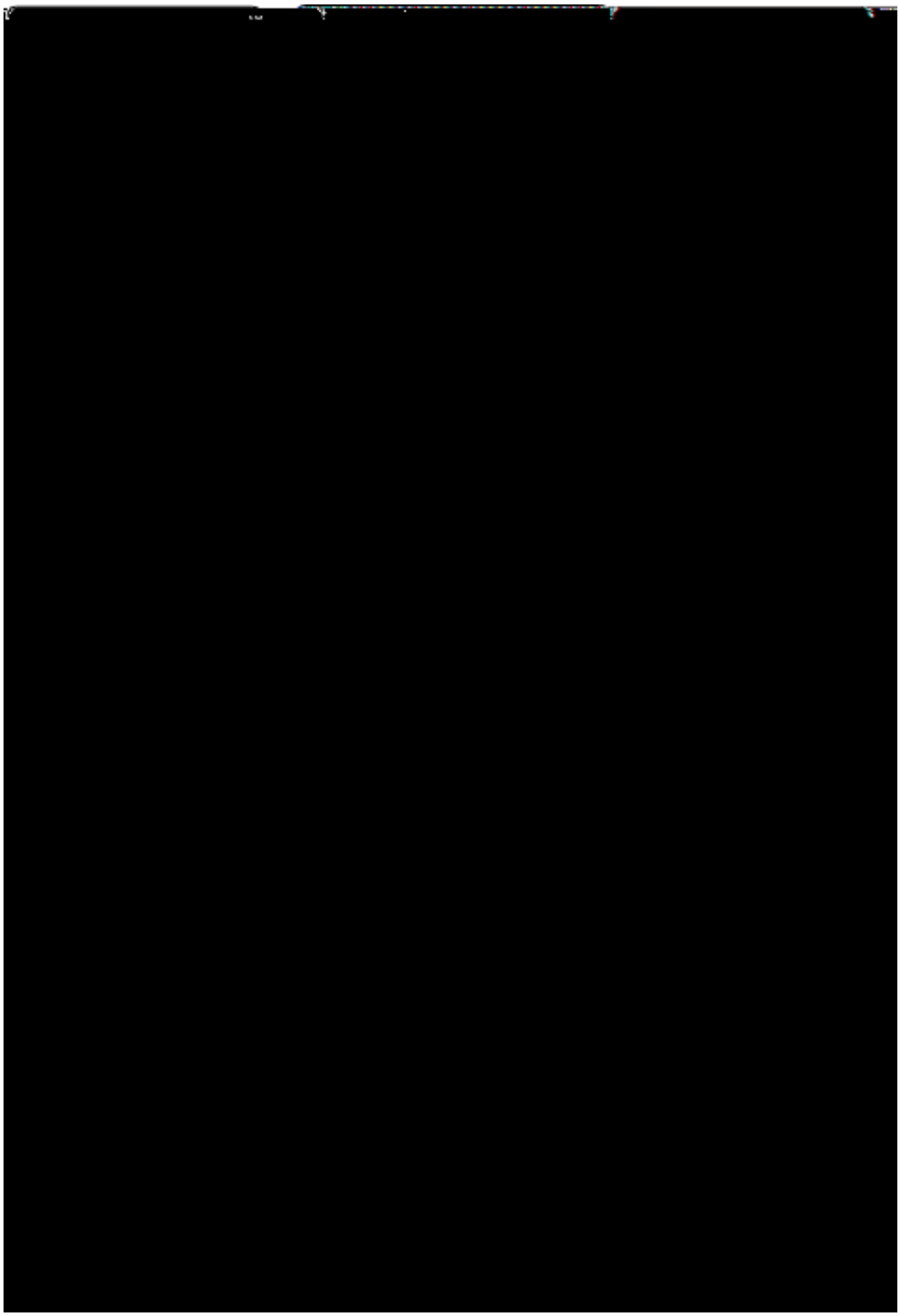


Figure 6.7: Network Topology — 2000 User Complex Design B

MS Windows clients cache information obtained from WINS lookups in a local NetBIOS name cache. This keeps WINS lookups to a minimum. On a network with 3500 MS Windows clients and a central WINS server, the total bandwidth demand measured at the WINS server, averaged over an 8-hour working day, was less than 30 KB/sec. Analysis of network traffic over a 6-week period showed that the total of all background traffic consumed about 11 percent of available bandwidth over 64 Kb/sec links. Background traffic consisted of domain replication, WINS queries, DNS lookups, and authentication traffic. Each of 11 branch

Chapter 7

Adding Domain Member Servers and Clients

Example 7.1

The user account information has been correctly obtained. This information has been merged with the winbind template information configured in the `smb.conf` file.

```
root# # getent group
...
MEGANET2+Domain Admins:x:10000:MEGANET2+root,MEGANET2+jht
MEGANET2+Domain Users:x:10001:MEGANET2+jht,MEGANET2+maryv,\+
```

Example 7.6 Samba Domain Member Server Using Local Accounts smb.conf File for NT4 Domain

```
# Global parameters
[
```

Samba-3by-3 o0(Example)]TJF524 896263Tf 6215.806 -1.479Td [(SW)]TJF524 7.1731Tf 68.7510 Gd [(SO)-62(R)-62(K)-62(I)-62(

```
        [Write All Properties]
------- ACE (type: 0x07, flags: 0x5a, size: 0x38,
               mask: 0x20, object flags: 0x3)
```

Example 7.8 Example smb.conf File Using idmap_rid

```
./configure --enable-rfc2307bis --enable-schema-mapping
make install
```

The following `/etc/nsswitch.conf` file contents are required:

```
...
passwd: files ldap
shadow: files ldap
group:  files ldap
...
hosts:  files wins
...
```

The `/etc/ldap.conf` file must be configured also. Refer to the PADL documentation and source code for nss_ldap instructions.

The next step involves preparation on the ADS schema. This is briefly discussed in the remaining part of this chapter.

7.3.4.3.1 IDMAP, Active Directory, and MEaining26 Tf 56.693 703.c-10(y)80(fon)-203.f0(prer)-203.UNIXq1 0 0.5f 86.333 0 Td [(.4.2

Example 7.13 Red Hat 9: PAM System Authentication File: /etc/pam.d/system-auth Module Using Winbind

```
#%PAM-1.0
```

```
   SBINDIR: /usr/sbin
   BINDIR: /usr/bin
   SWATDIR: /usr/share/samba/swat
   CONFIGFILE: /etc/samba/smb.conf
   LOGFILEBASE: /var/log/samba
   LMHOSTSFILE: /etc/samba/lmhosts
```

Before proceeding to NT4 migration using either a tdbsam or ldapsam, it is most strongly recommended to review for DNS and DHCP configuration. The importance of correctly functioning name resolution must be recognized. This applies equally for both hostname and NetBIOS names (machine names, computer names, domain names, workgroup names — ALL names!).

The migration process involves the following steps:

- Prepare the target Samba-3 server. This involves configuring Samba-3 for migration to either a tdbsam or an ldapsam backomai.•

Example 9.3 NT4 Migration LDAP Server Configuration File: /etc/openldap/slapd.conf Part A

```
include         /etc/openldap/schema/core.schema
include         /etc/openldap/schema/cosine.schema
```

Example 9.7 NT4 Migration NSS Control File: /etc/nsswitch.conf (Stage:2)

```
passwd:         files ldap
shadow:         files ldap
group:          files ldap

hosts:          files dns wins
networks:       files dns
```

- An LDAP backend is a suitable vehicle for NT4 migrations.
- A tdbsam backend can be used to perform a migration.
- Multiple NT4 domains can be merged into a single Samba-3 domain.
- The net Samba-3 domain most likely requires some administd [(fiso54 in.)]TJo[(fiso5Ign)-250(brfome)-250go5Ignrvn.

Example 10.4 Samba Configuration File smb.conf Part A

Example 10.11 Idealx smbldap-tools Control File Part A

Example 10.14

Example 10.17 Kixtart Control File File: setup.kix, Part A

```
ertinent registry keys which triggers it to happen again:
```

Example 10.18 Kixtart Control File File: setup.kix, Part B

```
; Now we will write the registry values to redirect the locations of "My
Documents"
; and other folders.
      ADDKEY("HKEY_CURRENT_USER\abmas\profile_copied")
      WRITEVALUE("HKEY_CURRENT_USER\Software\Microsoft\
Windows\CurrentVersion\Explorer\User
Shell Folders", "Personal","\\massive\@userID","REG_SZ")
      WRITEVALUE("HKEY_CURRENT_USER\Software\Microsoft\
Windows\CurrentVersion\Explorer\User
Shell Folders", "My Pictures", "\\massive\@userID\My Pictures", "REG_SZ")
      IF @PRODUCTTYPE="Windows 2000 Professional" or @PRODUCTTYPE="Windows XP
Professional"
      WRITEVALUE("HKEY_CURRENT_USER\Software\Microsoft\
Windows\CurrentVersion\Explorer\User
Shell Folders", "My Videos", "\\massive\@userID\My Videos", "REG_SZ")
      WRITEVALUE("HKEY_CURRENT_USER\Software\Microsoft\
```

CAMedia: Digital camera software for Canon cameras caused all kinds of trouble with the registry. I had to use the Run as service to open the registry of the local user while logged in as the domain user, and give the domain user the appropriate permissions to some registry keys, then export that portion of the registry to a file. Then, as the domain user, I had to import that file into the registry.

Crystal Reports version 7: More registry problems that were solved by recopying the user's profile.

Critics of Samba often ignore fundamental problems that may plague (or may have plagued) the users of Microsoft's

I tried to set `valid users = @Engineers`*, but it does not work. My Samba server is an Active Directory domain member*

Chapter 12

Integrating Additional Services

You've come a long way now. You have pretty much mastered Samba-3 for most uses it can be put to. Up until now, you

In the case of SUSE Linux, these packages are called:

- heimdal-lib
- heimdal-devel
- heimdal
- pam_krb5

If the required packages are not present on your system, you must install them from the vendor's installation media. Follow the administrative guide for your Linux system to ensure that the packages are correctly updated.

Note guie59edal-libine6(id50.408wi67(f.408be(f.408necessar50.0iy50.ie5-250.408t)-250(t41)-25at50.ie5y)2-25u(t41)-a50(t41)-using50

You would be well-advised to recognize that all cache-intensive proxying solutions demand a lot of memory. Make certain that

W

```
collision.parrots.com
```

Example 15.8 LDAP Pre-configuration Script: SMBLDAP-ldif-preconfig.sh Part C

- Display user/group/host and Domain entries.
- Manage entries (Add/Delete/Edit).
- Filter and sort entries.
- Store and use multiple operating profiles.
- Edit organizational units (OUs).
- Upload accounts from a file.
- Is compatible with Samba-2.2.x and Samba-3.

When correctly configured, LAM allows convenient management of UNIX (Posix) and Samba user, group, and windows domain member machine accounts.

The default password is 'lam.' It is highly recommended that you use only an SSL connection to your Web server for all remote operations involving LAM. If you want secure connections, you must configure your Apache Web server to permit connections to LAM using only SSL.

1. Extract the LAM package by untarring it as shown here:

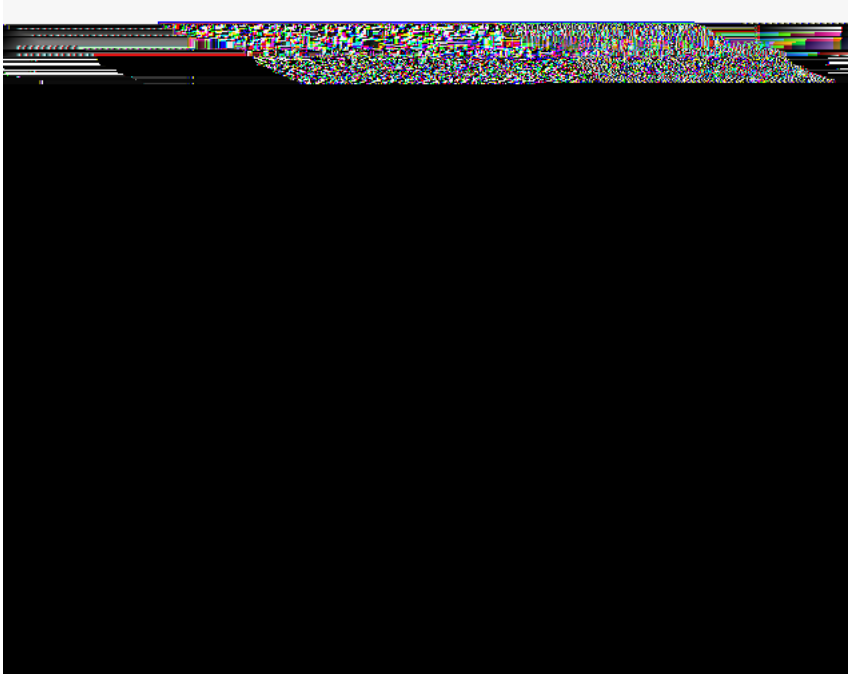


Figure 15.7: The LDAP Account Manager Configuration Screen

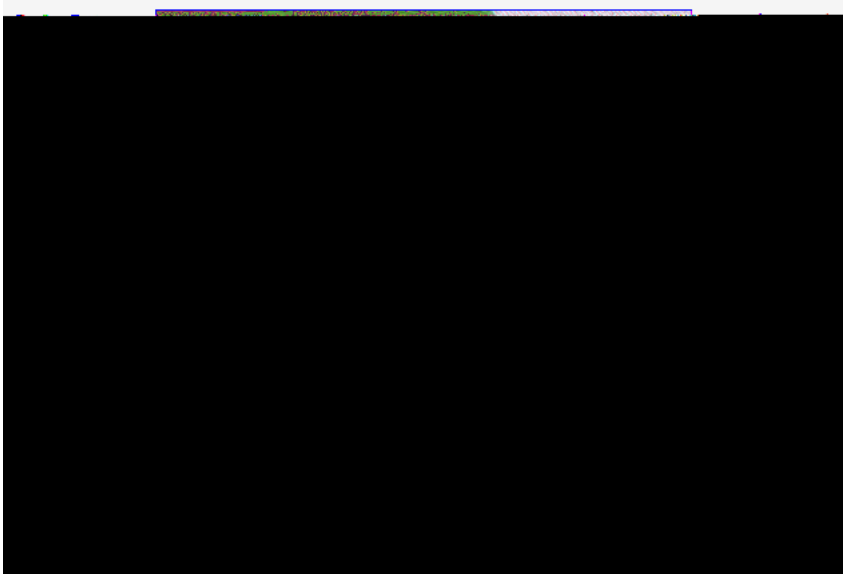


Figure 15.11: The LDAP Account Manager Host Edit Screen

One aspect of LAM that may annoy some users is the way it forces certain conventions on the administrator. For example, LAM

(d) Enable network name resolution

(e)

User IDentifier (UID)

The UNIX system user identifier; on older systems, a 32-bit unsigned integer, and on newer systems, an unsigned 64-bit integer. The UID is used in UNIX-like operating systems for all user-level access controy 98 w 08n9r w 08n-2810 0825626 Tf n

Replacement,

file system security, 257
filter, 251
financial5(,)]Tsesponsibilty, 254
filrewall 23 237-TJ0 g 0 G 0[, 254
filx

interdomain trusts, 138
interfaces, 35
intermittent, 271
internationalization, 190
Internet Explorer, 260
Internet Information Server, 266
interoperability, 88
IP forwarding, 21, 37, 67
IPC$, 309
iptables, 33
IRC, 273
isolated, 247
Italian, 265

J
jobs, 247
joining a domain, 275
274
interoperability, 88
138, 67, 67, 37, 37, 37 37 37 37
interoperabilitraies0 0rg1 0 0 RG [-250(138)]TJ069 0 G 0 -11.955 Td [(interopeMIT)74(0 0 rg 1 0 0 RG [-250(138)]TJ069 0 G 0 -1

bandwidth, 137, 151, 152
broadcast, 303
captures, 302
collisions, 269
load, 269
logon, 85
logon scripts, 199
management, 247
multi-segment, 87
overload, 86
performance, 270
routed, 135

pam_unix2.so, 101
    use_ldap, 102
parameters, 191
passdb backend, 35, 61, 88, 135, 139, 156, 183, 186, 188, 191, 192, 195, 198, 216
passdb.tdb, 199
passwd, 8, 13, 43
password
    backend, 22, 43, 68
password caching, 10
password change, 256
password length, 309, 312
payroll, 219
pdbedit, 110, 114, 119, 214–216
PDC, 62, 63_ldap, 102

raw printing, 23, 49, 66, 117
Rbase, 229
rcldap, 142dap,

tdbsam, 33, 35, 61, 87, 135, 139, 163, 183, 191, 195, 199,
216
testparm, 26, 52, 103, 170, 191, 269
tick,,,,, 1.926 T17[(testVTq1 024RG [-315(1.956 TdbDirecvf 21alidg 0 Gu0 Gs 0 0 rg 1 0 0 RG [-250(269)]TJ84 0 G [(,)]TJ[5 T881 0g 1 0 0 RG [-315(126.345562 l95[,,,,
tick,,,,, 1.926 T17[(testVTq1 024RG [-315(15.2162(R)]TJUNCg 0 Gna]TTq -141.558 Tprocessing50UNIX T881 0g 1 0 0 RG [-315(1

Windows Address Book, 225
Windows ADS Domain, 163
Windows clients, 266
Windows Explorer, 6
Windows explorer, 266
Windows security identifier, *see* SID
Windows Servers, 247
Windows Services for UNIX, *see* SUS
Windows XP, 18
WINS, 10, 19, 24, 27, 550(Address)-250(Book,)]TJ1 0 0 rg 1 0 0 RG [-2 Xc1pr21593l0 0(,)]T388ib87mSr258-.m 1 0 0 RG [-2 Xc1pr2
WINS,