Samba-3 by Example

Practical Exercises in Successful Samba Deployment

John H. Terpstra

ACKNOWLEDGMENTS

Samba-3 by Example

xx

List of Examples

List of Tables

1

the incumbent proprietary means of meeting information technology needs. They are the Apache Web Server and Samba.

Just as the Apache Web Server is the standard in web serving technology, Samba is the de nitive standard for providing interoperability with UNIX systems and other non-Microsoft operating system platforms. Both open source applications have a truly remarkable track record that extends for more than a decade. Both have demonstrated the unique capacity to innovate and maintain a level of development that has not only kept pace with demands, but, in many areas, each project has also proven to be an industry leader.

One of the areas in which the Samba project has demonstrated key leadership is in documentation. The OSSI was delighted

the need for which can be met from other resources that are dedicated to the subject.

Prerequisites

This book is not a tutorial on UNIX or Linux administration. UNIX and Linux training is best obtained from books dedicated to the subject. This book assumes that you have at least the basic skill necessary to use these operating systems, and that you can use a basic system editor to edit and con gure les. It has been written with the assumption that you have experience with Samba, have read *The O cial Samba-3 HOWTO and Reference Guide*

Preface

the original three buildings at the head-office campus. The head office is in New York and you have branch offices in Washington, Los Angeles, and London. Your desktop standard is Windows XP Professional. In many ways, everything has changed and yet it must remain the same. Your team is primed for another roll-out. You know there are further challenges ahead.

over, Samba-3 has won the day. Your team are delighted and now you nd yourself at yet another cross-roads. Abmas have acquired a snack food business, you made promises you must keep. IT costs must be reduced, you have new resistance, but you will win again. This time you choose to install the Squid proxy server to validate the fact that Samba is far more than just a le and print server. SPNEGO authentication support means that your Microsoft Windows clients

pact Samba deployment. Some readers would argue that everyone can be expected to know this information, or at least be able to find it

Table 1 Samba Changes | 3.0.2 to 3.0.20

New Feature	Description
Winbind Case Handling	User and group names returned by **winbindd** are now converted to lower case for

Part I

Example Network Con gurations

Chapter 1

NO-FRILLS SAMBA SERVERS

This is the start of the real journey toward the successful deployment of Samba. For some this chapter is the end of the road because their needs will have been adequately met. For others, this chapter is the beginning of a journey that will take them well past the contents of this book. This book provides example con gurationsfr che prrtcopl

that theeioat thb mo-gntarle-280ohemeio(Sint--)-28a-- priculavos

1. To check the ability to access the smbd daemon services, execute the following:

1.2.2 Charity Administration O ce

o ered a choice between the LPRng printing system or CUPS. It appears,

The 755 permissions on this directory (mount point) permit the owner to read, write, and execute, and the group and everyone else to read and execute only.

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

5. Install the \Client for Microsoft Networks." Ensure that the only option enabled in its properties is the option \Logon and restore network

1.2.2.3 Validation

Use the same validation process as was followed in Section 1.2.1.3.

1.2.3 Accounting O ce

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 ses Windows

1.2.3.1 Dissection and Discussion

Figure 1.2 Accounting Office Network Topology

Table 1.1 Accounting Office Network Information

1.3 Questions and Answers

Section

Chapter 2

SMALL OFFICE NETWORKING

Chapter 1, \No-Frills Samba Servers" focused on the basics of simple yet e ective network solutions. Network administrators who take pride in their work (that's most of us, right?) take care to deliver what our users want, but

conversion, he held another meeting asking for cooperation in the introduc-

the business over to a bright and capable executive who can make things happen. This means your network design must cope well with growth.

In a few months, Abmas will require an Internet connection for email and so58914Thiswae dates Mr Mans278(y-37h6c)1(ss-37h6c)278(aemngs-4Thisu)-TJ 0 -13.549

Section

the accounting department and the other for the nancial services depart-

4.

```
# File Format
# -----------
# Unix_ID = Windows_ID
#
# Examples:
# root = Administrator
# janes = "Jane Smith"
# jimbo = Jim Bones
#
# Note: If the name contains a space it must be double quoted.
#       In the example above the name 'jimbo' will be mapped to Windows
#       user names 'Jim' and 'Bones' because the space was not quoted.
##############################################################################
root = Administrator
####
# End of File
####
```

9. Create and map Windows Domain Groups to UNIX groups. A sample script is provided in Example 2.3.1. Create a l418(Cre)]Ta space it must be double quot

Example 2.3.1 Script to Map Windows NT Groups to UNIX Groups

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

# Create UNIX groups
groupadd acctsdep
groupadd finsrvcs

# Map Windows Domain Groups to UNIX groups
net groupmap add ntgroup="Domain Admins"  unixgroup=root type=d
net groupmap add ntgroup="Domain Users"   unixgroup=users type=d
net groupmap add ntgroup="Domain Guests"  unixgroup=nobody type=d

# Add Functional Domain Groups
net groupmap add ntgroup="Accounts Dept"  unixgroup=acctsdep type=d
net groupmap add ntgroup="Financial Services" unixgroup=finsrvcs type=d
```

```
    Administrators (S-1-5-32-544) -> -1
    Backup Operators (S-1-5-32-551) -> -1
    Domain Admins (S-1-5-21-194350-25496802-3394589-512) -> root
    Domain Guests (S-1-5-21-194350-25496802-3394589-514) -> nobody
    Domain Users (S-1-5-21-194350-25496802-3394589-513) -> users
    Financial Services (S-1-5-21-194350-25496802-3394589-2005) -> finsrvcs
    Guests (S-1-5-32-546) -> -1
    Power Users (S-1-5-32-547) -> -1
    Print Operators (S-1-5-32-550) -> -1
    Replicators (S-1-5-32-552) -> -1
    System Operators (S-1-5-32-549) -> -1
    Users (S-1-5-32-545) -> -1
```

10.

agement under UNIX, such as useradd and

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

17. Edit the file /etc/cups/mime.types

```
        SLEETH              Samba 3.0.20

        Workgroup           Master
        ---------           -------
        BILLMORE            SLEETH
```

This demonstrates that an anonymous listing of shares can be obtained. This is the equivalent of browsing the server from a Windows client to obtain a list of shares on the server. The `-U%` argument means

```
  .qt                         DH        0  Fri Sep  5 00:48:25 2003
  SMB                          D        0  Sun Oct 19 23:04:30 2003
  Documents                    D        0  Sat Nov  1 00:31:51 2003
  xpsp1a_en_x86.exe          A  131170400  Sun Nov  2 01:25:44 2003

                65387 blocks of size 65536. 28590 blocks available
smb: \> q
```

Section 2.4. Questions and Answers

7. Q: *I deleted my `root` account and now I cannot add it back! What can I*47

workstation?

A: Samba-3 implements a Windows NT4-style security domain architecture. This type of Domain cannot be managed using tools present on a Windows XP Professional installation. You may download from the Microsoft Web

Section 2.4. Questions and Answers

Chapter 3

as a marginal update. You decided to give everyone, even the notebook user, a new desktop computer.

You procured a DSL Internet connection that provides 1.5 Mb/sec (bidirectional) and a 10 Mb/sec ethernet port. You registered the domain abmas.us, and the Internet Service Provider (ISP) is supplying secondary DNS. Information furnished by your ISP is shown in Table 3.1.

speci ed in RFC1918 in the 172.16.0.0/16 range. This is done in subsequent chapters.

The high growth rates projected are a good reason to use the `tdbsam` passdb backend. The use of `smbpasswd`

agement software can also be run only from the central application server. Notebook users are provided with locally installed applications on a need-to-have basis only.

The introduction of roaming pro les support means that users can move between desktop computer systems without constraint while retaining full access to their data. The desktop travels with them as they3(with)-379(as)-3e

Section 3.3. Implementation

4. Create the username map file to permit the root account to be called Administrator from the Windows network environment. To do this, create the file /etc/samba/smbusers with the following contents:

```
####
# User mapping file
####
# File Format
# -----------
# Unix_ID = Windows_ID
#
# Examples:
# root = Administrator
# janes = "Jane Smith"
# jimbo = Jim Bones
#
# Note: If the name contains a space it must be double quoted.
#       In the example above the name 'jimbo' will be mapped to Windows
#       user names 'Jim' and 'Bones' because the space was not quoted.
##############################################################################
root = Administrator
####
# End of File
####
```

5. Create and map Windows Domain Groups to UNIX groups. A sample script is provided in Chapter 2, \Small Office Networking", Example 2.3.1. Create a file containing this script. We called ours /etc/samba/initGrps.sh. Set this file so it can be executed, and then execute the script. Sample output should be as follows:

```
root#  chmod 755 initGrps.sh
root#  /etc/samba # ./initGrps.sh
Updated mapping entry for Domain Admins
Updated mapping entry for Domain Users
Updated mapping entry for Domain Guests
No rid or sid specified, choosing algorithmic mapping
Successfully added group Accounts Dept to the mapping db
```

```
No rid or sid specified, choosing algorithmic mapping
Successfully added group Domain Guests to the mapping db

root#  /etc/samba # net groupmap list | sort
Account Operators (S-1-5-32-548) -> -1
Accounts Dept (S-1-5-21-179504-2437109-488451-2003) -> acctsdep
Administrators (S-1-5-32-544) -> -1
Backup Operators (S-1-5-32-551) -> -1
Domain Admins (S-1-5-21-179504-2437109-488451-512) -> root
Domain Guests (S-1-5-21-179504-2437109-488451-514) -> nobody
Domain Users (S-1-5-21-179504-2437109-488451-513) -> users
Financial Services (S-1-5-21-179504-2437109-488451-2005) -> finsrvcs
Guests (S-1-5-32-546) -> -1
Power Users (S-1-5-32-547) -> -1
Print Operators (S-1-5-32-550) -> -1
Replicators (S-1-5-32-552) -> -1
System Operators (S-1-5-32-549) -> -1
Users (S-1-5-32-545) -> -1
```

6. There is one preparatory step without which you will not have a working Samba network environment. You must add an account for each network user. For each user who needs to be given a Windows Domain account, make an entry in the /etc/passwd le as well as in the Samba password backend. Use the system tool of your choice to create the UNIX system account, and use the Samba smbpasswd to create a Domain user account. There are a number of tools for user management under UNIX, such as useradd, and adduser, as well as a plethora of custom tools. You also want to create a home directory for each user. You can do this by executing the following steps for each user:

```
root#  useradd -m username
root#  passwd username
Changing password for username.
New password: XXXXXXXX
Re-enter new password: XXXXXXXX
Password changed
root#  smbpasswd -a username
New SMB password: XXXXXXXX
```

```
Retype new SMB password: XXXXXXXX
Added user username.
```

You do of course use a valid user login ID in place of *username*.

7. Using the preferred tool for your UNIX system, add each user to the UNIX groups created previously as necessary. File system access control will be based on UNIX group membership.

8.

```
root#  mkdir -p /var/spool/samba
root#  mkdir -p /var/lib/samba/{netlogon/scripts,profiles}
root#  chown -R root:root /var/spool/samba
root#  chown -R root:root /var/lib/samba
root#  chmr-5252n1.drwxt /var/spool/samba
root#  chmr-5252n12775 /var/lib/samba/profiles
root#  chgrp users /var/lib/samba/profiles
```

For each user account that is created on the system, the following commands should be executed:

```
root#  mkdir /var/lib/samba/profiles/'username'
root#  chown 'username':users /var/lib/samba/profiles/'username'
root#  chmr-5252n1ug+wrx,o+rx,-w /var/lib/samba/profiles/'username'
```

```
root#  lpadmin -p qmsf -v socket://qmsf.abmas.biz:9100 -E
root#  lpadmin -p hplj6f -v socket://hplj6f.abmas.biz:9100 -E
```

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

4. Print queues may not be enabled at creation. Use `lpc stat` to check the status of the print queues and, if necessary, make certain that the queues you have just created are enabled by executing the following:

```
root#  /usr/bin/enable qmsa
```

Note: If the parameter *cups options = Raw* is speci ed in the smb.conf

3.3.6 Validation

Complex networking problems are most often caused by simple things that are poorly or incorrectly con gured. The validation process adopted here should be followed carefully; it is the result of the experience gained from years of making and correcting the most common mistakes. Shortcuts often lead to basic errors. You should refrain from taking shortcuts, from making basic assumptions, and from not exercising due process and diligence in network validation. By thoroughly testing and validating every step in the process of network installation and con guration, you can save yourself from sleepless nights and restless days. A well debugged network is a foundation for happy network users and network administrators. Later in this book you learn how to make users happier. For now, it is enough to learn to validate. Let's get on with it. Server Validation Steps

1. One of the most important facets of Samba con guration is to ensure that name resolution functions correctly. You can check name

2. So far, your installation is going particularly well. In this step we validate DNS server and name resolution operation. Using your favorite

```
sleeth1.abmas.biz has address 192.168.1.1
```

You may now remove the entry called

```
---------           -------
DIAMOND             Samba 3.0.20

Workgroup           Master
---------           -------
```

```
22/tcp      open        ssh
```

Please do not use an administrative installation of proprietary and commercially licensed software products to violate the copyright holders' property. All software is licensed, particularly software that is licensed for use free of charge. All software is the property of the copyright holder unless the author and/or copyright holder has explicitly disavowed ownership and has placed the software into the public domain.

Software that is under the GNU General Public License, like proprietary software, is licensed in a way that restricts use. For example, if you modify GPL software and then distribute the binary version of your modi cations, you must o er to provide the source code as well. This restriction is designed to maintain the momentum of the di usion of technology and to protect against the withholding of innovations.

Commercial and proprietary software generally restrict use to those who have paid the license fees and who comply with the licensee's terms of use. Software that is released under the GNU General Public License is restricted to particular terms and conditions also. Whatever the licensing terms may be, if you do not approve of the terms of use, please do not use the software.

Samba is provided under the terms of the 56(th-287se 7(w)27(2u(e)-28.sebJ 0 -ur-286u56(thT)27

11.

Section 3.4. Questions and Answers

Section

9. Q: *Why would you use WINS as well as DNS-based name resolution?*
A: WINS is to NetBIOS names as DNS is to fully quali ed domain names (FQDN). The FQDN is a name like \myhost.mydomain.tld" where *tld* means top-level domain. A FQDN is a longhand but easy-to-remember expression that may be up to 1024 characters in length and that represents an IP address. A NetBIOS name is always 16 characters long. The 16th character is a name type indicator. A speci c name type is registered[7] for each type of service that is provided by the Windows server or client and

Section 3.4. Questions and Answers

Example 3.3.4 130 User Network with *tdbsam* | Services Section Part B

```
[service]
```

Example 3.3.6 DHCP Server Con guration File | /etc/dhcpd.conf

Example 3.3.10 DNS 192.168.1 Reverse Zone File

```
$ORIGIN .
$TTL 38400  ; 10 hours 40 minutes
1.168.192.in-addr.arpa  IN SOA   sleeth.abmas.biz. root.abmas.biz. (
            2003021825 ; serial
            10800      ; refresh (3 hours)
            3600       ; retry (1 hour)
            604800     ; expire (1 week)
            38400      ; minimum (10 hours 40 minutes)
            )
         NS sleeth1.abmas.biz.
$ORIGIN 1.168.192.in-addr.arpa.
1        PTR   sleeth1.abmas.biz.
20       PTR   qmsa.abmas.biz.
30       PTR   hplj6a.abmas.biz.
```

Example 3.3.11 DNS 192.168.2 Reverse Zone File

```
$ORIGIN .
$TTL 38400  ; 10 hours 40 minutes
2.168.192.in-addr.arpa  IN SOA   sleeth.abmas.biz. root.abmas.biz. (
            2003021825 ; serial
            10800      ; refresh (3 hours)
            3600       ; retry (1 hour)
            604800     ; expire (1 week)
            38400      ; minimum (10 hours 40 minutes)
            )
         NS sleeth2.abmas.biz.
$ORIGIN 2.168.192.in-addr.arpa.
1        PTR   sleeth2.abmas.biz.
20       PTR   qmsf.abmas.biz.
30       PTR   hplj6f.abmas.biz.
```

Example 3.3.12 DNS Abmas.biz Forward Zone File

```
$ORIGIN .
$TTL 38400$TTL $ORIGIN0(;8400)-minimumTJ0N0108400
```

Chapter 4

THE 500-USER OFFICE

The Samba-3 networking you explored in Chapter 3, \Secure O ce Networking"

Section

DirectPointe Inc. receives from you a new standard desktop con guration every four months. They automatically roll that out to each desktop system. You must keep DirectPointe informed of all changes.

The new network has a single Samba Primary Domain Controller (PDC) located in the Network Operation Center (NOC). Buildings 1 and 2 each have a local server for local application servicing. It is a domain member. The new system uses the *tdbsam* passdb backend.

Because of the refusal to use an LDAP (ldapsam) passdb backend atdBecthis t(ssem(ctie,)-42he)-356

Section

Table 4.1 Domain: MEGANET, File Locations for Servers

Section 4.3. Implementation

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

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

```
application/octet-stream
```

14. Refer to the CUPS printing manual for instructions regarding how to configure CUPS so that print queues that reside on CUPS servers on remote networks route print jobs to the print server that owns that queue. The default setting on your CUPS server may automatically discover remotely installed printers and may permit this functionality

lation guidance will assist you in working through the process of con guring the PDC and then both BDC's.

If you just execute these commands manually, the route table entries you have created are not persistent across system reboots. You

Example 4.3.1 Server: MASSIVE (PDC), File: /etc/samba/smb.conf

```
# Global parameters
 [global]
        workgroup = MEGANET
        netbios name = MASSIVE
        interfaces = eth1, lo
        bind interfaces only = Yes
        passdb backend = tdbsam
        smb ports = 139
```

Section

```
root#  service named restart
root#  service cups restart
root#  service smb restart
root#  service swat restart
```

4.3.5 Windows Client Con guration

The procedure for desktop client con guration for the network in this chapter is similar to that used for the previous one. There are a few subtle changes that should be noted. Windows Client Con guration Steps

1. Install MS Windows XP Professional. During installation, con gure the client to use DHCP for TCP/IP protocol con guration. DHCP con gures all Windows clients to use the WINS Server address that has been de ned for the local subnet.

2. Join the Windows domain `MEGANET`

6. Now install all applications to be installed locally. Typical tools include Adobe Acrobat, NTP-based time synchronization software, drivers

the system, and then log on as the local administrator and clean out all temporary les stored on the system. Before shutting down, use the disk defragmentation tool so that the le system is in optimal condition before replication.

9. Boot the workstation using the Norton (Symantec) Ghosting disk (or CD-ROM) and image the machine to a net407(d357(sna)-334shar4)1he the

uo md357yoo replicaeo image using Gonsn
eduore to the machinsm.akn to useeduore
thatensuorisemact(mac)78(hine)-14(hase)-14(as)-15(uniqune)-14(Win(do)28(is)-15(securitd357yo)-14(

4.

Section

Example 4.3.9 Server: BLDG2, File: dhcpd.conf

```
# Abmas Accounting Inc.

default-lease-time 86400;
max-lease-time 172800;
default-lease-time 86400;
ddns-updates on;
ddns-update-style interim;

option ntp-servers 172.16.0.1;
option domain-name "abmas.biz";
option domain-name-servers 172.16.0.1, 172.16.4.1;
option netbios-name-servers 172.16.0.1;
option netbios-node-type 8;

subnet 172.16.8.0 netmask 255.255.252.0 {
        range dynamic-bootp 172.16.9.0 172.16.10.255;
        option subnet-mask 255.255.252.0;
        option routers 172.16.8.128;
        allow unknown-clients;
   }
subnet 127.0.0.0 netmask 255.0.0.0 {
        }
```

Example 4.3.11 Server: MASSIVE, File: named.conf, Part: B

```
zone "abmas.biz" {
   type master;
   file "/var/lib/named/master/abmas.biz.hosts";
   allow-query {
      mynet;
   };
   allow-transfer {
      mynet;
   };
   allow-update {
      mynet;
   };
};

zone "abmas.us" {
        type master;
        file "/var/lib/named/master/abmas.us.hosts";
        allow-query {
                all;
        };
        allow-transfer {
                seconddns;
        };
};
```

Example 4.3.12 Server: MASSIVE, File: named.conf, Part: C

```
zone "0.16.172.in-addr.arpa" {
   type master;
   file "/var/lib/named/master/172.16.0.0.rev";
   allow-query {
      mynet;
   };
   allow-transfer {
      mynet;
   };
   allow-update {
      mynet;
   };
};

zone "4.16.172.in-addr.arpa" {
   type master;
   file "/var/lib/named/master/172.16.4.0.rev";
   allow-query {
      mynet;
   };
   allow-transfer {
      mynet;
   };
   allow-update {
      mynet;
   };
};

zone "8.16.172.in-addr.arpa" {
   type master;
   file "/var/lib/named/master/172.16.8.0.rev";
   allow-query {
      mynet;
   };
   allow-transfer {
      mynet;
   };
   allow-update {
      mynet;
   };
};
```

Example 4.3.16 Servers: BLDG1/BLDG2, File: named.conf, Part: B

```
zone "abmas.biz" {
   type slave;
   file "/var/lib/named/slave/abmas.biz.hosts";
   allow-query {
      mynet;
   };
```

Example 4.3.17

of clients it can service reliably is reduced, and generally for low powered hardware should not exceed 30 machines (Windows workstations

ber of factors, including:

Network overload (typically indicated by a high network collision rate)

Server overload

Timeout causing the client to close a connection that is in use but has been latent (no tra c) for some time (5 minutes or more)

Defective networking hardware

Section 5.1. Regarding LDAP Directories and Windows Computer Accounts

well as for Samba. From the OpenLDAP perspective, UNIX system accounts are stored POSIX schema extensions. Samba provides its own schema to permit storage of account attributes Samba needs. Samba-3 can use the LDAP backend to store:

Windows Networking User Accounts

Windows NT Group Accounts

Mapping Information between UNIX Groups and Windows NT Groups

ID Mappings for SIDs to UIDs (also for foreign Domain SIDs)

The use of LDAP with Samba-3 makes it necessary to store UNIX accounts as well as Windows Networking accounts in the LDAP backend. This implies the need to use the PADL LDAP tools[14]. The resolution of the UNIX

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 NTUSER.DAT and a number of folders (My Documents, Application Data, Desk-

ing intelligent printing should review documentation on the Easy Software Products Web site.

Warning

Do not be lulled into thinking that you can easily adopt the examples in this book and adapt them without first working through the examples provided. A little thing overlooked can cause untold pain and may permanently tarnish your experience.

The Name Service Caching Daemon The name service caching daemon (nscd) is a primary cause of di culttodoltod-t.412(cacult3nsolud [(,cul3old)rti(diarl(primarwherecussion)]TJ/F28

Section

The diagnostic process should follow these steps: NSS$_L$

Let us consider an example of use where the following DIT has been implemented:

```
[global]
   ...
   log level = 1
   log file = /var/log/samba/%m.log
   max log size = 50
   ...
```

The log file can be analyzed by executing:

```
root#  cd /var/log/samba
root#  grep -v "^\[200" machine_name.log
```

Search for hints of what may have failed by looking for the words *fail* and

prepare yourself, and frequently review the steps ahead while making at least a mental note of what has already been completed. The following task list may help you to keep track of the task items that are covered:

Samba-3 PDC Server Con guration

1.

5. Install software

6. Creation of roll-out images**5.4.o0.8amba**

Note

Samba-3 and OpenLDAP will have a degree of interdependence that is unavoidable. The method for bootstrapping the LDAP and Samba-3 con guration is relatively straightforward. If you follow these guidelines, the resulting system should work ne. OpenLDAP Server Con- guration Steps

1. Install the le shown in Example 5.4.2 in the directory /etc/openldap.

2. Remove all les from the directory /data/ldap, making certain that the directory exists with permissions:

```
root#  ls -al /data | grep ldap
drwx------   2 ldap    ldap       48 Dec 15 22:11 ldap
```

Example 5.4.1 LDAP DB_CONFIG File

```
set_cachesize           0 150000000 1
set_lg_regionmax        262144
set_lg_bsize            2097152
#set_lg_dir             /var/log/bdb
set_flags               DB_LOG_AUTOREMOVE
```

5.4.2 PAM and NSS Client Con guration

The steps that follow involve con guration of LDAP, NSS LDAP-based resolution of users and groups. Also, so that LDAP-based accounts can log onto the system, the steps ahead con gure the Pluggable Authentication Modules (PAM) to permit LDAP-based authentication.

Since you have chosen to put UNIX user and group accounts into the LDAP database, it is likely that you may want to use them for UNIX system (Linux) local machine logons. This necessitates correct con guration of PAM. The pam

can use either implementation, but if the pam_unix2.so on your

```
Processing section "[pidata]"
Processing section "[homes]"
Processing section "[printerspidata]"
```

```
root#  cp smbldap*conf /etc/smbldap-tools/
root#  chmod 750 /opt/IDEALX/sbin/smbldap-*
root#  chmod 750 /opt/IDEALX/sbin/configure.pl
root#  chmod 640 /etc/smbldap-tools/smbldap.conf
root#  chmod 600 /etc/smbldap-tools/smbldap_bind.conf
```

4.

Section

```
sambaSID: S-1-5-21-3504140859-1010554828-2431957765-553
sambaGroupType: 2
displayName: Domain Computers
structuralObjectClass: posixGroup
entryUUID: 5e0a41d8-c536-1027-9d3b-b1f32350fb43
creatorsName: cn=Manager,dc=abmas,dc=biz
createTimestamp: 20031217234206Z
entryCSN: 2003121723:42:06Z#0x0002#0#0000
modifiersName: cn=Manager,dc=abmas,dc=biz
modifyTimestamp: 20031217234206Z
```

This looks good so far.

8. The next step is to prove that the LDAP server is rup16vTing anp16d responds to a search request. Execute the following as shown

```
dn: cn=Domain Computers,ou=Groups,dc=abmas,dc=biz
```

```
uid=1002(chrisr) gid=513(Domain Users) groups=513(Domain Users)
```

This confirms that the UNIX (POSIX) user account information can be resolved from LDAP by system tools that make a getentpw() system call.

13. The root account must have UID=0; if not, this means that operations conducted from a Windows client using tools such as the Domain User Manager fails under UNIX because the management of user and group accounts requires that the UID=0. Additionally, it is a good idea to make certain that no matter

This is precisely what we want to see.

16.

```
root#  ./smbldap-groupadd -a PIOps
```

The addition of groups does not involve keyboard interaction, so

```
  .urlview             H      311  Fri Jul  7 06:55:35 2000
  .dvipsrc             H      208  Fri Nov 17 11:22:02 1995

                57681 blocks of size 524288. 57128 blocks available
smb: \> q
```

Well done. All is working ne.

The server MASSIVEiscon(gured,g)-04(ands)-297itstimhee

.4.68 Prinpter on(gurationw)]TJ/F15 10.9091 Tf 0 -27
sm.confE

```
root#  mkdir -p /var/lib/samba/drivers/{W32ALPHA,W32MIPS,W32X86,WIN40}
root#  chown -R root:root /var/lib/samba/drivers
root#  chmod -R ug=rwx,o=rx /var/lib/samba/drivers
```

5.5 Samba-3 BDC Con guration

Con guration of BDC Called: BLDG1

1. Install the les in Example 5.5.1, Example 5.5.3, and Example 5.5.4 into the /etc/samba/ directory. The three les should be added together to form the smb.conf le.
2. Verify the smb.conf le as in step 2 of Section 5.4.3.
3. Carefully follow the steps outlined in Section 5.4.2, taking par-

Section 5.5. Samba-3 BDC Configuration

Section 5.6. Miscellaneous Server Preparation Tasks

Section 5.6. Mi701 T1ellaneousra

5.7.1 Con guration of Default Pro le with Folder Redirection

Log onto the Windows XP Professional workstation as the local `Administrator`. It is necessary to expose folders that are generally hidden to provide access to the `Default User` folder. Expose Hidden Folders

1.

Section

```
veto oplock files = /*.pdf/*.PST/
```

5.7.3 Con gure Delete Cached Pro les on Logout

Con gure the Windows XP Professional client to auto-delete roaming pro les on logout:

Click **Start** ! **Run**. In the dialog box, enter M M C and click **OK**.

Follow these steps to set the default behavior of the staging machine so that all roaming pro les are deleted as network users log out of the system. Click **File** ! **Add/Remove Snap-in** ! **Add** ! **Group Policy** ! **Add** ! **Finish** ! **Close** ! **OK**.

The Microsoft Management Console now shows the **Group Policy** utility that enables you to set the policies needed. In the left panel, click **Local Computer Policy** ! **Administrative Templates** ! **System** ! **User Pro les**. In the right panel, set the properties shown here by double-clicking on each item as shown:

> Do not check for user ownership of Roaming Pro le Folders = Enabled
>
> Delete cached copies of roaming pro les = Enabled

Close the Microsoft Management Console. The settings take immediate e ect and persist onto all image copies made of this system to deploy the new standard desktop system.

5.7.4 Uploading Printer Drivers to Samba Servers

Users want to be able to use network printers. You have a vested interest in making it easy for them to print. You have chosen to install the printer drivers onto the Samba servers and to enable point-and-click

that only minimal application stubware needs to be installed onto the desktop systems. You should proceed with software installation and

As a minimum, the LDAP server must be protected by way of Access Control Lists (ACLs), and it must be con gured to use secure protocols for all communications over the network. Of course, secure networking does not result just from systems design and implementation but involves constant user education training and, above all, disciplined attention to detail and constant searching for signs of unfriendly or alien activities. Security is itself a topic for a whole book. Please do consult appropriate sources. Jerry Carter's book *LDAP System Administration*[26] is a good place to start reading about OpenLDAP as well as security considerations.

The substance of this chapter that has been deserving of particular attention includes:

Implementation of an OpenLDAP-based passwd backend, nec-

F.A.Q.

1.

details of creating a whole solution framework. I have not tightened every nut and bolt, but I have touched on all the issues you need to

Example 5.4.2

Example 5.4.3 LDAP Master Con guration File | /etc/openldap/slapd.

Example 5.4.4 Con guration File for NSS LDAP Support | /etc/ldap.conf

```
host 127.0.0.1
```

Example 5.4.5

Chapter 6

A DISTRIBUTED 2000-USER NETWORK

as implementing a DNS or a DHCP server are under control. Even the basics of Samba are largely under control. So in this section you focus on the specifics of implementing LDAP changes, Samba changes, and

Section

6.2.1.2 The Nature of Windows Networking Protocols

Section

there can be only one PDC, all additional domain controllers are by de nition BDCs.

The provision of su cient servers that are BDCs is an important design factor. The second important design factor involves how each of the BDCs obtains user authentication data. That is the subject of the next section, which involves key decisions regarding Identity Management facilities.

6.2.1.3 Identity Management Needs

Network managers recognize that in large organizations users generally need to be given resource access based on needs, while being excluded from other resources for reasons of privacy. It is therefore essential that all users identify themselves at the point of network access. The network logon is the principal means by which user credentials are validated and ltered and appropriate rights and privileges are allocated.

Unfortunately, network resources tend to have their own Identity Management facilities, the quality and manageability of which varies from quite poor to exceptionally good. Corporations that use a mixture of

with those on the East Coast, each have their own domain name space and can be independently managed and controlled. One of the key drawbacks of this design is that it ies in the face of the ability for network users to roam globally without some compromise in how they may access global resources.

Desk-bound users need not be negatively a ected by this design, since

As the LDAP directory grows, it becomes increasingly important that its structure is implemented in a manner that mirrors organizational needs, so as to limit network update and referential tra c. It should be noted that all directory administrators must of necessity follow the same standard procedures for managing the directory, because retroactive correction of inconsistent directory information can be exceedingly di cult.

6.2.2 Political Issues

Additionally, it is possible to use multiple passdb backends concurrently as well as have multiple LDAP backends. As a result, you can specify a failover LDAP backend. The syntax for specifying a single LDAP backend in `smb.conf` is:

```
...
passdb backend = ldapsam:ldap://master.abmas.biz
...
```

This configuration tells Samba to use a single LDAP server, as shown in Figure 6.2.

Figure 6.2 Samba Configuration to Use a Single LDAP Server

Note

When the use of ldapsam is speci ed twice, as

```
userPassword: not24get

dn: cn=sambaadmin,dc=abmas,dc=biz
objectClass: person
cn: sambaadmin
sn: sambaadmin
userPassword: buttercup
```

4.

segment. As a rule, there should be two DHCP servers per network segment. This means that if one server fails, there is always another to

3. Q: *LDAP has a database. Is LDAP not just a fancy database front end?*

A: LDAP does store its data in a database of sorts. In fact, the

Example 6.3.3 Primary Domain Controller smb.conf File | Part A

```
# Global parameters
```

Example 6.3.4 Primary Domain Controller smb.conf File | Part B

Example 6.3.5 Primary Domain Controller smb.conf File | Part C

Example 6.3.6 Backup Domain Controller smb.conf File | Part A

Figure 6.6 Network Topology | 2000 User Complex Design A

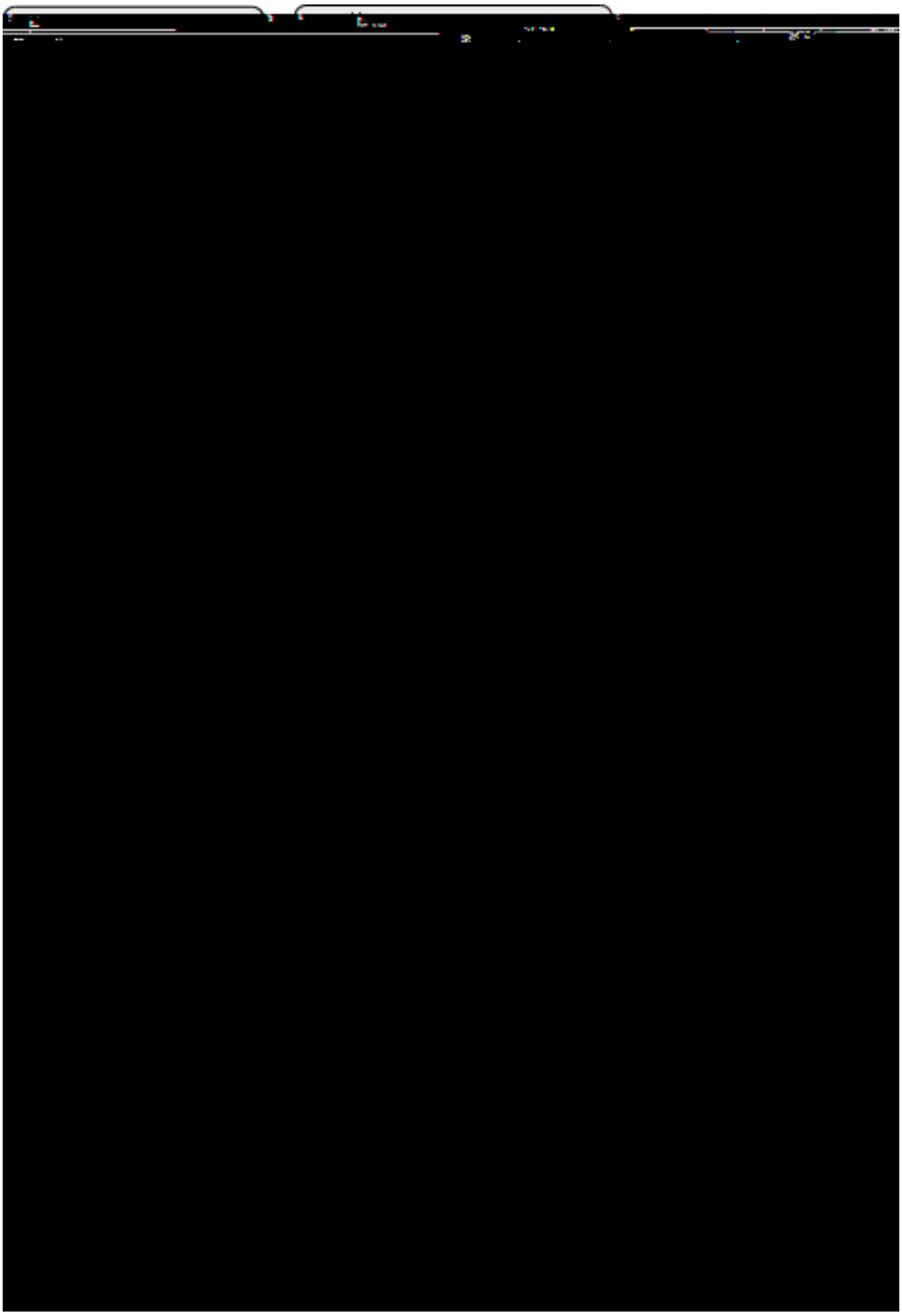
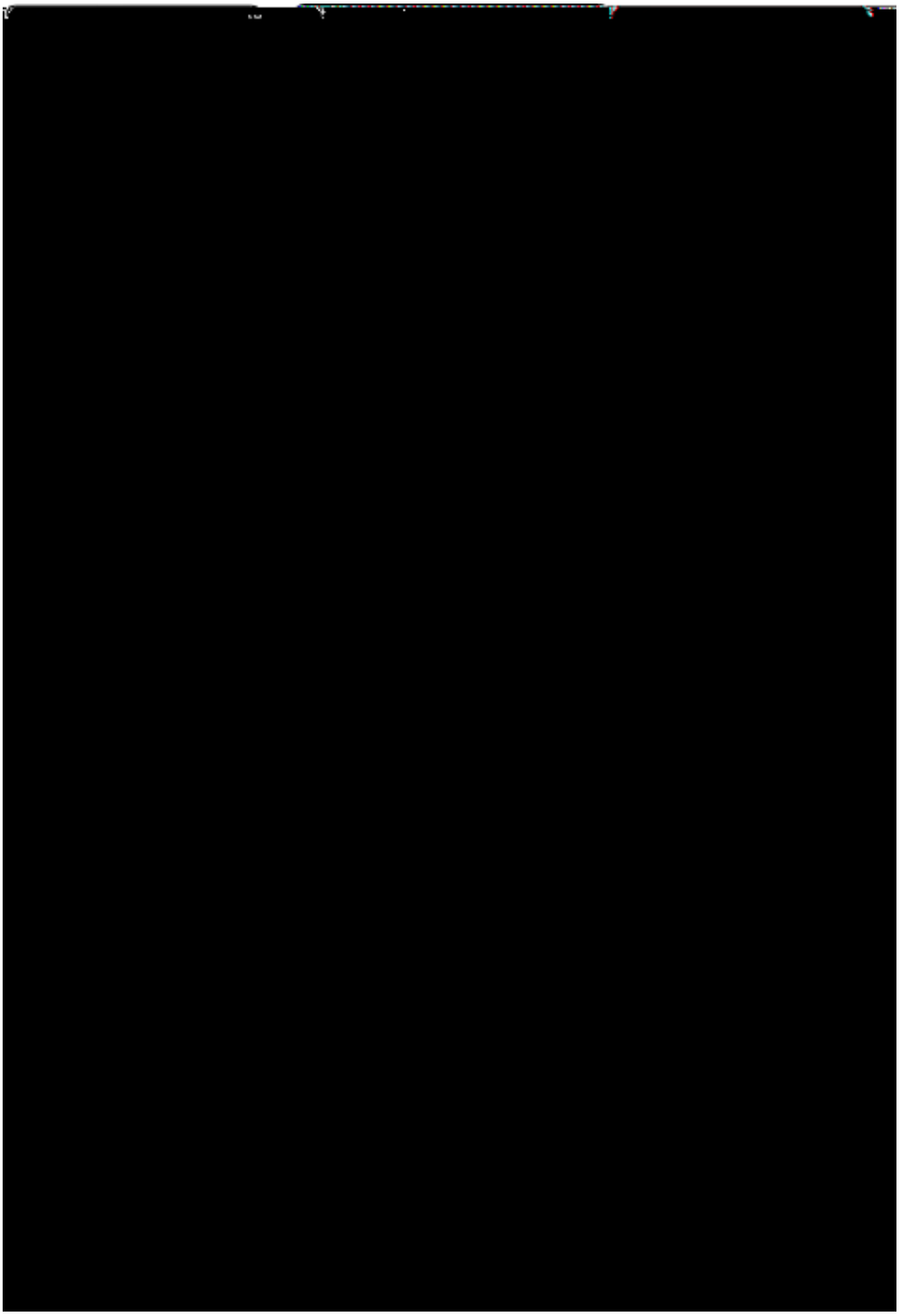


Figure 6.7 Network Topology | 2000 User Complex Design B



DOMAIN MEMBERS, UPDATING SAMBA AND

Chapter 7

ADDING DOMAIN MEMBER SERVERS AND CLIENTS

The most frequently discussed Samba subjects over the past 2 years have focused around domain control and printing. It is well known that h(jects,]-028(tis28(tiskcts,]-ma15110.ts,]-gi(fo)-28(28)-2[28(28)-ap-1(n)28aranc28(28)-)-2328)-e)-231(b)

Figure 7.1 Open Magazine Samba Survey

Over the past 6 months, you have hired several new sta who want Linux on their desktops. You must integrate these systems to make sure that Abmas is not building islands of technology. You ask Christine to do likewise at Swodniw Biz NL (your friend's company) to

For many administrators, it should be plain that the use of an LDAP-based repository for all network accounts (both for POSIX accounts and for Samba accounts) provides the most elegant and controllable facility. You eventually appreciate the decision to use LDAP.

If your networkfmaectiokede LD728(Ar)-40r(d)1(e)-repositorY

7.2.2 Political Issues

One of the most erce con icts recently being waged is resistance to the adoption of LDAP, in particular OpenLDAP, as a replacement for

idmap uid and *idmap gid* ranges. Where LDAP is used, the mappings can be stored in LDAP so that all domain member servers can

available. The home directories could be mounted o a domain controller using NFS or by any other suitable means. Second, the absence of the domain name in the home directory path is indicative that identity resolution is not being done via winbind.

```
root#  getent group
...
Domain Admins:x:512:root,jht
Domain Users:x:513:bobj,stans,chrisr,maryv,jht,josephj
Domain Guests:x:514:
Accounts:x:1000:
Finances:x:1001:
PIOps:x:1002:
sammy:x:4321:
```

an anonymous connection can be sustained, then try again. It is possible (perhaps even recommended) to use the following to validate the ability to connect to an NT4 PDC/BDC:

7.3.2 NT4/Samba Domain with Samba Domain Member Server: Using NSS and Winbind

lowing:

```
net rpc join -U root%not2g4et
Joined domain MEGANET2.
```

This indicates that the domain join succeed.

4. Validate operation of winbind using the wbinfo tool as follows:

```
root#  wbinfo -u
MEGANET2+root
MEGANET2+nobody
MEGANET2+jht
MEGANET2+maryv
MEGANET2+billr
MEGANET2+jelliott
MEGANET2+dbrady
MEGANET2+joeg
MEGANET2+balap
```

```
root#  getent passwd
...
MEGANET2+root:x:10000:10001:NetBIOS Domain Admin:
                        /home/MEGANET2/root:/bin/bash
MEGANET2+nobody:x:10001:10001:nobody:
                        /home/MEGANET2/nobody:/bin/bash
MEGANET2+jht:x:10002:10001:John H Terpstra:
                        /home/MEGANET2/jht:/bin/bash
MEGANET2+maryv:x:10003:10001:Mary Vortexis:
                        /home/MEGANET2/maryv:/bin/bash
MEGANET2+billr:x:10004:10001:William Randalph:
                        /home/MEGANET2/billr:/bin/bash
MEGANET2+jelliott:x:10005:10001:John G Elliott:
                        /home/MEGANET2/jelliott:/bin/bash
MEGANET2+dbrady:x:10006:10001:Darren Brady:1:Darren Brady:1:Darren Brady:1.
MEGANET2+jhtoeg:10006:70001:Johne525(G)-ree
                        /home/MEGANET2/rotoeg:in/bash
MEGANET2+bilalap:10006:80001:JoBala525(G)Plr:a1:Darren Brady:1:Darren Brady:1.olalap:in/bash
```

7.3.4 Active Directory Domain with Samba Domain Member Server

One of the much-sought-after features new to Samba-3 is the ability to join an Active Directory domain using Kerberos pro-

```
HAVE_KRB5_GET_PW_SALT
HAVE_KRB5_KEYBLOCK_KEYVALUE
HAVE_KRB5_KEYTAB_ENTRY_KEYBLOCK
HAVE_KRB5_MK_REQ_EXTENDED
HAVE_KRB5_PRINCIPAL_GET_COMP_STRING
HAVE_KRB5_SET_DEFAULT_IN_TKT_ETYPES
HAVE_KRB5_STRING_TO_KEY
HAVE_KRB5_STRING_TO_KEY_SALT
HAVE_LIBKRB5
```

This output was obtained on a SUSE Linux system and shows the output for Samba that has been compiled and linked with the Heimdal Kerberos libraries. The follow-

```
Joined 'FRAN' to realm 'LONDON.ABMAS.BIZ'
```

You have successfully made your Samba-3 server a member of the ADS domain using Kerberos protocols. In the event that you receive no output messages, a silent return means that the domain join failed. You should use ethereal to identify what may be failing. Common causes of a failed join include:

Defective or miscon gured DNS name resolution.

```
{
key = "SECRETS/MACHINE_PASSWORD/LONDON"
data = "le3Q5FPnN5.ueC\00"
}
{
key = "SECRETS/MACHINE_SEC_CHANNEL_TYPE/LONDON"
data = "\02\00\00\00"
}
{
key = "SECRETS/MACHINE_LAST_CHANGE_TIME/LONDON"
data = "E\89\F6?"
}
```

This is given to demonstrate to the skeptics that this pro-

```
LONDON+Domain Admins
LONDON+Domain Users
LONDON+Domain Guests
LONDON+Group Policy Creator Owners
LONDON+DnsUpdateProxy
```

Excellent. That worked also, as expected.

12. Now repeat this via NSS to validate that full identity resolution is functional as required. Execute:

```
root#  getent passwd
...
LONDON+Administrator:x:10000:10000:Administrator:
             /home/LONDON/administrator:/bin/bash
LONDON+Guest:x:10001:10001:Guest:
             /home/LONDON/guest:/bin/bash
LONDON+SUPPORT_388945a0:x:10002:10000:SUPPORT_388945a0:
             /home/LONDON/support_388945a0:/bin/bash
LONDON+krbtgt:x:10003:10000:krbtgt:
             /home/LONDON/krbtgt:/bin/bash
LONDON+jht:x:10004:10000:John H. Terpstra:
             /home/LONDON/jht:/bin/bash
```

Okay, ADS user ad1 Tf.ttpdatePt s -r.3fbxpked. No728(w)233y(w)28u(w)233try

...
LONDON+Domain
LONDON+Domain

```
LONDON+DnsUpdateProxy:x:10008:
```

This is very pleasing. Everything works as expected.

13. You may now perform final verification that communica-

```
uSNCreated: 28713
uSNChanged: 28717
name: fran
objectGUID: 58f89519-c467-49b9-acb0-f099d73696e
userAccountControl: 69632
badPwdCount: 0
codePage: 0
countryCode: 0
badPasswordTime: 0
lastLogoff: 0
lastLogon: 127175965783327936
localPolicyFlags: 0
pwdLastSet: 127175952062598496
primaryGroupID: 515
objectSid: S-1-5-21-4052121579-2079768045-1474639452-1109
accountExpires: 9223372036854775807
logonCount: 13
sAMAccountName: fran$
sAMAccountType: 805306369
operatingSystem: Samba
operatingSystemVersion: 3.0.20-SUSE
dNSHostName: fran
userPrincipalName: HOST/fran@LONDON.ABMAS.BIZ
servicePrincipalName: CIFS/fran.london.abmas.biz
servicePrincipalName: CIFS/fran
servicePrincipalName: HOST/fran.london.abmas.biz
servicePrincipalName: HOST/fran
objectCategory: CN=Computer,CN=Schema,CN=Configuration,
                              DC=london,DC=abmas,DC=biz
isCriticalSystemObject: FALSE
-------------- Security Descriptor (revision: 1, type: 0x8c14)
owner SID: S-1-5-21-4052121579-2079768045-1474639452-512
group SID: S-1-5-21-4052121579-2079768045-1474639452-513
------- (system) ACL (revision: 4-------915ICol6025(4---numb(owner
groupSID:1-039452-1109
```

```
------- ACE (type: 0x07, flags: 0x5a, size: 0x38,
               mask: 0x20, object flags: 0x3)
access SID:  S-1-1-0
access type: AUDIT OBJECT
Permissions:
        [Write All Properties]
------- (user) ACL (revision: 4, size: 1944, number of ACEs: 40)
------- ACE (type: 0x00, flags: 0x00, size: 0x24, mask: 0xf01ff)
access SID:  S-1-5-21-4052121579-2079768045-1474639452-512
access type: ALLOWED
Permissions: [Full Control]
------- ACE (type: 0x00, flags: 0x00, size: 0x18, mask: 0xf01ff)
access SID:  S-1-5-32-548
...
------- ACE (type: 0x05, flags: 0x12, size: 0x38,
                mask: 0x10, object flags: 0x3)
access SID:  S-1-5-9
access type: ALLOWED OBJECT
Permissions:
        [Read All Properties]
-------------- End Of Security Descriptor
```

And now you have conclusive proof that your Samba-3 ADS domain member server called `FRAN` is able to communicate fully with the ADS domain controllers.

Your Samba-3 ADS domain member server is ready for use. During training sessions, you may be asked what is inside the `winbindd`_

les. Since curios-

```
}
```

```
data = "\00\00\00\00bp\00\00\01\00\00\00-
   S-1-5-21-4052121579-2079768045-1474639452-500\0D
   Administrator\01\00\00\00"
}
{
key = "SEQNUM/LONDON\00"
data = "xp\00\00C\92\F6?"
}
{
key = "U/S-1-5-21-4052121579-2079768045-1474639452-1110"
data = "\00\00\00\00xp\00\00\03jht\10John H. Terpstra.
   S-1-5-21-4052121579-2079768045-1474639452-1110-
   S-1-5-21-4052121579-2079768045-1474639452-513"
}
{
key = "NS/S-1-5-21-4052121579-2079768045-1474639452-502"
data = "\00\00\00\00bp\00\00-
   S-1-5-21-4052121579-2079768045-1474639452-502"
}
{
key = "SN/S-1-5-21-4052121579-2079768045-1474639452-1001"
data = "\00\00\00\00bp\00\00\01\00\00\00\10SUPPORT_388945a0"
}
{
key = "SN/S-1-5-21-4052121579-2079768045-1474639452-500"
data = "\00\00\00\00bp\00\00\01\00\00\00\0DAdministrator"
}
{
key = "U/S-1-5-21-4052121579-2079768045-1474639452-502"
data = "\00\00\00\00bp\00\00\06krbtgt\06krbtgt-
   S-1-5-21-4052121579-2079768045-1474639452-502-
   S-1-5-21-4052121579-2079768045-1474639452-513"
}
....
```

```
   ticket_lifetime = 36000
   renew_lifetime = 36000
   forwardable = true
   krb4_convert = false
 }
```

Where Heimdal kerberos is installed, edit the /etc/krb5.conf le so it is either empty (i.e., no contents) or it has the following contents:

```
[libdefaults]
        default_realm = SNOWSHOW.COM
        clockskew = 300

[realms]
        SNOWSHOW.COM = {
                kdc = ADSDC.SHOWSHOW.COM
        }

[domain_realm]
        .snowshow.com = SNOWSHOW.COM
```

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

You will need the PADL[3]

is indicated by a silent return to the command prompt with no indication of the reason for failure.

7.3.4.3 IDMAP and NSS Using LDAP from ADS with RFC2307bis Schema Extension

free download

Section

Resolution of user and group identities on domain member machines may be implemented using direct LDAP services or using winbind.

On NSS/PAM enabled UNIX/Linux systems, NSS is responsible for identity management and PAM is responsible for authentication of logon credentials (username and password).

7.4 Questions and Answers

The following questions were obtained from the mailing list and also from private discussions with Windows network administrators.

F.A.Q.

1. Q: *We use NIS for all UNIX accounts. Why do we need winbind?*
A: You can use NIS for your UNIX accounts. NIS does not store the Windows encrypted passwords that need to be stored in

Section

Example 7.3.2 LDIF IDMAP Add-On Load File | File: /etc/openl-

Section 7.4. Questions and Answers

Example 7.3.12 SUSE: PAM xdm Module Using Winbind

```
# /etc/pam.d/gdm (/etc/pam.d/xdm)

#%PAM-1.0
```

Chapter 8

8.1 Introduction

A Windows network administrator explained in an email what changes he was planning to make and followed with the question: \Anyone done this before?" Many of us have upgraded and updated Samba without incident. Others have experienced much pain and user frustration. So it is to be hoped that the notes in this chapter will make a positive di erence by assuring that someone will be saved a lot of discomfort.

Before anyone commences an upgrade or an update of Samba, the one cardinal rule that must be observed is: Backup all Samba

8.1.1 Cautions and Notes

Someone once said, \It is good to be sorry, but better never to need to be!" These are wise words of advice to those contemplating a Samba upgrade or update.

Note

```
   PRIVATE_DIR: /etc/samba
...
```

It is important that both the `smb.conf` file and the `secrets.tdb` be backed up before attempting any upgrade. The `secrets.tdb`

Section

The recommended passdb backends at this time are

Section

After updating the LDAP schema, do not forget to re-index the LDAP database.

8.3.1.3 Updating from Samba Versions after 3.0.6 to a Current Release

Samba-3.0.8 introduced changes in how the *username map* behaves. It also included a change in behavior of

8.3.2.1 Replacing a Domain Member Server

Replacement of a domain member server should be done using the same procedure as outlined in Chapter 7, \Adding Domain Member Servers and Clients".

Section

Chapter 9

MIGRATING NT4 DOMAIN TO SAMBA-3

Ever since Microsoft announced that it was discontinuing support for Windows NT4, Samba users started to ask for detailed

The best advice that can be given to those who set out to merge NT4 domains into a single Samba-3 domain is to promote (sell) the action as one that reduces costs and delivers greater network interoperability and manageability.

9.3 Implementation

Section

Note

The **tdbdump**

perl scripts should be located in the `/opt/IDEALX/sbin` directory. Change into that location, or wherever the scripts have been installed. Execute the `configure.pl` script to con gure the Idealx package for use. Note: Use the domain SID obtained from the step above. The following is

```
. default login shell [/bin/bash] >
. default domain name to append to mail address [] >
                                                    terpstra-world.org
-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
backup old configuration files:
  /etc/smbldap-tools/smbldap.conf->
                                /etc/smbldap-tools/smbldap.conf.old
  /etc/smbldap-tools/smbldap_bind.conf->
                                /etc/smbldap-tools/smbldap_bind.conf.old
writing new configuration file:
  /etc/smbldap-tools/smbldap.conf done.
  /etc/smbldap-tools/smbldap_bind.conf done.
```

```
billw:19:EE35C3481CF7F7DB484448BC86A641A5:...
```

It is of vital importance that the domain SID portions of all group accounts are identical.

20. The nal responsibility in the migration process is to create identical shares and printing resources on the new Samba-3 server, copy all data across, set up privileges, and set share and le/directory access controls.

21. Edit the `smb.conf` le to reset the parameter *domain master* = Yes so that thecreate

24.

```
Creating unix group: 'Recieving'
Creating unix group: 'Rubberboot'
Creating unix group: 'Sales'
Creating unix group: 'Accounting'
Creating unix group: 'Shipping'
Creating account: Administrator
Creating account: Guest
Creating account: TRANSGRESSION$
```

```
Group members of Engineers: Administrator,
                  sharpec(primary),bridge,billw(primary),dhenwick
Group members of Marketoids: Administrator,jacko(primary),
                maryk(primary),jimbo,blue(primary),dork(primary)
Creating unix group: 'Gnomes'
Fetching BUILTIN database
SAM_DELTA_DOMAIN_INFO not handled
```

6. At this point, we can validate our migration. Let's look at the accounts in the form in which they are seen in a smbpasswd le. This achieves that:

```
root#  pdbedit -Lw
Administrator:505:84B0D8E14D158FF8417EAF50CFAC29C3:
     AF6DD3FD4E2EA8BDE1695A3F05EFBF52:[UXmehh4LCT-3DF7AA9F
      Aimbo,:512:6E9A2A51F64A1BD5C187B8085FE1D9DF
           aCDF7E35EF639664E489A0CFBF95EE5E0[UXmehh4LCT-3E9362BC
            Aharpec:511:E4301A7CD8FDD1EC6BBF9BC19CDF851.
```

7.

Section

Section 9.4. Questions and Answers

Example 9.3.2 NT4 Migration Samba-3 Server smb.conf | Part: B

Example 9.3.3 NT4 Migration LDAP Server Con guration File: /etc/openldap/slapd.conf | Part A

Example 9.3.4 NT4 Migration LDAP Server Con guration File: /etc/openldap/slapd.conf | Part B

```
#loglevel       256

#schemacheck     on
idletimeout     30
#backend         bdb
database        bdb
checkpoint      1024 5
cachesize       10000

suffix          "dc=terpstra-world,dc=org"
rootdn          "cn=Manager,dc=terpstra-world,dc=org"
```

Section 9.4. Questions and Answers

Example 9.3.7 NT4 Migration NSS Control File: /etc/nsswitch.conf

The company had outgrown this server several years before and was dealing with severe growing pains. Some of the problems experienced were:

Very slow performance

mation could be imported into LDAP. This would allow use of LDAP for Linux authentication, IMAP, POP3, and SMTP.

Because a decision was made to use Courier-IMAP the schema \authldap.schema" from the Courier-IMAP source, tarball is necessary to resolve Courier-speci c LDAP directory needs. Where

courier-imap
courier-imap-ldap
nss_ldap
openldap2-client
openldap2-devel (only for Samba compilation)
openldap2
pam_ldap
samba-3.0.20 or later
samba-client-3.0.20 or later
samba-winbind-3.0.20 or later
smbldap-tools Version 0.9.1

Each software application must be carefully con gured in preparation for migration. The con guration les used at Abmas are

```
pidfile   /var/run/slapd/run/slapd.pid
argsfile  /var/run/slapd/run/slapd.args

replogfile  /data/ldap/log/slapd.replog

# Load dynamic backend modules:
modulepath  /usr/lib/openldap/modules

########################################################################
# Logging parameters
########################################################################
loglevel 256

########################################################################
# SASL and TLS options
########################################################################
```

Section

Section

```
   "(Objectclass=*)"
Enter LDAP Password:
# extended LDIF
#
# LDAPv3
# base <dc=abmas,dc=biz> with scope sub
# filter: (ObjectClass=*)
# requesting: ALL
#

# abmas.biz
dn: dc=abmas,dc=biz
objectClass: dcObject
objectClass: organization
o: abmas
dc: abmas

# People, abmas.biz
dn: ou=People,dc=abmas,dc=biz
objectClass: organizationalUnit
ou: People

# Groups, abmas.biz
dn: ou=Groups,dc=abmas,dc=biz
objectClass: organizationalUnit
ou: Groups

# Idmap, abmas.biz
dn: ou=Idmap,dc=abmas,dc=biz
objectClass: organizationalUnit
ou: Idmap
...
```

a time, starting with the people who used the least amount of resources on the network. With each group that I moved, I first logged on as a standard user in that group and took careful note of the environment, mainly the printers he or she used, the PATH, and what network resources he or she had access to (most

Section

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

Printing from legacy applications: I found out that Novell sends its jobs to the printer in a raw format. CUPS sends them in PostScript by default. I had to make a second printer de nition for one printer and tell CUPS speci cally to send raw data to the printer, then assign this printer to the LPT port with Kixtart's version of the net use command.

Example 10.3.3 Samba Configuration File | smb.conf Part A

Example 10.3.4 Samba Con guration File | smb.conf Part B

```
[netlogon]
        comment = Network logon service
        path = /data/samba/netlogon
        wril /"@1(fD)(o)-1man                A-364dBm-93(Bi-364d)-334s1"]TJ0.93 g 0.93 GET
```

Section 10.3. Implementation

Example 10.3.8 Rsync Script

```
#!/bin/bash
```

SectionS10.3. Implementatin

Example 10.3.10 Idealx smbldap-tools Control File | Part A

Example 10.3.13 Idealx smbldap-tools Control File | Part D

```
##############################################################################
#
# SAMBA Configuration
#
##############################################################################

# The UNC path to home drives location (%U username substitution)
# Ex: \\My-PDC-netbios-name\homes\%U
# Just set it to a null string if you want to use the smb.conf
# 'logon home' directive and/or disable roaming profiles
userSmbHome=""

# The UNC path to profiles locations (%U username substitution)
# Ex: \\My-PDC-netbios-name\profiles\%U
# Just set it to a null string if you want to use the smb.conf
# 'logon path' directive and/or disable roaming profiles
userProfile=""

# The default Home Drive Letter mapping
# (will be automaticallyter ma-525pcles logon if home direorllyter
# Ex:
us5(Ho5(Drile="")]TJ0-27.098Td[(#)-525(The)-525(default)-52[(us(a)-525et5(logon)-52scripu
# reonma-525pundus(a)-52DOSxs
```

Example 10.3.14 Kixtart Control File | File: logon.kix

```
; This script just calls the other scripts.

; First we want to get things done lipts.

; wetoF-tim25(we)-445inther
```

Example 10.3.16 Kixtart Control File | File: setup.kix, Part A

```
; My setup.kix is where all of the redirection stuff happens.  Note that with
; the use of registry keys, this only happens the first time they log in ,or if
; I delete the pertinent registry keys which triggers it to happen again:
```

Example 10.3.17 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")
```

Part III

Reference Section

REFERENCE SECTION

This section *Samba-3 by Example*

Chapter 11

ACTIVE DIRECTORY, KERBEROS, AND SECURITY

By this point in the book, you have been exposed to many Samba-3 features and capabilities. More importantly, if you have implemented the examples given, you are well on your way to becoming a Samba-3 networking guru who knows a lot about Microsoft Windows. If you have taken the time to practice, you likely have thought of improvements and scenarios with which you can experiment. You are rather well plugged in to the many exible ways Samba can be used.

This is a book about Samba-3. Understandably, its intent is to present it in a positive light. The casual observer might conclude that this book is one-eyed about Samba. It is | what would you expect? This chapter exposes some criticisms that have been raised concerning the use of Samba. For eab-748oM-434(c)iticisms thaer tre ugor

tone of the objections re ects as closely as possible that of the original. The case presented is a straw-man example that is designed to permit each objection to be answered as it might occur in real life.

the role of Samba at his site. Here are key extracts from this hypothetical report:

> ... the implementation of Microsoft Active Directory at the Abmas Video Rentals, Bamingsham site, has been examined. We nd no evidence to support a notion that vulnerabilities exist at your site. ... we

Section

Section 11.2. Dissection and Discussion

Section

duced in Europe and is available from the Royal Institute[4] of Technology (KTH), Sweden. It is known as the Heimdal Kerberos project. In recent times the U.S. government has removed sanctions a ecting the global distribution of MIT Kerberos. It is likely that there will be a signi cant surge forward in the development of Kerberos-enabled applications and in the general deployment and use of Kerberos across the spectrum of the information technology industry.

attempts to make a connection to the Samba server. Create/Edit/Delete Share ACLs

1. From a Windows 200x/XP Professional workstation, log on to the domain using the Domain Administrator account (on Samba domains, this is usually the account called `root`).
2. Click **Start** *!* **Settings** *!* **Control Panel** *!* **Administrative Tools** *!* **Computer Management**.
3. In the left panel, **[Right mouse menu item] Computer Management (Local)** *!* **Connect to another computer ...** *!* **Browse...** *!* **Advanced** *!* **Find Now**. In the lower panel, click on the name of the another computer

require someone who wants to get through to meet certain requirements, so it is possible to require the user (or group the user belongs to) to meet specified credential-related objectives. It can be likened to a pile-driver by overriding default controls in that having met the credential-related objectives, the user can be granted powers and privileges that would not normally be available under default settings.

It must be emphasized that the controls discussed here can act as a filter or give rights of passage that act as a superstructure over normal directory and file access controls. However, share-level ACLs act at a higher level than do share definition controls because the user must filter through the share-level controls to get to the share-definition controls. The proper hierarchy of controls implemented by Samba and Windows networking consists of:

1. Share-level ACLs
2. Share-definition controls
3. Directory and file permissions
4. Directory and file POSIX ACLs

11.3.2.1 Checkpoint Controls

Consider the following extract from a `smb.conf` file defining the share called `Apps`:

Section

Section

Section

3. Set the files and directory permissions to be read/write for

This con rms that the change of POSIX ACL permissions has been e ective.

4. It is highly recommended that you read the online manual page for the setfacl and getfacl commands. This provides information regarding how to set/read the default ACLs and how that may be propagated through the directory tree. In Windows ACLs terms, this is the equivalent of setting inheritance properties.

11.3.5 Key Points Learned

The mish-mash of issues were thrown together into one chapter

11.4 Questions and Answers

F.A.Q.

1. Q: *Does Samba-3 require the `Sign'n'seal` registry hacks needed by Samba-2?*
A: No. Samba-3 fully supports `Sign'n'seal` as well as `schannel` operation. The registry change should not be applied when Samba-3 is used as a domain controller.

2. Q:

tioned only the use of the Windows 200x/XP MMC Computer Management utility?

A: Either tool can be used with equal e ect. There is no bene t of one over the other, except that the MMC utility is present on all Windows 200x/XP systems and does not require additional

12.2 Dissection and Discussion

The key requirements in this business example are straightforward. You are not required to do anything new, just to replicate an existing system, not lose any existing features, and improve performance. The key points are:

Internet access for most employees

Distributed system to accommodate load and geographical distribution of users

Seamless and transparent interoperability with the existing Active Directory domain

12.2.1 Technical Issues

Functionally, the user's Internet Explorer requests a browsing session with the Squid proxy, for which it o ers its AD authentication token. Squid hands o the authentication request to the Samba-3 authentication helper application called ntlm_auth. This helper is a hook into winbind, the Samba-3 NTLM authentication daemon. Winbind enables UNIX services to authenticate against Microsoft Windows domains, including Active Directory domains. As Active Directory authentication is a modi ed Kerberos authentication, winbind is assisted in this by local Kerberos 5 libraries con gured to check passwords with the Active Directory server. Once the token has been checked, a browsing

seamless to the user.

Enabling this consists of:

Preparing the necessary environment using precon gured packages

Setting up raw Kerberos authentication against the Active Directory domain

Con guring, compiling, and then installing the supporting Samba-3 components

Tying it all together

12.2.2 Political Issues

the administrative guide for your Linux system to ensure that the packages are correctly updated.

Note

If the requirement is for interoperation with MS Windows Server 2003, it will be necessary to ensure that you are using MIT Kerberos version 1.3.1 or later. Red Hat Linux 9 ships with MIT Kerberos 1.2.7 and thus requires updating.

Heimdal 0.6 or later is required in the case of SUSE Linux. SUSE Enterprise Linux Server 8 ships with Heimdal 0.4. SUSE 9 ships with the necessary version.

12.3.1 Removal of Pre-Existing Con icting RPMs

If Samba and/or Squid RPMs are installed, they should be updated. You can build both from source.

12.3.2 Kerberos Con guration

The systems Kerberos installation must be con gured to communicate with your primary Active Directory server (ADS KDC).

Strictly speaking, MIT Kerberos version 1.3.4 currently gives the

to interface with Active Directory. Securing Samba-3 With ADS Support Steps

1. Download the latest stable Samba-3 for Red Hat Linux from the o cial Samba Team FTP site.[1] The o cial Samba

5. We now need to test that Samba is communicating with the Active Directory domain; most speci cally, we want to see whether winbind is enumerating users and groups. Issue the following commands:

```
root#  wbinfo -t
checking the trust secret via RPC calls succeeded
```

This tests whether we are authenticating against Active Directory:

```
root#  wbinfo -u
LONDON+Administrator
LONDON+Guest
LONDON+SUPPORT_388945a0
LONDON+krbtgt
LONDON+jht
LONDON+xjht
```

This enumerates all the users in your Active Directory tree:

```
root#  wbinfo -g
LONDON+Domain Computers
LONDON+Domain Controllers
LONDON+Schema Admins
LONDON+Enterprise Admins
LONDON+Domain Admins
LONDON+Domain Users
LONDON+Domain GuestUomadomaUt.54Policy-13.549re.54913.54OwnTd[(LONDON+Domai
```

```
root#  /usr/bin/ntlm_auth --username=jht
password: XXXXXXXX
```

```
root#  squid
```

Example 12.3.4

Chapter 13

A signi cant number of reports concern problems with the smbfs

Section

Note

The use of DNS is not an acceptable substitute for WINS. DNS does not store specific information regarding NetBIOS networking particulars that get stored in the WINS name resolution database and that Windows clients require and depend on.

Many UNIX administrators like to fully document the settings in the smb.conf file. This is a bad idea because it adds content to the file. The smb.conf file is re-read by every smbd process every time the file timestamp changes (or, on systems where this does not work, every 20 seconds or so).

As the size of the smb.conf file grows, the risk of introducing parsing errors also increases. It is recommended to keep a fully documented smb.conf file on hand, and then to operate Samba only with an optimized file.

You now, of course, press the enter key to complete the command, or else abort it by pressing Ctrl-C. The important thing to note is the noted Server role, as well as warning messages. Noted

Defective NICs, HUBs, and switches may appear as intermittent

approximately 1.5 KB/sec. The net transfer was on the order of a factor of 20-fold slower.

The symptoms that will be observed on the Samba server when a large directory is accessed will be that aggregate I/O (typically blocks read) will be relatively low, yet the wait I/O times will be

Section 13.4. Key Points Learned

Chapter 14

SAMBA SUPPORT

One of the most di cult to answer questions in the information technology industry is, \What is support?". That question irritates some folks, as much as common answers may annoy others.

The most aggravating situation pertaining to support is typi-

Chapter 15

A COLLECTION OF USEFUL TIDBITS

Information presented here is considered to be either basic or well-known material that is informative yet helpful. Over the years, I have observed an interesting behavior. There is an expectation that the process for joining a Windows client to a Samba-controlled Windows domain may somehow involve steps different from doing so with Windows NT4 or a Windows ADS domain. Be assured that the steps are identical, as shown in the example given below.

Figure 15.2 The Computer Name Panel.

Figure 15.5 Computer Name Changes | User name and Password Panel

Section

15.3 Starting Samba

Samba essentially consists of two or three daemons. A daemon is a UNIX application that runs in the background and provides services. An example of a service is the Apache Web server for which the daemon is called **httpd**. In the case of Samba, there are three daemons, two of which are needed as a minimum.

The Samba server is made up of the following daemons:

nmbd This daemon handles all name registration and resolution requests. It is the primary vehicle involved in network browsing. It handles all UDP-based protocols. The **nmbd** daemon should be the first command started as part of the

of control script should be owned by user root and group root, and set so that only root can execute it.

A sample startup script for a Red Hat Linux system is shown in Example 15.3.2. This le could be located in the directory /etc/rc.d and can be called samba. A similar startup script is required to control winbind. If you want to nd more information regarding startup scripts please refer to the packaging section of

from the source shown. Because of its size, this file is located at the end of this chapter.

two files are parts A and B, respectively, of the `init-ldif.pat` file.

4. Change to the `/etc/openldap/SambaInit` directory. Execute the following:

```
root#  sh SMBLDAP-ldif-preconfig.sh

How do you wish to refer to your organization?
Suggestions:
        Black Tire Company, Inc.
        Cat With Hat Ltd.
How would you like your organization name to appear?
Your organization name is: My Organization
Enter a new name is this is not what you want, press Enter to Continue.
Name [My Organization]: Abmas Inc.

Samba Config File Location [/etc/samba/smb.conf]:
Enter a new full path or press Enter to continue.
Samba Config File Location [/etc/samba/smb.conf]:
Domain Name: MEGANET2
Domain SID: S-1-5-21-3504140859-1010554828-2431957765

The name of your Internet domain is now needed in a special format
as follows, if your domain name is mydomain.org, what we need is
the information in the form of:
        Domain ID: mydomain
        Top level: org
If your fully qualified hostname is: snoopy.bazaar.garagesale.net
where "snoopy" is the name of the machine,
```

```
dn: cn=domusers,ou=Groups,dc=abmas,dc=biz
objectClass: posixGroup
objectClass: sambaGroupMapping
gidNumber: 513
cn: domusers
sambaSID: S-1-5-21-3504140859-1010554828-2431957765-513
sambaGroupType: 2
displayName: Domain Users
description: Domain Users
structuralObjectClass: posixGroup
entryUUID: af7e98ba-c4a1-1027-900b-9421e01bf474
creatorsName: cn=manager,dc=abmas,dc=biz
modifiersName: cn=manager,dc=abmas,dc=biz
createTimestamp: 20031217055747Z
modifyTimestamp: 20031217055747Z
entryCSN: 2003121705:57:47Z#0x000a#0#0000
```

6. Your LDAP database is:

Section

Figure 15.7 The LDAP Account Manager Con guration Screen

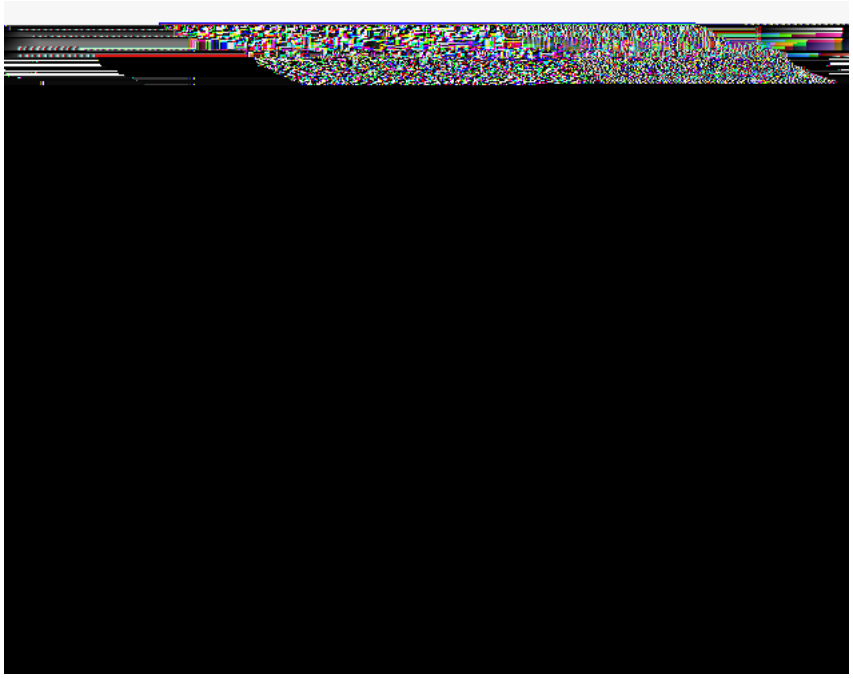
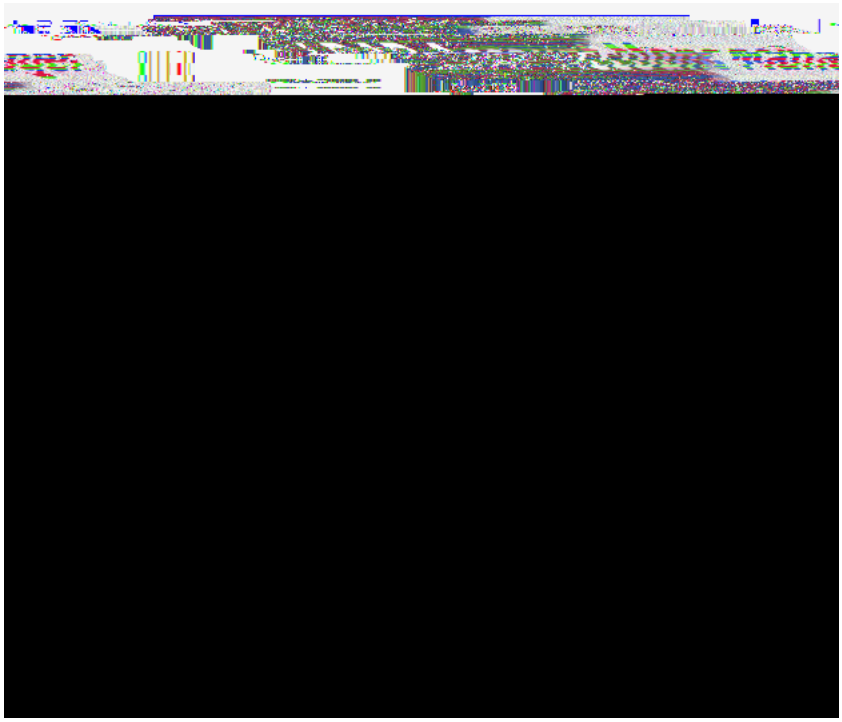
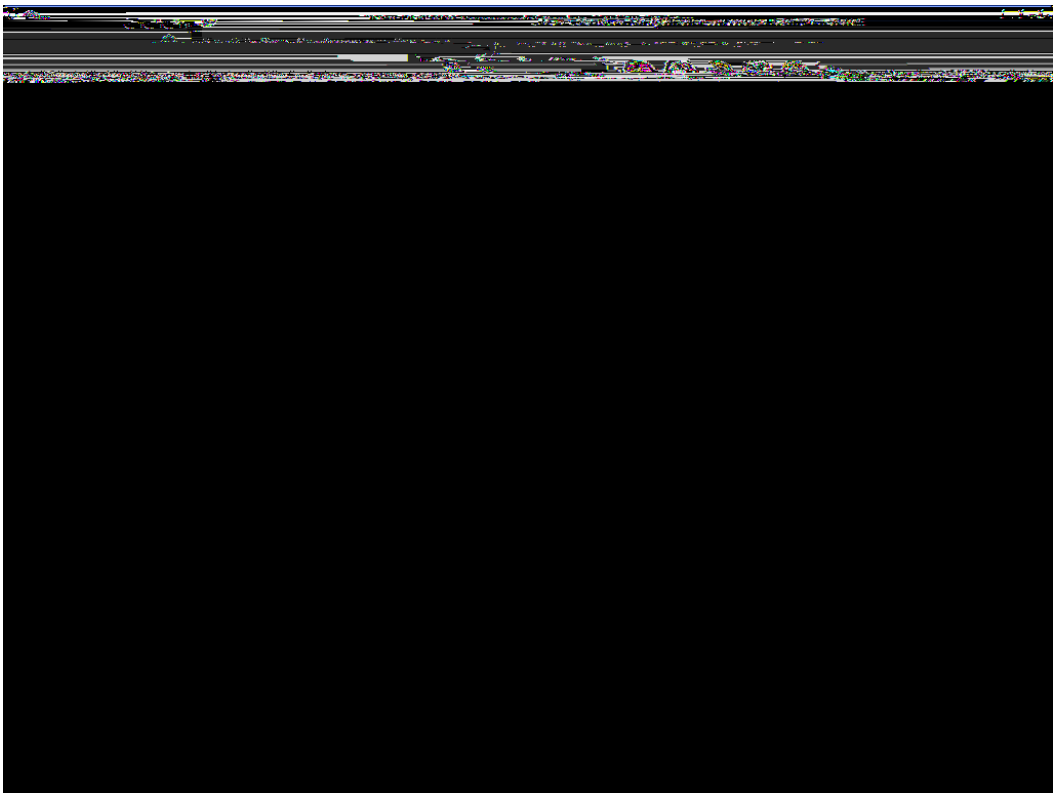


Figure 15.9 The LDAP Account Manager Group Edit Screen



Section 15.8. E ect of Setting File and Directory SUID/SGID Permissions Explained

Figure 15.12 The IMC Samba User Account Screen



```
root#  chmod ug+s file-or-directory
```

Let's consider the example of a directory `/data/accounts`. The

Section

Disabling of Oplocks usage may require server and client changes.

Section 15.9. Shared Data Integrity

Example 15.4.1 DNS Localhost Forward Zone File: /var/lib/named/localhost.zone

```
$TTL 1W
@     IN SOA   @   root (
            42    ; serial
            2D    ; refresh
            4H    ; retry
            6W    ; expiry
            1W )     ; minimum

      IN NS    @
      IN A     127.0.0.1
```

Example 15.4.2 DNS Localhost Reverse Zone File: /var/lib/named/127.0.0.zone

```
$TTL 1W
549Td[(42)-2100(;)-6550lSQ0Thost.zTJETq25(()]TJ..zTJETq258.726-13.549Td[(42)-215(;)-525(s
```

Example 15.5.1 LDAP Pre-configuration Script: SMBLDAP-ldif-preconfig.sh | Part A

Example 15.5.3 525LDAP Pre-configuration Script: SMBLDAP-ldif-

Chapter 16

NETWORKING PRIMER

You are about to use the equivalent of a microscope to look at the information that runs through the veins of a Windows network. We do more to observe the information than to interrogate it.

Section

of the Windows workstations. It is helpful for this machine to be passive (does not send broadcast information) to the network.

For these exercises, our test environment consisted of a SUSE 9.2 Professional Linux Workstation running VMWare 4.5. The following VMWare images were prepared:

Windows 98 | name: MILGATE98

Windows Me | name: WINEPRESSME

Windows XP Professional | name: LightrayXP

Samba-3.0.20 running on a SUSE Enterprise Linux 9

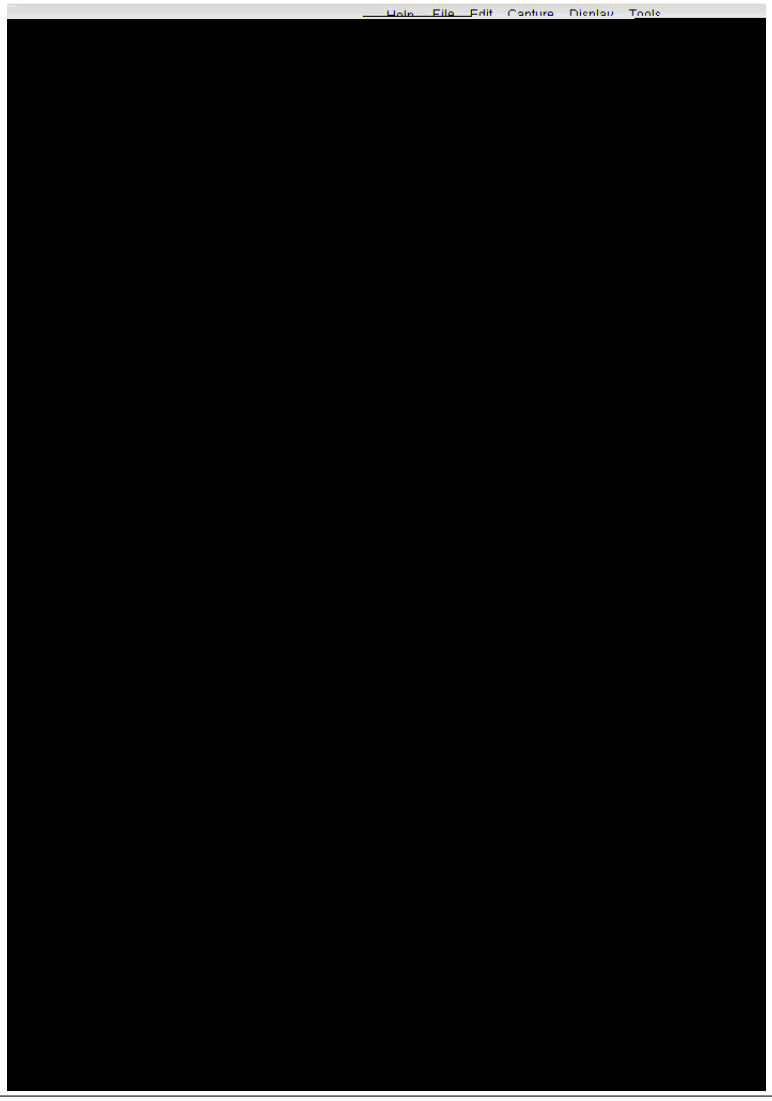
(d) Enable network name resolution

(e) Enable transport name resolution

Click **OK**.

2. Start the Windows 9x/Me machine to be monitored. Let

Figure 16.1 Windows Me | Broadcasts | The First 10 Minutes



The Common Internet File System," by Christopher Hertel, (Prentice Hall PTR, ISBN: 013047116X).

Table 16.1 Windows Me | Startup Broadcast Capture Statistics

3. At the conclusion of the capture time, stop the capture. Be sure to save the captured data so you can examine the network data capture again at a later date should that be necessary.

4. Analyze the capture trace, taking note of the transport protocols used, the types of messages observed, and what interaction took place between the two machines. Leave both machines running for the next task.

16.3.2.1 Findings

Table 16.2 summarizes capture statistics observed. As in the previous case, all announcements used UDP/IP broadcasts. Also, as was observed with the last example, the second Windhinews4(seco9x/MJ 0 -13.549 Tc

Table 16.2 Second Machine (Windows 98) | Capture Statistics

Message	Type

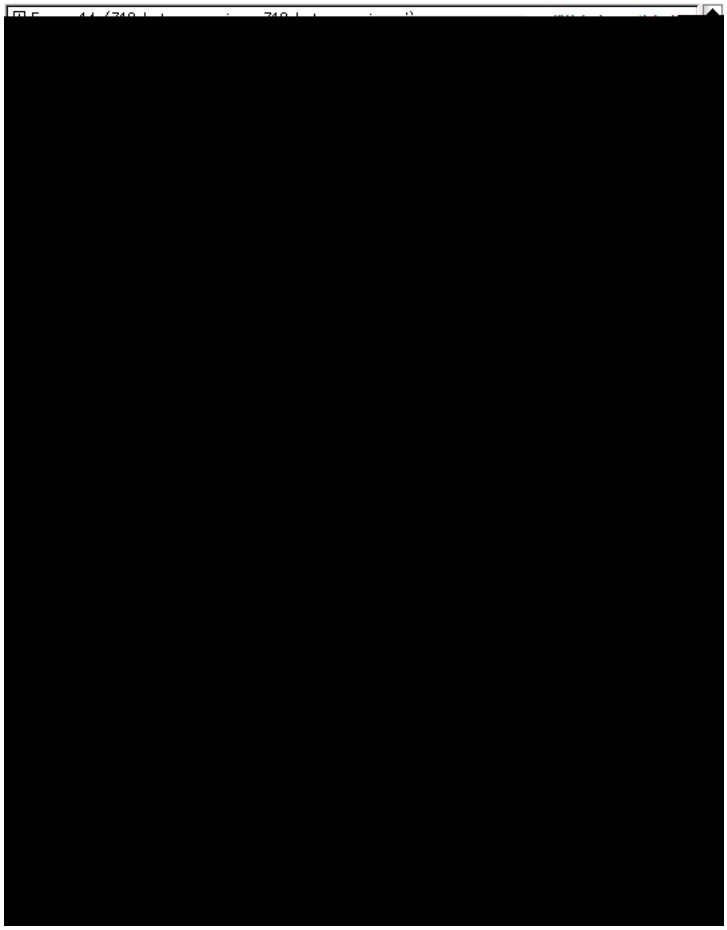
Figure 16.5 Typical Windows 9x/Me User SessionSetUp AndX Request

16.3.4 Windows 200x/XP Client Interaction with Samba-3

By now you may be asking, \Why did you choose to work with Windows 9x/Me?"

First, we want to demonstrate the simple case. This book is not intended to be a detailed treatise on the Windows networking protocols, but rather to provide prescriptive guidance for

Figure 16.6 Typical Windows XP NULL Session Setup AndX Request



16.3.4.1 Discussion

Figure 16.7 Typical Windows XP User Session Setup AndX Request

nouncements and workgroup announcements.

All Samba servers must be con gured with a mechanism for mapping the

Appendix A

GNU GENERAL PUBLIC LICENSE VERSION 3

Version 3, 29 June 2007

(and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

we wish to avoid the special danger that patents applied to a

user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays \Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The \source code" for a work means the preferred form of the work for making modi cations to it. \Object code" means any non-source form of a work.

A \Standard Interface" means an interface that either is an of- cial standard de ned by a recognized standards body, or, in the case of interfaces speci ed for a particular programming language, one that is widely used among developers working in that language.

5. Conveying Modi ed Source Versions.

You may convey a work based on the Program, or the modi cations to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a The work must carry prominent notices stating that you mod-

obligated to ensure that it is available for as long as needed to satisfy these requirements.

e Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being o ered to the general public at no charge under subsection 6d.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this

A contributor's \essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired

reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

If the program does terminal interaction, make it output a short

GLOSSARY

Domain Master Browser (DMB)

The Domain Master Browser maintains a list of all the

own directory database. LDAP is not a database per se; rather it is a technology that enables high-volume search and locate activity from clients that wish to obtain sim-

SUBJECT INDEX

migrates47ATJ0 gg333(O ce,)]TJ0 g 0 Gt2g0 g 0 G 0

,