Samba-3 by Example

Practical Exercises in Successful Samba Deployment

John H. Terpstra

April 19, 2007

ABOUT THE COVER ARTWORK

ACKNOWLEDGMENTS

x

5.6.1 Configuring Directory Share Point Roots 203
5.6.2 Configuring Profile Directories 204
5.6.3 Preparation of Logon Scripts 205
5.6.4 Assigning User Rights and Privileges 206
5.7 Windows Client Configuration 208
5.7.1 Configuration of Default Profile with Folder Redirection 209
5.7.2 Configuration of MS Outlook to Relocate PST File 210
5.7.3 Configure Delete Cached Profiles on Logout 214
5.7.4 Uploading Printer Drivers to Samba Servers 214
5.7.5 Software Installation 216
5.7.6 Roll-out Image Creation 217
5.8 Key Points Learned 217
5.9 Questions and Ansarr TJET1001493.9925608.3994cm0g0G100G1001-493.9925-498.1794c

7.2.2 Political Issues 272
7.3

8.3.1.3 Updating from Samba Versions after 3.0.6 to a Current Release 342

LIST OF EXAMPLES

Chapter 1

1.2.1

3.3.12 DNS Abmas.biz Forward Zone File 102
3.3.13 DNS Abmas.us Forward Zone File 103

Chapter 4

4.3.1 Server: MASSIVE (PDC), File: /etc/samba/smb.conf 121
4.3.2 Server: MASSIVE (PDC), File: /etc/samba/dc-common.conf 122

5.5.4 LDAP Based smb.conf File, Shares Section — Part B 232
5.5.5 LDIF IDMAP Add-On Load File — File: /etc/openldap/idmap.LDIF 232

12.3.4 Squid Configuration File Extract — /etc/squid.conf [ADMINISTRATIVE PARAMETERS Section] 469
12.3.5

6.7 Network Topology — 2000 User Complex Design B

FOREWORD

By John M. Weathersby, Executive Director, OSSI

The Open Source Software Institute (OSSI) is comprised of representatives from a broad spectrum of business and non-business organizations that share a common interest in the promotion of development and implementation of open source software solutions globally, and in particular within the United States of America.

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 definitive standard for providing interoperability with UNIX systems and other non-Microsoft operating system platforms. Both open source applications have

Foreword

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

Why Is This Book Necessary?

This book is the result of observations and feedback. The feedback from the Samba-HOWTO-Collection has been positive and complimentary. There have been requests for far more worked examples, a "Samba Cookbook,"

demands. This configuration uses Share Mode security and also

xl

Chapter 1

NO-FRILLS SAMBA SERVERS

Section 1.2. Assignment Tasks

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.

5. Use SUSE Linux system tools (refer to the SUSE Administrators Guide for correct procedures) to format the partition with a suitable file system. The reiserfs file system is suitable. Configure this drive to automount using the `/data` directory as the mount point. It must be mounted before proceeding.

6. Under the directory called `/data`, create two directories named `ftmfiles` and `officefiles`, and set ownership and permissions:

```
root#  mkdir -p /data/{ftmfiles,officefiles/{letters,invitations,misc}}
root#  chown -R abmas:office /data
root#  chmod -R ug+rwxs,o-w,o+rx /data
```

These demonstrate compound operations. The mkdir command creates in one step these directories:

```
/data/fmtfiles
/data/officefiles
/data/officefiles/letters
/data/officefiles/invitations
/data/officefiles/misc
```

The chown

```
application/octet-stream
```

13. Use the standard system tool to start Samba and CUPS to configure

Section 1.2. Assignment Tasks

Example 1.2.4

(d) You may be prompted for the name of a file to print to. If so, close the dialog panel. Right-click **HP LaserJet 5/5M Postscript → Properties → Details (Tab) → Add Port**.

(e) In the Network panel, enter the name of the print queue on the Samba server as follows: `\\SERVER\hplj5`. Click **OK**+**OK** to complete the installation.

(f) It is a good idea to test the functionality of the complete instal-

change anything on the workstations. Mr. Meany gave instructions to replace the server, "but leave everything else alone to avoid staff unrest."

You have tried to educate Mr. Meany and found that he has no desire to understand networking. He believes that Windows for Workgroups 3.11 was "the best server Microsoft ever sold" and that Windows NT and 2000 are "too fang-dangled complex!"

1.2.3.1 Dissection and Discussion

The requirements of this network installation are not unusual. The staff are

Figure 1.2 Accounting O□ce Network Topology

The data storage structure is now prepared for use.

Chapter 2

SMALL OFFICE NETWORKING

Chapter 1, “No-Frills Samba Servers”

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 so that sta can easily obtain software updates. Mr. Meany is warming up to the installation of antivirus software but is not yet ready to approve this expense. He told you to spend the money a virus scanner costs on better quality notebook computers for mobile users.

One of Mr. Meany's golfing partners convinced him to buy new laser printers, one black only, the other a color laser printer. Sta support the need for a color printer so they can present more attractive proposals and reports.

Mr. Meany also asked if it would be possible for one of the sta to manage user accounts from the Windows desktop. That person will be responsible

```
####
# 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
####
```

9. Create and map Windows Domain Groups to UNIX groups. A sample script is provided in 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:

(c) In the **Available ports:** panel, select `FILE:`. Accept the default printer name by clicking **Next**. When asked, "Would you like to print a test page?", click **No**. Click **Finish**.

to check the man page for this command for detailed instructions regarding the steps involved.

10. Q: *How can I manage user accounts from my Windows XP Professional workstation?*
A: Samba-3 implements a Windows NT4-style security domain architecture. This type of Domain cannot B8dnnouso(Thisot)28(olTd[(Thiprestail)em)-1(p)-28(e1(ai)1(a(ai)1(

Section

Example 2.3.4

Section 3.1. Introduction

networks. When the number of users on the network begins to approach the limit of usable addresses, it is a good idea to switch to a network address specified 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` for the backend may result in performance problems. The `tdbsam` passdb backend offers features that are not available with the older, flat ASCII-based `smbpasswd` database.

The proposed network design uses a single server to act as an Internet services host for electronic mail, Web serving, remote administrative access via

Section

An alternate m2685s5hod to verify the hos685s5nam685se is685s:

Section 3.3. Implementation

4. Create the username map file to permit the `root` account to be called `Administrator`

3.3.3 Configuration of DHCP and DNS Servers

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

Section

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

You may now remove the entry called

running:

```
root#  ps ax | grep dhcp
 2618 ?        S      0:00 /usr/sbin/dhcpd ...
 8180 pts/2    S      0:00 grep dhcp
```

This shows that the server is running. The proof of whether or not

Section

```
  zakadmin.exe                   161424  Thu Nov 27 15:06:52 2003
  zak.exe                       6066384  Thu Nov 27 15:06:52 2003
  dhcpd.conf                       1256  Thu Nov 27 15:06:52 2003
  smb.conf                         2131  Thu Nov 27 15:06:52 2003
  initGrps.sh                A     1089  Thu Nov 27 15:06:52 2003
  POLICY.EXE                       86542  Thu Nov 27 15:06:52 2003

                55974 blocks of size 65536. 33968 blocks available
smb: \> q
```

11. Your new server is connected to an Internet-accessible connection. Before you start your firewall, you should run a port scanner against your system. You should repeat that after the firewall has been started.

Section

Section

at which most networks tend to want backup domain controllers (BDCs). Samba-3 does not provide a mechanism for replicating tdbsam data so it can be used by a BDC. The limitation of 250 users per tdbsam is predicated only on the need for replication, not on the limits[6]

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 qualified 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 specific name type is registered[7] for each type of service that is provided by the Windows server or client and that may be registered where a WINS server is in use.

Example 3.3.2

Section 3.4. Questions and Answers

Example 3.3.8 DNS Master Configuration File — /etc/named.conf Forward Lookup Definition Section

```
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 {
      any;
   };
   allow-transfer {
      seconddns;
   };
};
```

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.
```

Chapter 4

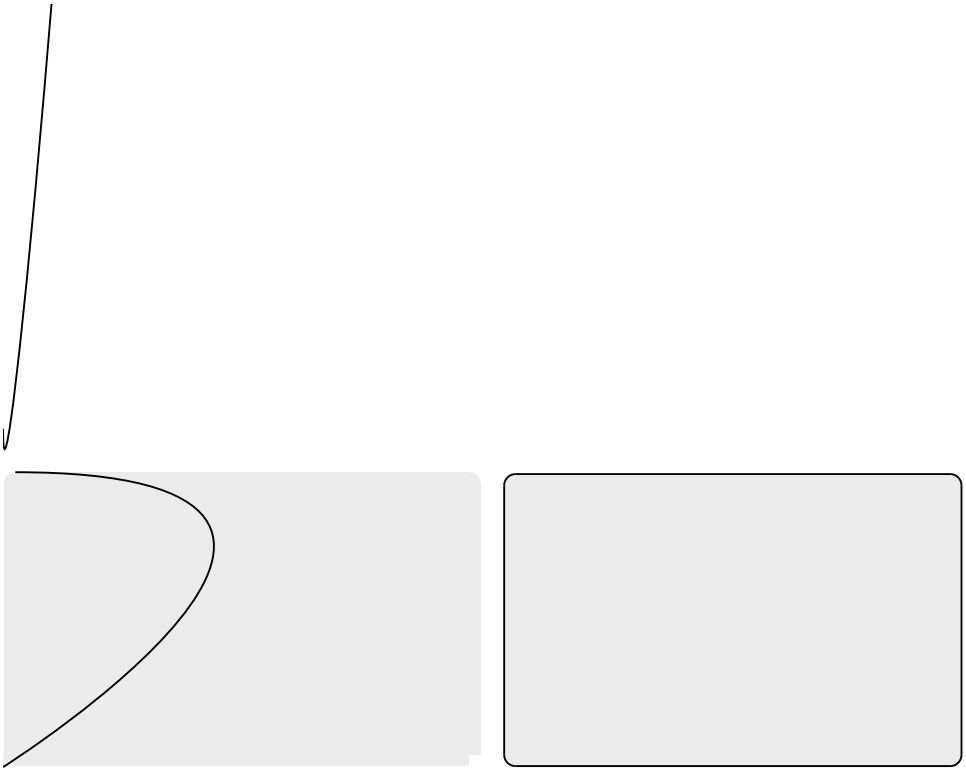
new network so that it is ready for operation when the old office moves into the new premises.

4.1.1 Assignment Tasks

The acquired business had 280 network users. The old Abmas building housed 220 network users in unbelievably cramped conditions. The network

- Because of the refusal to use an LDAP (ldapsam) passdb backend at this time, the only choice that makes sense with 500 users is to use

Figure 4.1 Network Topology — 500 User Network Using tdbsam passdb backend.



```
root#  smbpasswd -a root
New SMB password: XXXXXXXX
Retype new SMB password: XXXXXXXX
root#
```

The root account is the UNIX equivalent of the Windows domain administrator. This account is essential in the regular maintenance of your Samba server. It must never be deleted. If for any reason the account is deleted, you may not be able to recreate this account

as *insurance* against lost time. Edit file /etc/cups/mime.convs to uncomment the line:

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

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

Section 4.3. Implementation

13. Your server is ready for validation testing. Do not proceed with the steps in Section 4.3.3.2

5. Your server is ready for validation testing. Do not proceed with the steps in Section 4.3.3.2

Example 4.3.4 Server: BLDG1 (Member), File: smb.conf

each of the following in the sequence shown:

A: Replication of the *tdbsam*

Example 4.3.7 Server: MASSIVE, 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 172.16.1.0 netmask 255.255.252.0 {
        range dynamic-bootp 172.16.1.0 172.16.2.255;
        option subnet-mask 255.255.252.0;
        option routers 172.16.0.1, 172.16.0.128;
        allow unknown-clients;
   }
subnet 172.16.4.0 netmask 255.255.252.0 {
        range dynamic-bootp 172.16.7.0 172.16.7.254;
        option subnet-mask 255.255.252.0;
        option routers 172.16.4.128;
        allow unknown-clients;
   }
subnet 172.16.8.0 netmask 255.255.252.0 {
        range dynamic-bootp 172.16.11.0 172.16.11.254;
        option subnet-mask 255.255.252.0;
        option routers 172.16.4.128;
        allow unknown-clients;
   }
subnet 127.0.0.0 netmask 255.0.0.0 {
        }
subnet 123.45.67.64 netmask 255.255.255.252 {
        }
```

Example 4.3.8 Server: BLDG1, File: dhcpd.conf

Example 4.3.13 Forward Zone File: abmas.biz.hosts

```
$ORIGIN .
$TTL 38400  ; 10 hours 40 minutes
abmas.biz   IN SOA   massive.abmas.biz. root.abmas.biz. (
            2003021833 ; serial
            10800      ; refresh (3 hours)
            3600       ; retry (1 hour)
            604800     ; expire (1 week)
            38400      ; minimum (10 hours 40 minutes)
            )
         NS massive.abmas.biz.
         NS bldg1.abmas.biz.
         NS bldg2.abmas.biz.
         MX 10 massive.abmas.biz.
$ORIGIN abmas.biz.
massive        A  172.16.0.1
router0                 A       172.16.0.128
bldg1                   A       172.16.4.1
router4                 A       172.16.4.128
bldg2                   A       172.16.8.1
router8                 A       172.16.8.128
```

Example 4.3.14 Forwample 4

Caution

A significant number of network administrators have responded to the guidance given here. It should be noted that there are sites that have a single PDC for many hundreds of concurrent network clients. Network band-

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:

-

5.1 Regarding LDAP Directories and Windows Computer Accounts

Good morning,

> A few months ago we sat down to design the network. We discussed the challenges ahead and we all agreed to compromise our design to keep it simple. We knew there would be problems, but anticipated that we would have some time to resolve any issues

-

well as for Samba. From the OpenLDAP perspectdame, UNIX system accounts are stored POam schamma extensions. Samba pro:p8(vidam)es its own schema to permit storage of accoun:p8(t)-443(attrib)1(utes)-444(S)1(am)27(b)1(a)-444(nam)eeds. Samba-3 can use LDAP back:p8(e)-1(n)1(d)-333(to)-333(s)-1(toram)e:

•

Note

The following information applies to Samba-3.0.20 when used with the Idealx smbldap-tools scripts version 0.9.1. If using a di□erent version of Samba or of the smbldap-tools tarball, please verify that the versions you are about to use are matching. The smbldap-tools package uses counter-entries in the LDAP directory to avoid duplication of the UIDs and GIDs that are issued for POSIX accounts. The LDAP rdn under which this information is stored are called uidNumCwfienoudstoreDsou97.3626TJ/F61.Td[.3537514.47(d

Example 5.4.1 LDAP DB

Section

```
smbldap-tools configuration file Location (global parameters)
```

The following steps initialize the LDAP database, and then you can add user and group accounts that Samba can use. You use the **smbldap-populate** to seed the LDAP database. You then manually add the accounts shown in Table 5.3. The list of users does not cover all 500

Table 5.3 Abmas Network Users and Groups

Account Name

```
adding new entry: sambaDomainName=MEGANET2,dc=abmas,dc=biz
adding new entry: uid=root,ou=People,dc=abmas,dc=biz
adding new entry: uid=nobody,ou=People,dc=abmas,dc=biz
adding new entry: cn=Domain Admins,ou=Groups,dc=abmas,dc=biz
adding new entry: cn=Domain Users,ou=Groups,dc=abmas,dc=biz
adding new entry: cn=Domain Guests,ou=Groups,dc=abmas,dc=biz
adding new entry: cn=Domain Computers,ou=Groups,dc=abmas,dc=biz
adding new entry: cn=Administrators,ou=Groups,dc=abmas,dc=biz
adding new entry: cn=Print Operators,ou=Groups,dc=abmas,dc=biz
adding new entry: cn=Backup Operators,ou=Groups,dc=abmas,dc=biz
adding new entry: cn=Replicators,ou=Groups,dc=abmas,dc=biz
```

```
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 runx.-1200.7921469.0078cm050.79
modifyTimestamp:modifyTimestamp:
modifyTimestamp:
s,ZZ

following:

```
root#  ./smbldap-useradd -m -a username
root#  ./smbldap-passwd username
Changing password for username
New password : XXXXXXXX
Retype new password : XXXXXXXX

root#  smbpasswd username
New SMB password: XXXXXXXX
Retype new SMB password: XXXXXXXX
```

where username

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

Section

```
root#  rcwinbind restart
```

23.

```
.urlview              H      311  Fri Jul  7 06:55:35 2000
```

```
BUILTIN\Account Operators
No privileges assigned

BUILTIN\Backup Operators
No privileges assigned

BUILTIN\Server Operators
No privileges assigned

BUILTIN\Administrators
No privileges assigned

Everyone
No privileges assigned

MEGANET2\Domain Admins
SeMachineAccountPrivilege
SePrintOperatorPrivilege
SeAddUsersPrivilege
SeRemoteShutdownPrivilege
SeDiskOperatorPrivilege
```

5.7 Windows Client Configuration

In the next few sections, you can configure a new Windows XP Profes-

Section 5.7. Windows Client Configuration

machines. Notebook computers (mobile users) need to be accommodated using local profiles. This is not an uncommon assumption.

5. Click back to the root of the loaded hive `Default`. Click **File** → **Unload Hive...** → **Yes**.
6. Click **File** →

Section 5.7. Windows Client Configuration

printer drivers; there is also a check-box in this tab called “List in the directory”. When this box is checked, the printer will be published in Active Directory (Applicable to Active Directory use only.)

8. Click **OK**. It will take a minute or so to upload the settings to the server. You are now returned to the **Printers and Faxes on Massive**

Section 5.8. Key Points Learned

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 be familiar with. Over the years many people have approached me

that are not used. Is that a good thing?

A: I took this up with Idealx and found them most willing to change

9. Q:

Example 5.4.5 Configuration File for NSS LDAP Clients Support — /etc/ldap.conf

```
host 172.16.0.1

base dc=abmas,dc=biz

binddn cn=Manager,dc=abmas,dc=biz
bindpw not24get

timelimit 50
bind_timelimit 50
bind_policy hard

idle_timelimit 3600

pam_password exop

nss_base_passwd ou=People,dc=abmas,dc=biz?one
nss_base_shadow ou=People,dc=abmas,dc=biz?one
nss_base_group  ou=Groups,dc=abmas,dc=biz?one

ssl off
```

Example 5.5.3 LDAP Based smb.conf File, Shares Section — Part A

Chapter 6

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

Section

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

The provision of sufficient servers that are BDCs is an important design factor. The second important design factor involves how each of the

Figure 6.1

Section 6.4. Questions and Answers

A:

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

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

```
[apps]
        comment = Application Files
```

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

```
# \# Global parameters
 [global]
        unix charset = LOCALE
        workgroup = MEGANET2
        netbios name = BLDG1
        passdb backend = ldapsam:ldap://lapdc.abmas.biz
        username map = /etc/samba/smbusers
        log level = 1
        syslog = 0
```

Example 6.3.7 Backup Domain Controller smb.conf File — Part B

Figure 6.6 Network Topology — 2000 User Complex Design A

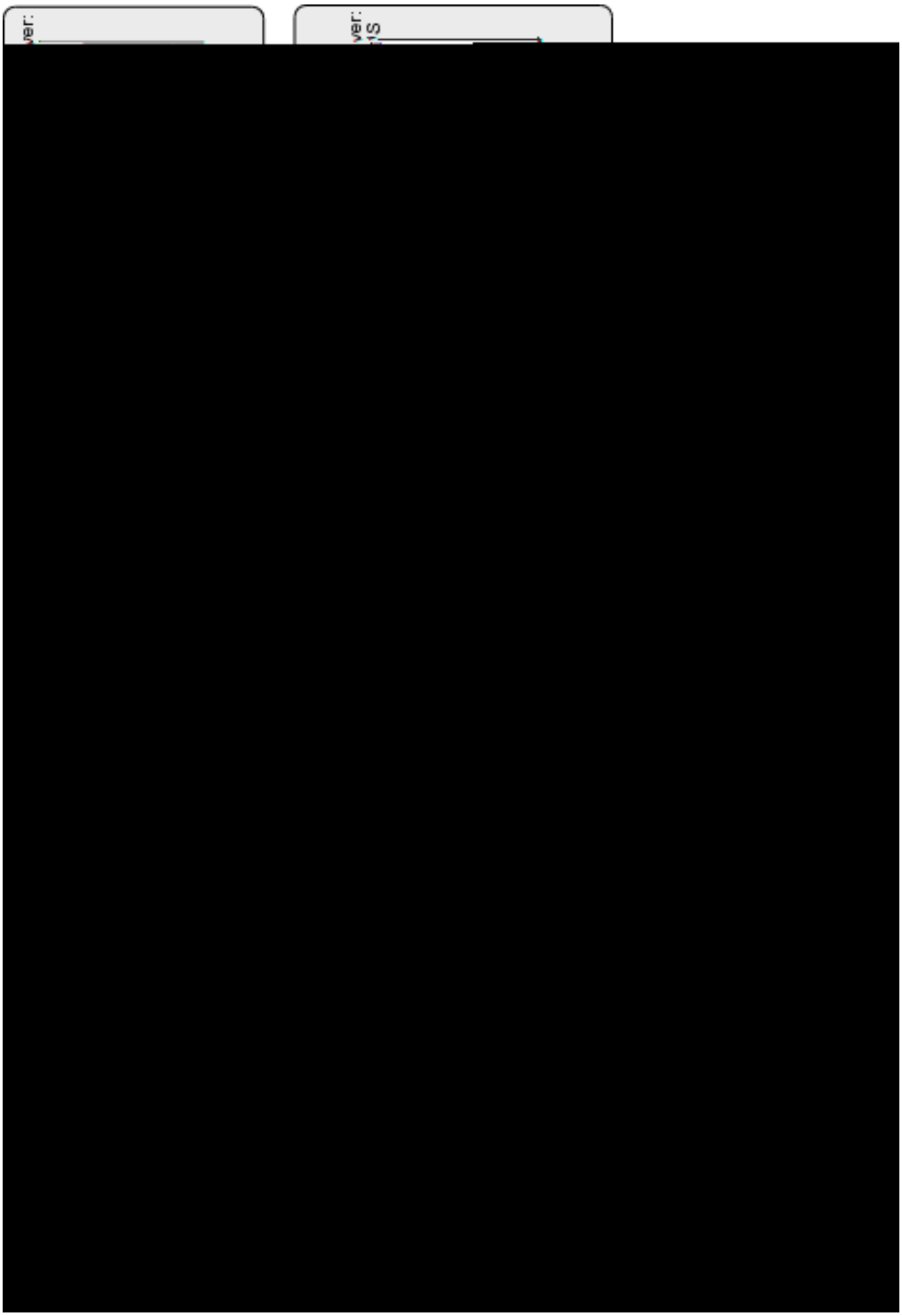
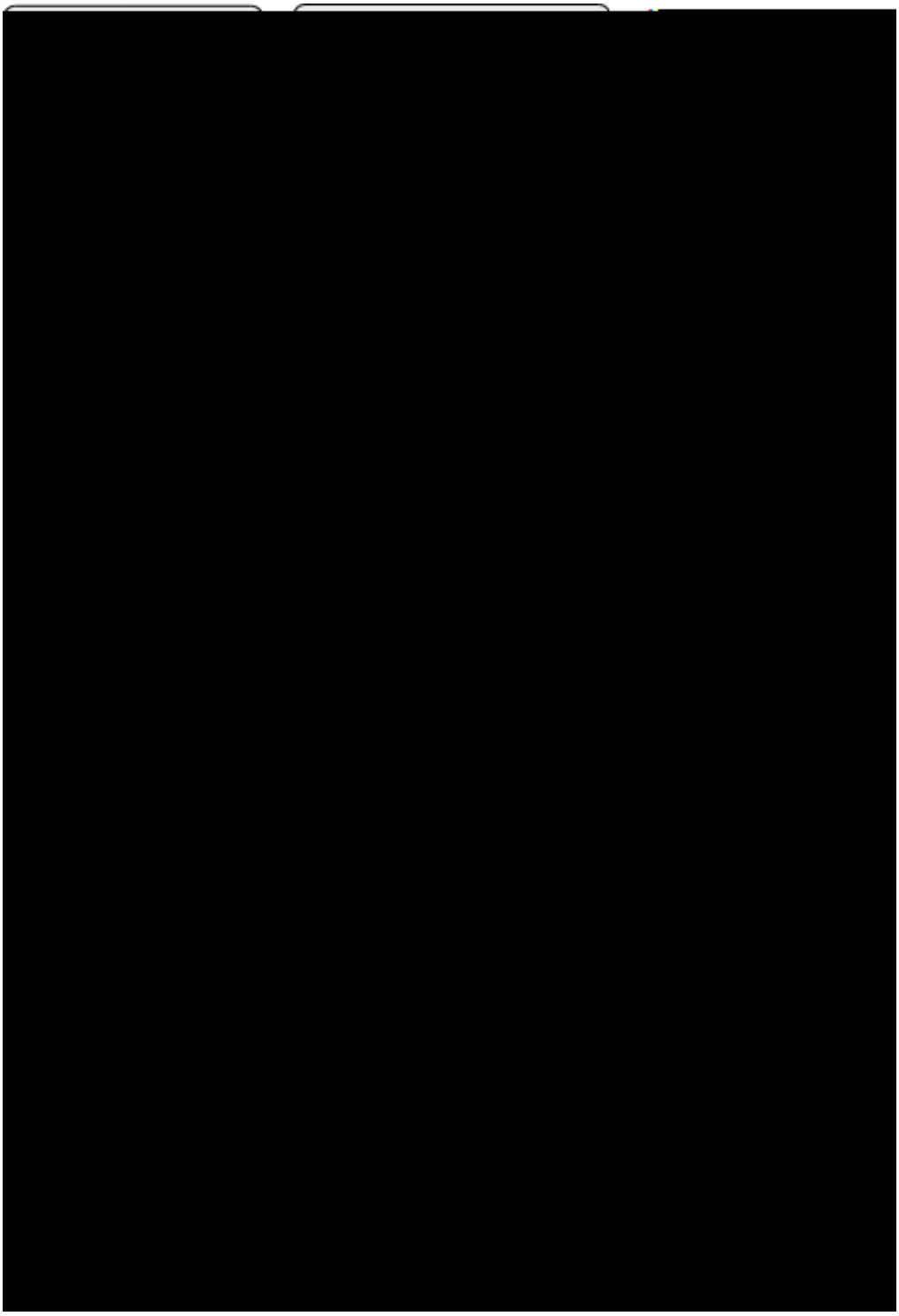


Figure 6.7 Network Topology — 2000 User Complex Design B



Part II

Domain Members, Updating Samba and Migration

Chapter 7

ADDING DOMAIN MEMBER SERVERS AND

Section

on servers. A workstation is frequently viewed as a disposable (easy to replace) item, but a server is viewed as a core component of the business.

We can look at this another way. If a workstation breaks down, one user is a□ected, but if a server breaks down, hundreds of users may not be able to work. The services that a workstation must provide are document- and file-production oriented; a server provides information storage and is distribution oriented.

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

If your installation is accessed only from clients that are members of

Section

Section

quired.

Note

abmas.biz and the name of the server is W2K3S. In ADS realm terms, the domain controller is known as w2k3s.london.abmas.biz. In NetBIOS nomenclature, the domain name is LONDON and

Section 7.3. Implementation

```
   HAVE_LIBKRB5
```

You can validate that Samba has been compiled and linked with LDAP support by executing:

```
root#  smbd -b | grep LDAP
massive:/usr/sbin # smbd -b | grep LDAP
   HAVE_LDAP_H
   HAVE_LDAP
   HAVE_LDAP_DOMAIN2HOSTLIST
   HAVE_LDAP_INIT
   HAVE_LDAP_INITIALIZE
   HAVE_LDAP_SET_REBIND_PROC
   HAVE_LIBLDAP
   LDAP_SET_REBIND_PROC_ARGS
```

This does look promising; smbd

Hat Linux RPMs may be obtained from the Samba FTP sites. SUSE Linux RPMs may be obtained from Sernet[2]

```
Using short domain name -- LONDON
Joined 'FRAN' to realm 'LONDON.ABMAS.BIZ'
```

You have successfully made your Samba-3 server a member

```
LONDON+Enterprise Admins
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 accounts are being resolved. Now you try group resolution:

```
root#  getent group
...
LONDON+Domain Computers:x:10002:
LONDON+Domain Controllers:x:10003:
LONDON+Schema Admins:x:10004:LONDON+Administrator
LONDON+Enterprise Admins:x:10005:LONDON+Administrator
LONDON+Domain Admins:x:10006:LONDON+jht,LONDON+Administrator
LONDON+Domain Users:x:10000:
LONDON+Domain Guests:x:10001:
LONDON+Group Policy Creator Owners:x:10007:LONDON+Administrator
```

Section 7.3. Implementation

```
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"
}
```

Section

Section

free download[4]

Section

Section 7.4. Questions and Answers

Example 7.3.5 Samba Domain Member Server Using Winbind smb.conf File for NT4 Domain

```
# Global parameters
 [global]
        unix charset = LOCALE
        workgroup = MEGANET2
        security = DOMAIN
        username map = /etc/samba/smbusers
        log level = 1
```

Example 7.3.6 Samba Domain Member Server Using Local Accounts smb.conf File for NT4 Domain

```
# Global parameters
 [global]
        unix charset = LOCALE
        workgroup = MEGANET3
```

Example 7.3.7 Samba Domain Member smb.conf File for Active Directory

Example 7.3.12 SUSE: PAM xdm Module Using Winbind

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

#%PAM-1.0
auth     sufficient     pam_unix2.so     nullok
auth     sufficient     pam_winbind.so   use_first_pass use_authtok
account  sufficient     pam_unix2.so
account  sufficient     pam_winbind.so   use_first_pass use_authtok
password sufficient     pam_unix2.so
password sufficient     pam_winbind.so   use_first_pass use_authtok
session  sufficient     pam_unix2.so
session  sufficient     pam_winbind.so   use_first_pass use_authtok
session  required       pam_dev perm.so
session  required       pam_resmgr.so
```

Example 7.3.13 Red Hat 9: PAM System Authentication File: /etc/pam.d/system-auth Module Using Winbind

```
#%PAM-1.0
auth        required      /lib/security/$ISA/pam_env.so
auth        sufficient    /lib/security/$ISA/pam_unix.so likeauth nullok
auth        sufficient    /lib/security/$ISA/pam_winbind.so use_first_pass
auth        required      /lib/security/$ISA/pam_deny.so

account     required      /lib/security/$ISA/pam_unix.so
account     sufficient    /lib/security/$ISA/pam_winbind.so use_first_pass

password    required      /lib/security/$ISA/pam_cracklib.so retry=3 type=
```

Chapter 8

In the course of the Samba 2.0.x series the **smbpasswd** was modified to permit the domain SID to be captured to the `secrets.tdb` file by executing:

Section 8.1. Introduction

Section

The recommended passdb backends at this time are

to much lost time as the uninformed administrator deals with apparent failure of the update to take e□ect.

The best advice for those lacking in code compilation experience is to use only vendor (or Samba-Team) provided binary packages. The Samba packages that are provided by the Samba-Team are generally built to use file paths that are compatible with the original OS vendor's practices.

If you are not sure whether a binary package complies with the

5. When migrating machines, always test first (using ADMT's test mode) and satisfy all errors before committing the migration. Note that the test will always fail, because the machine will not have been actually migrated. You'll need to interpret the errors to know whether the failure was due to a problem or simply to the fact that it was just a test.

There are some significant benefits of using the ADMT, besides just migrating user accounts. ADMT can be found on the Windows 2003 CD.

- You can migrate workstations remotely. You can specify that SIDs be simply added instead of replaced, giving you the option of joining a workstation back to the old domain

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 instructions on how to migrate from NT4 to Samba-3. This chapter provides background information that should meet these needs.

One wonders how many NT4 systems will be left in service by the time you read this book though.

9.1 Introduction

It is possible to just migrate the domain accounts to Samba-3 and then to switch machines, but as a hands-o transition, this is more the exception than the rule. Most systems require some tweaking after migration before an environment that is acceptable for immediate use is obtained.

Section

Figure 9.1 Schematic Explaining the net rpc vampire Process

Warning

Under absolutely no circumstances should the Samba daemons be started until instructed to do so. Delete the `/etc/samba/secrets.tdb` file and all Samba control tdb files before commencing the following configuration steps.

Table 9.1 Samba smb.conf Scripts Essential to Samba Operation

Entity	ldapsam Script	tdbsam Script

Note

perl scripts should be located in the `/opt/IDEALX/sbin` di-

```
                                                    [\\MERLIN\home\%U] > \\%L\%
. logon path: directory where roaming profiles are stored.
                                                 Ex:'\\MERLIN\profiles\%U'
  logon path (leave blank if you don't want roaming profile)
                                 [\\MERLIN\profiles\%U] > \\%L\profiles\%
```

```
. 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.
```

Note that the NT4 domain SID that was previously obtained was entered above. Also, the sambaUnixIdPooldn object was specified as sambaDomainName=DAMNATION.

```
Setting stored password for
            "cn=Manager,dc=terpstra-world,dc=org" in secrets.tdb
```

7. An expanded view of a user account entry shows more of what was obtained from the NT4 PDC:

```
sleeth:~ # pdbedit -Lv maryk
Unix username:        maryk
NT username:          maryk
Account Flags:        [UX         ]
User SID:             S-1-5-21-1988699175-926296742-1295600288-1003
Primary Group SID:    S-1-5-21-1988699175-926296742-1295600288-1007
Full Name:            Mary Kathleen
Home Directory:       \\diamond\maryk
HomeDir Drive:        X:
Logon Script:         scripts\logon.bat
Profile Path:         \\diamond\profiles\maryk
Domain:               MEGANET
Account desc:         Peace Maker
Workstations:
Munged dial:
Logon time:           0
Logoff time:          Mon, 18 Jan 2038 20:14:07 GMT
Kickoff time:         Mon, 18 Jan 2038 20:14:07 GMT
Password last set:    Wed, 02 Apr 2003 13:05:04 GMT
Password can change:  0
Password must change: Mon, 18 Jan 2038 20:14:07 GMT
```

8. The following command lists the long names of the groups that have been imported (vampired) from the NT4 PDC:

```
root#  net group -l -Uroot%not24get -Smassive

Group name            Comment
----------------------------
Engineers             Snake Oil Engineers
Marketoids            Untrustworthy Hype Vendors
Gnomes                Plain Vanilla Garden Gnomes
Replicator            Supports file replication in a domain
```

an autogenerated SID. The typical SID looks like this: S-1-5-21-XXXXXXXXXX-XXXXXXXXXX-XXXXXXXXXX, where the XXXXXXXXXX can be any number with from 6 to 10 digits. On the other hand, why would you really want to create your own SID? I cannot think of a good reason. You may want to set the SID to one that is already in use somewhere on your network, but that is a little different from straight out creating your own domain SID.

3. Q: *When using a tdbsam passdb backend, why must I have all domain user and group accounts in `/etc/passwd` and `/etc/group`?*

A: Samba-3 must be able to tie all user and group account SIDs to a UNIX UID or GID. Samba does not fabricate the UNIX IDs

5. Q: *How would you merge 10 tdbsam-based domains into an*

Example 9.3.1 NT4 Migration Samba-3 Server smb.conf — Part: A

Example 9.3.6 NT4 Migration NSS Control File: /etc/nsswitch.conf (Stage:1)

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

hosts:          files dns wins
networks:       files dns

services:       files
protocols:      files
rpc:            files
ethers:         files
netmasks:       files
netgroup:       files
publickey:      files

bootparams:     files
automount:      files nis
aliases:        files
#passwd_compat: ldap       #Not needed.
#group_compat:  ldap      #Not needed.
```

Example 9.3.7 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

services:       files
protocols:      files
rpc:            files
ethers:         files
netmasks:       files
netgroup:       files
publickey:      files

bootparams:     files
automount:      files nis
aliases:        files
#passwd_compat: ldap       #Not needed.
#group_compat:      #Not needed.
```

NLM for rsync to migrate files from the NetWare server to the Samba server. The UNIX administrator might prefer tools that are part of the Mars_NWE (Martin Stovers' NetWare Emulator)

Example 10.2.1

```
## Admins and HR can add and delete groups
access to dn.sub="ou=groups,dc=abmas,dc=biz"
```

Section

```
"(Objectclass=*)"
```

Section 10.3. Implementation

•

Example 10.3.2 The PAM Conu500yoTheSSuritConEx10

Example 10.3.6 Samba Configuration File — smb.conf Part D

```
[APPS]
        path = /data/samba/shares/Apps
        force group = "Domain Users"
        read only = No
 [ACCT]
        path = /data/samba/shares/Accounting
```

Example 10.3.7 Samba Configuration File — smb.conf Part E

```
[X]
```

Section

Section 10.3. Implementation

Example 10.3.15

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")
      WRITEVALUE("HKEY_CURRENT_USER\Software\Microsoft\
```

REFERENCE SECTION

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

I apologize for the leak of internal discussions to the new business. It reflects poorly on our professionalism and has put you in an unpleasant position. I regret the incident.

must be able to support his or her claims, keep emotions to the side, and answer technically.

11.2 Dissection and Discussion

Samba-3 is a tool. No one is pounding your door to make you

Where Samba and the ADS domain account information obtained through the use of

The report that is critical of Samba really ought to have exercised greater due diligence: the real weakness is on the

attached storage (NAS) industry. Unfortunately, for the past few years, Microsoft has been absosAcye37730()e-3y-9dn(&)n-3y-9dnsxerc

Section 11.2. Dissection and Discussion

Section

communications data stream for their Windows interoperability, particularly when Samba is expected to emulate a Windows Server 200x domain controller. But the interoperability issue goes far deeper than this. In the domain control proto-

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 server you wish to administer. Click **OK → OK → OK**. In the left panel, the entry **Computer Management (Local)** should now reflect the change made. For example, if the server you are administering is called FRODO, the Computer Management entry should now say **Computer Management (FRODO)**.
4. In the left panel, click **Computer Management (FRODO) → [+] Shared Folders → Shar**[illegible]T1001155.4372391.60557.57.540G1001

11.3.2.2 Override Controls

Override controls implemented by Samba permit actions like the

while waiting for the file system transaction (read or write) to complete. The result can be a profound apparent performance degradation as the client continually attempts to reconnect to overcome the effect of the lost `oplock break`, or time-out.

Section 11.3. Implementation

using the following command:

```
root#  chmod ug+rwx,o-rwx /usr/data/finance
```

4. Set the SGID (supergroup) bit on all directories from the

11.4 Questions and Answers

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

A: Either tool can be used with equal effect. There is no benefit of one over the other, except that the MMC utility is present on

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 have cast Samba-3 in the leading role, and where authentication was required, you have used one or another of Samba's many authentication backends (from flat text files with smbpasswd to LDAP directory integration with ldapsam). Now you can design a solution for a new Abmas business. This business is running Windows Server 2003 and Active Directory, and these are to stay. It's time to master implementing Samba and Samba-supported services in a domain controlled by the latest Windows authenti-

of its chosen user authentication scheme being changed for now.

Section 12.3. Implementation

Section

```
root#  squid
```

Example 12.3.4 Squid Configuration File Extract — /etc/squid.conf [ADMINISTRATIVE PARAMETERS Section]

```
cache_effective_user squid
cache_effective_group squid
```

Example 12.3.5 Se3(TIONET1003110032E7580.802532270Tdi[(MIN]0d0J0.3985w00.199248608278550.199

12.4 Questions and Answers

The development of the ntlm_auth

Section

Chapter 13

PERFORMANCE, RELIABILITY, AND AVAILABILITY

Well, you have reached one of the last chapters of this book. It

of clustering because each clustering methodology uses its own custom tools and methods. Only passing comments are o□ered concerning these methods.

A search[1] for]t3(s)-7namba cluster" produced 71,600 hits. And a

A significant number of reports concern problems with the smbfs

Section

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

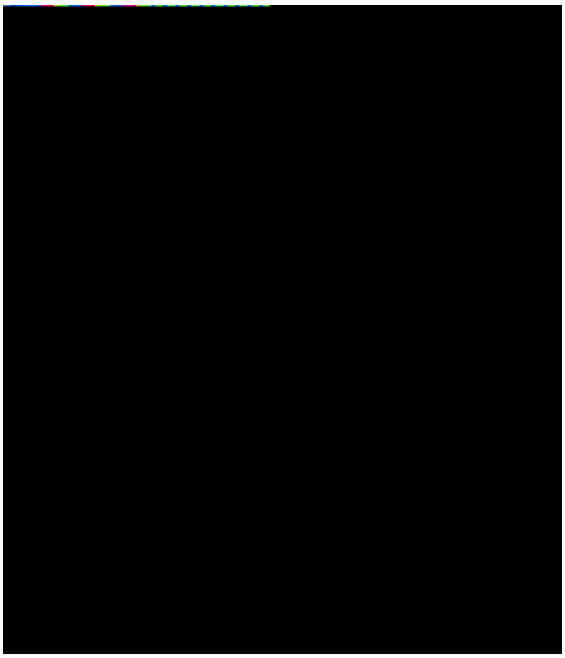
the information provided in this chapter may help someone to

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

Figure 15.2 The Computer Name Panel.



word) of a domain administrativ1365nist.00(ad)1(nistralJ/F30ud)1(m(adtm)-1(ithd)1atr

```
   LMHOSTSFILE: /etc/samba/lmhosts
   LIBDIR: /usr/lib/samba
   SHLIBEXT: so
   LOCKDIR: /var/lib/samba
   PIDDIR: /var/run/samba
   SMB_PASSWD_FILE: /etc/samba/smbpasswd
   PRIVATE_DIR: /etc/samba
...
```

15.3 Starting Samba

Samba essentially consists of two or three daemons. A daemon

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

15.5 Alternative LDAP Database Initialization

The following procedure may be used as an alternative means

Section

```
root#
```

Section

5. Start your Web server then, using your Web browser, connect to LAM[3] URL. Click on the the *Configuration Login*

Figure 15.6 The LDAP Account Manager Login Screen

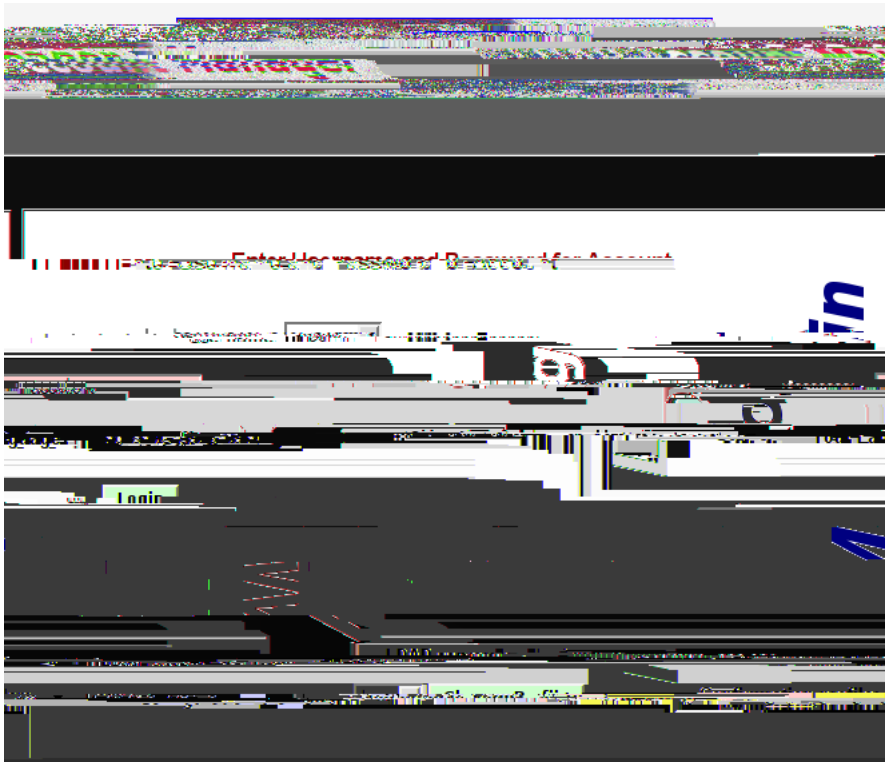
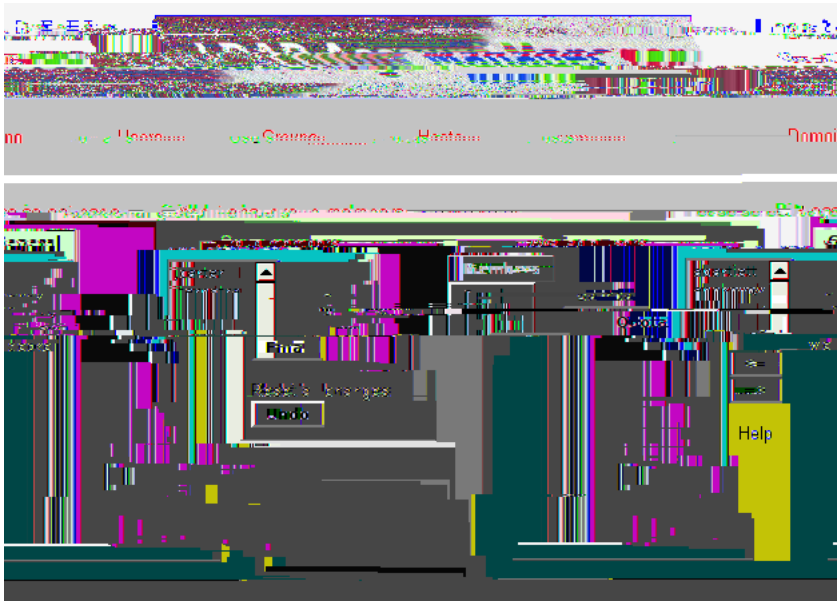


Figure 15.8 The LDAP Account Manager User Edit Screen

Figure 15.10 The LDAP Account Manager Group Membership Edit Screen



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

The setting of the SUID/SGID bits on the file or directory permissions flag has particular consequences. If the file is executable and the SUID bit is set, it executes with the privilege of (with bi ise

In this example, if the user maryv creates a file, it is owned by her. If maryv has the primary group of Accounts, the file is

•

Example 15.3.2 A Sample Samba Control Script for Red Hat Linux

```
#!/bin/sh
#
# chkconfig: 345 81 35
```

Example 15.4.3 DNS Root Name Server Hint File: /var/lib/named/root.hint

```
; This file is made available by InterNIC under anonymous FTP as
;       file                /domain/named.root
;       on server           FTP.INTERNIC.NET
; last update: Nov 5, 2002. Related version of root zone: 2002110501
; formerly NS.INTERNIC.NET
.                        3600000  IN  NS    A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.      3600000      A     198.41.0.4
; formerly NS1.ISI.EDU
.                        3600000      NS    B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.      3600000      A     128.9.0.107
; formerly C.PSI.NET
.                        3600000      NS    C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET.      3600000      A     192.33.4.12
; formerly TERP.UMD.EDU
.                        3600000      NS    D.ROOT-SERVERS.NET.
D.ROOT-SERVERS.NET.      3600000      A     128.8.10.90
; formerly NS.NASA.GOV
.                        3600000      NS    E.ROOT-SERVERS.NET.
E.ROOT-SERVERS.NET.      3600000      A     192.203.230.10
; formerly NS.ISC.ORG
.                        3600000      NS    F.ROOT-SERVERS.NET.
F.ROOT-SERVERS.NET.      3600000      A     192.5.5.241
; formerly NS.NIC.DDN.MIL
.                        3600000      NS    G.ROOT-SERVERS.NET.
G.ROOT-SERVERS.NET.      3600000      A     192.112.36      NS    G.ROOT-SERVERS
.                        3600000      NS    G.ROOT-SHRVERS.NET.
```

Section

Example 15.5.2 LDAP Pre-configuration Script: SMBLDAP-ldif-preconfig.sh — Part B

Chapter 16

NETWORKING PRIMER

regarding this tool from the Ethereal[1] Web s

16.2.1 Assignment Tasks

You are about to witness how Microsoft Windows computer networking functions. The exercises step through identification of

(d) Enable network name resolution

(e) Enable transport name resolution

Click **OK**.

2. Start the Windows 9x/Me machine to be monitored. Let it run for a full 30 minutes. While monitoring, do not press i1583.y-369(k)-8(w)-1(sy)-27(eoard-3690k)-8(w)-1(sys,-369(d)1(o)-469(i)1(

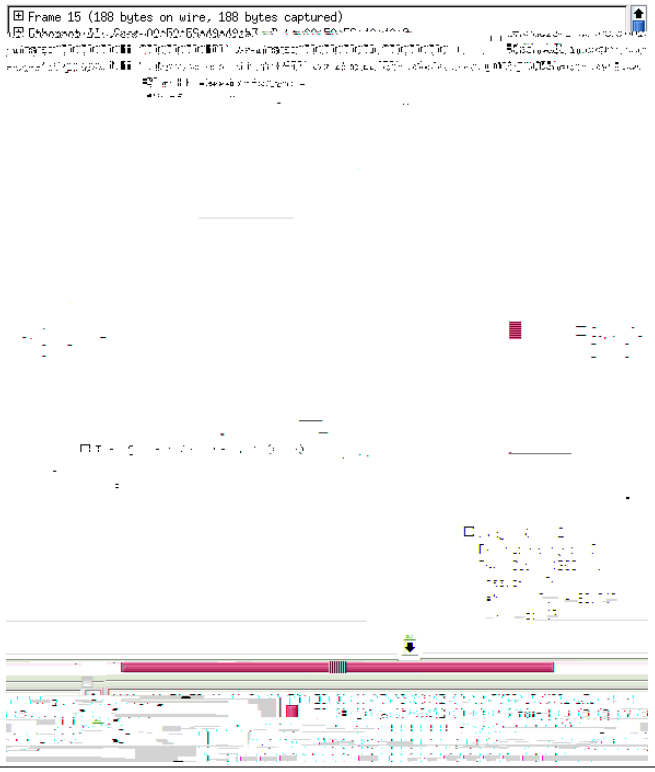
Figure 16.2

3.

Table 16.2 Second Machine (Windows 98) — Capture Statistics

Figure 16.3 Typical Windows 9x/Me Host Announcement

Figure 16.4 Typical Windows 9x/Me NULL SessionSetUp AndX Request



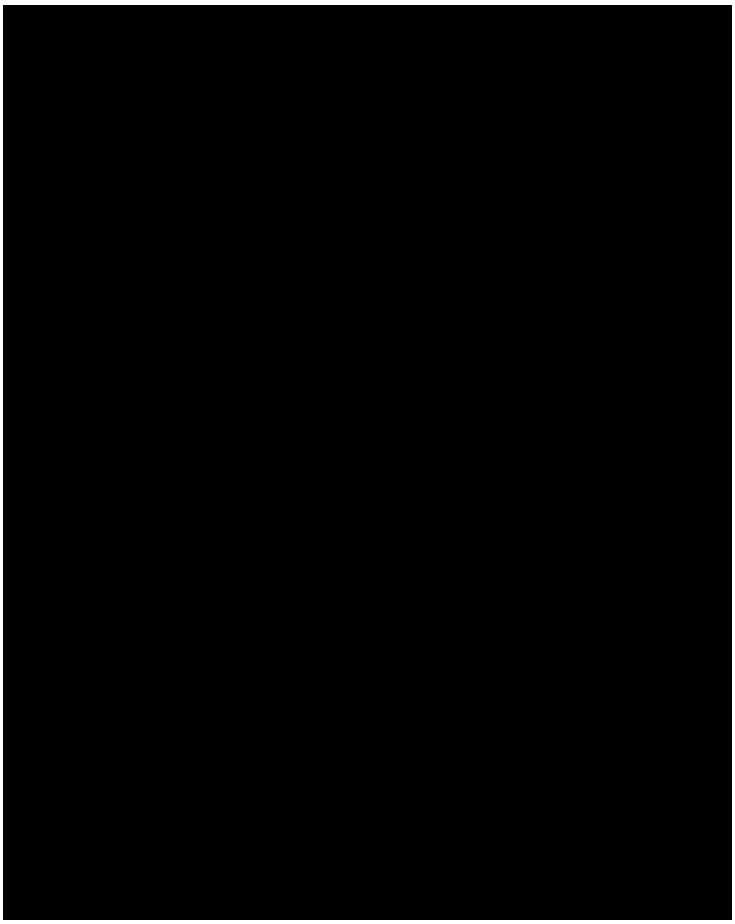
When a UNIX/Linux system does not have a nobody

Section

To complete this exercise, you need a Windows XP Professional client that has been configured as a domain member of either a Samba-controlled domain or a Windows NT4 or 200x Active Directory domain. Here we do not provide details for how to configure this, as full coverage is provided earlier in this book.

Section

Figure 16.7 Typical Windows XP User Session Setup AndX Request



nouncements and workgroup announcements.

- All Samba servers must be configured with a mechanism for mapping the `NULL-Session` to a valid but nonprivileged UNIX system account.

- The use of Microsoft encrypted passwords is built right into

second method requires a correctly configured DNS server (see *TOSHARG2*, Chapter 9, Section 9.3, "Discussion").

Appendix A

Section A.2. TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND

at no charge to all third parties under the terms of this License.

3. If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License.

Exception:

A.2.4 Section 3

You may copy and distribute the Program (or a work based on it, under Section A.2.3 in object code or executable form under the terms of Section A.2.2 and

Section A.2. TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

A.2.10 Section 9

The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such

Section

GLOSSARY

Access Control List (ACL)

Lightweight Directory Access Protocol (LDAP)

The Lightweight Directory Access Protocol is a technology that originated from the development of X.500 protocol specifications and implementations. LDAP was designed

SUBJECT INDEX

/data/ldap,

broadcast, 477, 550

criticism, 427, 431
Critics, 436
Cryptographic, 436
CUPS, 10, 33, 38, 45, 62, 72, 114, 149, 157, 196

export, 350
extent, 432
External Domains, 271
extreme demand, 476

fail, 239
fail-over, 242, 244
failed, 278
failed join, 278,

groupmem,

interoperability, 439
libraries, 288
MIT, 288
unspecified fields, 439
kerberos, 438
server, 438
Kerberos ticket, 464
kinit, 463
Kixtart, 402
klist, 463
krb5, 460
krb5.conf, 462

LAM, 504, 505
configuration editor, 507

Defective, 290
name resolve order, 62, 551

passwd, 11, 22, 68
password
    backend, 37, 68,

RPM, 329, 334, 388
    install, 6
rpm, 461, 497
RPMs, 464
rpms, 468
rsync, 175, 311, 396, 482
rsyncd.conf,

shared resource, 434, 450
shares, 433
SID, 87, 147, 242, 270, 298, 325–

sync always,

valid users, 311, 443, 454, 455
validate, 373, 443
validated, 240, 288, 429
validation, 7, 75, 471
vampire, 375
vendor, 433
vendors, 340
VFS modules, 496
virus, 63
VPN, 234
vulnerabilities, 429

wbinfo,