The O cial Samba 3.0.x HOWTO and

ABOUT THE COVER ARTWORK

The cover artwork of this book continues the freedom theme of the first edition of \The Official Samba-3 HOWTO and Reference Guide". We may look back upon the past to question the motives of those who have gone

take the time to think through what may lie ahead. Above all, take stock of the freedom of choice that Samba provides in your world, and enjoy the new potential for seamless interoperability.

ATTRIBUTION

Chapter 1, \How to Install and Test SAMBA"

Shirish Kalele<mailto:samba@samba.org>

John H. Terpstra<mailto:jht@samba.org>

Chapter 21, \Classical Printing Support"

Kurt Pfei e<mailto:kpfeifle@danka.de>

Gerald (Jerry) Carter

<

John H. Terpstra<mailto:jht@samba.org>

Gerald (Jerry) Carter<mailto:jerry@samba.org>

Chapter 36, \Migration from NT4 PDC to Samba-3 PDC"

John H. Terpstra<mailto:jht@samba.org>

Chapter 37, \SWAT: The Samba Web Administration Tool"

John H. Terpstra<mailto:jht@samba.org>

Chapter 38, \The Samba Checklist"

Andrew Tridgell<mailto:tridge@samba.org>

John H. Terpstra<mailto:jht@samba.org>

Chapter 44, \Samba and Other CIFS Clients"

Jelmer R. Vernooij<mailto:jelmer@samba.org>

John H. Terpstra<mailto:jht@samba.org>

Dan Shearer<mailto:dan@samba.org>

Jim McDonough<mailto:jmcd@us.ibm.com> (OS/2)

Chapter 45, \Samba Performance Tuning"

Paul Cochrane<mailto:paulc@dth.scot.nhs.uk>

Jelmer R. Vernooij<mailto:jelmer@samba.org>

John H. Terpstra<mailto:jht@samba.org>

Chapter 46, \LDAP and Transport Layer Security"

Gavin Henry<mailto:ghenry@suretecsystems.com>

Chapter 48, \DNS and DHCP Con guration Guide"

John H. Terpstra<mailto:jht@samba.org>

CONTENTS

Contents

GM0 gm G 2-10727(449 22.7 Network Printing (Windows)28(-)]TJ-25.091 -13.549 Td [(Serv)28(ews))]TJ0 g 0 G0 g 0 G [240616(475)]T

 GAssumpion

LIST OF EXAMPLES

Chapter 7

LIST OF FIGURES

List of Tables

lvi

TOSHARG2 is used as an abbreviation for the book, \The O cial Samba-3 HOWTO and Reference Guide, Second Edition" Editors: John H. Terpstra and Jelmer R. Vernooij, Publisher: Prentice Hall, ISBN: 0131882228.

S3bE2a(.-585.3S3bE2)2723(ea585.3S3n)-4.3S3nbreviation eook,ba-3by-5.3S3Example ISeond 0dition0ditiors:-4424John 0. T0ublisher:tice 0.ll, ISBN: 0131882221X

SDireciorieca in-4410amono-foti F834er

INTRODUCTION

\A man's gift makes room for him before great men. Gifts are like hooks

Chapter 1

1.2.2 TDB Database File Information

This section contains brief descriptions of the databases that are used by Samba-3.

Make sure you put the `smb.conf` file in the correct place. Note, the correct location of this file depends on how the binary files were built. You can discover the correct location by executing from the directory that contains the

Section

Chapter 2

FAST START: CURE FOR

domain member servers as well as Samba domain control (PDC/BDC) and nally describes in detail a large distributed network with branch o ces in remote locations.

2.3 Worked Examples

The con guration examples are designed to cover everything necessary to get Samba running. They do not cover basic operating system platform con guration, which is clearly beyond the scope of this text.

It is also assumed that Samba has been correctly installed, either by way of installation of the packages that are provided by the operating system vendor or through other means.

2.3.1 Standalone Server

Example 2.3.1 Anonymous Read-Only Server Con guration

```
# Global paramet
```

```
root#  testparm
```

The information above (following # Global parameters) provides the complete contents of the /etc/samba/smb.conf file.

2.3.1.2 Anonymous Read-Write Document Server

We should view this configuration as a progression from the previous example. The difference is that shared access is now forced to the user identity of jackb and to the primary group jackb belongs to. On t513.539(a.iennemden)28(539(a.wt)27ef)]T

f

value of the

Section

Example 2.3.6 Member Server smb.conf (Shares and Services)

```
[homes]
        comment = Home Directories
        valid users = %S
        read only = No
        browseable = No
 [spytfull]
        comment = Accounting Application Only
```

```
group:  files winbind
hosts:  files dns winbind
```

7. Set the password for wbinfo to use:

```
root# wbinfo --set-auth-user=root%'bigsecret'
```

8. Validate that domain user and group credentials can be correctly resolved by executing:

```
root# wbinfo -u
MIDEARTH\maryo
MIDEARTH\jackb
MIDEARTH\ameds
...
MIDEARTH\root

root# wbinfo -g
MIDEARTH\Domain Users
MIDEARTH\Domain Admins
MIDEARTH\Domain Guests
...
MIDEARTH\Accounts
```

9. Check that winbind is working. The following demonstrates correct username resolution via the getent system utility:

```
root# getent passwd maryo
maryo:x:15000:15003:Mary Orville:/home/MIDEARTH/maryo:/bin/false
```

10. A nal test that we have this under control might be reassuring:

```
root# touch /export/a_file
root# chown maryo /export/a_file
root# ls -al /export/a_file
...
```

Section 2.3. Worked Examples

Linux distributions tend to install the Idealx scripts in the /usr/share/doc/packages/sambaXXXXXX/examples/LDAP/smbldap-tools directory. Idealx scripts version smbldap-tools-0.9.1 are known to work well.

1. Obtain from the Samba sources ~/examples/LDAP/samba.schema and copy it to the /etc/openldap/schema/ directory.

2. Set up the LDAP server. This example is suitable for OpenLDAP 2.1.x. The /etc/openldap/slapd.conf le. Example slapd.conf File

```
# Note commented out lines have been removed
```

Section 2.3. Worked Examples

FIRST STEPS IN SERVER CONFIGURATION

Chapter 3

SERVER TYPES AND SECURITY MODES

This chapter provides information regarding the types of server that Samba may be con gured to be. A Microsoft network administrator who wishes to migrate to or use Samba will want to know the meaning, within a Samba context, of terms familiar to the MS Windows administrator. This means that it is essential also to de ne how critical security modes function before we get into the details of how to con gure the server itself.

This chapter provides an overview of the security modes of which Samba is capable and how they relate to MS Windows servers and clients.

Ats.

3.3.1.1 Example Con guration

The smb.conf parameter that sets user-level security is:

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

In the example shown here (not likely to be used in practice) the lookup will check /etc/passwd and /etc/group, if not found it will check NIS, then LDAP.

3.3.2.1 Example Con guration

The smb.conf parameter that sets share-level security is:

Section

Note

Samba-2.2.4 and later Samba 2.2.x series releases can autojoin a Windows NT4-style domain just by executing:

```
root# smbpasswd -j DOMAIN_NAME -r PDC_NAME \
    -U Administrator%password
```

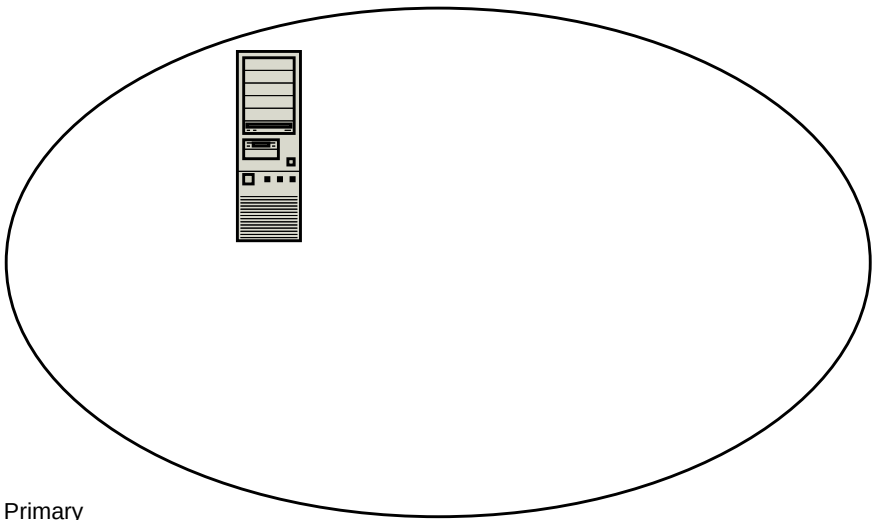
3.3.4 ADS Security Mode (User-Level Security)

Both Samba-2.2, and Samba-3 can join an Active Directory domain using NT4 style RPC based security. This is possible if the domain is run in native

3.5.1 What Makes Samba a Server?

Chapter 4

Figure 4.1 An Example Domain.



Understanding how MS Windows clients interoperate in a network environment.

Do not be put o ; on the surface of it MS Windows networking seems so

a well-designed network to log onto any workstation that is a member of

Samba-3 implements group mapping between Windows NT groups and UNIX groups (this is really quite complicated to explain in a short space). This is discussed more fully in Chapter 12, \Group Mapping: MS Windows and UNIX".

Samba-3, like an MS Windows NT4 PDC or a Windows 200x Active Directory, needs to store user and Machine Trust Account information in a

Section

(SOAP) message for the computer-to-computer communications needed for Web services. Or they may be passed between Web servers of federated organizations that share live services. The Liberty Alliance, an industry group formed to promote federated-identity standards, has adopted SAML 1.1 as part of its application framework. Microsoft and IBM have proposed an al-

to override any downstream controller, but a downline controller has control only over its downline. With Samba-3, this functionality can be implemented using an LDAP-based user and machine account backend.

No Group Policy Objects.

No synchronously executed Active Directory logon scripts.

Can't use Active Directory management tools to manage users and machines.

le). Additionally, one server in a Samba-3 domain must advertise itself as the domain master browser.[3] This causes the PDC to claim a domain-speci c NetBIOS name that identi es it as a DMB for its given domain or

Example 4.4.1 smb.conf for being a PDC

```
[global]
        netbios name
        workgrou30 6e
```

Section 4.5. Samba ADS Domain Control

Microsoft Windows NT4-style domain controllers have. Samba-3 does not have all the capabilities of Windows NT4, but it does have a number of features that Windows NT4 domain controllers do not have. In short, Samba-3 is not NT4 and it is not Windows Server 200x: it is not an Active Directory

Section

Section 10.4.1; Microsoft PDCs expect to win the election to become the DMB, if it loses that election it will report a continuous and rapid sequence of warning messages to its Windows event logger complaining that it has

Section

on the Samba PDC. The following command will remove all network drive connections:

```
C:\> net use * /d
```

This will break all network connections.

Further, if the machine is already a \member of a workgroup" that is the same name as the domain you are joining (bad idea), you will get this

4.7.4 The Machine Trust Account Is Not Accessible

\When I try to join the domain I get the message, "The machine account for this computer either does not exist or is not accessible." What's wrong?"

This problem is caused by the PDC not having a suitable Machine Trust Account. If you are using the *add machine script* method to create accounts, then this would indicate that it has not worked. Ensure the domain admin user system is

fsos are creamin1(gs)-269(accoun)28(t)-269eunri(es)-260(mun)28uallyTthen teys havks not n1(akw)27enenthatoshavks theryefor the

Trust

A domain controller has to announce its role on the network. This usually takes a while. Be patient for up to 15 minutes, then try again.

4.7.7 Cannot Log onto Domain Member Workstation After Joining Domain

Chapter 5

the slave nds its master down at the wrong time, you will have stability and operational problems.

Samba-3 cannot function as a BDC to an MS Windows NT4 PDC, and Samba-3 cannot function correctly as a PDC to an MS Windows NT4 BDC. Both Samba-3 and MS Windows NT4 can function as a BDC to its own type of PDC.

The BDC is said to hold a *read-only* of the SAM from which it is able to process network logon requests and authenticate users. The BDC can continue to provide this service, particularly while, for example, the wide-area network link to the PDC is down. A BDC plays a very important role in both the maintenance of domain security as well as in network integrity.

In the event that the NT4 PDC should need to be taken out of service, or if it dies, one of the NT4 BDCs can be promoted to a PDC. If this happens while the original NT4 PDC is online, it is automatically demoted to an NT4 BDC. This is an important aspect of domain controller management. The tool that is used to e ect a promotion or a demotion is the Server Manager for Domains. It should be noted that Samba-3 BDCs cannot be promoted in

change to the machine account in the LDAP tree must take place on the master LDAP server. This is not replicated rapidly enough to the slave server that the PDC queries. It therefore gives an error message on the client machine about not being able to set up account credentials. The machine account is created on the LDAP server, but the password fields will

as a mere NIS client would not be enough, as the BDC would not be able to access its user database in case of a PDC failure. NIS is by no means the only method to synchronize passwords. An LDAP solution would also work.

The Samba password database must be replicated from the PDC to the BDC. Although it is possible to synchronize the smbpasswd file with rsync and ssh, this method is broken and flawed, and is therefore not recommended. A better solution is to set up slave LDAP servers for each BDC and a master LDAP server for the PDC. The use of rsync is inherently flawed by the fact that the data will be replicated at timed intervals. There is no guarantee that the BDC will be operating at all times with correct and current machine and user account

application of Local Machine Trust Account password updates to the local

5.4.4 Can I Do This All with LDAP?

Chapter 6

DOMAIN MEMBERSHIP

Domain membership is a subject of vital concern. Samba must be able

A Windows NT4 PDC stores each Machine Trust Account in the Windows Registry. The introduction of MS Windows 2000 saw the introduction of Active Directory, the new repository for Machine Trust Accounts. A Samba PDC, however, stores each Machine Trust Account in two parts, as follows:

A domain security account (stored in the *passdb backend*) that has been con gured in the `smb.conf` le. The precise nature of the account information that is stored depends on the type of backend database that has been chosen.

The older format of this data is the `smbpasswd` database that contains the UNIX login ID, the UNIX user identi er (UID), and the LanMan and NT-encrypted passwords. There is also some other information in this le that we do not need to concern ourselves with here.

The two newer database types are called ldapsam and tdbsam. Both store considerably more data than the older `smbpasswd` le did. The extra information enables new user account controls to be implemented.

A corresponding UNIX account, typically stored in `/etc/passwd`. Work

There are three ways to create Machine Trust Accounts:

Join the client to the domain immediately

Manually creating a Machine Trust Account using this

1. From the menu select **Computer**.
2. Click **Select Domain**.
3. Click the name of the domain you wish to administer in the **Select Domain** panel and then click **OK**.
4. Again from the menu select **Computer**.
5. Select

6.2.4.1 Windows 200x/XP Professional Client

When the user elects to make the client a domain member, Windows 200x prompts for an account and password that has privileges to create machine accounts in the domain. A Samba administrator account (i.e., a Samba

Section

daemon lasts. This can drain the connection resources on a Microsoft NT server and cause it to run out of available connections. With *security* = domain, however, the Samba daemons connect to the PDC or BDC only for as long ba67lssarya

regarding Kerberos interoperability is RFC1510[4]. This RFC explains much of the magic behind the operation of Kerberos.

MIT's, as well as Heimdal's, recent KRB5 libraries default to checking for SRV records, so they will automatically find the KDCs. In addition, `krb5.conf` only allows specifying a single KDC, even there if there may be more

note that forward slashes must be used, because backslashes are both valid characters in an OU name and used as escapes for other characters. If you need a backslash in an OU name, it may need to be quadrupled to pass through the shell escape and ldap escape.

6.4.3.1 Possible Errors

ADS support not compiled in Samba must be recon gured (remove con-g.cache) and recompiled (make clean all install) after the Kerberos libraries and headers les are installed.

net ads join prompts for user name You need to log in to the domain using `kinit` *USERNAME@REALM*. *USERNAME* must be a user who has rights to add a machine to the domain.

Unsupported encryption/or checksum types Make sure that the `/etc/krb5.conf` is correctly con gured for the type and version of Kerberos installed on the system.

6.4.4 Testing Server Setup

If the join was successful, you will see a new computer account with the NetBIOS name of your Samba server in Active Directory (in the \Computers" folder under Users and Computers.

On a Windows 2000 client, try `net use * \\server\share`.

6.4.5 Testing with smbclient

6.6 Common Errors

In the process of adding/deleting/re-adding domain member machine trust accounts,

the *log level* in the `smb.conf` file to level 10, then try to rejoin the domain.

conf le. Example 7.3.1 is the smb.conf le that will do this. Assume that all the reference documents are stored in the directory /export, and the documents are owned by a user other than nobody. No home directories are

1. The print server must require no administration.
2.

Sect125 7.9 ET q 1.0[0.8.892 689.596ple Con guraSect125 7.9 ET q 1.0[03 cm []0 d125J 0.398 wct125m 358.659.90l S Q 0289.0[(Sect753gura)]TJ 7.9128.150.636.11509 T

The example in Example 7.3.2 uses CUPS for direct printing via the CUPS libarary API. This means that all printers will be exposed to Windows users without need to configure a printcap file. If there is necessity to expose only a sub-set of printers, or to define a special type of printer (for example, a PDF filter) the *printcap name = cups* can be replaced with the entry, for example,

Chapter 8

MS WINDOWS NETWORK CONFIGURATION GUIDE

8.1 Features and Bene ts

Occasionally network administrators report di culty getting Microsoft Windows clients to interoperate correctly with Samba servers. It seems that some folks just cannot accept the fact that the right way to con gure an MS Windows network client is precisely as one would do when using MS Windows NT4 or 200x servers. Yet there is repetitious need to provide detailed Windows client con guration instructions.

The purpose of this chapter is to graphically illustrate MS Windows client con guration for the most common critical aspects of such con guration. An experienced network administrator will not be interested in the details of this chapter.

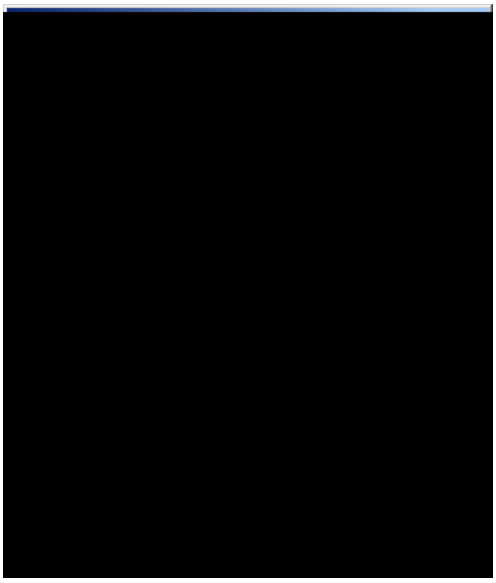
8.2 Technical Details

This chapter discusses TCP/IP protocol con guration as well as network

Figure 8.3

Figure 8.5 WINS Con guration

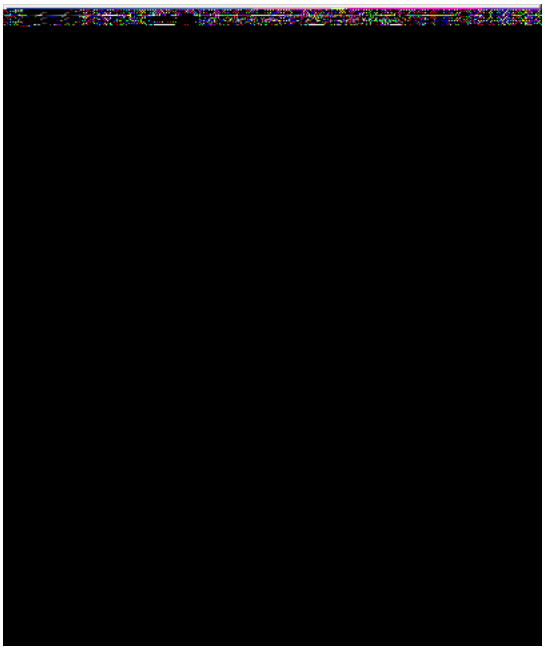
Figure 8.6 Local Area Connection Properties.



4. If necessary, click the **DNS Con guration** tab to add DNS server settings. Click the **WINS Con guration** tab to add WINS server settings. The **Gateway** tab allows additional gateways (router addresses) to be added to the network interface settings. In most cases where DHCP

Figure 8.7

Figure 8.9 DNS Con guration.



Note

Windows XP Home edition cannot participate in domain

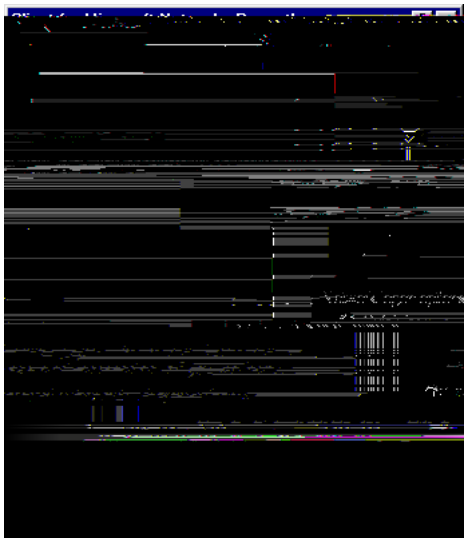
Section

Figure 8.12 IP Address.

Section

Figure 8.20 The Network Panel.

Figure 8.21 Client for Microsoft Networks Properties Panel.



Part III

Advanced Con guration

Assume that a group named *developers* exists with a UNIX GID of 782. In this case this user does not exist in Samba's group mapping table. It would be perfectly normal for this group to be appear in an ACL editor. Prior to Samba-3.0.23, the group SID might appear as `S-1-5-21-647511796-4126122067-3123570092-2565`.

With the release of Samba-3.0.23, the group SID would be reported as `S-1-22-2-782`. Any security descriptors associated with files stored on a Windows NTFS disk partition will not allow access based on the group permissions if the user was not a member of the `S-1-5-21-647511796-4126122067-3123570092-2565` group. Because this group SID is `S-1-22-2-782` and not reported in a user's token, Windows would fail the authoriza-

ould48.907 -23.T1 Tf itowsno0 T0 Td itof0(cl)-4 itokermi itoID in Smi itop704(Piza-).1e4no0 Tf itt2iSIDstresso

Note

10.3.1 NetBIOS over TCP/IP

Local Master Browser, set the following options in the *[global]* section of the smb.conf file as shown in Example 10.4.4

Example 10.4.4 Local Master Browser smb.conf

```
[global]
```

i m93 g5 9.966i4393d33 653.4 Td ro373l23 g5 9.966i43s =ws32(,3 84.).96602m93 g03mh3 602m [()]TJ0.93 g

you upgrade to a recent version, or at the very least set the parameter to

10.5.2 WINS Replication

Samba-3 does not support native WINS replication. There was an approach to implement it, called `wrepld`, but it was never ready for action and the development is now discontinued.

```
"MADMAN#03" 1155298378 192.168.1.2 66R
```

DNS | is a good choice but lacks essential NetBIOS name_type information.

Many sites want to restrict DNS lookups and avoid broadcast name resolution tra c. The *name resolve order* parameter is of great help here. The syntax of the *name resolve order* parameter is:

Section

Table 10.2 Browse Subnet Example 2

Subnet	Browse Master	List

Section

Samba NetBIOS name cache and cause it to be rebuilt. This does not make

\ But, the share is immediately available from a command shell (cmd, followed by exploration with DOS command. Is this a Samba problem, or is it a Windows problem? How can I solve this?"

Here are a few possibilities:

(can take a long time) it times out and browsing will appear to be mostly normal again.

Chapter 11

ACCOUNT INFORMATION DATABASES

Early releases of Samba-3 implemented new capability to work concurrently

11.1 Features and Bene ts

Samba-3 provides for complete backward compatibility with Samba-2.2.x functionality as follows:

11.1.1 Backward Compatibility Account Storage Systems

Plaintext

Section 11.1. Features and Bene ts

11.2 Technical Information

Old Windows clients send plaintext passwords over the wire. Samba can

It is not uncommon, for sites that have existing LDAP DITs to nd necessity

In short, the Sarbanes-Oxley Act of 2002 is an instrument that enforces

Section

Section 11.3. Account Management Tools

Section 11.3. Account Management Tools

Table 11.2 Samba SAM Account Control Block Flags

Flag	Description
D	Account is disabled.
H	A home directory is required.
I	An inter-domain trust account.
L	Account has been auto-locked.

As a result of these de ciencies, a more robust means of storing user attributes used by smbd was developed. The API that de nes access to user accounts is commonly referred to as the samdb interface (previously, this was called the passdb API and is still so named in the Samba source code trees).

Samba provides an enhanced set of passdb backends that overcome the de ciencies of the smbpasswd plaintext database. These are tdbsam and ldapsam. Of these, ldapsam will be of most interest to large corporate or enterprise sites.

11.4.3 tdbsam

ration. Idealx also produced the smbldap-tools and the Interactive

Section

Section

Section

Table 11.4 Attributes in the sambaSamAccount ObjectClass (LDAP), Part B

Chapter 12

GROUP MAPPING: MS WINDOWS AND UNIX

Section 12.2. Discussion

Having completed these two steps, the execution of getent group demo

modify user accounts, without requiring root privileges. Such a request violates every understanding of basic UNIX system security.

There is no safe way to provide access on a UNIX/Linux system without providing root-level privileges. Provision of root

group.

Table 12.1 Well-Known User Default RIDs

Well-Known Entity	RID	Type	Essential
Domain Administrator	500	User	

For complete details on net groupmap, refer to the net(8) man page.

12.3 Con guration Scripts

Everyone needs tools. Some of us like to create our own, others prefer to use canned tools (i.e., prepared by someone else for general use).

12.3.1 Sample smb.conf Add Group Script

A script to create complying group names for use by the Samba group interfaces is provided in Example 12.3.1. This script adds a temporary entry in the /etc/group le and then renames it to the desired name. This is

Section 12.4. Common Errors

Chapter 13

REMOTE AND LOCAL MANAGEMENT: THE NET COMMAND

The net command is one of the new features of Samba-3 and is an attempt to provide a useful tool for the majority of remote management operations necessary for common tasks. The net tool is exible by design and is intended for command-line use as well as for scripted control application.

Originally introduced with the intent to mimic the Microsoft Windows command that has the same name, the net

Section

Section

The following demonstrates that the use of the net command to add a group account results in immediate mapping of the POSIX group that has been created to the Windows group account as shown here:

is ignored. The following command demonstrates how the Windows group \SupportEngrs" can be renamed to \CustomerSupport":

```
root#  net rpc group rename SupportEngrs \
    CustomerSupport -Uroot%not24get
```

13.3.2 Manipulating Group Memberships

Three operations can be performed regarding group membership. It is possible to (1) add Windows users to a Windows group, to (2) delete Windows users from Windows groups, and to (3) list the Windows users that are members of a Windows group.

To avoid confusion, it makes sense to check group membership before attempting to make any changes. The **getent group** will list UNIX/Linux group membership. UNIX/Linux group members are seen also as members of a Windows group that has been mapped using the **net groupmap** command (see Chapter 12, \Group Mapping: MS Windows and UNIX"). The following list of UNIX/Linux group membership shows that the user `ajt` is a member of the UNIX/Linux group `Engineers`.

```
root#  getent group
...
Domain Admins:x:512:root
Domain Users:x:513:jht,lct,ajt,met,vlendecke
Domain Guests:x:514:
Print Operators:x:550:
Backup Operators:x:551:
Replicator:x:552:
Domain Computers:x:553:
Engineers:x:1000:jht,ajt
```

The UNIX/Linux groups have been mapped to Windows groups, as is shown here:

```
root#  net groupmap list
Domain Admins (S-1-5-21-72630-412605-116429-512) -> Domain Admins
```

```
DOM\Engineers
DOM\jamesf
DOM\jht
```

Nested group members can be removed (deleted) as shown here:

```
root#  net rpc group delmem demo "DOM\jht" -Uroot%not24get
```

13.3.3.1 Managing Nest Groups on Workstations from the Samba Server

Windows network administrators often ask on the Samba mailing list how it is possible to grant everyone administrative rights on their own workstation. This is of course a very bad practice, but commonly done to avoid user

Note

When user rights and privileges are correctly set, there is no longer a need for a Windows network account for the `root` user (nor for any synonym of it) with a UNIX UID=0. Initial user rights and privileges can be assigned by any account that is a member of the `Domain Admins` group. Rights can be assigned to user as well as group accounts.

By default, no privileges and rights are assigned. This is demonstrated by executing the command shown here:

```
root#  net rpc rights list accounts -U root%not24get
BUILTIN\Print Operators
```

13.6.1 Machine Trust Accounts

The net command looks in the smb.conf le to obtain its ow10.9091284(nAMuration)]TJ -196.081 -13.549 T

There is no speci c option to remove a machine account from an NT4 domain. When a domain member that is a Windows machine is withdrawn from the domain, the domain membership account is not automatically removed either. Inactive domain member accounts can be removed using any convenient too-con,BT/47(the)273rawn

```
root#  net rpc trustdom list -Uroot%not24get
Trusted domains list:

none

Trusting domains list:

none
```

There are no interdomain trusts at this time; the following steps will create them.

It is necessary to create a trust account in the local domain. A domain controller in a second domain can create a trusted connection with this account. That means that the foreign domain is being trusted to access resources in the local domain. This command creates the local trust account:

```
root#  net rpc trustdom add DAMNATION f00db4r -Uroot%not24get
```

The account can be revealed by usJ 0 -2-28(e)-37d [(The)(0 -n)27202.5152 0 Td [p;db;ediet

```
root# Lwd DAMNATIO\$s
DAMNATIO$:1016:9AC1F121DF897688AAD3B435B51404EE:d
 ]:LCT-428934B1:t
```

trust accounb willaccin33alwn lwn eId40(acch)-4in33alwn lwnsqu lwnbracealetsTJ 0 -20.324 Td [(It)-f

Trusting domains list:

Section

Often it is desirable also to permit a share to be removed using a command-line tool. The following step permits the share that was previously added to be removed:

```
root#  net rpc share delete Bulge -S MERLIN -Uroot%not24get
```

The net rpc share command may be used to migrate shares, directories,

The steps taken so far perform only the migration of shares. Directories and directory contents are not migrated by the steps covered up to this point.

13.8.3.2 File and Directory Migration

Everything covered to this point has been done in preparation for the migration of le and directory data. For many people preparation is potentially boring and the real excitement only begins when datn byThe
t steps the ecn ta(t)-507cany by os ransftermigrat)d
osbeen)1ter F datn the
RMS-copyTd28(-1)5 10.9091 Tf21.3527(0)-5d1[(Remod)7045tw Win)428(M)e)43(a)-30912(200Xer)43(s-1er)

Where it is necessary to preserve all le ACLs, the *--acls* switch should be added to the above command line. Original le timestamps can be preserved by specifying the *--timestamps* switch, and the DOS le attributes (i.e., hidden, archive, etc.) can be preserved by specifying the *--attrs* switch.

Note

Printer migration from a Windows print server (NT4 or 200x) is shown. This instruction causes the printer share to be created together with the underlying print queue:

```
net rpc printer MIGRATE PRINTERS [printer] [misc. options] [targets]
```

Printer drivers can be migrated from the Windows print server to the Samba server using this command-line instruction:

```
net rpc printer MIGRATE DRIVERS [printer] [misc. options] [targets]
```

Printer forms can be migrated with the following operation:

```
net rpc printer MIGRATE FORMS [printer] [misc. options] [targets]
```

Printer security settings (ACLs) can be migrated from the Windows server to the Samba server using this command:

```
net rpc printer MIGRATE SECURITY [printer] [misc. options] [targets]
```

Printer con guration settings include factors such as paper size d8(e35 2 L-ta)]TJ 0 -13.549 Td [the Samba server with this command:

```
net rpc printer MIGRATE STTINGMS [printer] [misc. options] [targets]
```

If the asterisk (*) is used in place of the printer_name argument, a list of all printers will be returned.

Chapter 14

Section

Winbind/NSS with the default local IDMAP table: There are many sites that require only a simple Samba server or a single Samba server that is a member of a Windows NT4 domain or an ADS domain. A typical example is an appliance like file server on which no local accounts are configured and winbind is used to obtain account credentials from the domain controllers for the domain. The domain control can be provided by Samba-3, MS Windows NT4, or MS Windows Active Directory.

Winbind is a great convenience in this situation. All that is needed is a range of UID numbers and GID numbers that can be defined in the `smb.conf` file. The `/etc/nsswitch.conf` file is configured to use

a SID is encountered that has the value `S-1-5-21-34567898-12529001-32973135-1234`, the resulting UID will be `1000 + 1234 = 2234`.

Winbind with an NSS/LDAP backend-based IDMAP facility: In this configuration **winbind** resolved SIDs to UIDs and GIDs from the *idmap uid* and *idmap gid* ranges specified in the `smb.conf` file, but

14.1.3 Primary Domain Controller

Microsoft Windows domain security systems generate the user and group

```
...
passwd: files winbind
shadow: files winbind
group:  files winbind
```

An example smb.conf file for and ADS domain environment is shown in Example 14.2.3.

Example 14.2.3 ADS Domain Member smb.conf using idmap_rid

```
# Global parameters
 [global]
        workgroup = KPAK
        netbios name = BIGJOE
```

...

The following procedure can use the idmap rid facility:

1. Create or install an smb.conf le with the abom.-TClyra [(0 Tdguration.t)28(y:)]TJ0 g 598

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

You will need the PADL[2] nss_ldap tool set for this solution. Configure the /etc/ldap.conf

Chapter 15

USER RIGHTS AND PRIVILEGES

Access as the root user (UID=0) bypasses all privilege checks.

15.1.2 Description of Privileges

The privileges that have been implemented in Samba-3.0.11 are shown be-

Table 16.1 Managing Directories with UNIX and Windows

Figure 16.1

of the immutible ag is NOT consistent with published documentation. For

16.3 Share De nition Access Controls

settings on the share itself the only way to create those settings is to use either the NT4 Server Manager or the Windows 200x Microsoft Management Console (MMC) for Computer Management. There are currently no plans to provide this capability in the Samba command-line tool set.

Samba stores the per-share access control settings in a file called `share_info.tdb`

16.5.3 Viewing File Ownership

Clicking on the **Ownership** button brings up a dialog box telling you who

Section

The second set of directory permissions has no real meaning in the UNIX permissions world and represents the inherited permissions that any le

If you wish to remove all permissions from a user/group/world component, you may either highlight the component and click on the **Remove** button or set the component to only have the special `Take Ownership` permission (displayed as O) highlighted.

16.5.6 Interaction with the Standard Samba \create mask" Parameters

There are four parameters that control interactiontrerd San

mass parameter:6 curityrmf crecuritymodes) -37[securitymmass huster crere51(ctorye)-38[securityrmodes

```
        security mask = 0777
        force security mode = 0
        directory security mask = 0777
        force directory security mode = 0
```

noticeably increased standardization on the UNIX world.,

ministration and thus adopts the limitations of POSIX ACLs. Therefore, where POSIX ACLs lack a capability of the Windows ACL, the

```
other::---              <-- perms applied to everyone else (other)
```

16.5.8.3 Mapping of Windows Directory ACLs to UNIX POSIX ACLs

Note

Table 16.4 Other Controls

Table 16.5 How Windows File ACLs Map to UNIX POSIX File ACLs

Windows ACE	File Attribute Flag

Chapter 17

Note

Sometimes it is necessary to disable locking control settings on the Samba server as well as on each MS Windows client!

17.2 Discussion

The second class of locking is the *deny modes*. These are set by an application when it opens a file to determine what types of access should be allowed

local locks, and discard read-ahead data. The break is then complete, the deferred open is granted, and the multiple processes can enjoy

bene t is worth the potential for delays. The following recommendations will help to characterize the environment where oplocks may be e ectively con gured.

Windows oplocks is a lightweight performance-enhancing feature. It is not a robust and reliable protocol. Every implementation of oplocks should

17.2.1.4 Slow and/or Unreliable Networks

The biggest potential performance improvement for oplocks occurs when the client-side caching of reads and writes delivers the most di erential over sending those reads and writes over the wire. This is most likely to occur when the network is extremely slow, congested, or distributed (as in a WAN). However, network latency also has a high impact on the reliability of the

Level1 Oplocks (also known as just plain \oplocks") is another term for opportunistic locking.

Level2 Oplocks provides opportunistic locking for a le that will be treated as

```
[acctdata]
        oplocks = False
        level2 oplocks = False
```

be enabled on a per-share basis, or globally for the entire server, in the `smb.conf` file as shown in Example 17.3.1.

Example 17.3.1 Share with Some Files Oplocked

in the past 3 years) and all attempts to reproduce the problem have

the con guration of the host server that is running Samba, and Samba itself.

Samba permits a most exible approach to network security. As far as possible Samba implements the latest protocols to permit more secure MS Windows le and print operations.

Samba can be secured from connections that originate from outside the local network. This can be done using *host-based protection*, using Samba's implementation of a technology known as \tcpwrappers," or it may be done be using *interface-based exclusion* so smbd will bind only to speci cally permitted interfaces. It is also possible to set speci c share- or resource-based exclusions, for example, on the *[IPC$]* autoshare. The *[IPC$]* share is used for browsing purposes as well as to establish TCP/IP connections.

Another method by which Samba may be secured is by setting Access Control Entries (ACEs) in an Access Control List (ACL) on the shares them-

```
        hosts deny = 0.0.0.0/0
```

Chapter 19

INTERDOMAIN TRUST RELATIONSHIPS

Samba-3 supports NT4-style domain trust relationships. This is a feature that many sites will want to use if they migrate to Samba-3 from an NT4-style domain and do not want to adopt Active Directory or an LDAP-based authentication backend. This chapter explains some background information regarding trust relationships and how to create them. Iardingwppossiblre

Samba-3 to trust NTtandrsa),d sd w sd to Samba-

on hef

bpW(in)28bindSmopdeppt
tme ppfalidfalidf hef

access rights to users in your domain. You will also need to enter a pass-

Section

server. In the /export/dfsroot directory, you set up your DFS links to other servers on the network.

```
root# cd /export/dfsroot
root# chown root /export/dfsroot
root# chmod 755 /export/dfsroot
root# ln -s msdfs:storageA\\shareA linka
root# ln -s msdfs:serverB\\share,serverC\\share linkb
```

Example 20.1.1 smb.conf with DFS Con gured

Chapter 21

book, Samba tolerates some spelling errors (such as *browseable* instead of *browsable*), and spelling is case-insensitive. It is permissible to use *Yes/No* or *True/False*

```
        lppause command =
        lpresume command =
        printer name =
        use client driver = No

[homes]

[printers]
        path = /var/spool/samba
        printable = Yes
```

You can easily verify which settings were implicitly added by Samba's default behavior. *Remember: it may be important in your future dealings with Samba.*

Note

The **testparm** in Samba-3 behaves di erently from that in 2.2.x: used without the \-v" switch, it only shows you the settings actually written into! To see the complete con guration used, .5.therameter.5.testparm.

ea49 Td 182-526-402(settings)qiiceas66(71la66(71lwc)28arno)30(r71l -69.2371lt),s74erson354(S71lext),s74er525ceeS71lva'stR belo9552 362190 =

```
root# testparm -v /etc/samba/smb.conf | egrep "(load printers)"
        load printers = Yes
```

be if you used this minimalistic con guration. Here is what you can expect to nd:

```
root# testparm -v smb.conf-minimal | egrep "(print|lpq|spool|driver|ports|[)"
 Processing section "[printers]"
 WARNING: [printers] service MUST be printable!
 No path in service printers - using /tmp

        lpq cache time = 10
        load printers = Yes
        printcap name = /etc/printcap
        disable spoolss = No
        enumports command =
        addprinter command =
        deleteprinter command =
        show add printer wizard = Yes
        os2 driver map =
        printer admin =
        min print space = 0
        max print jobs = 1000
        printable = No
        printing = bsd
        print command = lpr -r -P%p %s
        lpq command = lpq -P%p
        printer name =
        use client driver = No

 [printers]
        printable = Yes
```

testparm issued two warnings:

We did not specify the *[printers]*

Example 21.4.1 Extended BSD Printing Con guration

```
[global]
```

Section 21.4. Extended Printing Con guration

max print jobs

could regard this section as a convenient shortcut to share all printers with minimal con guration. It is also a container for settings that should apply

Section 21.4. Extended Printing Con guration

that have been placed into the Samba print spool directory for that printer. (That spool directory was, if you remember, set up with the *path*

%z | the size of the spooled print job (in bytes).

The print command must contain at least one occurrence of *%s* or *%f*. The *%p* is optional. If no printer name is supplied, the

9x/Me printer servers always have a *[printer$]* service that provides read-only access (with no password required) to support printer driver downloads.

Example 21.5.1 [print$] Example

```
[global]
 # members of the ntadmin group should be able to add   -
    drivers and set
```

Section

and driver properties for a queue that has this default NULL driver assigned. This will result in the following error message: \Device settings cannot be displayed. The driver for the speci ed printer is not installed, only spooler properties will be displayed. Do you want to install the driver now?"

Do *not* click on **Yes**! Instead, click on **No** in the error dialog. Now you will be presented with the printer properties window. From here, the way to assign a driver to a printer is open. You now have the choice of:

Select a driver from the pop-up list of installed drivers. Initially this list will be empty.

Click on **New Driver** to install a new printer driver (which will start up the APW).

Once the APW is started, the proceduc6s57(pro)457(starexact362(is)--457(pro)sam56(APW)as

```
[...]
```

After this command is complete, the les are in our current local directory. You probably have noticed that this time we passed several commands to the -c parameter, separated by semicolons. This ensures that all commands are executed in sequence on the remote Windows server before smbclient exits again.

Remember to repeat the procedure for the WIN40 architecture should you need to support Windows 9x/Me/XP clients. Remember too, the les for these architectures are in the WIN40/0/ subdirectory. Once this is complete, we can run smbclient. . .put to store the collected les on the Samba server's *[print$]* share.

21.6.2.3 Installing Driver Files into [print

Notice that there are already driver files present in the 2 subdirectory (probably from a previous installation). Once the files for the new driver are there too, you are still a few steps away from being able to use them on the clients.

error message. These become obvious. Other changes might install the driver les successfully but render the driver unworkable. So take care! Hints about the syntax of the adddriver command are in the man page. provides a more detailed description, should you need it.

21.6.2.6 Checking adddriver Completion

instaleed

6. At the bottom of the context menu select **Properties** (if the menu still

this step, you'll get a lot of help desk calls from your users, but maybe you like to talk to people.

21.8 Other Gotchas

Your driver is installed. It is now ready for Point'n'Print installation by the clients. You may have tried to download and use it on your first client machine, but wait. Let's make sure you are acquainted first with a few tips and tricks you may find useful. For example, suppose you did not set the

Tip

Try (on Windows 200x/XP) to run this command (as a user with the right privileges):

```
rundll32 printui.dll,PrintUIEntry /p /t3 /
n\\SAMBA-SERVER\printersharename
```

To see the tab with the **Printing Defaults** button (the one you need), also run this command:

```
rundll32 printui.dll,PrintUIEntry /p /t0 /
n\\SAMBA-SERVER\printersharename
```

To see the tab with the **Printing Preferences** button (the one that does not set systemwide defaults), you can start the commands from inside a DOS box or from **Start -> Run**.

```
 [Windows NT x86]
 Printer Driver Info 1:
   Driver Name: [infotec  IS 2075 PCL 6]

 Printer Driver Info 1:
   Driver Name: [DANKA InfoStream]

 Printer Driver Info 1:
   Driver Name: [Heidelberg Digimaster 9110 (PS)]

 Printer Driver Info 1:
   Driver Name: [dm9110]

 Printer Driver Info 1:
   Driver Name: [mydrivername]

 [....]


root# rpcclient SAMBA-CUPS -U root%secret -c 'enumprinters'
 cmd = enumprinters
   flags:[0x800000]
   name:[\\SAMBA-CUPS\dm9110]
   description:[\\SAMBA-CUPS\dm9110,,110ppm HiVolume DANKA Stuttgart]
   comment:[110 ppm HiVolume DANKA Stuttgart]
 [....]


root# rpcclient SAMBA-CUPS -U root%secret -c \
  'setdriver dm9110 "Heidelberg Digimaster 9110 (PS)"'
 cmd = setdriver dm9110 Heidelberg Digimaster 9110 (PPD)
 Successfully set dm9110 to driver Heidelberg Digimaster 9110 (PS).


root# rpcclient SAMBA-CUPS -U root%secret -c 'enumprinters'
 cmd = enumprinters
   flags:[0x800000]
   name:[\\SAMBA-CUPS\dm9110]
```

21.8.4 Error Message: \Cannot connect under a di erent Name"

Once you are connected with the wrong credentials, there is no means to reverse the situation other than to close all Explorer windows, and perhaps reboot.

> The net use *nn*SAMBA-SERVER*n*sharename /user:root gives you an error message: \Multiple connections to a server or a shared resource by the same user utilizing several user names are not allowed.

```
        Dependentfiles: [\\10.160.50.8\print$\W32X86\3\cns3407.dll]
        Dependentfiles: [\\10.160.50.8\print$\W32X86\3\CnS3G.cnt]
        Dependentfiles: [\\10.160.50.8\print$\W32X86\3\NBAPI.DLL]
        Dependentfiles: [\\10.160.50.8\print$\W32X86\3\NBIPC.DLL]
        Dependentfiles: [\\10.160.50.8\print$\W32X86\3\cpcview.exe]
        Dependentfiles: [\\10.160.50.8\print$\W32X86\3\cpcdspl.exe]
        Dependentfiles: [\\10.160.50.8\print$\W32X86\3\cpcedit.dll]
        Dependentfiles: [\\10.160.50.8\print$\W32X86\3\cpcqm.exe]
        Dependentfiles: [\\10.160.50.8\print$\W32X86\3\cpcspl.dll]
        Dependentfiles: [\\10.160.50.8\print$\W32X86\3\cfine32.dll]
        Dependentfiles: [\\10.160.50.8\print$\W32X86\3\cpcr407.dll]
        Dependentfiles: [\\10.160.50.8\print$\W32X86\3\Cpcqm407.hlp]
        Dependentfiles: [\\10.160.50.8\print$\W32X86\3\cpcqm407.cnt]
        Dependentfiles: [\\10.160.50.8\print$\W32X86\3\cns3ggr.dll]

        Monitorname: []
        Defaultdatatype: []

Printer Driver Info 3:
        Version: [2]
        Driver Name: [Canon iR5000-6000 PS3]
        Architecture: [Windows NT x86]
        Driver Path: [\\10.160.50.8\print$\W32X86\2\cns3g.dll]
        Datafile: [\\10.160.50.8\print$\W32X86\2\IR5000sg.xpd]
```

Section 21.8. Other Gotchas

Providing an installation client that will obtain printer drivers from a central Internet (or intranet) Imprints Server repository and install them on remote Samba and Windows NT4 print servers.

21.9.2 Creating Printer Driver Packages

1. rpcclient: Get the appropriate upload directory on the remote server.
2. smbclient: Upload the driver les.
3. rpcclient: Issues an AddPrinterDriver() MS-RPC.

rpcclient: Issues an AddPrinterEx() MS-RPC to actually create the printer.

One of the problems encountered when implementing the Imprints tool set was the namespace issues between various supported client architectures. For example, Windows NT includes a driver named \Apple LaserWriter II NTX v51.8", and Windows 95 calls its version of this driver \Apple Laser-Writer II NTX".

The problem is how to know what client drivers have been uploaded for a printer. An astute readerisd0s 89 (clienn)28(tT4a)-40s the Windows NT Printer

and so on). These parameters are passed on to Samba by the APW. If the addprinter command is designed in a way that it can create a new printer

using smbclient and rpcclient. See the Imprints installation client on the Imprints[6] web site for example. See also the discussion of rpcclient usage in Chapter 22, \CUPS Printing Support".

21.13 Publishing Printer Information in Active Directory or LDAP

This topic has also been addressed in Chapter 13, \Remote and Local Management: The Net Command". If you wish to volunteer your services to help document this further, please contact John H. Terpstra[7].

21.14 Common Errors

spool directory are typically restrictive to the owner and/or group. On the other hand, the Samba spool directory must be world writable, and should have the 't' bit set to ensure that only a temporary spool file owner can change or delete the file.

Depending on the type of print spooling system in use on the UNIX/Linux host, files that the spool management application finds and that are not currently part of job queue that it is managing can be deleted. This may explain the observation that jobs are spooled (by Samba) into this directory and just disappear.

Chapter 22

CUPS PRINTING SUPPORT

22.1 Introduction

22.1.1 Features and Bene ts

(or locally) via a Web browser (giving you platform-independent access to the CUPS print server). Additionally, it has the traditional command line and several more modern GUI interfaces (GUI interfaces developed by third parties, like KDE's overwhelming KDEPrint[2]).

CUPS allows creation of *raw* printers (i.e., no print file format translation) as well as *smart* printers (i.e., CUPS does file format conversion as required for

Example 22.2.2 Overriding Global CUPS Settings for One Printer

```
#application/octet-...
```

2. Do the same for the file /etc/cups/mime.convs.

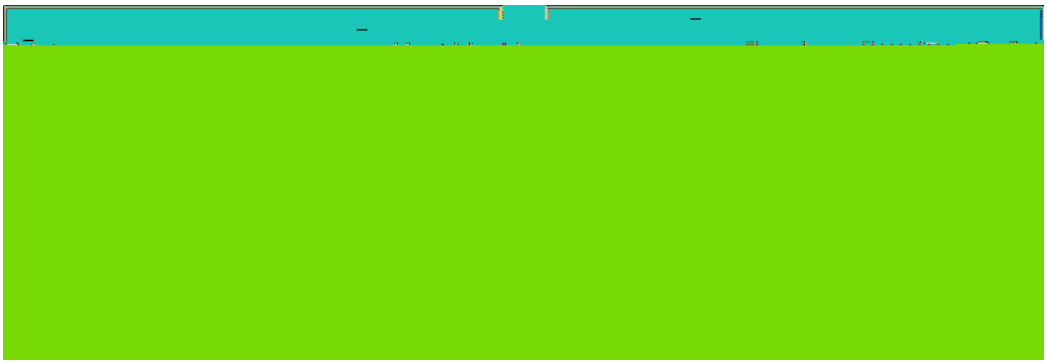
3. Add a raw printer using the Web interface. Point your browser at http://localhost:631

By default, you can only send other (known) MIME types \raw." Sending data \raw" means that CUPS does not try to convert them and passes them to the printer untouched.

This is all you need to know to get the CUPS/Samba combo printing \raw" les prepared by Windows clients, which have vendor drivers locally installed. If you are not interested in background information about more

 46rF50 8eiETq1 Td10.00.892 68

Figure 22.2 Printing to a PostScript Printer.



Tip

Use the \gs -h" command to check for all built-in \devices" on your Ghostscript version. If you specify a parameter of *-sDEVICE=png256*

Linuxprinting.org[5]. This uses the classical Ghostscript approach, doing ev-

Note

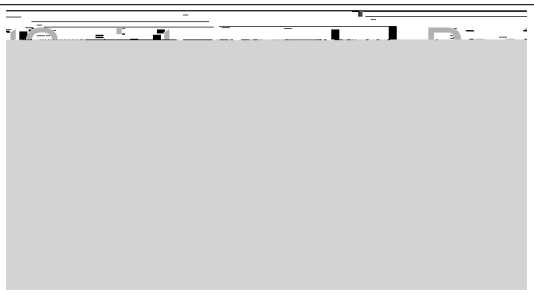
There is an important di erence between two similar MIME types in CUPS: one is *application/postscript*, the other is *application/vnd.cups-postscript*. While *application/postscript*

job

Figureinng4(CUPS)34(tong)33(F)-38ormngPostScript.67

application/vnd.cups-postscript; its output is application/vnd.cups-raster. This output format is not yet meant to be printable. Its aim is to serve as a general-purpose input format for more specialized *raster drivers* that are able to generate device-speci c printer data. This is shown in Figure 22.6.

Figure 22.6 PostScript to Intermediate Raster Format.



CUPS raster is a generic raster format with powerful features. It is able to include per-page information, color pro les, and more, to be used by the downstream raster drivers. Its MIME type is registered with IANA and its speci cation is, of course, completely open. It is designed to make it quite easy and inexpensive for manufacturers to develop Linux and UNIX raster drivers for their printer models should they choose to do so. CUPS always takes care of the rst stage of rasterization so these vendors do not need

Figure 22.8 Image Format to CUPS-Raster Format Conversion.

Figure 22.9

ipp This backend sends print les to IPP-connected network8(end)-415(send5s)-4worend5e1(sl

```
application/octet-stream
```

22.5.15 PostScript Printer Descriptions for Non-PostScript Print-

22.5.17 Examples for Filtering Chains

The le must rst pass the *pdftops*

The Gutenprint Project[8] (GPL, free software) provides around 140

Section

Figure 22.15 Printing via CUPS/Samba Server.

22.8.2 PPDs for Non-PS Printers on Windows

CUPS-PPDs can also be used on Windows clients, on top of a \core"

because until now there have been only two di erent PostScript drivers: the

Development Kit) for Windows NT (which used to be available at no cost to licensees of Visual Studio) includes the source code of the Microsoft driver, and licensees of Visual Studio are allowed to use and modify it for their

Section 22.10. Con guring CUPS for Driver Download

```
root# tar xvzf cups-samba-1.1.19.tar.gz
cups-samba.install
cups-samba.license
cups-samba.readme
cups-samba.remove
cups-samba.ss
```

the driver les from the normal download area of the ESP Print Pro software at Easy Software[14] web site. You need to locate the link labeled \SAMBA" among the **Download Printer Drivers for ESP Print Pro 4.x** area and download the package. Once installed, you can prepare any driver by simply highlighting the printer in the Printer Manager GUI and selecting **Export Driver...** from the menu. Of course, you need to have prepared Samba beforehand to handle the driver les; that is, set up the *[print$]* share, and so on. The ESP Print Pro package includes the CUPS driver les as well as

Note

Win 9x/Me clients will not work with the CUPS PostScript driver. For these you still need to use the ADOBE*.* drivers, as previously stated.

Note

It is not harmful if you still have the ADOBE*.* driver files from previous installations in the /usr/share/cups/drivers/ directory. The new **cupsaddsmb** (from 1.1.16) will automatically prefer its own drivers if it finds both.

Note

Should your Windows clients have had the old ADOBE*.* les for the Adobe PostScript driver installed, the download and installation of the new CUPS PostScript driver for Windows NT/200x/XP will fail at rst. You need to wipe the old driver from the clients rst. It is not enough to \delete" the printer, because the driver les will still

The CUPS PostScript driver supports the inclusion of the new *`*cupsJobTicket`*

```
 -c 'mkdir W32X86; \
 put /var/spool/cups/tmp/3e98bf2d333b5 W32X86/infotec_2105.ppd; \
put /usr/share/cups/drivers/cupsdrvr.dll W32X86/cupsdrvr.dll; \
 put /usr/share/cups/drivers/cupsui.dll W32X86/cupsui.dll; \
 put /usr/share/cups/drivers/cups.hlp W32X86/cups.hlp'
```

1. Call the CUPS server via IPP and request the driver files and the PPD file for the named printer.
2.

2. *Printer Driver infotec_2105 successfully installed.* # (for the WIN40 == Windows

22.10.15 Installing the PostScript Driver on a Client

After cupsaddsmb is completed, your driver is prepared for the clients to use. Here are the steps you must perform to download and install it via

you are treating your Ghostscript installation on your CUPS host with the output your client driver settings produce. Treat it well:

Avoid the PostScript Output Option: Optimize for Speed setting. Use

Section

rpcclient subcommands (adddriver and setdriver) need to encounter the following preconditions to complete successfully:

This installs a printer with the name *mysmbtstprn* to the CUPS system. The printer is accessed via a socket (a.k.a. JetDirect or Direct TCP/IP) connection. You need to be root for this step.

2. (Optional.) Check if the printer is recognized by Samba.

```
root# rpcclient -Uroot%xxxx -c 'enumprinters' localhost \
  | grep -C2 mysmbtstprn
flags:[0x800000]
name:[\\kde-bitshop\mysmbtstprn]
description:[\\kde-bitshop\mysmbtstprn,,mysmbtstprn]
```

```
sharename:[mysmbtstprn]
portname:[Samba Printer Port]
drivername:[]
comment:[mysmbtstprn]
location:[]
sepfile:[]
printprocessor:[winprint]

root# rpcclient -U root%xxxx -c 'getdriver mysmbtstprn' localhost
 result was WERR_UNKNOWN_PRINTER_DRIVER
```

None of the three commands shown above should show a driver. This

```
drivername:[mydrivername]

root# rpcclient -Uroot%xxxx -c 'getprinter mysmbtstprn 2' localhost \
  | grep -C4 driv
servername:[\\kde-bitshop]
printername:[\\kde-bitshop\mysmbtstprn]
sharename:[mysmbtstprn]
portname:[Done]
drivername:[mydrivername]
comment:[mysmbtstprn]
location:[]
sepfile:[]
printprocessor:[winprint]

root# rpcclient -U root%xxxx -c 'getdriver mysmbtstprn' localhost
[Windows NT x86]
Printer Driver Info 3:
     Version: [2]
     Driver Name: [mydrivername]
     Architecture: [Windows NT x86]
     Driver Path: [\\kde-bitshop\print$\W32X86\2\cupsdrvr.dll]
     Datafile: [\\kde-bitshop\print$\W32X86\2\mysmbtstprn.PPD]
     Configfile: [\\kde-bitshop\print$\W32X86\2\cupsui.dll]
     Helpfile: [\\kde-bitshop\print$\W32X86\2\cups.hlp]
     Monitorname: []
     Defaultdatatype: [RAW]
     Monitorname: []
     Defaultdatatype: [RAW]

root# rpcclient -Uroot%xxxx -c 'enumprinters' localhost \
   | grep mysmbtstprn
     name:[\\kde-bitshop\mysmbtstprn]
     description:[\\kde-bitshop\mysmbtstprn,mydrivername,mysmbtstprn]
     comment:[mysmbtstprn]
```

Compare these results with the ones from steps 2 and 3. Every one of these commands show the driver is installed. Even the enumprinters command now lists the driver on the \description" line.

11.

need to read a word. Just put it in a frame and bolt it to the wall with the heading "MY FIRST RPCCLIENT-INSTALLED PRINTER" |

22.12.3 Losing *.tdb Files

It is very important that all

22.13 CUPS Print Drivers from Linuxprinting.org

CUPS ships with good support for HP LaserJet-type printers. You can install the generic driver as follows:

```
root# lpadmin -p laserjet4plus -v parallel:/dev/lp0 -E -m laserjet.ppd
```

The `-m` switch will retrieve the `laserjet.ppd` from the standard repository for not-yet-installed PPDs, which CUPS typically stores in `/usr/share/cups/model`

Taylor already had in his database a respectable compilation of facts about many more printers and the Ghostscript \drivers" they run with. His idea, to generate PPDs from the database information and use them to make standard Ghostscript filters work within CUPS, proved to work very well.

Section

The host that sent the job (included since version 1.1.19)

```
my_PJL_stripping_filter
```

You will need to write a *my_PJL_stripping_filter* (which could be a shell

PreserveJobFiles Yes This keeps the job les themselves in cupsd's mind

and a *print command* = lp -d %P %s; rm %s may do what you need.

22.17 Printing from CUPS to Windows-Attached Printers

From time to time the question arises, how can you print *to* a Windows-attached printer *from* Samba? Normally the local connection from Windows host to printer would be done by USB or parallel cable, but this does not

Section

22.19.2 \cupsaddsmb" Keeps Asking for Root Password in Never-ending Loop

Have you set *security* = user? Have you used smbpasswd to give root a Samba account? You can do two things: open another terminal and execute smbpasswd -a root to create the account and continue entering the password into the rst terminal. Or, break out of the loop by pressing Enter twice (without trying to type a password).

If the error is \Tree connect failed: NT_STATUS_BAD_NETWORK_NAME", you may have forgotten to create the /etc/samba/drivers directory.

22.19.3 \cupsaddsmb" or \rpcclient addriver" Emit Error

If cupsaddsmb, or rpcclient addriver emit the error message WERR_ _

22.19.6 New Account Reconnection from Windows 200x/XP Troubles

Once you are connected as the wrong user (for example, as nobody, which often occurs if you have *map to guest* = bad user), Windows Explorer will not accept an attempt to connect again as a di erent user. There will not be any bytes transferred on the wire to Samba, but still you'll see a

22.19.9 Can't Use \cupsaddsmb" on Samba Server, Which Is a PDC

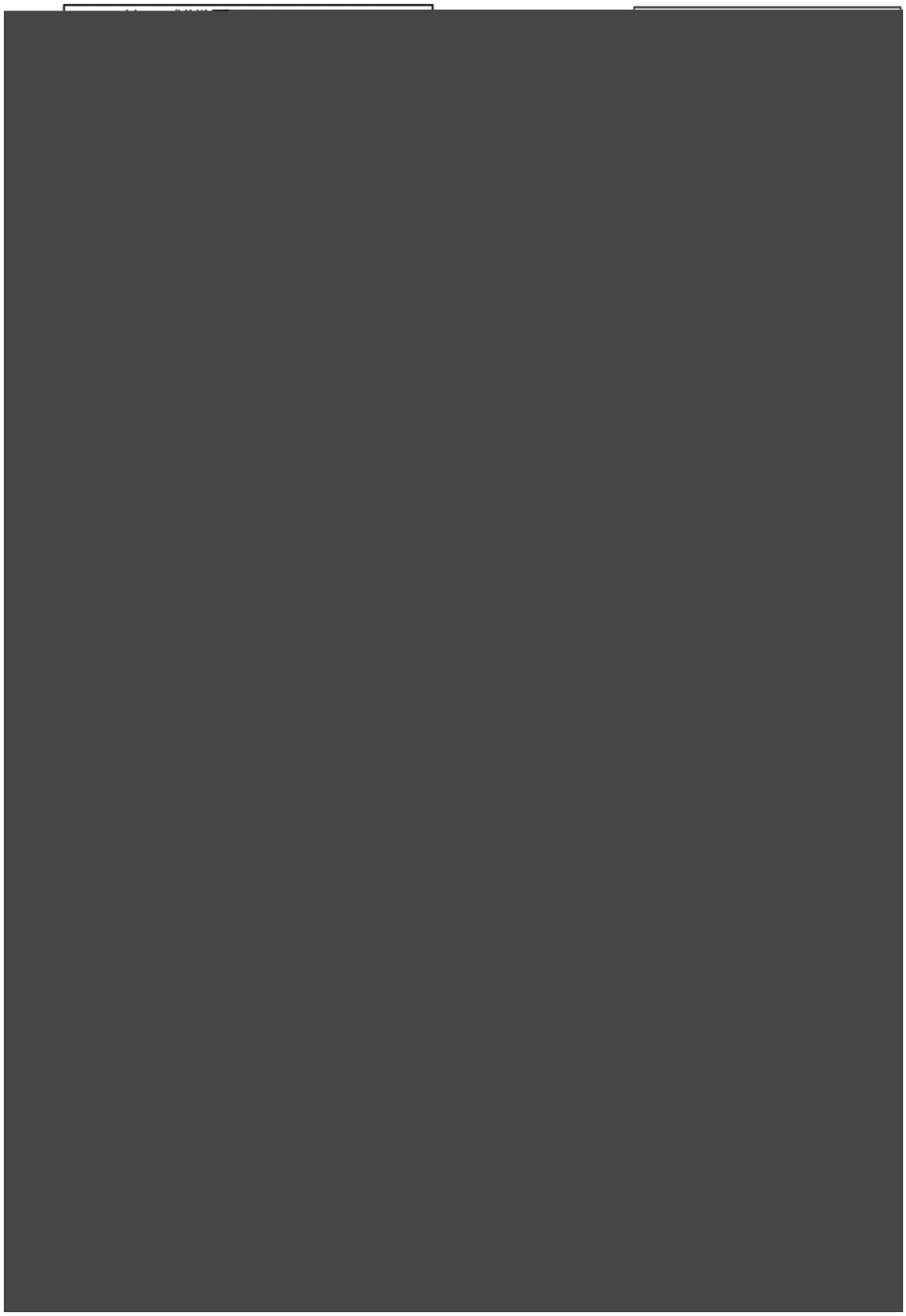
(a) Open the **Printers** folder.

(b) Right-click on the printer (**remoteprinter on cupshost**) and select the context menu **Properties**.

(c) Click on the **Advanced** tab. (If everything is \grayed out," then you are not logged in as a user with enough privileges).

(d)

Figure 22.19 CUPS Printing Overview.



Chapter 23

STACKABLE VFS MODULES

23.1 Features and Bene ts

Stackable VFS (Virtual File System) modules support was new to Samba-3Sarovenquiteopular. SambapasseshtoSccess
UNIX le system through the loaded VFS modules. This chapter covers the modules that come with the Samba source and provides references to some external modules.

23.2 Discussion

If not supplied with your platform distribution binary Samba package, you

mypre x:uid nolimit This parameter takes a boolean argument that specifies if the stored default quota values also be reported for the user record, or if the value NO_LIMIT should be reported to the windows client for the user specified by the *prefix:uid* parameter.

The default value is yes (which means to report NO_LIMIT). An example of use is shown here:

```
vfs objects = default_quota:myprefix
myprefix:   uid nolimit = no
```

mypre x:gid

```
vfs objects = default_quota:quotasettings
quotasettings: uid nolimit = no
quotasettings: gid = 65534
quotasettings: gid nolimit = no
...
```

23.3.3 extd_audit

This module is identical with the audit module above except that it sends audit logs to both syslog as well as the smbd log files. The *log level* for this module is set in the smb.conf file.

An example of detailed per-user and per-machine logging can be obtained by setting *log file* = /var/log/samba/%U.%m.log.

Auditing information often must be preserved for a long time. So that the log files do not get rotated it is essential that the *max log size* = 0 be set in the `smb.conf` file.

23.3.4 fake_perms

This module was created to allow Roaming Profiles files and directories to be set (on the Samba server under UNIX) as read only. This module will, if installed on the Profiles share, report to the client that the Profile files and

23.4 VFS Modules Available Elsewhere

This section contains a listing of various other VFS modules that have been posted but do not currently reside in the Samba CVS tree for one reason or another (e.g., it is easy for the maintainer to have his or her own CVS tree).

No statements about the stability or functionality of any module should be implied due to its presence here.

23.4.1 DatabaseFS

URL: Taylors University DatabaeFS[10]

By Eric Lorimer.[11]

23.4.3 vscan-clamav

Samba users have been using the RPMS from SerNet without a problem.

```
; if communication to clamd fails, should access to file denied?
; (default: yes)
deny access on error = no

; if daemon failes with a minor error (corruption, etc.),
; should access to file denied?
; (default: yes)
deny access on minor error = no

; 5(accew5(eu2m2wcg-525(on525ag525(filviccew5(eWindow(if)-52f25(shoul5(to)-525(file)-525(
```

```
; socket name of clamd (default: /var/run/clamd). Setting will be ignored if
; libclamav is used
clamd socket name = /tmp/clamd

; limits, if vscan-clamav was build for using the clamav library (libclamav)
; instead of clamd

; maximum number of files in archive (default: 1000)
libclamav max files in archive = 1000

; maximum archived file size, in bytes (default: 10 MB)
libclamav max archived file size = 5242880

; maximum recursion level (default: 5)
libclamav max recursion level = 5
```

Obviously, a running clam daemon is necessary for this to work. This is a working example for me using ClamAV. The ClamAV documentation should provide additional con guration examples. On your system these may be located under the /usr/share/doc/ directory. So

Chapter 24

24.2 Introduction

It is well known that UNIX and Microsoft Windows NT have different models for representing user and group information and use different technologies for implementing them. This fact has made it difficult to integrate the two systems in a satisfactory manner.

One common solution in use today has been to create identically named user accounts on both the UNIX and Windows systems and use the Samba suite of programs to provide file and print services between the two. This solution is far from perfect, however, because adding and deleting users on both sets

the lookup. Because Winbind hooks into the operating system at a low level (via the NSS name resolution modules in the C library), this redirection to the NT domain controller is completely transparent.

```
root# ln -s /usr/lib/libnss_winbind.so /usr/lib/nss_winbind.so.2
```

As root, edit /etc/nsswitch.conf to allow user and group entries to be visible from the winbindd daemon. My /etc/nsswitch.conf le looked like this after editing:

```
passwd:     files winbind
shadow:     files
group:      files winbind
```

The libraries needed by the winbindd

Note

Before attempting to join a machine to the domain, verify that Samba is running on the target domain controller (usually PDC) and that it is capable of being reached via ports 137/udp, 135/tcp, 139/tcp, and 445/tcp (if Samba or Windows Server 2Kx).

The use of the net rpc join facility is shown here:

```
root# /usr/local/samba/bin/net rpc join -S PDC -U Administrator
```

The proper response to the command should be \Joined the domain *DOMAIN*" where *DOMAIN* is your domain name.

24.5.3.5 Starting and Testing the winbindd Daemon

Eventually, you will want to modify your Samba startup script to automatically invoke the winbindd daemon when the other parts of Samba start, but it is possible to test out just the Winbind portion rst. To start up Winbind services, enter the following command as root:

```
root# /usr/local/samba/sbin/winbindd
```

Use the appropriate path to the location of the winbindd executable le.

You can do the same sort of thing to get group information from the PDC:

```
root# /usr/local/samba/bin/wbinfo -g
CEO\Domain Admins
CEO\Domain Users
CEO\Domain Guests
CEO\Domain Computers
CEO\Domain Controllers
CEO\Cert Publishers
CEO\Schema Admins
CEO\Enterprise Admins
CEO\Group Policy Creator Owners
```

The function

```
        echo -n $"Shutting down $KIND services: "
        killproc smbd
        RETVAL=$?
        echo
        KIND="NMB"
        echo -n $"Shutting down $KIND services: "
        killproc nmbd
        RETVAL2=$?
        echo
        KIND="Winbind"
        echo -n $"Shutting down $KIND services: "
        killproc winbindd
        RETVAL3=$?
        [ $RETVAL -eq 0 -a $RETVAL2 -eq 0 -a $RETVAL3 -eq 0 ] && \
       rm -f /var/lock/subsys/smb
        echo ""
        return $RETVAL
}
```

Solaris Winbind does not work on Solaris 9; see Section 43.6.2 for details.

in the script above with:

```
/usr/local/samba/sbin/winbindd -D rtingD
```

```
#
#ident "@(#)pam.conf 1.14 99/09/16 SMI"
#
# Copyright (c) 1996-1999, Sun Microsystems, Inc.
# All Rights Reserved.
#
# PAM configuration
#
# Authentication management
#
login   auth required   /usr/lib/security/pam_winbind.so
login auth required  /usr/lib/security/$ISA/pam_unix.so.1 try_first_pass
login auth required  /usr/lib/security/$ISA/pam_dial_auth.so.1 try_first_pass
#
rlogin  auth sufficient /usr/lib/security/pam_winbind.so
rlogin  auth sufficient /usr/lib/security/$ISA/pam_rhosts_auth.so.1
rlogin auth required  /usr/lib/security/$ISA/pam_unix.so.1 try_first_pass
#
dtlogin auth sufficient /usr/lib/security/pam_winbind.so
dtlogin auth required  /usr/lib/security/$ISA/pam_unix.so.1 try_first_pass
#
rsh auth required /usr/lib/security/$ISA/pam_rhosts_auth.so.1
other   auth sufficient /usr/lib/security/pam_winbind.so
other auth required /usr/lib/security/$ISA/pam_unix.so.1 try_first_pass
#
# Account management
#
login   account sufficient      /usr/lib/security/pam_winbind.so
login account requisite /usr/lib/security/$ISA/pam_roles.so.1
login account required /usr/lib/security/$ISA/pam_unix.so.1
#
dtlogin account sufficient      /usr/lib/security/pam_winbind.so
dtlogin account requisite /usr/lib/security/$ISA/pam_roles.so.1
dtlogin account required /usr/lib/security/$ISA/pam_unix.so.1
#
other   account sufficient      /usr/lib/security/pam_winbind.so
other account requisite /usr/lib/security/$ISA/pam_roles.so.1
other account required /usr/lib/security/$ISA/pam_unix.so.1
#
```

following, it all works ne."

```
root# wbinfo -u
MIDEARTH\maryo
MIDEARTH\jackb
MIDEARTH\ameds
...
MIDEARTH\root

root# wbinfo -g
MIDEARTH\Domain Users
MIDEARTH\Domain Admins
MIDEARTH\Domain Guests
...
MIDEARTH\Accounts

root# getent passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/bin/bash
...
maryo:x:15000:15003:Mary Orville:/home/MIDEARTH/maryo:/bin/false
```

\But the following command just fails:"

```
root# chown maryo a_file
chownphown
```

\This is driving me nuts! What can be wrong?"

Same problem as the one above. Your system is likely running **nscd**, the

Chapter 25

ADVANCED NETWORK MANAGEMENT

This section documents peripheral issues that are of great importance to network administrators who want to improve network resource access control, to automate the user environment, and to make their lives a little easier.

25.1 Features and Bene ts

Often the di erence between a working network environment and a well-appreciated one can best be measured by the *little things* that make everything work more harmoniously. A key part of every network environment solution is the ability to remotely manage MS Windows workstations, remotely access the Samba server, provide customized logon scripts, as well

Microsoft distributes a version of these tools called `Nexus.exe` for installa-

Section 25.3. Remote Desktop Management

Now the best thing for last: All the core compression and caching technologies are released under the GPL and available as source code to anybody who wants to build on it! These technologies are working, albeit started from the command line only (and very inconvenient to use in order to get a fully running remote X session up and running).

To answer your questions:

Section

Example 25.4.1 Script to Enforce Single Resource Logon

```
#!/bin/bash

IFS="-"
RESULT=$(smbstatus -S -u $1 2> /dev/null | awk 'NF \
```

Chapter 26

SYSTEM AND ACCOUNT POLICIES

will appear in the Start menu). An additional new feature is the ability to make available particular software Windows applications to particular users and/or groups.

Remember, NT4 policy files are named `NTConfig.POL` and are stored in the

26.4.2 Windows NT4/200x

The tools that mabNT4o0(to)-28

6. An ordered list of user GPOs is obtained. The list contents depends

Chapter 27

DESKTOP PROFILE MANAGEMENT

Before discussing how to con gure roaming pro les, it is useful to see how Windows 9x/Me and Windows NT4/200x clients implement these features.

Windows 9x/Me clients send a NetUserGetInfo request to the server to get the user's pro les location. However, the response does not have room for a separate pro les locatione

Note

Section 27.2. Roaming Pro les

618

3. Click on the **User Pro les** tab.
4.

```
Computer Configuration\Administrative Templates\System\User Profiles\
```

Note

Note

Be careful with group profiles. If the user who is a member of a group also has a personal profile, then the result

2. If the user account has a pro le path, but at its location a pro- le does not exist, then a new pro le is created in the %System-Root%\Profiles\%USERNAME% directory from reading the Default User pro le.
3. If the NETLOGON share on the authenticating server (logon server) contains a policy le (NTConfig.POL), then its contents are applied to the NTUser.DAT

```
\Microsoft
   \Windows
      \CurrentVersion
         \Explorer
```

27.5.3 MS Windows 200x/XP

Note

MS Windows XP Home Edition does use default per-user pro les, but cannot participate in domain security, cannot log onto an NT/ADS-style domain, and thus can obtain the pro le only from itself. While there are bene ts in doing this, the beauty of those MS Windows clients that can participate in domain logon processes is that they allow the administrator to create a global default pro le and enforce it through the use of Group Policy Objects (GPOs).

When a new user rst logs onto an MS Windows 200x/XP machine, the default pro le is obtained from

If a default profile does not exist in this location, then MS Windows 200x/XP will use the local default profile.

On logging out, the user's desktop profile is stored to the location specified in the registry settings that pertain to the user. If no specific policies have been created or passed to the client during the login process (as Samba does automatically), then the user's profile is written to the local machine only under the path `C:\Documents and Settings\%USERNAME%`.

Those wishing to modify the default behavior can do so through these three methods:

Section

In this case, the local cache copy is deleted on logout.

27.6 Common Errors

The following are some typical errors, problems, and questions that have been asked on the Samba mailing lists.

27.6.1 Con guring Roaming Pro les for a Few Users or Groups

With Samba-2.2.x, the choice you have is to enable or disable roaming pro-
les suppe23(y013iG7333Iat)-429(is)4The isto haveroaming
the fadisableldtrne,thneshayeroamingt.gfeenabld-
you andto mca thne tosme mca
With (Samba3e),-99(u Pro le)-99(su(ppe23(y01e)-99((is)-99(no1e)-99(wa)87any)28teds,)-154itu)-9

Chapter 28

PAM-BASED DISTRIBUTED AUTHENTICATION

This chapter should help you to deploy Winbind-based authentication on any PAM-enabled UNIX/Linux system. Winbind can be used to enable user-level application access authentication from any MS Windows NT domain, MS Windows 200x Active Directory-based domain, or any Samba-based

facility to provide all authentication, authorization, and resource control services. Prior to the introduction of PAM, a decision to use an alternative to the system password database (`/etc/passwd`) would require the provision

ones. As of Linux-PAM v0.60, this control- ag can be de ned with one of two syntaxes.

The simpler (and historical) syntax for the control- ag is a single keyword de ned to indicate the severity of concern associated with the success or failure of a speci c module. There are four such keywords: *required*, *requisite*, *sufficient*, and *optional*.

ok: This tells PAM that the administrator thinks this return code should contribute directly to the return code of the full stack of modules. In other words, if the former state of the stack would lead to a return of PAM_SUCCESS, the module's return code will

given module path is appended to the default module path: `/lib/security` (but see the previous notes).

The arguments are a list of tokens that are passed to the module when it is invoked, much like arguments to a typical Linux shell command. Generally, valid arguments are optional and are specific to any given module. Invalid arguments are ignored by a module; however, when encountering an invalid argument, the module is required to write an

28.2.2.1 PAM: Original Login Con g

The following example for the login program replaces the use of the pam_pwdb.so module that uses the system password database (/etc/passwd, /

```
#%PAM-1.0
# The PAM configuration file for the samba service
#
auth       required     pam_smbpass.so nodelay
account    required     pam_pwdb.so audit nodelay
session    required     pam_pwdb.so nodelay
```

= yes. The reason is that PAM modules cannot support the challenge/response authentication mechanism needed in the presence of SMB password encryption.

Default: *obey pam restrictions* = no

650

```
#%PAM-1.0
# kdc-pdc
#
auth       requisite   pam_nologin.so
auth       requisite   pam_krb5.so
```

see if things work. If they do, look at /etc/pam.d/system-auth and copy only what you need from it into your /etc/pam.d/login file. Alternatively, if you want all services to use Winbind, you can put the Winbind-specific stuff in /etc/pam.d/system-auth.

Section 28.3. Common Errors

system. Likewise, many UNIX and Linux administrators have not been

At this point, it will be possible to ping any MS Windows machine by its

lations where the system administrator traditionally determines in the /etc/hosts

lowed, the precise nature of which is dependent on how the NetBIOS Node Type parameter is con gured. A Node Type of 0 means that NetBIOS broadcast (over UDP broadcast) is used if the name that is the subject of a name lookup is not found in the NetBIOS name cache. If that fails, then DNS, HOSTS, and LMHOSTS are checked. If set to Node Type 8, then a NetBIOS Unicast (over UDP Unicast) is sent to the WINS server to obtain a lookup before DNS, HOSTS, LMHOSTS, or broadcast lookup is used.

29.4.5 WINS Lookup

Chapter 30

Chapter 31

BACKUP TECHNIQUES

31.1 Features and Bene ts

A useful Web site I recently stumbled across that you might like to refer to is located at www.allmerchants.com[1].

The following three free software projects might also merit consideration.

31.2.1 BackupPC

checksum-search algorithm described in the technical report that accompanies the rsync package.

Chapter 32

HIGH AVAILABILITY

32.1 Features and Bene ts

CIFS/SMB (the Windows networking protocols) uses TCP connections.

This means that from a basic design perspective, failover is not seriously considered.

{ All current SMB clusters are failover solutions | they rely on the clients to reconnect. They provide server failover, but clients can lose information due to a server failure.

Servers keep state information about client connections.

{

32.2.2.5 Server Pool Communications

Most backend le systems support POSIX le semantics. This makes it

32.2.3 A Simple Solution

Allowing failover servers to handle di erent functions within the exported le system removes the problem of requiring a distributed locking protocol.

If only one server is active in a pair, the need for high-speed server interconnect is avoided. This allows the use of existing high-availability solutions,

32.2.5 MS-DFS: The Poor Man's Cluster

MS-DFS links can be used to redirect clients to disparate backend servers. This pushes complexity back to the network client, something already included by Microsoft. MS-DFS creates the illusion of a simple, continuous le system name space that works even at the le level.

Above all, at the cost of complexity of management, a distributed system (pseudo-cluster) can be created using existing Samba functionality.

32.2.6 Conclusions

Chapter 34

Example 34.1.2 CDROM Server smb-cdserver.conf le

35.1.1 Upgrading from Samba-3.0.x to Samba-3.2.0

35.1.2 Upgrading from Samba-2.x to Samba-3.0.25

This chapter deals exclusively with the differences between Samba-3.0.25 and Samba-2.2.8a. It points out where configuration parameters have changed,

Section 35.2. New Featuers in Samba-3.x Series

- add machine script
- add user to group script
- algorithmic rid base
- delete group script
- delete user from group script
- passdb backend
- rename user script
- set primary group script
- username map script

Authentication

- auth methods
- ldap password sync
- passdb expand explicit
- realm

Protocol Options

- add port command
- afs token lifetime
- client lanman auth
- client NTLMv2 auth
- client schannel
- client signing
- client use spnego
- defer sharing violations
- disable netbios
- dmapi support
- enable privileges
- use kerberos keytab

kernel change notify

mangle pre x

map acl inherit

map read only

max stat cache size

msdfs proxy

open les database hash size

set quota command

store dos attributes

use send le

usershare allow guests

usershare max shares

usershare owner only

usershare path

usershare pre x allow list

usershare pre x deny list

usershare template share

vfs objects

Printing

cups options

cups server

force printername

iprint server

max reported print jobs

printcap cache time

Unicode and Character Sets

display charset

35.2.3 New Functionality

The major changes in behavior since the Samba-2.2.x series are documented in this chapter. The [illegible]

The old sambaAccount

Chapter 36

MIGRATION FROM NT4 PDC TO SAMBA-3 PDC

This is a rough guide to assist those wishing to migrate from NT4 domain control to Samba-3-based 59(NT4).549 r(Sam)28r.(C)]TJ/7 12.951491 Tf 044.16549 Td 36.1PDPlannshingrt

Before attempting a migration to a Samba-3-controlled network, make every possible e ort to gain all-round commitment to the change. Know precisely

The Account Migration Process

1. Create a BDC account in the old NT4 domain for the Samba server using NT Server Manager. *Samba must not be running.*

2. `net rpc join -S` *`NT4PDC`* `-w` *`DOMNAME`* `-U Administrator%`*`passwd`*

3. `net rpc vampire -S` *`NT4PDC`* `-U administrator%`*`passwd`*

4. `pdbedit -L` Note: Did the users migrate?

5. Now assign each of the UNIX groups to NT groups: (It may be useful to copy this text to a script called `initGroups.sh`)

```
#!/bin/bash
#### Keep this as a shell script for future re-use

# First assign well known domain global groups
net groupmap add ntgroup="Domain Admins" unixgroup=root rid=512 type=d
net groupmap add ntgroup="Domain Users"  unixgroup=users rid=513 type=d
net groupmap add ntgroup="Domain Guests" unixgroup=nobody rid=514 type=d

# Now for our addedoups
```

Add/Delete Groups: Note OS limits on size and nature. Linux limit is 16 char, no spaces, and no uppercase chars (groupadd).

Chapter 37

37.2.1.1 Locating the SWAT File

```
   # swat is the Samba Web Administration Tool
   swat stream tcp nowait.400 root /usr/sbin/swat swat
```

A control file for the newer style xinetd could be:

```
# default: off
# description: SWAT is the Samba Web Admin Tool. Use swat \
#              to configure your Samba server. To use SWAT, \
#              connect to port 901 with your favorite web browser.
service swat
{
   port    = 901
```

As long as you log onto SWAT as the user *root*, you should obtain full change and commit ability. The buttons that will be exposed include **HOME**, **GLOBALS**, **SHARES**, **PRINTERS**, **WIZARD**, **STATUS**, **VIEW**, and **PASSWORD**.

37.2.3 Securing SWAT through SSL

Many people have asked about how to set up SWAT with SSL to allow for secure remote administration of Samba. Here is a method that works, courtesy of MarkuMaKrieger.TJ 0 -1321.671d [(Mano28(oudi cion)-s333(of)-463(of)n671d [hl671d-0 10a3-35

The **Edit** button permits the editing (setting) of the minimal set of options that may be necessary to create a working Samba server.

Finally, there are a limited set of options that determine what type of serv Samba will be con gured for, whether it will be a WINS server, participate

Chapter 38

THE SAMBA CHECKLIST

38.1 Introduction

Example 38.2.1 smb.conf with [tmp] Share

Section 38.7.e

Note

Example 38.3.2 Con guration for Allowing Connections from a Certain Subnet and localhost

7. Run the command **smbclient //BIGSERVER/TMP**. You should

To overcome it, you could do one of the following (you only need to choose one of them):

(a) Fix the nmbd installation.

(b) Add the IP address of BIGSERVER to the wins server box in the advanced TCP/IP setup on the PC.

(c) Enable Windows name resolution via DNS in the advanced section of the TCP/IP setup.

(d) Add BIGSERVER to your lmhosts le on the PC.

If you get a message \invalid network name" or \bad password error," then apply the same xes as for the

Section

Chapter 39

Always remember that the developers are volunteers; they are not paid and they never guarantee to produce a particular feature at a particular time. Any timelines are \best guess," and nothing more.

39.4 How to Get O the Mailing Lists

To have your name removed from a Samba mailing list, go291 3 92 6499Lists

Chapter 40

REPORTING BUGS

40.1 Introduction

Please report bugs using Samba's Bugzilla[1] facilities and take the time to

Run testparm to check your con g le for correct syntax.

Have you looked through Chapter 38, \The Samba Checklist"? This is extremely important.

If you include part of a log le with your bug report, then be sure to annotate it with exactly what you were doing on the client at the time and exactly what the results were.

40.3 Debug Levels

40.3.1 Debugging-Speci c Operations

Samba-3.x permits debugging (logging) of speci c functional components without unnecessarily cluttering the log les with detailed logs for all oper-

You should also detail how to reproduce the problem, if possible. Please make this reasonably detailed.

You may also find that a core file appeared in a `corefiles` subdirectory

Chapter 41

MANAGING TDB FILES

41.1 Features and Bene ts

Samba uses a lightweight database called Trivial Database (tdb) in which it stores persistent and transient data. Some tdb les can be disposed of before restarting Samba, but others are used to store information that is vital to Samba con guration and behavior. The following information is provided to help administratout har1(ae-485(hseekng)-444(to)-485(h)-27(e)ter)-385(hmanage-444(toheir]T ptem adpplianceeould-3975ado-3975aeell-3975ato-367(atak)7(e)-467(anote-3975atat)-4975atb a014les

```
myserver# > cd /var/lib/samba
myserver@ > tdbbackup *.tdb
```

The default extension is .bak

Table 41.1 Samba's Trivial Database Files

brlock8(w)-se.datTJETq1 0 0 1 1542.879 562110 09mÎ0 d 0 J 0.398 w 0 0 m 0 13.549 l SOBT/F15 10.9091 Tf 7968.655 58052.504d

Chapter 42

HOW TO COMPILE SAMBA

You can obtain the Samba source le from the Samba Web site[1]. To obtain a development version, you can download Samba from Subversion or using rsync.

42.1 Access Samba Source Code via Subversion

42.1.1 Introduction

Samba is developed in an open environment. Developers use a Subversion to \checkin" (also known as \commit") new source code. Samba's various Subversion branches can be accessed via anonymous Subversion using the instructions detailed in this chapter.

This chapter is a modi ed version of the instructions found at the Samba[2] Web site.

42.1.2 Subversion Access to samba.org

The machine samba.org runs a publicly accessible Subversion repository for access to the source code of several packages, including Samba, rsync, distcc,

42.1.2.1 Access via ViewCVS

You can access the source code via your favorite WWW browser. This allows

Section 427 [TJ ET 1 0 0 1 72 595.33 cm [(y)] TJ 1 0 0 1 72 595.33 cm [(y)] TJ 1 0 0 1 72 595.33 cm [(y)] TJ

```
$ wget http://us1.samba.org/samba/ftp/samba-pubkey.asc
```

The first file is the PGP signature for the Samba source file; the other is the

As you can see from this, building and installing Samba does not need to result in disaster!

Section

Note

If you use the SVR4-style init system, you may like to look at the `examples/svr4-startup` script to make Samba

Chapter 43

PORTABILITY

If you have a mix of jfs and jfs2 lesystems on the same host, simply use both ioo commands.

43.6 Solaris

43.6.1 Locking Improvements

Some people have been experiencing problems with F_

Chapter 44

SAMBA AND OTHER CIFS CLIENTS

This chapter contains client-speci c information.

44.1 Macintosh Clients

Yes. Thursby[1] has a CIFS client/server called DAVE[2]. They test it against Windows 95, Windows NT/200x/XP, and Samba for compatibility issues. At the tir549 Td l SQBT/F1eh5 Td [oetSa551]TJ/729 7.9701 w-508a(t)14 Ta(tir549vJ/72ers.95tir5495.14(

44.2 OS2 Client

44.2.1 Con guring OS/2 Warp Connect or OS/2 Warp 4

Basically, you need three components:

```
20=netwksta.sys
20=netvdd.sys
```

44.4.1 Speed Improvement

Section

Chapter 45

SAMBA PERFORMANCE TUNING

45.1 Comparisons

The Samba server uses TCP to talk to the client, so if you are trying to see if it performs well, you should really compare it to programs that use the same protocol. The most readily available programs for le transfer that

45.4 Max Xmit

At startup the client and server negotiate a *maximum transmit* size, which limits the size of nearly all SMB commands. You can set the maximum size that Samba will negotiate using the *max xmit* option in `smb.conf`. Note that this is the maximum size of SMB requests that Samba will accept, but not the maximum size that the client will accept. The client maximum receive size is sent to Samba by the client, and Samba honors this limit.

It defaults to 65536 bytes (the maximum), but it is possible that some clients

Chapter 46

LDAP AND TRANSPORT LAYER SECURITY

46.1 Introduction

Up until now, we have discussed the straightforward con guration of OpenLDAP™, with some advanced features such as ACLs. This does not however, deal with the fact that the network transmissions are still in plain text. This is where *Transport Layer Security (TLS)* comes in.

OpenLDAP™ clients and servers are capable of using the Transport Layer Security (TLS) framework to provide integrity and con dentiality protec-

802

804

```
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:AU
State or Province Name (full name) [Some-State]:NSW
Locality Name (eg, city) []:Sydney
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Abmas
Organizational Unit Name (eg, section) []:IT
Common Name (eg, YOUR name) []:ldap.abmas.biz
Email Address []:support@abmas.biz

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
```

```
stateOrProvinceName       = NSW
localityName              = Sydney
organizationName          = Abmas
```

Chapter 47

Section

Chapter 48

DNS AND DHCP CONFIGURATION GUIDE

48.1 Features and Bene ts

There are few subjects in the UNIX world that might raise as much contention as Domain Name System (DNS) and Dynamic Host Con guration

```
   multiple-cnames yes;
   listen-on {
      mynet;
      };
};

# The following three zone definitions do not need any modification.
# The first one defines localhost while the second defines the
# reverse lookup for localhost. The last zone "." is the
# definition of the root name servers.

zone "localhost" in {
   type master;
   file "localhost.zone";
};

zone "0.0.127.in-addr.arpa" in {
   type master;
   file "127.0.0.zone";
};

zone "." in {
   type hint;
   file "root.hint";
};

# You can insert further zone records for your own domains below.

zone "quenya.org" {
   type master;
   file "/var/named/w.

      fynet;};
falowi-transfr z
   fynet;
   };
```

```
   };

zone "1.168.192.in-addr.arpa" {
   type master;
   file "/var/named/192.168.1.0.rev";
   allow-query {
      mynet;
   };
   allow-transfer {
      mynet;
   };
   allow-update {
      mynet;
   };
};
```

The following les are all located in the directory /var/named. This is the /var/named/localhost.zone

```
                1W )            ; minimum

                IN NS           localhost.
```

```
1                       PTR     frodo.quenya.org.
2                       PTR     marvel.quenya.org.
```

The con guration les shown here were copied from a fully working system.

Appendix A

GNU GENERAL PUBLIC LICENSE VERSION 3

Version 3, 29 June 2007

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source xed on a durable physical medium customarily used for software interchange.

b Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written o er, valid for at least three years and valid for as long as you o er spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no

operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented

d Limiting the use for publicity purposes of names of licensors or authors of the material; or

e Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f

arrange, in a manner consistent with the requirements of this License, to

for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU A ero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of

How to Apply These Terms to Your New Programs

propriate parts of the General Public License. Of course, your program's commands might be di erent; for a GUI interface, you would use an \about box".

You should also get your employer (if you work as a programmer) or school, if any, to sign a \copyright disclaimer" for the program, if necessary. For more information on this, and how to apply and follow the GNU GPL, see <http://www.gnu.org/licenses/>.

GLOSSARY

Access Control List (ACL)

A detailed list of permissions granted to users or groups with respect to le and network resource access. See Chapter 16, \File, Directory, and Share Access Controls", for details.

Active Directory Service (ADS)

A service unique to Microsoft Windows 200x servers that provides a centrally managed directory for management of user identities and

SUBJECT INDEX

Subject Index