The O□cial Samba-3 HOWTO and Reference Guide

Jelmer R. Vernooij, John H. Terpstra, and Gerald (Jerry) Carter

March 21, 2007

ABOUT THE COVER ARTWORK

The cover artwork of this book continues the freedom theme of the first

take the time to think through what may lie ahead. Above all, take stock of the freedom of choice that Samb355(374(m))1(at)T4(macod1es355(S)in4(m))1ygh-354(Arw7(

ATTRIBUTION

Chapter 1, “How to Install and Test SAMBA”

- Andrew Tridgell <

Chapter 10, “Network Browsing”

Chapter 14, “Identity Mapping (IDMAP)”

- John H. Terpstra <jht@samba.org[41]>

Chapter 15, “User Rights and Privileges”

- Gerald (Jerry) Carter <jerry@samba.org[42]>
- John H. Terpstra <jht@samba.org[43]>

Chapter 16, “File, Directory, and Share Access Controls”

- John H. Terpstra <jht@samba.org[44]>
- Jeremy Allison <jra@samba.org[45]>
- Jelmer R. Vernooij <jelmer@samba.org[46]> (drawing)

Chapter 17, “File and Record Locking”

- Jeremy Allison <jra@samba.org[47]>
- Jelmer R. Vernooij <jelmer@samba.org

Attribution

- John H. Terpstra <jht@samba.org

- Gerald (Jerry) Carter <jerry@samba.org[91]>

Chapter 36, “Migration from NT4 PDC to Samba-3 PDC”

- John H. Terpstra <jht@samba.org[92]>

Chapter 37, “SWAT: The Samba Web Administration Tool”

- John H. Terpstra <jht@samba.org[93]>

Chapter 38, “The Samba Checklist”

- Andrew Tridgell <tridge@samba.org[94]>
- Jelmer R. Vernooij <jelmer@samba.org[95]>

- Jelmer R. Vernooij <jelmer@samba.org[104]

CONTENTS

Contents

List of Figures

FOREWORD

When John first asked me to write an introductory piece for his latest book,

PREFACE

The editors wish to thank you for your decision to purchase this book. The

- 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.
-

INTRODUCTION

Part I

General Installation

PREPARING SAMBA FOR CONFIGURATION

1.2.2 TDB Database File Information

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

The directory in which Samba stores the tdb files is determined by compile-time directives. Samba-3 stores tdb files in two locations. The best way to determine these locations is to execute the following command:

```
root#  smbd -b | grep PRIVATE_DIR
   PRIVATE_DIR: /etc/samba/private
```

This 2DIRieans that the confidential tdb files are stored in the /etc/samba/private directory. Samba-3 also uses a number of tdb files that contain more mundane data. The location of these files can be found by executing:

```
root#  smbd -b | grep LOCKDIR
   LOCKDIR: /var/lib/samba
```

Therefore the re2DIRiaining control files will, in the example shown, be stored in the /var/lib/samba directory.

The persistent tdb files are described in Table 1.1. All persistent tdb files should be regularly backed up. Use the **tdbbackup** utility to backup the tdb

Make sure you put the `smb.conf` file in the correct place. Note, the correct

The spoolservice is the name of the printer (actually the print queue) on

1.6 Common Errors

Section

Table 1.2 Temporary TDB File Descriptions

Name	Description	Backup
brlock	Byte-range locking information.	No
connections	A temporary cache for current connec-	

Chapter 2

FAST START: CURE FOR IMPATIENCE

When we first asked for suggestions for inclusion in the Samba HOWTO documentation, someone wrote asking for example configurations — and lots

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

2.3 Worked Examples

The configuration examples are designed to cover everything necessary to get Samba running. They do not cover basic operating system platform configuration, 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

```
root#  testparm
```

Note any error messages that might be produced. Proceed only if error-free output has been obtained. An example of typical output that should be generated from the above configuration file is shown here:

```
Load smb config files from /etc/samba/smb.conf
Processing section "[data]"
Loaded services file OK.
Server role: ROLE_STANDALONE
Press enter to see a dump of your service definitions
[Press enter]

# Global parameters
[global]
   workgroup = MIDEARTH
   netbios name = HOBBIT
   security = share

[data]
   comment = Data
   path = /export
   read only = Yes
   guest only = Yes
```

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

7. Check that Samba is running correctly:

```
root# smbclient -L localhost -U%
Domain=[MIDEARTH] OS=[UNIX] Server=[Samba-3.0.20]

Sharename      Type      Comment
---------      ----      -------
public         Disk      Data
IPC$           IPC       IPC Service (Samba-3.0.20)
ADMIN$         IPC       IPC Service (Samba-3.0.20)
hplj4          Printer   hplj4

Server               Comment
---------            -------
OLORIN               Samba-3.0.20

Workgroup            Master
---------            -------
MIDEARTH             OLORIN
```

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

7. Set the password for wbinfo

Example 2.3.7 Engineering Office smb.conf (globals)

Section

Section

Example 2.3.8 Engineering O□ce smb.conf (shares and services)

Part II

Server Configuration Basics

FIRST STEPS IN SERVER CONFIGURATION

Samba can operate in various modes within SMB networks. This HOWTO

Chapter 3

SERVER TYPES AND SECURITY MODES

This chapter provides information regarding the types of server that Samba may be configured to be. A Microsoft network administrator who wishes to migrate to or use Samba will want to know the meaning, within a Samba

–

in with the client/server approach of SMB. In SMB everything is initiated and controlled by the client, and the server can only tell the client what is available and whether an action is allowed.

The term

Section

```
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 Configuration

The

- Does not work with Winbind, which is particularly needed when storing profiles remotely.

-

3.4 Password Checking

Chapter 4

DOMAIN CONTROL

There are many who approach MS Windows networking with incredible

Section

Section

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 server. We hope this is plain and simple enough for all to understand.

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 lost the election to become a DMB. For this reason, in networks where a Samba server is the PDC it is wise to configure the Samba domain controller as the DMB.

Note

SMB/CIFS servers that register the DOMAIN<1C> name do so because they provide the network logon service. Server that register the DOMAIN<1B> name are

Chapter 5

BACKUP DOMAIN CONTROL

the slave finds 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

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 be empty. Unfortunately, some sites are unable to avoid such configurations, and these sites should review the *ldap replication sleep* parameter, intended to slow down Samba sufficiently for the replication to catch up. This is a kludge, and one that the administrator must manually duplicate in any

as a mere NIS client would not be enough, as the BDC would not be

Section

Chapter 6

- MS Windows workstation users get the benefit of SSO.
-

Section 6.2. MS Windows Workstation/Server Machine Trust Accounts

There are three ways to create Machine Trust Accounts:

- Manual creation from the UNIX/Linux command line. Here, both the Samba and corresponding UNIX account are created by hand.
- Using the MS Windows NT4 Server Manager, either from an NT4 domain member server or using the Nexus toolkit available from the Microsoft Web site. This tool can be run from any MS Windows

Join the client to the domain immediately

Manually creating a Machine Trust Account using this method is the equivalent of creating a Machine Trust Account on a Windows NT PDC using the Server Man-

Section

6.2.4.1 Windows 200x/XP Professional Client

Section

Section 6.3. Domain Member Server

daemon lasts. This can drain the connection resources on a Microsoft NT server and cause it to run out of available connections. With *security*

Section

Section 6.4. Samba ADS Domain Membership

note that forward slashes must be used, because backslashes are both valid

the *log level* in the

Chapter 7

STANDALONE SERVERS

Standalone servers are independent of domain controllers on the network. They are not domain members and function more like workgroup servers. In many cases a standalone server is configured with a minimum of security control with the intent that all data served will be readily accessible to all users.

7.1 Features and Benefits

7.2 Background

The term *standalone server* means that it will provide local authentication and access control for all resources that are available from it. In general this

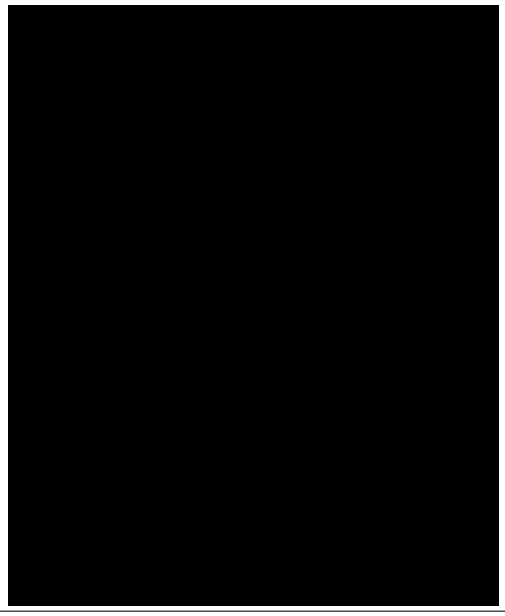
1. The print server must require no administration.
2.

Section

Chapter 8

MS WINDOWS NETWORK CONFIGURATION GUIDE

Figure 8.1 Network Bridge Configuration.



Section 47.2.2, Section 47.2.2. If it is necessary to provide a fixed IP address, click on “Use the following IP address” and enter the IP Address, the subnet mask, and the default gateway address in the boxes provided.

3. Click the **Advanced** button to proceed with TCP/IP configuration.

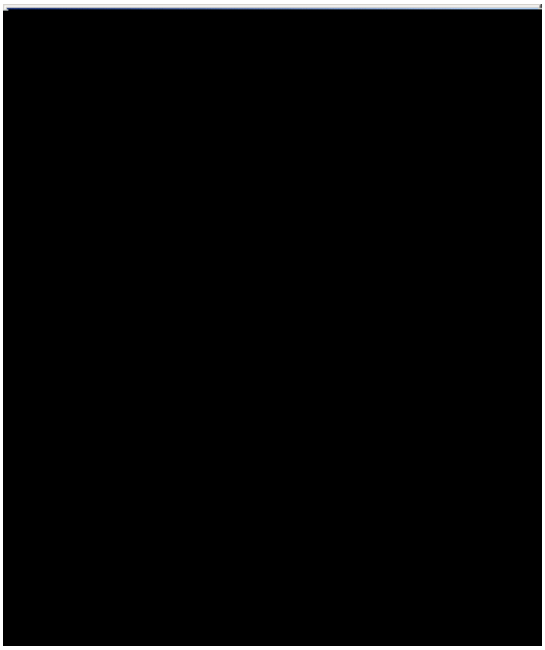
ad[illegible](i)1((iocal)-389(IP)-569(ad)1-e)]TJ0-
ef(aul)1(t)-472ggatsewayis (pru(tes().n)-40(Int)-472mose)-1(t)-472casseessd,e
itwal1(lt).399noitbeessarycea(e)-399aAddlet(i)1(gs(.)6417See.)]TJET10014105454

Section

Figure 8.4 DNS Configuration.

Figure 8.5 WINS Configuration

Figure 8.9 DNS Configuration.



Note

Windows XP Home edition cannot participate in domain or LanManager network logons.

1. Right-click on the**t317(w308(o308r(k)-66[NDe)-1i4)1(hbn)-38(o318(r))1(on)-08(o)-38d9**

Figure 8.11

Figure 8.12 IP Address.

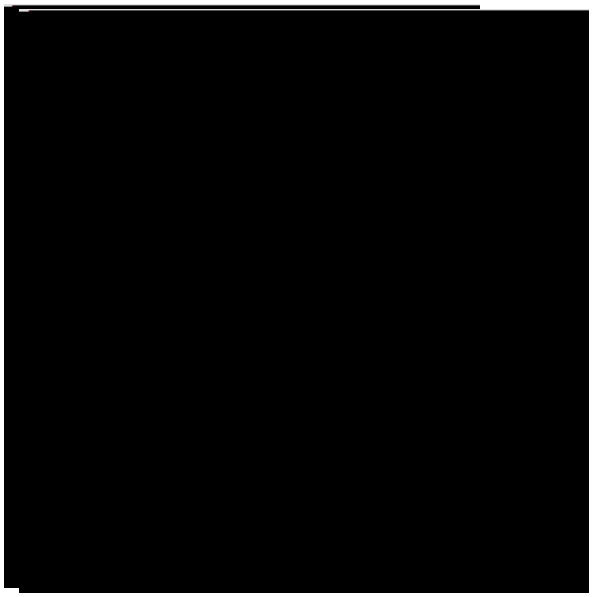


Figure 8.16 The Computer Name Panel.

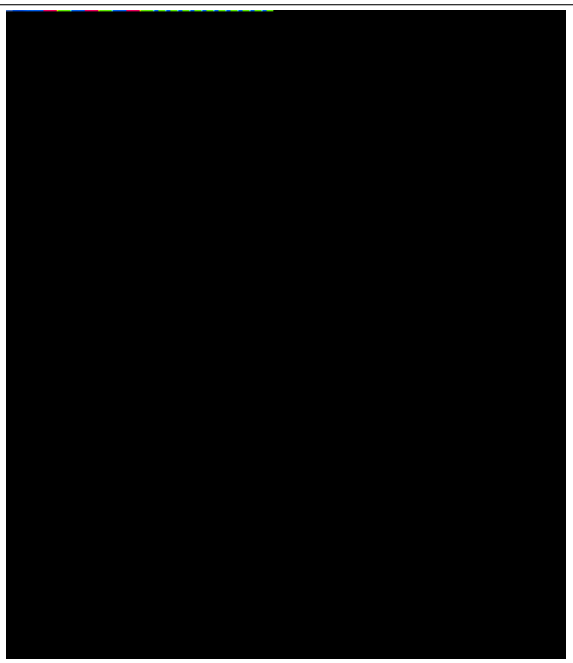


Figure 8.17 The Computer Name Changes Panel.

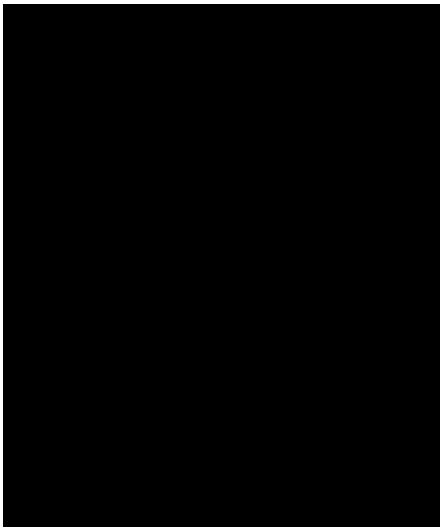


Figure 8.18 The Computer Name Changes Panel — Domain MIDEARTH.

Figure

Figure 8.20 The Network Panel.

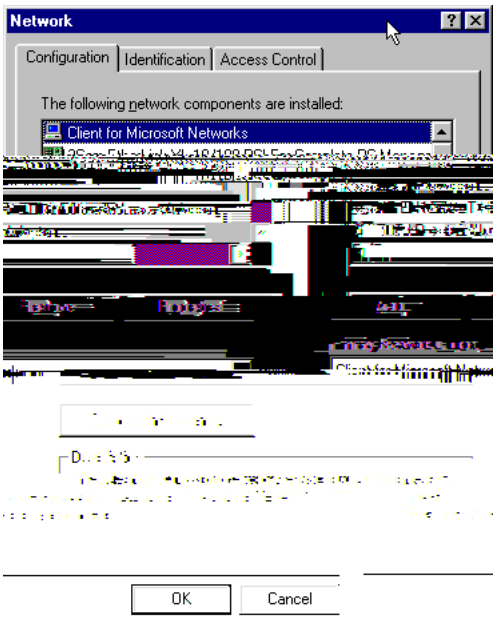


Figure 8.21 Clien0.3983td043tr3td04Microsoft Networks Properties Panel.

Figure 8.22 Identification Panel.

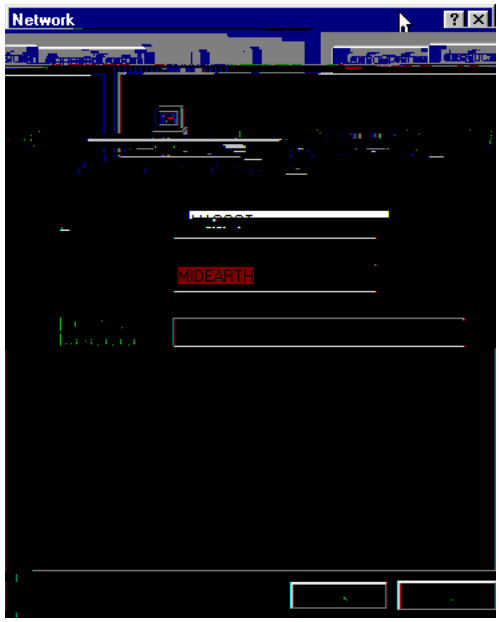


Figure 8.23 Access Control Panel.

Part III

Advanced Configuration

Chap 9

Chapter 10

Samba provides the ability to implement a WINS (Windows Internetworking Name Server) and implements extensions to Microsoft's implementation of WINS. These extensions help Samba to e□ect stable WINS operations beyond the normal scope of MS WINS.

WINS is exclusively a service that applies only to those systems that run NetBIOS over TCP/IP. MS Windows 200x/XP have the capacity to operate

- *lm announce*
- *lm interval*
- *preferred master* (*)
- *local master* (*)
- *domain master* (*)
- *browse list*
- *enhanced browsing*

Name Resolution Method:

- *name resolve order* (*)

WINS options:

-

Example 10.4.2 Local master browser smb.conf

WINS also forces browse list synchronization by all LMBs. LMBs must

Section

"unusual" purposes: announcements over the Internet, for example. See *remote announce* in the `smb.conf` man page.

10.7.2 Problem Resolution

Section 10.7. Technical Overview of Browsing

Section

Table 10.2 Browse Subnet Example 2

10.8.5 Invalid Cached Share References A□ects Network Brows-

Chapter 11

ACCOUNT INFORMATION DATABASES

11.1.2 New Account Storage Systems

Samba-3 introduces a number of new password backend capabilities.

tdbsam

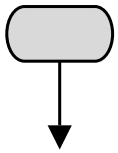
11.2 Technical Information

Old Windows clients send plaintext passwords over the wire. Samba can check these passwords by encrypting them and comparing them to the hash stored in the UNIX user database.

Newer Windows clients send encrypted passwords (LanMan and NT hashes) instead of plaintext passwords over the wire. The newest clients will send only encrypted passwords and refuse to send plaintext passwords unless their registry is tweaked.

Many people ask why Samba cannot simply use the UNIX password database. Windows requires passwpptha25(p94i1(da3(UN88(or555(p)ed)-5(p)et-38(p)1(Win)1n38(p)1f223

Figure 11.1 IDMAP: Resolution of SIDs to UIDs.



Section 11.2. Technical Information1nformation

11.2.4 Comments Regarding LDAP

11.2.4.1 Caution Regarding LDAP and Samba

Samba in the same way that Windows NT4/200X treats them. A user account and a machine account are indistinquishable from each other, except that the machine account ends in a $ character, as do trust accounts.

The need for Windows user, group, machine, trust, and other accounts to be tied to a valid UNIX UID is a design decision that was made a long way back in the history of Samba development. It is unlikely that this decision

Section

Section 11.3. Account Management Tools

Section 11.3. Account Management Toocco

An example of a simple change in the user account information is the change of the full name information shown here:

```
root#  pdbedit -r --fullname="Victor Aluicious Laan" vlaan
...
Primary Group SID:    S-1-5-21-726309263-4128913605-1168186429-513
```

```
Profile Path:         \\aurora\profiles\jht
Domain:               MIDEARTH
Account desc:         BluntObject
Workstations:
Logon time:           0
Logoff time:          Mon, 18 Jan 2038 20:14:07 GMT
Kickoff time:         0
Password last set:    Sun, 03 Jul 2005 23:19:18 GMT
Password can change:  Sun, 03 Jul 2005 23:19:18 GMT
Password must change: Mon, 18 Jan 2038 20:14:07 GMT
Last bad password   : 0
Bad password count  : 0
Logon hours         : FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
```

The flags can be reset to the default settings by executing:

```
root#  pdbedit -r -c "[]" jra
Unix username:        jht
NT username:          jht
Account Flags:        [U          ]
```

```
account policy value for maximum password age was 4294967295
account policy value for maximum password age is now 7776000
root#  pdbedit -P "minimum password age" -C 7
account policy value for minimum password age was 0
account policy value for minimum password age is now 7
root#  pdbedit -P "bad lockout attempt" -C 8
account policy value for bad lockout attempt was 0
account policy value for bad lockout attempt is now 8
root#  pdbedit -P "lockout duration" -C -1
account policy value for lockout duration was 30
account policy value for lockout duration is now 4294967295
```

No.

To s 106-he maximum (infinite) lockou.

```
    MUST ( uid $ sambaSID )
    MAY  ( cn $ sambaLMPassword $ sambaNTPassword $ sambaPwdLastSet $
           sambaLogonTime $ sambaLogoffTime $ sambaKickoffTime $
           sambaPwdCanChange $ sambaPwdMustChange $ sambaAcctFlags $
           displayName $ sambaHomePath $ sambaHomeDrive $ sambaLogonScript $
           sambaProfilePath $ description $ sambaUserWorkstations $
           sambaPrimaryGroupSID $ sambaDomainName ))
```

The `samba.schema` file has been formatted for OpenLDAP 2.0/2.1. The Samba Team owns the OID space used by the above schema and recommends its use. If you translate the schema to be used with Netscape DS, please

```
root# cp samba.schema /etc/openldap/schema/
```

```
## posixGroup entries in the directory as well
```

11.4.4.11 Using OpenLDAP Overlay for Password Syncronization

Howard Chu has written a special overlay called smbk5pwd. This tool modifies the SambaNTPassword, SambaLMPassword and Heimdal hashes in an OpenLDAP entry when an LDAP_EXOP_X_MODIFY_PASSWD operation is performed.

The overlay is shipped with OpenLDAP-2.3 and can be found in the contrib/slapd-modules/smbk5pwd subdirectory. This module can also be used with OpenLDAP-2.2.

11.5 Common Errors

11.5.1 Users Cannot Logon

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

sambaUserWorkstations	Here you can give a comma-separated list of machines on which the user is allowed to login. You may observe problems when you try to connect to a Samba domain member. Because domain members are not in this list, the domain controllers will reject them. Where this attribute is omitted, the default implies no restrictions.
sambaSID	

Chapter 12

Section

```
root# net groupmap add ntgroup="Domain Admins" unixgroup=domadm rid=512 type=d
```

The quotes around "Domain Admins" are necessary due to the space in the group name. Also make sure to leave no white space surrounding the equal character (=).

Now joe, john, and mary the egg

Having completed these two steps, the execution of **getent group demo** will show demo members of the global `Domain Users` group as members of the group `demo`. This also works with any local or domain user. In case the domain DOM trusts another domain, it is also possible to add global users and groups of the trusted domain as members of `demo`. The users from the foreign domain who are members of the group that has been added to
367(of)23(The)-271(u)1(s)-1((to)]T5492Td[-367(d05he)-273)-4Tf72.43620Td[(13(nill)-340(13(h.66

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 privileges can be done

Section

Note

Versions of Samba-3 prior to 3.0.23 automatically create default group mapping for the `Domain Admins, Domain Users`

The Power Users group is a group that is local to each Windows 200x/XP Professional workstation. You cannot add the Domain Users group to the Power Users group automatically, it must be done on each workstation by logging in as the local workstation *administrator* and then using the following procedure:

1. Click **Start ->** **Control Panel ->** **Users and Passwords**.
2. Click the **Advanced** tab.
3. Click the **Advanced** button.
4. Click Groups.
5. Double-click Power Users. This will launch the panel to add users or groups to the local machine Power Users group.
6. Click the **Ad.9091Tf178.973951405er Usertton.**29oup.

13.1 Overview

The tasks that follow the installation of a Samba-3 server, whether standalone or domain member, of a domain controller (PDC or BDC) begins with the need to create administrative rights. Ovr1ativxgine creialto os

global. Global groups can contain as members, global users. This membership is a□ected in the normal UNIX manner, but adding UNIX users to

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:

```
root#  net groupmap list
Domain Admins (S-1-5-21-72630-4128915-11681869-512) -> Domain Admins
Domain Users (S-1-5-21-72630-4128915-11681869-513) -> Domain Users
Domain Guests (S-1-5-21-72630-4128915-11681869-514) -> Domain Guests
Print Operators (S-1-5-21-72630-4128915-11681869-550) -> Print Operators
Backup Operators (S-1-5-21-72630-4128915-11681869-551) -> Backup Operators
Replicator (S-1-5-21-72630-4128915-11681869-552) -> Replicator
Domain Computers (S-1-5-21-72630-4128915-11681869-553) -> Domain Computers
Engineers (S-1-5-21-72630-4128915-11681869-3005) -> Engineers
SupportEngrs (S-1-5-21-72630-4128915-11681869-3007) -> SupportEngrs
```

13.3.1.2 Mapping Windows Groups to UNIX Groups

Windows groups must be mapped to UNIX system (POSIX) groups so that file system access controls can be asserted in a manner that is consistent with the methods appropriate to the operating system that is hosting the Samba server.

All file system (file and directory) access controls, within the file system of a UNIX/Linux server that is hosting a Samba server(tro289ors)84stemeratteg adeit3hle. Sa
UNIXfiles(m)-1(an)29(ics)-1s.u isesarys that Windows
netwgope(at)1ionsgthataccesspheafilethat
ma(s)-393(s)-32[(Win)1(do)28(ws)-393us(er)-32[(to)-393(s)-32[pa(r)1(iculaer)-32[(UNIX/Lin)9(u

Allbaemone(at)doon9d222(eefalts)-39d222((ap)2366)1(ng)-36s9d223222(]TJ/F5210.9091Tf0-3205

Two types of Windows groups can be created:

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

Section

user name to be mapped to a different UNIX/Linux user name. The `smb.conf` file must also be amended so that the `[global]`

Section

description, and simple security settings that permit write access to files. One of the first steps necessary following migration is to review the share stanzas to ensure that the settings are suitable for use.

The shares are created on the fly as part of the migration process. The smbd

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

Note

The ability to preserve ACLs depends on appropriate support for ACLs as well as the general file system semantics of the host operating system on the target server. A migration from one Windows file server to another will perfectly preserve all file attributes. Because of the difficulty of mapping Windows ACLs onto a POSIX ACLs-supporting system, there can be no perfect migration of Windows ACLs to a Samba server.

13.8.3.3 Share-ACL Migration

Section 13.8. Share Management

If the asterisk (*) is used in place of the printer_name argument, a list of all printers argum-227.3(b)-334eum

Section

```
root#  net rpc info
Domain Name: RAPIDFLY
Domain SID: S-1-5-21-399034208-633907489-3292421255
Sequence number: 1116312355
Num users: 720
Num domain groups: 27
Num local groups: 6
```

Another useful tool is the **net time** tool set. This tool may be used to query the current time on the target server as shown here:

```
root#  net time -S SAURON
Tue May 17 00:50:43 2005
```

In the event that it is the intent to pass the time information obtained to the UNIX **/bin/time**, it is a good idea to obtain the time from the target server in a format that is ready to be passed through. This may be done by executing:

```
root#  net time system -S FRODO
051700532005.16
```

The time can be set on a target server by executing:

```
root#  net time set -S MAGGOT -U Administrator%not24get
Tue May 17 00:55:30 MDT 2005
```

It is possible to obtain the time zone of a server by executing t3cm0gorllwning]TJ0-13.5492Td[(

```
root#  net time sone -S SAURON
```

Chapter 14

IDENTITY MAPPING

```
...
passwd: files winbind
shadow: files winbind
group:  files winbind
...
hosts:  files [dns] wins
...
```

14.2.1.2 ADS Domains

The procedure for joining an ADS domain is similar to the NT4 domain join, except the `smb.conf` file will have the contents shown in Example 14.2.2

Example 14.2.2 ADS Domain Member Server smb.conf

```
# Global parameters
 [global]
        workgroup = BUTTERNET
```

Section 14on

. . .

The following procedugoceu(ugs(ce)e)28w3(t[(The)-3i(ugdmap(14)]TJET100138407615.6755308c

```
dns_lookup_kdc = true
```

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

You will need the PADL

```
dn: dc=snowshow,dc=com
objectClass: dcObject
objectClass: organization
dc: snowshow
o: The Greatest Snow Show in Singapore.
description: Posix and Samba LDAP Identity Database

dn: cn=Manager,dc=snowshow,dc=com
objectClass: organizationalRole
cn: Manager
description: Directory Manager

dn: ou=Idmap,dc=snowshow,dc=com
objectClass: organizationalUnit
ou: idmap
```

6.

```
hosts:  files wins
...
```

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

The next step involves preparation of the ADS schema. This is briefly

```
SeIncreaseQuotaPrivilege  Increase quotas
```

backend can be set to the well-known RID of the default administrator account. To obtain the domain SID on a Samba domain controller, run the following command:

```
root#  net getlocalsid
SID for domain FOO is: S-1-5-21-4294955119-3368514841-2087710299
```

You may assign the domain administrator RID to an account using the **pdbedit** command as shown here:

```
root#  pdbedit -U S-1-5-21-4294955119-3368514841-2087710299-500 -u root -r
```

Note

tors group on the client. Any user who is a member of the domain global Domain Admins group will have administrative rights on the Windows client.

This is often not the most desirable solution because it means that the user will have administrative rights and privileges on domain servers also. The Power Users group on Windows client workstations permits local adminis-

This is an opportune point to mention that Samba was created to provide

•

this is not so rigorously observed because all names are considered arbitrary.

What MS Windows calls a folder, UNIX calls a directory.

Section

achieve this is called the `immutible` bit. Unfortunately, the implementation

Section 16.4. Access Controls on Shares

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

16.5.3 Viewing File Ownership

Clicking on the **Ownership**

ministration and thus adopts the limitations of POSIX ACLs. Therefore, where POSIX ACLs lack a capability of the Windows NT/200X ACLs, the POSIX semantics and limitations are imposed on the Windows administrator.

POSIX ACLs present an interesting challenge to the UNIX administrator

```
other::---              <-- perms appli308cm.'o
```

16.5.8.3 Mapping of Windows Directory ACLs to UNIX POSIX ACLs

Interesting things happen in the mapping of UNIX POSIX directory per-

Table 16.4 Other Controls

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

Windows ACE	File Attribute Flag
Full Control	#
Traverse Folder/Execute File	x
List Folder/Read Data	r
Read Attributes	r
Read Extended Attribures	r
Create Files/Write Data	w
Create Folders/Append Data	

Chapter 17

FILE AND RECORD LOCKING

One area that causes trouble for many network administrators is locking. The extent of the problem is readily evident from searches over the Internet.

17.1 Features and Benefits

Samba provides all the same locking semantics that MS Windows clients expect and that MS Windows NT4/200x servers also provide.

The term *locking*

Note

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

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 simultaneously with its open. A client may ask for

local locks, and discard read-ahead data. The break is then complete,

In mission-critical, high-availability environments, careful attention should be given to oplocks. Ideally, comprehensive testing should be done with all a□ected applications with oplocks enabled and disabled.

17.2.1.1 Exclusively Accessed Shares

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 differential over sending those reads and writes over the wire. This is most likely to occur

When a workstation attempts to access shared data files located on another Windows 2000/XP computer, the Windows 2000/XP operating system will

17.4.2 Server Service Entries

```
\HKEY_LOCAL_MACHINE\SysteuCAL_]TJ/17.18167-153.542ld[(CurrentCotriolSet134Syr
```

17.5 Persistent Data Corruption

If you have applied all of the settings discussed in this chapter but data

17.7 Additional Reading

You may want to check for an updated documentation regarding file and record locking issues on the M0.9664366(Read3e)-1(o20(at)-502(Ss)-5ped)-42ort10.90931f100.8917233.180

Chapter 18

SECURING SAMBA

18.1 Introduction

The information contained in this chapter applies in general to all Samba

the configuration of the host server that is running Samba, and Samba itself. Samba permits a most flexible approach to network security. As far as

```
        hosts allow = 192.168.115.0/24 127.0.0.1
        hosts deny = 0.0.0.0/0
```

Chapter 19

access rights and privileges in another domain. The language that describes this capability is couched in terms of *trusts*. Specifically, one domain will *trust* the users from another domain. The domain from which users can

Section

19.5 NT4-Style Domain Trusts with Windows 2000

Chapter 21

CLASSICAL PRINTING SUPPORT

21.1 Features and Benefits

It is apparent from postings on the Samba mailing list that print configura-

Global Parameters

Section

be if you used this minimalistic configuration. Here is what you can expect to find:

```
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

Example 21.4.1

printing = bsd Causes Samba to use default print commands applicable for the BSD (also known as RFC 1179 style or LPR/LPD) printing

max print jobs = 100 Sets the upper limit to 100 print jobs being active on the Samba server at any one time. Should a client submit a job that exceeds this number, a "no more space available on server" type of error message will be returned by Samba to the client. A setting of zero (the default) means there is *no* limit at all.

printcap name = /etc/printcap Tells Samba where to look for a list of available printero3985cm0gcm7obcrprinCUP317Svnvs a

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

public = yes Is a synonym for *guest ok* = yes. Since we have *guest ok* =

Section

- *%z* — the size of the spooled print job (in bytes).

The print command must contain at least one occurrence of *%s* or *%f*. The

21.5.1 Point'n'Print Client Drivers on Samba Servers

Section

Access may be granted to download and install printer drivers on clients. The requirement for *guest ok = yes* depends on how your site is configured. If users will be guaranteed to have an account on the Samba host, then this is a non-issue.

Note

If all your Windows NT users are guaranteed to be authenticated by the Samba server (for example, if Samba authenticates via an NT domain server and the user has already been validated by the domain controller in order to log on to the Windows NT session), then guest access is not necessary. Of course, in a workgroup environment where you just

Section

```
root# rpcclient -U'Danka%xxxx' -c \
   'getdriver "Heidelberg Digimaster 9110 (PS)" 3' TURBO_XP
cmd = getdriver "Heidelberg Digimaster 9110 (PS)" 3

[Windows NT x86]
Printer Driver Info 3:
  Version: [2]
  Driver Name: [Heidelberg Digimaster 9110 (PS)]
  Architectur5(3)]TJ0-21ows NT x86]
```

at it. The Windows 9x/Me driver files will end up in subdirectory `0` of the `WIN40` directory. The full path to access them is `\\WINDOWSHOST\print$\WIN40\0\`.

Note

More recent drivers on Windows 2000 and Windows XP

```
[...]
```

Section

(you must of course adapt the name to your Samba server instead of *SAMBA-CUPS*):

```
rundll32 printui.dll,PrintUIEntry /s /t2 /n\\SAMBA-CUPS
```

-

connection (do not confuse this with logging o from the local workstation; that is a di erent matter). On Windows NT/200x, you can force a logo from all smb/cifs connections by restarting the *workstation* service. You can try to close all Windows file explorers and Internet Explorer for Windows. As a last resort, you may have to reboot. Make sure there is no automatic reconnection set up. It may be easier to go to a di erent workstation and try from there. After you have made sure you are connected as a printer admin user (you can check this with the smbstatus

```
        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]
        Configfile: [\\10.160.50.8\print$\W32X86\2\cns3gui.dll]
        Helpfile: [\\10.160.50.8\print$\W32X86\2\cns3g.hlp]

        Dependentfiles: [\\10.160.50.8\print$\W32X86\2\AUCPLMNT.DLL]
        Dependentfiles: [\\10.160.50.8\print$\W32X86\2\aussdrv.dll]
        Dependentfiles: [\\10.160.50.8\print$\W32X86\2\cnspdc.dll]
        Dependentfiles: [\\10.160.50.8\print$\W32X86\2\aussapi.dat]
        Dependentfiles: [\\10.160.50.8\print$\W32X86\2\cns3407.dll]
        Dependentfiles: [\\10.160.50.8\print$\W32X86\2\CnS3G.cnt]
        Dependentfiles: [\\10.160.50.8\print$\W32X86\2\NBAPI.DLL]
        Dependentfiles: [\\10.160.50.8\print$\W32X86\2\NBIPC.DLL]
        Dependentfiles: [\\10.160.50.8\print$\W32X86\2\cns3gum.dll]

        Monitorname: [CPCA Language Monitor2]
        Defaultdatatype: []
```

If we write the "version 2" files and the "version 3" files into different text files and compare the result, we see this picture:

```
root# sdiff 2-files 3-files


 cns3g.dll                       cns3g.dll
 iR8500sg.xpd                    iR8500sg.xpd
 cns3gui.dll                     cns3gui.dll
 cns3g.hlp                       cns3g.hlp
 AUCPLMNT.DLL                  | aucplmNT.dll
                               > ucs32p.dll
                               > tnl32.dll
 aussdrv.dll                     aussdrv.dll
 cnspdc.dll                      cnspdc.dll
 aussapi.dat                     aussapi.dat
 cns3407.dll                     cns3407.dll
 CnS3G.cnt                       CnS3G.cnt
 NBAPI.DLL                       NBAPI.DLL
 NBIPC.DLL                       NBIPC.DLL
 cns3gum.dll                   | cpcview.exe
                               >cpcdspl.exe
```

21.8.7 Avoiding Common Client Driver Misconfiguration

So now the printing works, but there are still problems. Most jobs print

Section 21.12. Migration of Classical Printing to Samba

Section 21.14. Common Errors

Chapter 22

CUPS PRINTING SUPPORT

22.1 Introduction

22.1.1 Features and Benefits

The Common UNIX Print System (CUPS

it maps to the System V commands with an additional -oraw option for printing. On a Linux system, you can use the ldd utility to find out if smbd has been linked with the libcups library (the

Example 22.2.2

Section 22.3. Advanced Configuration

e2tiv

This is all you need to know to get the CUPS/Samba combo printing “raw”

22.4.2 Windows Drivers, GDI, and EMF

In Windows OS, the format conversion job is done by the printer drivers. On MS Windows OS platforms all application programmers have at their

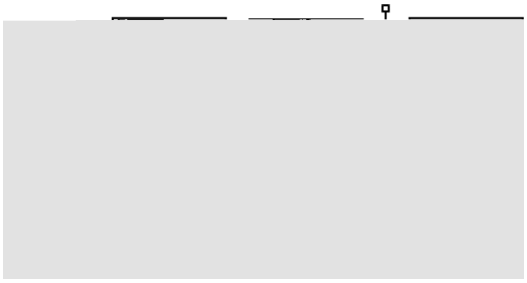
However, there are other types of printers out there. These do not know how to print PostScript. They use their own PDL, often proprietary. To print to them is much more demanding. Since your UNIX applications mostly produce PostScript, and since these devices do not understand PostScript, you need to convert the print files to a format suitable for your printer on the host bef(m)27(uce)-3(s)-25i-1(e(s)-25iu48F2)1(s)-1nd5i-1(eiost)-33aHow368(2367(8483(8)]TJ

Tip

Note

Section

Figure 22.4 Prefiltering in CUPS to Form PostScript.



cups-postscript. As stated earlier, this filter inserts all device-specific print options (commands to the printer to ask for the duplexing of output, or stapling and punching it, and so on) into the PostScript file. An example is illustrated in

Figure 22.8 Image Format to CUPS-Raster Format Conversion.

22.5.9 CUPS Backends

The last part of any CUPS filtering chain is a backend. Backends are special programs that send the print-ready file to the final device. There is a sep-

ipp

Table 22.1 PPDs Shipped with CUPS

PPD file	Printer type
deskjet.ppd	older HP inkjet printers and compatible
deskjet2.ppd	newer HP inkjet printers and compatible
dymo.ppd	label printers
epson9.ppd	Epson 24-pin impact printers and compatible

Figure 22.10

Section

developers themselves and its sales help finance the further development of CUPS, as they feed their creators).

- The Gimp-Print Project[8] (GPL, free software) provides around 140 PPDs (supporting nearly 400 printers, many driven to photo quality

```
        -i /path/to/interface-script
```

Interface scripts might be the "unknown animal" to many. However, with CUPS they provide the easiest way to plug in your own custom-written filtering script or program into one specific print queue (some information about the traditional use of interface scripts is found at http://playground.sun.com/printing/documentation/interfa

22.6 Network Printing (Purely Windows)

Network printing covers a lot of ground. To understand what exactly goes

22.8 Network PostScript RIP

This section discusses the use of CUPS filters on the server — configuration where clients make use of a PostScript driver with CUPS-PPDs.

PPDs can control all print device options. They are usually provided by the manufacturer — if you own a PostScript printer, that is. PPD files are always a component of PostScript printer drivers on MS Windows or Apple Mac OS systems. They are ASCII files containing user-selectable

22.10.8 Windows CUPS PostScript Driver Versus Adobe Driver

Are you interested in a comparison between the CUPS and the Adobe PostScript drivers? For our purposes, these are the most important items

Section

500

1. Call the CUPS server via IPP and request the driver files and the PPD

most interesting ones. *rpcclient* implements an important part of the MS-RPC protocol. You can use it to query (and command) a Windows NT (or 200x/XP) PC, too. MS-RPC is used by Windows clients, among other things, to benefit from the Point'n'Print features. Samba can now mimic this as well.

22.11.1 A Check of the rpcclient man Page

First let's check the*rpcclient*

Section

This installs a printer with the name *mysmbtstprn* to the CUPS sys-

11. (Optional.) Tickle the driver into a correct device mode. You

Section

Section

amount of new information and new printers. He also developed the support for other spoolers, like PPR[29] (via ppromatic), GNUlpr[30], and LPRng[31] (both via an extended lpdomatic) and spooler-less printing (directomatic[32]).

So, to answer your question, "Foomatic" is the general name for all the overlapping code and data behind the "*omatic" scripts. Foomatic, up to versions 2.0.x, required (ugly) Perl data structures attached to Linuxprinting.org PPDs for CUPS. It had a different "*omatic" script for every spooler, as well as different printer configuration files.

22.13.1.5 The *Grand Unification* Achieved

This has all changed in Foomatic versions 2.9 (beta) and released as "stable" 3.0. It has ng1(9)90u310(n)hediereveatic511oripts.(s)-25511oa1(d)-384(n)i(s)-25511ocl

22.13.1.7 Forums, Downloads, Tutorials, Howtos (Also for Mac OS X

Section 22.13. CUPS Print Drivers from Linuxprinting.org

Section

on the real print subsystem you're using. Samba's part is always to receive the job files from the clients (filtered *or* unfiltered) and hand them over to this printing subsystem.

Of course one could hack things with one's own scripts. But then there is

•

- A user being denied a job because of a filled-up quota does not get

```
PreserveJobFiles Yes
```

and a

Section

transferred when you want to download them from Samba.

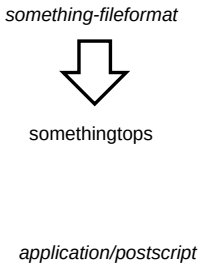
22.19.2 “cupsaddsmb” Keeps Asking for Root Password in Never-

Section

22.19.14 Win XP-SP1

Win XP-SP1 introduced a Point and Print Restriction Policy (this restric-

Figure 22.18 Filtering Chain with cupsomatic



Chapter 23

STACKABLE VFS MODULES

23.1 Features and Benefits

- file open/close/rename/unlink/chmod

23.3.2 default_quota

myprefix:uid nolimit This parameter takes a boolean argument that specifies i:0.50f151.7n argument that spec-

Section

23.3.6 netatalk

A netatalk module will ease co-existence of Samba and netatalk file sharing services.

Advantages compared to the old netatalk module:

- Does not care about creating .AppleDouble forks, just keeps them in sync.
- If a share in `smb.conf`

Member File Server, but it is assumed that you have a working Samba

Chapter 24

WINBIND: USE OF DOMAIN ACCOUNTS

24.1 Features and Benefits

- Winbind maintains a database called winbind_idmap.tdb in which it stores mappings between UNIX UIDs, GIDs, and NT SIDs. This

24.2 Introduction

the lookup. Because Winbind hooks into the operating system at a low level

Section 24.4. How Winbind Works

24.5 Installation and Configuration

24.5.1 Introduction

This section describes the procedures used to get Winbind up and running. Winbind is capable of providing access and authentication control for Windows Domain users through an NT or Windows 200x PDC for regular services, such as telnet and ftp, as well for Samba services.

- *Why should I do this?*

  This allows the Samba administrator to rely on the authentication mechanisms on the Windows NT/200x PDC for the authentication of domain members. Windows NT/200x users no longer need to have

```
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` file looked like this after editing:

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

The libraries needed by the winbindd

```
##

if [ ! -d /usr/bin ]
then                    # /usr not mounted
   exit
fi

killproc() {            # kill the named process(es)
   pid=‘/usr/bin/ps -e |
        /usr/bin/grep -w $1 |
        /usr/bin/sed -e ’s/^  *//’ -e ’s/ .*//’‘
   [ "$pid" != "" ] && kill $pid
}

# Start/stop processes required for Samba server

case "$1" in

’start’)
#
# Edit these lines to suit your installation (paths, workgroup, host)
#
echo Starting SMBD
   /usr/local/samba/bin/smbd -D -s \
   /usr/local/samba/smb.conf

echo Starting NMBD
   /usr/local/samba/bin/nmbd -D -l \
   /usr/local/samba/var/log -s /usr/local/samba/smb.conf

echo Starting Winbind Daemon
   /usr/local/samba/sbin/winbinddlocal/samba/sbin/winbid
```

```
*)
   echo "Usage: /etc/init.d/samba.server { start | stop }"
   ;;
esac
```

Note

The directory in *template homedir* is not created automatically! Use pam_mkhomedir or pre-create the directories of users to make sure users can log in on UNIX with their own home directory.

Warning

```
root# chown maryo a_file
chown: ‘maryo’: invalid user
```

“This is driving me nuts! What can be wrong?”

Section 25.3. Remote Desktop Management

Section

Section

Chapter 27

Note

Windows 9x/Me and NT4 and later profiles should not be stored in the

```
HKEY_LOCAL_MACHINE\Windows\CurrentVersion\ProfileList
```

618

620

27.2.5.3 moveuser.exe

The Windows 200x professional resource kit has moveuser.exe. moveuser.exe changes the security of a profile from one user to another. This allows the account domain to change and/or the username to change.

This command is like the Samba profiles tool.

27.2.5.4 Get SID

You can identify the SID by using

Section

27.5.3 MS Windows 200x/XP

Note

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

Table 27.3 Defaults of Default User Profile Paths Registry Keys

Name	Default Value
AppData	%USERPROFILE%\Application Data
Cache	%USERPROFILE%\Local Settings\Temporary Internet Files
Cookies	%USERPROFILE%\Cookies

Section 27.6. Common Errors

Chapter 28

PAM-BASED DISTRIBUTED AUTHENTICATION

SMB Server The

Section

Section

Section

Warning

The RID to UNIX ID database is the only location where the user and group mappings are stored by **winbindd**. If this file is deleted or corrupted, there is no way for **winbindd** to determine which user and group IDs correspond to Windows NT user and group RIDs.

28.2.5 Password Synchronization Using pam_smbpass.so

pam_smbpass is a PAM module that can be used on conforming systems to keep the smbpasswd (Samba password) database in sync with the UNIXeo(th)the70y

```
#%PAM-1.0
# kdc-pdc
#
auth       requisite   pam_nologin.so
auth       requisite   pam_krb5.so
auth       optional    pam_smbpass.so migrate
account    required    pam_krb5.so
password   requisite   pam_cracklib.so retry=3
password   optional    pam_smbpass.so nullok use_authtok try_first_pass
password   required    pam_krb5.so use_authtok try_first_pass
session    required    pam_krb5.so
```

28.3 Common Errors

see if things work. If they do, look at `/etc/pam.d/system-auth` and copy

Chapter 29

INTEGRATING MS WINDOWS NETWORKS WITH SAMBA

- /etc/resolv.conf
- /etc/host.conf
- /etc/nsswitch.conf

29.3.1 /etc/hosts

29.3.4 /etc/nsswitch.conf

This file controls the actual name resolution targets. The file typically has

Section

```
# \0xnn notation to specify a hex value for a non-printing character.
#
# The following example illustrates all of these extensions:
#
# 102.54.94.97     rhino     #PRE #DOM:networking  #net group's DC
# 102.54.94.102    "appname  \0x14"       #special app server
# 102.54.94.123    popular   #PRE         #source server
# 102.54.94.117    localsrv  #PRE         #needed for the include
#
# #BEGIN_ALTERNATE
# #INCLUDE \\localsrv\public\lmhosts
# #INCLUDE \\rhino\public\lmhosts
# #END_ALTERNATE
#
# In the above example, the "appname" server contains a special
# character in its name, the "popular" and "localsrv" server names are
# pre-loaded, and the "rhino" server name is specified so it can be used
# to later #INCLUDE a centrally maintained lmhosts file if the "localsrv"
# system is unavailable.
#
# Note that the whole file is parsed including comments on each lookup,
# so keeping the number of comments to a minimum will improve performance.
# Therefore it is not advisable to simply add lmhosts file entries onto the
```

lowed, the precise nature of which is dependent on how the NetBIOS Node Type parameter is configured. 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

29.5.1 Pinging Works Only One Way

Chapter 30

UNICODE/CHARSETS

character encoding scheme used by computers to date. This employs a charset that contains 256 characters. Using this mode of encoding, each character takes exactly one byte.

There are also charsets that support extended characters, but those need at

clients. The default depends on the charsets you have installed on your system. Run

Section

care of containing a "\(0x5c)" in a filename, but filenames are not

Table 30-56

Chapter 31

Section

Chapter 32

HIGH AVAILABILITY

- 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.

-

Section

32.2.5 MS-DFS: The Poor Man's Cluster

Chapter 33

Of course, use your own path and settings, but set the case options to match

Chapter 34

ADVANCED CONFIGURATION TECHNIQUES

situation where it may be beneficial to host a generic (anonymous) server is

Section

Example 34.1.3 Master smb.conf File Global Section

```
# Global parameters
 [global]
        workgroup = MIDEARTH
        netbios name = MERLIN
```

Example 34.1.4 MERLIN smb-merlin.conf File Share Section

```
# Global parameters

        workgroup = MIDEARTH


        comment = Home Directories
        valid users = %S
        read only = No
        browseable = No
```

Part IV

Migration and Updating

Chapter 35

Section

- abort shutdown script
- shutdown script

- disable netbios
- dmapi support
- enable privileges
- use kerberos keytab
-

-

- max reported print jobs
- printcap cache time

Unicode and Character Sets

- display charset
- dos charset
- UNIX charset

SID to UID/GID Mappings

- idmap backend
- idmap gid
- idmap uid
- username map script

- preload modules
- reset on zero vc
- privatedir

35.3.3 Modified Parameters (Changes in Behavior)

- acl group control (new default is No, deprecated parameter)
-

Section

Section 35.4. New Functionality

- ldap su□x — used to search for user and computer accounts.
-

Chapter 36

MIGRATION FROM NT4 PDC TO SAMBA-3 PDC

- Greater stability, reliability, performance, and availability.
- Manageability via an SSH connection.
- Flexible choices of backend authentication technologies (tdbsam, ldapsam).
- Ability to implement a full single-sign-on architecture.
-

and the PDC. If it's long (more than 100 ms), locate a BDC on the remote segment to serve as the local authentication and access control server.

36.1.1.2 Server Sha0more

Logon scripts can be created on the fly so all commands executed are specific to the rights and privileges granted to the user. The preferred controls should be e□ected through group membership so group information can be

The Account Migration Process

1.

Section

- Add/Delete Groups: Note OS limits on size and nature. Linux

Chapter 37

SWAT: THE SAMBA WEB ADMINISTRATION TOOL

Section

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 server Samba will be configured for, whether it will be a WINS server, participate as a WINS client, or operate with no WINS support. By clicking one button, you can elect to expose (or not) user home directories.

37.3.6 The Status Page

The status page serves a limited purpose. First, it allows control of the

Chapter 38

THE SAMBA CHECKLIST

38.1 Introduction

```
frodo:~ # iptables -L -v
Chain INPUT (policy DROP 98496 packets, 12M bytes)
 pkts bytes target     prot opt in     out     source     destination
 187K  109M ACCEPT     all  --  lo     any     anywhere   anywhere
 892K  125M ACCEPT     all  --  eth0   any     anywhere   anywhere
1399K 1380M ACCEPT     all  --  eth1   any     anywhere   anywhere  \
               state RELATED,ESTABLISHED

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source     destination
 978K 1177M ACCEPT     all  --  eth1   eth0    anywhere   anywhere \
               state RELATED,ESTABLISHED
 658K   40M ACCEPT     all  --  eth0   eth1    anywhere   anywhere
    0     0 LOG        all  --  any    any     anywhere   anywhere \
               LOG level warning

Chain OUTPUT (policy ACCEPT 2875K packets, 1508M bytes)
 pkts bytes target     prot opt in     out     source     destination

Chain reject_func (0 references)
 pkts bytes target     prot opt in     out     source     destination
```

3. Run the command smbclient -L BIGSERVER on the UNIX box. You should get back a list of available shares. If you get an error message containing the string “bad password”, then you probably have either an incorrect *hosts allow*, *hosts deny*, or *valid users* line in your smb.conf, or else guest access is not working.

Section 38.3. The Tests

Chapter 39

ANALYZING AND SOLVING SAMBA PROBLEMS

There are many sources of information available in the form of mailing lists,

the connection. Pressing ctrl-alt-delete and going down to the domain box is sufficient (at least, the first time you join the domain) to generate a *LsaEnumTrustedDomains*

Figure 39.1 Starting a Capture.

750

Chapter 40

Run testparm to check your config file for correct syntax.

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

If you include part of a log file 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

If the bug has anything to do with Samba behaving incorrectly as a server

```
root# ./configure --help
```

This will help you to see what special options can be enabled. Now execute `./configure` with any arguments it might need:

```
root# ./configure [... arguments ...]
```

in addition to the standard development environment.

If these files are not installed on your system, you should check the installation CDs to find which has them and install the files using your tool of choice. If in doubt about what tool to use, refer to the Red Hat Linux documentation.

Note

Note

Section

Chapter 42

PORTABILITY

Samba works on a wide range of platforms, but the interface all the platforms provide is not always compatible. This chapter contains platform-specific information about compiling and using Samba.

42.1 HPUX

Hewlett-Packard's implementation of supplementary groups is nonstandard (for historical reasons). There are two group files, `/etc/group` and `/etc/logingroup`; the system maps UIDs to numbers using the former, but initgroups() reads the latter. Most system admins who know the ropes symlink `/etc/group` to

Section

from the DNIX section of `includes.h`.

42.4 Red Hat Linux

By default during installation, some versions of Red Hat Linux add an entry to `/etc/hosts` as follows:

```
127.0.0.1 loopback "hostname"."domainname"
```

Section

Chapter 44

44.4 Max Xmit

At startup the client and server negotiate a *maximum transmit* size, which

Chapter 45

LDAP AND TRANSPORT LAYER SECURITY

45.1 Introduction

Tip

Section 45.2. Configuring

Section

Then, using ldapsearch, test an anonymous search with the -ZZ[7] option:

```
root#  ldapsearch -x -b "dc=ldap,dc=abmas,dc=biz" \
        -H 'ldap://ldap.abmas.biz:389' -ZZ
```

Your results should be sef(ts)r40(s)-1yYourser83(ov)287ur83(of5542(f(ts)r=biz"0134)]TJ45.817

```
sambaSID: S-1-5-21-238355452-1056757430-1592208922
sambaAlgorithmicRidBase: 1000
objectClass: sambaDomain
sambaNextUserRid: 67109862
sambaNextGroupRid: 67109863
```

If you have any problems, please read Section 45.4

Chapter 46

SAMBA SUPPORT

One of the most difficult to answer questions in the information technology

Section 46.2. Commercial Support

Section

Section

812

Section

816

2. Accompany it with a written o□er, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of

A.2.6 Section 5

distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

A.2.12 NO WARRANTY Section 11

BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE

The domain master browser maintains a list of all the servers that have

A syntax for specifying the location of network resources (such as file

Subject Index

285