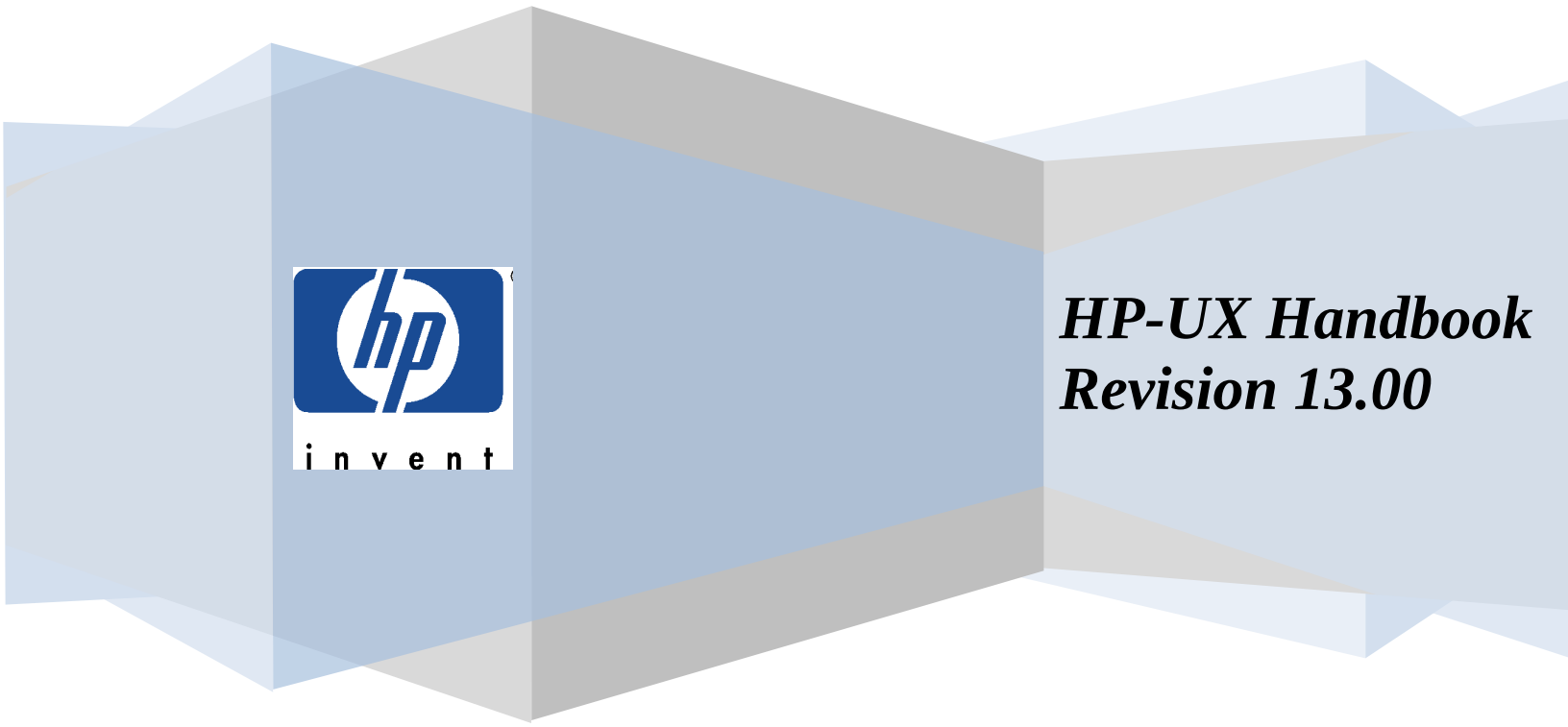
Chapter 20

CIFS



HP-UX Handbook
Revision 13.00

TERMS OF USE AND LEGAL RESTRICTIONS FOR THE HP-UX RECOVERY HANDBOOK

ATTENTION: PLEASE READ THESE TERMS CAREFULLY BEFORE USING THE HP-UX HANDBOOK. USING THESE MATERIALS INDICATES THAT YOU ACCEPT THESE TERMS. IF YOU DO NOT ACCEPT THESE TERMS, DO NOT USE THE HP-UX HANDBOOK.

THE HP-UX HANDBOOK HAS BEEN COMPILED FROM THE NOTES OF HP ENGINEERS AND CONTAINS HP CONFIDENTIAL INFORMATION.

THE HP-UX HANDBOOK IS NOT A PRODUCT QUALITY DOCUMENT AND IS NOT NECESSARILY MAINTAINED OR UP TO DATE. THE HP-UX HANDBOOK IS HERE MADE AVAILABLE TO HP CONTRACT CUSTOMERS FOR THEIR INTERNAL USE ONLY AND ON THE CONDITION THAT NEITHER THE HP-UX HANDBOOK NOR ANY OF THE MATERIALS IT CONTAINS IS PASSED ON TO ANY THIRD PARTY.

Use of the HP-UX Handbook: Hewlett-Packard Company ("HP") authorizes you to view and download the HP-UX Handbook only for internal use by you, a valued HP Contract Customer, provided that you retain all copyright and other proprietary notices contained in the original materials on any copies of the materials. You may not modify the HP-UX Handbook in any way or publicly display, perform, or distribute or otherwise use them for any public or purpose outside your own business. The materials comprising the HP-UX Handbook are copyrighted and any unauthorized use of these materials may violate copyright, trademark, and other laws. If you breach any of these Terms, your authorization to use the HP-UX Handbook automatically terminates and you must immediately destroy any downloaded or printed materials.

Links To Other Web Sites: Links to third party Web sites provided by the HP-UX Handbook are provided solely as a convenience to you. If you use these links, you will leave this Site. HP has not reviewed all of these third party sites and does not control and is not responsible for any of these sites or their content. Thus, HP does not endorse or make any representations about them, or any information, software or other products or materials found there, or any results that may be obtained from using them. If you decide to access any of the third party sites linked to this Site, you do this entirely at your own risk.

Disclaimer: THE HP-UX HANDBOOK IS PROVIDED "AS IS" WITHOUT ANY WARRANTIES OF ANY KIND INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT OF INTELLECTUAL PROPERTY. HP further does not warrant the accuracy and completeness of the materials in the HP-UX Handbook. HP may make changes to the HP-UX Handbook at any time without notice. The HP-UX Handbook may be out of date, and HP makes no commitment to update the HP-UX Handbook. Information in the HP-UX Handbook may refer to products, programs or services that are not available in your country. Consult your local HP business contact for information regarding the products, programs and services that may be available to you.

Limitation of Liability: IN NO EVENT WILL HP, ITS SUPPLIERS, OR OTHER ANY THIRD PARTIES MENTIONED IN THE HP-UX HANDBOOK BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, THOSE RESULTING FROM LOST PROFITS, LOST DATA OR BUSINESS INTERRUPTION) ARISING OUT OF THE USE, INABILITY TO USE, OR THE RESULTS OF USE OF THE HP-UX HANDBOOK, WHETHER BASED ON WARRANTY, CONTRACT, TORT OR ANY OTHER LEGAL THEORY AND WHETHER OR NOT ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS DOES NOT APPLY IN CASE OF INTENT OR IF LIABILITY IS LEGALLY STIPULATED. IF YOUR USE OF THE HP-UX HANDBOOK RESULTS IN THE NEED FOR SERVICING, REPAIR OR CORRECTION OF EQUIPMENT OR DATA, YOU ASSUME ALL COSTS THEREOF.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Applicable Laws: These Terms will be governed by and construed in accordance with the laws of the State of California, without giving effect to any principles of conflicts of laws.

General: HP may revise these Terms at any time by updating this posting. ***Revised Oct 2013***

FEEDBACK or QUESTIONS: please email essam.ackleh@hp.com
(please use subject syntax: *HP-UX Handbook v13.00 Chapter <YY> - <Feedback Title>*

TABLE OF CONTENTS

This chapter will introduce you to the ability of HP-UX to communicate in heterogeneous networks with MS-Windows-computers. (Windows NT, Windows 2000, Windows XP Windows 2003 and Windows 2008). There are some products which enable data exchange in mixed environments: there was Advanced Server for Unix (ASU), which is obsolete for HP-UX but still alive on Tru64-Unix. There is Samba (from samba.org) and the HP CIFS bundle. As we do not support Samba (besides within a LINUX contract), we'll focus on the HP CIFS software bundle. The structure of this chapter refers to the recent software versions first and keeps information about older versions at the end.

Introduction

The *Common Internet File System* (CIFS; formerly known as *Server Message Block*, SMB) is a high level protocol developed to provide advertising of available resources and the sharing of network printers and file systems. It is developed and maintained by Microsoft Corp..
In its most basic form it provides for a server to broadcast its name and resources, it handles the handshaking for client to server requests and replies. Broadcasts are generally UDP unidirectional announcements. It provides necessary overhead for the transferring of files, for print requests, directory searches and file manipulations as requested by the client. This file and printer sharing is generally accomplished through high level request/response transactions over Netbios and TCP/IP. All CIFS packets are recognizable with their leading **FF 53 4D 42** (SMB) at the start of the SMB portion of the packet. This is followed by a hex number that represents the type of packet (read, open, write, etc.) being issued.
Wireshark, formerly known as ethereal, is a network analyzer available at http://www.wireshark.org does a great job of formatting network traces for SMB traffic. Wireshark is also capable of displaying the output captured by nettl, the HP-UX network capture utility.

If session communication is lost, the client redirector sends a reset forcing the existing session to be torn down and a new connection to be established starting at the TCP level. Once the TCP connection is in place a new negotiation takes place and a new session is established. The redirector does this most times without the intervention of the user. The users request will simply take longer than normal to succeed. The client and server negotiate the version level of the protocol to allow for improvements as new clients and servers have evolved. Compatibility is maintained to allow for new servers to communicate with older server and vice versa. CIFS protocol is built into all recent MS-Windows operating systems.

Software

The HP CIFS products are available for the HP-UX 11i versions at no charge. The latest version can be found at http://software.hp.com under the "Internet ready and networking" link. The products can be use independent from the hardware below the operating system.

- **HP CIFS Client** (B8724AA; current version A.02.02.02)
  allows the mounting of windows-shares onto HP-UX. This functionality is only similar to

smbmount (from the Samba product suite). Cifsclient offers more options than smbmount e.g. the ability to validate users against the Windows-computer that offered the share even with Kerberos Authentication and it behaves different. The HP CIFS Product Suite includes a NTLM PAM module to authenticate unix users to against a Windows Domain Controller by NTLM authentication.
(http://www.software.hp.com/portal/swdepot/displayProductInfo.do?productNumber=B8724AA)

- **HP CIFS Server** B8725AA; current versions are as follows:

  HP-UX 11.11:
  A.02.03.06 based on Samba 3.0.22
  A.02.04.04 based on Samba 3.0.30

  HP-UX 11.23 and 11.31:
  A.02.04.04 based on Samba 3.0.22
  A.03.01.01 based on Samba 3.4.3

  The url to download CIFS Server is:
  http://www.software.hp.com/portal/swdepot/displayProductInfo.do?productNumber=B8725AA)

  HP CIFS Server contains some extensions and product configuration that HP can support. The various possibilities that samba offers by compiling it in different ways make it nearly impossible to support. To guarantee this supportability the HP-release of HP CIFS Server is delayed for approximately ½ years compared with the new samba releases. As samba is bound to the **GNU Public License** (**GPL**; http://www.gnu.org/copyleft/gpl.html) HP delivers the source code with HP CIFS Server as well.

Documentation

The documentation including Administration Guide and Release Notes can be found either at http://docs.hp.com under "I/O Cards and Networking Software" or in the file system after installing HP CIFS products:

for HP CIFS Client refer to:	`/opt/cifsclient/HP_Docs`
for HP CIFS Server refer to	`/opt/samba/HP_docs`.

Optionally you'll find information about CIFS server configuration in http://us1.samba.org/samba/oreilly/using_samba/ (O'Reilly Book online) as well as in your unix file system `/opt/samba/swat/using_samba`, which is the same book. The O'reilly book, which came out as second edition recently: www.oreilly.com (ISBN: 0-596-00256-4). The excellent help in swat can as well help to find the right parameter.

Please see list of weblinks at the end of this chapter too, at "Additonal Information".

Differences between HP CIFS and Samba

The main difference between HP CIFS Server and Samba is that HP guarantees support for the product. To guarantee this support the labs need to do extensive testing before a new release comes out. This means on the other hand that the HP CIFS Server release is approx ½ years

delayed. Security fixes will be back ported to HP CIFS Server asap in order to maintain a stable product.

Samba offers much more compile options and thus a large variety of usage, which makes it difficult to support. The compile options that are used for HP CIFS server can be seen in `/opt/samba_src/samba/source/configure_hp_options.sh`.

HP does as well provide the compiled Samba binaries for HP-UX on http://www.samba.org (External) for the latest Samba-version. But HP does not deliver Support for those binaries

Release Differences

The major differences in the three releases available for download as the types of Windows servers and clients that are supported. The clients that are supported by HP CIFS Server are as follows:

A.02.03.06 – Windows XP, Windows NT, Windows 2000/2003
A.02.04.04 – Windows XP, Windows NT, Windows 2000/2003/2003R2/2008, Vista
A.03.01.01 – Windows XP, Windows NT, Windows 2000/2003/2003R2/2008/2008R2, Vista, Windows 7.

HP CIFS Client A.02.02.02 has not been tested and is therefore not supported with Windows Server 2008 or 2008 R2.

Download

You can download HP CIFS Server from www.software.hp.com ”Internet ready and networking”.

Documentation

For those who are at their beginning of their samba-career we would recommend the following article, which is not essential to Samba3 but gives a very good understanding what samba is about: http://us4.samba.org/samba/docs/SambaIntro.html (HP external)

For the HP CIFS Server product we will deliver an Administrator’s Guide which will be on www.docs.hp.com meanwhile the best sources are:
Samba documentation pages http://us4.samba.org/samba/docs/ (HP external)

Book references for Samba3:

The Official Samba-3 HOWTO and Reference Guide: (Prentice Hall PTR (October 22, 2003) ISBN: 0131453556)

Samba-3 By Example / practical experience to successful deployment (John H. Terpstra; Prentice Hall PTR; Bk&CD-Rom edition (March 29, 2004) ISBN: 0131472216)

Both books are under GPL, so you can download them as pdf from samba.org:
"The Official Samba-3 HOWTO and Reference Guide"
"Samba-3 by Example"

Especially the HOWTO coolection is available in other languages: German for example: http://gertranssmb3.berlios.de/Samba-HOWTO-Sammlung.pdf (a link for French and Japanese is there on the samba/docs page as well.)

Install HP CIFS Server

In order to install HP CIFS Server you must have the LDAP-UX Client and the Kerberos Client installed. On HP-UX 11.11 systems you may need to install the LDAP-UX client, which is available from www.software.hp.com. On HP-UX 11.23 and 11.31 systems the LDAP-UX client and a base Kerberos client should be installed by default. However, you want to ensure you install the upgraded krb5client, which is also available on www.software.hp.com. The Release Notes for HP CIFS Server will give minimum versions of these clients that are required, but as a general rule having the latest version is recommended.

As of the writing of this document, the latest LDAP and Kerberos Clients are as follows:

HP-UX 11.11:
LDAP-UX Client B.05.01
KRB5CLIENT C.1.3.5.11

HP-UX 11.23:
LDAP-UX Client B.05.01
KRB5CLIENT D.1.6.2.09

HP-UX 11.31:
LDAP-UX Client B.05.01
KRB5CLIENT E.1.6.2.09

First steps

After swinstalling you should use /opt/samba/bin/samba_setup, unfortunately it did not work well in the technology preview, so here is the way doing it manually. (Sample for joining a Windows domain which uses ADS with Kerberos, one of the most common installations.)

Edit the /etc/opt/samba/smb.conf. The [global] section should contain

```
[global]
```

```
encrypt passwords = yes          # must be yes for actual Windows versions
security =  ads                  # if Kerberos should be used, choose ads
workgroup = gel2000              # ADS domain name
realm = GEL2000.GRC.HP.COM       # the same realm that you ADS is,
                                   and which is in /etc/krb5.conf
netbios name = picard            # hostname or netbios name,
                                   be sure DNS can resolve it
server string = CIFS Server 3    # just how samba presents itself
password server = grcdg227, *    # it is useful to name the KDC first
wins server = 15.140.145.16      # Wins is very useful in large environments
name resolve order = wins bcast # recommended resolve order
```

Use man smb.conf (or help offered in swat) to read about the available values. Use the 'testparm' command to check the syntax and unknown parameters in the smb.conf file.

Now you should check the /etc/krb5.conf:

```
[libdefaults]
        default_realm = gel2000
        kdc_req_checksum_type = 2

[realms]
        GEL2000.GRC.HP.COM = {
                kdc = grcdg227.grc.hp.com
        }

[domain_realm]
        .grc.hp.com = gel2000
[logging]
        kdc = FILE:/var/log/krb5kdc.log
```

The password server in smb.conf, and kdc in krb5.conf should have the same Windows ADS domain controller specified. It might be helpful (not mandantory) to choose the "Operations Master" for this.

Stop samba and (re-)move the /var/opt/samba/private/sectrets.tdb, then you should be able to join the domain by:

```
# net ads join -w gel2000 -U administrator
administrator's password: <enter domain admin password here>
Successfully joined domain gel2000.
```

If the computer account is not yet there it will be created. If it exists it should be reset automatically. You should be able to start samba now and test connections to the shares from the Windows clients.

If you get errors like:

```
[2004/11/19 09:06:41, 0] libads/kerberos.c:ads_kinit_password(135)
kerberos_kinit_password administrator@GEL2000.GRC.HP.COM failed:
Can't open/find Kerberos configuration file
[2004/11/19 09:06:41, 0] utils/net_ads.c:ads_startup(183)
  ads_connect: Can't open/find Kerberos configuration file
```

or

```
[2004/11/19 11:31:43, 0] libads/kerberos.c:ads_kinit_password(135)
```

```
kerberos_kinit_password administrator@GEL2000.GRC.HP.COM failed:
Cannot find KDC for requested realm
[2004/11/19 11:31:43, 0] utils/net_ads.c:ads_startup(183)
  ads_connect: Cannot find KDC for requested realm
```

➔ check the confirguration of the /etc/krb5.conf file. It must macht realm and password server in the smb.conf. Check nameresolution and network connection to the KDC. You can as well use the command:

```
# kinit Administrator@GEL2000.GRC.HP.COM
```

Runtime check

```
# ps -ef|grep mbd
    root  2767     1  0  Nov 23  ?         0:00 /opt/samba/bin/smbd -D
    root  2775  2767  0  Nov 23  ?         0:27 /opt/samba/bin/smbd -D
    root  2765     1  0  Nov 23  ?       149:03 /opt/samba/bin/nmbd -D
rdoelker  5821  2767  1 19:55:44 ?         0:00 /opt/samba/bin/smbd -D

# netstat -an |grep -e 139 -e 445 -e 137 -e 138
tcp        0      0  *.445                  *.*                    LISTEN
tcp        0      0  *.139                  *.*                    LISTEN
udp        0      0  *.137                  *.*
udp        0      0  *.138                  *.*
udp        0      0  15.140.10.103.137      *.*
udp        0      0  15.140.10.103.138      *.*
```

You will not see the smbd-ports in the lsof output, but there are 2 parent smbd's (here pid 2767 and 2775, which serve both tcp netbios-session ports: 139 and 445. The other smbd is 2 user-session as you can see in smbstatus as well:

```
root@hprtdu96:>smbstatus
Samba version 3.0.7 based HP CIFS Server T.30.PV.04
PID     Username      Group         Machine
-------------------------------------------------------------------
 7000   rdoelker      users         rdoelker     (16.58.6.204)
 7016   rdoelker      users         rdoelker     (16.58.6.204)

Service      pid     machine       Connected at
-------------------------------------------------------
kunden         7000   rdoelker      Mon Dec  6 14:30:37 2004
IPC$           7016   rdoelker      Mon Dec  6 16:04:46 2004
IPC$           7000   rdoelker      Mon Dec  6 10:25:51 2004
kunden         7016   rdoelker      Mon Dec  6 16:04:48 2004

Locked files:
Pid    DenyMode   Access      R/W        Oplock           Name
--------------------------------------------------------------
5821   DENY_NONE  0x2019f     RDWR    EXCLUSIVE+BATCH  /tmp/currently_open.doc  Mon Dec 6 14:31:48 2004
```

smbstatus –p # list pid and user
smbstatus –S # list shares
smbstatus –L # list locks

There is one smbd for rdoelker, which is from a mapped drive and another one which is from entering the UNC patch \\hprtdu96\kunden into the run line of the windows-client. Each time a IPC$ share is connected too.

Kernel

The sytem-requirements did not change much since CIFS A.01.08 (see table in "System requirements for Samba 2.2 on HP-UX 11.0 for PA-Risc). There might be some changes if you are running on HP-UX 11.23 September04 release. We will update this section if needed.

Generally each smbd needs 2Mb memory and uses 12 entries in the unix filetable (nfiles). The use of unix file locks (nflocks) should be the same as in the recommendations below. It was not possible to investigate the kernel values with the existing technology preview.

A word on HP-UX 11.0

As we have mentioned before HP CIFS Server 3 will not be offered for HP-UX 11.0, this is because the end of product life was 2004. As I know that the base of 11.0 users is very large I've tested a **UNSUPPORTED** configuration. You may get the 11.11 binaries to work on 11.0, but your HP support will **not support** this.

You need:

```
# swlist -l product |grep -e krb -e ldap
  KRB5-Client           B.11.00.15     Kerberos V5 Client 1.11
  LdapUxClient          B.03.20        LDAP-UX Client Services
```

Check for patches in the patch database and for newer version on www.software.hp.com. (KRB5-Client is named pam kerberos version 1.11 on software.hp.com)

Upon swinstall you may need the option "Allow installation of incompatible software", maybe you need to disable "enable script errors" to make it work. Then continues as describes above. I've taken the many of the systemoutputs from my 11.0 system. (rainer.doelker@hp.com).

Security parameters

A good document for protecting samba is http://www.samba.org/samba/docs/server_security.html (HP external). Besides we list some of the new smb.conf parameters which might be worth to think about.

server schannel
the server schannel is a global parameter which rules if a netlogon schannel is offered or demanded. If set to auto (default) it offers the schannel but does not enforce it. If set to yes Clients prior to NT4SP4 will be excluded. This seems similar to the WindowsXP Registry value requireSignOrSeal

server signing
server signing is another global parameter which offers [auto|mandatory|disable]. Auto (default) will offer SMB signing but not enforce it.Mandatory will SMB signing is required, this will exclude connections to older Windows Servers. SMB signing is a feature which approx started with Windows 2000 SP3.

The same values exist for the communication with the clients: **client schannel** and **client signing**. Furthermore there are two values which should be kept to Yes: **client use spnego** and **use spnego**. Samba will try to use Simple and Protected NEGOciation (as specified by rfc2478) with WindowsXP and Windows2000 servers and clients to agree upon an authentication mechanism.

Copy = other service (S)

HP CIFS client

A simplified way to explain HP CIFS Client is that it is a translation mechanism for NFS-RPC calls into CIFS protocol and back. HP CIFS Client enables HP-UX users to mount shares as UNIX filesystems from a CIFS/SMB protocol speaking file servers (including W95, W98, WinNT, W2K, W2K3, ASU, CIFS server or Samba)

CIFS client allows to restrict access permissions for users. Users are being validated against the connected Windows/smb server. CIFS client can as well be part of a domain to easily validate domain-users. CIFS client can archive mounts and cifslogins in a binary database file to re-establish connections after restarting.

The basic configuration file is `/etc/opt/cifsclient/cifsclient.cfg`

HP CIFS Client current version

The current version of HP CIFS Client is A.02.02.02, which offers extended kerberos support. This means that cifsclient depends on an additional software package which brings the relevant kerberos libaries. The bundle is called "pam kerberos J5849AA" you can download the software from www.software.hp.com <security and manageability> for free. The actual cifsclient version will be found on www.software.hp.com as well under <internet ready and networking>

HP CIFS Client technically seen

cifsclientd acts as NFS server for the internal HP-UX kernel, whilst the kernel is the NFS client to cifsclientd. Externally cifsclientd speaks smb/cifs protocol. Having understood this it is much easier to work with cifsclient and understand the messages in syslog.log which are are flagged as NFS. (e.g. "NFS server <windows-server> not responding", that is cifsclientd which is not responding.) Furthermore this would explain that if the kernel believes that a mount is still active

and cannot be unmounted the only way to get rid of the mountpoint is reboot. It is the same as with nfs.

General commands

Generally all commands deliver a short help if you start them with argument "-?" or "-h"

cifsclient {start|stop|restart|ver|force_umount}:
cifsclient does start and stop the daemon.The cifsclient startup would give back a process id. The cifsclient stop would unmount all cifsmounts while stopping the daemon. There are other options like "start, stop, restart, status, ver". A very special one is the "force_umount" option, which should be used only if cifsclient is down. This might be helpful if a mountpoint is hanging and could not be unmounted when cifsclient was shutdown.

cifsmount; mount –F cifs:
'cifsmount' and 'mount –F cifs' are the same. The most common mount is

```
cifsmount //<server>/<share> <mountpoint> -U <username> -s
```

This will prompt you for the password of the remote (windows) user. If you perform the command as root and do not parse a username then the 'remote root' is equal to the windows Administrator.

If you use cifsmount with options `-s -U` you can save password and mount into a databasefile which is located in `/var/opt/cifsclient/cifsclient.udb`. This will cause that every time cifsclient is restarted (including reboot) the cifsmounts are reactivated. This is an enhanced functionality compared with mount.

`-s` Save mount and password in database (please do not use unless you understand the security implications). This is expecially useful it you want to have mounts enabled with the cifsclient start. `-U <username>` Username sent to (windows) server.

cifslogin:
The cifslogin command is used to authenticate additional users at a server. Only authenticated users may access mounted files. Each user accesses the file at the server with his or her privilege status at that server. Because there must be a one to one (many to one) mapping from local users to remote user names, every user can log in only once at a given server. By default, cifslogin sends the user's login name to the server. If this is not desired, the username can be given in the commandline.

cifslist:

```
root@hp-ux:>cifslist
=====================================================================
server NTSERV:
=====================================================================
Remote Username: administrator  Local Username: root
```

```
Share: \\NTSERV\PUBLIC
  rw /cifs_mnt
```

cifslist is a command to view which shares and servers are connected and which user is logged in. Users normally need to validate against the NT-server by using the cifslogin command to be able to access the share.

cifslogout <server>:
A user needs to use cifslogout to end his session with a dedicated server. An option available is "-a" which will log the user out from all their current sessions.

cifsumount {<mountpoint>|-a}; umount:
cifsmount is used to unmount a cifs filesystem. Usually you specify a mountpoint but you can as well use `-a` to unmount all connected cifs filesystems. You have the `-d` option available to remove an entry from the database file so that share is not remounted after restarting cifsclientd. You can as well keep users logged in to the windows-server, if several shares are mounted, and you only unmount one of those. This is done by the `-k` option.

Guest account

It is possible to setup a “guest” user in CIFS Client if you have a mount point what you want to allow any user on the HP-UX server to access with no authentication. With the CIFS Client product on HP-UX, if not guest access is permitted then each Unix user or process has to be individually authenticated as a Windows/SMB user. This is different from other CIFS Client type applications, like the OpenSource smbmount (smbfs). If a share is mounted on linux using smbmount all unix users can access the files on the share. However, cifsclientd has a separate authentication mechanism that verifies access permissions with the windows server where the share is shared.

The following /etc/opt/cifsclient/cifsclient.cfg parameters are what is used to setup guest access to a mount:

guestPassword = "guest";
guestRemoteUser = "guest";

The guestUser configuration solves the following problem: Each Unix user must be logged in at the windows server, that means being authenticated as a user on the Windows/SMB server, in order to access anything, even if the share is public. It may be impractical to log in each user if there's a large number of Unix users who want to access a public share where access permissions are not important. If you define a "guestRemoteUser", all Unix users that are not logged in to the windows-server are treated as if they were the given Windows/SMB username behind guestRemoteUser. The “guestPassword” must be the valid password for the Windows/SMB user account specified.

HP CIFS Client and WAN

Some configurations require special settings. So we noted that when using cifsclient connections over a wide area network (e.g. ISDN router) then you might have to adapt some of the parameters in `/etc/opt/cifsclient/cifsclient.cfg`:

```
//nfsTransferSize       =       8192;       //       unchanged       !
connectTimeout  =  5000  //  timeout  for  netbios  connection  in  ms
requestTimeout  =  40000     //  timeout  for  SMB  reply  in  ms
nfsTimeout  =  600     //  initial  nfs  timeout  in  1/10  seconds
nfsRetransmit = 8 // number of nfs retransmissions
```

HP CIFS Client and permanent mounts (fstab)

Usually HP-UX administrators would write a mount that they want to be initialised at boot time into the `/etc/fstab`, which is processed during system startup. During that time cifsclientd is not yet running. This means that mounting a smb/cifs-share to a HP-UX-system should be possible without a manual mount or an entry in the `/etc/fstab`! HP CIFS client offers a very nice feature, which holds the connected shares, servers, users and password in a binary database. This enables cifsclientd to remount each share that was in use after it has been stopped and restarted. Therefore no `/etc/fstab` entry is needed. The option to use is `-s`. The databasefile containing this info is `/var/opt/cifsclient/cifsclient.udb`.

```
root@hp-ux:>cifsmount //NTSERV/public /cifs_mnt -U administrator -P -s

root@hp-ux:>cifslist -A
==========================================================================
server NTSERV:
==========================================================================
Remote Username: administrator  Local Username: root

Share: \\NTSERV\PUBLIC
  rw /cifs_mnt
```

So you can see that we're now connected to NTSERV as administrator which is locally handled as root. We can now check for the existance of the database file we mentioned and check its contend:

```
root@hp-ux:>ll                                  /var/opt/cifsclient/cifsclient.udb
-rw------- 1 root sys 244 Jul 11 13:59 /var/opt/cifsclient/cifsclient.udb

root@hp-ux:>cifslist -M
mountpoints in database:
--------------------------------------------------------------------------
Mountpoint Share
  Server Name  Server IP  Port  Client Name  Local User
--------------------------------------------------------------------------
rw /cifs_mnt \\NTSERV\public   NTSERV 139 root
```

This would survive a `cifsclient stop` or even a reboot. As cifsclientd connects the servers and mounts the shares which are in its databasefile. That would finally mean that if you start cifsclient in runlevel 2 by its startscript it would map all the shares for you, so that they are

usable by the system.

Debugging

To enable an enhanced logging you need to edit `/etc/opt/cifsclient/cifsclient.cfg`. Remove slashes before the statement you want to get more information about. The changes will become active as soon as you close the file. A restart of the cifsclient is not needed. Logfiles will be found in `/var/opt/cifsclient/debug` the naming convention is `cifsclient-log.pid`.

```
# The following section defines the logging verbosity. All possible levels
# of logging are given, most of them are remarked.
logLevels = (
  info,
  error,
//  debug,
//  resource,
  netbiosError,
//  netbiosDebug,
//  netbiosTrace,
//  nfsTrace,
//  rare,
//  cacheDebug,
//  cifsTrace,
//  oplock,
  warn,
//  smbSequence,
//  debugAttributes,
//  debugSSL,
)
```

If the cifsclient cores then the core files are below `/var/opt/cifsclient/core`. A file cifsclientCoreFileInfo to document the cores is there too. It as well documents if a starting cifsclient renamed one of the core-files these are then called core.renamed.by.pid.

Cifsclient may result in communication difficulties with server that implemented their own cifsprotocol. We know about some difficulties with "DELL PowerVault NAS 740 N", "EMC celerra"; "USS (Unix System Services) of OS/390" and "Network Appliance". Note that these servers are not in the tested list and therefore not supported. If we encounter a problem that is caused by us we will take care to find a fix, but if it is a protocol error of the server we have no influence to this.

CIFS client at one glance

Info commands

Info Command	*Options*	*Comment*
`cifslist`	`-A`	List connected servers with shares and mountpoints.
	`-M, -U`	Readout database (mounts, users).
	`-s <server>`	List open shares to a server
	`-u <server>`	List users logged in to a server
	`-m <share>`	List mountpoints fore a share

Info Command	*Options*	*Comment*
`cifsclientd`	`ver`	Get version information from cifsclientd

Daemons

Daemons	Options	Comment
`cifsclientd`	`{stop|start|restart}`	Start, stop or restart the main daemon
	`force_umount`	Umount a hanging mountpoint after cifsclient is shutdown

Start commands

Startup Commands	Options	Comment
`/sbin/init.d/cifsclient`	`{stop|start}`	Startscript
`/etc/rc.config.d/cifsclient`	`RUN_SAMBA={0|1}`	Runvariable
`/sbin/rc2.d/S900cifsclient`		Cifsclientstartscript for booting.
`/sbin/rc1.d/K100cifsclient`		Cifsclientstopscript for shutdown

Relevant directories

Directories	Subdirectories	Purpose
`/opt/cifsclient/`	`bin/`	binaries
	`HP_docs/`, `docs/`	documentation
	`pam/`	the ntlm pam module
`/etc/opt/cifsclient`		configuration data
	`pam/`	the ntlm pam module config
`/var/opt/cifsclient`		sockets and pid-file
	`core/` and `debug/`	location of corefiles and debug files
	`pam/`	the ntlm pam module data

HP CIFS Server

Introduction to CIFS server

Generally speaking the following descriptions will fit to the most Samba servers as well as HP CIFS server is based on Samba. Mainly some of the UNIX path will be different and some small programs may not be available. Therefore we will continue to speak about “Samba” instead of “HP CIFS server”.

HP Samba offers a configuration script `/opt/samba/bin/samba_setup` that will do the initial

basic configuration:

```
Proceeding with samba_setup...

You now must choose a role for your server.
1) primary_domain_controller
2) backup_domain_controller
3) Windows_domain_member_server
4) ADS_member_server
5) workgroup
6) CANCEL
```

To understand what the script is about it is important to know what's behind the concepts you may choose:

- Samba can be a PDC or BDC (this does not yet allow synchronization to NT-BDCs)
- Samba can be a domain member server
- Samba can be a workgroup server, whereas the workgroup server offers itself three different validation methods.

These different concepts are represented by the `smb.conf` parameter "`security = …`". In the following context we will explain roughly what these parameters are about. For detailed reading check out the O'Reilly book "Using Samba" (Chapter 6).

The **WindowsNT domain model** provides advantages like grouping workstations and servers under the authority of a domain controller (DC) which allows central administration. The domain controllers are the servers which perform all user logons and authentication. In Windows Active Directory domains the domain controllers all share updates so that each DC contains the same information in the accounts database. Domain trusts allow access to resources over domain boarders. Microsoft provides graphical tools, such as Active Directory Users and Computers, to administrate the domain.

Samba can be a PDC

PDC (*Primary Domain Controller*) is responsible for several tasks within the domain such as: Authenticating user logons for users and workstations that are members of the domain. A PDC acts as a centralized point for managing user account and group information for the domain. A user logged on to the PDC as the domain administrator can add, remove or modify Windows domain account information on any machine that is part of the domain.

HP CIFS Server provides the ability to act as a Primary Domain Controller for Windows 95, 98, NT, 2000 and XP-clients including domain logon feature for Windows NT 4.0 SP3+ and Windows 2000 clients. You can map built-in Windows groups and username to Unix groups. It allows to view resources by the MS-server manager. It supports local and roaming profiles for domainusers and with a specified logon home share for domainusers.

Features like SAM database (*Security Accounts Manager* database; containing NT user account

information) and any *BDC* (*Backup Domain Controller*) features are currently not implemented. So the Samba PDC is not able to synchronize with any native NT-BDC which means BDCs are currently not supported in a Samba domain. Because of this, if the PDC fails, there is no way for Windows clients to authenticate to the domain. And, if a disk fails on the PDC, there is no backup on the domain with the critical credential data. This means that it is very important to make backups of users credential files. It also means that there is no system that can easily be promoted to a PDC to replace the current one.
All necessary settings will be done by `samba_setup` for you. For more detailed maintenance information check the section later in this chaper.

Samba can be a domain member server

HP CIFS Server can operate in a Windows Active Directory domain as a "domain member server." This allows the clients that want to connect to and use resources on the CIFS Server to be authenticated based on their Windows Domain account information. ver, a Windows NT workstation, or a Windows 98 or a HP CIFS server machine. The domain member servers will contact a domain controller and request the DC authenticate the credentials of the client requesting access to the resource. The advantage of this is a separate password is not required to be maintained on the HP CIFS Server. The authentication is done using the Windows NTLM or NTLMv2 authentication protocol.

To use Samba as domain member you need to select the following in the smb.conf file:

```
security = domain
```

Samba can be a ADS Member Server

HP CIFS Server can operate in a Windows Active Directory domain as a "ADS member server." When CIFS is configured as a ADS member server the authentication protocol that will be used by default is Kerberos, as opposed to the NTLM/NTLMv2 that is used when configured for a domain member server. Starting with Windows 2000 domains Microsoft started using Kerberos as their default authentication protocol. The NTLM and NTLMv2 is still available for compatibility with older clients, but Kerberos is considered more secure and the preferred method. When a client attempts to connect to a resource on the CIFS Server, their credentials will be checked by the Windows domain controller using the Kerberos protocol if available.

To use Samba as a ADS member server you need to select the following in the smb.conf file:

```
security = ads
```

Because the default authentication protocol is Kerberos this means you will need to have the Kerberos client configured and functional on HP-UX. When you run the samba_setup script, it will create the Kerberos configuration file, /etc/krb5.conf, if one does not exist. In order for CIFS Server to join the Windows AD domain, the Kerberos client must be functional which can be tested with the 'kinit username' command.

Samba can be a workgroup server

A workgroup server is a server in an environment with several windows clients and servers, which are not centrally administered. Samba can act as a workgroup server with three different security levels:

- `security = share`
  this security level is one which is hard to understand as any valid password by any user to any share can be used. HP does not recommend this security level.
- `security = user`
  this security level clearly validates users against their user databases. This can be the unix passwd or the smbpasswd file, depending on the value *encrypted passwords*.
- `encrypt passwords = {yes|no}`
  depending on this value samba gets to know how to handle incoming passwords. If set to `yes` then all passwords are encrypted and must be checked in the Samba encrypted smbpasswd file. If set to `no` then Samba requires an unencrypted password that is checked in the unix password database.

The default entry that `samba_setup` does for you if you choose workgroup server is `encrypt passwords = yes`. Windows clients by default only will send an encrypted password. There are registry changes required to have the client send a unencrypted password, but this is not recommended.

After doing this basic configuration you may want to start the server, do some first access tests and do additional configurations.

Starting the services

Besides the start scripts to start Samba during boot time HP offeres two other useful scripts to stop and start Samba daemons: `startsmb` and `stopsmb`. These are located like all other Samba binaries in `/opt/samba/bin`. View as well the table at the end of this chapter.

SWAT

The *SWAT* tool (Samba Web Administration Tool) is provided with Samba suite which can be used to set up or change your Samba configuration in the smb.conf file via web access. In other words it is an enhanced vi for smb.conf with a webserver frontend that offers excellent help to each configuration item. You can modify globals, shares, and printers using SWAT.
The startup of swat should be enabled by appropriate configuration in the unix services (ruled by `/etc/nsswitch.conf`) and `/etc/inetd.conf`. The entry in `/etc/inetd.conf` should look like:

```
swat  stream tcp nowait.400 root /opt/samba/bin/swat swat
```

You can start swat from any web browser by entering the URL http://<sambaserver>:901. Then

you need to authenticate as root.

Useful share configuration parameters

strict allocate
This is a boolean that controls the handling of disk space allocation in the server. When this is set to yes the server will change from UNIX behaviour of not committing real disk storage blocks when a file is extended to the Windows behaviour of actually forcing the disk system to allocate real storage blocks when a file is created or extended to be a given size. In UNIX terminology this means that Samba will stop creating sparse files. This can be slow on some systems.
When strict allocate is no the server does sparse disk block allocation when a file is extended or created. Sparse file means that a file with zero byte is written with a large enough offset and zeros are written to it to make sure the physical space adequate for the entire eventual operation is available before writing data to the file. A zero byte write request to an offset beyond the eof is typically used by MS applications (Outlook, writing pst files; MS Office) to 'extend' a file. If the used OS is actually reserving this space by writing 'zeros' to each and every byte between 0 and the offset, this could conceivably take a long time.

Setting strict allocate to yes would cause Samba to reject a zero write request and instead start writing data imidiately:

```
strict allocate = yes
```

level2 oplocks
This parameter controls whether Samba supports level2 (read-only) oplocks on a share. Level2, or read-only oplocks allow Windows NT clients that have an oplock on a file to downgrade from a read-write oplock to a read-only oplock once a second client opens the file (instead of releasing all oplocks on a second open, as in traditional, exclusive oplocks). This allows all openers of the file that support level2 oplocks to cache the file for read-ahead only (ie. they may not cache writes or lock requests) and increases performance for many accesses of files that are not commonly written (such as application .exe files).
The `oplocks` parameter must be set to true on this share in order for this parameter to have any effect.

oplocks
This boolean option tells smbd whether to issue oplocks (*opportunistic locks*) to file open requests on this share. The oplock code can dramatically (approx. 30% or more) improve the speed of access to files on Samba servers. It allows the clients to aggressively cache files locally and you may want to disable this option for unreliable network environments (it is turned on by default in Windows NT Servers). For more information see the file Speed.txt in the Samba docs/ directory.

Oplocks may be selectively turned off on certain files with a share. See the `veto oplock` files parameter.

We have often realized that applications such as MS Outlook and SAP printing have problems if oplocks is turned to yes. At least as a test we recommend to set it to no:

```
oplocks = no
```

General user validation

Sometimes it is important to have a good insight to what happens if a user “maps a network drive” on his Windows client or just enters a UNC path in the run command line of the startmenu like \\sambasrv. The first step is called session-setup and the second is called tree-connect.

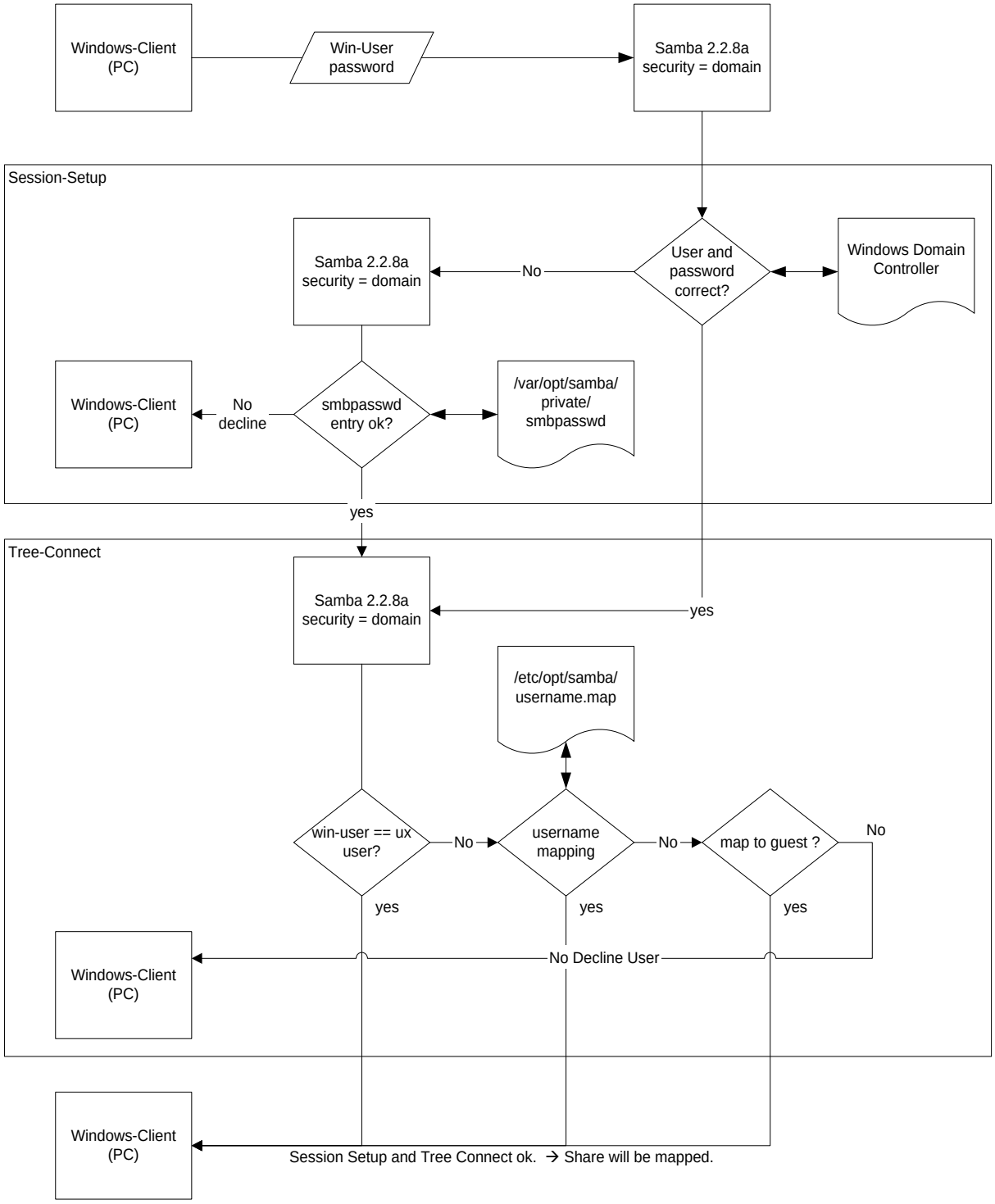
session-setup:
At first cifs-server (samba) examines if a Windows-account/Windows-user is known to the system. How cifs-server will authenticate the user which sends an "encrypted password" from Windows is ruled by smb.conf configuration:

smbpasswd (security = share/user)
a Windows-password-server (security = domain/server)

tree-connect:
After successful validation of the Windows-access the Windows-user will be mapped. If the Windows-user equals a unix-user then cifs-server will look into the /etc/passwd (NIS respectively). If the Windows-user does not match a unix-user cifs-server will look up the the nt-user in the user.map file:

mapable to unix-user then /etc/passwd (or NIS)
if unknown then map to "guest account"

The following picture will illustrate this for a Samba which is configured as Domain-Member-Server. Which includes "encrypt passwords = yes”, as WindowsNT, Windows2000 and WindowsXP send encrypted passwords only.



Maintaining a Samba PDC

Create the Machine Trust Accounts on the HP CIFS Server:

Creating machine trust accounts for Windows clients means creating machine accounts in the

/etc/passwd file and machine. account entries in the /var/opt/samba/private/smbpasswd file. The following are the steps to create a machine account for a Windows client on a HP CIFS Server acting as a PDC: create a new group called "machines" in the /etc/group file then create the machine trust account for a Windows client in the /etc/passwd file.

```
groupadd machines
```

Create the machine trust account for a Windows client in the /etc/passwd file. For example, the /etc/passwd entry for the Windows client named "CLIENT1" machine would be:

```
client1$:*:801:800:NT Workstation 1:/home/temp:/bin/false
```

Where 801 is a uid and 800 is the group id of a group called "machines". The machine account is the machine name with a "$"appended. The home directory is /home/temp. The shell field in the /etc/passwd file is not used and can be set to /bin/false. The same with the password, as it is set to asterix you do not expect anyone to log in as client1. The suitable useradd command line is:

```
useradd -g machines -c "NT Workstation 1" -s /bin/false
        -d /home/temp -u 801 client1\$
```

NOTE: useradd supports only 8 character names! Therefore if you want to use long netbios names you need to edit the Unix passwd manually.
In addition to this you need to run the smbpasswd program to add a machine entry for a Windows client to the /var/opt/samba/private/smbpasswd file:

```
smbpasswd                  -a                  -m                  client1
smbpasswd  -e  -m  client1
```

NOTE: smbpasswd supports netbios-names up to 15 characters.

To remove a Windows client you need to delete it from /etc/passwd and use the following smbpasswd commandline:

```
smbpasswd -x -m client1
```

To successfully join the Samba domain with a PC client you need to connect with a user from smbpasswd that has the Unix-id "0"!

Configure Domain Users:

You can use useradd command to configure domain users, domain administrators and domain guests on a samba PDC:
Create a "Domain Users" in the unixgroup users with unixname domuser:

```
useradd -g users -c "Domain Users" -s /usr/bin/sh domuser
```

Create a "Domain Administrators" in unixgroup adm with domadmin as unixname:

```
useradd -g adm -c "Domain Administrators" -s /usr/bin/sh domadmin
```

Create a account in the unixgroup guest (this might not be there yet) with unix name domguest

and realname "Domain guest":

```
useradd -g guest -c "Domain Guest" -s /usr/bin/sh domguest
```

Create a user that will be the admin-user which needs to have unix-id "0" to create computer accounts etc.:

```
useradd -g sys -c "Samba Admin" -s /sbin/sh -d /home/sambaadm –s /bin/false
sambaadm
```

You will have to change the uid manually to "0" in /etc/passwd. You need to put this kind of root-user into the smbpasswd as well!

If you are using NIS, do not forget to publish the new passwd and group file into your environment.

smb.conf file should look like this:

```
[global]
workgroup = SAMBADOM
security = user
domain logon = yes
domain master = yes
local master = yes
encrypt passwords = yes
admin users = sambaadm
printer admin = sambadm
domain admin group = sambaadm, @adm
domain guest group = @guest
logon script = \\%N\%U.bat

[netlogon]
comment = The domain logon service
path= /var/opt/samba/netlogon
writeable = no
guest ok = no
```

The above configuration parameters do significantly show that the HP CIFS Server is configured as a PDC:

domain logons = yes	this parameter indicates that cifs server is acting like a PDC
encrypt passwords = yes	if this parameter is set to yes, passwords used to authenticate users will be encrypted. This parameter must be set to yes when the HP CIFS Server acts as a PDC. This is as well needed for WinNT-, WinXP- and Win2k-clients as these send encrypted passwords.
domain admin group	this parameter offers a list of users which have permissioins as domain administrators.
admin users	is a share-level option to have users administering a share, all operations of the listed users will then be performed as root.

Printer driver upload within Samba

To configure printers and uploadable printer drivers for HP CIFS server you would at first create a [printers] share to provide the printers known by the server (e.g. via lpstat). Be sure the path has a valid path that is accessable. To configure a [printers] share you would edit the `/etc/opt/samba/smb.conf` file:

```
[printers]
path = /var/opt/samba/tmp
printable = yes
browseable = no
```

This share is required if you want the printer's list to be displayed in SWAT which is not defined in the `smb.conf` file, but exists on the HP CIFS Server. If this share is not defined, the printer list will display only those printer-shares which are defined in the `smb.conf` file. The path is only a suggestion you may as well simply use `/tmp` or `/var/tmp`. The path `/var/opt/samba/tmp` does not yet exist, you need to create it:

```
mkdir /var/opt/samba/tmp
```

To setup CIFS version A.01.08 (Samba2.2.x)or later for automatically uploading of printer drivers to a PC client you need the following setup. The account used to connect to the Samba server must have a uid of "0" (ie. a root account) or it must be a member of the "printer admin" list.

This will require a [global] smb.conf parameter as follows:

```
[global]
printer admin = ntadmin
```

Make sure you have the printer admin defined properly in the global section of the `smb.conf and added the user to smbpasswd file`. Use smbstatus to make sure you are logged in as root. If you have an outstanding IPC$ connection to the server, you may find that you aren't getting logged on as expected.

Now create a [print$] share in the `smb.conf` file that points to the directory `/etc/opt/samba/printers` on the HP CIFS Server:

```
[print$]
path = /etc/opt/samba/printers
browseable = yes
guest ok = yes
read only = yes
write list = ntadmin
```

In this example, the parameter "write list" specifies that the user accounts with administrative level have write access to update files on the share.

In order for the HP CIFS Server to support the downloading or uploading of multiple client

architectures, we need to create subdirectories under the [print$] share that correspond to each of the supported client architectures. Create the subdirectory tree, under the [print$] share, for each architecture that needs to be supported:

```
cd /etc/opt/samba/printers
mkdir W32X86
mkdir Win40
```

The driver files will be stored in the `/etc/opt/samba/printers/W32X86/2` subdirectory for the Windows NT/2000 client or `W32X86/3` for WinXP clients. The driver files for Windows 9x will be stored in `/etc/opt/samba/printers/Win40/0` subdirectory.

Select a suitable driver for the client e.g. Windows 2000. When selecting a recent driver from the web http://welcome.hp.com/country/us/eng/software_drivers.htm for your printer, it might be that the driver is not uploadable. Sometimes it is then helpful to switch to the postscript driver for the same printer.

It is important to go in the right path to get the message *"Device settings can not be displayed. The driver for the specified printer is not installed, only spooler properties will be displayed. Do you want to install the driver now?".* In our example on Windows 2000:

Right click on "My Network Places"
Explore -- Expand "Entire Network"
expand "Microsoft Windows Network"
expand down to the servername
double-click on the "Printers" folder (not the printer at this level if it shows up)
doubleclick on the printer at this level.
Use Printer -> Properties menu.

This should display the error message *"Device settings can not be dis....."*(see above). From here follow the prompts to add the device in the "Add Printer Driver Wizard". This will place the device files on the CIFS Server in the subdirectories under the [print$] share.
Download the device files from the web and uncompress them into a directory on the PC which you would like to use when clicking on the "Have Disk" button in the "Add Printer Driver Wizard". When the Wizard completes you can see a popup window which indicates the files are being copied to the path on the CIFS Server. You can then go to the path on the CIFS server and verify that the drivers were copied correctly.

The printer driver files can be automatically uploaded from a Windows NT, XP or Windows 2000 client to a HP CIFS Server. However, in order to upload Windows 9x printer files to a HP CIFS Server, the files must first be copied (using a floppy disk, CD or similar transfer medium) to a Windows NT, XP or Windows 2000 client. Once they are stored on this client, they may be uploaded to a HP CIFS Server.

Otherwise you could simply install the printer locally to a windows workstation and then map the print$ share and pull up the files from c:\windows\system32\spool\drivers\w32x86. Then you

will need to use the rpcclient command to announce the driver to the printer.

```
root@hprtdu96:>rpcclient hprtdu96 -U ntadmin%password -c enumprinters
cmd = enumprinters

        flags:[0x800000]
        name:[\\hprtdu96\grcdg101]
        description:[\\hprtdu96\grcdg101,,BW/Laser 5si ground floor]
        comment:[BW/Laser 5si ground floor]
```

You may lookup the correct name for the dirver when choosing it from the APW (add printer wizard) if you pretend to install it locally.

```
root@hprtdu96:>rpcclient hprtdu96 -U ntadmin%password -c "setdriver grcdg101
\"HP LaserJet 5Si/5Si MX PS\" "
cmd = setdriver grcdg101 "HP LaserJet 5Si/5Si MX PS"
Succesfully set grcdg101 to driver HP LaserJet 5Si/5Si MX PS.
```

After that the printer will look like this.

```
root@hprtdu96:>rpcclient hprtdu96 -U ntadmin%password -c enumprinters
cmd = enumprinters
        flags:[0x800000]
        name:[\\hprtdu96\grcdg101]
        description:[\\hprtdu96\grcdg101,HP LaserJet 5Si/5Si MX PS,BW/Laser 5si
ground floor]
        comment:[BW/Laser 5si ground floor]
```

Now APW (add printer wizard) selected printer, driver automatically mapped!!

MC/ServiceGuard packages and configuration

The steps to configure CIFS Server to run as part of a ServiceGuard package are described in detail in the `/opt/samba/HA` directory. The README.txt file in this directory contains the instructions needed to setup CIFS to work with ServiceGuard. This file is always kept current for the version of CIFS Server that is installed on the system and should be used as the primary reference guide. You will also find template files to be used to add CIFS to the package, and to monitor the status of CIFS on the node once running.

CIFS Server can be configured to run in an "active-active" ServiceGuard cluster because multiple instances of its NetBIOS and SMB master daemons are allowed on the same node.
Each CIFS Server has its own smb.conf file to define its behavior. The NetBIOS name and IP address that the client connects to is used to decide which smb.conf file is used for the connection. This multiple CIFS master daemon configuration allows HP CIFS Server
to run multiple Serviceguard packages simultaneously.

When a failover occurs, Serviceguard transfers the IP address from the failing cluster node to another node. When Serviceguard moves the package from the failing cluster node to the other node, it activates the appropriate CIFS Server on a remaining node. With the

IP address switched, all the traffic that was going to the failed node now goes to the other active node. The key is to have a CIFS Server configured to look and act just like the CIFS Server that was running on the original node.

The /opt/samba/HA/README.txt file provides the smb.conf parameters that need to be configured and the detailed instructions for completing the MC/SG configuration for CIFS.

Troubleshooting

The first thing is to separate the messages, according to client, process and time-stamp. If this is done you need to ask the users what they did when expiring the problem.

Add to `smb.conf` into the [global] section:

`debug timestamps = Yes`	default
`debug pid = Yes`	this will prompt the smbd-pid for each message
`log file = /var/opt/samba/log.%m`	this will create a logfile separately for each client where `%m` is substituted to the netbios name of the client
`syslog = 0`	this determines which loglevel is put to syslog, even with "log level = 10" only errors (level 0) will go to syslog.
`debug level = 1`	this will write down new established connections as well. the same as "log level"
`max log size = 1000`	eventually more, depending on diskspace in `/var/opt/samba`

These options together will do the following (clientname: fish):
The client fish connects a Samba share. A file `/var/opt/samba/log.fish` will be written and according to log level the start of the smbd is documented with its pid. So it is possible to see if the pid changes meanwhile you monitor the problem. You should ask the users when they happened to see the problem. If you can identified the action that leads to the problem it might be worthwhile to increase the log level and max log size (described below) in order to take a snapshot of the problem only.

If you have identified the client which has got the problem, and you do not want to increase the log level for all pc-client-connections you may increase the log level by sending the serving smbd a specific signal:

Finding the serving smbd can be managed by smbstatus:

```
# /opt/samba/bin/smbstatus

Samba version 2.2.12
Service  uid  gid  pid machine
----------------------------------------------
trainings  rdoelker users  383 fish (15.139.20.64) Tue Apr  1 17:11:23 2003
IPC$ rdoelker users  383 fish (15.139.20.64) Tue Apr  1 10:36:55 2003
```

So in this example the process for client "fish" is 383.

You would find the process that serves the client by `smbstatus` and send it a signal using `smbcontrol <pid> debug 10` in order to get directly to debug level 10:

```
# /opt/samba/bin/smbcontrol 383 debug 10
```

Troubleshooting the startup:
This helped for troubleshooting problems where the connection is working properly, e.g. a problem deleting a file. But if you need to debug a client from it's start, e.g. to see as whom you are connected. You could turn on full debug (for all clients) or you work with an include-statement in smb.conf:

```
[global]
include = /etc/opt/samba/include.%m
```

additional create for the client (e.g. fish)you want to debug an includefile:

```
/etc/opt/samba/include.fish

debug level = 10
max log size = 10000
```

This will cause two 10 Mbyte logs to be created with debug level 10 data stored for client fish as soon as it connects. This allows to decide if the connection is made by the user you think it is done.

In any case it is worth to empty the logfile for a client before doing a specific test. This is done by:

```
# cat /dev/null > log.fish
```

Deleting logfile content for all clients without affecting the smbd output could be done by:

```
# for i in `ls |grep log. `; do cat /dev/null > $i; done
```

If you move a file the filedescriptor that smbd knows about will move as well and the writing continues. If you delete the file a running smbd will not direcly write a new one.

Troubleshooting a specific problem:
Lets say an application cannot save a file it has created. It would be good to have logging

enabled as described above and it might be worth to see as whom you are connected therefore the include file is the best option, especially for CIFS server that handle connections.

- Empty the logfile and connect to the share.
- Make a copy of the log while it was connecting.
- Prepare everything to reproduce the error.
- Empty the logfile again.
- Reproduce the error and
- Make another copy of the logfile which has captured the error.
- Be able to describe what steps are needed on the client to reproduce the error.

To be able to find the error a copy of `smb.conf` and output from `/opt/samba/bin/testparm -s` is needed along with special information what the share is like: e.g. nfs-mounted or using jfs-acl's. Of great interest are as well software-versions (i.e. **Client operating system** and **ServicePack**, **programs** involved and their **versions**).

Using nmblookup and about browsing

nmblookup is a tool to troubleshoot networking, name resolution, browsing (e.g. "search computers") and WINS items. Generally items of browsing are nothing that can be debugged very fast, because browsing and propagating information might take hours (according to MS-Q-Articles). Now we will provide a short overview about the usability of nmblookup and useful `smb.conf` parameters regarding browsing. You will find browsing explained in more detail in `/opt/samba/docs/textdocs/BROWSING.txt`. Usually browsing should not work across subnet borders as the broadcasts are not forwarded. If your network is subnetted and you need to reach another subnet the best way is to make use of a wins server:

wins server = 192.9.200.1

> This specifies the IP address of the WINS server that nmbd should register with. You need to set up Samba to point to a WINS server if you have multiple subnets and wish cross-subnet browsing to work correctly. See nmblookup usage if you do not know who the WINS is, alternatively ask a Windows administrator or check `ipconfig /all` in the DOS box of a PC client. (WINS service is using port 42)

wins support = yes

> This boolean controls if the nmbd process in Samba will act as a WINS server. You do not need to set this to 'yes' is you have another windows server which offers the WINS service.

Generally speaking browsing is done by broadcast requests which are normally answered by so called master browsers. These are servers that keep a list (name cache) and answer the broadcasts and as well propagate the browse list to other master browsers. There are 2 kinds of master browsers: domain master browser (DMB) and local master browser (LMB). The master browsers

are dynamically elected by the kind of OS they run. A windows domain controller is often the DMB as well. Some parameters to which influence an election are:

domain master	specifies if this nmbd will take part in an election to become a DMB
local master	specifies if this nmbd will take part in an election to become a LMB
preferred master	specifies if nmbd will force an election upon its startup
os level	specifies a value of the OS in order to win an election (e.g. NT4 = 32)
browse list	determines if smbd will offer its clients a browse list. (Default: yes)

enhanced browsing

this offers some enhancements to the MS standard browsing, it will operate especially with a Samba WINS. (Default: yes)

remote announce

This parameter would cause that nmbd announces itself (the Samba server) to a given broadcast address or a masterbrowser if there is a fix one:

```
remote announce = 192.168.2.255/SERVERS 192.168.4.125
```

This example would announce the sambaserver to workgroup SERVERS by the given broadcast address and with its own workgroup name to the masterbrowser 192.168.4.125. This could be an alternative if there is no wins server available in your network.

remote browse sync

With this option you can specify a broadcast or server address where nmbd would periodically request synchronization of browse lists with the master browser of a smb server that is on a remote segment. To specify a server address you need to have a fix master browser on the remote subnet.

```
remote browse sync = 192.168.2.255 192.168.4.125
```

browseable (share parameter) determins if a share is visible in the list of a 'net view' command or a browse list. (Default: yes)

As mentioned before more information can be found in:
`/opt/samba/docs/textdocs/BROWSING.txt`.

`nmblookup` can be used to:

- find a master browser of the domain (e.g. gel2000):

```
nmblookup -T -R gel2000#1B
querying gel2000 on 15.140.15.255
grcdg226.grc.hp.com, 15.140.10.224 gel2000<1b>
```

- verify additionally that this DMB is as well a WINS server:

```
telnet grcdg226  42
Trying...
Connected to grcdg226.grc.hp.com.
Escape character is '^]'.

 (stop with <ctrl>+<d>)
```

- retrieve a list of master browsers on the subnet you can use:

```
nmblookup -M -
querying __MSBROWSE__ on 15.140.15.255
15.140.10.224 __MSBROWSE__<01>
15.140.11.132 __MSBROWSE__<01>
...
```

- list computers and services in a domain:

```
root@hprtdu96:>nmblookup -T -S gel2000
querying gel2000 on 15.140.15.255
grcdg226.grc.hp.com, 15.140.10.224 gel2000<00>
hprtdu96, 15.140.10.103 gel2000<00>
grcdg319.grc.hp.com, 15.140.11.19 gel2000<00>
grcdg430.grc.hp.com, 15.140.11.129 gel2000<00>
Looking up status of 15.140.10.224
        ..__MSBROWSE__. <01> - <GROUP> M <ACTIVE>
        ADMINISTRATOR   <03> -         M <ACTIVE>
        GEL2000         <00> - <GROUP> M <ACTIVE>
        GEL2000         <1b> -         M <ACTIVE>
        GEL2000         <1c> - <GROUP> M <ACTIVE>
        GEL2000         <1d> -         M <ACTIVE>
        GEL2000         <1e> - <GROUP> M <ACTIVE>
        GRCDG226        <00> -         M <ACTIVE>
        GRCDG226        <01> -         M <ACTIVE>
        GRCDG226        <03> -         M <ACTIVE>
        GRCDG226        <20> -         M <ACTIVE>
        INet~Services   <1c> - <GROUP> M <ACTIVE>
        IS~GRCDG226     <00> -         M <ACTIVE>
```

If you specify the option `-S` a bit more `nmblookup -S gel2000#1d` you will not query all clients. You can as well request only a specific client:

```
nmblookup -S hprtdu96
querying hprtdu96 on 15.140.15.255
15.140.10.103 hprtdu96<00>
Looking up status of 15.140.10.103
        HPRTDU96        <00> -         M <ACTIVE>
        HPRTDU96        <03> -         M <ACTIVE>
        HPRTDU96        <20> -         M <ACTIVE>
        GEL2000         <00> - <GROUP> M <ACTIVE>
        GEL2000         <1e> - <GROUP> M <ACTIVE>
```

The NetBIOS naming convention allows for 16 characters in a NetBIOS name. Microsoft limits NetBIOS names to 15 characters and uses the 16th character as a NetBIOS suffix. The NetBIOS suffix is used by Microsoft Networking software to identify functionality installed on the registered device. It is good to know hot to interpret the NetBIOS suffix which are hidden in the

16th byte of a NetBIOS packet. (MS: Q163409)

Name	*Number(h)*	*Type*	*Usage*
<computername>	00	U	Workstation Service
<computername>	01	U	Messenger Service
<computername>	03	U	Messenger Service
<computername>	20	U	File Server Service
<username>	03	U	Messenger Service
<domain>	00	G	Domain Name
<domain>	1B	U	Domain Master Browser
<domain>	1C	G	Domain Controllers
<domain>	1D	U	Master Browser
<domain>	1E	G	Browser Service Elections
<INet~Services>	1C	G	IIS
<IS~computer name>	00	U	IIS
<\\--__MSBROWSE__>	01	G	Master Browser

Special user/client config

If you have a large environment with lots of users which should get dedicated shares (besides the home share) you usually have a large `smb.conf`. This can affect the performance as smbd's reread the configuration from time to time. Instead you could work with user specific include files:

```
include = /etc/opt/samba/smb.conf.%U
```

This configuration results that user `%U` would source an additional `smb.conf.<username>`. If user johndoe logs in Samba would additionally read `smb.conf.johndoe`. This `smb.conf` may contain a special share or perhaps additional debugging and could look like this:

```
# requires smb.conf parameter
# "config file = /etc/opt/samba/smb.conf.%U"
# is read if  johndoe  logs in.
      debug level = 10
# shares only for johndoe
[projekt1]
      path = /VA7100/projekt1
      # read permissions for  UNIX-group  projekt1
      read list = @projekt1
      valid users = johndoe
```

NTFS and POSIX ACL's

The HP CIFS Server supports HP-UX POSIX Access Control Lists (ACLs). The mapping of NTFS permissions to *ACL* (Access Control List) allows access and modification of ACLs from Windows NT4.0, XP or Windows 2000 clients. This provides access to UNIX permission information. *CIFS UNIX Extensions* support enables the cifsclient() and CIFS Server to implement standard UNIX file system features, such as permissions, file ownership, symbolic

and hard links, UID/GID, etc.

HP CIFS Server supports viewing and changing both UNIX file permissions and VxFS (JFS) POSIX ACLs from Windows clients. This is done through the standard Windows Explorer interface as if changing NTFS permissions (Windows ACLs). ACL support is not an emulation of native NTFS (like it was with Advances Server Unix), but it allows access to UNIX ACLs through the Windows client. You cannot run Windows applications which require native NTFS options.

The use of VxFS (JFS) POSIX ACLs requires VxFS 3.3 with disk layout version 4. This is available as of HP-UX 11.x and is standard in HP-UX 11i. To convert a HP-UX 11.00 file system to disklayout 4 check out the JFS Chapter in this book. POSIX ACL's allow up to 17 settings on a file or directory. To maintain these ACLs from the shell you would use commands like `getacl()` and `setacl()`. Currently the loopback file system (lofs) cannot handle POSIX ACLs on directories.

With HP CIFS Server version A.01.08 and onwards, the configuration parameter `nt acl support` can be set on share level basis. It was previously a global level variable to versions prior to Samba 2.2.2 (A.01.08). The default value is `yes`.

```
nt acl support = yes
```

This boolean parameter controls whether smbd(8) will attempt to map UNIX permissions into Windows access control lists or not. Setting `nt acl support = yes` lets users control the ACL support on a per-share basis and there is no further special configuration needed for supporting ACLs. For a share supporting Windows ACLs, the CIFS Server always tries to get or set POSIX *ACE*s (Access Control Entries) on the UNIX file system. If the underlying file system does not support POSIX ACLs, then the CIFS Server will use the UNIX file permissions as fallback. This means that only three default ACEs (owner, group and everyone) can be set. Additional ACEs will be ignored.

In order to assign ACL entries from the Windows-client:

```
"File properties"-dialog
"Security"-tag → "Permissions"-button
"File permissions"-dialog
"Add"-button
"List names from"-pulldown menu
select "\\sambaserver*" !!!
"Add users and groups"-dialog
"Show users"-button
```

The "names"-field will only list those users who are in the smbpasswd file. ACEs can only be assigned to those users.

Recommendations for kernel parameters

Requirement for each client connection	PA System			IA System
	A.01.05	A.01.07	A.01.08	A.01.08
Memory space	0.789MB	0.799MB	1.173MB	1.08MB
Swap space	1.9MB	1.9MB	2.0MB	2.0MB
nproc	1	1	1	1
nfile	7	7	20	20
nflocks			10	10

Besides the new features of CIFS-Server 2.2 (A.01.08 and later) some server requirements have changed. Each smbd takes now approx 10 unix locks. CIFS-Server A.01.08 (Samba2.2) uses as well more file-handles approximately three times as much as before. Also remember that each smbd consumes one entry in the process table. You may rule this by the kernel tunable `maxusers`. maxusers affects `nproc`, `nfile` and others. The previous recommendation for CIFS Server A.01.07 was to increase `maxusers` by the number of estimated samba users. So we will keep this as basic thought for the recommendation here. (The notation used is "#(variable)" = value .)

maxusers:

```
maxusers = #(samba-user) + #(unix-user)
```

So the recommendation could be to increase maxusers by #(of estimated simultanious logged in samba-users) or by #(of estimated smbd's). As `nproc` and `nfile` depend on maxusers they increase rapidly and it might be too much although it is simple.

If you consider not to increase `maxusers`, you could as well change the formulas for `nproc` and `nfile`. Adapting the formulas might still be better than setting a fixed value.

nproc:

`nproc` needs to be increased at least by #(estimated smbd's):

```
nproc = (20+8*MAXUSERS) + #(estimated smbd's)
```

nflock:

The use of unix locks has increased with Samba 2.2, therefore increase `nflock` by "10 * #(estimated smbd's)". `nflock` is usually a fixed number, you could think of relating it to `maxusers` if `maxusers` is defined as above, e.g.:

```
nflock =  #(prev. nflock) + 10*#(estimated smbd's)
```

nfile:

here is a detailed calculation to determine how to increase `nfile`: increase `nfile` by NFILE, where NFILE does only concern the filetable entries used by Samba.

```
NFILE = #(files of daemons) + #(of estimated smbd's) *
        [#(files open for plain smbd)
        + #(estimated simultanious open files by one user/session)]
where:
#(files of daemons) = #(files by nmbd -D) + #(files by smbd -D)
⇔ #(files of daemons) = [10 + 2* #(IP's configured in samba)] + 12
#(files open for plain smbd) = 20
#(estimated simultanious open files by one user/session)
⇔ #(open user files)
```

nfile ruled by maxusers:
If you choose to fit parameters by using the `maxusers` macro you would best change the formula as follows:

```
nfile = 16(nproc + 16 + 3* maxusers)/10 + 32 + 2*(npty + nstrpty + nstrtel)
```

the "3*maxusers" represents the fact that Samba 2.2 uses 3 times more filehandles as previous versions. Remember that `nproc` in this formula depends on `maxusers` as well.

nfile ruled by nproc:
If you choose to fit parameters separately – not using the `maxusers` macro – you may want to use `nproc` to rule the size of `nfile`. We suggest the change of the formula as follows:

```
nfile = 16(20* nproc + 16 + #(open user files)* maxusers)/10
       + 32 + 2*(npty + nstrpty + nstrtel)
```

the "20*nproc" represents the open files for each smbd and "#(open user files)* maxusers " represent the files opened during user operations. These have been added to the formula and might be useful for systems doing mainly Samba.

Memory:
It is recommended to have approximately 1.173MB memory per smbd with respect to the resident set size of the private memory regions.

About ninode:
The "inode Cache" means the number of referenced files in cache memory used for inode. In the tables of the document, the increasing in the column of inode cache completely depends on torture tool usage. `smbtorture` used for the test simulating one client each consumes 1 inode of the torture file so that each 100 client connections would generate about 100 inode consuming. If you take a look at the function call rw_torture() in utils/torture.c, then it's clearly shown. Thence inode cache would be affected in application environment, and must be less than `ninode`

limitation.

The `ninode` means the maximum number of open inodes that can be in memory, which is one of kernel configurable parameters. It's defined as `nproc+48+maxusers+(2*npty)`, rather than dependence on any application. If kernel parameters `nproc` or `maxuser` or `npty` are changed, then `ninode` would be changed. **So `ninode` does not need to be adapted**.

CIFS server at one glance

Info commands

Info Command	*Options*	*Comment*
`smbstatus`		View samba information.
	`-V`	View version.
	`-h`	View help information.
	`-u username`	View information about one user.
`testparm`		Get information running smbd and configuration file. Configuration errors are reported.
	`-s`	Suppress prompt for enter.
	`-x`	Exclude default values.

Daemons

Daemons	**Options**	**Comment**
`nmbd`		Netbios-daemon, responding/listening to UDP on port 137 and 138
	`-s config file`	Specify a smb.conf file
	`-D`	Become a daemon
	`-d number`	Specify a debug level (1-10)
	`-V`	Print out version
	`-H filename`	Specify a netbios hostfile; (lmhost)
	`-h`	Print usage
`smbd`		Samba daemon cares for sessions, listens to port 139 and 445 if configured
	`-s config file`	Specify a smb.conf file
	`-D`	Become a daemon
	`-d number`	Specify a debug level (1-10), usually done by smb.conf parameter
	`-V`	Print out version
	`-h`	Print usage

Start and configuration commands

Startup Commands	Options	Comment
startsmb		Used to start nmbd and smbd. It will report if daemons are already running.
stopsmb		Used to stop nmbd and smbd's.
/sbin/init.d/samba	{stop|start}	Startscript
/etc/rc.config.d/samba	RUN_SAMBA={0|1}	Runvariable
/sbin/rc2.d/S900samba		Sambastartscript for booting.
/sbin/rc1.d/K100samba		Sambastopscript for shutdown
/opt/samba/bin/samba_setup		basic samba setup
/opt/samba/bin/rpcclient		for printer and driver management

Troubleshooting commands

Troubleshooting Commands	Comment
smbclient \\server\service -U user	Connect a user to a service, to test user access
smbclient -M host "message"	Send message to windows client host
smbclient -L host	List services from host
Smbcontrol <pid> debug <number>	Send debug level 1 – 10 to smbd pid
nmblookup -S	Lookup node status
Nmblookup -M -	Find master browser
Nmblookup -T	Resolve IP to name

Relevant directories

Directories	Subdirectories	Purpose
/opt/samba/	bin/	Binaries
	Swat/, HP_docs/, docs/,	dokumentation
	HA/	Templates for use in MC/ServiceGuard
/etc/opt/samba		Configuration data
/var/opt/samba	private/ and locks/	Sensitive data

Additional Information

HP Links
http://www.software.hp.com/ Software Bundles
http://docs.hp.com Administration Guides and Release Notes

Samba.org Links
http://samba.org/samba/docs/:

The best souce one can get for detailed reading about Samba 2.x and for introduction is the O'reilly book, which came out as second edition recently: www.oreilly.com (ISBN: 0-596-00256-4) 1st editon Using Samba online and 2nd editon Using Samba online

http://samba.org the maintainer of samba.
other languages: Deutsche Samba Seiten; Français; Italiano; Hebrew; Chinese

HP-internal links

Administration Guides and Release Notes

GSE tools

MSIT-team: The GSE team responsible for CIFS