

# Setting up CIFS Server (Samba) in an LDAP Environment

Don McCall

Hewlett-Packard WTEC

E0300

Printed in: U.S.A.

©Copyright 2000 Hewlett-Packard Company

## Legal Notices

The information in this document is subject to change without notice. Hewlett-Packard makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Warranty. A copy of the specific warranty terms applicable to your Hewlett-Packard product and replacement parts can be obtained from your local Sales and Service Office.

Restricted Rights Legend. Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 for DOD agencies, and subparagraphs (c) (1) and (c) (2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.

Hewlett-Packard Company  
19420 Homestead Road  
Cupertino, California 95014 U.S.A.

Use of this manual and flexible disk(s) or tape cartridge(s) supplied for this pack is restricted to this product only. Additional copies of the programs may be made for security and back-up purposes only. Resale of the programs in their present form or with alterations, is expressly prohibited.

### Copyright Notices

©copyright 1983-2000 Hewlett-Packard Company, all rights reserved.

Reproduction, adaptation, or translation of this document without prior written permission is prohibited, except as allowed under the copyright laws.

©copyright 1979, 1980, 1983, 1985-96, 2000 Regents of the University of California. This software is based in part on the Fourth Berkeley Software Distribution under license from the regents of the University of California.

Contents	
Setting up CIFS Server (Samba) in an LDAP Environment.....	1
Legal Notices.....	1
Legal Notices.....	2
Introduction.....	5
Part one: Setting up a simple Netscape DS server. ....	6
Install Netscape Directory Server V6 for HP-UX: J4258CA .....	6
Configure your Netscape Directory Server .....	6
A Note on Startconsole versus Netscape Console 6.1.....	7
Part two: Setting up ldapux client.....	8
Install J4269AA LDAP-UX Integration product on the server you will be using CIFS Server on.....	8
Configure you ldapux client:.....	8
Migrate all your data stores to the Netscape directory server: .....	9
Part Three: Extending the schema for CIFS Server .....	10
Install a version of CIFS Server with LDAP enabled.....	10
Extend the schema with the sambaAccount subschema .....	10
Verify the schema update .....	11
Part four: Modifying smbldap tools and configuration files.....	11
Modifying the smb.conf file .....	11
Modifying the smbldap_conf.pm file .....	11
Sourcing select parameters from smb.conf instead of smbldap_conf.pm.....	12
Part Five: Installing your CIFS Server users in the directory .....	12
Storing your CIFS Server LDAP credentials .....	12
Adding your CIFS Server users to the LDAP directory .....	13
Setting passwords for your new users .....	14
Part Six: Start CIFS Server and test.....	14
Starting CIFS Server.....	14
Verifying CIFS Server LDAP user and password authentication .....	14
Recommended Reading.....	15
CIFS Server .....	15
Netscape Directory Server and LDAP-UX Client Services.....	15



## Introduction

CIFS Server A.01.11 and later offer the ability to store and access CIFS Server user information in an LDAP directory store; specifically the Netscape Directory Server product shipped with HP-UX 11.0 and later. This paper will describe, step by step, the procedure to set up a simple Netscape DS server on HP-UX, the LDAP-UX client needed to access posix account information that the CIFS Server user accounts in the LDAP directory depend on, and configuring CIFS Server and the perl scripts shipped with it to access and manage your CIFS Server user account information.

## Part one: Setting up a simple Netscape DS server.

### Install Netscape Directory Server V6 for HP-UX: J4258CA

You can obtain this free software from

<http://software.hp.com/portal/swdepot/displayProductInfo.do?productNumber=J4258CA>

### Configure your Netscape Directory Server

login as root.

```
cd /var/opt/netscape/servers/setup
./setup
```

(take all defaults, EXCEPT type in your FQDN instead of just your hostname the first time it presents that as a default)

For example, if the server you are installing CIFS Server, Netscape DS and ldap-ux client is named rkm-nt.alf.cpqcorp.net, these are the questions and answers you would use:

```
Choose installation type [2] (Typical installation)
Computer name [rkm-nt]: rkm-nt.alf.cpqcorp.net (don't take default, put in FQDN)
System User [www]: www (may have to create this first using useradd)
System Group [other]: other
Do you want to register this software with an existing Netscape configuration
directory server? [no]: no
Do you want to use another directory to store your data? [no]: no
Directory server network port [389]: 389
Directory server identifier [rkm-nt]: rkm-nt
Netscape configuration directory server administrator ID [admin]: admin
Password: yourchoice
Password (again): yourchoice
Suffix [dc=alf, dc=cpqcorp, dc=net]: dc=alf, dc=cpqcorp, dc=net
Directory Manager DN [cn=Directory Manager]: cn=Directory Manager
Password: yourchoice (but must be at least 8 characters long)
Password (again): yourchoice
Administration Domain [alf.cpqcorp.net]: alf.cpqcorp.net
Administration port [33565]: 33565 (or anything between 1024 and 65535 that is
NOT being used currently as a port on your system; make it easy to remember, as
you will be using it to connect remotely to administer your Netscape DS later)
Run Administration Server as [root]: root (allows you to stop and start Netscape DS
remotely)
```

You will then see:

```
[slapd-rkm-nt]: starting up server ...  
and a number of informational messages, and finally  
startup: server started successfully  
Press any key to continue...
```

This will set the user and group that the Netscape DS server runs as

```
User=www  
Group=other  
Directory Server network port=389  
Directory Server identifier=[your hostname]  
Administrator id=admin  
    Password=<whatever you want – write it down....>  
Suffix= the dns domain part of your FQDN, for example  
    FQDN is rkm-nt.alf.cpqcorp.net, then Suffix would be  
    [dc=alf, dc=cpqcorp, dc=net]  
Directory Manager DN= Directory Manager  
    Password=<whatever you want, but MUST be at least 8 characters>  
Administration Domain = the dns domain part of your FQDN  
Administration Port = <random number between 1024 and 65535>  
    (write this down, as it will be the port you will use to connect  
    to the server to administer the Netscape DS via the gui!)  
Admin server will be run as: root
```

After you are done, it will automatically start up the admin console daemon to listen on the port you chose.

## A Note on Startconsole versus Netscape Console 6.1

NOTE: this installation will mention to use startconsole to manage your servers. This is SLOW. I would recommend installing the pc version of the Netscape Console 6.1 instead. Much faster, and an invaluable tool to look at your database and schema during this installation and testing process to make sure that the ldap database contains what you expect at various stages.

You can download this from:

<http://sbsdownload.mcom.com/download/golic.cgi>

you have to download the whole thing, but then when you install, you can choose to JUST install the console, NOT the pc server.

## Part two: Setting up ldapux client.

Install J4269AA LDAP-UX Integration product on the server you will be using CIFS Server on.

This needs to be version B.03.20 or greater (only this version and later contains the ldap-ux sdk needed by CIFS Server)

You can obtain this from

<http://software.hp.com/portal/swdepot/displayProductInfo.do?productNumber=J4269>

[AA](#)

### Configure you ldapux client:

Login as root.

```
cd /opt/ldapux/config
```

```
./setup
```

For example:

Directory Server: [1]: (Netscape Directory)

Directory server host [rkm-nt.alf.cpqcorp.net = 16.113.9.137]:

Directory Server port number [389]:

Would you like to extend the schema in this directory server? [Yes]:

Would you like to extend the printer schema in this directory server? [Yes]: NO

User DN [cn=Directory Manager]:

Password: yourchoice (same as you entered when you setup Netscape DS)

Profile Entry DN: []: cn=ldapuxprofile,dc=alf,dc=cpqcorp,dc=net

User DN [cn=Directory Manager]: (this is to add the profile you are creating)

Password: yourchoice

Authentication method: [1]: (if you change this, you will have to read up on ssl/tls communication)

Enter the number of hosts you want to specify [0]: (leave at zero, for a single Netscape DS lookup)

Default base DN [dc=alf,dc=cpqcorp,dc=net]:

Accept remaining defaults? (y/n [y]):

Are you ready to create the Profile Entry? [Yes]:

You will then get messages indicating that you have 'created/changed the configuration'

And it will then ask if you want to start/restart the LDAP-UX daemon. Respond yes.

This will set up you client to:

- talk to a Netscape/iplanet DS server rather than a Win2k one

- use your hostname=ip address as the address of the directory server where you want to store your ldap-ux profile; if you have Netscape DS running on a different server, this will need to change, obviously.

- use port 389 as the port to connect to the DS service on the previous ipaddress.

(note: make sure that the slapd daemon is up and running on whatever ip address you give!)

-will extend the schema on this server for the posixAccount objectclass and attributes necessary to store all of your info, like passwd,group,hosts,services, etc...

-will cause your base dn for user and group searches to be your suffix.

-will start your ldapux client daemon.

NOTE: at this point the ldapux daemon is running, but no one is using it yet – your pam.conf file will have to be changed (see /etc/pam.conf.ldap as an example) and your nsswitch.conf will also have to be updated to use ldap.

Don't do this yet!

## Migrate all your data stores to the Netscape directory server:

```
cd /opt/ldapux/migrate
./migrate_all_online.sh
```

EXAMPLE migration session:

Enter the X.500 naming context you wish to import into: [] dc=alf,dc=cpqcorp,dc=net

Enter the name of your LDAP server [ldap]: rkm-nt.alf.cpqcorp,net

Enter the manager DN: [cn=manager,o=hp.com]:

uid=admin,ou=Administrators,ou=TopologyManagement,o=NetscapeRoot

Enter the credentials to bind with: <enter password you set for admin user when you installed Netscape Directory Server>

Importing into dc=alf,dc=cpqcorp,dc=net...

Creating naming context entries...

Migrating aliases...

Migrating groups...

Migrating hosts...

Migrating networks...

Migrating users...

Migrating protocols...

Migrating rpcs...

Migrating services...

Migrating netgroups...

Migrating netgroups (by user)...

Migrating netgroups (by host)...

Your data has been migrated to the following ldif file: /tmp/nis.1942.ldif

Do you wish to import that file into your directory now (y/n): y

NOTE: At this point you have an ldap server with everything you would need to use as a backing store for pam and nsswitch. You need this first, as CIFS Server is going to share some attributes from the posixAccount objectclass with the sambaAccount objectclass that we are going to extend the schema with in the next steps.

Set nsswitch.conf to use ldap as a store:

(back up you current nsswitch.conf file first, if you have one!)

```
cp /etc/nsswitch.ldap /etc/nsswitch.conf
```

## Part Three: Extending the schema for CIFS Server

### Install a version of CIFS Server with LDAP enabled

Download the free CIFS Server version A.01.11.01 or later from

<http://software.hp.com/portal/swdepot/displayProductInfo.do?productNumber=B8725AA>

### Extend the schema with the sambaAccount subschema

```
cd /opt/samba/LDAP
ftp yournetscapeds-server
  user root
  password xxxxx
  cd /var/opt/netscape/servers/slapd-<yourservername>/config/schema
  bin
  put 98samba.ldif 98samba.ldif
  quit
```

You will need to login to your Netscape DS server and restart slapd for these extensions to be recognized:

```
/var/opt/netscape/servers/slapd-<yourservername>/restart-slapd
```

You should also restart your ldapux client on the system that CIFS Server will be running on:

```
/opt/ldapux/bin/ldapclntd -r
```

You can also extend the schema online, without the need to shutdown and restart the ldap server or client by using the following command:

```
ldapmodify -D <Directory Manager DN> -w <Password> -h <Hostname> -p <Port> -f <Samba Schema File>
```

For instance:

```
cd /opt/ldapux/bin
./ldapmodify -D "cn=Directory Manager" -w ldapdap -h rkm-nt -p 389 -f /opt/samba/LDAP/98samba.ldif
```

## Verify the schema update

```
# /opt/ldapux/bin/ldapsearch -h rkm-nt -p 389 -b "cn=schema" "(objectclass=*)" |  
grep -i sambaAccount
```

(substituting YOUR ldap server name for 'rkm-nt')  
You should get something like this back:

```
objectClasses: ( 1.3.1.5.1.4.1.7165.2.2.3 NAME 'sambaAccount' SUP top AUXILIA
```

## Part four: Modifying smbldap tools and configuration files.

### Modifying the smb.conf file

Edit your smb.conf global section with the following parameters (this assumes you took the defaults when you set up your Netscape DS server and LDAP-UX client):

```
security = user  
encrypt passwords = yes  
  
ldap enable = yes  
ldap port = 389  
ldap ssl = no  
ldap server = <your Netscape DS Server>  
ldap suffix = "dc=alf,dc=cpqcorp,dc=net" (or whatever you used when setting up your  
Netscape directory)  
ldap admin dn = uid=admin,ou=Administrators,ou=TopologyManagement,o=NetscapeRoot  
(or whatever you are using for your ldap directory manager)  
ldap filter = "(&(uid=%u)(objectclass=sambaAccount))"
```

### Modifying the smbldap\_conf.pm file

Edit the following variables in /opt/samba/LDAP/smbldap-tools/smbldap\_conf.pm:

To customize for your Netscape DS installation (note the SLAVELDAP and MASTERLDAP should point to the same server, unless you have gotten REALLY into this and set up master/slave ldap servers):

```
$slaveLDAP = "_SLAVELDAP_"; (the FQDN to your Netscape DS Server)  
$masterLDAP = "_MASTERLDAP_"; (the FQDN to your Netscape DS Server)  
$suffix = "_SUFFIX_"; (YOUR ldap suffix from step 2 above)  
$binddn = "_BINDDN_"; (Your directory manager dn, from step 2 above)  
$bindpasswd = "_BINDPW_"; (Your directory manager password from step 2 above)
```

To customize the names for your CIFS Server groups:

Replace the following texts with the names YOU are using in your LDAP directory:

```
_USERS_  
_GROUPS_  
_COMPUTERS_
```

(For instance,    \_USERS\_ = People,  
                  \_GROUPS\_ = Group,  
                  \_COMPUTERS\_ = Computers

To customize for your posix and CIFS Server variables (these variables are used when creating a new CIFS Server user for defaults):

```
$_userLoginShell = q( _USERLOGINSHELL_ ) (for instance /usr/bin/sh)  
$_userHomePrefix= q( _USERHOMEPREFIX_ ) (for instance /home/)  
$_userHomeDrive = q( _HOMEDRIVE_ ) (for instance U:)  
$_userProfile = q(\\$_PDCNAME \profiles\ ) (for instance \\rkm-nt\profiles\)  
$_userSmbHome = q(\\$_PDCNAME \homes ) (for instance \\rkm-nt\homes\)
```

Sourcing select parameters from smb.conf instead of smbldap\_conf.pm

**NOTE: you can use the '-S' parameter in the scripts to force the scripts to pull**

```
$slaveLDAP  
$masterLDAP  
$suffix  
$binddn
```

**configuration information from the smb.conf file instead of the smbldap\_conf.pm file. This is recommended, since putting your bindpasswd into the smbldap\_conf.pm file is NOT secure; each of the smbldap-tools scripts have a command line option '-w' that will allow you to pass the password via the commandline, rather than having it hardcoded in the .pm file. This is the recommended way of supplying your Directory Manager password.**

## Part Five: Installing your CIFS Server users in the directory

Storing your CIFS Server LDAP credentials

Save your ldap credentials for the user that will be modifying the ldap directory for CIFS Server:

```
smbpasswd -w <Directory Manager password>
```

## Adding your CIFS Server users to the LDAP directory

NOW populate your netscape directory with your CIFS Server users:

If you already have an smbpasswd file, you can import this into your ldap directory as follows:

```
cat /var/opt/samba/private/smbpasswd |  
/opt/samba/LDAP/import_smbpasswd.pl
```

Otherwise, you can add users individually in the following manner:

```
/opt/samba/LDAP/smbldap-tools/smbldap-useradd.pl -S -w <ldap passwd> -a  
username
```

verify that this step worked:

```
./smbldap-usershow.pl -S -w <directory manager passwd> username
```

For instance to look up a user named 'ddmc' that was previously added:

```
# ./smbldap-usershow.pl -S -w expert88 ddmc  
dn: uid=ddmc,ou=People,dc=alf,dc=cpqcorp,dc=net  
objectClass: top  
objectClass: account  
objectClass: posixAccount  
objectClass: sambaAccount  
cn: ddmc  
uid: ddmc  
uidNumber: 1000  
gidNumber: 100  
homeDirectory: /home/ddmc  
loginShell: /usr/bin/sh  
gecos: System User added by samba  
description: System User added by samba  
userPassword: {crypt}x  
pwdLastSet: 0  
logonTime: 0  
logofftime: 2147483647  
kickoffTime: 2147483647  
pwdCanChange: 0  
pwdMustChange: 2147483647  
displayName: System User added by samba  
acctFlags: [UX]  
rid: 3000  
primaryGroupID: 1201
```

```
homeDrive: U:  
smbHome: \\cai\homes  
profilePath: \\cai\profiles\ddmc  
scriptPath: ddmc.cmd  
lmPassword: XXX  
ntPassword: XXX
```

## Setting passwords for your new users

You can set passwords for your CIFS Server users with the smbpasswd command:

```
smbpasswd <username>  
New SMB password:  
Retype new SMB password:  
ldap_connect_system: Binding to ldap server as "cn=Directory Manager"  
ldap_connect_system: Binding to ldap server as "cn=Directory Manager"  
Password changed for user <username>.
```

## Part Six: Start CIFS Server and test

Start CIFS Server and check it out!

### Starting CIFS Server

```
/opt/samba/sbin/nmbd -D  
/opt/samba/sbin/smbd -D
```

or

```
/opt/samba/bin/start smb
```

### Verifying CIFS Server LDAP user and password authentication

use smbclient to verify user and password authentication:

```
/opt/samba/bin/smbclient -L localhost -U <CIFS Server user ONLY contained in  
LDAP directory>
```

And you're DONE!

## Recommended Reading

### CIFS Server

HP CIFS Server 2.2h Administrator's Guide, **HP Part number B8725-90061**. You can also view the contents of this book online at

<http://docs.hp.com/hpux/onlinedocs/B8725-90061.html>

There is also terse but useful information on the various perl scripts and their usage in the README file in the directory /opt/samba/LDAP and /opt/samba/LDAP/smbldap-tools.

### Netscape Directory Server and LDAP-UX Client Services

For further information on Netscape Directory Server and the LDAP-UX integration products, the following manuals will prove useful:

Netscape Directory Server Admin Guide, viewable online at

<http://docs.hp.com/hpux/onlinedocs/2330/ds61admin.pdf>

LDAP-UX Client Services B.03.20 Administrator's Guide, viewable online at

<http://docs.hp.com/hpux/onlinedocs/J4269-90030/J4269-90030.html>

