The SAMBA-2.2.4/LDAP PDC HOWTO

Olivier Lemaire

Revision : 1:24, generated June 7, 2002

This document is the propertatedeu

1 Introduction

I hope this document can help: it express our personal experience using Samba[2] and OpenLDAP[3]

3 Download & compile

To stick to this Howto[10], you must have the following requirements prior to download anything :

RedHat *Linux* 7.2 installed and operational (network included),

you must be prepared (if not already done) to use pam_ldap and nss_ldap (we'll see later how to con gure them correctly).

Additionnaly, you must download :

Samba release 2.2.4 (see below),

OpenLDAP release 2.0.11 or 2.0.21 (see below),

nss_ldap and pam_ldap (see below),

smbldap-tools release 0.7 (see below).

3.1 OpenLDAP

3.2 Samba 2.2.4

Samba 2.2.4 is the last release of Samba

4 Configuring OpenLDAP

4.1 Schemas

First, copy the Samba samba.schema to /etc/openldap/schema/samba.schema.

You'll find this Samba schema shipped with the Samba-2.2.4 release (/example/LDAP/samba.schema in the source package, or in /usr/share/doc/samba-2.2.4/examples/LDAP/samba.schema if you used the modified RedHat RawHide package to build and install Samba)

If you plan using inetOrgPerson schema, then edit this schema to comment the 'display-

verify that /var/lib/ldap exist and is owned by the user who run sladp (ldap user for RedHat OpenLDAP packages),

consult the OpenLDAP documentation.

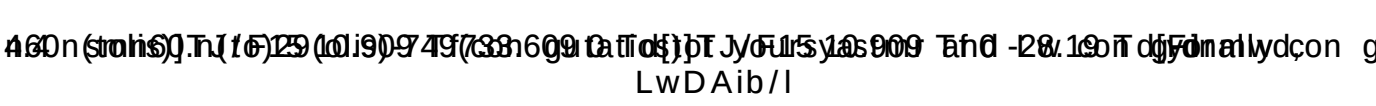
4.3 Initial entries

Next, we'll inject some initial entries on the brand new OpenLDAP server con gured and started above.

A sample LDIF le is presented on 22.2 on page 53. copy/paste it on a le named base.ldif and add it using:

```
ldapadd -x -h localhost -D "cn=manager,dc=IDEALX,dc=ORG" -f base.ldif -W
```

(type your admin DN password, 'secret' to complete the command)



```
[user@host-one:~]$ ssc testuser1@pdc-srv
testuser1@pdc-srv's password:
Last login: Sun Dec 23 15:49:40 2001 from host-one

[testuser1@pdc-srv testuser1]$ id
uid=1000(testuser1) gid=100(users) groupes=100(users)
```

Dont forget to delete this testuser1 after having completed your tests :

```
[root@pdc-srv]# smbldap-userdel.pl testuser1
```

6 Configuring Samba

Here, we'll configure Samba as a Primary Domain Controler for the Microsoft Windows NT Domain named IDEALX-NT with the SAM database stored in our OpenLDAP server.

6.1 Configuration

We need to configure /etc/samba/smb.conf like in the example of 22.4 on page 55, assuming that :

Our Microsoft Windows NT Domain Name will be : IDEALX-NT

```
  passwd program = /usr/local/sbin/smbldap-passwd.pl -o %u
  passwd chat = *new*password* %n\n *new*password* %n\n *successfully*
  unix password sync = Yes
  ...
; SAMBA-LDAP declarations
  ldap suffix = dc=IDEALX,dc=ORG
  ldap admin dn = cn=Manager,dc=IDEALX,dc=ORG
  ldap port = 389
  ldap server = 127.0.0.1
```

To do so, use the following command (assuming 'secret' is the ldap admin dn password, see your /etc/openldap/slapd.conf con guration le to be sure) :

```
[root@pdc-srv samba]# smbpasswd -w secret
Setting stored password for "cn=Manager,dc=IDEALX,dc=ORG" in secrets.tdb
```

Samba will store this datas in /etc/samba/secrets.tbd.

Note that this ldap admin dn may be another account than Root DN : you should use another ldap account who should have permissions to wri
attrs (see ?? on page ??). In this HOWTO, we're using the Root DN.

Then, you should create your 'Administrator' user :

```
[root@pdc-srv samba]# smbldap-useradd.pl -a -m -g 200 administrator
adding new entry "uid=administrator,ou=Users,dc=IDEALX,dc=ORG"

modifying entry "uid=administrator,ou=Users,dc=IDEALX,dc=ORG"

modifying entry "uid=administrator,ou=Users,dc=IDEALX,dc=ORG"


[root@pdc-srv samba]# smbldap-passwd.pl administrator
Changing password for administrator
New password :
Retype new password :
all authentication tokens updated successfully
```

In fact, any user placed in the "Domain Admins" group will be granted Windows admin rights.

6.4 Testing

To validate your Samba con guration, use testparm who should return 'Loaded services le OK.' without any warnings nor unknow parameter. See man testparm for more info.

7 Start-Stop servers

8 User management

To manager user accounts, you can use:

1. smbldap-tools, using the following scripts:

   smbldap-useradd.pl : to add a new user
   smbldap-userdel.pl : to delete an existing user
   smbldap-usermod.pl : to modify an existing user data

2. idxldapaccounts if you are looking for a nice Graphical User Interface.

Both method will be presented hereafter.

8.1 A LDAP view

First, let's have a look on what is really a user accounts for LDAP. In fact, there is two kinds of user accounts :

P357x1893:2B(ts)[(os)wi091 (for)-30-a(is)-30728(ou)systems(n-3Firik-334ou)Und[(P)27((.091 T38s:)]TJ/

```
dn: uid=testsmbuser2,ou=Users,dc=IDEALX,dc=ORG
objectClass: top
objectClass: account
objectClass: posixAccount
objectClass: sambaAccount
cn: testsmbuser2
uid: testsmbuser2
uidNumber: 1006

```

8.1.3 scriptPath

The script path override the 'logon script' directive of smb.conf (if exist). Variable substitution

```
all authentication tokens updated successfully
```

8.2.3 Setup an user password

You can use smbldap-passwd.pl as a replacement for the system command

10 Computer management

To manage computer accounts, we'll use the following scripts (from `smbldap-tools`) :

smbldap-useradd.pl : to add a new computer

11 Profile management

WARNING : Under writing !

TODO: Howto manage profiles (NT profiles, as Unix do the job since... AT&T time...)

11.1 Roaming/Roving profiles

When a Microsoft Windows NT user joined the IDEALX-NT domain, his profile is stored in the directory defined in the *profile* section of the samba configuration file. He has to log out

11.4 LDAP or not LDAP?

Perhaps, you'll want to use an alternative system policy concerning pro les : granting some user the yTming privilebe the while some other mayve only yTming

```
--- passdb/pdb_ldap.c.orig      Thu May 16 00:17:39 2002
+++ passdb/pdb_ldap.c   Thu May 16 00:20:36 2002
@@ -75,11 +75,16 @@ static BOOL ldap_open_connection (LDAP *
        int version, rc;
        int tls = LDAP_OPT_X_TLS_HARD;

+/* Q&D patch : permit non root bind to LDAP
+   because if so (original code), you cannot add W2K/WXP workstations accounts
+   via the W2K/WXP requester, using an uid != from 0 (ex: user 'administrator'
+   from a " @"Domain Admin" " group (from 'domain admin group' directive in smb.conf)
+
        if (geteuid() != 0) {
                DEBUG(0, ("ldap_open_connection: cannot access LDAP when not root..\n"));
                return False;
        }
-
+*/
        if (lp_ldap_ssl() == LDAP_SSL_ON && lp_ldap_port() == 389) {
                port = 636;
        }
```


TODO

13 Servers integration

13.1 Samba

14.4 Creating an user account

You cannot[16] create user accounts with Microsoft Windows NT

15 Real life considerations

Now we've detail how to set up your brand new PDC-Killer prototype, we're ready to go further: the real life, the one where users don't care about looking for solutions to a given problem, but will first consider they've got one and you're the guilty :-)

To struggle in this pleasant world, you should have a look on the following considerations : they may help you.

First, if this HOWTO was your first approach with Samba and OpenLDAP, you should have a look on:

a very good OpenLDAP brief by Adam Williams available at ftp://kalamazoolinux.org/pub/pdf/ldapv3.pdf: an excellent presentation/briefing on OpenLDAP on the *Linux* Platform.

18 Contributions

Some useful scripts and tools may help you when setting up your Samba+OpenLDAP PDC server:

smbldap-tools: PERL scripts to manager user and group accounts. See http://samba.idealx.org/. Note that these scripts are now shipped with Samba release 2.2.5,

idxldapaccounts Webmin module: a Webmin module to manager user and group accounts

21 Samba-Ldap on Debian Woody

The standard Samba Debian package is compiled with PAM Support. So you have to get the samba source and recompile it yourself.

samba-common.con les: get rid of the /etc/pam.d/samba entry (yes the le is then empty)

winbind. les: get rid of the lib/security/pam_winbind.so

Afterwards make a dpkg-buildpackage from the main directory level. when nished you have the .deb les ready to be installed:

```
# dpkg -i samba-common_2.2.4-1_i386.deb libsmbclient_2.2.4-1_i386.deb
samba_2.2.4-1_i386.deb smbclient_2.2.4-1_i386.deb smbfs_2.2.4-1_i386.deb
swat_2.2.4-1_i386.deb winbind_2.2.4-1_i386.deb
```

```
46
47  attributetype ( 1.3.6.1.4.1.7165.2.1.6 NAME 'logoffTime'
48          DESC 'NT logoffTime'
49          EQUALITY integerMatch
50          SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )
51
52  attributetype ( 1.3.6.1.4.1.7165.2.1.7 NAME 'kickoffTime'
53          DESC 'NT kickoffTime'
54          EQUALITY integerMatch
55          SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )
56
57  attributetype ( 1.3.6.1.4.1.7165.2.1.8 NAME 'pwdCanChange'
58          DESC 'NT pwdCanChange'
59          EQUALITY integerMatch
60          SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )
61
62  attributetype ( 1.3.6.1.4.1.7165.2.1.9 NAME 'pwdMustChange'
63          DESC 'NT pwdMustChange'
```

SYNTAX 1.3

```
cn: Domain Admins
memberUid: administrator
description: Windows Domain Users

dn: cn=Domain Users,ou=Groups,dc=IDEALX,dc=ORG
objectClass: posixGroup
gidNumber: 201
cn: Domain Users
description: Windows Domain Users

dn: cn=Domain Guests,ou=Groups,dc=IDEALX,dc=ORG
objectClass: posixGroup
gidNumber: 202
cn: Domain Guests
description: Windows Domain Guests Users

dn: cn=Administrators,ou=Groups,dc=IDEALX,dc=ORG
description: Members can fully administer533(ca)-5rlcer533(ca)-5rlcer533(ca)-5rlcer533(caRur53/dTJ/F194 Td[(40)]TJ/F43 7.9
```

```
dns proxy = No
wins support = Yes

; SAMBA-LDAP declarations
ldap suffix = dc=IDEALX,dc=ORG
ldap admin dn = cn=Manager,dc=IDEALX,dc=ORG
ldap port = 389
ldap server = 127.0.0.1
ldap ssl = No

printing = lprng

; Deactivate opportunistic locks (wised)19 5.978 Tf -27.729 -9.465 Td[(32)]TJ 4
; encoding character set = iso8859-1 -27.729 -9.465 Td[(32)]TJ 6

; using smbldap-tools to add machines
add user script = /usr/local/sbin/smbldap-useradd.pl -w %u19 5.978 Tf -27.729 -9.465 Td[(32)]TJ40
machine admin 'Domain'Dom"3(Admins')]TJ/F19 5.978 Tf -27.729 -9.264 Td[(37)]TJ 0 -94464 Td[(33)]TJ/F4
```