CentOS 5.x Samba Domain Controller With LDAP Backend

This will show you how to set up a Samba Domain Controller with a local LDAP backend, using CentOS 5.x (tested on 5.3, still successfully running on 5.4). Includes a web-interface for managing LDAP users/groups/etc.

January 2010 -- Now with support for Windows 7 domain logins (see end of guide).

Disable selinux:

It will only cause problems, I'm not going to mess with SELinux in this guide other than disabling it.

echo 0 >/selinux/enforce

Within /etc/sysconfig/selinux, set:

```
SELINUX=disabled
```

Install some tools

rpm -Uvh http://download.fedora.redhat.com/pub/epel/5/i386/epel-release-5-3.noarch.rpm
yum update
yum install openldap-servers nss_ldap samba httpd openssl mod_ssl mysql mysql-server php php-xml php-ldap php-mysql php-pdo php-cli php-common smbldap-tools

Installing **smbldap-tools** this way should install all the dependent perl modules, however the version available on yum has some bugs, so we'll upgrade to the latest version afterwards, keeping the dependencies, but overwriting the smbldap-tools package:

rpm -Uvh http://download.gna.org/smbldap-tools/packages/smbldap-tools-0.9.5-1.noarch.rpm

Set up the hostname

For our purposes in this guide, we are calling the server's hostname "dc1" and the domain "DOMAINNAME". Note: If you want to use your fqdn for your Samba domain, wherever you see ,dc=DOMAINNAME below, replace it with ,dc=example,dc=com, assuming your fqdn is example.com. Also note that "root" will be the samba administrator username, if you don't like that, change it as well. Related lines are: **cn=root** and **cn: root**

Within /etc/hosts, add or replace your line (following the file's format, assuming 192.168.0.5 is your server's network-accessible IP):

```
192.168.0.5 dc1.DOMAINNAME dc1
```

Set your hostname on the command line:

hostname dc1.DOMAINNAME

Generate a master password and set up ldap

slappasswd

Note the output of slappasswd, you will insert it into slapd.conf in a minute.

mv -f /etc/openldap/slapd.conf /etc/openldap/slapd.conf.dist

Insert the following text into /etc/openldap/slapd.conf:

include /etc/openldap/schema/core.schema
```
include /etc/openldap/schema/cosine.schema
include /etc/openldap/schema/inetorgperson.schema
```

```
include /etc/openldap/schema/nis.schema
include /etc/openldap/schema/samba.schema
allow bind_v2
pidfile /var/run/openldap/slapd.pid
argsfile /var/run/openldap/slapd.args
database bdb
suffix "dc=DOMAINNAME"
rootdn "cn=root,dc=DOMAINNAME"
rootpw {SSHA}TTzshhAbmZPPb8F2s7sgf9B+IrZt+nUD
password-hash {SSHA}
directory /var/lib/ldap
index cn,sn,uid,displayName pres,sub,eq
index uidNumber,gidNumber eq
index sambaSID eq
index sambaPrimaryGroupSID eq
index sambaDomainName eq
index objectClass pres,eq
index default sub
```

Note the rootpw line in the above text, that's where you paste your output from slappasswd.

cp /usr/share/doc/samba-3.*/LDAP/samba.schema /etc/openldap/schema/
cp /etc/openldap/DB_CONFIG.example /var/lib/ldap/DB_CONFIG
chown ldap:ldap /var/lib/ldap/DB_CONFIG
chmod 600 /var/lib/ldap/DB_CONFIG

Insert the following text into /etc/openldap/init.ldif:

```
dn: dc=DOMAINNAME
objectclass: dcObject
objectclass: organization
o: CentOS Directory Server
dc: DOMAINNAME
dn: cn=root,dc=DOMAINNAME
objectclass: organizationalRole
cn: root
```

slapadd -l /etc/openldap/init.ldif
chown -R ldap:ldap /var/lib/ldap
chmod 600 /var/lib/ldap/*
slapcat

slapcat should produce something very similar to the following output:

```
dn: dc=DOMAINNAME
objectClass: dcObject
objectClass: organization
o: CentOS Directory Server
dc: DOMAINNAME
structuralObjectClass: organization
entryUUID: 717d1b1e-ce90-102d-88c3-df22563ebfee
creatorsName: cn=root,dc=DOMAINNAME
modifiersName: cn=root,dc=DOMAINNAME
createTimestamp: 20090506134920Z
modifyTimestamp: 20090506134920Z
entryCSN: 20090506134920Z#000000#00#000000
dn: cn=root,dc=DOMAINNAME
objectClass: organizationalRole
cn: root
structuralObjectClass: organizationalRole
entryUUID: 71858556-ce90-102d-88c4-df22563ebfee
```

```
creatorsName: cn=root,dc=DOMAINNAME
modifiersName: cn=root,dc=DOMAINNAME
createTimestamp: 20090506134920Z
modifyTimestamp: 20090506134920Z
entryCSN: 20090506134920Z#000001#00#000000
```

service ldap start
chkconfig ldap on
ldapsearch -x -b "dc=DOMAINNAME"

The output from ldapsearch should be very similar to the following:

```
# extended LDIF
#
# LDAPv3
# base <dc=domainname> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# DOMAINNAME
dn: dc=DOMAINNAME
objectClass: dcObject
objectClass: organization
o: CentOS Directory Server
dc: DOMAINNAME
# root, DOMAINNAME
dn: cn=root,dc=DOMAINNAME
objectClass: organizationalRole
cn: root
# search result
search: 2
result: 0 Success
# numResponses: 3
# numEntries: 2
</dc=domainname>
```

Setting up remote administration of the ldap directory

Edit /etc/php.ini and make sure memory_limit is set to at least 32 MB:

memory_limit = 32M

Last I checked, the version of phpldapadmin available via yum is broken, so we'll get the latest & extract it: Go To http://sourceforge.net/project/showfiles.php?group_id=61828&package_id=177751 & download the latest version. In my case that resulted in the following commands, your package may be newer:

mkdir /var/www/html/samba && cd /var/www/html/samba
wget http://softlayer.dl.sourceforge.net/sourceforge/phpldapadmin/phpldapadmin-1.1.0.7.tar.gz
tar zxf phpldapadmin-1.1.0.7.tar.gz
ln -s phpldapadmin-1.1.0.7 pla
cp pla/config/config.php.example pla/config/config.php

Now edit ./pla/config/config.php and uncommment the following line:

```
$config->custom->jpeg['tmpdir'] = "/tmp";
```

Make newly setup software available

service httpd restart
chkconfig httpd on

Edit /etc/sysconfig/iptables and copy & modify line about ssh (--dport 22 -j ACCEPT), and right after it, add (assuming your CentOS install produced the default iptables file):

```
#Allow Https://
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 443 -j ACCEPT
#Allow samba:
-A RH-Firewall-1-INPUT -m multiport -p udp --dport 137,138 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m multiport -p tcp --dport 139,445
-j ACCEPT
```

Now open your webbrowser and visit https://192.168.0.5/samba/pla/ and login with Username **cn=root,dc=DOMAINNAME** & your password. You should be able to look around and see some junk.

Integrate ldap and Samba

mv /etc/samba/smb.conf /etc/samba/smb.conf.dist
cp /usr/share/doc/smbldap-tools-0.9.5/smb.conf /etc/samba/smb.conf

Edit /etc/samba/smb.conf to your likings, the default ldap part should be fine.
Under [global], you will need to add these three settings not there by default:

ldap ssl = off
nt acl support = yes
socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192 SO_KEEPALIVE

cp /usr/share/doc/smbldap-tools-0.9.5/smbldap.conf /etc/smbldap-tools/smbldap.conf
net getlocalsid

Note, **net getlocalsid** will error a bunch until the end, because you haven't fully configured samba yet -- but will produce the sid you need for the next step.

Edit /etc/smbldap-tools/smbldap.conf and insert **sid, domain, etc**, all throughout the file till the end.

Edit /etc/smbldap-tools/smbldap_bind.conf and change both applicable lines, change "secret" to your password.

chmod 644 /etc/smbldap-tools/smbldap.conf
chmod 600 /etc/smbldap-tools/smbldap_bind.conf
authconfig-tui

Check that the output from authconfig-tui contains:

```
[ ] Local authorization is sufficient
```

Now test your samba config:

testparm

smbpasswd -w YOUR_ROOT_LDAP_PASS_HERE
smbldap-populate

smbldap-populate will ask for the password, enter it.

Start the LDAP Samba installation up

/etc/init.d/smb start
chkconfig smb on

Add users/groups, correlate between unix and ldap:

useradd user1
smbldap-useradd -a -G 'Domain Users' -m -s /bin/bash -d /home/user2 -F "" -P user1

Get a picture of the UNIX groups that aren't there yet that LDAP assumes:

net groupmap list

Output is something like:

```
Domain Admins (S-1-5-21-990788473-1556064292-4137819756-512) -> domain_admins
```

```
Domain Users (S-1-5-21-990788473-1556064292-4137819756-513) -> domain_users
Domain Guests (S-1-5-21-990788473-1556064292-4137819756-514) -> 514
Domain Computers (S-1-5-21-990788473-1556064292-4137819756-515) -> 515
Administrators (S-1-5-32-544) -> 544
Account Operators (S-1-5-32-548) -> 548
Print Operators (S-1-5-32-550) -> 550
Backup Operators (S-1-5-32-551) -> 551
Replicators (S-1-5-32-552) -> 552
```

Add correlating groups to unix, using the suggested GIDs:

groupadd -g 514 samba_domain_guests
groupadd -g 515 samba_domain_computers
groupadd -g 544 samba_administrator
groupadd -g 548 samba_account_operators
groupadd -g 550 samba_print_operators
groupadd -g 551 samba_backup_operators
groupadd -g 552 samba_replicators

If you want to add a non-built-in group to LDAP/Samba, say for controlling which users can write/read files on a share, and have it determine that by groups:

smbldap-groupadd -a "People In Our Office"

Then get the output from **net groupmap list** again and correlate the newly created group # just like last time, adding the group to the unix system:

groupadd -g 1001 samba_people_in_our_office

Add users to LDAP groups via the web interface, then correlate in unix:

usermod -a -G UNIX_GROUP_NAME UNIX_USERNAME

Also add computer accounts to unix, using the group "samba_domain_computers" from above, and where your allowed computer names end with a "$":

useradd -M -g 515 -s /bin/false officecomp1$

Last, but certainly not neccessary, you may want to turn off the unneccesary services CentOS runs by default. I determined that **I**, specifically, don't need any of the following. You might be different, so look them up before you turn them off:

chkconfig ntpd off
chkconfig bluetooth off
chkconfig xinetd off
chkconfig smartd off
chkconfig yum-updatesd off
chkconfig rpcidmapd off
chkconfig rpcgssd off
chkconfig restorecond off
chkconfig portmap off
chkconfig pcscd off
chkconfig nfslock off
chkconfig mcstrans off
chkconfig mdmonitor off
chkconfig irqbalance off
chkconfig kudzu off
chkconfig ip6tables off
chkconfig hidd off
chkconfig gpm off
chkconfig haldaemon off
chkconfig autofs off
chkconfig avahi-daemon off
service ntpd stop
service bluetooth stop
service xinetd stop
service smartd stop
service yum-updatesd stop
service rpcidmapd stop

service rpcgssd stop
service restorecond stop
service portmap stop
service pcscd stop
service nfslock stop
service mcstrans stop
service mdmonitor stop
service irqbalance stop
service kudzu stop
service ip6tables stop
service hidd stop
service gpm stop
service haldaemon stop
service autofs stop
service avahi-daemon stop

(Optional) Upgrade Samba so Windows 7 computers can join the domain

Make sure **ldap ssl = off** is set in /etc/samba/smb.conf, as this wasn't required for the CentOS distro version of Samba to run properly, but will be required once we upgrade (3.0.x vs 3.3.x, which supports Windows 7).

We will get the newer samba RPMs built for CentOS from Sernet:

cd /etc/yum.repos.d/
wget http://ftp.sernet.de/pub/samba/3.3/centos/5/sernet-samba.repo
yum update

Your samba packages will update from the Sernet repo.
Since the upgrade, our CentOS service for samba disappeared; let's re-add it:

chkconfig --add smb
chkconfig smb on

Now add the Windows 7 computer to Unix (assuming your domain computers' group name is "samba_domain_computers"):

useradd -M -g `cat /etc/group|grep samba_domain_computers|cut -d: -f3` -s /bin/false win7-computername$
usermod -a -G samba_domain_computers win7-computername$

Now join your Windows 7 PC to the domain using this official Samba mini guide:
http://wiki.samba.org/index.php/Windows7