CentOS 6 LDAP authentication and NFS V4

17.02.25

Pegasi Knowledge
https://ghost.pegasi.fi/wiki/

Table of Contents

CentOS 6 LDAP authentication and NFS V4

LDAP and sssd

LDAP authentication has changed from earleier CentOS. Now all you need is sssd and an LDAP server like openLDAP or Novell eDirectory I am using.

This is short and sweet (or dirty?) list of things to make it work. I don't use tls so it required a bit customization. But if you use encryption you might get off by just configuring it with system-config-authentication. If not then read on.

- See that you don't have nslcd or nss-pam-ldapd to mess with you

```
yum erase nss-pam-ldapd nslcd
```

- Make basic ldap configuration in /etc/openldap/ldap.conf

```
URI ldap://yourldapserver/
BASE o=base
TLS_CACERTDIR /etc/openldap/cacerts
```

- Do the basic configuration with one command

```
authconfig --enablesssd --enablesssdauth --enablelocauthorize --update
```

- Start of sssd is not necessary succesful since you may not have a working configuration as of now
- And make your /etc/sssd/sssd.conf look something like this (customize the rows marked)

```
[sssd]
config_file_version = 2
services = nss, pam
domains = default

[nss]
filter_users = root,bin,postfix,ldap,avahi,haldaemon,dbus,nscd
enum_cache_timeout = 3600

[domain/default]
cache_credentials = True
id_provider = ldap
auth_provider = ldap
chpass_provider = ldap
```

```
#eDirectory ldap, long timeouts
ldap_tls_reqcert = never
ldap_schema = rfc2307bis
ldap_search_base = o=pegasi
ldap_uri = ldaps://ldap.company.com:636/
ldap_access_filter = objectclass=posixaccount
ldap_tls_cacert = /etc/openldap/cacerts/myca.b64
ldap_user_member_of = groupMembership
entry_cache_timeout = 14400
entry_cache_user_timeout = 14400
entry_cache_group_timeout = 14400
ldap_enumeration_refresh_timeout = 1200
ldap_purge_cache_timeout = 21600

ldap_default_bind_dn = cn=sssuser,o=xxx
ldap_default_authtok_type = password
ldap_default_authtok = MyComplexPasswordX,Y.Z-123

[pam]
```

- Open /etc/sysconfig/authconfig and edit

```
FORCELEGACY=yes
```

- Edit /etc/nsswitch.conf

```
passwd:     files sss
shadow:     files sss
group:      files sss
```

- Restart and test

```
/etc/init.d/sssd restart
id some_login
```

NFS V4

After competing the above we set up NFS V4.

Things to do in both server and clients

- Edit the configuration file /etc/idmapd.conf to common domain

```
Domain = yourdomain
```

- To prevent future headaces, include static mappings for all users not in LDAP

```
Method = nsswitch,static
```

```
[Static]
apache@yourdomain = apache
```

Things to do in server

- Add your shares to /etc/exports

```
/mnt/homedirs   192.168.1.0/24(rw,sync,no_root_squash,no_all_squash)
```

- Restart and enable services

```
/etc/rc.d/init.d/rpcidmapd restart
/etc/rc.d/init.d/rpcbind restart
/etc/rc.d/init.d/nfslock restart
/etc/rc.d/init.d/nfs restart
chkconfig rpcidmapd on
chkconfig rpcbind on
chkconfig rpcidmapd on
chkconfig rpcidmapd on
```

- Check that the services are allowed in /etc/hosts.allow
- Check that iptables rules allow clients to mount

Things to do in clients

- Check that you have nfs-utils package
- Check that your idmapd.conf is in order, look above
- Put mountpoints to /etc/fstab

```
server:/mnt/home   /net/home   nfs4   defaults,_netdev   0 0
```

- Enable and restart services

```
chkconfig rpcbind on
chkconfig rpcidmapd on
chkconfig nfslock on
chkconfig netfs on
/etc/rc.d/init.d/rpcbind start
/etc/rc.d/init.d/rpcidmapd start
```

```
/etc/rc.d/init.d/nfslock start
/etc/rc.d/init.d/netfs start
```

- Mount and test

```
mount -a
```