CentOS 7 LDAP authentication

26.06.22

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

Table of Contents

CentOS 7 LDAP authentication 1
LDAP and sssd 1

CentOS 7 LDAP authentication

LDAP and sssd

This is an updated document from CentOS 6 LDAP I did before.. since I am doing it now so why not write it down while I am at it. I am using NetIQ eDirectory as an LDAP backend but since it is V3 standard LDAP you should be fine with other compliant LDAP servers too (such as openLDAP).

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
- Install openldap-clients to help with the testing
- Install sssd packets

```
yum erase nss-pam-ldapd nslcd
yum install sssd sssd-client
```

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

```
URI ldap://yourldapserver/
BASE ou=your_ou,o=your_org
TLS_CACERTDIR /etc/openldap/cacerts
```

- test with

```
ldapsearch -x objectclass=* dn
```

If you get a timeout you have a firewall blocking somewhere or routing issues. If you get an instant response but do object list then it might be a rights issue and you can try again with a known user:

```
ldapsearch -x -D "cn=user,ou=my_ou,o=my_org" objectclass=* dn
```

- Do the basic configuration with one command

```
authconfig \
--enablesssd \
--enablesssdauth \
--enablelocauthorize \
--enableldap \
--enableldapauth \
--ldapserver=ldap://yourldapserver:389 \
--disableldaptls \
--ldapbasedn=ou=my_ou,o=my_org \
```

```
--enablerfc2307bis \
--enablemkhomedir \
--enablecachecreds \
--update
```

- Make your /etc/sssd/sssd.conf look something like this

```
[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]
```

- Edit /etc/nsswitch.conf

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

```
group:      files sss
```

- Enable sssd at startup

```
systemctl enable sssd.service
```

- Restart and test

```
systemctl restart sssd
id some_login
ssh user@localhost
```