**Instalación cliente de LDAP en Centos**

Se deben instalar estos paquetes del repositorio

dnf install nss-pam-ldapd openssl nscd dbus oddjob oddjob-mkhomedir

1. Modificar el /etc/nslcd.conf con esta configuración (Para Centos 8)

uid nslcd

gid ldap

# This comment prevents repeated auto-migration of settings.

uri ldap://128.2.1.42/ ldap://128.2.1.43/

base dc=coto,dc=com,dc=ar

ssl no

tls\_cacertdir /etc/openldap/cacerts

1. Crear la carpeta cacerts

mkdir /etc/openldap/cacerts

1. Modificar el /etc/nsswitch.conf con estos parámetros:

passwd: files **ldap** systemd sss

group: files **ldap** systemd sss

netgroup: sss files

automount: sss files

services: sss files

shadow: files **ldap** sss

hosts: files dns myhostname

aliases: files

ethers: files

gshadow: files

networks: files dns

protocols: files

publickey: files

rpc: files

1. Modificar el archive /etc/authselect/system-auth

# Generated by authselect on Fri Jan 7 13:16:54 2022

# Do not modify this file manually.

auth required pam\_env.so

auth required pam\_faildelay.so delay=2000000

auth sufficient pam\_fprintd.so

auth [default=1 ignore=ignore success=ok] pam\_usertype.so isregular

auth [default=1 ignore=ignore success=ok] pam\_localuser.so

auth sufficient pam\_unix.so nullok try\_first\_pass

auth [default=1 ignore=ignore success=ok] pam\_usertype.so isregular

auth sufficient pam\_sss.so forward\_pass

auth required pam\_deny.so

**auth sufficient pam\_ldap.so use\_first\_pass**

account required pam\_unix.so

account sufficient pam\_localuser.so

account sufficient pam\_usertype.so issystem

account [default=bad success=ok user\_unknown=ignore] pam\_sss.so

account required pam\_permit.so

**account [default=bad success=ok user\_unknown=ignore] pam\_ldap.so**

password requisite pam\_cracklib.so retry=3 minlen=7 dcredit=-2 ocredit=-2 difok=2 maxrepeat=2

password sufficient pam\_unix.so sha512 shadow nullok try\_first\_pass use\_authtok

**password sufficient pam\_ldap.so use\_authtok**

password sufficient pam\_winbind.so use\_authtok

password required pam\_deny.so

session optional pam\_keyinit.so revoke

session required pam\_limits.so

session optional pam\_systemd.so

session [success=1 default=ignore] pam\_succeed\_if.so service in crond quiet use\_uid

session required pam\_unix.so

session optional pam\_sss.so

**session optional pam\_ldap.so**

1. Modificar el archive /etc/authselect/password-auth con estos valores:

auth required pam\_env.so

auth sufficient pam\_unix.so nullok try\_first\_pass

auth requisite pam\_succeed\_if.so uid >= 500 quiet

auth sufficient pam\_ldap.so use\_first\_pass

auth required pam\_deny.so

account required pam\_unix.so broken\_shadow

account sufficient pam\_localuser.so

account sufficient pam\_succeed\_if.so uid < 500 quiet

account [default=bad success=ok user\_unknown=ignore] pam\_ldap.so

account required pam\_permit.so

password requisite pam\_cracklib.so try\_first\_pass retry=3 type=

password sufficient pam\_unix.so sha256 shadow nullok try\_first\_pass use\_authtok

password sufficient pam\_ldap.so use\_authtok

password required pam\_deny.so

session optional pam\_keyinit.so revoke

session required pam\_limits.so

session optional pam\_oddjob\_mkhomedir.so umask=0077

session [success=1 default=ignore] pam\_succeed\_if.so service in crond quiet use\_uid

session required pam\_unix.so

session optional pam\_ldap.so

1. Modificar el archivo /etc/pam.d/sshd con estos valores:

#%PAM-1.0

auth substack password-auth

auth include postlogin

account required pam\_sepermit.so

account required pam\_nologin.so

account include password-auth

password include password-auth

# pam\_selinux.so close should be the first session rule

session required pam\_selinux.so close

session required pam\_loginuid.so

# pam\_selinux.so open should only be followed by sessions to be executed in the user context

session required pam\_selinux.so open env\_params

session required pam\_namespace.so

session optional pam\_keyinit.so force revoke

session optional pam\_motd.so

session include password-auth

session include postlogin

**session required pam\_oddjob\_mkhomedir.so**

Por ultimo levantar los servicios y habilitarlos para en caso de un reinicio.

systemctl restart nslcd.service

systemctl restart nscd.service

systemctl restart messagebus

systemctl restart oddjobd.service

systemctl enable nslcd.service

systemctl enable nscd.service

systemctl enable oddjobd.service