#!/bin/bash

#import git that has config.php

yum install -y git

cd /tmp

git clone https://github.com/AmritSSC/hello-nti-310.git

#install ldap server material

yum install -y openldap-servers openldap-clients

#copy server example to production ldap

cp /usr/share/openldap-servers/DB\_CONFIG.example /var/lib/ldap/DB\_CONFIG

#change ownership to ldap from root

#chown ldap:ldap /var/lib/ldap/DB\_CONFIG

#Faster version of above indented command

chown ldap. /var/lib/ldap/DB\_CONFIG

#enable and slapd daemon

systemctl enable slapd

systemctl start slapd

#check status if desired:

systemctl status slapd

#install apache server: httpd (http daemon)

yum install httpd -y

#special repo of community driven project not installed in redhat( included in CentOS 7)

yum install epel-release -y

#install php ldap admin

yum install phpldapadmin -y

#Let apache server to connect to ldap without SELinux objecting

setsebool -P httpd\_can\_connect\_ldap on

#enable and start httpd; start apache server

systemctl enable httpd

systemctl start httpd

#modifies out apache server (httpd) so it can be accessed from external url.

#modifying phpldapadmin.conf server

sed -i 's,Require local,#Require local\n Require all granted,g' /etc/httpd/conf.d/phpldapadmin.conf

#remove alias for cp so it doesn't question copy overrides during automation process

unalias cp

#make backup copy of config file before modifying it:

cp /etc/phpldapadmin/config.php /etc/phpldapadmin/config.php.orig

#copy php config file here from repo

cp /tmp/hello-nti-310/config/config.php /etc/phpldapadmin/config.php

#change ownership to ldap group apache

chown ldap:apache /etc/phpldapadmin/config.php

#restart apache server

systemctl restart httpd.service

#give feedback to user that phpldapadmin install was successful, and continuing with configurations.

echo "phpldapadmin is now up and running"

echo "we are configuring ldap and ldapadmin"

#Generate, store, and hash new secret password securely

newsecret=$(slappasswd -g)

newhash=$(slappasswd -s "$newsecret")

#stores only in root/ldap\_admin\_pass file

echo -n "$newsecret" > /root/ldap\_admin\_pass

#restricts ldap\_admin\_pass to be read only by user

chmod 600 /root/ldap\_admin\_pass

#ldiff file, configures root domain name, assign username, domain component name and location, and password

echo -e "dn: olcDatabase = {2}hdb,cn=config

changetype: modify

replace: olcSuffix

olcSuffix: dc=nti310,dc=local

\n

dn: olcDatabase = {2}hdb,cn=config

changetype: modify

replace: olcRootDN

olcRootDN: cn=ldapadm,dc=nti310,dc=local

\n

dn: olcDatabase = {2}hdb,cn=config

changetype: modify

replace: olcRootPW

olcRootPW: $newhash" > db.ldif

#modifying root password according to domain specs

ldapmodify -Y EXTERNAL -H ldapi:/// -f db.ldif

#Auth restriction, giving external access to ldapadmin.nti310.local

echo 'dn: olcDatabase = {1}monitor,cn=config

changetype: modify

replace: olcAccess

olcAccess: {0}to \* by dn.base="gidNumber=0+uidNumber=0, cn=peercred, cn=external, cn=auth" read by dn.base="cn=ldapadmin,dc=nti310,dc=local" read by \* none' > monitor.ldif

#Reading in ldif just created

ldapmodify -Y EXTERNAL -H ldapi:/// -f monitor.ldif

#Generate ssl certs, will expire in a year

openssl req -new -x509 -nodes -out /etc/openldap/certs/nti310ldapcert.pem -keyout /etc/openldap/certs/nti310ldapkey.pem -days 365 -subj "/C=US/ST=WA/L=Seattle/O=SCC/OU=IT/CN=nti310.local"

#Change ownership to ldap user from root to make certs available in ldap

chown -R ldap. /etc/openldap/certs/nti\*.pem

#inserting certificates generated above into ldap, giving it certs and key

#Note: Key file must be executed before cert file

echo -e "dn: cn=config

changetype: modify

replace: olcTLSCertificateKeyFile

olcTLSCertificateKeyFile: /etc/openldap/certs/nti310ldapkey.pem

\n

dn: cn=config

changetype: modify

replace: olcTLSCertificateFile

olcTLSCertificateFile: /etc/openldap/certs/nti310ldapcert.pem" > certs.ldif

ldapmodify -Y EXTERNAL -H ldapi:/// -f certs.ldif