|  |
| --- |
| #!/bin/bash |
|  |

|  |
| --- |
|  |
|  |

|  |
| --- |
| yum install -y git |
|  |

|  |
| --- |
| cd /tmp |
|  |

|  |
| --- |
| git clone https://github.com/DFYT42/Linux-Automation-2 |
|  |

|  |
| --- |
|  |
|  |

|  |
| --- |
| yum -y install openldap-servers openldap-clients |
|  |

|  |
| --- |
|  |
|  |

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

|  |
| --- |
| #giving ownership from root to ldap bc ldap has to be owner of ldap daemon to get info |
|  |

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

|  |
| --- |
|  |
|  |

|  |
| --- |
| #ldap daemon |
|  |

|  |
| --- |
| systemctl enable slapd |
|  |

|  |
| --- |
| systemctl start slapd |
|  |

|  |
| --- |
|  |
|  |

|  |
| --- |
| #apache server |
|  |

|  |
| --- |
| yum -y install httpd |
|  |

|  |
| --- |
| yum -y install phpldapadmin |
|  |

|  |
| --- |
|  |
|  |

|  |
| --- |
| #Let's SELinux - know what is going on |
|  |

|  |
| --- |
| #NSA to harden and secure Linux systems |
|  |

|  |
| --- |
| #Apache connecct to ldap |
|  |

|  |
| --- |
| setsebool -P httpd\_can\_connect\_ldap on |
|  |

|  |
| --- |
|  |
|  |

|  |
| --- |
| systemctl enable httpd |
|  |

|  |
| --- |
| syetmctl start httpd |
|  |

|  |
| --- |
|  |
|  |

|  |
| --- |
| #modifies our httpd.conf to access from external URL |
|  |

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

|  |
| --- |
| unalias cp |
|  |

|  |
| --- |
|  |
|  |

|  |
| --- |
| #making backup in case something goes wrong |
|  |

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

|  |
| --- |
|  |
|  |

|  |
| --- |
| cp /tmp/DFYT42/Linux-Automation-2/config.php /etc/phpldapadmin/config.php |
|  |

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

|  |
| --- |
|  |
|  |

|  |
| --- |
| systemctl restart httpd.service |
|  |

|  |
| --- |
|  |
|  |

|  |
| --- |
| echo "phpldapadmin is now up and running" |
|  |

|  |
| --- |
| echo "we are configuring ldap and ldap admin" |
|  |

|  |
| --- |
|  |
|  |

|  |
| --- |
| #Generates and stores new passwords & restricts only root user to read |
|  |

|  |
| --- |
| newsecret=$(slappasswd -g) |
|  |

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

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

|  |
| --- |
| chmod 0600 /root/ldap\_admin\_pass |
|  |

|  |
| --- |
|  |
|  |

|  |
| --- |
| #Becomes ldif and configures root domain |
|  |

|  |
| --- |
| 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 |
|  |

|  |
| --- |
|  |
|  |

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

|  |
| --- |
|  |
|  |

|  |
| --- |
| #Auth restriction |
|  |

|  |
| --- |
|  |
|  |

|  |
| --- |
| 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=ldapadm,dc=nti310,dc=local" read by \* none' > monitor.ldif read by \* none' > monitor.ldif |
|  |

|  |
| --- |
|  |
|  |

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

|  |
| --- |
|  |
|  |

|  |
| --- |
| #Generates Certs |
|  |

|  |
| --- |
| 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" |
|  |

|  |
| --- |
|  |
|  |

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

|  |
| --- |
|  |
|  |

|  |
| --- |
| ##Error [root@ldap-b tmp]# ldapmodify -Y EXTERNAL -H ldapi:/// -f certs.ldif |
|  |

|  |
| --- |
| #SASL/EXTERNAL authentication started |
|  |

|  |
| --- |
| #SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth |
|  |

|  |
| --- |
| #SASL SSF: 0 |
|  |

|  |
| --- |
| #modifying entry "cn=config" |
|  |

|  |
| --- |
| #ldap\_modify: Other (e.g., implementation specific) error (80) |
|  |

|  |
| --- |
| #Solved this error by switching |
|  |

|  |
| --- |
|  |
|  |

|  |
| --- |
| 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 |
|  |

|  |
| --- |
|  |
|  |

|  |
| --- |
| #Test what certs are there: ldapsearch -Y EXTERNAL -H ldapi:/// -b cn=config | grep olcTLS |
|  |

|  |
| --- |
| #Test to see if cert config works |
|  |

|  |
| --- |
|  |
|  |

|  |
| --- |
| slaptest -u |
|  |

|  |
| --- |
| echo "it works" |
|  |

|  |
| --- |
|  |
|  |

|  |
| --- |
| unalias cp |
|  |

|  |
| --- |
|  |
|  |

|  |
| --- |
| ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/cosine.ldif |
|  |

|  |
| --- |
| ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/nis.ldif |
|  |

|  |
| --- |
| ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/inetorgperson.ldif |
|  |

|  |
| --- |
|  |
|  |

|  |
| --- |
| #creates group and people structure base |
|  |

|  |
| --- |
|  |
|  |

|  |
| --- |
| echo -e "dn: dc=nti310,dc=local |
|  |

|  |
| --- |
| dc: nti310 |
|  |

|  |
| --- |
| objectClass: top |
|  |

|  |
| --- |
| objectClass: domain |
|  |

|  |
| --- |
| \n |
|  |

|  |
| --- |
| dn: cn=ldapadm,dc=nti310,dc=local |
|  |

|  |
| --- |
| objectClass: organizationalRole |
|  |

|  |
| --- |
| cn: ldapadm |
|  |

|  |
| --- |
| description: LDAP Manager |
|  |

|  |
| --- |
| \n |
|  |

|  |
| --- |
| dn: ou=People,dc=nti310,dc=local |
|  |

|  |
| --- |
| objectClass: organizationalUnit |
|  |

|  |
| --- |
| ou: People |
|  |

|  |
| --- |
| \n |
|  |

|  |
| --- |
| dn: ou=Group,dc=nti310,dc=local |
|  |

|  |
| --- |
| objectClass: organizationalUnit |
|  |

|  |
| --- |
| ou: Group" > base.ldif |
|  |

|  |
| --- |
|  |
|  |

|  |
| --- |
| #Turn off SELinux to test |
|  |

|  |
| --- |
| setenforce 0 |
|  |

|  |
| --- |
|  |
|  |

|  |
| --- |
| #authenticate with this user and build org specifications from imported base.ldif |
|  |

|  |
| --- |
| #authenticate sourcing from previously created passwd w -y |
|  |

|  |
| --- |
| ldapadd -x -W -D "cn=ldapadm,dc=nti310,dc=local" -f base.ldif -y /root/ldap\_adim\_pass |
|  |

|  |
| --- |
|  |
|  |

systemctl restart httpd