OpenLDAP Kurulumu, Konfigürasyonu ve PasswordPolicy Kurulumu

Dosyayı burdan indirebilirsiniz - slapd.sh

Aşağıdaki adımlar Pardus 17.4 Server sürümünde test edilmiştir. Değişkenleri kendi kuracağınız ldap ortamına göre değiştirebilirsiniz.

NOT: kodu ekteki dosyayı indirerek kullanınız. Bu sayfa üzerinden yaptığınız kopyalamalarda ldapadd komutu boşluklara karşı hassas olduğundan problem çıkartabilir. (Confluence çalışma şeklinden dolayı boş satırlara bir adet space karakteri koyuyor. Bu da ldapadd komutunu bozuyor.)

```
#!/bin/bash
#TEST AMACLIDIR.
#slapd kurulumu

set -eux

#gerektigi sekilde duzenleyiniz.
config_organization_name=parduslab
config_fqdn="tlsldap.parduslab.com"
config_domain=parduslab.com
#ilk kurulumda sorulan cn=admin,cn=config kullanicinin parolasi
config_admin_password=plsecret
#otomatik olusturulan kullanicilarin parolalari
user_password=123

#degiskenler yukaridakiler, asagiya mudahale etmenize gerek yok.


config_domain_dc="dc=$(echo $config_domain | sed 's/\./,dc=/g')"
config_admin_dn="cn=admin,$config_domain_dc"
basedn=$config_domain_dc
rootdn="cn=admin,$basedn"
defaultpolicy="defaultppolicy"


#Balamadan önce etc/hosts dosyasna  ldap.example.com gibi ip kaydnz giriniz. dig ldap.example.com
# dediginizde dnsin cözümlemesi gerek.
echo "127.0.0.1 $config_fqdn" >>/etc/hosts

# these anwsers were obtained (after installing slapd) with:
#
#   #sudo debconf-show slapd
#   sudo apt-get install debconf-utils
#   # this way you can see the comments:
#   sudo debconf-get-selections
#   # this way you can just see the values needed for debconf-set-selections:
#   sudo debconf-get-selections | grep -E '^slapd\s+' | sort
export DEBIAN_FRONTEND=noninteractive
debconf-set-selections <<EOF
slapd slapd/password1 password $config_admin_password
slapd slapd/password2 password $config_admin_password
slapd slapd/domain string $config_domain
slapd shared/organization string $config_organization_name
EOF

apt-get install -y --no-install-recommends slapd ldap-utils

sleep 2
# create the people container.
# NB the `cn=admin,$config_domain_dc` user was automatically created
#    when the slapd package was installed.


ldapadd -D $config_admin_dn -w $config_admin_password <<EOF
dn: ou=people,$config_domain_dc
objectClass: organizationalUnit
ou: people
```

```
dn: ou=hq,$config_domain_dc
objectClass: organizationalUnit
ou: hq
EOF


# add people.
function add_person {
    local n=$1; shift
    local name=$1; shift
    ldapadd -D $config_admin_dn -w $config_admin_password <<EOF
dn: uid=$name,ou=people,$config_domain_dc
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
homeDirectory: /home/$name
loginShell: /bin/bash
objectClass: top
uidNumber: 512$((n+1))
gidNumber: 512$((n+1))
userPassword: $(slappasswd -s $user_password)
uid: $name
mail: $name@$config_domain
cn: $name
givenName: $name
sn: $name
#telephoneNumber: +1 888 555 000$((n+1))
#labeledURI: http://yavuz.com/~$name Personal Home Page
EOF
#jpegPhoto::$(base64 -w 66 avatar-$n.jpg | sed 's,^, ,g')

}
#people=(alice bob carol dave eve frank grace henry)
people=(yavuz enes serdar ciho)
for n in "${!people[@]}"; do
    add_person $n "${people[$n]}"
done


# show the configuration tree.
ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b cn=config dn | grep -v '^$'

# show the data tree.
ldapsearch -x -LLL -b $config_domain_dc dn | grep -v '^$'

# search for people and print some of their attributes.
ldapsearch -x -LLL -b $config_domain_dc '(objectClass=person)' cn mail

# ------ ou=people ve test kullanicilari eklenmesi bitti group  eklenmesi ile devam edilecek.


# config databsei icin rootpw tanimlanmasi
#configg kullanicisi ile bir sey yapacagin zaman parolan bu olacak
ldapmodify -Y EXTERNAL -H ldapi:///  <<EOF
dn: olcDatabase={0}config,cn=config
changetype: modify
add: olcRootPW
olcRootPW: $(slappasswd -s $config_admin_password)
EOF
#----slappasswd nin yanindaki 1111111111 hard coded parola deikene cevirdim.
#----ou=group  eklenmesi
ldapadd -D $config_admin_dn -w $config_admin_password <<EOF
dn: ou=groups,$config_domain_dc
objectClass: organizationalUnit
ou: groups
EOF

ldapmodify -Y EXTERNAL -H ldapi:///  <<EOF
dn: olcDatabase={1}mdb,cn=config
changetype: modify
replace: olcAccess
```

```
olcAccess: {0}to attrs=userPassword by self write by anonymous auth by * none
olcAccess: {1}to attrs=shadowLastChange by self write by self read by * none
olcAccess: {2}to * by self read by * none
EOF

ldapmodify -a -x -D "cn=admin,cn=config" -w $config_admin_password -f /etc/ldap/schema/ppolicy.ldif


ldapmodify -a -x -D "cn=admin,cn=config" -w $config_admin_password <<EOF
dn: cn=module{0},cn=config
changetype: modify
add: olcModuleLoad
olcModuleLoad: ppolicy
EOF

ldapmodify -a -x -D "cn=admin,cn=config" -w $config_admin_password <<EOF
dn: olcOverlay={0}ppolicy,olcDatabase={1}mdb,cn=config
objectClass: olcOverlayConfig
objectClass: olcPPolicyConfig
olcOverlay: {0}ppolicy
olcPPolicyDefault: cn=$defaultpolicy,ou=policy,$basedn
olcPPolicyHashCleartext: TRUE
olcPPolicyUseLockout: TRUE
olcPPolicyForwardUpdates: FALSE
EOF


systemctl restart slapd.service

sleep 3
#Policy öesini oluturma

ldapadd -x -w $config_admin_password -D "cn=admin,$basedn" <<EOF
dn: ou=policy,$basedn
objectClass: organizationalUnit
objectClass: top
ou: policy
description: password policy group

dn: cn=$defaultpolicy,ou=policy,$basedn
objectClass: person
objectClass: pwdPolicy
objectClass: top
cn: DefaultPolicy
pwdAttribute: userPassword
sn: DefaultPolicy
description: default password policy
pwdAllowUserChange: TRUE
pwdCheckQuality: 0
pwdExpireWarning: 599
pwdFailureCountInterval: 0
pwdGraceAuthNLimit: 2
pwdInHistory: 3
pwdLockout: TRUE
pwdLockoutDuration: 300
pwdMaxAge: 600
pwdMaxFailure: 3
pwdMinAge: 0
pwdMinLength: 4
pwdMustChange: TRUE
pwdSafeModify: FALSE
EOF
```

Bazı Password Policy yapılandırma ayarlarının karşılıkları aşağıdaki gibidir;

pwdExpireWarning: Şifrenin geçerliliğini yitireceği süreye dair uyarıların şifre geçerliliğini bitirmeden ne kadar süre önceden verilmeye başlayacağını belirler. Süre cinsi saniyedir.

pwdFailureCountInterval: Hatalı şifre sayacının, deneme yapılmaz ise, ne kadar sürede sıfırlanacağını belirler. 0 sayacın sıfırlanmayacağı anlamına gelir. Süre cinsi saniyedir.

pwdGraceAuthNLimit: Geçerliliğini yitirmiş ve değiştirilmiş şifrenin kaç kere kabul edileceğini belirler.

pwdInHistory: Sistemin kullanıcının en son kullandığı kaç şifreyi hatılayacağını belirler. Bu liste içerisindeki şifrelerin yeniden kullanımına izin verilmez. Parametre şifre sayısını belirler.

pwdLockout: TRUE ya da FALSE olabilir. Kullanıcıların şifrelerini ilgili alanda belirtilen sayı kadar hatalı girdikleri zaman hesaplarının kilitlenip kilitlenmeyeceğini belirler.

pwdLockoutDuration: Kullanıcıların hesapları eğer kilitlenirse, ne kadar süre kilitli kalacağını belirler. Süre cinsi saniyedir.

pwdMaxAge: Kullanıcıların şifrelerinin ne kadar süre geçerli olacağını belirler. Süre bitimi sonrasında kullanıcının şifresi güncellenmelidir. Yoksa kullanıcı giriş yapamaz. Süre cinsi saniyedir.

pwdMaxFailure: Kullanıcının hesabının kaç hatalı şifre girişi sonucu kilitleneceğini belirler.

pwdMinLength: Kullanıcının yeni şifresinin en az kaç karakter uzunluğunda olacağını belirler.

pwdMustChange: TRUE ya da FALSE olabilir. Kullanıcının şifre geçerliliği sona erdikten sonra şifresinin değiştirilmesi zorunluluğunu belirler.

pwdSafeModify: TRUE ya da FALSE olabilir. Kullanıcının şifre değiştirebilmesi için eski şifresini openLDAP sunucuya gönderip göndermeyeceğini belirler.