1→ Instalar OpenLDAP

```
[root@ldap-server carlos]#  yum install -y openldap openldap-clients openldap-servers migrationtools compat-openldap
```

```
[root@ldap-server carlos]# cp /usr/share/openldap-servers/DB_CONFIG.example /var/lib/ldap/DB_CONFIG
[root@ldap-server carlos]# chown ldap:ldap /var/lib/ldap/DB_CONFIG
```

```
[root@ldap-server carlos]#  systemctl start slapd
[root@ldap-server carlos]#  systemctl enable slapd
Created symlink from /etc/systemd/system/multi-user.target.wants/slapd.service to /usr/lib/systemd/system/slapd.service.
[root@ldap-server carlos]#  systemctl status slapd
● slapd.service - OpenLDAP Server Daemon
   Loaded: loaded (/usr/lib/systemd/system/slapd.service; enabled; vendor preset: disabled)
   Active: active (running) since mar 2017-03-07 19:02:23 CET; 31s ago
     Docs: man:slapd
           man:slapd-config
           man:slapd-hdb
           man:slapd-mdb
           file:///usr/share/doc/openldap-servers/guide.html
 Main PID: 6355 (slapd)
   CGroup: /system.slice/slapd.service
           └─6355 /usr/sbin/slapd -u ldap -h ldapi:/// ldap:///

mar 07 19:02:23 ldap-server.example.com systemd[1]: Starting OpenLDAP Server Daemon...
mar 07 19:02:23 ldap-server.example.com runuser[6341]: pam_unix(runuser:session): session opened for user ldap by (uid=0)
mar 07 19:02:23 ldap-server.example.com slapd[6352]: @(#) $OpenLDAP: slapd 2.4.40 (Nov  6 2016 01:21:28) $

mockbuild@worker1.bsys.centos.org:/builddir/build/BUILD/openldap-2.4.40/openlda...s/slapd
mar 07 19:02:23 ldap-server.example.com slapd[6355]: slapd starting
mar 07 19:02:23 ldap-server.example.com systemd[1]: Started OpenLDAP Server Daemon.
Hint: Some lines were ellipsized, use -l to show in full.
```

2→ Asignar password para admin

```
[root@ldap-server openldap]# cd /etc/openldap/
[root@ldap-server openldap]# slappasswd -s redhat -n > /etc/openldap/secret-passwd
```

```
[root@ldap-server openldap]# vi ch_olcDatabase={0}config.ldif
dn: olcDatabase={0}config,cn=config
changetype: modify
add: olcRootPW
olcRootPW: {SSHA}eg/ga/VKF17IZFlcl6J6DgGrXHMFCodQ
```

```
[root@ldap-server openldap]# ldapadd -Y EXTERNAL -H ldapi:/// -f ch_olcDatabase\=\{0\}config.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "olcDatabase={0}config,cn=config"
```

3→ Importación de schemas

```
[root@ldap-server openldap]# ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/cosine.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "cn=cosine,cn=schema,cn=config"
```

```
[root@ldap-server openldap]# ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/nis.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "cn=nis,cn=schema,cn=config"
```

```
[root@ldap-server openldap]# ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/inetorgperson.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "cn=inetorgperson,cn=schema,cn=config"
```

4→ Configurar Monitorización

```
[root@ldap-server openldap]# vi ch_olcDatabase={1}monitor.ldif
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=admin,dc=example,dc=com" read by * none
```

```
[root@ldap-server openldap]# ldapadd -Y EXTERNAL -H ldapi:/// -f ch_olcDatabase\=\{1\}monitor.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "olcDatabase={1}monitor,cn=config"
```

5→ Asignar dominio en la DB

```
[root@ldap-server openldap]# vi ch_olcDatabase={2}hdb.ldif
```

```
dn: olcDatabase={2}hdb,cn=config
changetype: modify
replace: olcSuffix
olcSuffix: dc=example,dc=com

dn: olcDatabase={2}hdb,cn=config
changetype: modify
replace: olcRootDN
olcRootDN: cn=admin,dc=example,dc=com

dn: olcDatabase={2}hdb,cn=config
changetype: modify
add: olcRootPW
olcRootPW: {SSHA}eg/ga/VKF17IZFlcl6J6DgGrXHMFCodQ

dn: olcDatabase={2}hdb,cn=config
changetype: modify
add: olcAccess
olcAccess: {0}to attrs=userPassword,shadowLastChange by
  dn="cn=admin,dc=example,dc=com" write by anonymous auth by self write by * none
olcAccess: {1}to dn.base="" by * read
olcAccess: {2}to * by dn="cn=admin,dc=example,dc=com" write by * read
```

```
[root@ldap-server openldap]# ldapmodify -Y EXTERNAL -H ldapi:/// -f ch_olcDatabase\=\{2\}hdb.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "olcDatabase={2}hdb,cn=config"

modifying entry "olcDatabase={2}hdb,cn=config"

modifying entry "olcDatabase={2}hdb,cn=config"

modifying entry "olcDatabase={2}hdb,cn=config"
```

6→ Añadir la base del dominio

```
[root@ldap-server openldap]# vi ch_base.ldif
```

```
dn: dc=example,dc=com
objectClass: top
```

```
objectClass: dcObject
objectclass: organization
o: Server example
dc: example

dn: cn=admin ,dc=example,dc=com
objectClass: organizationalRole
cn: admin
description: LDAP Manager

dn: ou=People,dc=example,dc=com
objectClass: organizationalUnit
ou: People

dn: ou=Group,dc=example,dc=com
objectClass: organizationalUnit
ou: Group
```

```
[root@ldap-server openldap]# ldapadd -x -D cn=admin,dc=example,dc=com -W -f ch_base.ldif
Enter LDAP Password:
adding new entry "dc=example,dc=com"

adding new entry "cn=admin ,dc=example,dc=com"

adding new entry "ou=People,dc=example,dc=com"

adding new entry "ou=Group,dc=example,dc=com"

[root@ldap-server openldap]# slaptest -u
config file testing succeeded
```

```
[root@ldap-server carlos]# ldapsearch -x -b dc=example,dc=com
# extended LDIF
#
# LDAPv3
# base <dc=example,dc=com> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# example.com
dn: dc=example,dc=com
objectClass: top
objectClass: dcObject
objectClass: organization
o: Server example
dc: example
```

```
# admin, example.com
dn: cn=admin,dc=example,dc=com
objectClass: organizationalRole
cn: admin
description: LDAP Manager

# People, example.com
dn: ou=People,dc=example,dc=com
objectClass: organizationalUnit
ou: People

# Group, example.com
dn: ou=Group,dc=example,dc=com
objectClass: organizationalUnit
ou: Group

# search result
search: 2
result: 0 Success

# numResponses: 5
# numEntries: 4

[root@ldap-server slapd.d]# ldapsearch -W -x -D cn=config -b olcDatabase={2}hdb,cn=config
Enter LDAP Password:
# extended LDIF
#
# LDAPv3
# base <olcDatabase={2}hdb,cn=config> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# {2}hdb, config
dn: olcDatabase={2}hdb,cn=config
objectClass: olcDatabaseConfig
objectClass: olcHdbConfig
olcDatabase: {2}hdb
olcDbDirectory: /var/lib/ldap
olcSuffix: dc=example,dc=com
olcAccess: {0}to attrs=userPassword,shadowLastChange by dn="cn=admin,dc=exampl
 e,dc=com" write by anonymous auth by self write by * none
olcAccess: {1}to dn.base="" by * read
olcAccess: {2}to * by dn="cn=admin,dc=example,dc=com" write by * read
olcRootDN: cn=admin,dc=example,dc=com
olcRootPW: {SSHA}eg/ga/VKF17IZFlcl6J6DgGrXHMFCodQ
olcDbIndex: objectClass eq,pres
```

```
olcDbIndex: ou,cn,mail,surname,givenname eq,pres,sub

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1

[root@ldap-server slapd.d]# ldapsearch -W -x -D cn=config -b cn=config
"(objectclass=olcGlobal)"
Enter LDAP Password:
# extended LDIF
#
# LDAPv3
# base <cn=config> with scope subtree
# filter: (objectclass=olcGlobal)
# requesting: ALL
#

# config
dn: cn=config
objectClass: olcGlobal
cn: config
olcArgsFile: /var/run/openldap/slapd.args
olcPidFile: /var/run/openldap/slapd.pid
olcTLSCACertificatePath: /etc/openldap/certs
olcTLSCertificateFile: "OpenLDAP Server"
olcTLSCertificateKeyFile: /etc/openldap/certs/password

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

7→ Habilitar ldaps y chequear puertos

```
[root@ldap-server openldap]# vi /etc/sysconfig/slapd
# OpenLDAP server configuration
# see 'man slapd' for additional information

# Where the server will run (-h option)
# - ldapi:/// is required for on-the-fly configuration using client tools
#   (use SASL with EXTERNAL mechanism for authentication)
# - default: ldapi:/// ldap:///
# - example: ldapi:/// ldap://127.0.0.1/ ldap://10.0.0.1:1389/ ldaps:///
```

```
SLAPD_URLS="ldapi:/// ldap:/// ldaps:///"

# Any custom options
#SLAPD_OPTIONS=""

# Keytab location for GSSAPI Kerberos authentication
#KRB5_KTNAME="FILE:/etc/openldap/ldap.keytab"
```

```
[root@ldap-server openldap]# netstat -lt |grep ldap
tcp        0      0 0.0.0.0:ldaps           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:ldap            0.0.0.0:*               LISTEN
tcp6       0      0 [::]:ldaps              [::]:*                  LISTEN
tcp6       0      0 [::]:ldap               [::]:*                  LISTEN
```

```
[root@ldap-server openldap]# netstat -tunlp |egrep "389|636"
tcp        0      0 0.0.0.0:636             0.0.0.0:*               LISTEN      2900/slapd
tcp        0      0 0.0.0.0:389             0.0.0.0:*               LISTEN      2900/slapd
tcp6       0      0 :::636                  :::*                    LISTEN      2900/slapd
tcp6       0      0 :::389                  :::*                    LISTEN      2900/slapd
```