***LDAP***

|  |  |
| --- | --- |
| Easy steps for adding users:  1. Create unix user  2. Create unix user's ldap passwd file  3. Convert passwd.file to ldif file  4. Add ldap file to LDAP Directory using ldapadd  Step #1. Requirements  compat-openldap.i386 0:2.1.30-6.4E  openldap-clients.i386 0:2.2.13-6.4E  openldap-devel.i386 0:2.2.13-6.4E  openldap-servers.i386 0:2.2.13-6.4E  openldap-servers-sql.i386 0:2.2.13-6.4E  Step #2. Start the service  [root@ldap ~]# chkconfig --levels 235 ldap on  [root@ldap ~]# service ldap start  Step #3. Create LDAP root user password  [root@ldap ~]# slappasswd  New password:  Re-enter new password:  {SSHA}cWB1VzxDXZLf6F4pwvyNvApBQ8G/DltW  [root@ldap ~]#  Step #4. Update /etc/openldap/slapd.conf for the root password  [root@ldap ~]# vi /etc/openldap/slapd.conf  #68 database bdb  #69 suffix "dc=ensat,dc=ma"  #70 rootdn "cn=Manager,dc=ensat,dc=ma"  #71 rootpw {SSHA}cWB1VzxDXZLf6F4pwvyNvApBQ8G/DltW  Step #5. Apply Changes  [root@ldap ~]# service ldap restart  Step #10. Update root.ldif file for the "Manager" of LDAP Server  [root@ldap ~]# vi /etc/openldap/root.ldif  #1 dn: uid=root,ou=People,dc=ensat,dc=ma  #2 uid: root  #3 cn: Manager  #4 objectClass: account  Step #11. Create a domain ldif file (/etc/openldap/ensat.ma.ldif)  [root@ldap ~]# cat /etc/openldap/ensat.ma.ldif  dn: dc=ensat,dc=ma  dc: ensat  description: LDAP Admin  objectClass: dcObject  objectClass: organizationalUnit  ou: rootobject  dn: ou=People, dc=ensat,dc=ma  ou: People  description: Users of ensat  objectClass: organizationalUnit  Step #12. Import all users in to the LDAP  Add the Domain ldif file  [root@ldap ~]#vi /etc/openldap/ldap.conf  [root@ldap ~]# ldapadd -x -D "cn=Manager,dc=ensat,dc=ma" -W -f /etc/openldap/ensat.ma.ldif  Enter LDAP Password:  adding new entry "dc=ensat,dc=ma"  adding new entry "ou=People, dc=ensat,dc=ma"  [root@ldap ~]#  Add the users:  [root@ldap ~]# ldapadd -x -D "cn=Manager,dc=ensat,dc=ma" -W -f /etc/openldap/root.ldif  Enter LDAP Password:  adding new entry "uid=root,ou=People,dc=ensat,dc=ma"  adding new entry "uid=operator,ou=People,dc=ensat,dc=ma" | Step #6. Create test users  [root@ldap ~]# useradd test1  [root@ldap ~]# passwd test1  Changing password for user test1.  New UNIX password:  Retype new UNIX password:  passwd: all authentication tokens updated successfully.  [root@ldap ~]# useradd test2  [root@ldap ~]# passwd test2  Changing password for user test2.  New UNIX password:  Retype new UNIX password:  passwd: all authentication tokens updated successfully.  [root@ldap ~]#  Step #7. Migrate local users to LDAP  [root@ldap ~]# grep root /etc/passwd > /etc/openldap/passwd.root  [root@ldap ~]# grep test1 /etc/passwd > /etc/openldap/passwd.test1  [root@ldap ~]# grep test2 /etc/passwd > /etc/openldap/passwd.test2  Step #8. Update default settings on file /usr/share/openldap/migration/migrate\_common.ph  #71 $DEFAULT\_MAIL\_DOMAIN = "ensat.ma";  #74 $DEFAULT\_BASE = "dc=ensat,dc=ma";  Step #9. Convert passwd.file to ldif (LDAP Data Interchange Format) file  [root@ldap ~]# /usr/share/openldap/migration/migrate\_passwd.pl /etc/openldap/passwd.root /etc/openldap/root.ldif  [root@ldap ~]# /usr/share/openldap/migration/migrate\_passwd.pl /etc/openldap/passwd.test1 /etc/openldap/test1.ldif  [root@ldap ~]# /usr/share/openldap/migration/migrate\_passwd.pl /etc/openldap/passwd.test2 /etc/openldap/test2.ldif  [root@ldap ~]# ldapadd -x -D "cn=Manager,dc=ensat,dc=ma" -W -f /etc/openldap/test1.ldif  Enter LDAP Password:  adding new entry "uid=test1,ou=People,dc=ensat,dc=ma"  [root@ldap ~]#  [root@ldap ~]# ldapadd -x -D "cn=Manager,dc=ensat,dc=ma" -W -f /etc/openldap/test2.ldif  Enter LDAP Password:  adding new entry "uid=test2,ou=People,dc=ensat,dc=ma"  [root@ldap ~]#  Note: Repeat the same for the rest of users  Step #13. Apply Changes  [root@ldap ~]# service ldap restart  Step #14. Test LDAP Server  It prints all the user information:  [root@ldap ~]# ldapsearch -x -b 'dc=ensat,dc=ma' '(objectclass=\*)'  authconfig-gtk  getent passwd test1  userdel test1  getent passwd test1  Step #15. Modifier un mot de passe  dn: uid=test1,ou=People,dc=ensat,dc=ma  changetype: modify  replace: userPassword  userPassword: {SSHA}AjHGT0UqSa/JnhVA8LTo0QMp1DtFslZo  ldapmodify -W -D "cn=Manager,dc=ensat,dc=ma" -x -H ldap://192.168.2.1 -f /etc/openldap/test11.ldif |