Autoryzacja 1

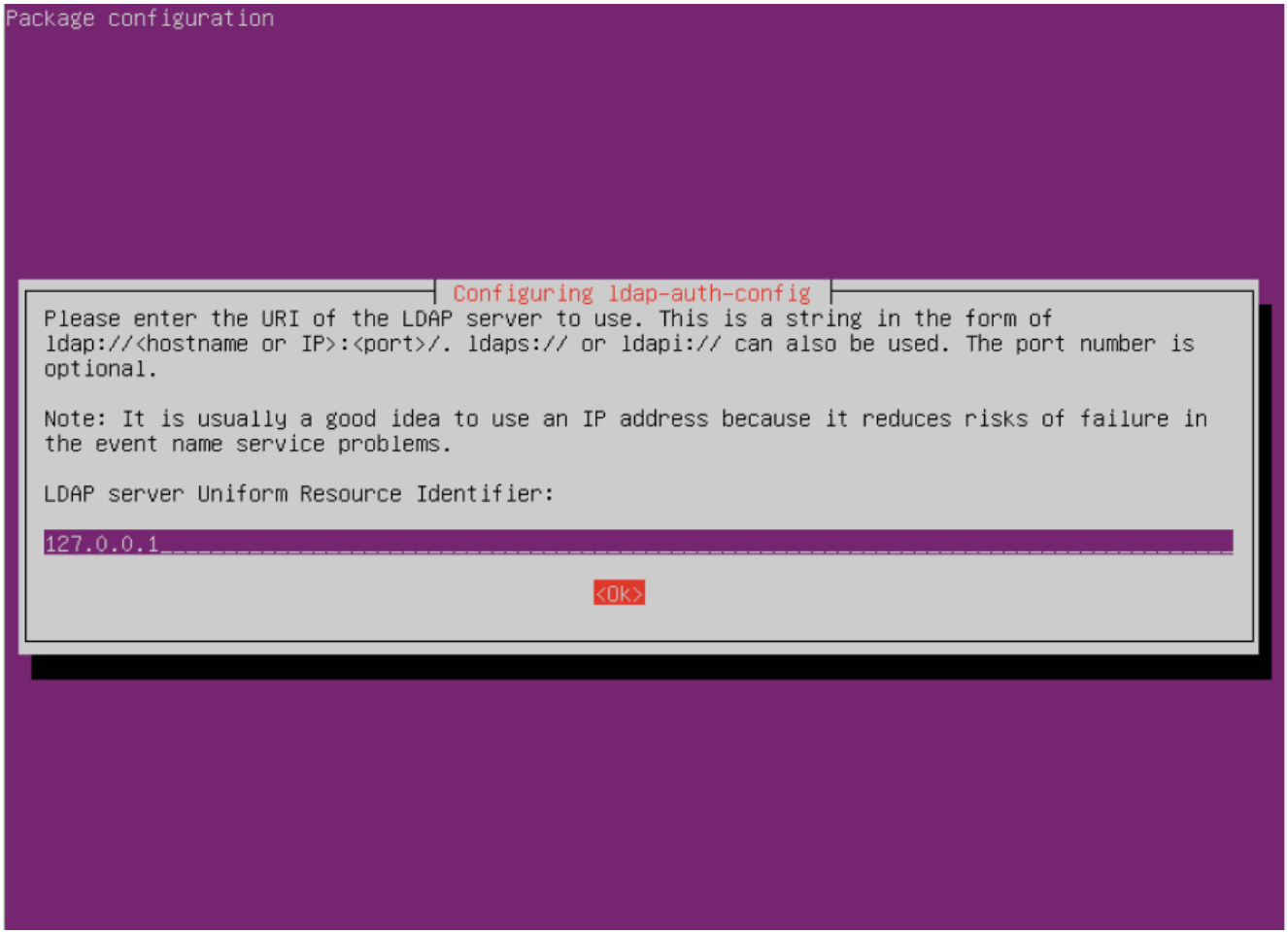
written by archi | 16 października 2019

vcwilab.wi.zut.edu.pl

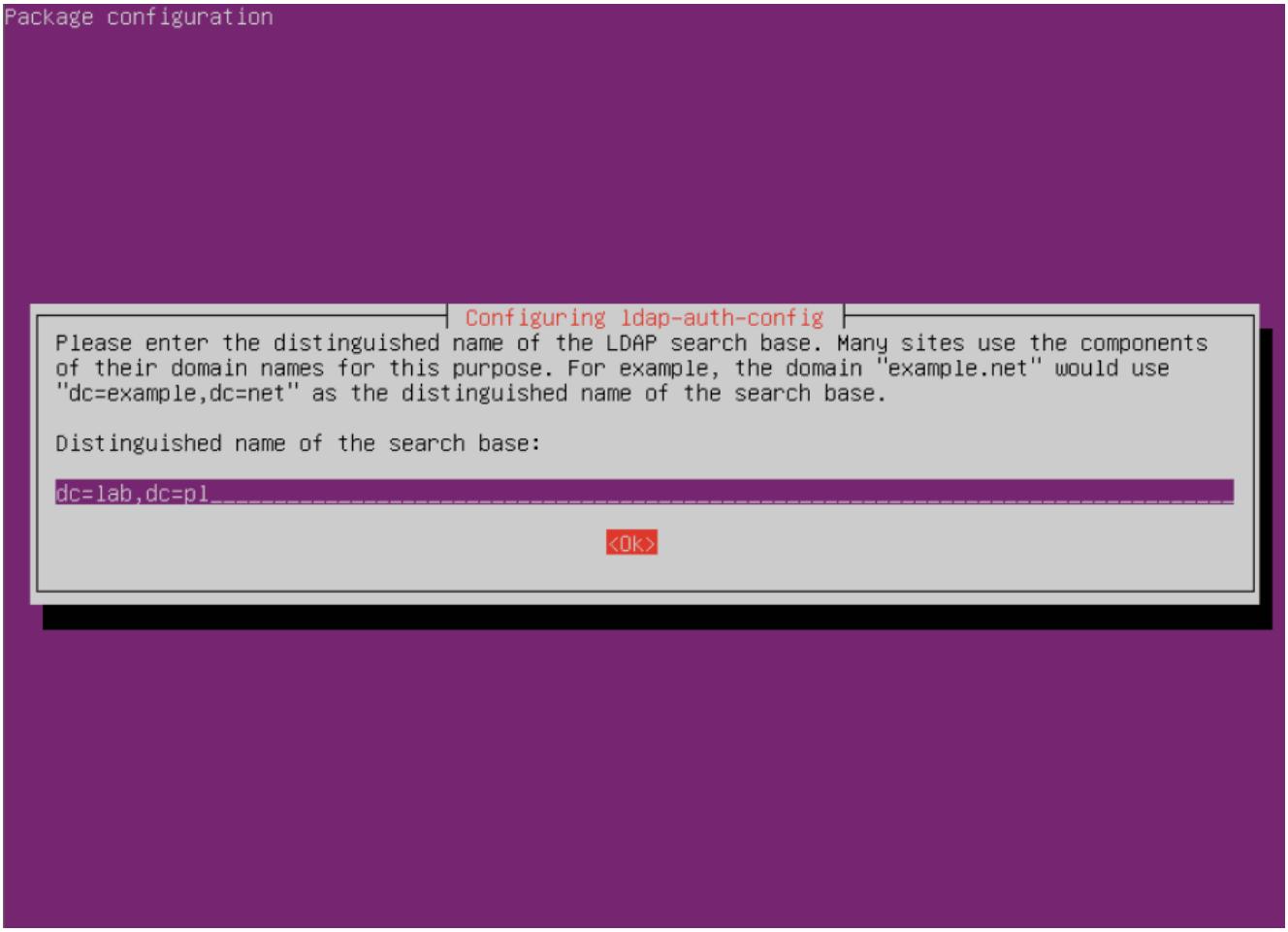
Uruchamiamy integrację systemu operacyjnego z LDAP. W tym celu musimy zainstalować kilka dodatków rozszerzających możliwości systemu operacyjnego:

- „`libnss-ldap`„

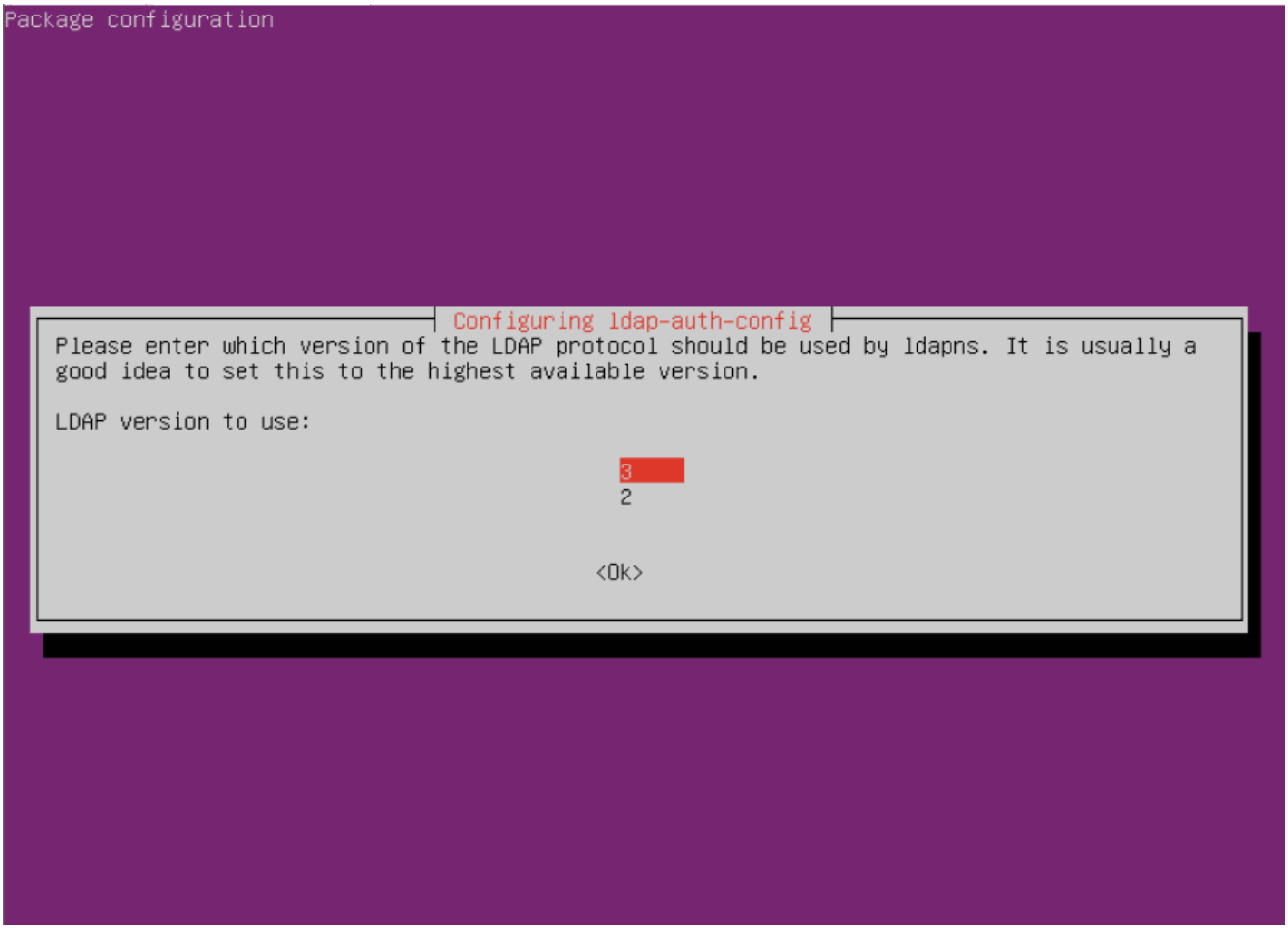
2. W trakcie instalacji system poprosi o podanie danych pozwalających na przyłączenie się do LDAP (**podaj wyłącznie w tej linii !!!!! : 127.0.0.1**):



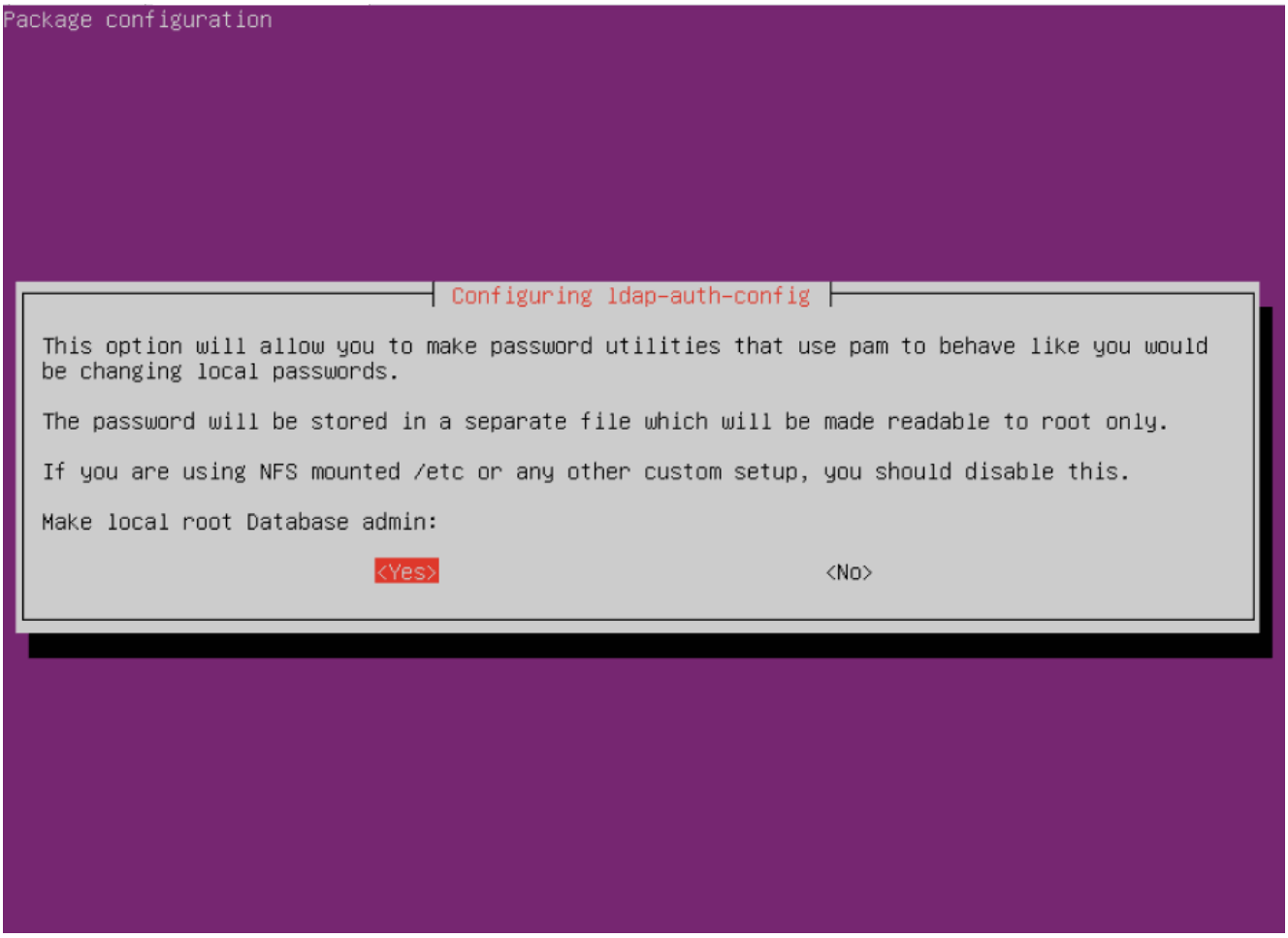
UWAGA! : zmieniona domena LDAP na: **dc=lab,dc=pl**



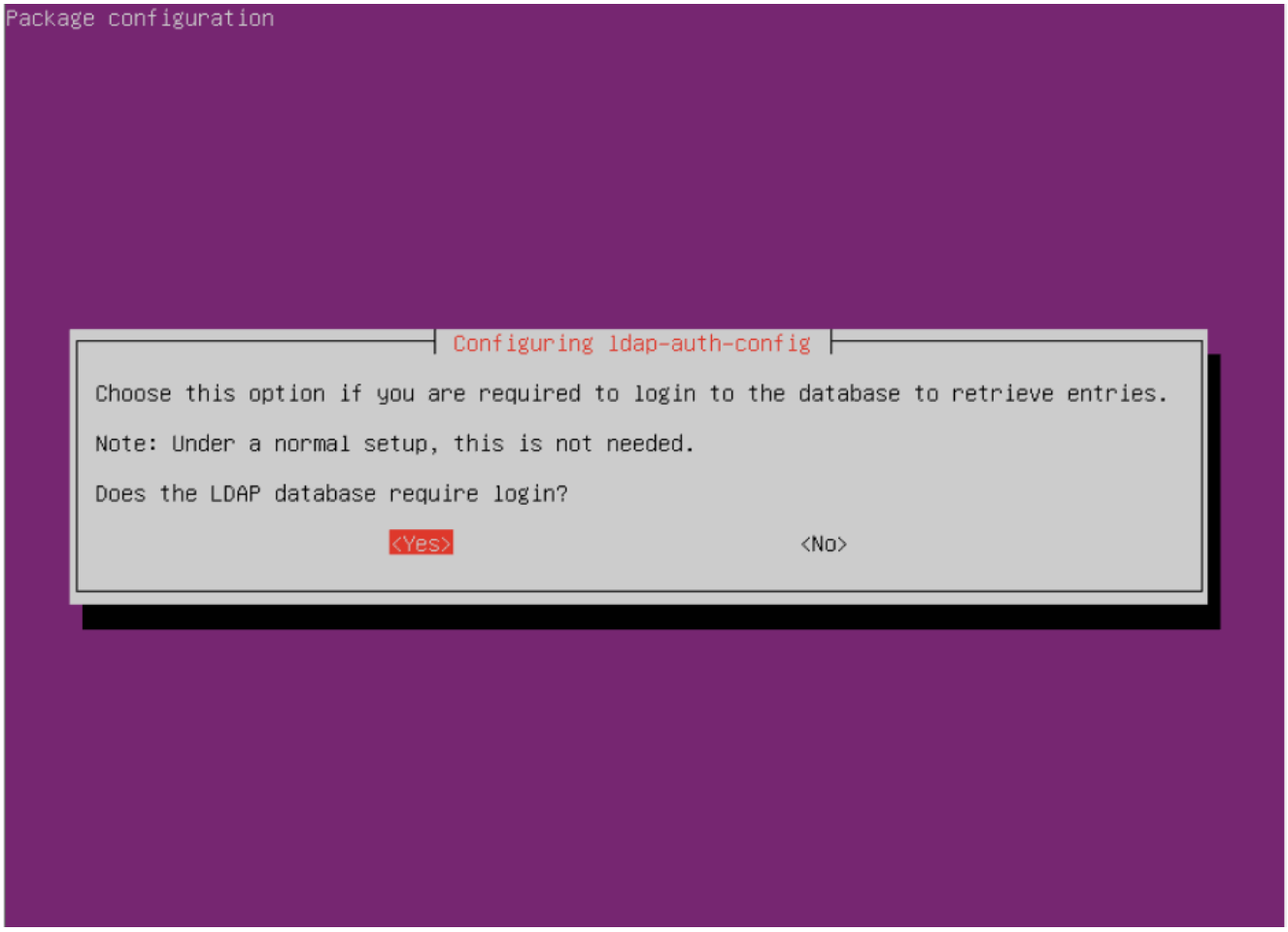
LDAP version: 3



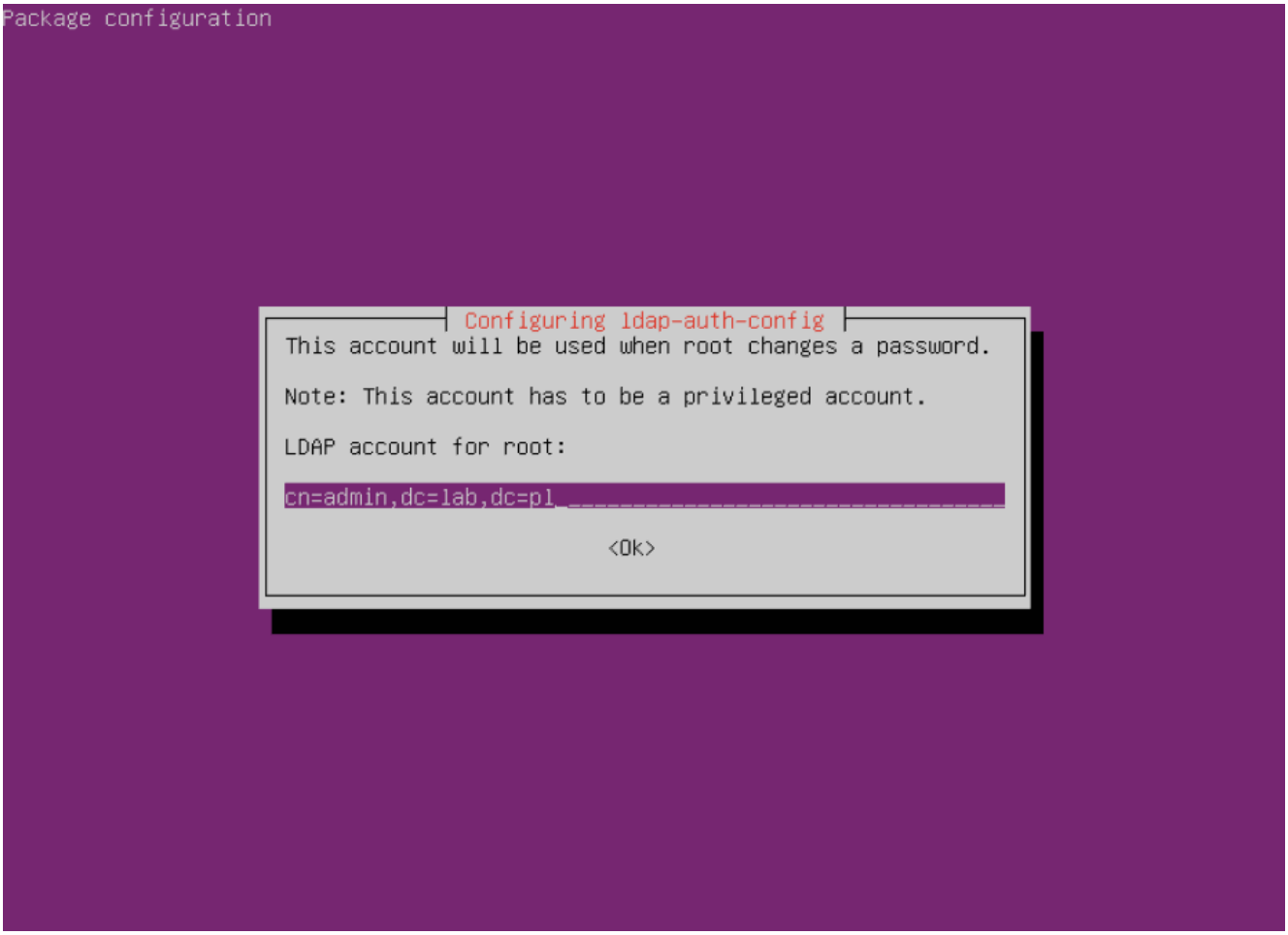
Ustawiamy konto root jako admina LDAP



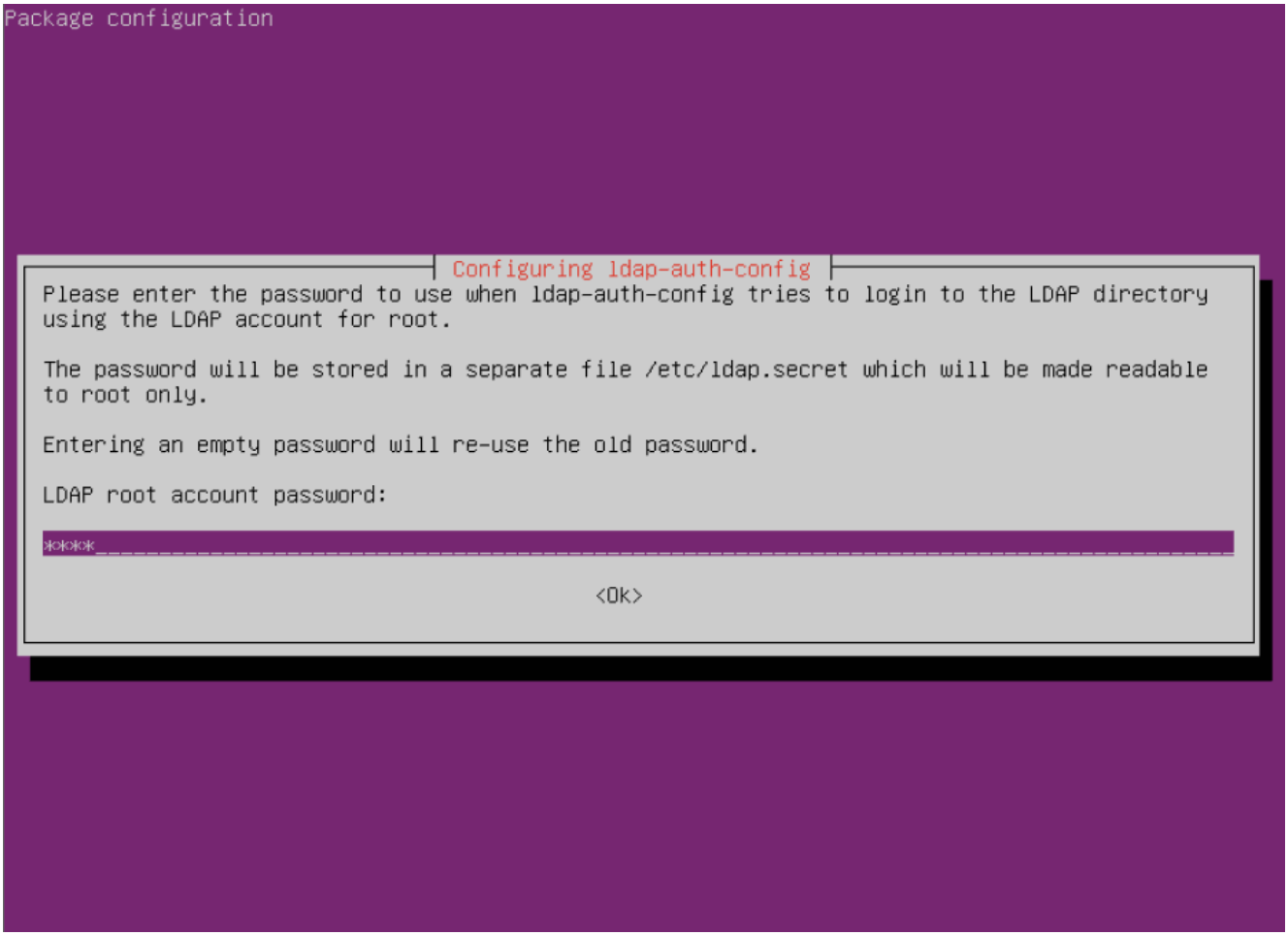
Włączamy wymaganie logowania do dostępu do bazy LDAP



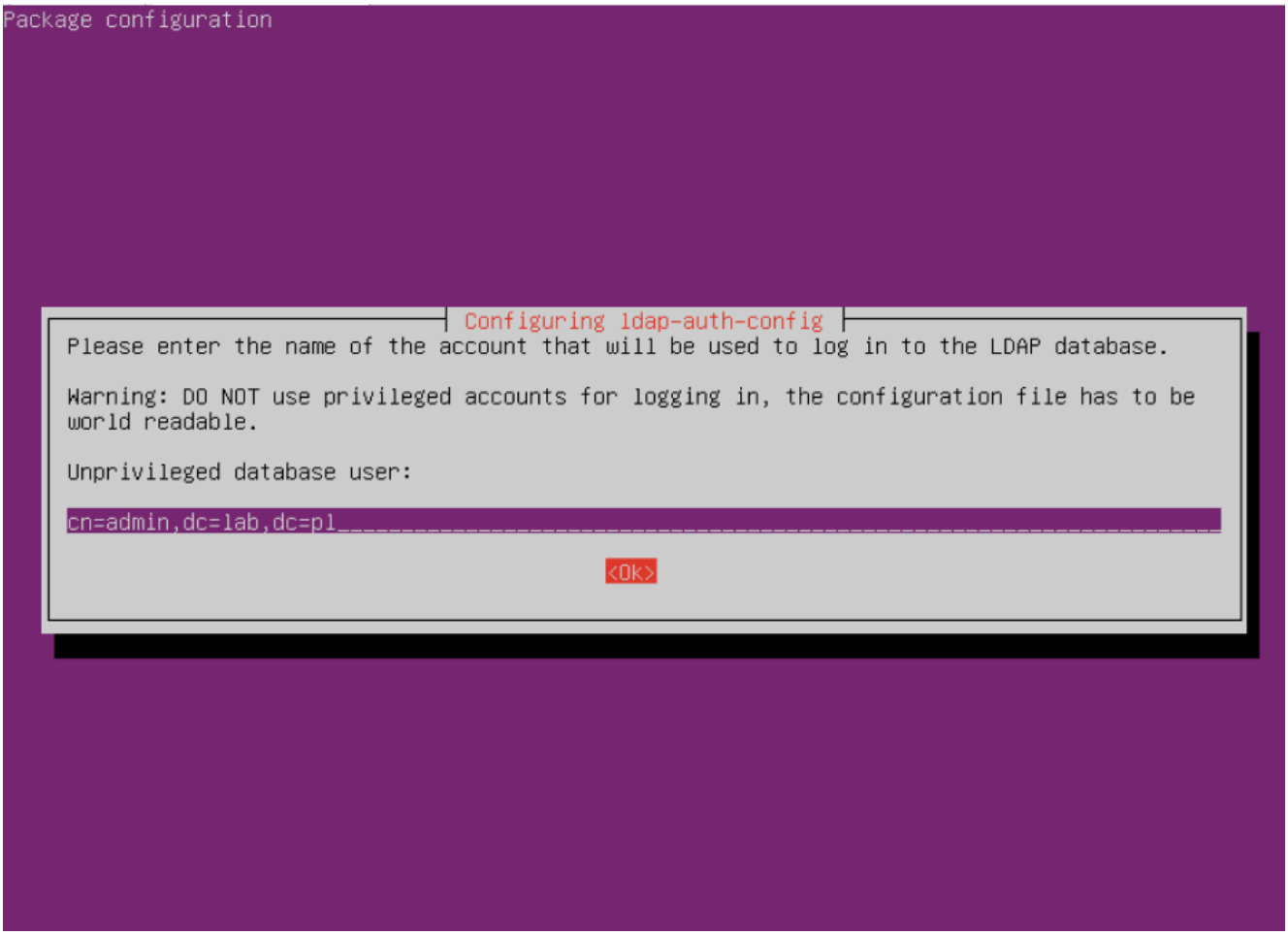
LDAP account for root: cn=admin,dc=lab,dc=pl



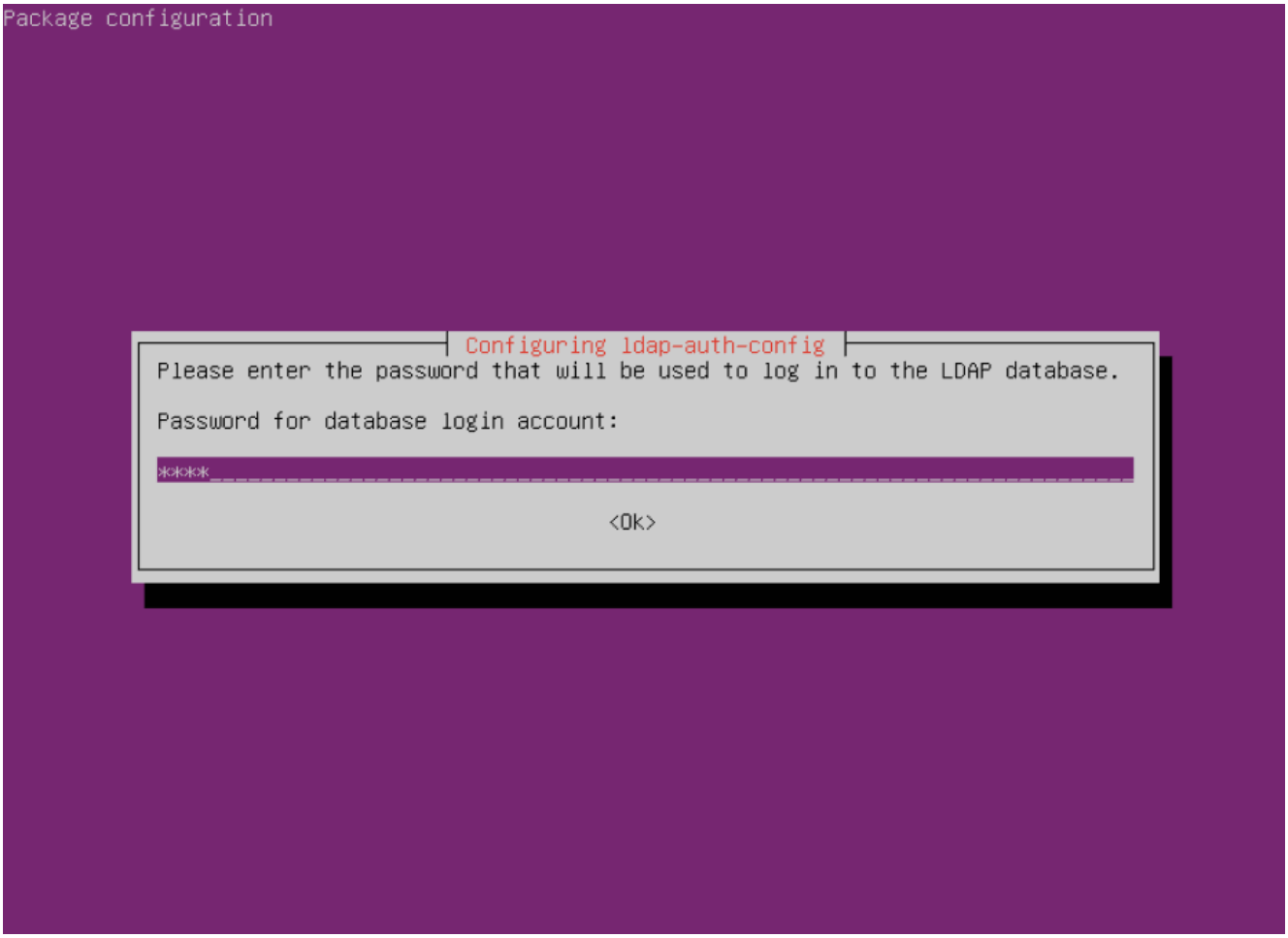
Podać właściwe hasło dla użytkownika ADMIN (podane w poprzednim laboratorium)



Wskazać jako użytkownika uprzywilejowanego na: cn=admin,dc=lab,dc=pl



Podać właściwe hasło (jak było wcześniej)

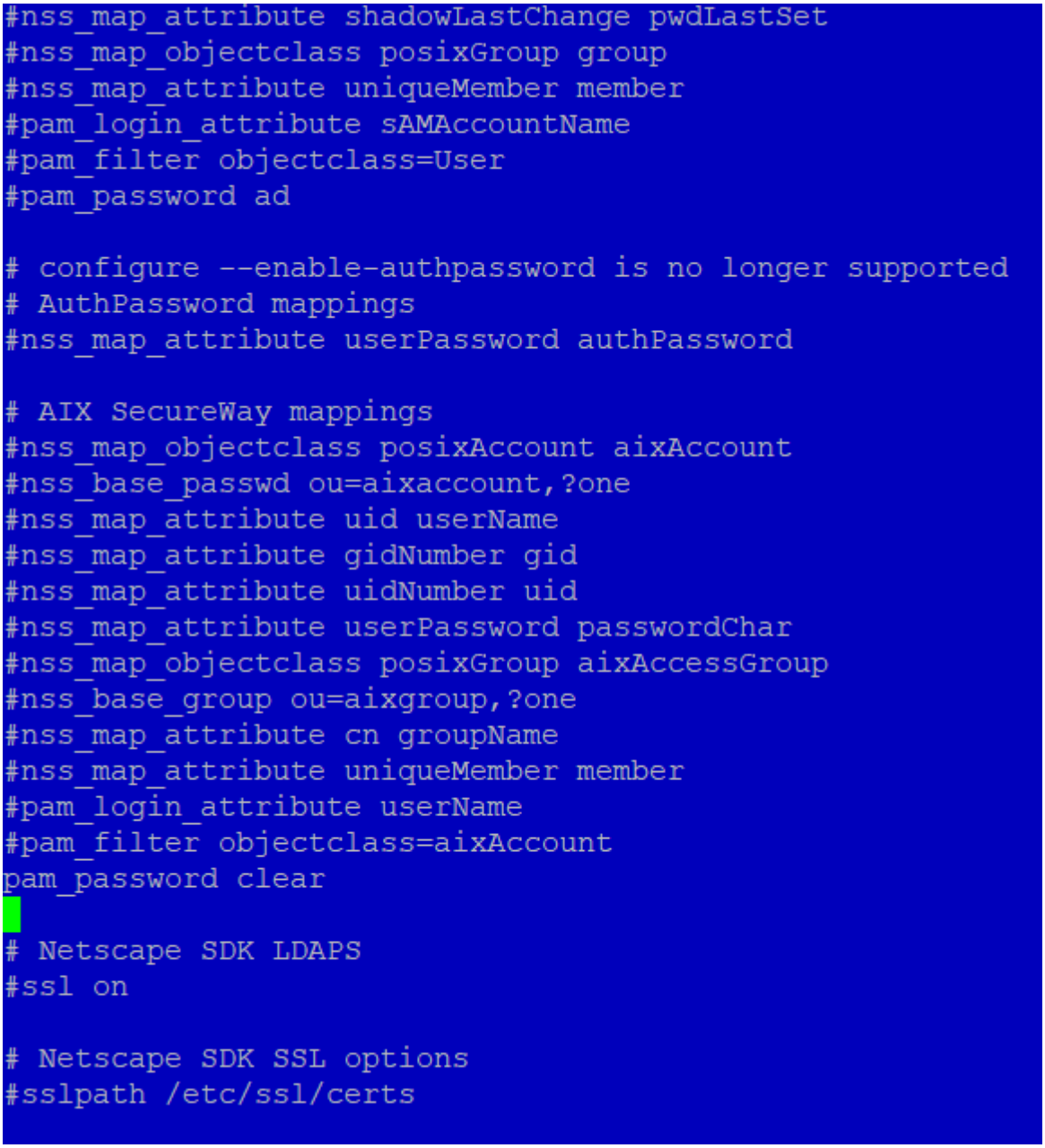


3. Zmieniamy ustawienia w pliku „`/etc/ldap.conf`„

- Przestawiamy SCOPE na „SUB”

```
#uri ldaps://127.0.0.1/...
#uri ldapi://%2fvar%2frun%2fldapi_sock/
# Note: %2f encodes the '/' used as directory separator

# The LDAP version to use (defaults to 3
# if supported by client library)
ldap_version 3

# The distinguished name to bind to the server with.
# Optional: default is to bind anonymously.
binddn cn=admin,dc=lab,dc=pl

# The credentials to bind with..
# Optional: default is no credential.
bindpw user

# The distinguished name to bind to the server with
# if the effective user ID is root. Password is
# stored in /etc/ldap.secret (mode 600)
rootbinddn cn=admin,dc=lab,dc=pl

# The port.
# Optional: default is 389.
#port 389

# The search scope.
scope sub
#scope one
#scope base

# Search timelimit
#timelimit 30
```

- Włączamy obsługę przesyłania jawnych haseł

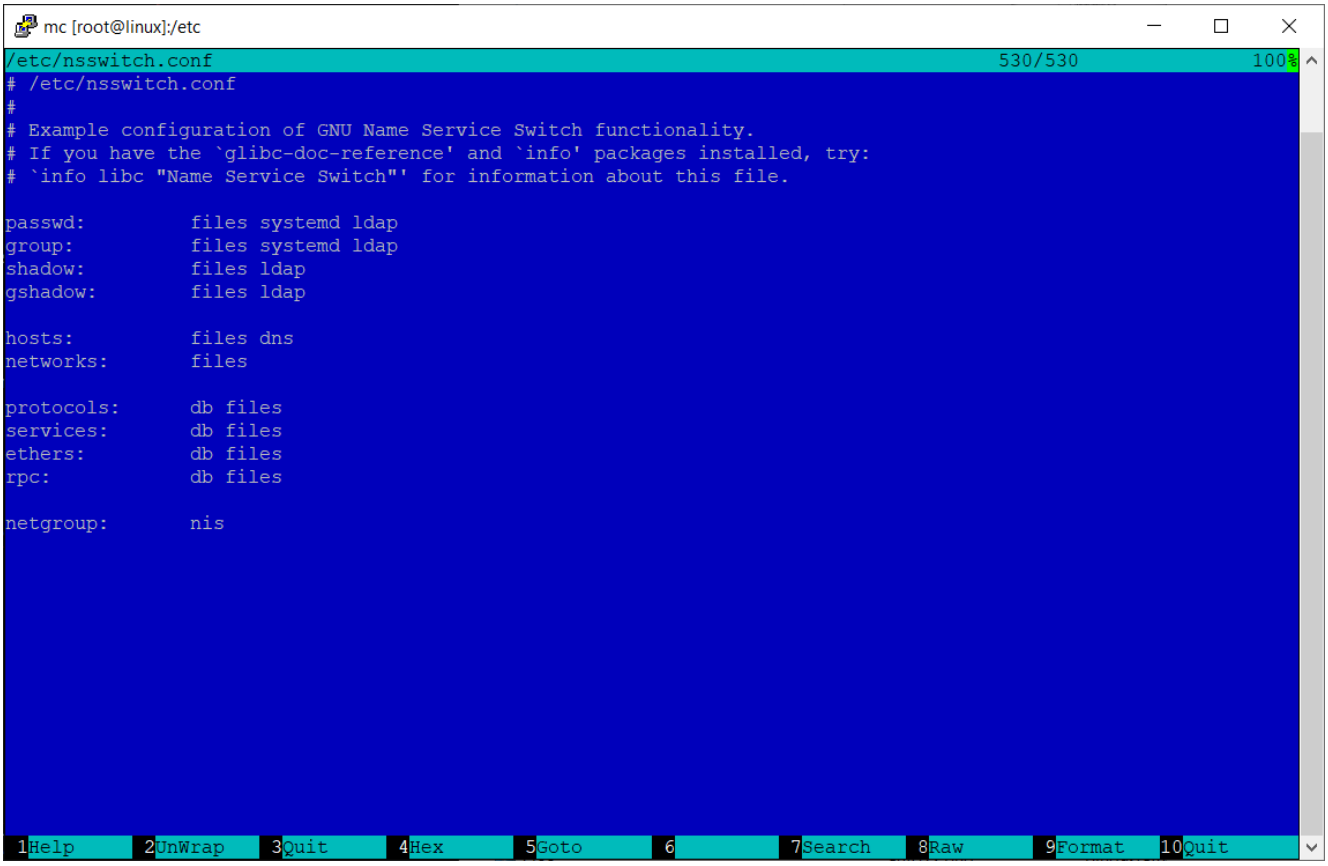


```
#nss_map_attribute shadowLastChange pwdLastSet
#nss_map_objectclass posixGroup group
#nss_map_attribute uniqueMember member
#pam_login_attribute sAMAccountName
#pam_filter objectclass=User
#pam_password ad

# configure --enable-authpassword is no longer supported
# AuthPassword mappings
#nss_map_attribute userPassword authPassword

# AIX SecureWay mappings
#nss_map_objectclass posixAccount aixAccount
#nss_base_passwd ou=aixaccount,?one
#nss_map_attribute uid userName
#nss_map_attribute gidNumber gid
#nss_map_attribute uidNumber uid
#nss_map_attribute userPassword passwordChar
#nss_map_objectclass posixGroup aixAccessGroup
#nss_base_group ou=aixgroup,?one
#nss_map_attribute cn groupName
#nss_map_attribute uniqueMember member
#pam_login_attribute userName
#pam_filter objectclass=aixAccount
pam_password clear

# Netscape SDK LDAPS
#ssl on

# Netscape SDK SSL options
#sslpath /etc/ssl/certs
```

- Zapisujemy modyfikacje w pliku...

4. Dopisujemy obsługę LDAP do „`/etc/nsswitch.conf`„

- Dopisujemy wykorzystanie bazy LDAP



- Zapisujemy modyfikacje...

5. Jeżeli wykonaliśmy wszystko poprawnie powinni być widoczni użytkownicy z bazy LDAP. Można to sprawdzić przy pomocy polecenia „id” ze wskazaniem nazwy użytkownika np.:

```
id user1
```

W wyniku otrzymamy informacje o użytkowniku user1 (jego UID i GID)

```
uid=10000(user1) gid=100(users) grupy=100(users)
```