Wielo-serwerowe środowisko linux (OpenLDAP + NFS)

written by archi | 17 stycznia 2022

Laboratoria mają na celu uruchomienie współdzielenia zasobów sieciowych pomiędzy serwerami Linux z wykorzystaniem protokołu NFS oraz stworzenie jednorodnego środowiska użytkownika tej sieci z wykorzystaniem usługi katalogowej OpenLDAP.

Wymagania laboratorium:

- dwa serwery linux
- zainstalowanie na jednym z nich usługi OpenLDAP
- przygotowanie udostępnienia NFS Share dla drugiego serwera

Przygotowanie nowego serwera Ubuntu – klient usługi.

Bazując na wcześniejszych laboratoriach (lab 4 i lab 1) przygotuj nową maszynę wirtualną Ubuntu 22.04 LTS o podanych poniżej parametrach wraz z zainstalowanym systemem operacyjnym Ubuntu.

- CPU: 2 wirtualny procesor
- RAM: 2 GB pamięci

- DYSK: 10 GB jako urządzenie SCSI

Po zakończonej instalacji systemu proszę w pierwszej kolejności zaktualizować system i następnie doinstalować na kliencie pakiet **nfs-common**. Będzie on niezbędny do wykonania montowania (przyłączenia) udziału udostępnionego po NFS.

Przygotowanie serwera NFS

Na maszynie wirtualnej którą aktualnie używasz (poprzednie laboratoria) po aktualizacji systemu (apt update; apt upgrade) zainstaluj pakiet **nfs-kernel-server**. Jest to usługa dystrybucji folderów i plików na zdalną maszynę (klienta) z wykorzystaniem protokołu NFS

Po zainstalowaniu pakietu należy skonfigurować udostępnienia. W tym celu edytuj plik **`/etc/exports`** i wewnątrz dodaj na końcu wpis udostępnienia folderu **`/home.`**

odpowiednio należy wskazać w konfiguracji:

- ścieżka do udostępnienia
- adres IP klienta dla którego udostępniamy
- parametry udostępnienia: **rw** – odczyt/zapis; **sync** – tryb natychmiastowej synchronizacji; **no_subtree_check** – brak sprawdzania struktury folderów; **no_root_squash** – nie odejmowanie uprawnień użytkownika root = na każdym serwerze tj. kliencie i serwerze NFS root ma te same prawa do udostępnienia

```
/etc/exports                                                    451/451   100%
# /etc/exports: the access control list for filesystems which may be exported
#               to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes       hostname1(rw,sync,no_subtree_check) hostname2(ro,sync,no_subtree_check)
#
# Example for NFSv4:
# /srv/nfs4        gss/krb5i(rw,sync,fsid=0,crossmnt,no_subtree_check)
# /srv/nfs4/homes  gss/krb5i(rw,sync,no_subtree_check)
#
/home   192.168.99.120(rw,sync,no_subtree_check,no_root_squash)
```

Na obrazku jest przykładowy adres IP – Ty będziesz miał inny adres IP

Zapisz konfigurację i zrestartuj usługę nfs-kernet-server

```
root@linux:~# service nfs-kernel-server restart
root@linux:~# service nfs-kernel-server status
● nfs-server.service - NFS server and services
     Loaded: loaded (/lib/systemd/system/nfs-server.service; enabled; vendor preset: enabled)
     Active: active (exited) since Thu 2021-04-29 19:28:33 UTC; 2s ago
    Process: 58919 ExecStartPre=/usr/sbin/exportfs -r (code=exited, status=0/SUCCESS)
    Process: 58920 ExecStart=/usr/sbin/rpc.nfsd $RPCNFSDARGS (code=exited, status=0/SUCCESS)
   Main PID: 58920 (code=exited, status=0/SUCCESS)

Apr 29 19:28:32 linux systemd[1]: Starting NFS server and services...
Apr 29 19:28:33 linux systemd[1]: Finished NFS server and services.
root@linux:~#
```

Na serwerze klienta możesz sprawdzić czy udział jest dla ciebie dostępny poprzez polecenia showmount

```
root@klient:~# showmount -e 192.168.99.124
Export list for 192.168.99.124:
/home 192.168.99.120
root@klient:~#
```

Przetestuj możliwość podłączenia do swojego systemu udostępnienia przy pomocy polecenia

mount -t nfs adres_ip_maszyny_serwera_nfs:/home /mnt

Wykonując polecenie **mount** zobaczysz przypięte systemy plików w tym podłączony udział

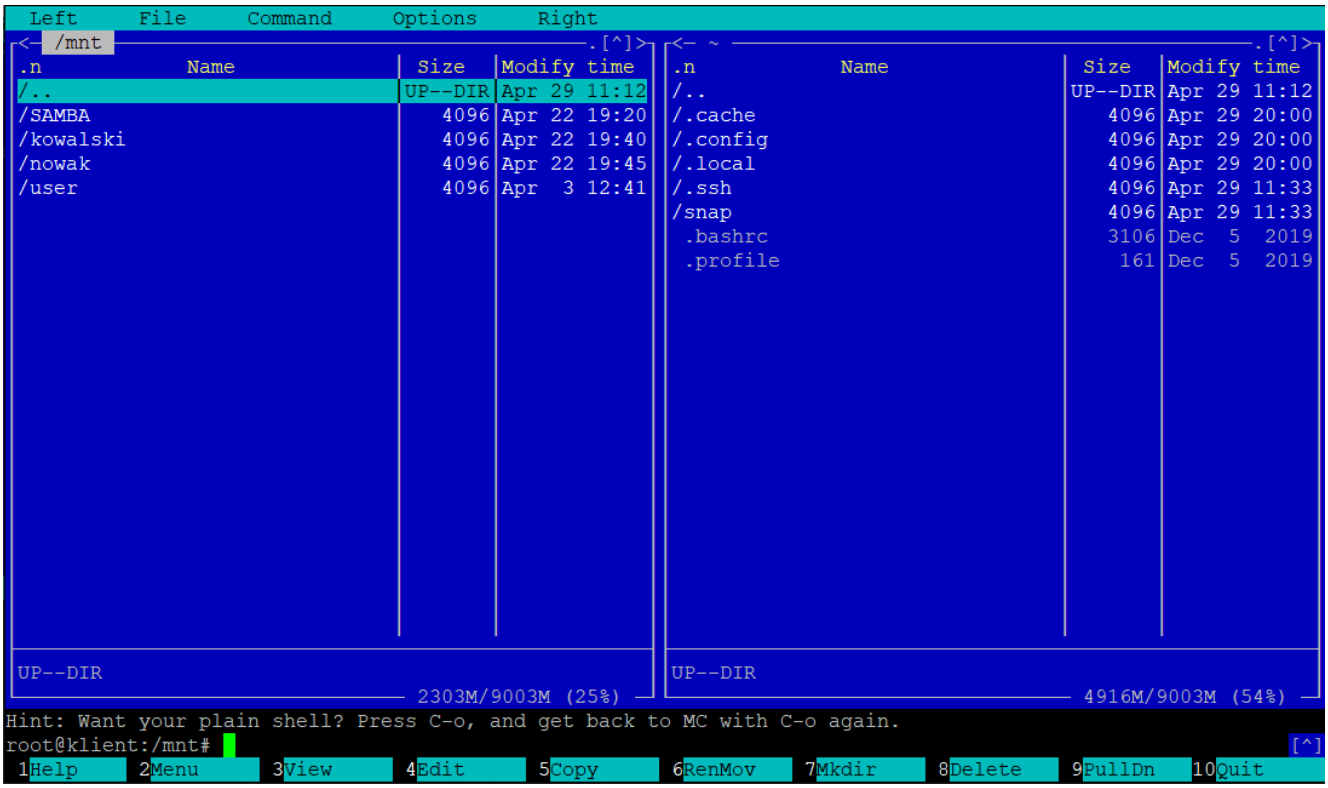
```
192.168.99.124:/home on /mnt type nfs4 (rw,relatime,vers=4.2,rsize=131072,wsize=131072,namlen=255,hard,proto=tcp,timeo=600,retrans=2,sec=sys,clientaddr=192.168.99.120,local_lock=none,addr=192.168.99.124)
```

lub używając polecenia **df -h** także możesz potwierdzić poprawność

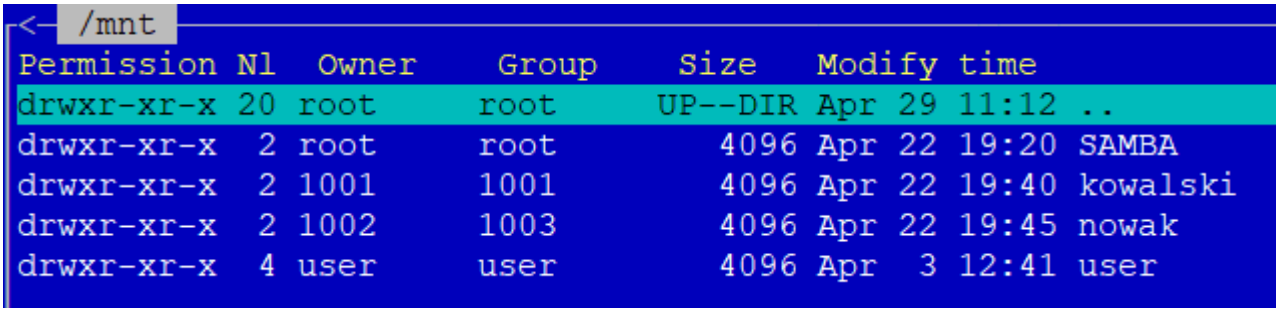
przyłączenia

```
root@klient:~# df -h
Filesystem                         Size  Used Avail Use% Mounted on
udev                               434M     0  434M   0% /dev
tmpfs                               96M  1.3M   95M   2% /run
/dev/mapper/ubuntu--vg-ubuntu--lv  8.8G  4.0G  4.4G  48% /
tmpfs                              477M     0  477M   0% /dev/shm
tmpfs                              5.0M     0  5.0M   0% /run/lock
tmpfs                              477M     0  477M   0% /sys/fs/cgroup
/dev/sda2                          976M  105M  805M  12% /boot
/dev/loop0                          70M   70M     0 100% /snap/lxd/19188
/dev/loop1                          32M   32M     0 100% /snap/snapd/10707
/dev/loop2                          56M   56M     0 100% /snap/core18/1944
tmpfs                               96M     0   96M   0% /run/user/1000
/dev/loop3                          56M   56M     0 100% /snap/core18/1997
/dev/loop4                          33M   33M     0 100% /snap/snapd/11588
/dev/loop5                          71M   71M     0 100% /snap/lxd/19647
192.168.99.124:/home               8.8G  6.6G  1.8G  79% /mnt
```

po stronie klienta możesz zobaczyć zawartość folderu home z serwera NFS który został podłączony do folderu /mnt



Zauważyć możesz również że nie poprawnie wyświetlane są dane o właścicielach i grupach. Powodem problemu jest niezgodność baz danych o użytkownikach i grupach.



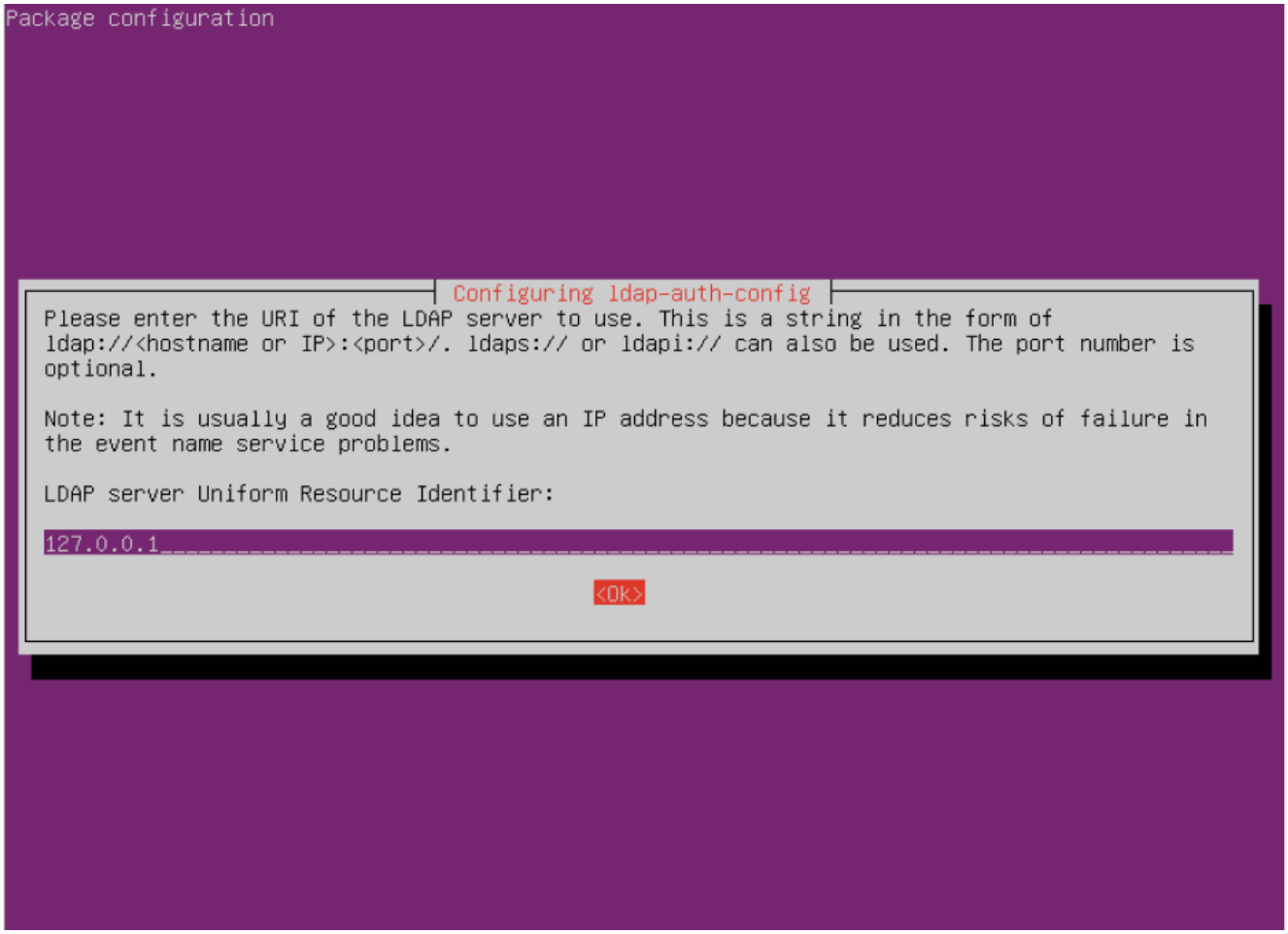
Aby to wyeliminować i doprowadzić do integralności danych należy uruchomić usługę integrującą w postaci usług katalogowych OpenLDAP

Podpięcie systemu do usługi OpenLDAP – operacja dla klienta

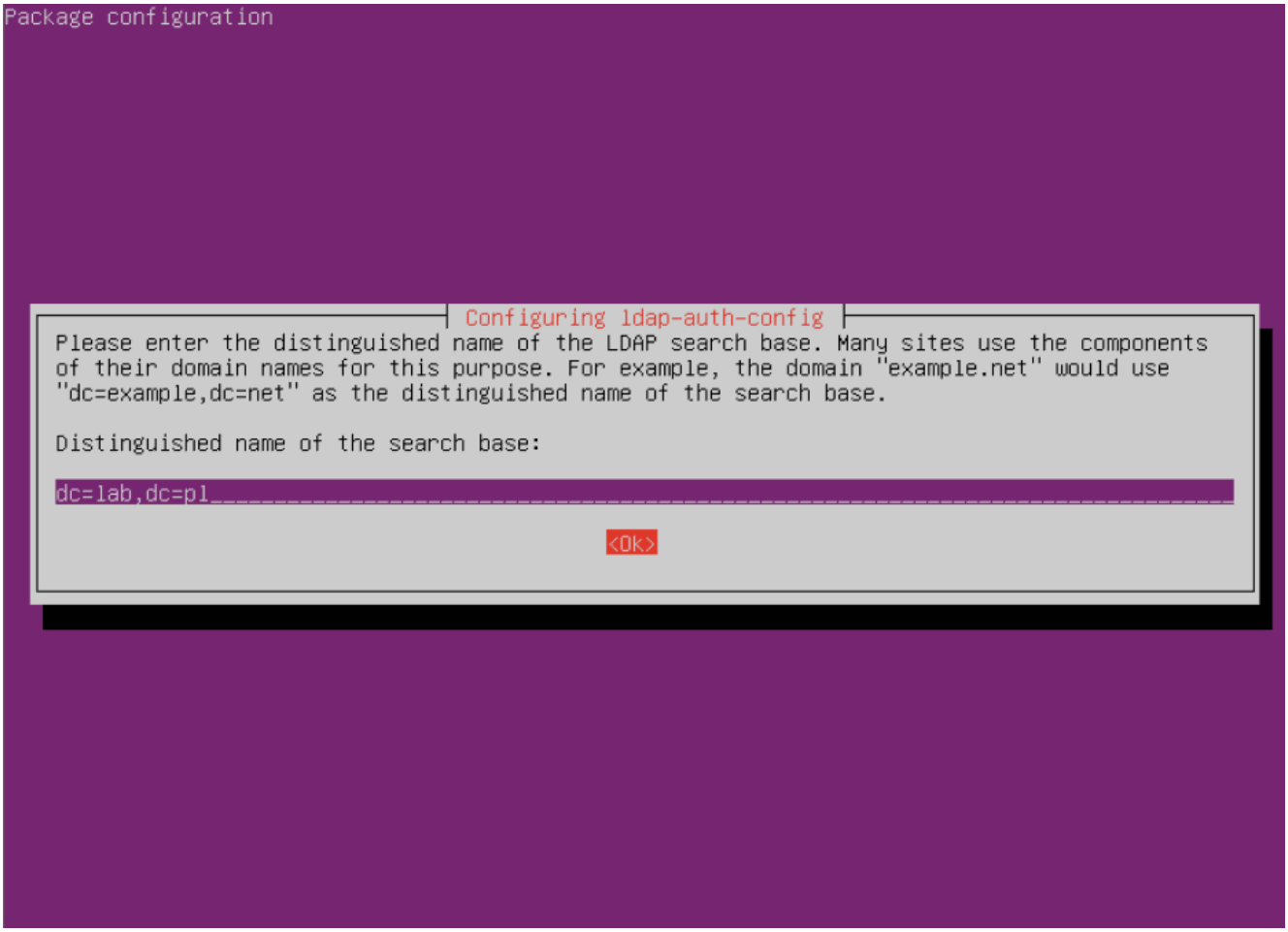
Uruchamiamy integrację systemu operacyjnego z LDAP. W tym celu musimy zainstalować dodatek rozszerzający możliwości systemu operacyjnego:

- „libnss-ldap”

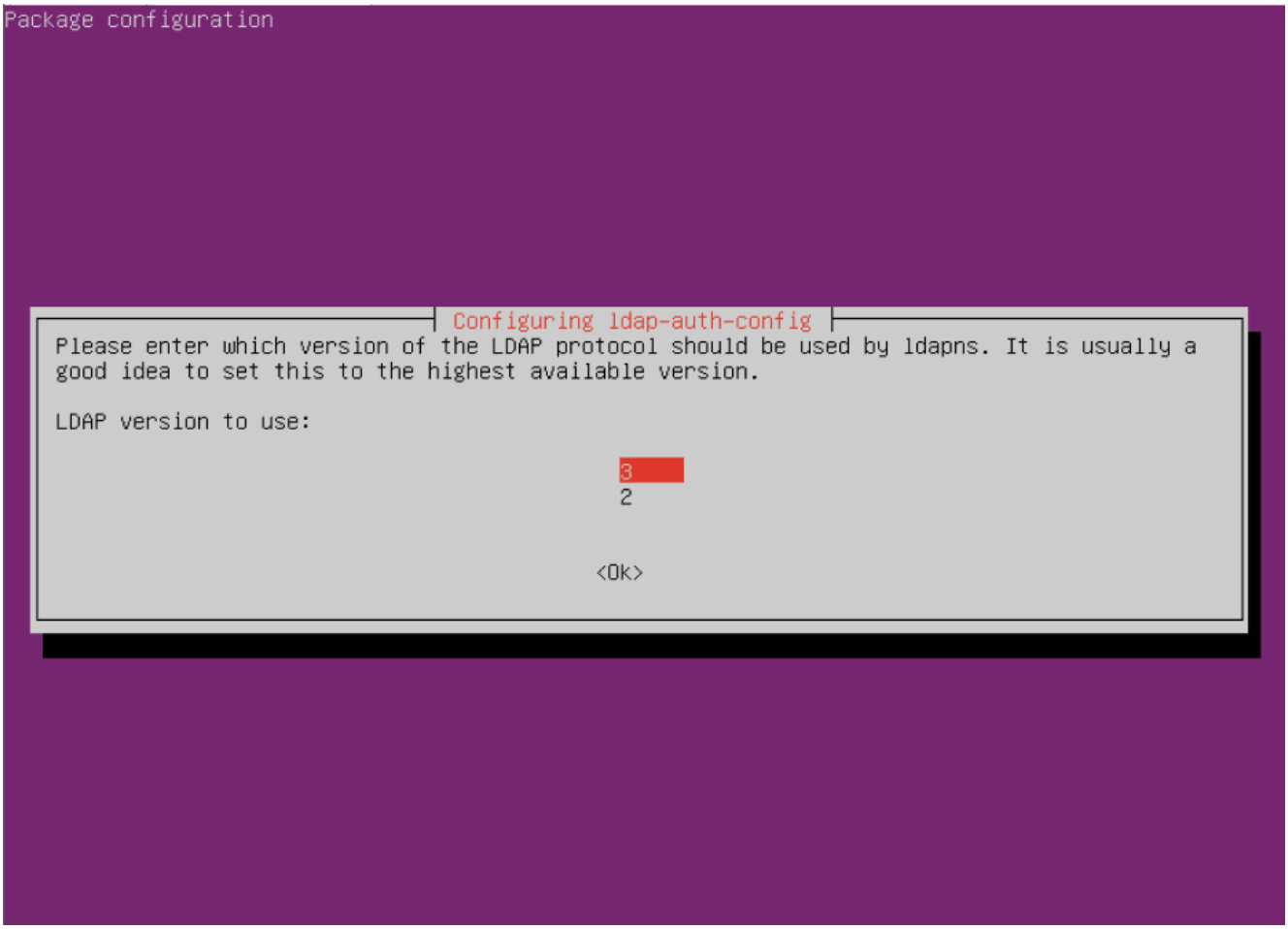
2. W trakcie instalacji system poprosi o podanie danych pozwalających na przyłączenie się do LDAP (**podaj wyłącznie w tej linii !!!!! : *adres IP serwera OpenLDAP* serwera**):



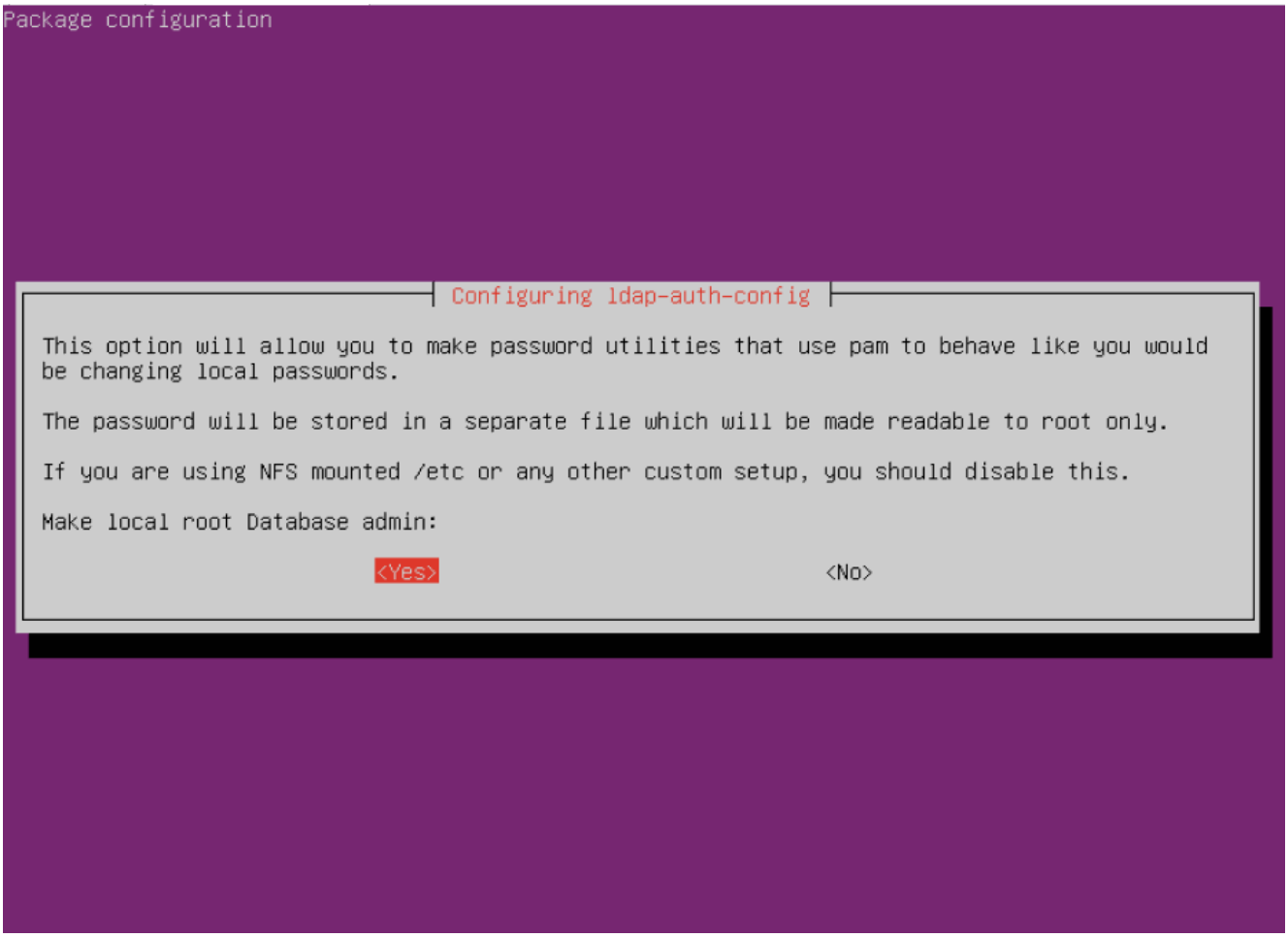
UWAGA! : zmieniona domena LDAP na: **dc=lab,dc=pl**



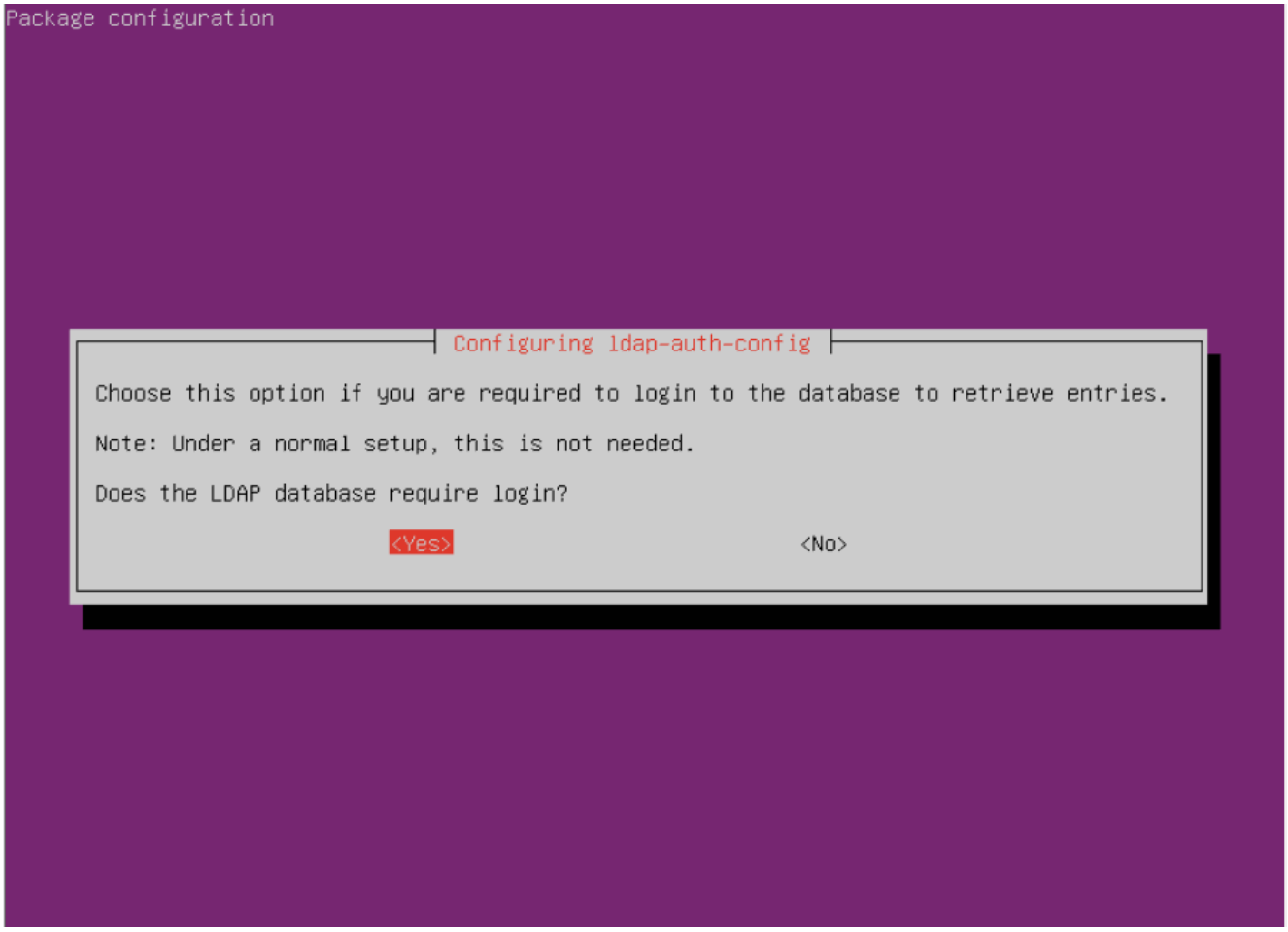
LDAP version: 3



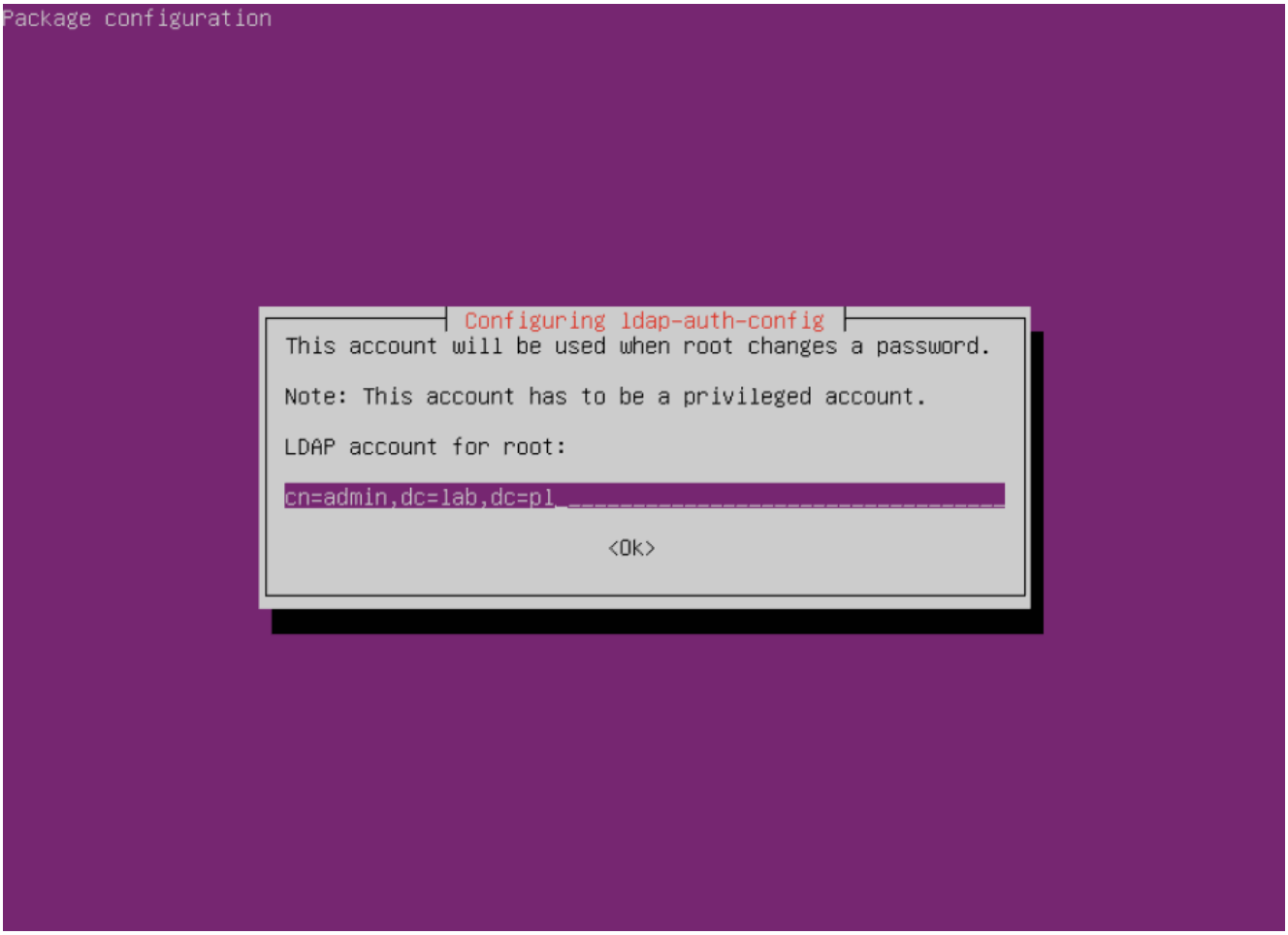
Ustawiamy konto root jako admina LDAP



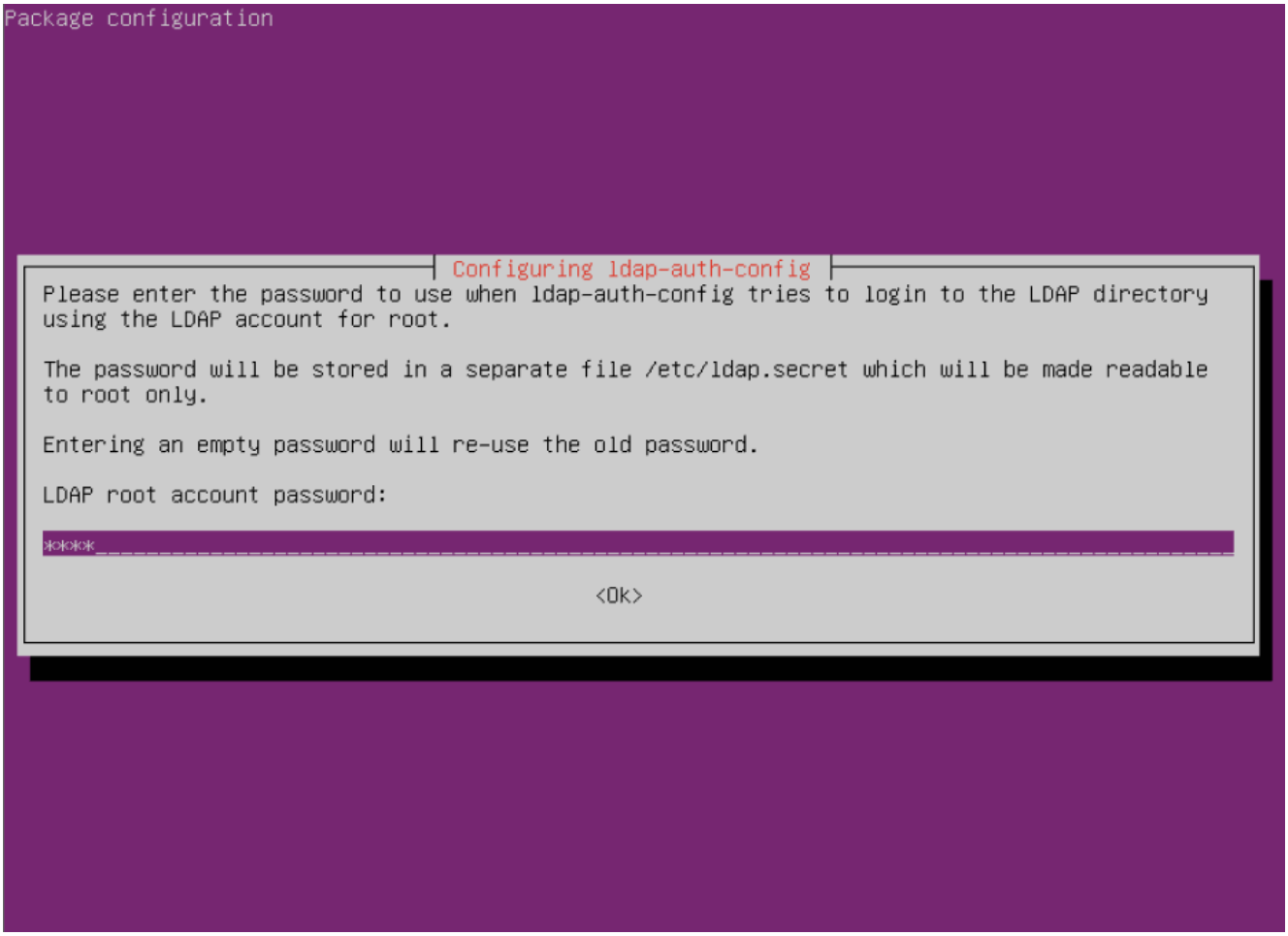
Włączamy wymaganie logowania do dostępu do bazy LDAP



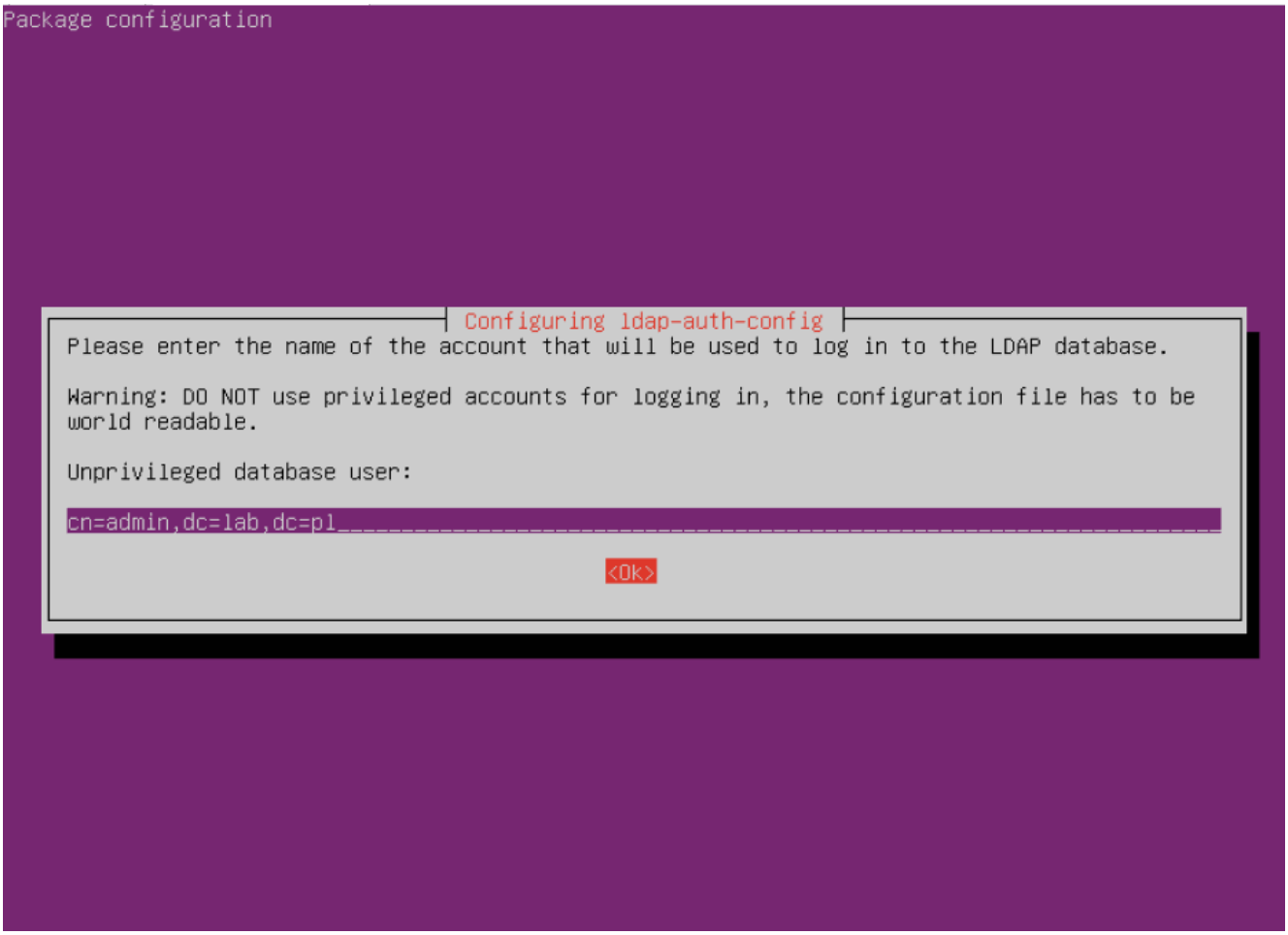
LDAP account for root: cn=admin,dc=lab,dc=pl



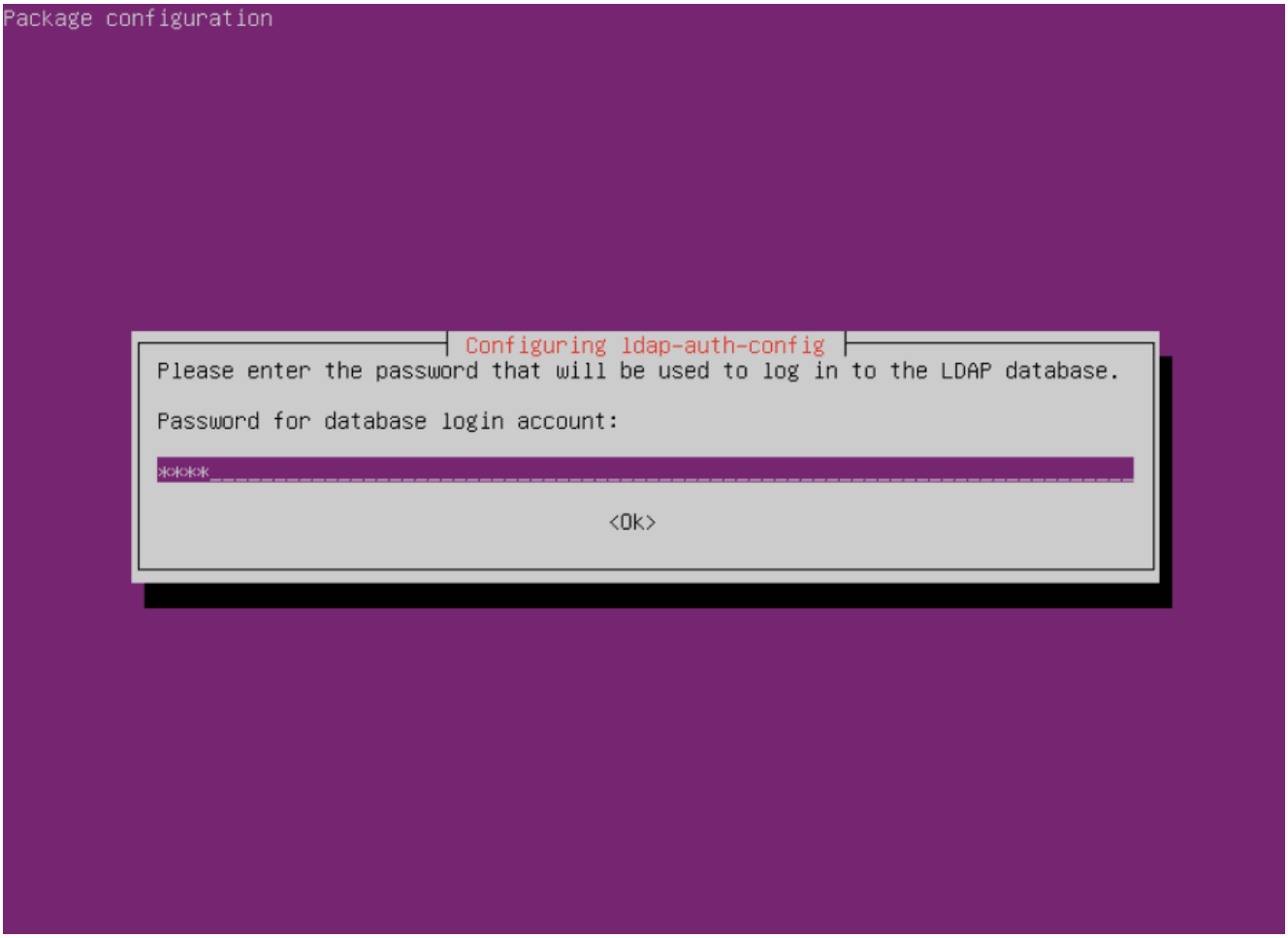
Podać właściwe hasło dla użytkownika ADMIN (podane w poprzednim laboratorium)



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
```

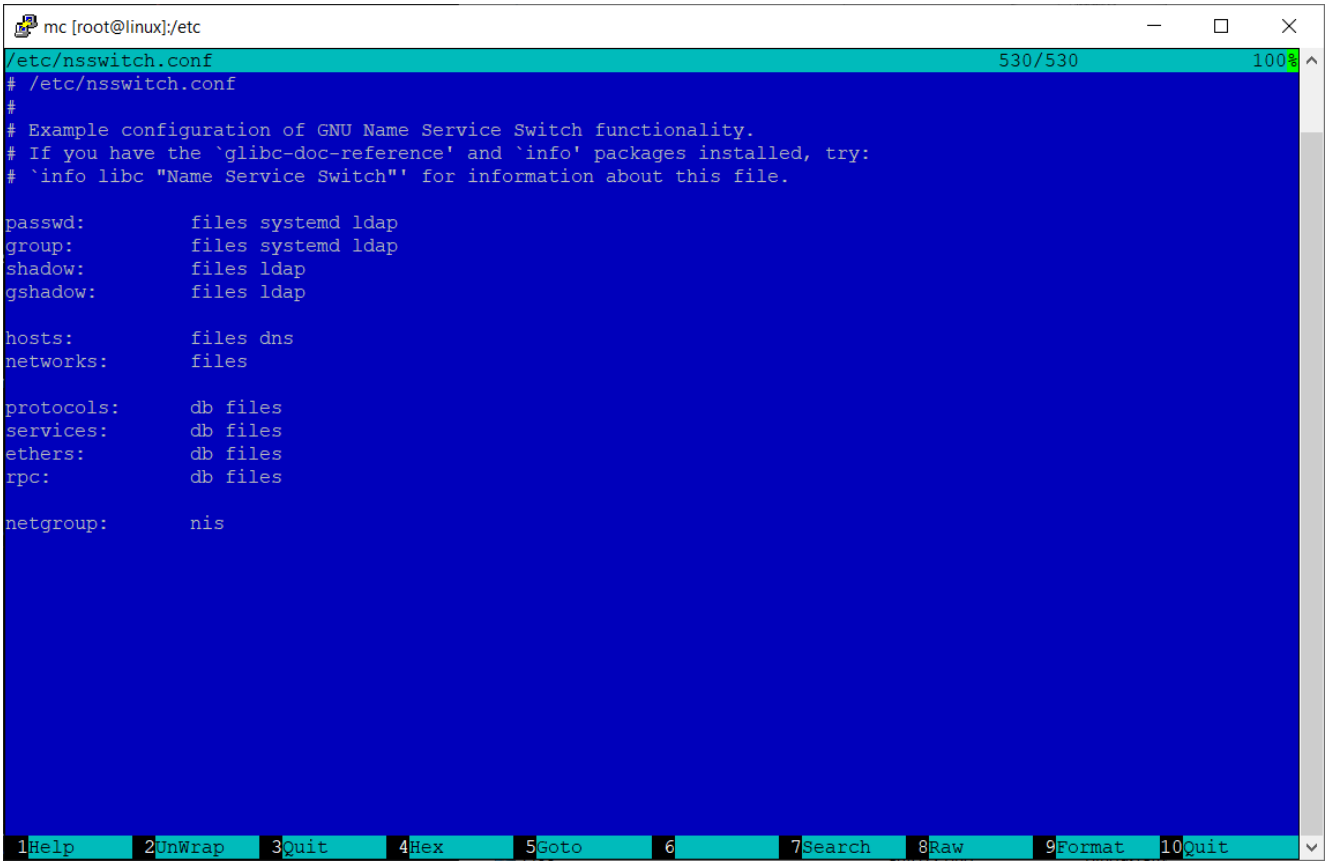
- Włączamy obsługę przesyłania jawnych haseł

```
#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



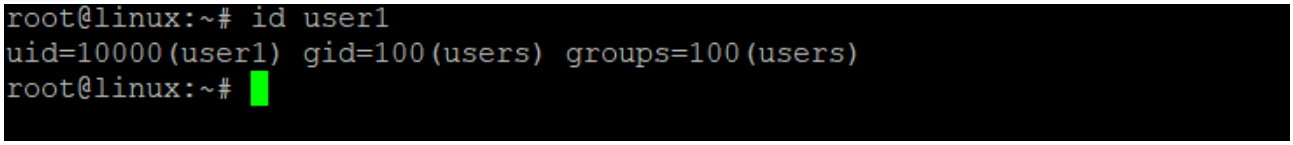
- Zapisujemy modyfikacje...

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)
```



Umożliwienie uwierzytelnienia do usługi OpenLDAP – operacja dla klienta

1. Zainstaluj pakiet „libpam-ldap”. Prawdopodobnie otrzymasz komunikat, że pakiet jest już zainstalowany. Został dołączony przy poprzednim laboratorium.

2. Następujące polecenia powinny być rozpoznawane prawidłowo w systemie:

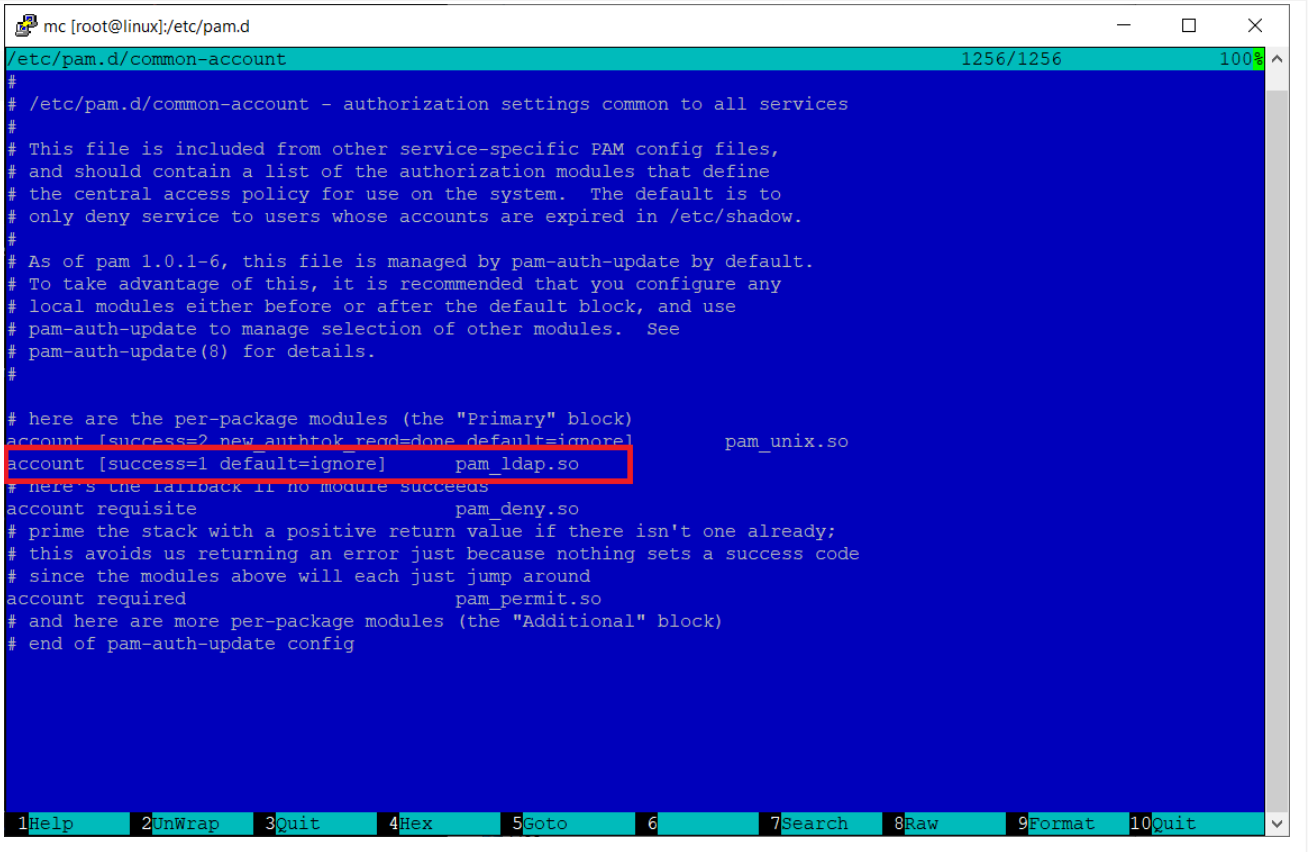
```
id user1
cd ~user1    (tylko po ponownym zalogowaniu się do putty)
```

3. System PAM wykorzystuje ten sam plik konfiguracji („/etc/ldap.conf”) jak libnss-LDAP. System automatycznie również skonfiguruje dostęp w systemie PAM wewnątrz katalogu /etc/pam.d należy jedynie sprawdzić poprawność wpisów.

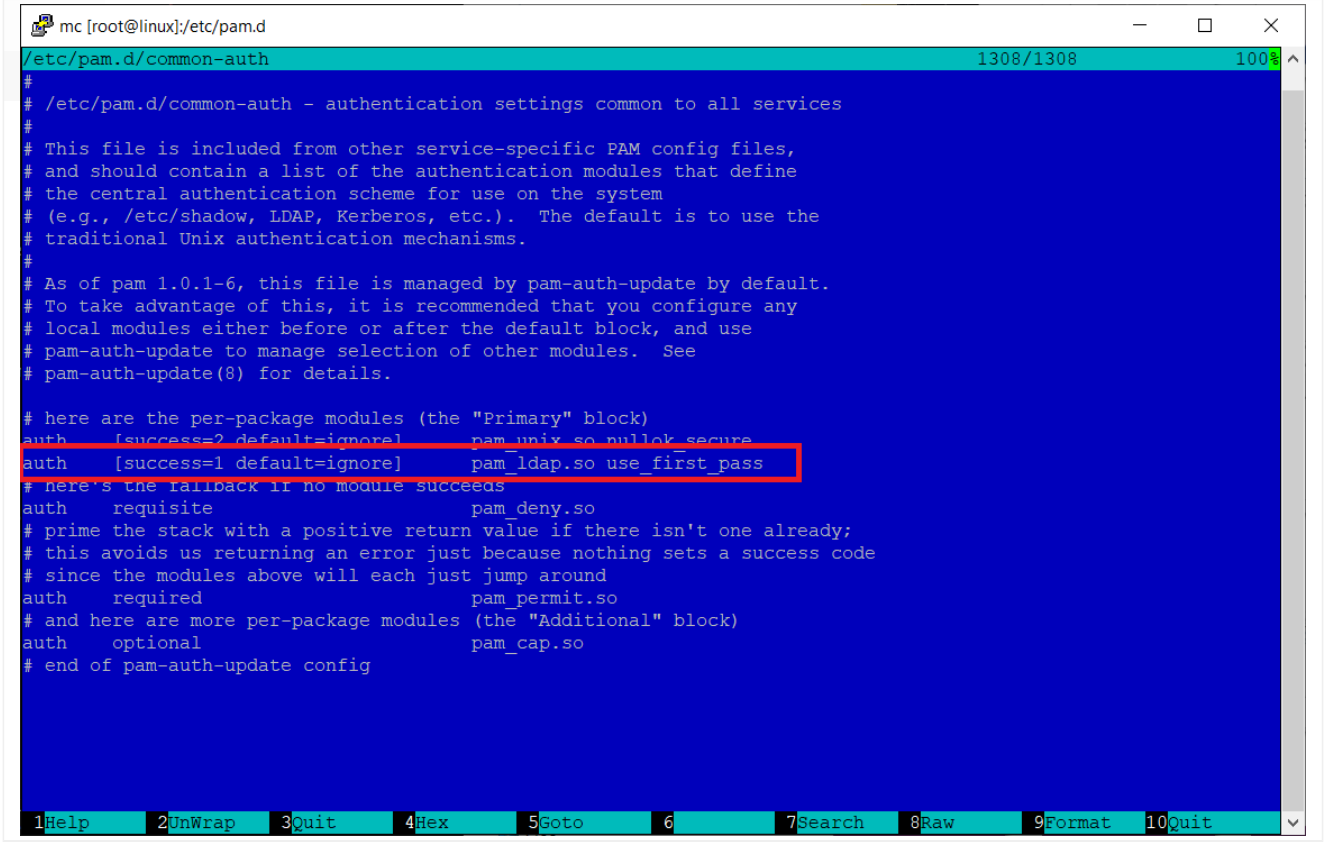
NIE WOLNO NIC ZMIENIAĆ – tylko sprawdzić !!!!!!!!!!!! czy występują w każdym pliku pozycje na czerwono !!! Jeśli tak o wszystko OK.

4. Prawidłowa postać wszystkich wpisów:

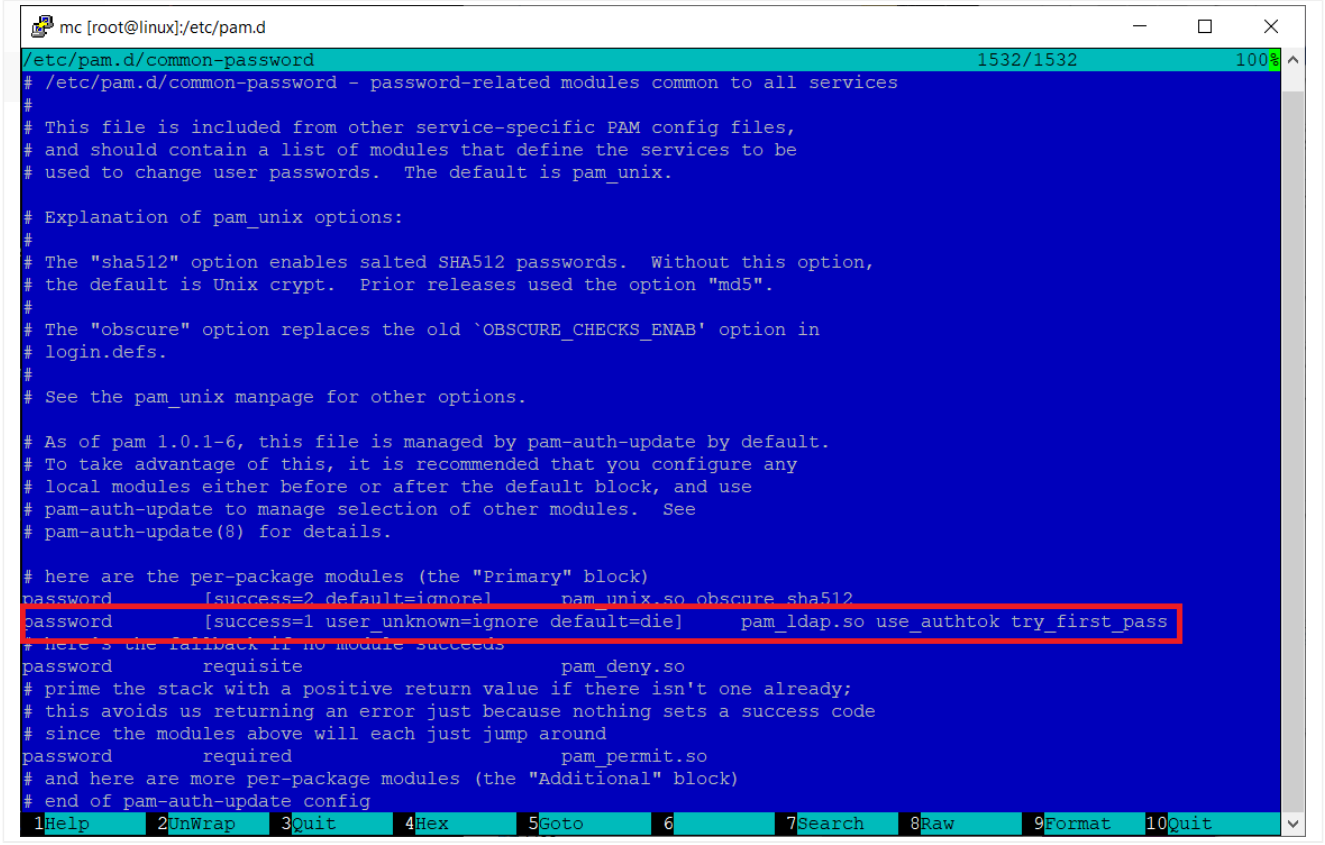
common-account:



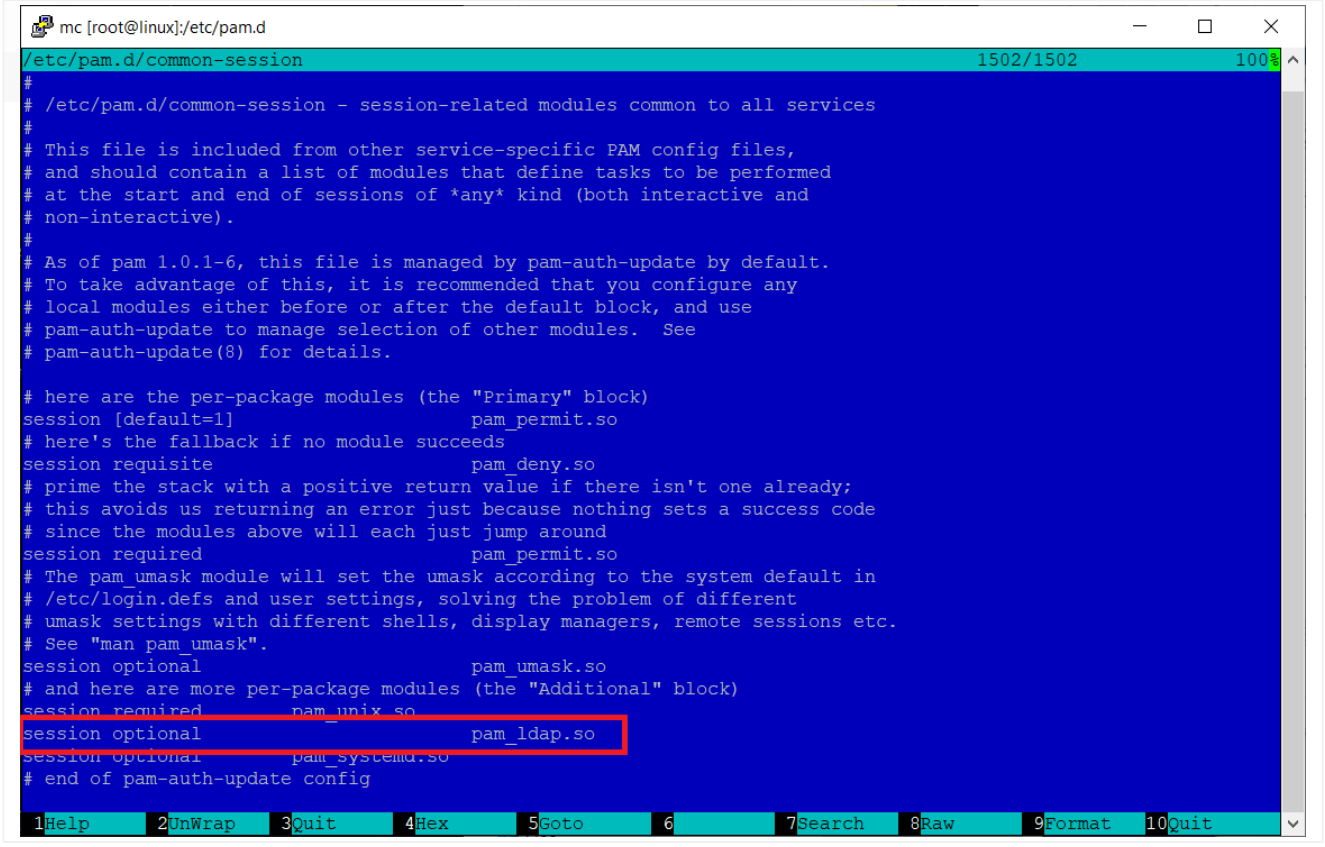
common-auth:



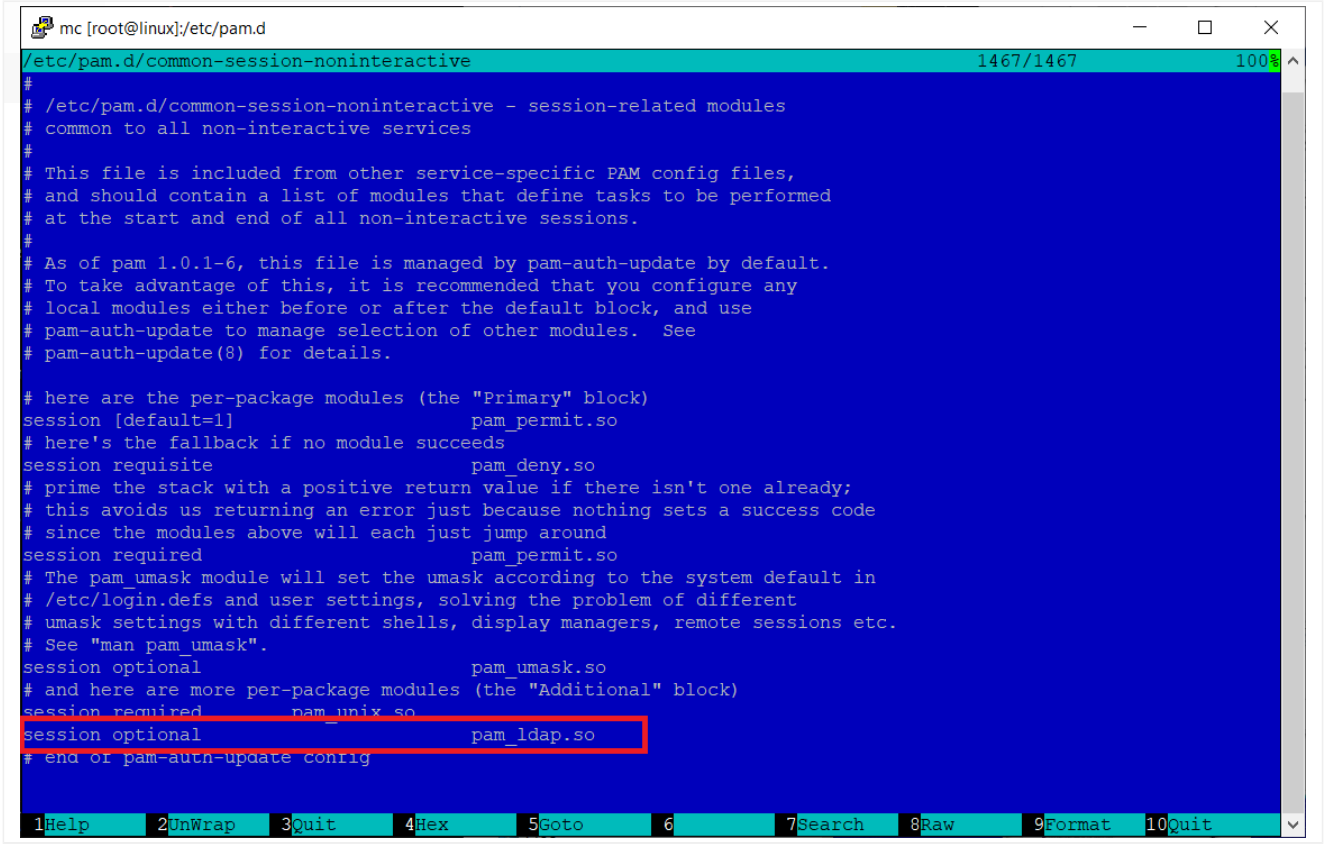
common-password:



common-session:



common-session-noninteractive:



5. Prawidłowo wykonane wpisy po zrestartowaniu usługi SSH powinny pozwolić na zalogowanie się przy pomocy użytkownika z LDAP do systemu.

restart: **service ssh restart**

6. Połączenie wykonujemy przez kolejną sesję SSH (nowa sesja) i logowaniu się użytkownikiem i hasłem z LDAP

7. Sprawdź folder z zamontowanym udziałem NFS, gdzie teraz powinny być widoczne nazwy obiektów a nie ich identyfikatory cyfrowe