

Środowisko wielo-serwerowe linux

written by archi | 29 kwietnia 2021

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 20.04 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-kernel-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

```
Left      File      Command  Options  Right
<- /mnt  .[.]>    <- ~     .[.]>
.n        Name      Size     Modify time  .n        Name      Size     Modify time
/..      UP--DIR   4096    Apr 29 11:12 /..      UP--DIR   4096    Apr 29 11:12
/SAMBAs  4096     Apr 22 19:20 /..cache 4096     Apr 29 20:00
/kowalski 4096     Apr 22 19:40 /..config 4096     Apr 29 20:00
/nowak    4096     Apr 22 19:45 /..local  4096     Apr 29 20:00
/user     4096     Apr  3 12:41 /..ssh   4096     Apr 29 11:33
          /snap    4096     Apr 29 11:33
          .bashrc  3106    Dec  5 2019
          .profile  161     Dec  5 2019

UP--DIR 2303M/9003M (25%)  UP--DIR 4916M/9003M (54%)

Hint: Want your plain shell? Press C-o, and get back to MC with C-o again.
root@klient:/mnt#
```

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

Permission	Nl	Owner	Group	Size	Modify	time	
drwxr-xr-x	20	root	root	UP--DIR	Apr 29	11:12	..
drwxr-xr-x	2	root	root	4096	Apr 22	19:20	SAMBA
drwxr-xr-x	2	1001	1001	4096	Apr 22	19:40	kowalski
drwxr-xr-x	2	1002	1003	4096	Apr 22	19:45	nowak
drwxr-xr-x	4	user	user	4096	Apr 3	12:41	user

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

Uruchomienie usługi OpenLDAP WYŁĄCZNIE po stronie serwera usługi NFS

- Zainstaluj pakiety:
 - „slapd” (zapyta o hasło dla administratora LDAP)
 - „ldap-utils”
- Poniżej wykonaj:
 - wykonaj „dpkg-reconfigure slapd”
 - Ekran 1 : NIE
 - Ekran 2 : zamień domenę „nodomain” na „lab.pl”
 - Ekran 3 : zamień „nodomain” na „lab.pl”
 - Ekran 4 : Podaj hasło administratora bazy LDAP
 - Ekran 5 : Powtórz hasło
 - Ekran 6 : „Remove old ...” : NIE
 - Ekran 7 : „Move old data” : TAK
- Instalacja SLAPD w folderze /etc/ldap poprawiamy zawartość pliku ldap.conf uzupełniając BASE i URI właściwymi informacjami (*zauważ do czego służy znak „#”*):
 - BASE dc=lab,dc=pl
 - URI ldap://localhost

4. Ze strony <http://jxplorer.org/> pobrać JXplorer w aktualnej wersji dla systemu Windows lub jeśli instalacja jest nie możliwa to pobierz zip ze strony google'a i rozpakuj go w katalogu, a następnie uruchom `jxplorer.bat`
5. Należy zainstalować JXplorer (Dla WI uruchom program dostępny na serwerze terminali windows - dysk H: folder jxplorer)
6. Konfiguracja połączenia:
 - Host: 192.168.203.xxx
 - Port: 389
 - Base DN: dc=lab,dc=pl
 - Level: User + Password
 - User DN: cn=admin,dc=lab,dc=pl
 - Password: *(hasło podane w czasie instalacji pakietu slapd)*

Open LDAP/DSML Connection

Host: 192.168.x.x Port: 389

Protocol: LDAP v3

Optional Values

Base DN: dc=lab,dc=pl

Read Only:

Security

Level: User + Password

User DN: cn=admin,dc=lab,dc=pl

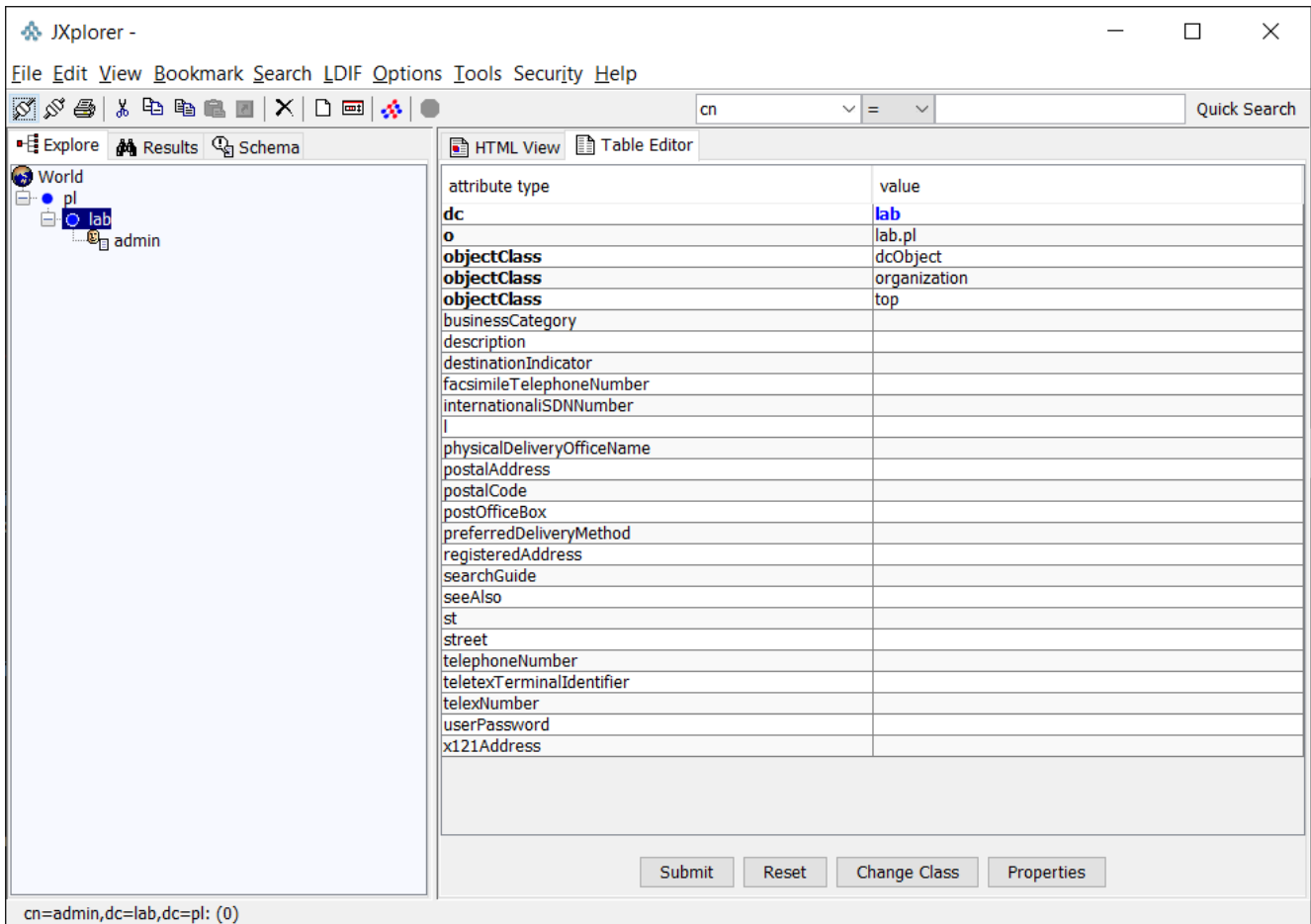
Password: ●●●●●

Use a Template

Save [] Delete Default

OK Cancel Help

7. Po wykonaniu połączenia będzie widoczne drzewo usługi z użytkownikiem admin



8. Tworzenie nowego użytkownika (na obiekcie kontener -> menu kontekstowe /prawy klawisz myszy/ -> New — wybieramy podane poniżej klasy):

- Nazwa: user1
- UIDNumber: 10000
- GIDNumber: 100
- HomeDirectory: /home/user1
- UID: user1
- Sn: jakieś nazwisko
- userPassword: u1
- Kasy obiektu LDAP: **Top, Person, PosixAccount, SimpleSecurityObject**

Set Entry Object Classes

Suggest Classes?

Parent DN:

Enter RDN:

Available Classes:	Selected Classes:
residentialPerson	top
RFC822localPart	person
room	posixAccount
shadowAccount	simpleSecurityObject
strongAuthenticationUser	

JXplorer -

File Edit View Bookmark Search LDAP Options Tools Security Help

cn = Quick Search

Explore Results Schema

World

- pl
 - lab
 - admin

Table Editor

attribute type	value
cn	user1
gidNumber	100
homeDirectory	/home/user1
objectClass	person
objectClass	posixAccount
objectClass	simpleSecurityObject
objectClass	top
sn	Nazwisko user1
uid	user1
uidNumber	10000
userPassword	(non string data)
description	
gecos	
loginShell	
seeAlso	
telephoneNumber	

cn=admin,dc=lab,dc=pl: (0)

9. Po zakończeniu tworzenia konta zatwierdzamy wprowadzone dane poprzez SUBMIT

10. Wracamy do konsoli PuTTY

11. Testujemy działanie komend ldapsearch

Wymagane parametry:

- -x
- -LLL

12. Wynikiem powinno być wyświetlenie całej zawartości drzewa LDAP

```
root@linux:~# ldapsearch -x -LLL
dn: dc=lab,dc=pl
objectClass: top
objectClass: dcObject
objectClass: organization
o: lab.pl
dc: lab

dn: cn=admin,dc=lab,dc=pl
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator

dn: cn=user1,dc=lab,dc=pl
cn: user1
gidNumber: 100
homeDirectory: /home/user1
objectClass: person
objectClass: posixAccount
objectClass: simpleSecurityObject
objectClass: top
sn: Nazwisko user1
uid: user1
uidNumber: 10000
```

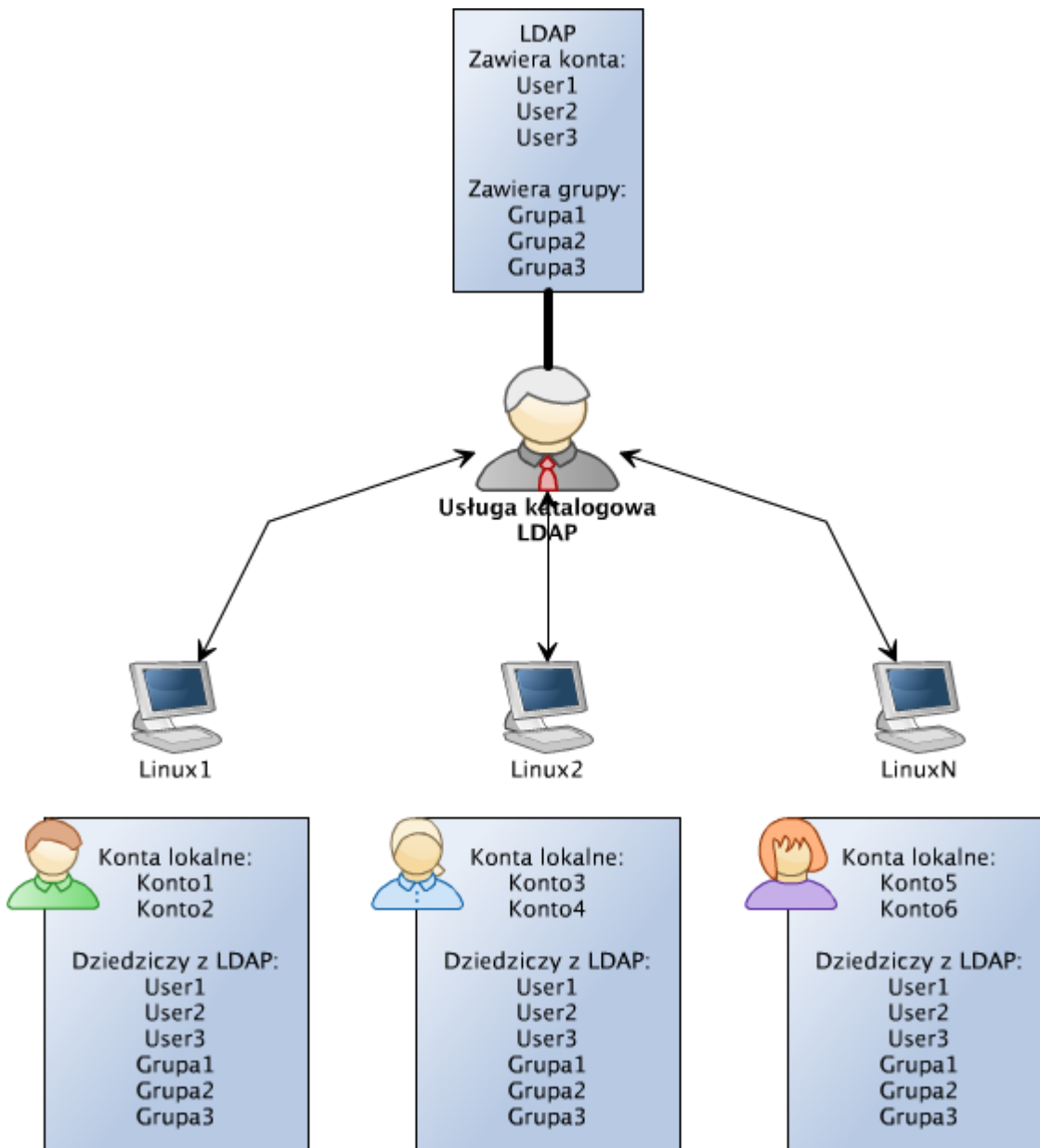
(jeśli masz błąd (32) to sprawdź wpisy w pkt 3.)

13. Tworzymy folder użytkownika user1 który będzie jego katalogiem domowym (/home/user1) i nadajemy uprawnienia do tego folderu tj.:

```
chown 10000:100 /home/user1
```

Przy wykorzystaniu LDAP uzyskać można wspólną bazę usług katalogowych

dla wielu serwerów



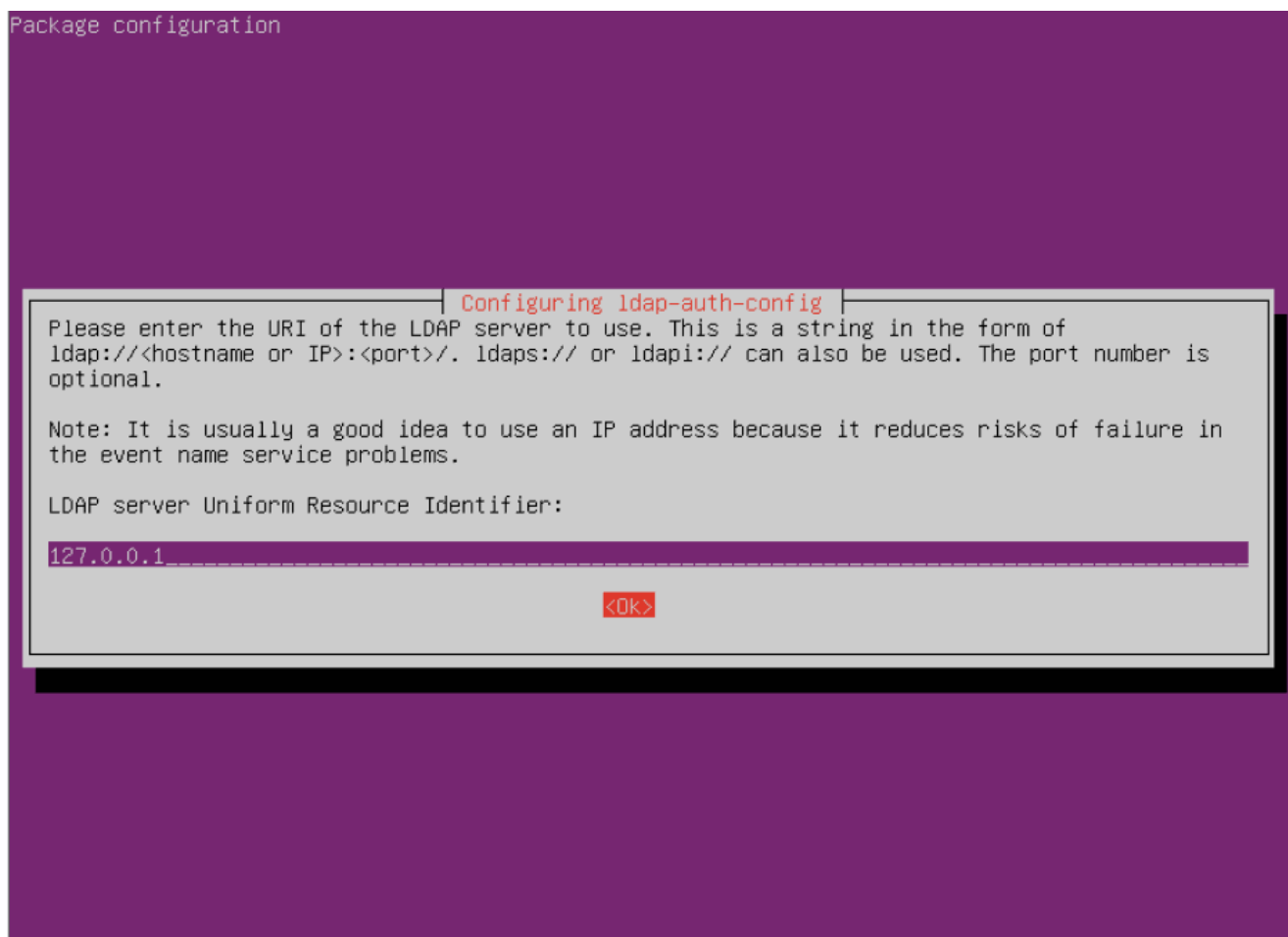
Podpięcie systemu do usługi OpenLDAP - operacja dla serwera i klienta

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 !!!!! : 127.0.0.1 dla serwera, a w przypadku uruchamiania na kliencie podaj adres IP serwera**):



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

Package configuration

Configuring ldap-auth-config

Please enter the distinguished name of the LDAP search base. Many sites use the components of their domain names for this purpose. For example, the domain "example.net" would use "dc=example,dc=net" as the distinguished name of the search base.

Distinguished name of the search base:

dc=lab,dc=pl

<Ok>

LDAP version: 3

Package configuration

Configuring ldap-auth-config

Please enter which version of the LDAP protocol should be used by ldapns. It is usually a good idea to set this to the highest available version.

LDAP version to use:

3
2

<Ok>

Ustawiamy konto root jako admina LDAP

Package configuration

Configuring ldap-auth-config

This option will allow you to make password utilities that use pam to behave like you would be changing local passwords.

The password will be stored in a separate file which will be made readable to root only.

If you are using NFS mounted /etc or any other custom setup, you should disable this.

Make local root Database admin:

<Yes>

<No>

Włączamy wymaganie logowania do dostępu do bazy LDAP

Package configuration

Configuring ldap-auth-config

Choose this option if you are required to login to the database to retrieve entries.

Note: Under a normal setup, this is not needed.

Does the LDAP database require login?

<Yes>

<No>

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

Package configuration

Configuring ldap-auth-config

This account will be used when root changes a password.

Note: This account has to be a privileged account.

LDAP account for root:

<Ok>

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

Package configuration

Configuring ldap-auth-config

Please enter the password to use when ldap-auth-config tries to login to the LDAP directory using the LDAP account for root.

The password will be stored in a separate file /etc/ldap.secret which will be made readable to root only.

Entering an empty password will re-use the old password.

LDAP root account password:

<OK>

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

Package configuration

Configuring ldap-auth-config

Please enter the name of the account that will be used to log in to the LDAP database.

Warning: DO NOT use privileged accounts for logging in, the configuration file has to be world readable.

Unprivileged database user:

cn=admin,dc=lab,dc=pl

<Ok>

Podać właściwe hasło (jak było wcześniej)

Package configuration

Configuring ldap-auth-config

Please enter the password that will be used to log in to the LDAP database.

Password for database login account:

<Ok>

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

- Przeszawiamy 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

```
mc [root@linux]:/etc
/etc/nsswitch.conf 530/530 100%
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the `glibc-doc-reference' and `info' packages installed, try:
# `info libc "Name Service Switch"' for information about this file.

passwd:      files systemd ldap
group:       files systemd ldap
shadow:     files ldap
gshadow:    files ldap

hosts:       files dns
networks:   files

protocols:  db files
services:   db files
ethers:     db files
rpc:        db files

netgroup:   nis
```

- 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)
```

```
root@linux:~# id user1
uid=10000(user1) gid=100(users) groups=100(users)
root@linux:~#
```

6. Powtarzamy powyższe czynności dla drugiej maszyny wirtualnej (klienta) -

[TUTAJ](#)

Umożliwienie uwierzytelnienia do usługi OpenLDAP - operacja dla serwera i 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:

```
mc [root@linux]:/etc/pam.d
/etc/pam.d/common-account 1256/1256 100%
#
# /etc/pam.d/common-account - authorization settings common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of the authorization modules that define
# the central access policy for use on the system. The default is to
# only deny service to users whose accounts are expired in /etc/shadow.
#
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules. See
# pam-auth-update(8) for details.
#
# here are the per-package modules (the "Primary" block)
account [success=2 new_authtok_reqd=done default=ignore] pam_unix.so
account [success=1 default=ignore] pam_ldap.so
# here's the fallback if no module succeeds
account requisite pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
account required pam_permit.so
# and here are more per-package modules (the "Additional" block)
# end of pam-auth-update config

1Help 2UnWrap 3Quit 4Hex 5Goto 6 7Search 8Raw 9Format 10Quit
```

common-auth:

```
mc [root@linux]:/etc/pam.d
/etc/pam.d/common-auth 1308/1308 100%
#
# /etc/pam.d/common-auth - authentication settings common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of the authentication modules that define
# the central authentication scheme for use on the system
# (e.g., /etc/shadow, LDAP, Kerberos, etc.). The default is to use the
# traditional Unix authentication mechanisms.
#
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules. See
# pam-auth-update(8) for details.
#
# here are the per-package modules (the "Primary" block)
auth [success=2 default=ignore] pam_unix.so nullok_secure
auth [success=1 default=ignore] pam_ldap.so use_first_pass
# here's the fallback if no module succeeds
auth requisite pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
auth required pam_permit.so
# and here are more per-package modules (the "Additional" block)
auth optional pam_cap.so
# end of pam-auth-update config

1Help 2UnWrap 3Quit 4Hex 5Goto 6 7Search 8Raw 9Format 10Quit
```

common-password:


```
mc [root@linux]:/etc/pam.d
/etc/pam.d/common-password 1532/1532 100%
# /etc/pam.d/common-password - password-related modules common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of modules that define the services to be
# used to change user passwords. The default is pam_unix.
#
# Explanation of pam_unix options:
#
# The "sha512" option enables salted SHA512 passwords. Without this option,
# the default is Unix crypt. Prior releases used the option "md5".
#
# The "obscure" option replaces the old `OBSOLETE_CHECKS_ENAB' option in
# login.defs.
#
# See the pam_unix manpage for other options.
#
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules. See
# pam-auth-update(8) for details.
#
# here are the per-package modules (the "Primary" block)
password [success=2 default=ignore pam_unix.so obscure sha512
password [success=1 user unknown=ignore default=die] pam_ldap.so use_authok try_first_pass
# here's the fallback if no module succeeds
password requisite pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
password required pam_permit.so
# and here are more per-package modules (the "Additional" block)
# end of pam-auth-update config
1Help 2UnWrap 3Quit 4Hex 5Goto 6 7Search 8Raw 9Format 10Quit
```

common-session:

```
mc [root@linux]:/etc/pam.d
/etc/pam.d/common-session 1502/1502 100%
#
# /etc/pam.d/common-session - session-related modules common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of modules that define tasks to be performed
# at the start and end of sessions of *any* kind (both interactive and
# non-interactive).
#
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules. See
# pam-auth-update(8) for details.
#
# here are the per-package modules (the "Primary" block)
session [default=1] pam_permit.so
# here's the fallback if no module succeeds
session requisite pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
session required pam_permit.so
# The pam_umask module will set the umask according to the system default in
# /etc/login.defs and user settings, solving the problem of different
# umask settings with different shells, display managers, remote sessions etc.
# See "man pam_umask".
session optional pam_umask.so
# and here are more per-package modules (the "Additional" block)
session required pam_unix.so
session optional pam_ldap.so
session optional pam_systemd.so
# end of pam-auth-update config
1Help 2UnWrap 3Quit 4Hex 5Goto 6 7Search 8Raw 9Format 10Quit
```

common-session-noninteractive:

```
mc [root@linux]:/etc/pam.d
/etc/pam.d/common-session-noninteractive 1467/1467 100%
#
# /etc/pam.d/common-session-noninteractive - session-related modules
# common to all non-interactive services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of modules that define tasks to be performed
# at the start and end of all non-interactive sessions.
#
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules. See
# pam-auth-update(8) for details.
#
# here are the per-package modules (the "Primary" block)
session [default=1]          pam_permit.so
# here's the fallback if no module succeeds
session requisite           pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
session required            pam_permit.so
# The pam_umask module will set the umask according to the system default in
# /etc/login.defs and user settings, solving the problem of different
# umask settings with different shells, display managers, remote sessions etc.
# See "man pam_umask".
session optional            pam_umask.so
# and here are more per-package modules (the "Additional" block)
session required            pam_unix.so
session optional            pam_ldap.so
# end of pam-auth-update config

1Help 2UnWrap 3Quit 4Hex 5Goto 6 7Search 8Raw 9Format 10Quit
```

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. Powtarzamy czynność umożliwienia uwierzytelnienia na maszynie wirtualnej klienta - [TUTAJ](#)

Test kompetencji

Do wykonania testu niezbędne jest uzyskanie oceny z poprzedniego 3-ciego testu dostępnego na tej samej platformie

<https://e-edukacja.zut.edu.pl/course/view.php?id=976>

Link do testu: <https://e-edukacja.zut.edu.pl/mod/quiz/view.php?id=23071>

