# 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 **nfscommon**. 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-kernelserver**. 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



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

Zapisz konfigurację i zrestartuj usługę nfs-kernet-server



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



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

=600,retrans=2,sec=sys,clie

192.168.99.124:/home on /mnt type nfs4 (rw,relatime,ver ddr=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	0응	/dev
tmpfs	96M	1.3M	95M	2%	/run
/dev/mapper/ubuntuvg-ubuntulv	8.8G	<b>4.</b> 0G	<b>4.4</b> G	48%	/
tmpfs	477M	0	477M	0응	/dev/shm
tmpfs	5.0M	0	5.0M	0응	/run/lock
tmpfs	477M	0	477M	0응	/sys/fs/cgroup
/dev/sda2	976M	105M	805M	12%	/boot
/dev/loop0	70M	70M	0	100%	/snap/1xd/19188
/dev/loop1	32M	32M	0	100%	/snap/snapd/10707
/dev/loop2	56M	56M	0	100%	/snap/core18/1944
tmpfs	96M	0	96M	0응	/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/1xd/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	5						
<pre>/mnt .n / /SAMBA /kowalski /nowak /user</pre>	Name		Size UP-DIR 4096 4096 4096 4096	Modify t Apr 22 1 Apr 22 1 Apr 22 1 Apr 22 1 Apr 3 1	.[^]>- cime 1:12 L9:20 L9:40 L9:45 L2:41	<pre>.n / /.cache /.config /.local /.ssh /snap .bashrc .profile</pre>	Name		Size UPDIR 4096 4096 4096 3106 161	Modify Apr 29 Apr 29 Apr 29 Apr 29 Dec 5 Dec 5	[^]≻ time 11:12 20:00 20:00 20:00 11:33 11:33 2019 2019
UPDIR			- 2303M/9	9003M (25	5%)	UPDIR			4916M/9	9003 <b>m (</b> !	54%)
Hint: Want y root@klient	your pla: :/mnt#	in shell? Pre	ss C−o, a	and get k	back to	MC with C-	o again.				[^]
1Help	2 <mark>M</mark> enu	3 <mark>View</mark>	4 <mark>Edit</mark>	5 <mark>Copy</mark>	7	6RenMov	7 <mark>Mkdir</mark>	8 <mark>Delete</mark>	9 <mark>PullDn</mark>	10Qu:	it

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

-<- /mnt							
/ mire	_			- •			
Permission	N1	Owner	Group	Size	Modify	time	
drwxr-xr-x	20	root	root	UPDIR	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

## 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**):

ackage configuration
Configuring ldap-auth-config
Please enter the URI of the LDAP server to use. This is a string in the form of ldap:// <hostname ip="" or="">:<port>/. ldaps:// or ldapi:// can also be used. The port number is optional.</port></hostname>
Note: It is usually a good idea to use an IP address because it reduces risks of failure in the event name service problems.
LDAP server Uniform Resource Identifier:
127.0.0.1
< <u>Ck&gt;</u>

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

ackage 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
KOKS

LDAP version: 3

ackage 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:
2
<0k>

Ustawiamy konto root jako admina LDAP



Włączamy wymaganie logowania do dostępu do bazy LDAP

	Configuring 1	dap-auth-config	
Choose this option	if you are required to	login to the database to retrieve	e entries.
Note: Under a norm	al setup, this is not ne	eeded.	
Does the LDAP data	base require login?		
	<yes></yes>	<no></no>	

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



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

ackage 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:
xoloick
<0k>

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

ckage 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
KOK>

Podać właściwe hasło (jak było wcześniej)

ge con	figuration
ſ	Configuring ldap-auth-config
	Please enter the password that will be used to log in to the LDAP database. Password for database login account:
	<0k>

- 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)
```

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

## Umożliwienie uwierzytelnienia do usługi OpenLDAP - operacja dla klienta

 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:

P mc [root@linux]:/etc/pam.d	-		×
/etc/bam.d/common-bassword 1532/1532			100 <mark>%</mark> ^
<pre># /etc/pam.d/common-password - password-related modules common to all services #</pre>			
# 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.			
<pre># Explanation of pam_unix options: #</pre>			
<pre># The "sha512" option enables salted SHA512 passwords. Without this option, # the default is Unix crypt. Prior releases used the option "md5". #</pre>			
<pre># The "obscure" option replaces the old `OBSCURE_CHECKS_ENAB' option in # login.defs. #</pre>			
# See the pam_unix manpage for other options.			
<pre># 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.</pre>			
<pre># here are the per-package modules (the "Primary" block) password [success=2 default=ignore] pam unix so obscure sha512</pre>			
password [success=1 user unknown=ignore default=die] pam ldap.so use authtok try fir:	st pass		
riere's che faitback if no moutre success	_		
password requisite pam_deny.so			
<pre># prime the stack with a positive return value if there isn't one already;</pre>			
this avoids us returning an error just because nothing sets a success code			
# since the modules above will each just jump around			
# and here are more per-package modules (the "Additional" block)			
# end of pam-auth-update config			
1Help 2UnWrap 3Quit 4Hex 5Goto 6 7Search 8Raw 9Forma	it <mark>10</mark> Qi	it	~

## common-session:

Pmc [root@linux]:/etc/pam.d		- 1	⊐ ×
/etc/pam.d/common-session	1502/1502		100 <mark>%</mark> ^
<pre># # /etc/pam.d/common-session - session-related modules common to all services #</pre>			
<pre># 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).</pre>			
<pre># # 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.</pre>			
<pre># here are the per-package modules (the "Primary" block) session [default=1] pam_permit.so # here's the fallback if no module succeeds</pre>			
<pre># since is requisite</pre>			
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.			
<pre># Seemain_pam_umask . session optional pam_umask.so # and here are more per-package modules (the "Additional" block) session required</pre>			
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	: <mark>10</mark> Qui	t v

## common-session-noninteractive:

🛃 mc [root@linux]:/etc/pam.d							—		×
/etc/pam.d/common-session-no	ninteractive				14	467/1467			100 <mark>%</mark> ^
# # /etc/pam.d/common-session- # common to all non-interact #	noninteractiv ive services	re – session-re	elated mod	ules					
This file is included from and should contain a list at the start and end of al	other servic of modules th l non-interac	ce-specific PAN hat define task ctive sessions.	4 config f ks to be p	iles, erformed					
<pre># As of pam 1.0.1-6, this fi # To take advantage of this, # local modules either befor # pam-auth-update to manage # pam-auth-update(8) for det</pre>	le is managed it is recomm e or after th selection of ails.	d by pam-auth-u mended that you me default bloc other modules.	update by 1 configur ck, and us . See	default. e any e					
<pre># here are the per-package m session [default=1] # here's the fallback if no</pre>	odules (the " p module succee	'Primary" bloc} pam_permit.so eds	k)						
session requisite # prime the stack with a pos # this avoids us returning a # since the modules above wi	p itive return n error just ll each just	oam_deny.so value if there because nothir jump around	e isn't on ng sets a	e already; success code					
session required # The pam_umask module will # /etc/login.defs and user s # umask settings with differ	p set the umask ettings, solv ent shells, d	pam_permit.so according to ving the proble display manager	the syste em of diff rs, remote	m default in erent sessions etc					
# See "man pam_umask". session optional # and here are more per-pack	p age modules (	oam_umask.so (the "Additiona	al" block)						
session optional	p	am ldap.so							
# ena or pam-autn-upaate con	IIG								
1Help 2UnWrap 3Ouit	4Hex	5 <mark>G</mark> oto	6	7 Search	8Raw	9 Format	10	Ouit	

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