

# Autoryzacja 2

written by archi | 16 października 2019



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)
```

1. 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.**
2. 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
```

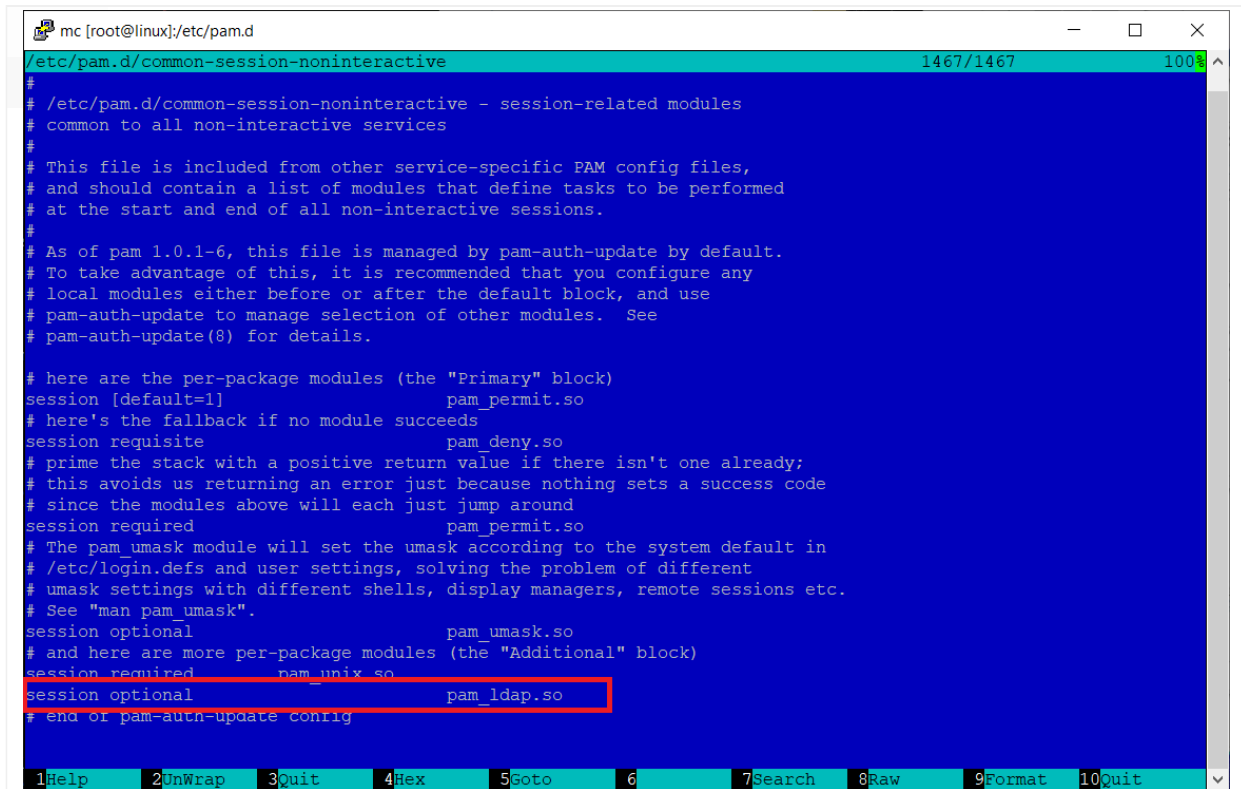
- common-password:

```
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_authtok try_first_pass
# here's the fallback if no module succeeds
password requisite pam_permit.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_permit.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_denial.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
```

3. Prawidłowo wykonane wpisy po zrestartowaniu usługi SSH powinny pozwolić na zalogowanie się przy pomocy użytkownika z LDAP do systemu.  
restart: **service ssh restart**
4. Połączenie wykonujemy przez kolejną sesję SSH (nowa sesja) i logowaniu się użytkownikiem i hasłem z LDAP. Znak zachęty jest bez przypisanego shella. Dlatego też w dalszej części rozszerzymy schemat LDAPa, przy okazji konfigurując narzędzie graficzne LDAP Account Manager.
5. Poniżej zrzuty ekranu z konfiguracją

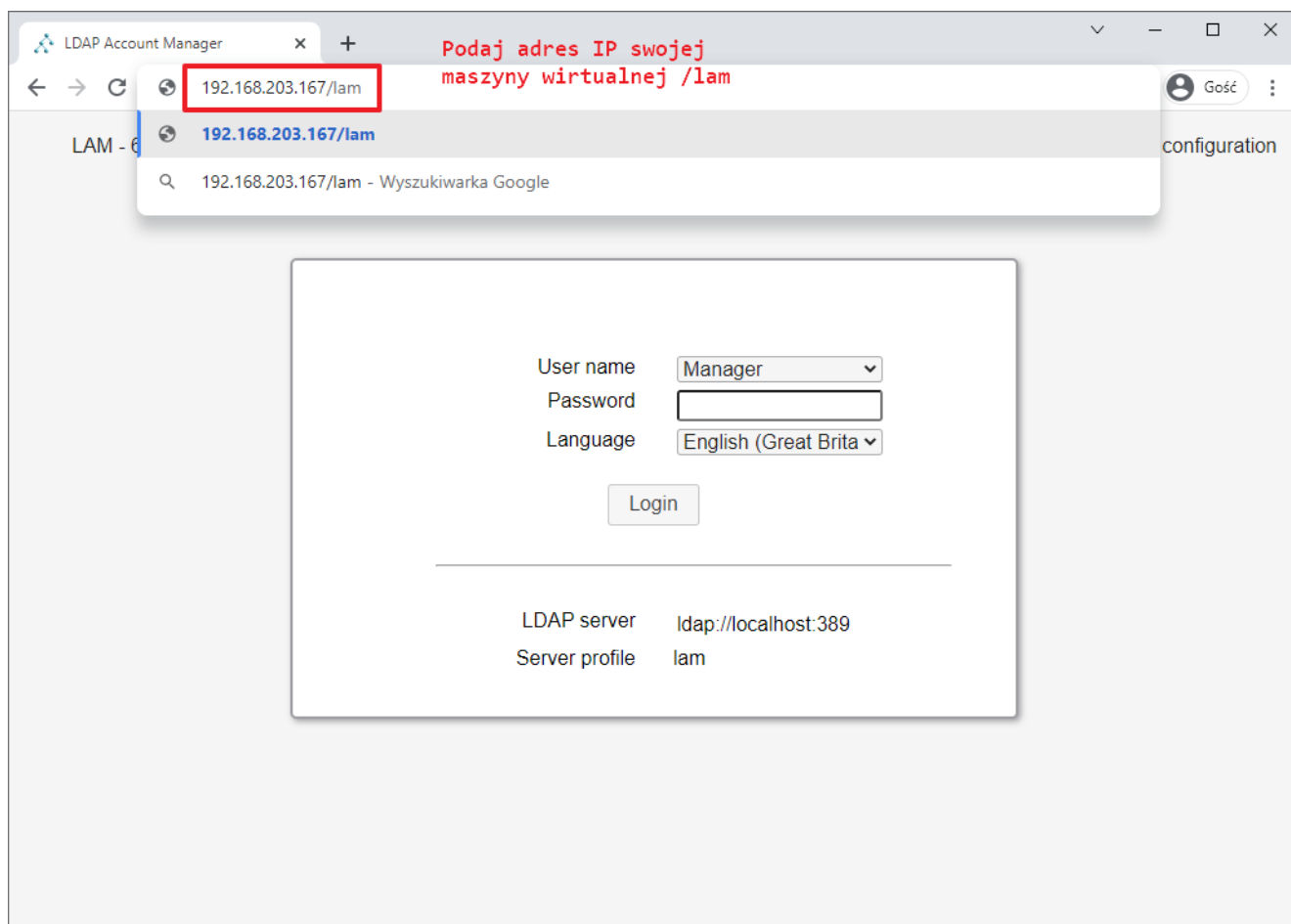
---

Pobierz za pośrednictwem wget pakiet aktualnej wersji LAM  
([https://gsliwinski.wi.zut.edu.pl/sieci/ldap-account-manager\\_7.7-1\\_all.deb](https://gsliwinski.wi.zut.edu.pl/sieci/ldap-account-manager_7.7-1_all.deb))

Z wykorzystaniem polecenia **dpkg -i ldap-account-manager\_7.7-1\_all.deb** rozpocznij proces instalacji – zakończy się błędem zależności

Napraw ten stan poleceniem **apt install -f**

Otwórz w przeglądarce witrynę LAM poprzez swój adres IP maszyny VM dodając przyrostek /lam

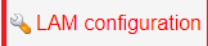


LDAP Account Manager x +

192.168.203.167/lam

LAM - 6.7

Want more features? Get LAM Pro!

 LAM configuration

User name

Password

Language

---

LDAP server ldap://localhost:389


Server profile lam


192.168.203.167/lam/templates/config/index.php

Configuration overview x +

Niezabezpieczona | 192.168.203.167/lam/templates/config/index.php

LDAP Account Manager

 [Edit general settings](#)

 Edit server profiles

[Back to login](#)

192.168.203.167/lam/templates/config/mainlogin.php

Login x +

Niezabezpieczona | 192.168.203.167/lam/templates/config/mainlogin.php

Gość

### LDAP Account Manager

Please enter the master password to change the general preferences:

Master password

**Pierwsze hasło lam**

[Back to login](#)

Edit general settings x +

Niezabezpieczona | 192.168.203.167/lam/templates/config/mainmanage.php

Gość

Minimum character classes

Number of rules that must match

Password must not contain user name

Password must not contain part of user/first/last name

External password check

#### Logging

Log level

Log destination

PHP error reporting

#### Change master password

New master password

Reenter password

**Ustaw własne hasło**

LDAP Account Manager x +

Niezabezpieczona | 192.168.203.167/lam/templates/login.php?confMainSavedOk=1

LAM - 6.7 Want more features? Get LAM Pro! [LAM configuration](#)

**Your settings were successfully saved.**

User name

Password

Language

---


LDAP server ldap://localhost:389  
Server profile lam


192.168.203.167/lam/templates/config/index.php

Configuration overview x +

Niezabezpieczona | 192.168.203.167/lam/templates/config/index.php

LDAP Account Manager

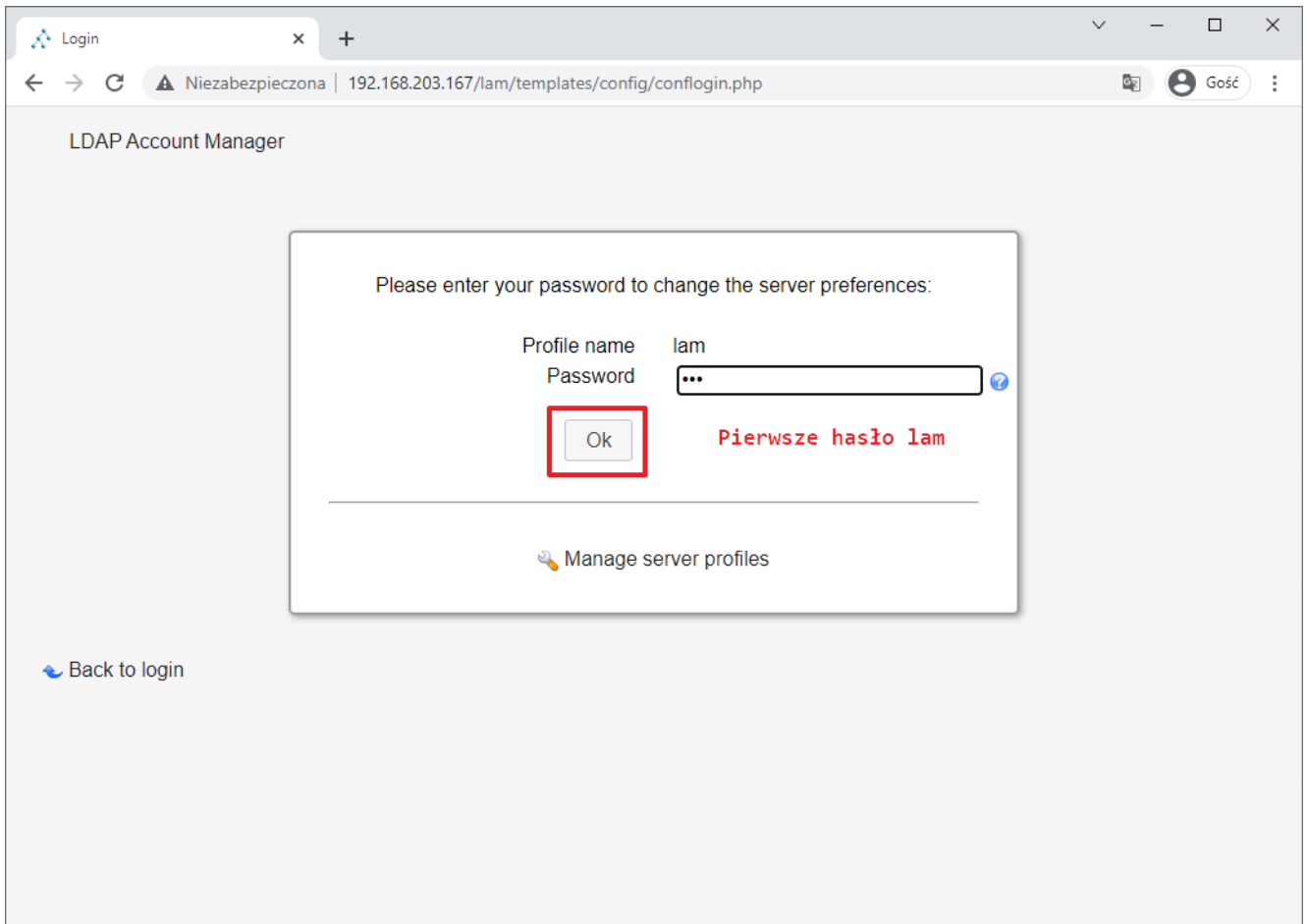
 Edit general settings

 **Edit server profiles**

[Back to login](#)

192.168.203.167/lam/templates/config/conflogin.php





Tu możesz zostaw adres LOCALHOST zamiast adresu IP ldap://localhost:389 ,  
„Tree suffix” jest trochę niżej w tym okienku.

LDAP Account Manager Configur x +

Niezabezpieczona | 192.168.203.167/lam/templates/config/confmain.php

Gość

LDAP Account Manager Server profile: lam

General settings Account types Modules Module settings

### Server settings

Server address \* ldap://192.168.203.167:389

Activate TLS no

Tree suffix dc=lab,dc=pl

LDAP search limit -

Advanced options

### Language settings

Default language English (Great Britain)

Time zone Europe/London

### Lamdaemon settings

Server list

OU editor  Profile editor  Server information

PDF editor  LDAP import/export  File upload

### Security settings

Login method Fixed list

List of valid users \* cn=admin,dc=lab,dc=pl

### 2-factor authentication

Provider None

### Profile password

New password .....

Reenter password .....

Ustaw własne hasło

Save Cancel

LDAP Account Manager x +

Niezabezpieczona | 192.168.203.167/lam/templates/login.php?configSaveOk=1&configSaveFile=lam

LAM - 6.7 Want more features? Get LAM Pro! [LAM configuration](#)

**Your settings were successfully saved.**  
lam

User name: admin  
Password:   
Language: English (Great Brita)

Login

LDAP server: ldap://192.168.203.167:389  
Server profile: lam

192.168.203.167/lam/templates/config/index.php

Configuration overview x +

Niezabezpieczona | 192.168.203.167/lam/templates/config/index.php

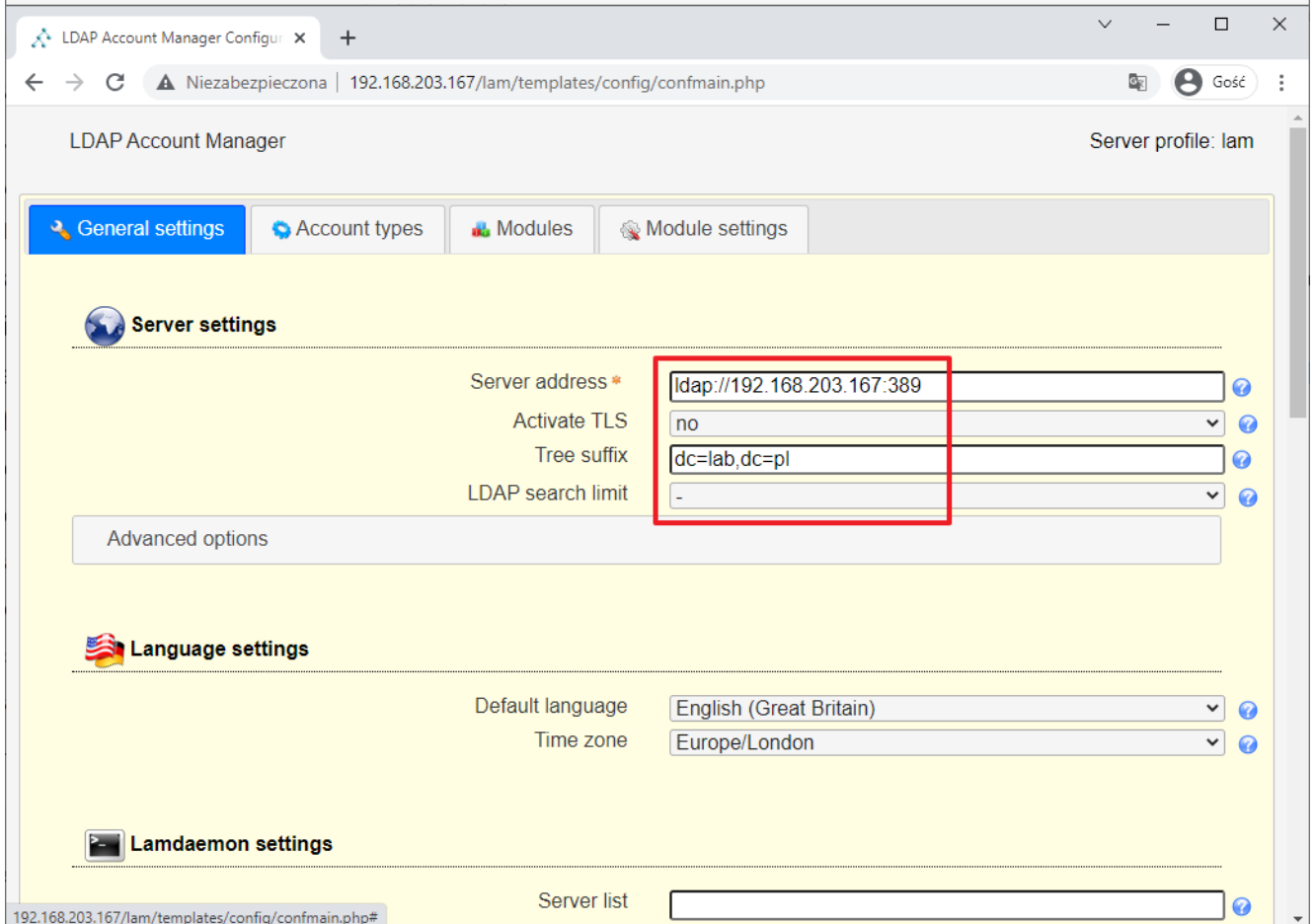
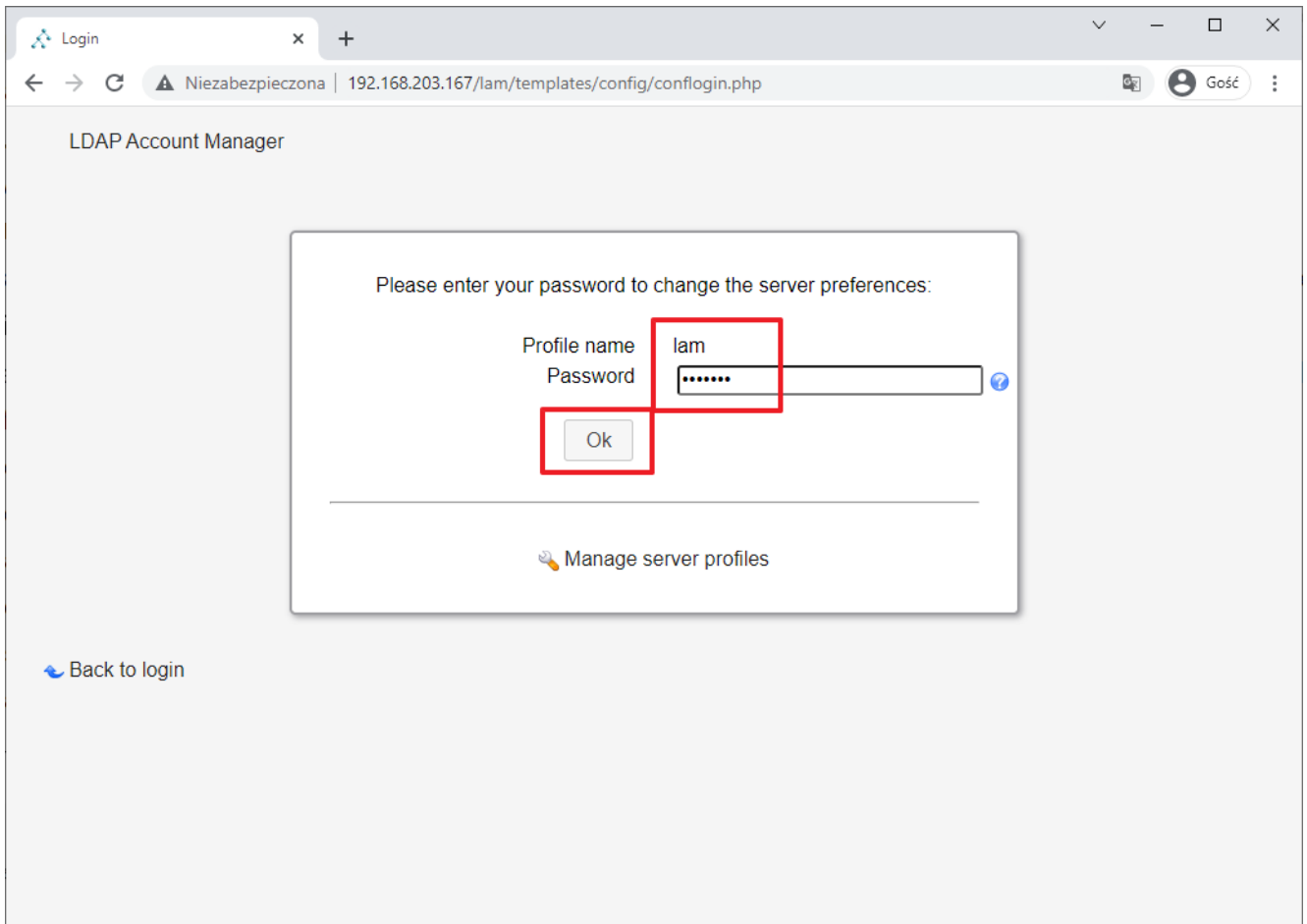
LDAP Account Manager

[Edit general settings](#)

[Edit server profiles](#)

[Back to login](#)

192.168.203.167/lam/templates/config/conflogin.php



W zakładce „Account types” ustaw

LDAP Account Manager Configur x +

Niezabezpieczona | 192.168.203.167/lam/templates/config/conftypes.php

Gość

### Users

User accounts (e.g. Unix, Samba and Kolab)

**Active account types**

**Users**

User accounts (e.g. Unix, Samba and Kolab) ↓ ×

LDAP suffix: dc=lab,dc=pl

List attributes: #uid,#givenName,#sn,#uidNumber,#gidNumber

Custom label:

Additional LDAP filter:

Hidden:

**Groups**

Group accounts (e.g. Unix and Samba) ↑ ×

LDAP suffix: dc=lab,dc=pl

List attributes: #cn,#gidNumber,#memberUID,#description

Custom label:

Additional LDAP filter:

Hidden:

**Save** Cancel

LDAP Account Manager x +

Niezabezpieczona | 192.168.203.167/lam/templates/login.php?configSaveOk=1&configSaveFile=lam

Gość

LAM - 6.7 Want more features? Get LAM Pro! LAM configuration

**Your settings were successfully saved.**

lam

User name: admin

Password: .....

Language: English (Great Brita)

**Login**

LDAP server: ldap://192.168.203.167:389

Server profile: lam

LDAP Account Manager (192.168.203.167) x +

Niezabezpieczona | 192.168.203.167/lam/templates/lists/list.php?type=user

Gość

LDAP Account Manager - 6.7 (Logged in as: admin) Tree view Tools Help Logout

Users Groups

New user Delete selected users File upload

User count: 6

Actions	User name	First name	Last name	UID number	GID number
Sort sequence					
<input type="checkbox"/> Filter	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	adamnowak		Nowak	10008	100
<input type="checkbox"/>	anowak		Nowak	10006	100
<input type="checkbox"/>	mkwiatkowski		Kwiatkowski	10007	100
<input type="checkbox"/>	user1		Kowalski	10002	100

192.168.203.167/lam/templates/lists/list.php?type=group

LDAP Account Manager (192.168.203.167) x +

Niezabezpieczona | 192.168.203.167/lam/templates/lists/list.php?type=group

Gość

LDAP Account Manager - 6.7 (Logged in as: admin) Tree view Tools Help Logout

Users Groups

New group File upload

Group count: 0

Actions	Group name	GID number	Group members	Group description
Sort sequence				
<input type="checkbox"/> Filter	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

LDAP Account Manager (192.168.203.167) x +

Niezabezpieczona | 192.168.203.167/lam/templates/account/edit.php?type=group&suffix=dc=lab,dc=pl

Gość

LDAP Account Manager - 6.7 (Logged in as: admin) Tree view Tools Help Logout

Users Groups

Save Set password default Load profile

### New group

Suffixlab > pl RDN identifiercn

Unix

Group name \* marketing

GID number 11001

Description

Group members Edit members

LDAP Account Manager (192.168.203.167) x +

Niezabezpieczona | 192.168.203.167/lam/templates/account/edit.php

Gość

LDAP Account Manager - 6.7 (Logged in as: admin) Tree view Tools Help Logout

Users Groups

**LDAP operation successful.**  
Account was created successfully.

Create another group Create PDF file Back to group list Edit again

LDAP Account Manager (192.168.203.167) x +

Niezabezpieczona | 192.168.203.167/lam/templates/lists/list.php?type=user

Gość

LDAP Account Manager - 6.7 (Logged in as: admin) Tree view Tools Help Logout

Users Groups

New user Delete selected users

File upload

User count: 6

Wybierz dowolnego użytkownika, którego niedawno stworzyłeś

Actions	User name	First name	Last name	UID number	GID number
Sort sequence					
<input type="checkbox"/> Filter					
<input type="checkbox"/>	adamnowak		Nowak	10008	100
<input type="checkbox"/>	anowak		Nowak	10006	100
<input type="checkbox"/>	mkwiatkowski		Kwiatkowski	10007	100
<input type="checkbox"/>	user1		Kowalski	10002	100

192.168.203.167/lam/templates/account/edit.php?type=user&DN=%27cn%3Danowak%2Cdc%3Dlab%2Cdc%3Dpl%27

LDAP Account Manager (192.168.203.167) x +

Niezabezpieczona | 192.168.203.167/lam/templates/account/edit.php?type=user&DN=%27cn%3Danowak%2Cdc%3... Gość

Save Reset changes Set password default Load profile

anowak

Suffixlab > pl RDN identifier cn

Unix Shadow Personal

Invalid configuration detected. Please edit your server profile (module settings) and fill all required fields.

User name \* anowak

Common name anowak

UID number 10006

Gecos

Primary group marketing

Additional groups Edit groups

Home directory \* /home/anowak

Login shell /bin/bash

Password Lock password Remove password



LDAP Account Manager (192.168.203.167) x +

Niezabezpieczona | 192.168.203.167/lam/templates/account/edit.php?type=user&DN=%27cn%3Danowak%2Cdc%3... Gość

Save Reset changes Set password default Load profile

**anowak**

Suffixlab > pl RDN identifier cn

Invalid configuration detected. Please edit your server profile (module settings) and fill all required fields.

Unix Shadow Personal

User name \* anowak

Common name anowak

UID number 10006

Gecos

Primary group marketing

Additional groups Edit groups

Home directory \* /home/anowak

Login shell /bin/csh

Password

/bin/csh /bin/bash /bin/csh /bin/dash /bin/false /bin/ksh

LDAP Account Manager (192.168.203.167) x +

Niezabezpieczona | 192.168.203.167/lam/templates/account/edit.php Gość

Save Reset changes Set password default Load profile

**anowak**

Suffixlab > pl RDN identifier cn

Invalid configuration detected. Please edit your server profile (module settings) and fill all required fields.

Unix Shadow Personal

User name \* anowak

Common name anowak

UID number 10006

Gecos

Primary group marketing

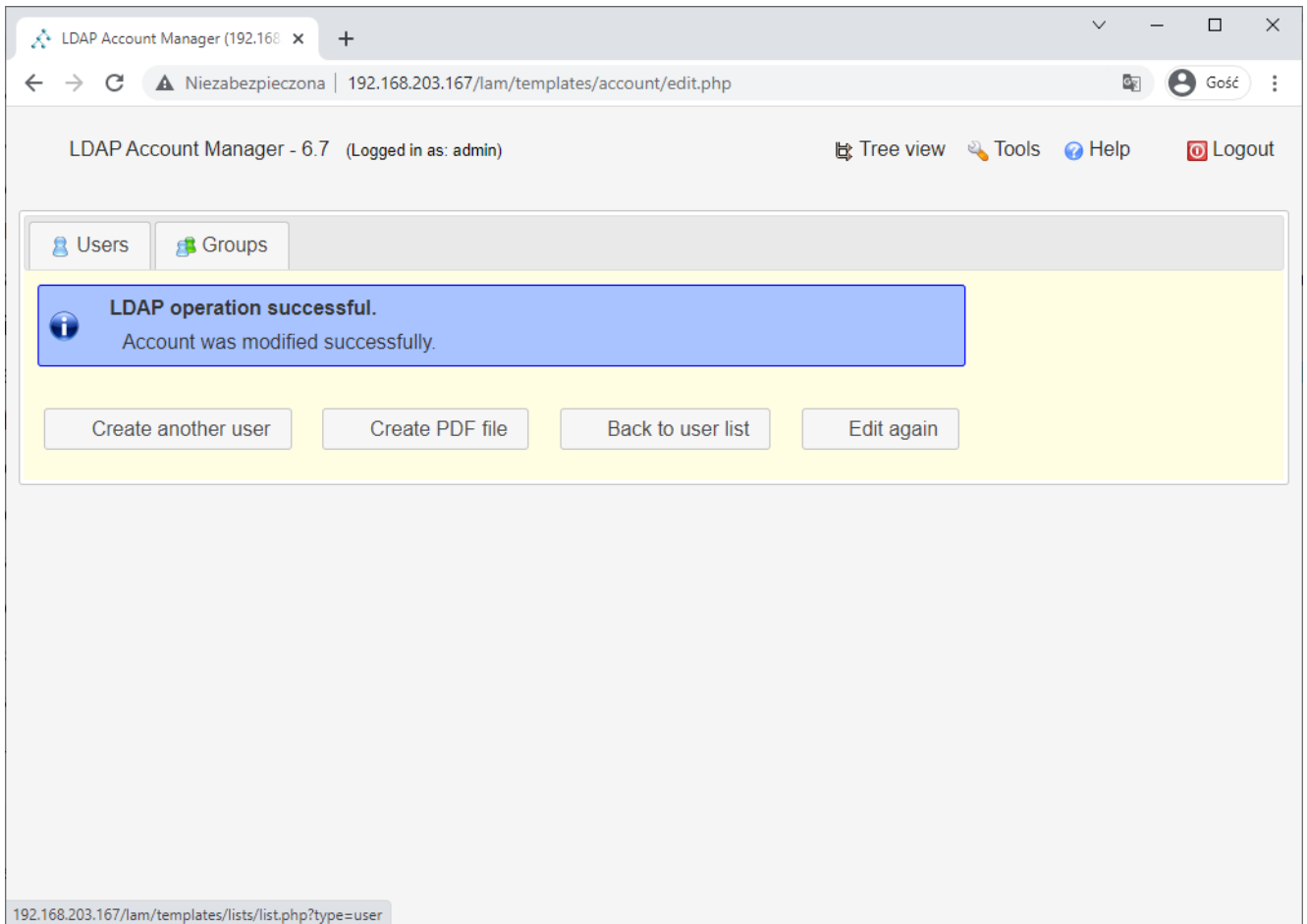
Additional groups Edit groups

Home directory \* /home/anowak

Login shell /bin/csh

Password Lock password Remove password

1 2



Sprawdź jeszcze raz Putty łączność za pomocą wybrane użytkownika z katalogu LDAP. Znak zachęty wskazuje na shella /bin/bash

```
192.168.203.167 - PuTTY
login as: anowak
anowak@192.168.203.167's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-91-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Mon 13 Dec 2021 04:33:52 PM UTC

System load:  0.0          Processes:           214
Usage of /:   78.2% of 8.79GB   Users logged in:   1
Memory usage: 70%          IPv4 address for ens160: 192.168.203.167
Swap usage:   8%

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

102 updates can be installed immediately.
1 of these updates is a security update.
To see these additional updates run: apt list --upgradable

Last login: Mon Dec 13 16:27:35 2021 from 100.100.202.76
anowak@linux:~$
```

**Rozszerzyliśmy schemat LDAPa  
zmodyfikowaliśmy atrybut  
shella /bin/bash dla  
wybranego użytkownika**