

LDAP

Spis treści

CZĘŚĆ I – WSTĘP	2
1. CZYM JEST USŁUGA KATALOGOWA?	2
2. CZYM JEST LDAP?	3
CZĘŚĆ II – PODSTAWY W/ CLI	5
1. INSTALACJA I WSTĘPNA KONFIGURACJA	5
2. KONFIGURACJA SERWISU	6
<i>Struktura konfiguracji nowoutworzonej usługi katalogowej</i>	9
<i>Wpisy w nowoutworzonej usłudze katalogowej</i>	10
3. EDYTOWANIE OBIEKTÓW W USŁUDZE KATALOGOWEJ	11
<i>Dodawanie</i>	11
<i>Modyfikowanie</i>	12
<i>Usuwanie</i>	14
4. WYŚWIETLANIE TYLKO NIEKTÓRYCH PARAMETRÓW ZA POMOCĄ `LDAPSEARCH`	15
5. UTWORZENIE UŻYTKOWNIKA W STANDARDZIE POSIX I WYŚWIETLENIE ZA POMOCĄ GUI	16
CZĘŚĆ III – PODSTAWY W/ GUI	18
1. INSTALACJA APACHE DIRECTORY STUDIO	18
2. EDYTOWANIE OBIEKTÓW W USŁUDZE KATALOGOWEJ	20
<i>Dodawanie:</i>	20
• Jednostki organizacyjnej	20
• Użytkownika	22
<i>Modyfikowanie</i>	25
• Zmienianie wartości atrybutów	25
• Dodawanie dodatkowej wartości dla atrybutu	26
• Usuwanie atrybutu	27
<i>Usuwanie</i>	28
3. UTWORZENIE UŻYTKOWNIKA W STANDARDZIE POSIX I WYŚWIETLENIE GO	29
<i>Dodanie hasła</i>	31
4. DODATKOWA KONFIGURACJA: TWORZENIE DODATKOWEJ DOMENY	32
CZĘŚĆ IV – ZASTOSOWANIE W PRAKTYCE	33
1. LOGOWANIE DO SYSTEMU ZA POMOCĄ KONT LDAP:	33
<i>Przygotowanie: klienta (Linux)</i>	33
• Instalacja potrzebnych paczek	33
• Konfiguracja libnss i libpam podczas instalacji	34
• Konfiguracja nss i ldap	37
• Logowanie	38
<i>Przygotowanie: (Windows)</i>	39
2. LOGOWANIE DO APLIKACJI ZA POMOCĄ INTEGRACJI Z LDAP (NA PRZYKŁADZIE NEXTCLOUD)	40
<i>Przygotowanie i instalacja Nextcloud-a</i>	40
• Instalacja narzędzi do konteneryzacji	40
• Utworzenie pliku docker-compose o treści:	41
• Utworzenie sekretów z hasłami	42
• Utworzenie i uruchomienie kontenerów z pomocą docker-compose	42
<i>Konfiguracja Nextcloud-a</i>	43
• Konfiguracja integracji z LDAP	45
• Logowanie	49
ZAGADNIENIA UZUPEŁNIAJĄCE	51
1. NSS – NAME SERVICE SWITCH (PRZELĄCZNIK USŁUGI NAZW)	51
2. KONTENERYZACJA	51

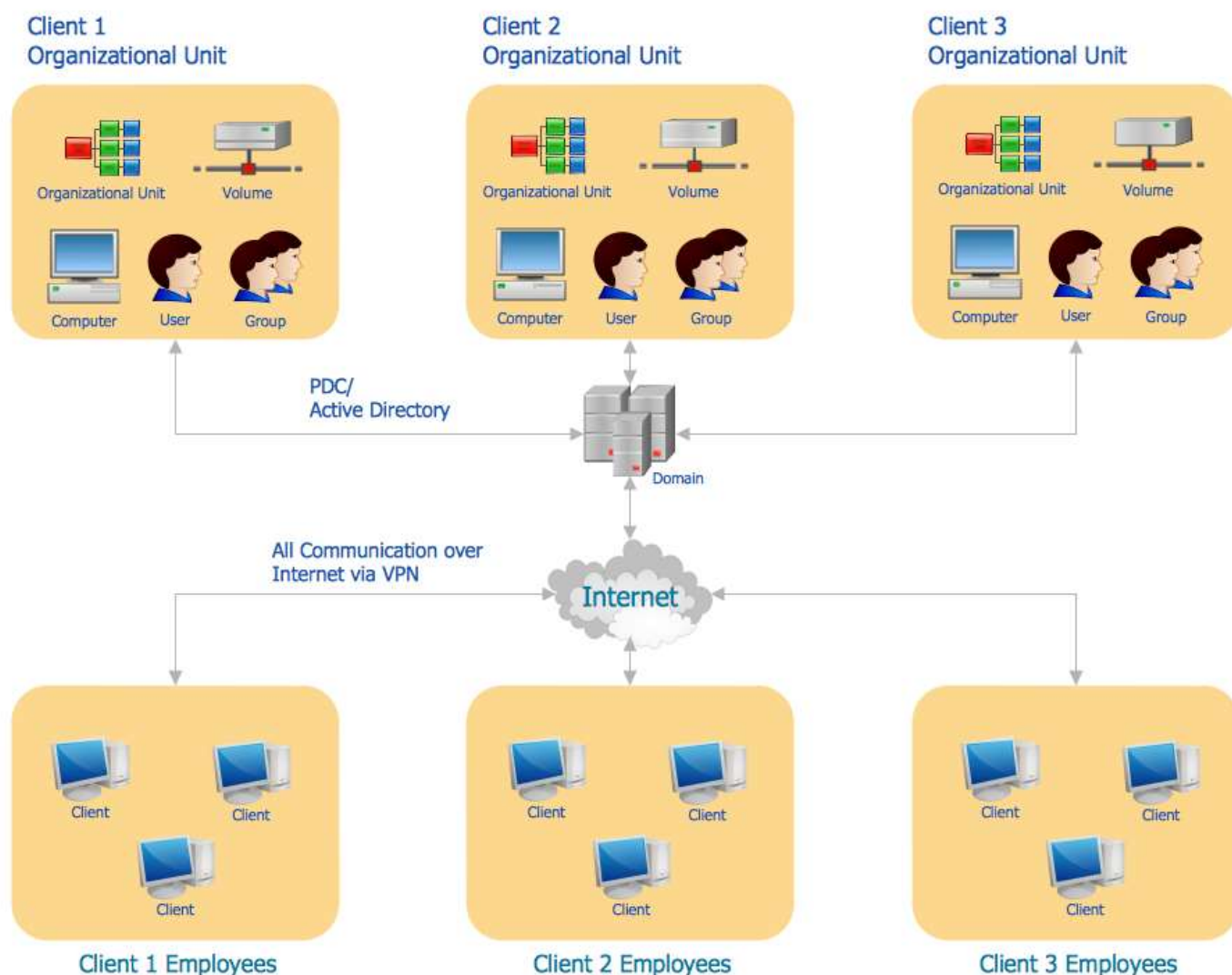
Część I – Wstęp

1. Czym jest usługa katalogowa?

Usługa katalogowa – jest to baza danych zawierająca następujące obiekty:

- użytkowników,
- aplikacje,
- urządzenia sieciowe (np.: drukarki),
- inne zasoby sieciowe (np.: pliki).

Pozwala ona na łatwiejsze zarządzanie relacji między ludźmi, urządzeniami, sieciami, aplikacjami i innymi zawartymi w sieci informacjami. Usługa katalogowa zapewnia bezpieczeństwo, kontrolując dostęp i oferując pewien stopień odporności na błędy.



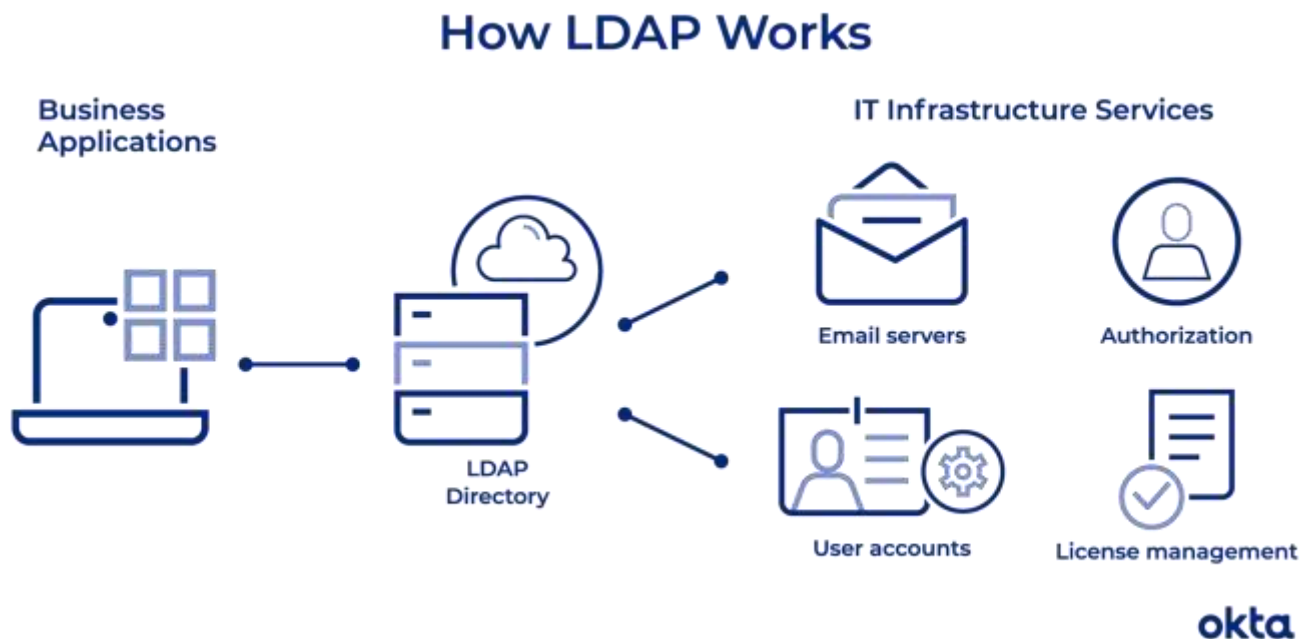
Grafika 1

Dostępne na rynku przykładowe usługi katalogowe:

- Active Directory (Windows)
- Apache Directory Project
- Apple Open Directory (macOS)
- Fedora Directory Server
- IBM Tivoli Directory Server
- OpenLDAP
- Red Hat Directory Server
- Sun Java System Directory Server

2. Czym jest LDAP?

LDAP (ang. **Lightweight Directory Access Protocol**) jest to protokół przeznaczony do korzystania z usług katalogowych, a także narzędzie usługi katalogowej pozwalającej na wymianę informacji za pośrednictwem TCP/IP.



Grafika 2

3. Atrybuty i klasy obiektów w LDAP

Każdy wpis LDAP zawiera zestaw atrybutów LDAP reprezentujących różne rodzaje cech samego wpisu. Atrybut składa się z typu atrybutu i co najmniej jednej wartości atrybutu. Przykładem typu atrybutu może być „mail” z wartością „pp@mail.pp” albo „surname” z wartością „Pasternak”.

Typy atrybutów

W sumie istnieją trzy rodzaje atrybutów.

- **Atrybuty tekstu.** Schemat LDAP zawsze oznacza je jako „czytelne dla człowieka”. Te atrybuty nie mogą zawierać w swoich wartościach symboli niedrukowalnych. Oto kilka przykładów atrybutów tekstowych: *mail*, *displayName*, *telephoneNumber*.
- **Atrybuty binarne.** Atrybuty binarne mogą zawierać w swoich wartościach dowolne symbole i mają opisywać jednostki, takie jak obrazy, dane audio, certyfikaty i tak dalej.
- **Atrybuty operacyjne.** Są one używane przez serwery LDAP do administrowania samym systemem katalogów i nie są zwracane w wynikach wyszukiwania, chyba że wyraźnie zażądamy tego nazwa. Na przykład atrybuty operacyjne mogą służyć jako wskaźnik, do kogo i kiedy został utworzony i zmodyfikowany wpis, do którego należy taki atrybut itp.

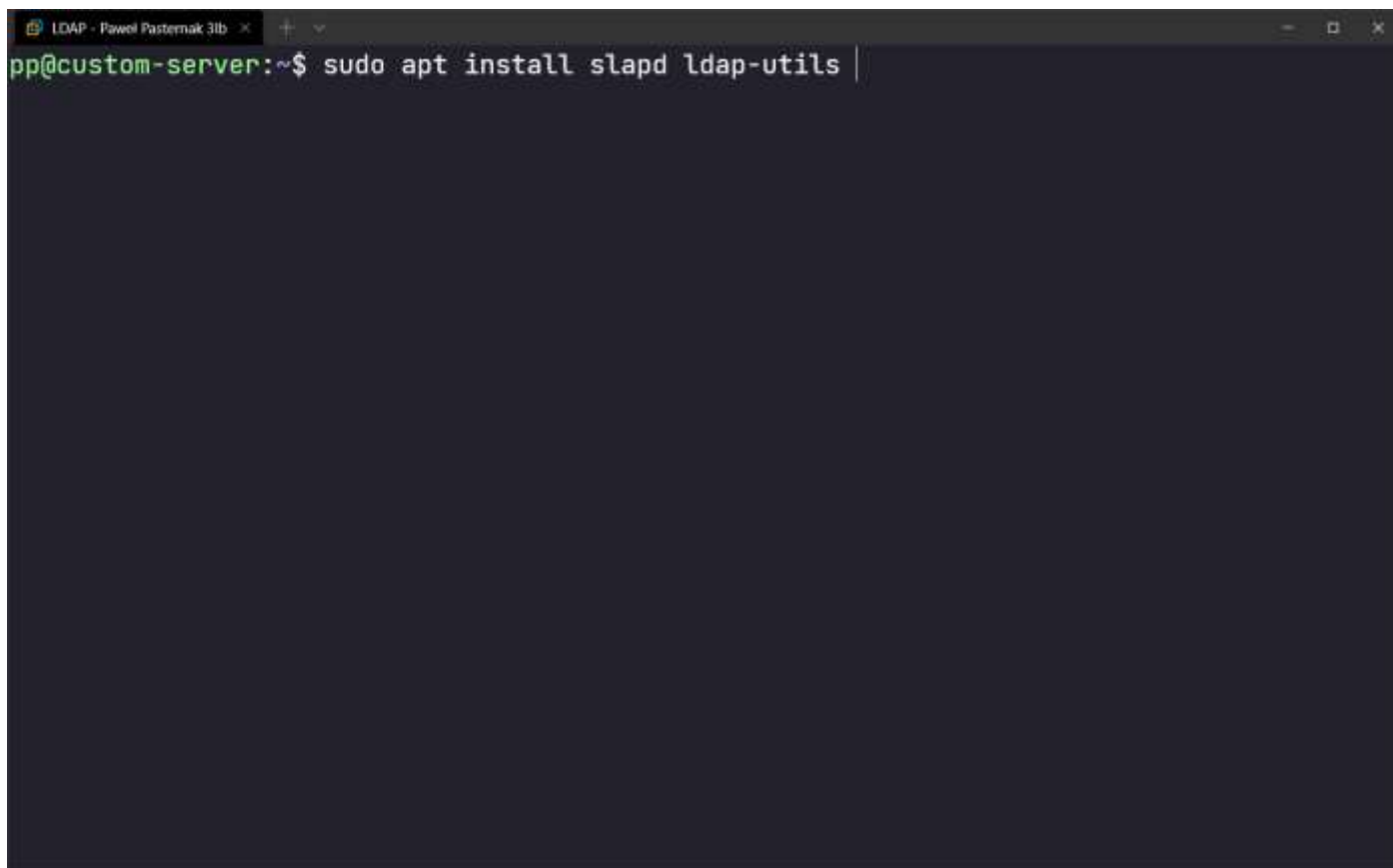
objectClass to specjalny atrybut wpisu, który definiuje, jaki rodzaj obiektu opisuje wpis wraz z zestawem atrybutów, które wpis ten może zawierać. Zdecydowanie odradzamy ręczną edycję tego atrybutu — należy raczej używać kreatora dodawania lub usuwania klas obiektów specjalnie zaprojektowanego do tego celu.

PRZYDATNE LINKI:

- https://pl.wikipedia.org/wiki/Us%C5%82uga_katalogowa
- <https://www.conceptdraw.com/examples/active-directory-structure>
- https://pl.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol
- https://youtu.be/sz43X-y_ddY
- <https://www.linuxjournal.com/article/5689>
- <https://www.linux.com/news/linux-ldap-authentication/>
- https://ldapcon.org/2015/wp-content/uploads/2015/09/ivanova-samba_backend.pdf
- <https://www.ibm.com/docs/en/scf/4.2.2?topic=directory-remote-nfs-server>
- https://hub.docker.com/_/nextcloud
- https://docs.nextcloud.com/server/stable/admin_manual/configuration_user/user_auth_ldap.html

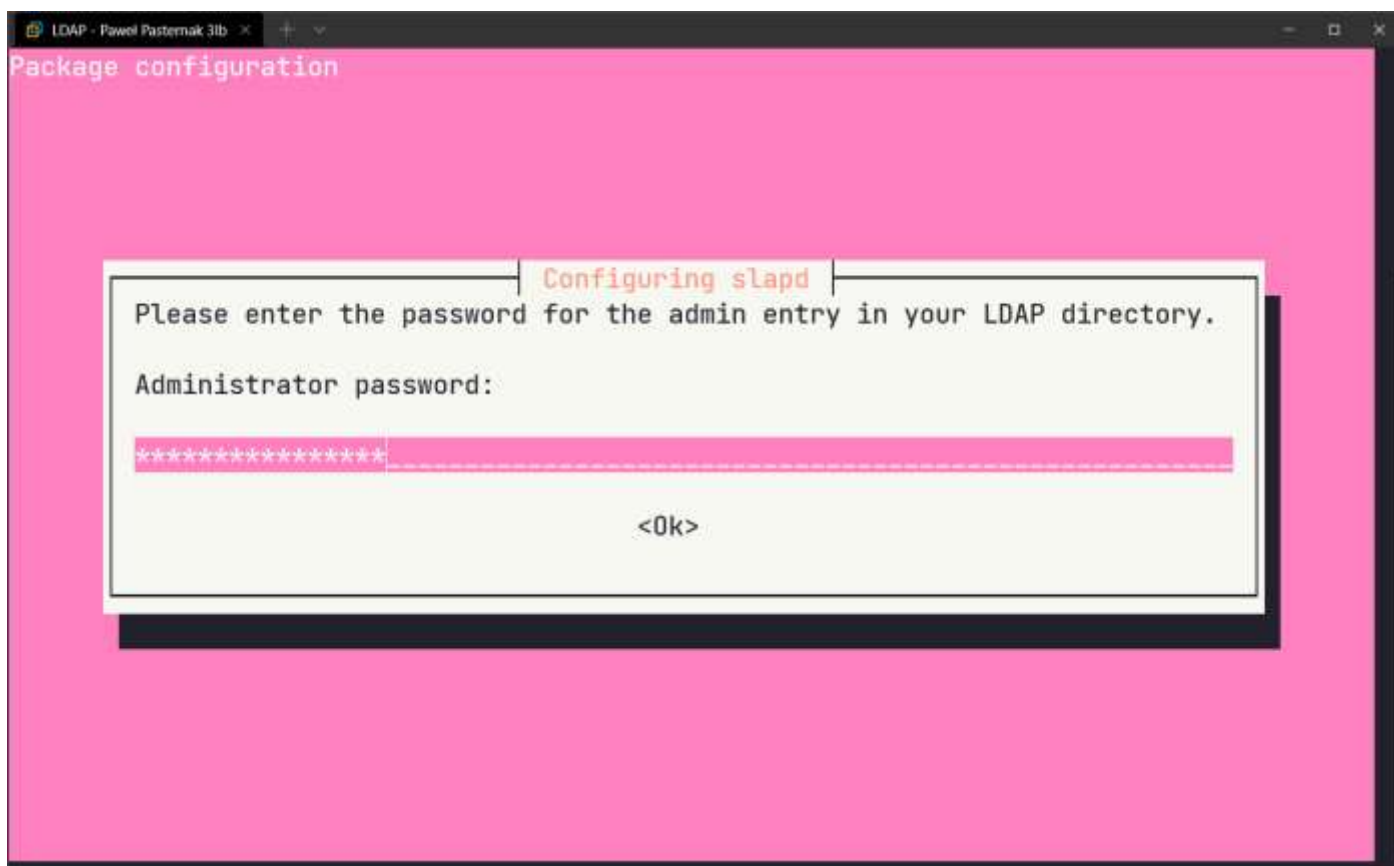
Część II – Podstawy w/ CLI

1. Instalacja i wstępna konfiguracja



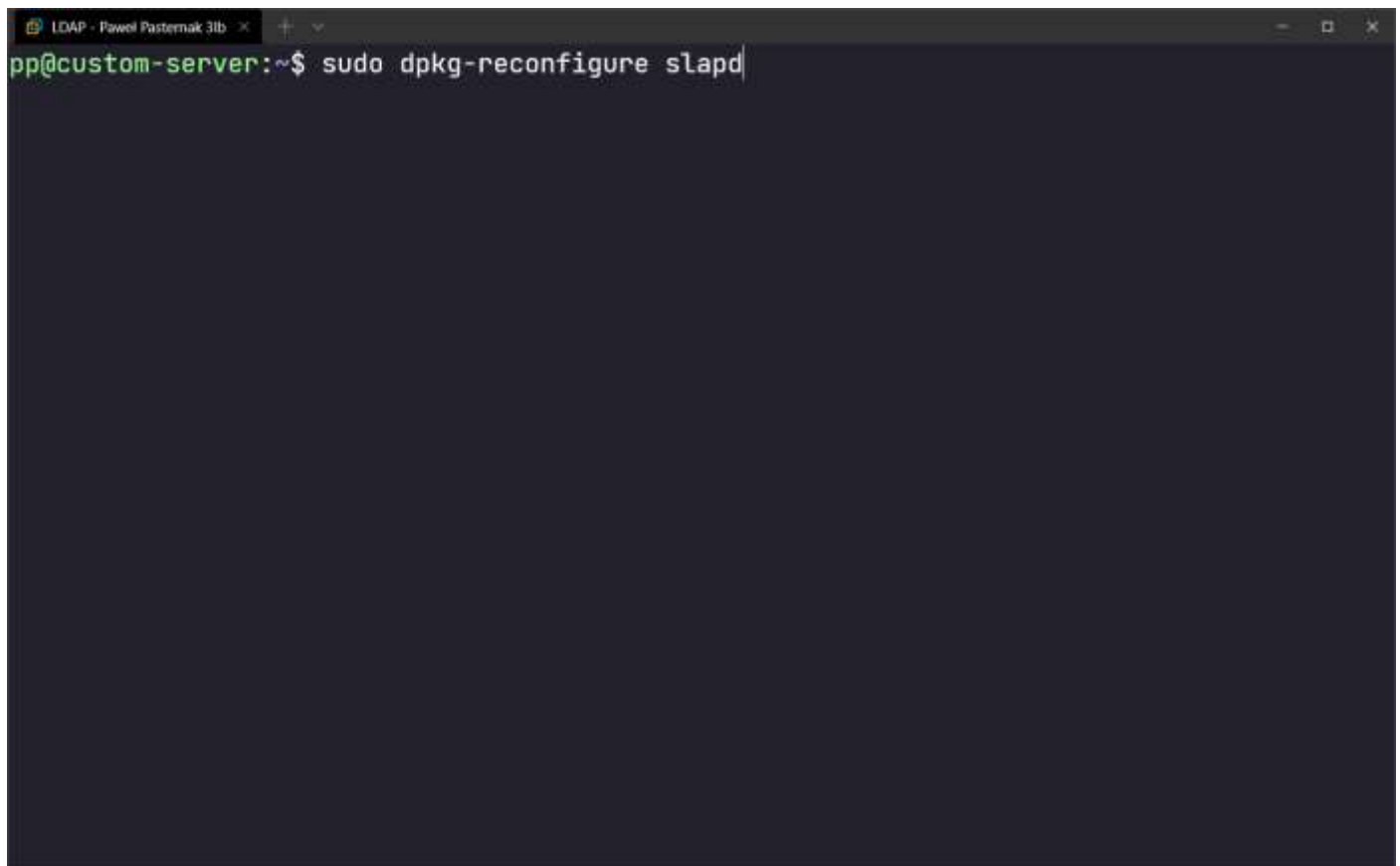
```
pp@custom-server:~$ sudo apt install slapd ldap-utils
```

Zrzut Ekranu 1 - instalacja serwera ldap i narzędzi z nim związanych

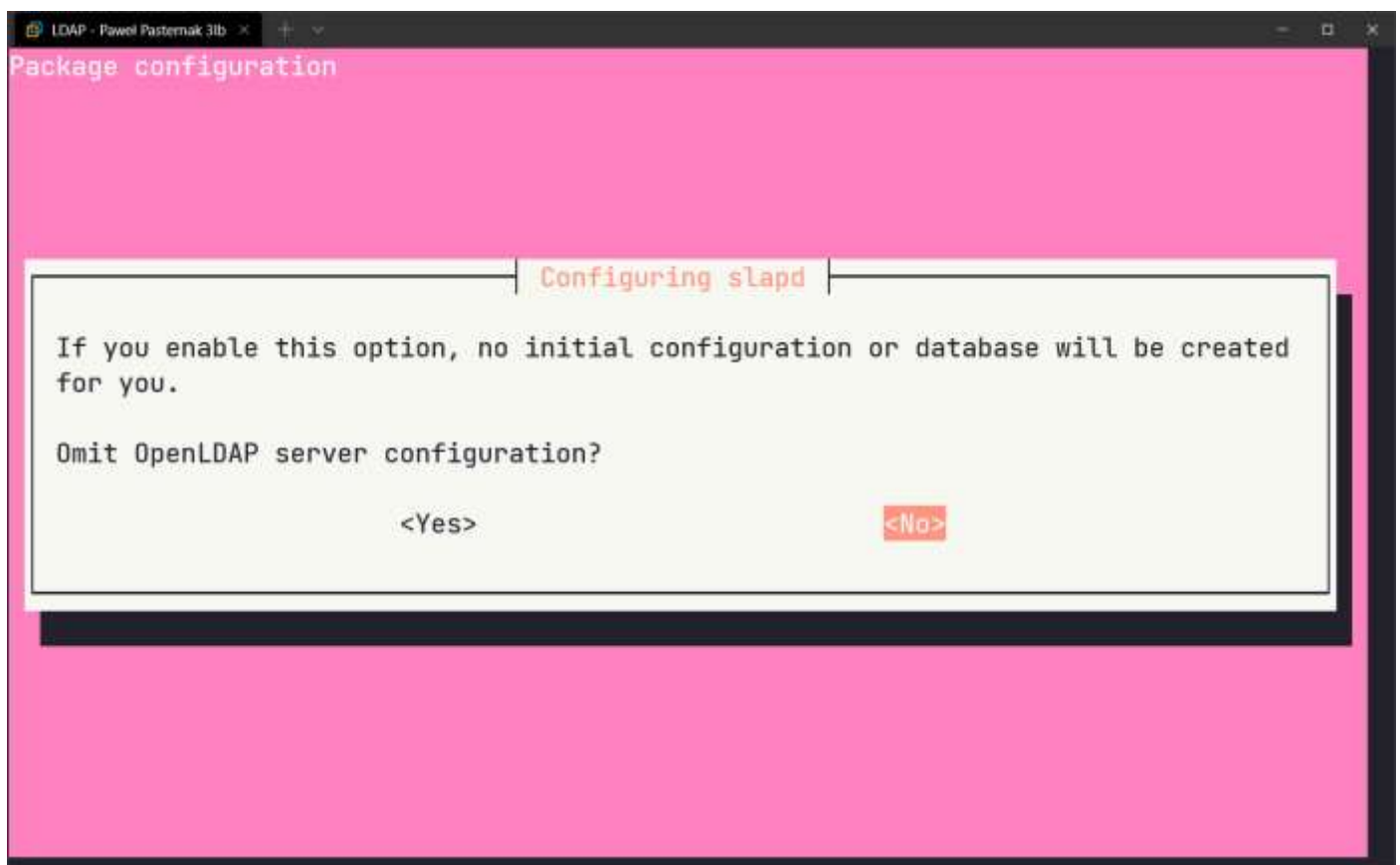


Zrzut Ekranu 2 - ustawienie hasła dla administratora LDAP

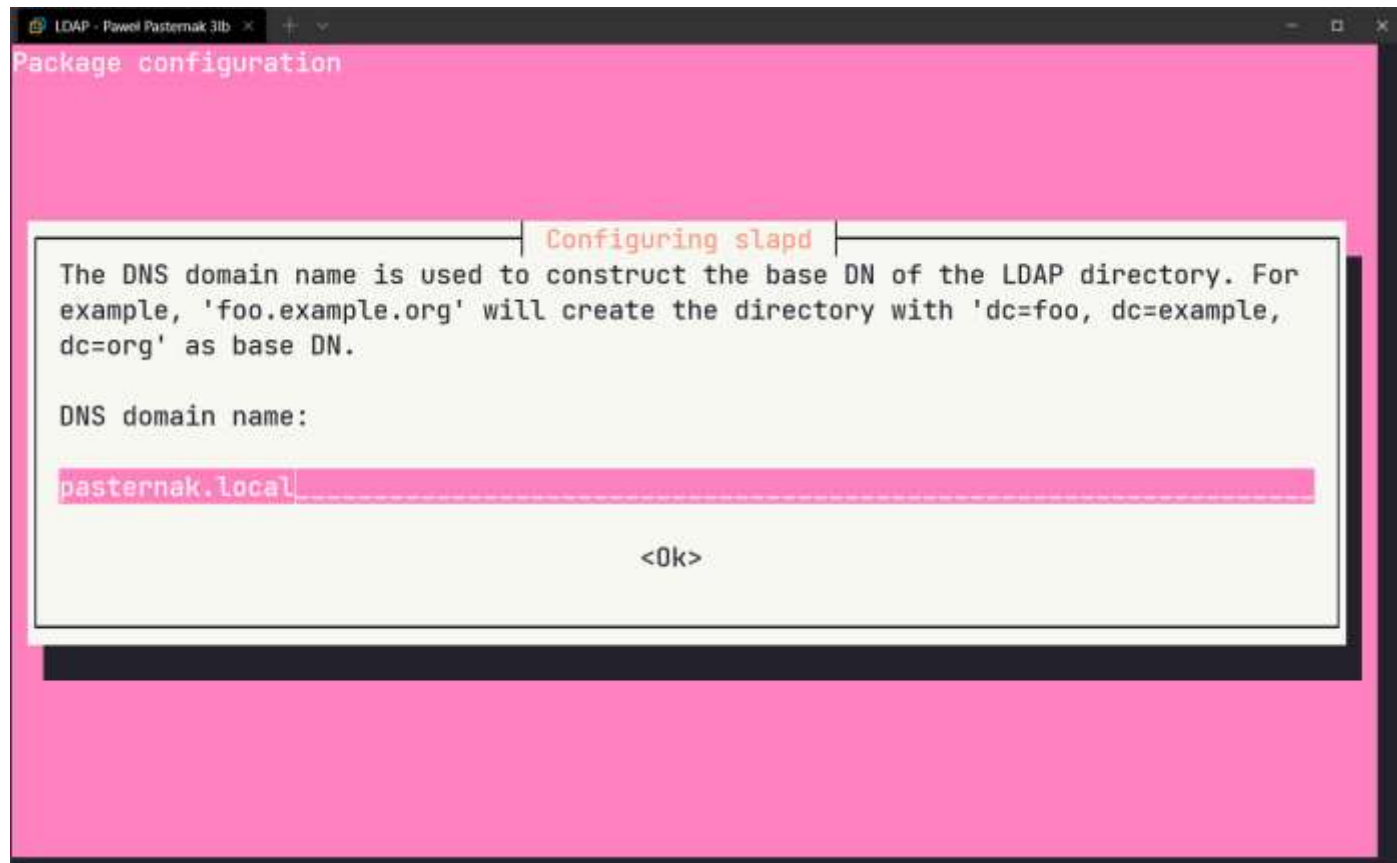
2. Konfiguracja serwisu



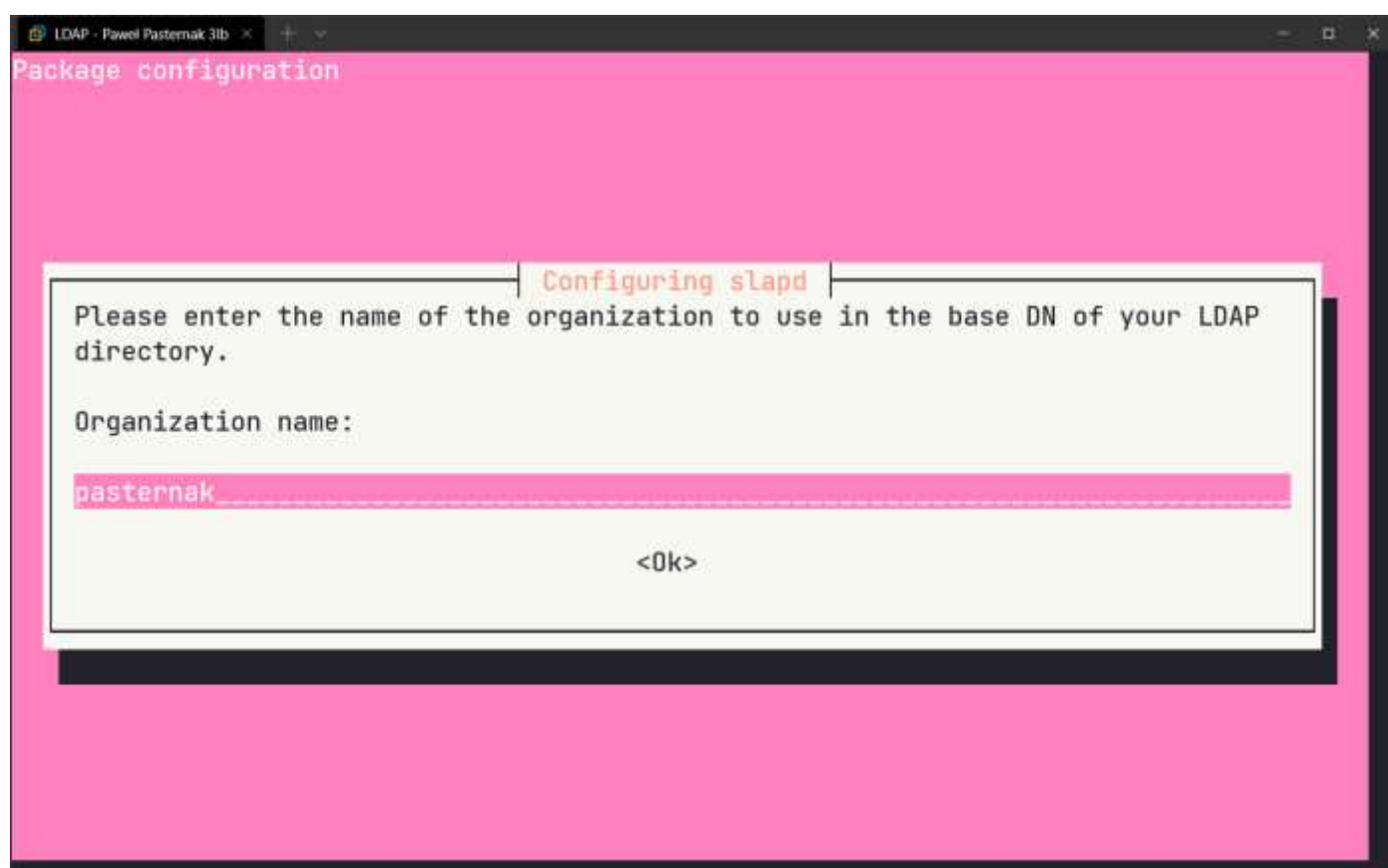
Zrzut Ekranu 3 - uruchomienie skryptu konfiguracyjnego LDAP



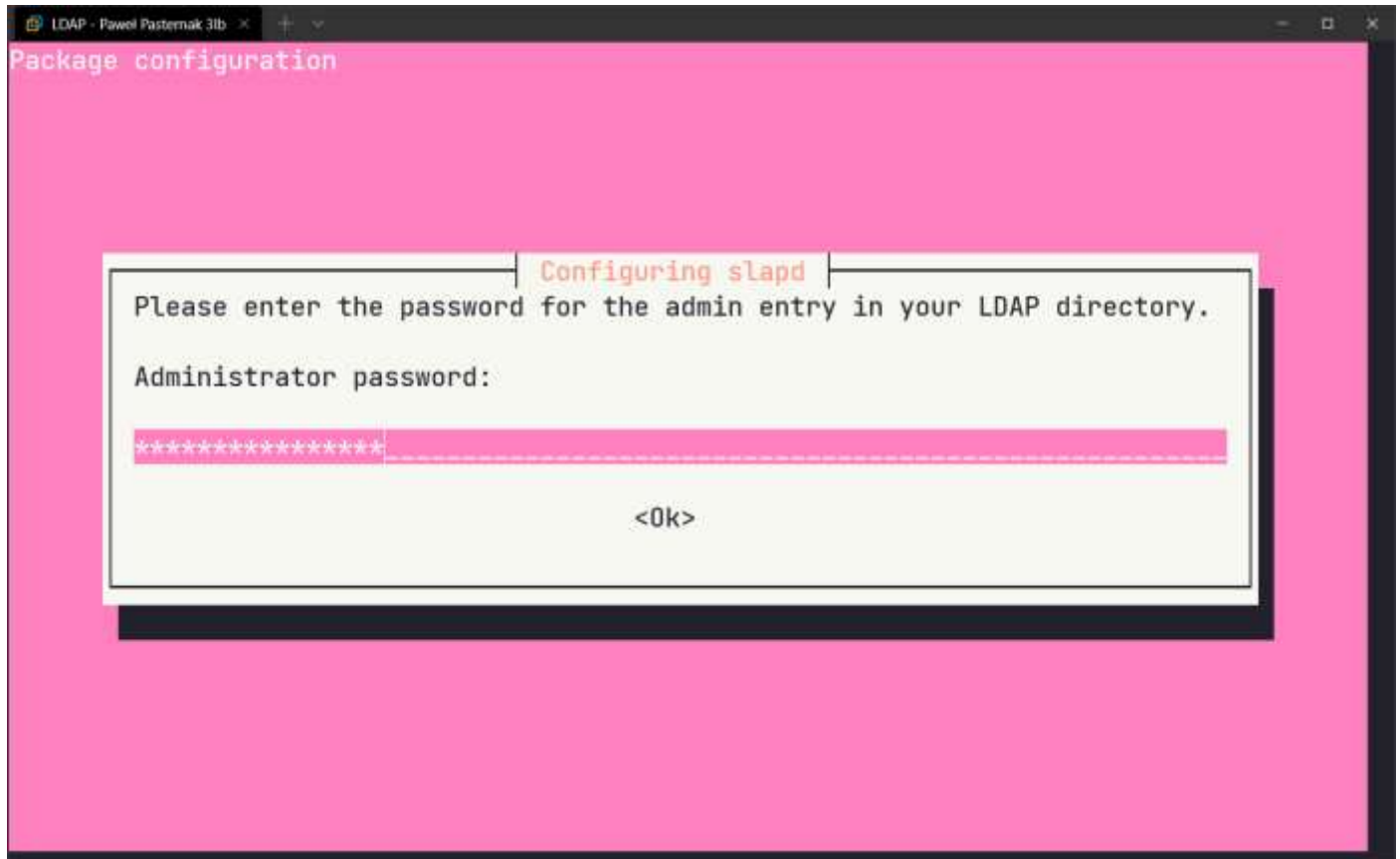
Zrzut Ekranu 4 - utworzenie pierwszej bazy danych



Zrzut Ekranu 5 - ustawienie domeny



Zrzut Ekranu 6 - ustawienie nazwy organizacji



Zrzut Ekranu 7 - potwierdzenie ustawień hasłem administratora LDAP

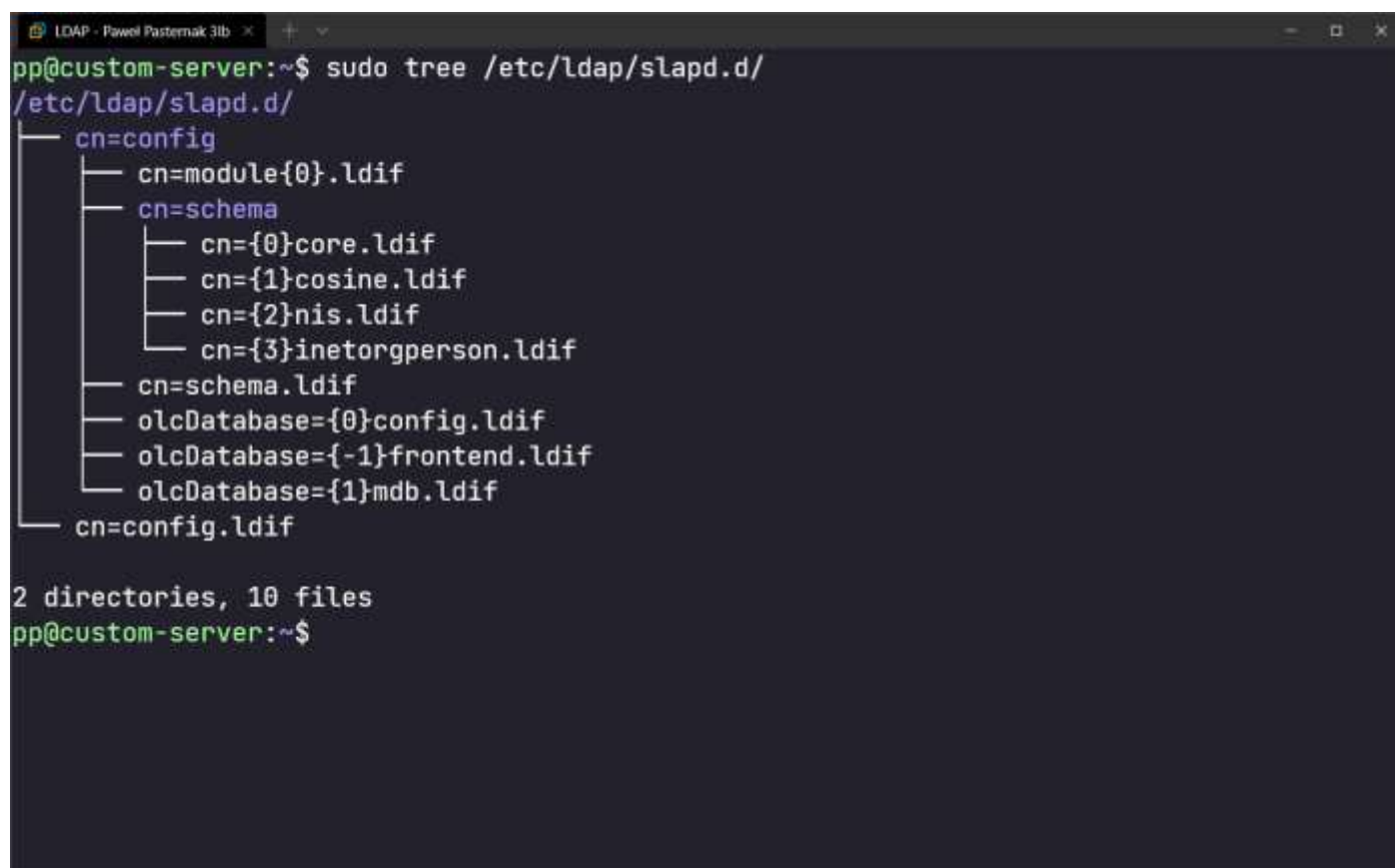


Zrzut Ekranu 8 - pytanie o usunięcie bazy danych gdy będzie odinstalowywany pakiet slapd

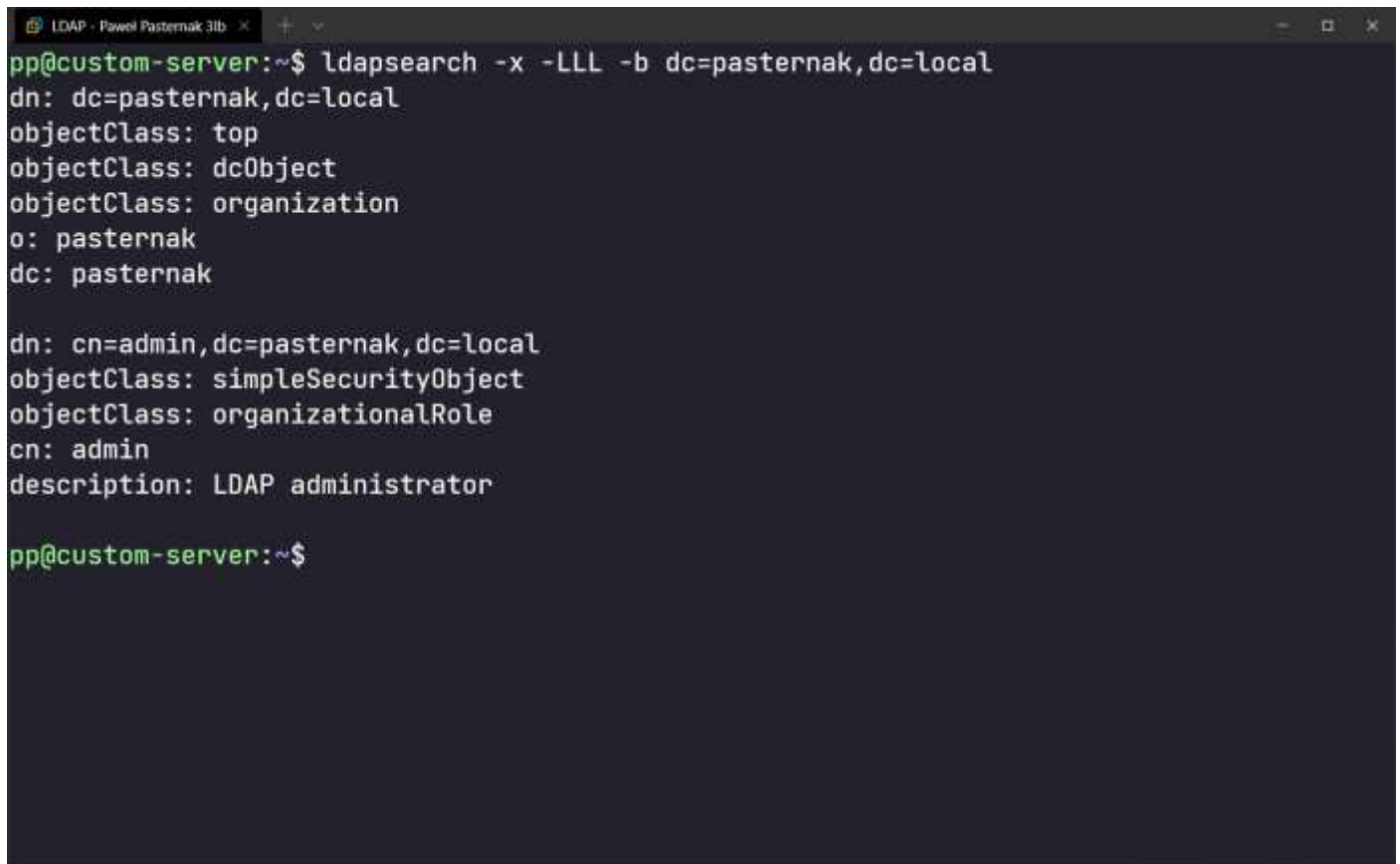


Zrzut Ekranu 9 - pytanie o przeniesienie starej bazy danych

Struktura konfiguracji nowoutworzonej usługi katalogowej



Zrzut Ekranu 10 - struktura ustawień ldap

A screenshot of a terminal window titled "LDAP - Paweł Pasternak 31b". The terminal shows the output of the command "ldapsearch -x -LLL -b dc=pasternak,dc=local". The output lists two LDAP entries. The first entry is for the organization "dc=pasternak,dc=local" with object classes "top", "dcObject", and "organization", and object name "pasternak". The second entry is for the user "cn=admin,dc=pasternak,dc=local" with object classes "simpleSecurityObject" and "organizationalRole", and a description of "LDAP administrator". The prompt "pp@custom-server:~\$" is visible at the bottom of the terminal.

```
pp@custom-server:~$ ldapsearch -x -LLL -b dc=pasternak,dc=local
dn: dc=pasternak,dc=local
objectClass: top
objectClass: dcObject
objectClass: organization
o: pasternak
dc: pasternak

dn: cn=admin,dc=pasternak,dc=local
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator

pp@custom-server:~$
```

Zrzut Ekranu 11 - wyświetlenie wpisów usługi katalogowej

3. Edytowanie obiektów w usłudze katalogowej

Dodawanie

```
LDAP - Paweł Pasternak 3lb x + v - □ x
# Utworzenie grupy instruktorzy
dn: ou=instructors, dc=pasternak, dc=local
changetype: add
objectClass: organizationalUnit
ou: instructors

# Utworzenie grupy studenci
dn: ou=students, dc=pasternak, dc=local
changetype: add
objectClass: organizationalUnit
ou: students

# Utworzenie i dodanie użytkownika ppasternak do grupy studenci
dn: uid=ppasternak, ou=students, dc=pasternak, dc=local
changetype: add
objectClass: inetOrgPerson
description: Paweł Pasternak uczeń trzeciej klasy Technikum Łączności na kierunku techn
ik informatyk
cn: Paweł Pasternak
givenName: Paweł
surname: Pasternak
uid: ppasternak
"k1.ldif" 21L, 607C written 1,1 All
```

Zrzut Ekranu 12 - plik ldif k1

```
LDAP - Paweł Pasternak 3lb x + v - □ x
pp@custom-server:~/WD/LDAP$ ldapadd -x -D cn=admin,dc=pasternak,dc=local -W -f k1.ldif
Enter LDAP Password:
adding new entry "ou=instructors, dc=pasternak, dc=local"

adding new entry "ou=students, dc=pasternak, dc=local"

adding new entry "uid=ppasternak, ou=students, dc=pasternak, dc=local"

pp@custom-server:~/WD/LDAP$
```

Zrzut Ekranu 13 - wykonanie poleceń zawartych w pliku k1

Modyfikowanie

Zrzut Ekranu 15 - plik Idif k2

```
LDAP - Paweł Pasternak 31b x + v
pp@custom-server:~/WD/LDAP$ ldapadd -x -D cn=admin,dc=pasternak,dc=local -W -f k2.ldif
Enter LDAP Password:
modifying entry "uid=ppasternak,ou=students,dc=pasternak,dc=local"

pp@custom-server:~/WD/LDAP$
```

Zrzut Ekranu 16 - wykonanie poleceń zawartych w pliku k2

```
LDAP - Paweł Pasternak 31b x + v
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator

dn: ou=instructors,dc=pasternak,dc=local
objectClass: organizationalUnit
ou: instructors

dn: ou=students,dc=pasternak,dc=local
objectClass: organizationalUnit
ou: students

dn: uid=ppasternak,ou=students,dc=pasternak,dc=local
objectClass: inetOrgPerson
description: Paweł Pasternak uczen trzeciej klasy Technikum Łączności na kierunku technik informatyk
description: w sumie LDAP jest do ogarnięcia
sn: Pasternak
uid: ppasternak
cn: Pasternak Paweł

pp@custom-server:~/WD/LDAP$ |
```

Zrzut Ekranu 17 - wyświetlenie dokonanych zmian

```
# Usunięcie użytkownika ppasternak
dn: uid=ppasternak, ou=students, dc=pasternak, dc=local
changetype: delete
```

```
"k3.ldif" 3L, 112C                               1,1                      All
```

Zrzut Ekranu 18 - plik Idif k3

```
LDAP - Pawel Pasternak 3lb x + v
pp@custom-server:~/WD/LDAP$ vim k2.ldif
pp@custom-server:~/WD/LDAP$ ldapadd -x -D cn=admin,dc=pasternak,dc=local -W -f k2.ldif
Enter LDAP Password:
deleting entry "uid=ppasternak, ou=students, dc=pasternak, dc=local"

pp@custom-server:~/WD/LDAP$ |
```

Zrzut Ekranu 19 - wykonanie poleceń zawartych w pliku k3


```
pp@custom-server:~/WD/LDAP$ ldapsearch -x -LLL -b dc=pasternak,dc=local
dn: dc=pasternak,dc=local
objectClass: top
objectClass: dcObject
objectClass: organization
o: pasternak
dc: pasternak

dn: cn=admin,dc=pasternak,dc=local
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator

dn: ou=students,dc=pasternak,dc=local
objectClass: organizationalUnit
ou: students

dn: ou=instructors,dc=pasternak,dc=local
objectClass: organizationalUnit
ou: instructors

pp@custom-server:~/WD/LDAP$
```

Zrzut Ekranu 20 - wyświetlenie dokonanych zmian

4. Wyświetlanie tylko niektórych parametrów za pomocą `ldapsearch`.

```
pp@custom-server:~/WD/LDAP$ ldapsearch -x -LLL -b dc=pasternak,dc=local \
> "uid=ppasternak" cn sn \
>
dn: uid=ppasternak,ou=students,dc=pasternak,dc=local
sn: Pasternak
cn: Pasternak Paweł

pp@custom-server:~/WD/LDAP$ |
```

Zrzut Ekranu 21 - użycie polecenia ldapsearch

5. Utworzenie użytkownika w standardzie POSIX i wyświetlenie za pomocą GUI.

```

LDAP - Paweł Pasternak 31b x
# Utworzenie grupy students w standardzie posix
dn: cn=group1, ou=students, dc=pasternak, dc=local
changetype: add
objectClass: posixGroup
cn: group1
gidNumber: 20000

# Utworzenie użytkownika ppasternak z kontem w standardzie posix
dn: uid=ppasternak, ou=students, dc=pasternak, dc=local
changetype: add
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: Paweł Pasternak
sn: Pasternak
uid: ppasternak
uidNumber: 11000
gidNumber: 20000
userPassword: haslo123
loginShell: /bin/sh
homeDirectory: /home/ppasternak
~
"k4.ldif" 21L, 545C 1,1 ALL

```

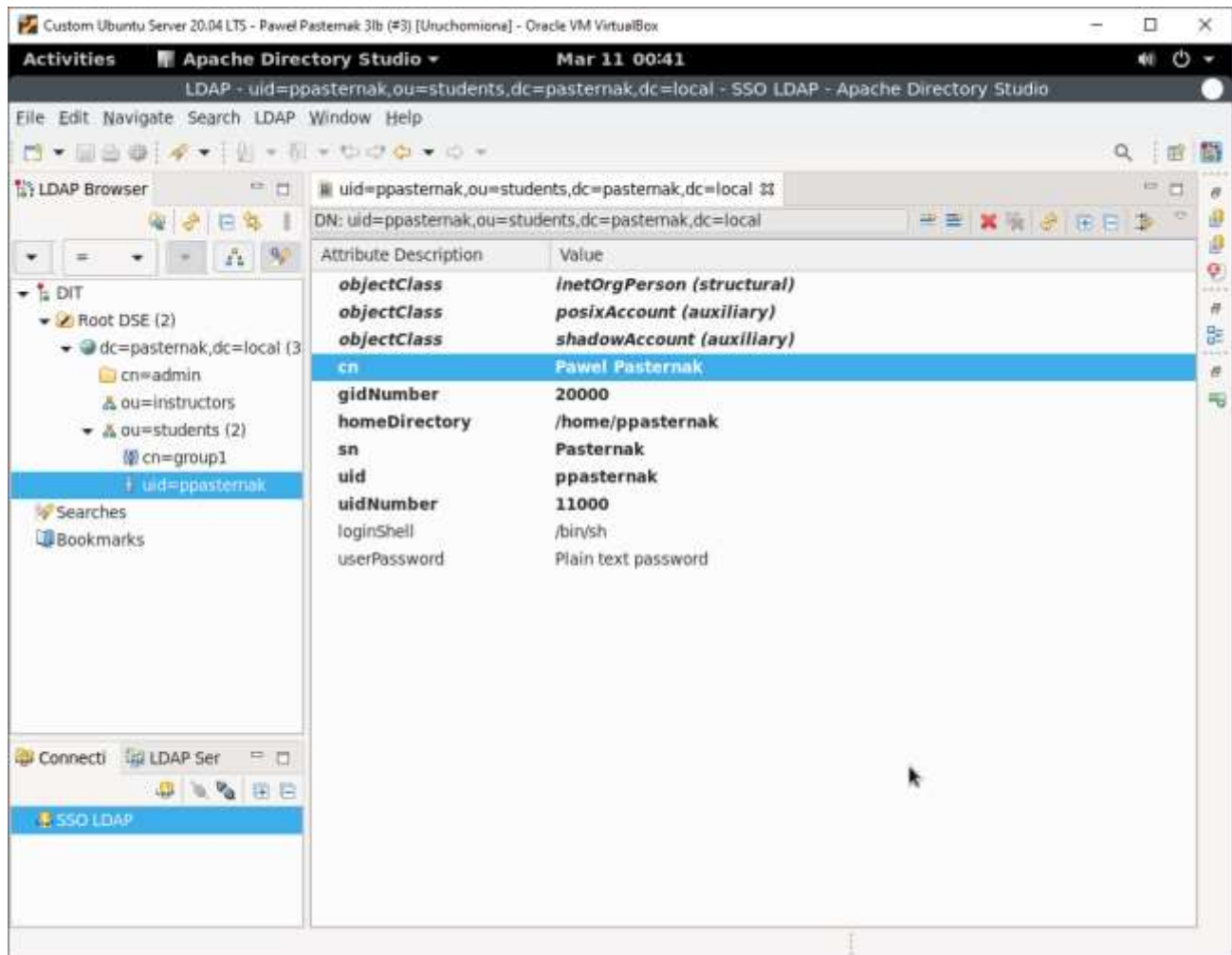
Zrzut Ekranu 22 - plik ldif k4

The screenshot shows the LDAP Admin window with the entry **uid=ppasternak, ou=students, dc=pasternak, dc=local** selected. The entry is expanded, showing its attributes and values in a table.

Attribute	Value	Type	S...
uid	ppasternak	Text	10
objectClass	posixAccount	Text	12
objectClass	inetOrgPerson	Text	13
objectClass	shadowAccount	Text	13
cn	Paweł Pasternak	Text	15
homeDirectory	/home/ppasternak	Text	16
gidNumber	20000	Text	5
uidNumber	11000	Text	5
loginShell	/bin/sh	Text	7
userPassword	haslo123	Text	8
sn	Pasternak	Text	9

The bottom status bar shows: Server: custom-server, User: CN=admin,DC=pasternak,DC=local, uid=ppasternak,ou=students,dc=pasternak,dc=local, 0 subentries.

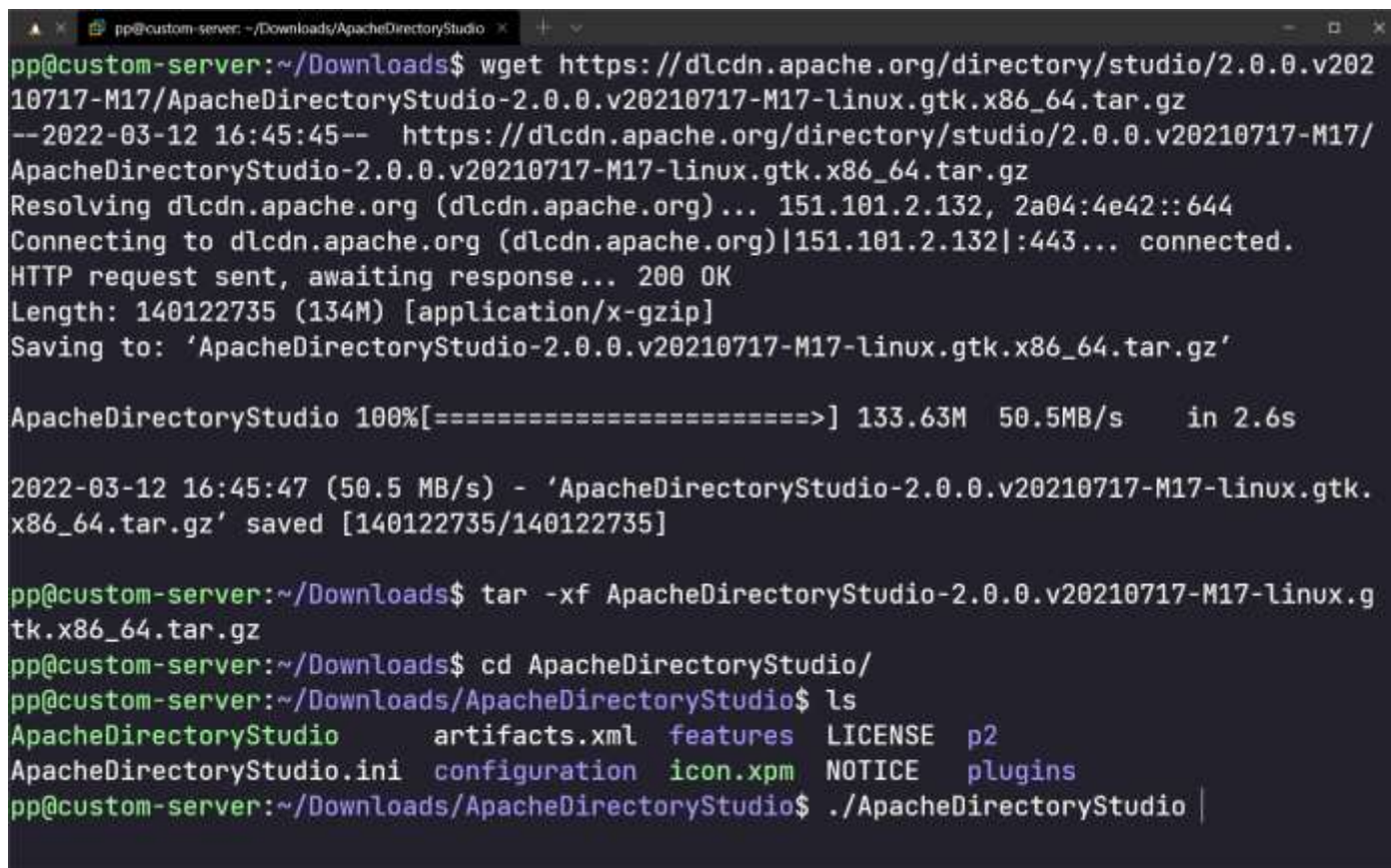
Zrzut Ekranu 23 - struktura wpisów wyświetlona w programie LDAP Admin



Zrzut Ekranu 24 - struktura wpisów wyświetlona w programie Apache Directory Studio

Część III – Podstawy w/ GUI

1. Instalacja Apache Directory Studio



```
pp@custom-server: ~/Downloads/ApacheDirectoryStudio
pp@custom-server:~/Downloads$ wget https://dldn.apache.org/directory/studio/2.0.0.v20210717-M17/ApacheDirectoryStudio-2.0.0.v20210717-M17-linux.gtk.x86_64.tar.gz
--2022-03-12 16:45:45-- https://dldn.apache.org/directory/studio/2.0.0.v20210717-M17/ApacheDirectoryStudio-2.0.0.v20210717-M17-linux.gtk.x86_64.tar.gz
Resolving dldn.apache.org (dldn.apache.org)... 151.101.2.132, 2a04:4e42::644
Connecting to dldn.apache.org (dldn.apache.org)|151.101.2.132|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 140122735 (134M) [application/x-gzip]
Saving to: 'ApacheDirectoryStudio-2.0.0.v20210717-M17-linux.gtk.x86_64.tar.gz'

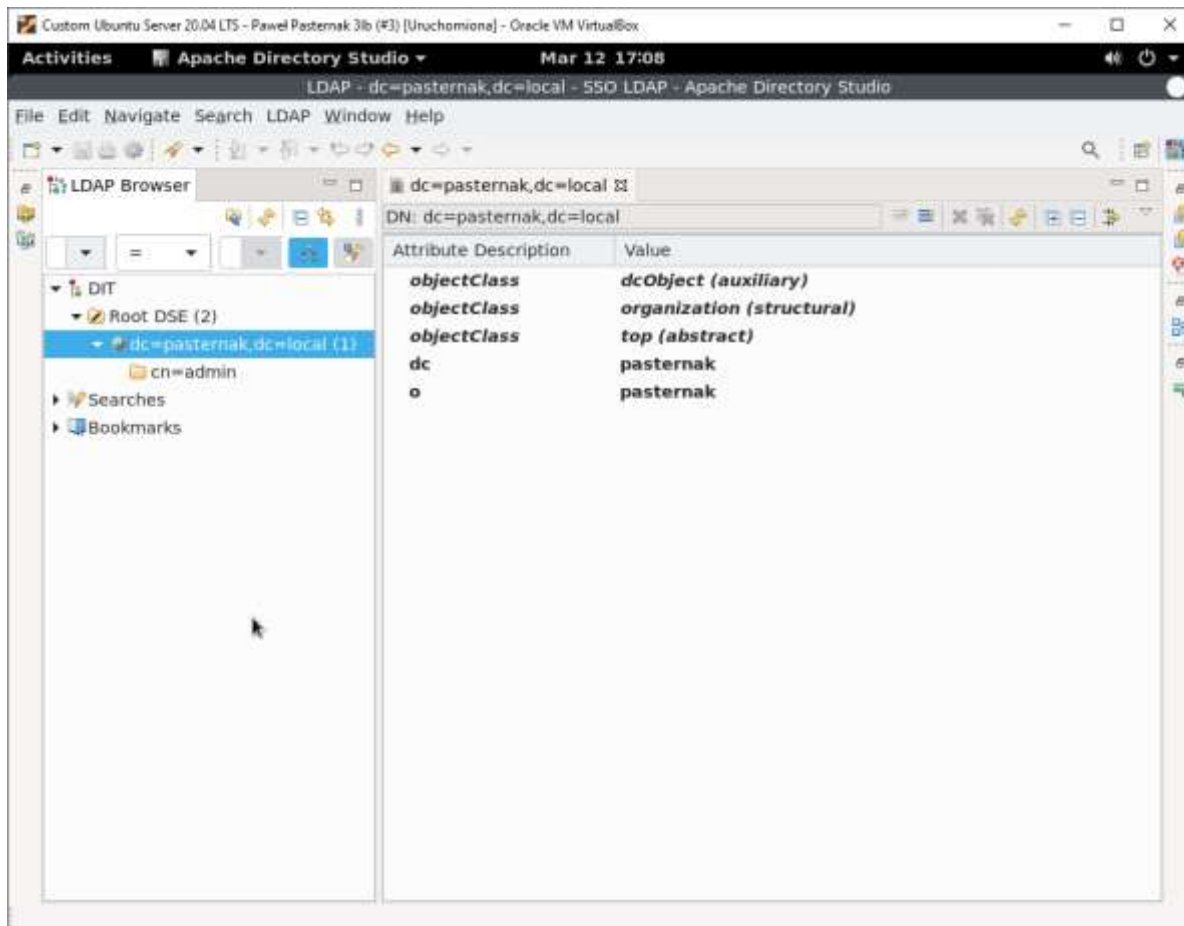
ApacheDirectoryStudio 100%[=====>] 133.63M  50.5MB/s   in 2.6s

2022-03-12 16:45:47 (50.5 MB/s) - 'ApacheDirectoryStudio-2.0.0.v20210717-M17-linux.gtk.x86_64.tar.gz' saved [140122735/140122735]

pp@custom-server:~/Downloads$ tar -xf ApacheDirectoryStudio-2.0.0.v20210717-M17-linux.gtk.x86_64.tar.gz
pp@custom-server:~/Downloads$ cd ApacheDirectoryStudio/
pp@custom-server:~/Downloads/ApacheDirectoryStudio$ ls
ApacheDirectoryStudio  artifacts.xml  features  LICENSE  p2
ApacheDirectoryStudio.ini  configuration  icon.xpm  NOTICE  plugins
pp@custom-server:~/Downloads/ApacheDirectoryStudio$ ./ApacheDirectoryStudio |
```

Zrzut Ekranu 25 - Pobranie archiwum, odpakowanie go i uruchomienie Apache Directory Studio

Paweł Pasternak 31b - LDAP

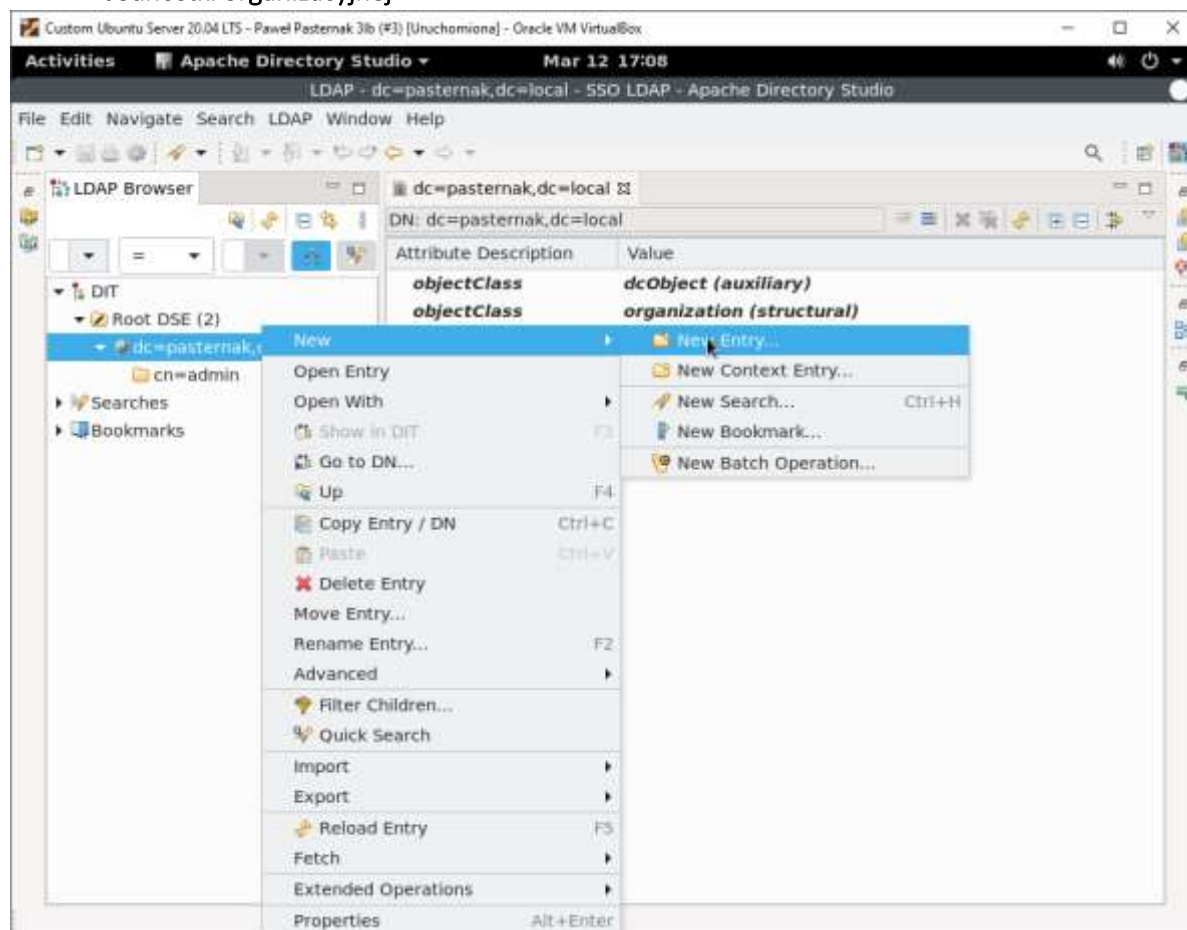


Zrzut Ekranu 26 - wyświetlenie obiektów w nowoutworzonej bazie danych usługi katalogowej

2. Edytowanie obiektów w usłudze katalogowej.

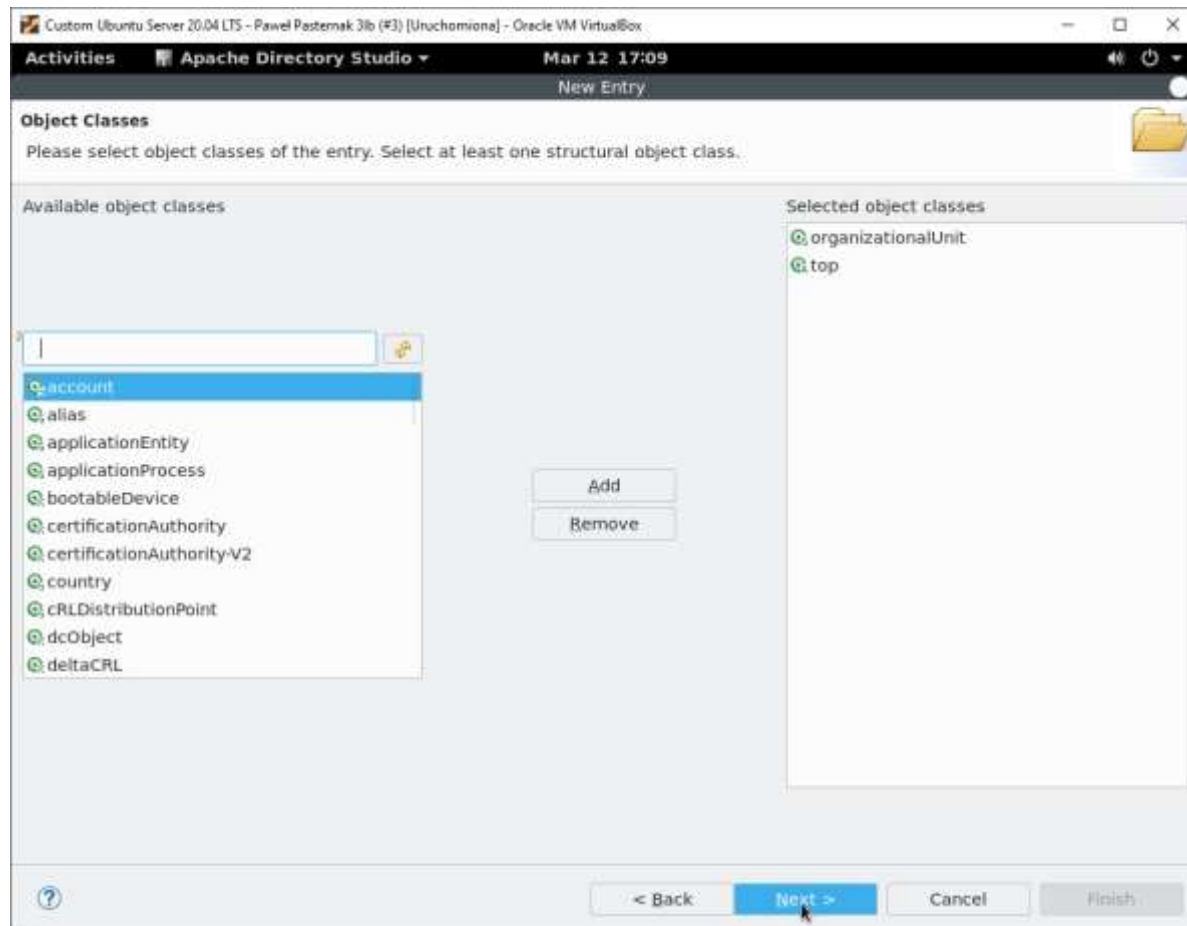
Dodawanie:

- Jednostki organizacyjnej

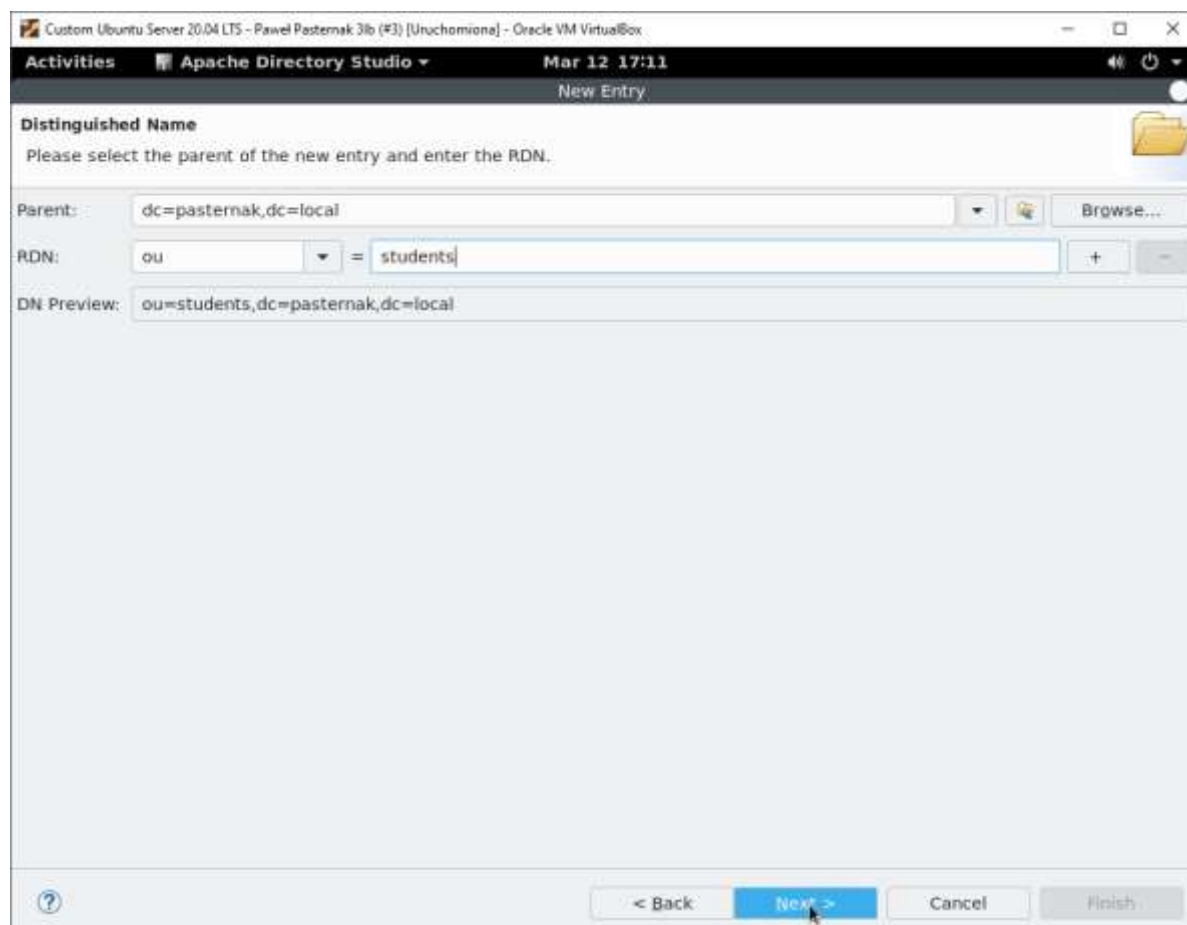


Zrzut Ekranu 27 - dodawanie nowego wpisu

Paweł Pasternak 3lb - LDAP

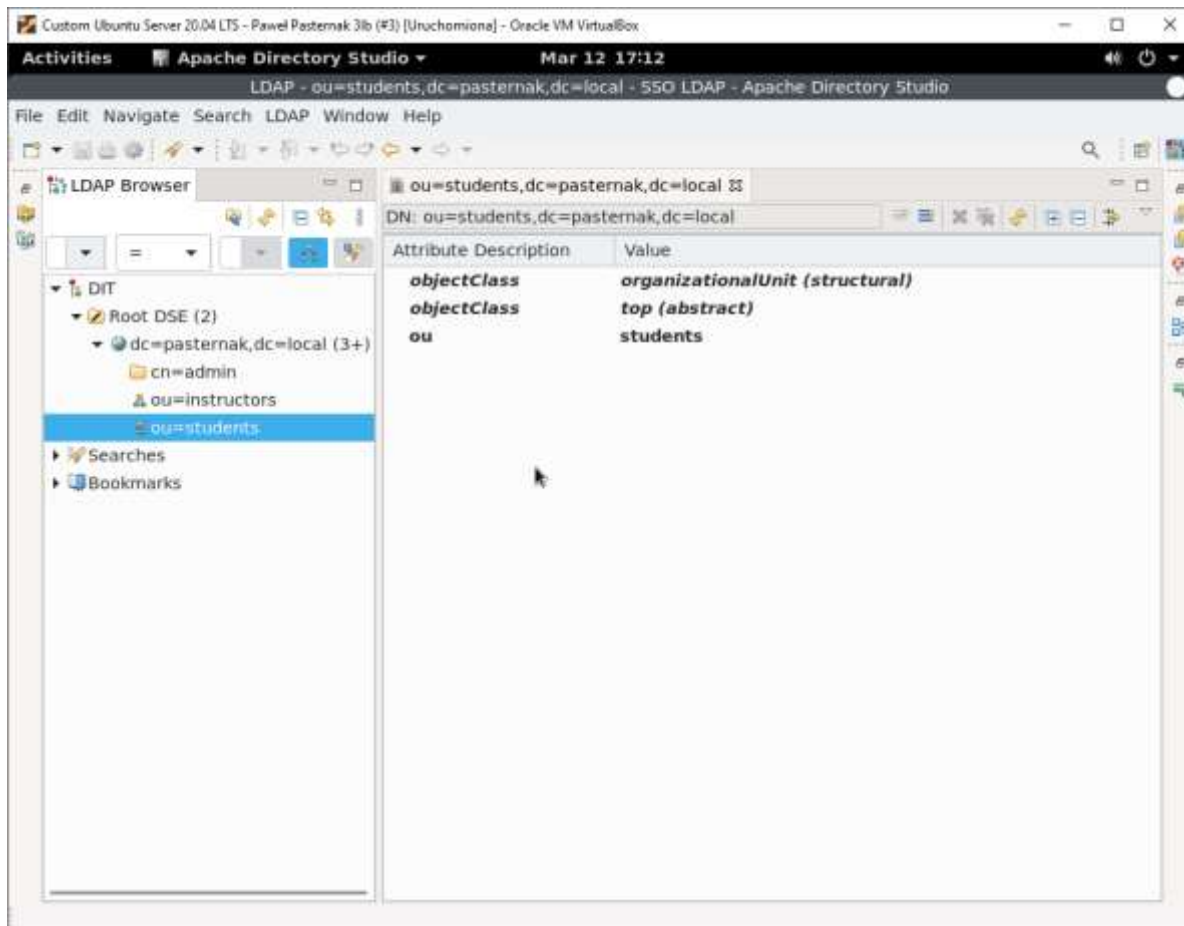


Zrzut Ekranu 28 - dodanie klas atrybutów



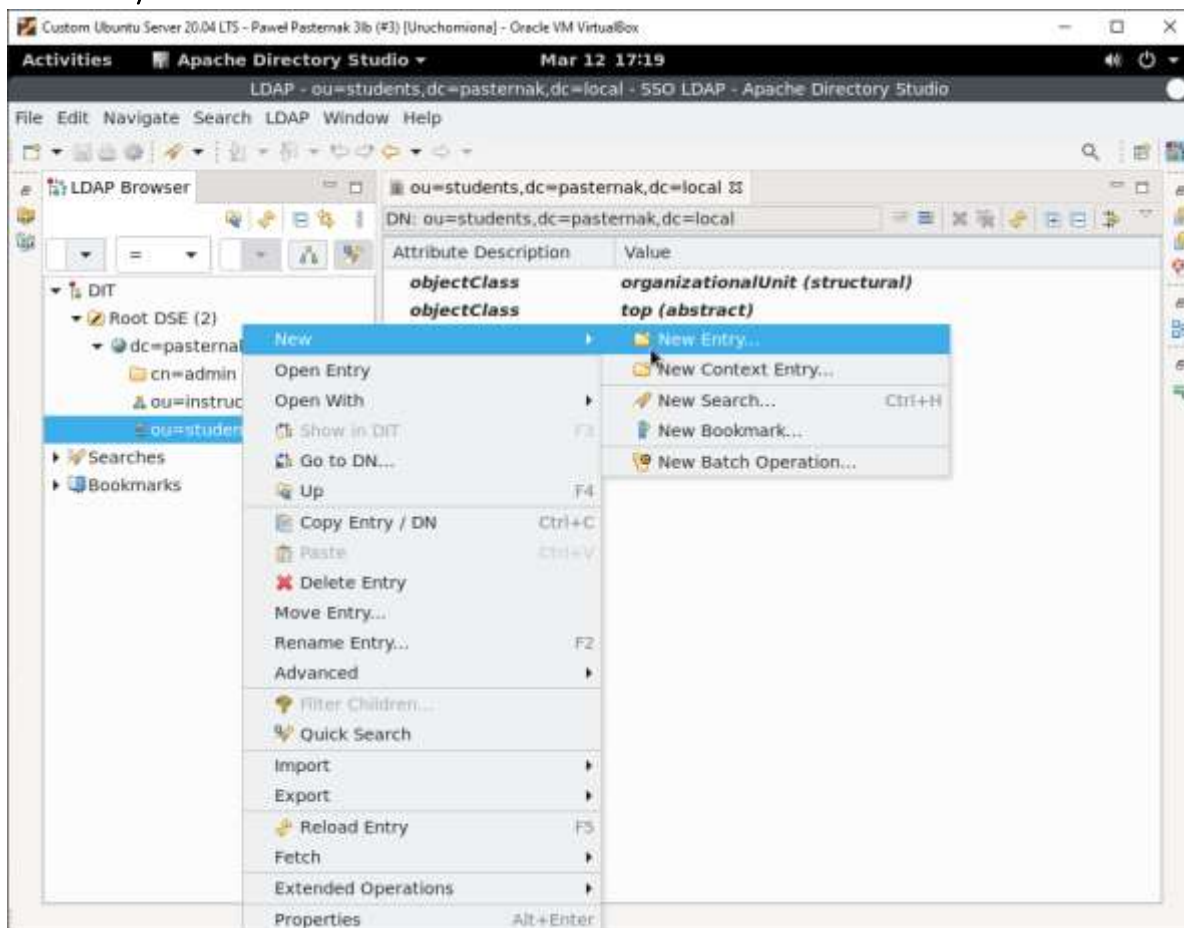
Zrzut Ekranu 29 - dodanie atrybutu

Paweł Pasternak 31b - LDAP

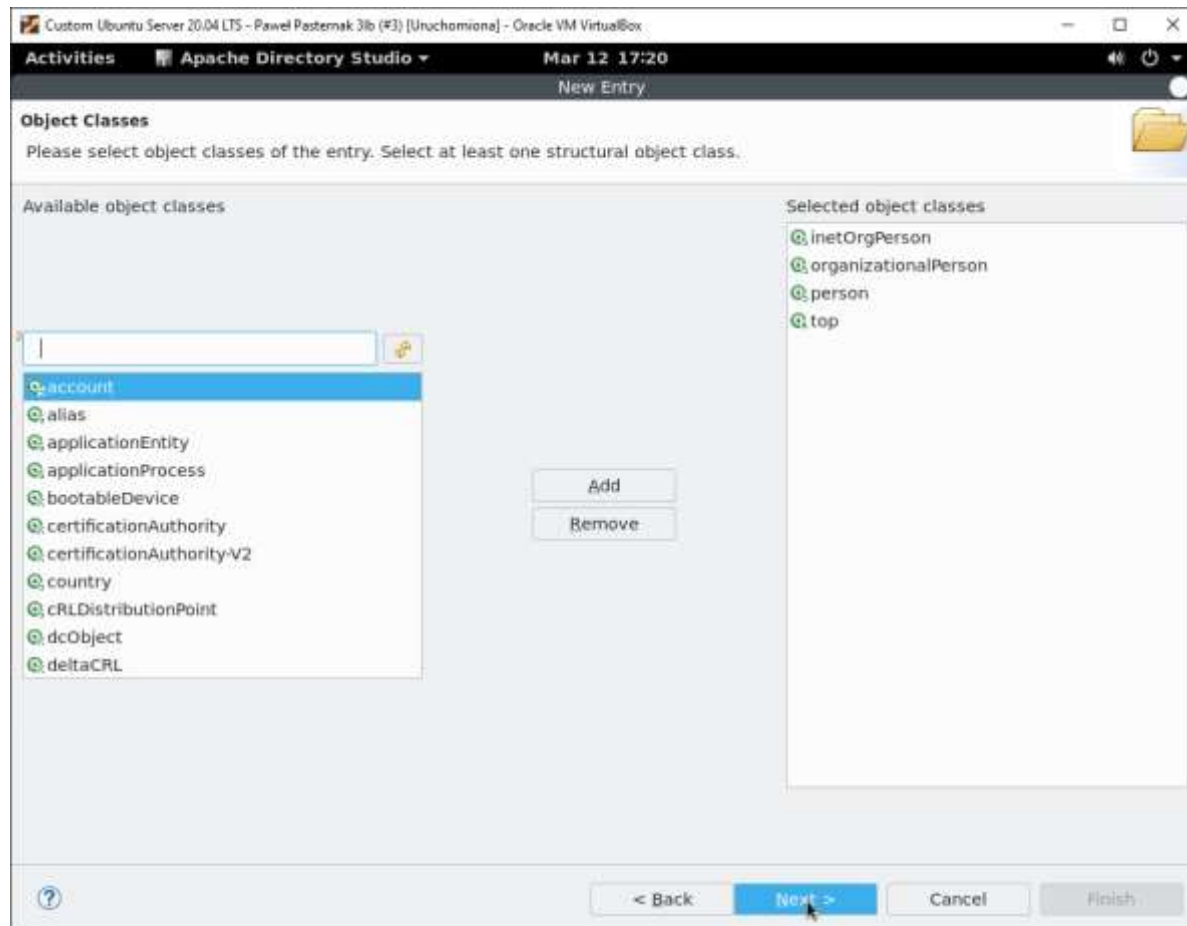


Zrzut Ekranu 30 - wyświetlenie wpisu

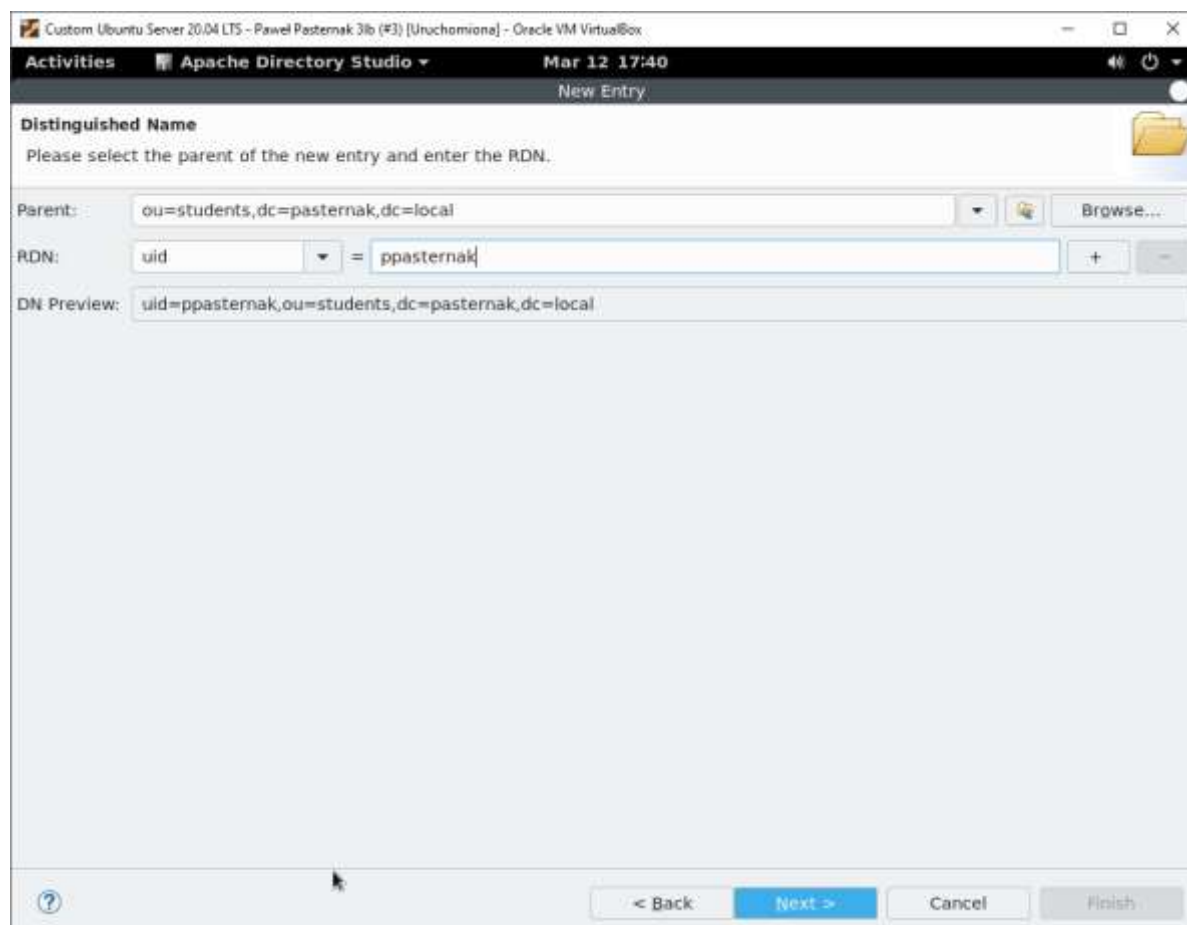
- Użytkownika



Zrzut Ekranu 31 - dodawanie nowego wpisu

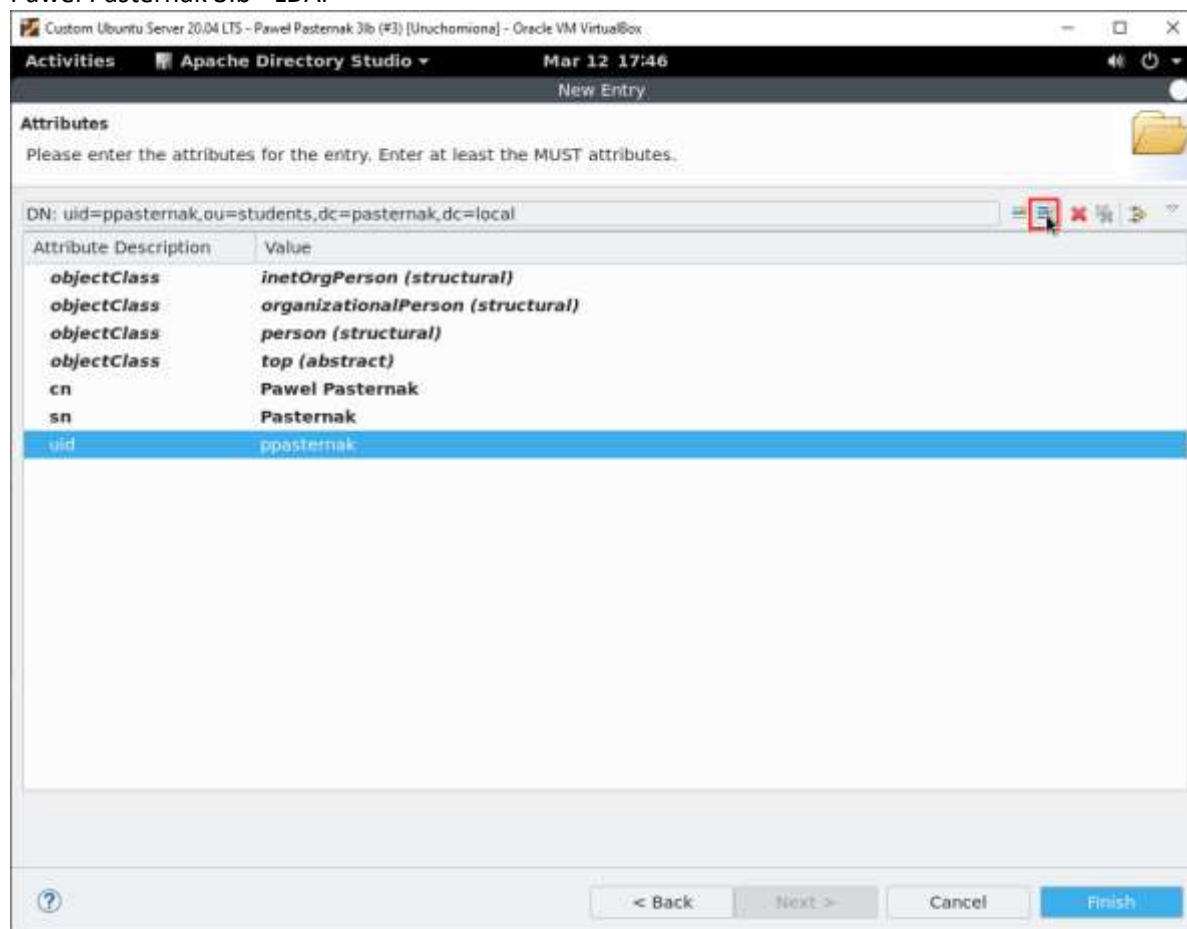


Zrzut Ekranu 32 - dodanie klas atrybutów



Zrzut Ekranu 33 - dodanie atrybutu dla nazwy

Paweł Pasternak 31b - LDAP



Custom Ubuntu Server 20.04 LTS - Paweł Pasternak 31b (#3) [Unuchomiona] - Oracle VM VirtualBox

Activities Apache Directory Studio Mar 12 17:46

New Entry

Attributes

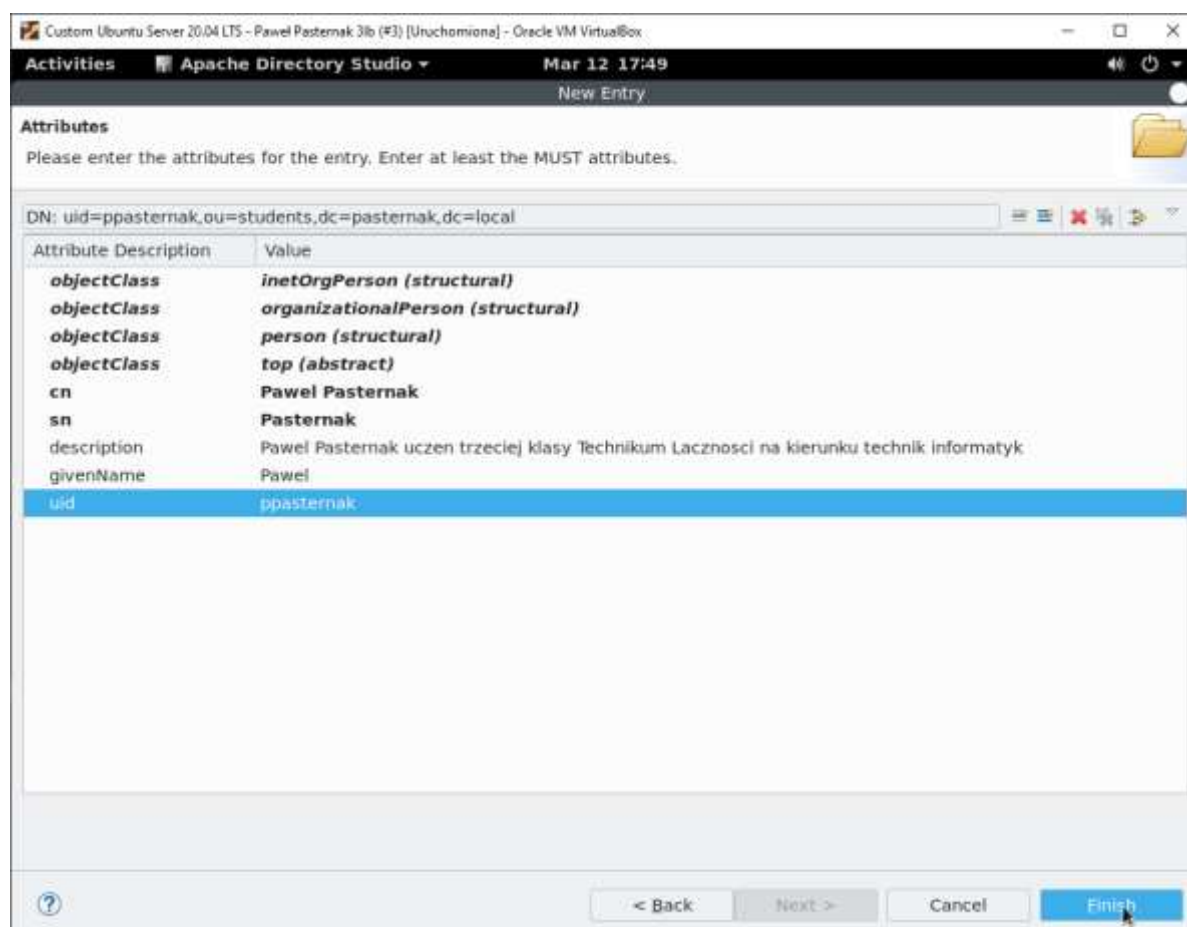
Please enter the attributes for the entry. Enter at least the MUST attributes.

DN: uid=ppasternak,ou=students,dc=pasternak,dc=local

Attribute Description	Value
objectClass	inetOrgPerson (structural)
objectClass	organizationalPerson (structural)
objectClass	person (structural)
objectClass	top (abstract)
cn	Paweł Pasternak
sn	Pasternak
uid	ppasternak

< Back Next > Cancel Finish

Zrzut Ekranu 34 - dodanie pozostałych atrybutów



Custom Ubuntu Server 20.04 LTS - Paweł Pasternak 31b (#3) [Unuchomiona] - Oracle VM VirtualBox

Activities Apache Directory Studio Mar 12 17:49

New Entry

Attributes

Please enter the attributes for the entry. Enter at least the MUST attributes.

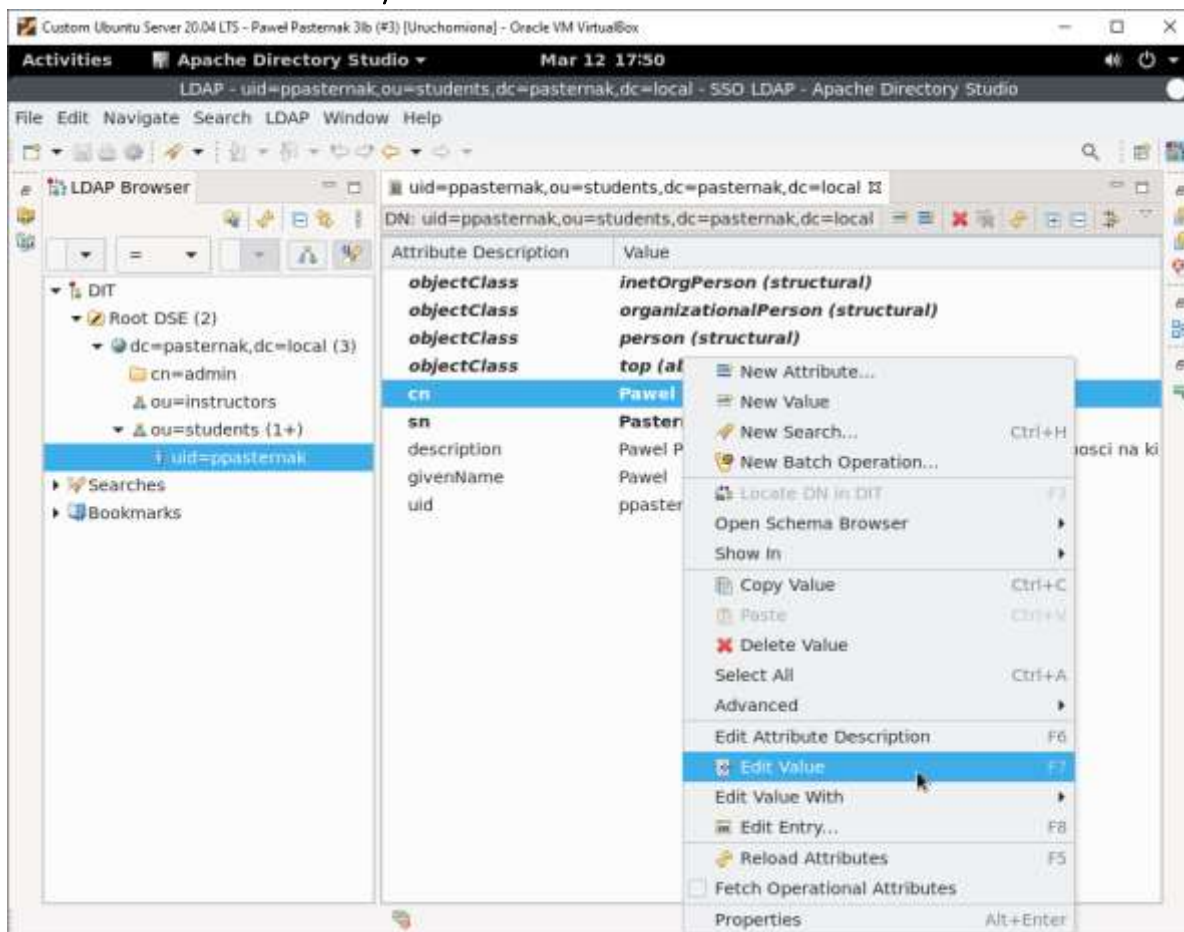
DN: uid=ppasternak,ou=students,dc=pasternak,dc=local

Attribute Description	Value
objectClass	inetOrgPerson (structural)
objectClass	organizationalPerson (structural)
objectClass	person (structural)
objectClass	top (abstract)
cn	Paweł Pasternak
sn	Pasternak
description	Paweł Pasternak uczeń trzeciej klasy Technikum Łączności na kierunku technik Informatyk
givenName	Paweł
uid	ppasternak

< Back Next > Cancel Finish

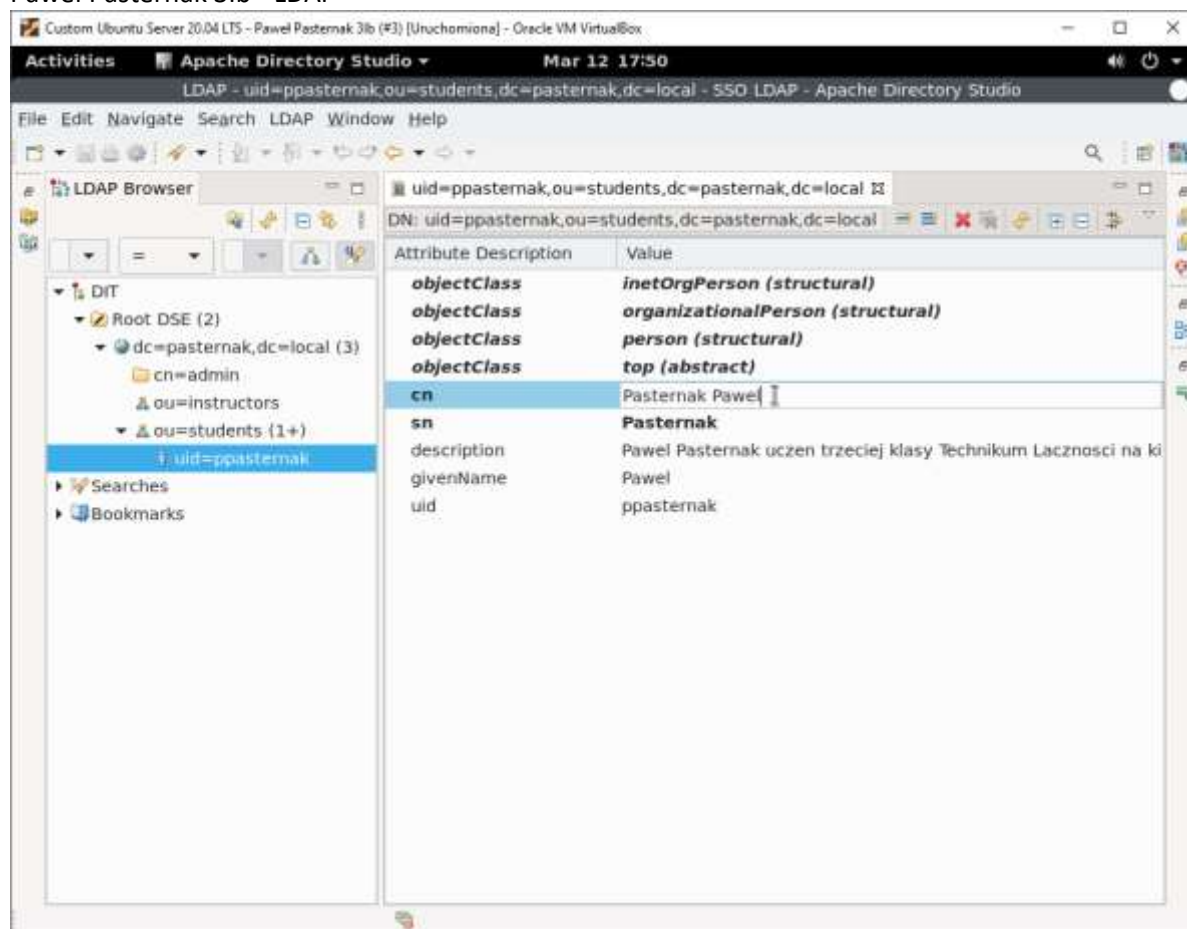
Zrzut Ekranu 35 - dodanie pozostałych atrybutów

- Zmianianie wartości atrybutów



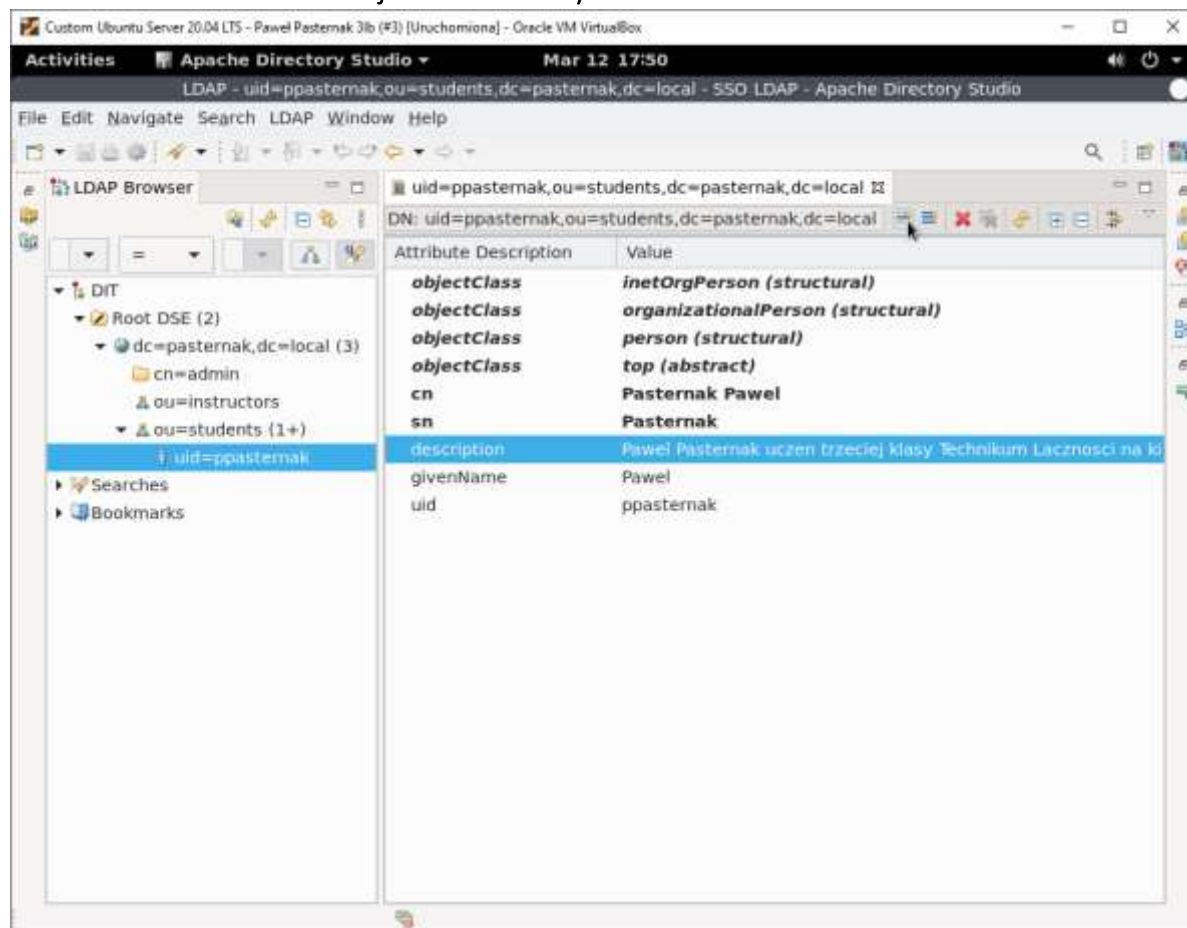
Zrzut Ekranu 36 - zmienianie wartości wpisu

Paweł Pasternak 31b - LDAP



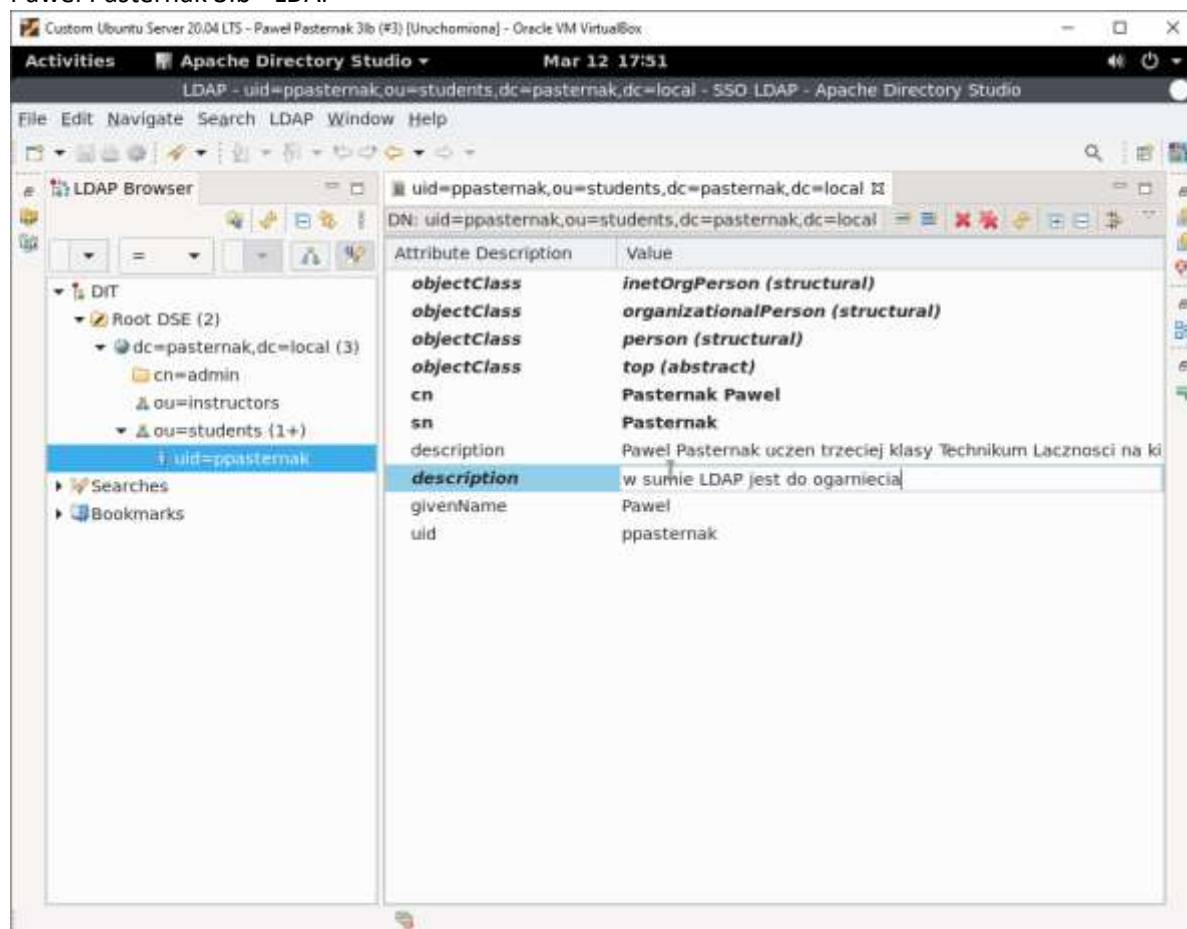
Zrzut Ekranu 37 - zmienianie wartości atrybutu poprzez dwukrotne kliknięcie na niego

- Dodawanie dodatkowej wartości dla atrybutu



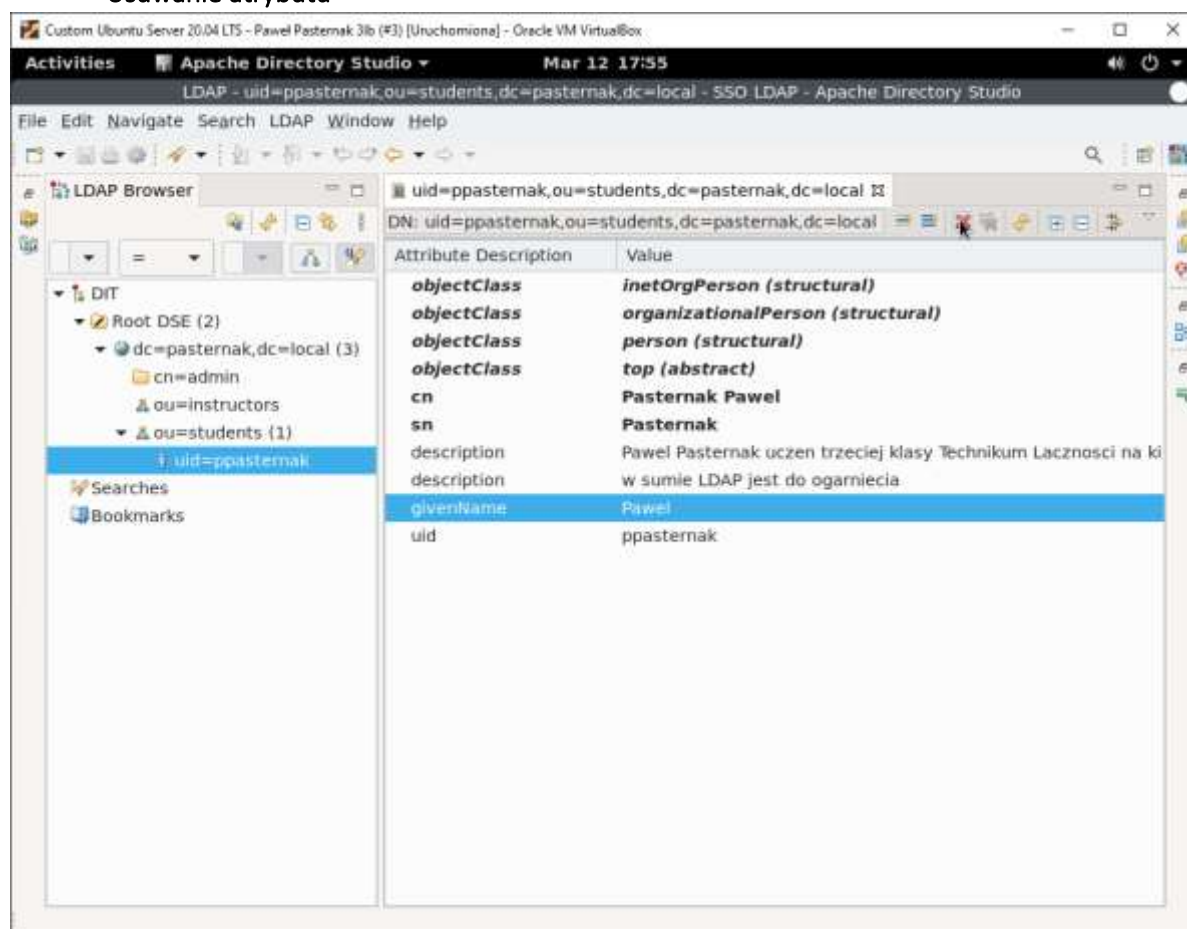
Zrzut Ekranu 38 - jak w nagłówku

Paweł Pasternak 31b - LDAP



Zrzut Ekranu 39 - jak wyżej

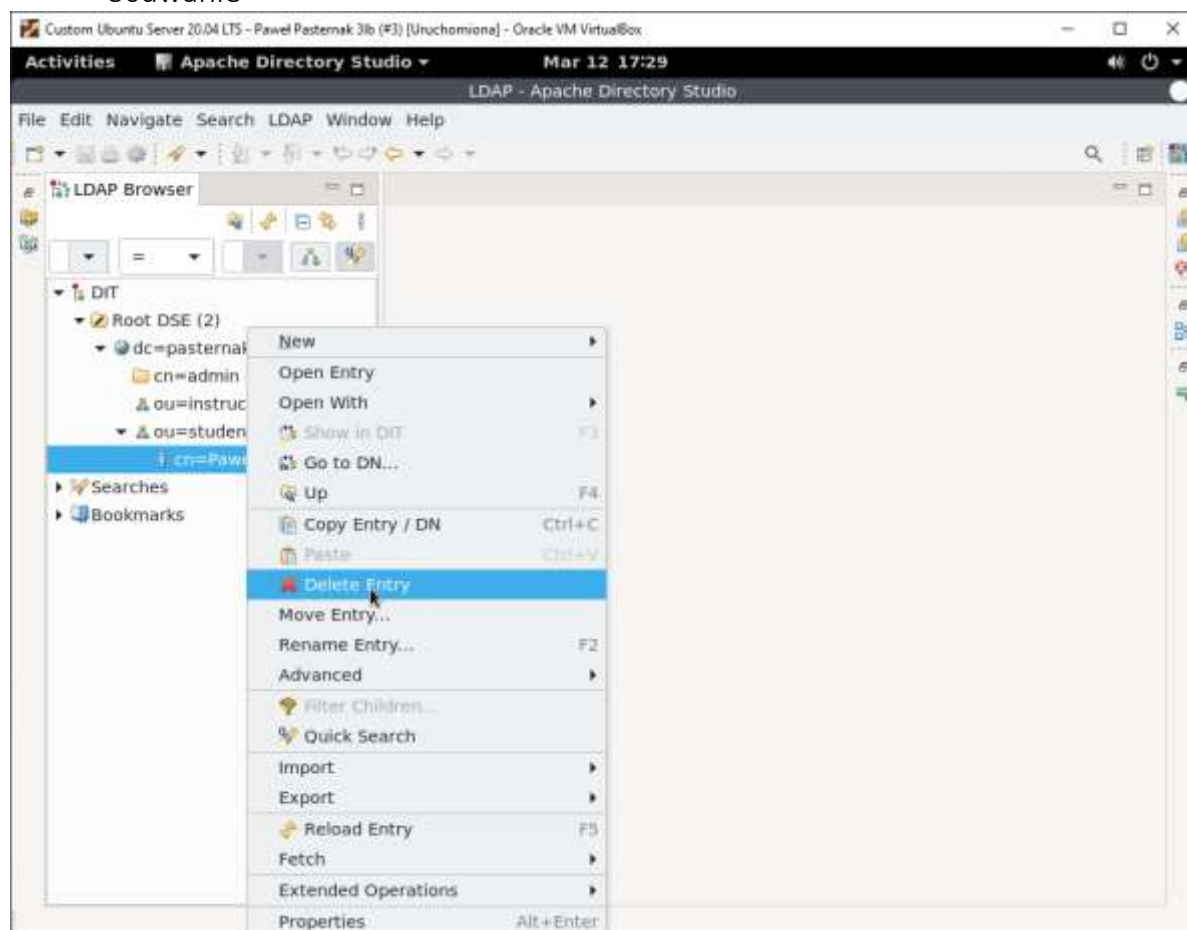
- Usuwanie atrybutu



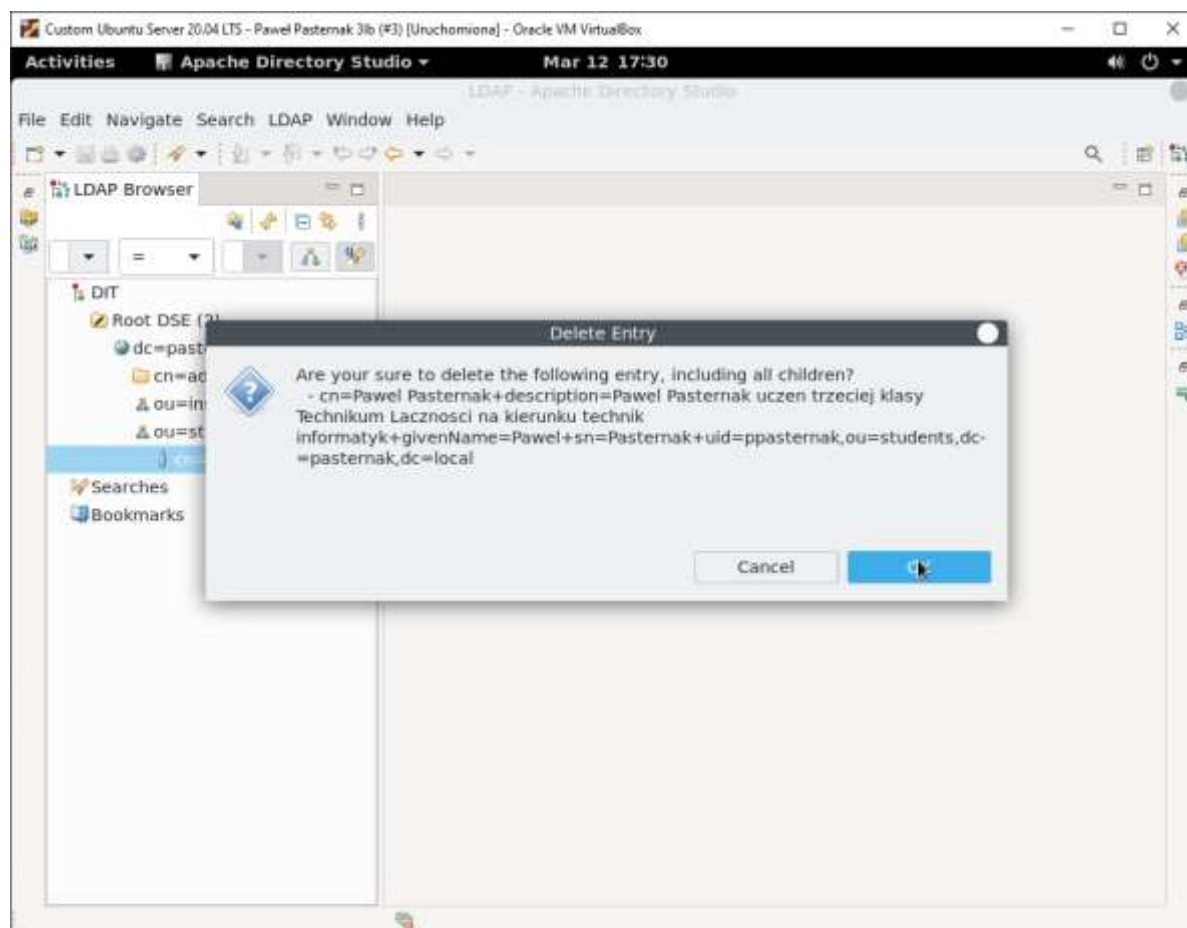
Zrzut Ekranu 40 - usuwanie atrybutu

Paweł Pasternak 31b - LDAP

Usuwanie

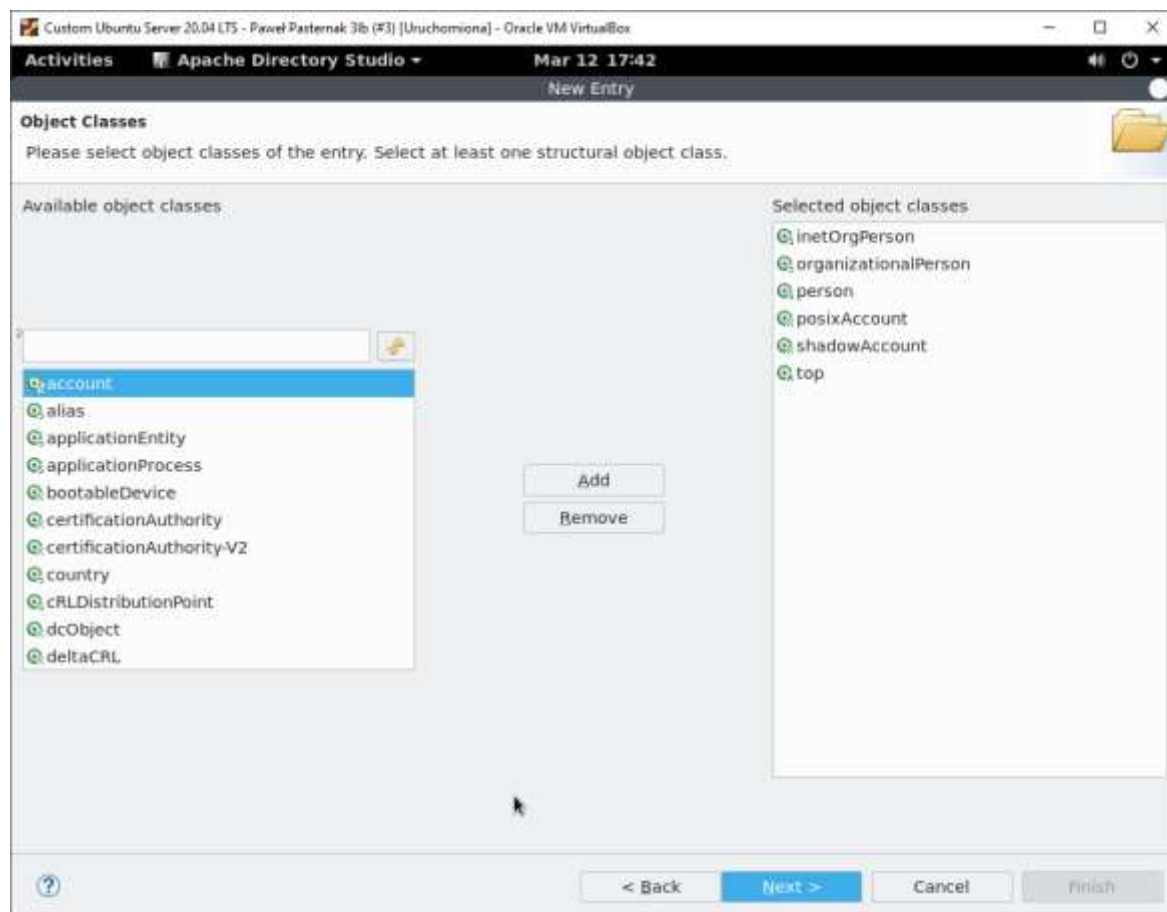


Zrzut Ekranu 41 - usuwanie wpisu

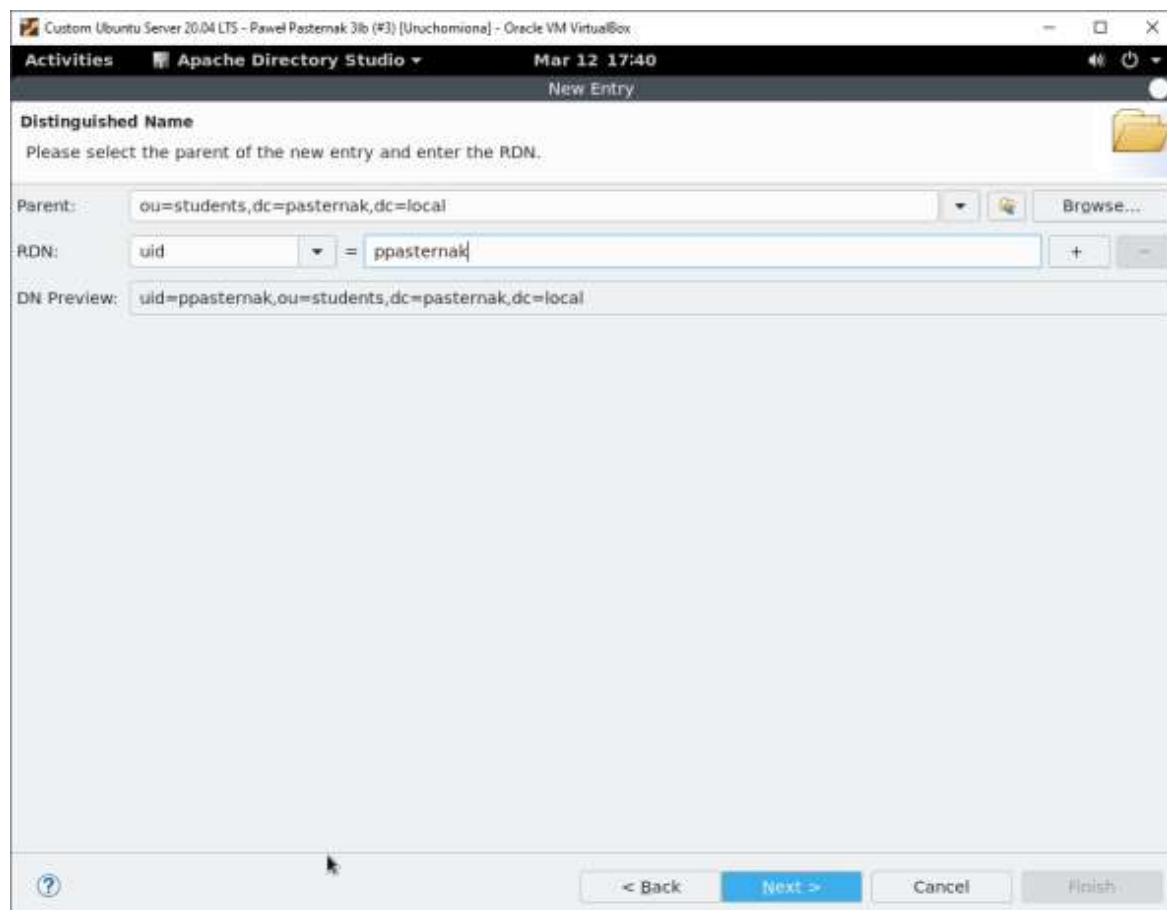


Zrzut Ekranu 42 - potwierdzenie naszych działań

3. Utworzenie użytkownika w standardzie POSIX i wyświetlenie go.



Zrzut Ekranu 43 - dodanie klas atrybutów



Zrzut Ekranu 44 - dodanie atrybutu dla nazwy

Paweł Pasternak 3lb - LDAP

Custom Ubuntu Server 20.04 LTS - Paweł Pasternak 3lb (#3) [Unuchomiona] - Oracle VM VirtualBox

Activities Apache Directory Studio Mar 12 17:42

New Entry

Attributes

Please enter the attributes for the entry. Enter at least the MUST attributes.

DN: uid=ppasternak,ou=students,dc=pasternak,dc=local

Attribute Description	Value
objectClass	inetOrgPerson (structural)
objectClass	organizationalPerson (structural)
objectClass	person (structural)
objectClass	posixAccount (auxiliary)
objectClass	shadowAccount (auxiliary)
objectClass	top (abstract)
cn	Paweł Pasternak
gidNumber	11000
homeDirectory	/home/ppasternak
sn	Pasternak
uid	ppasternak
uidNumber	11000
loginShell	/bin/sh

< Back Next > Cancel Finish

Zrzut Ekranu 45 - dodanie pozostałych atrybutów

Custom Ubuntu Server 20.04 LTS - Paweł Pasternak 3lb (#3) [Unuchomiona] - Oracle VM VirtualBox

Activities Apache Directory Studio Mar 12 17:43

LDAP - uid=ppasternak,ou=students,dc=pasternak,dc=local - SSO LDAP - Apache Directory Studio

File Edit Navigate Search LDAP Window Help

LDAP Browser

- Root DSE (2)
 - dc=pasternak,dc=local (3)
 - cn=admin
 - ou=instructors
 - ou=students (1+)
 - uid=ppasternak

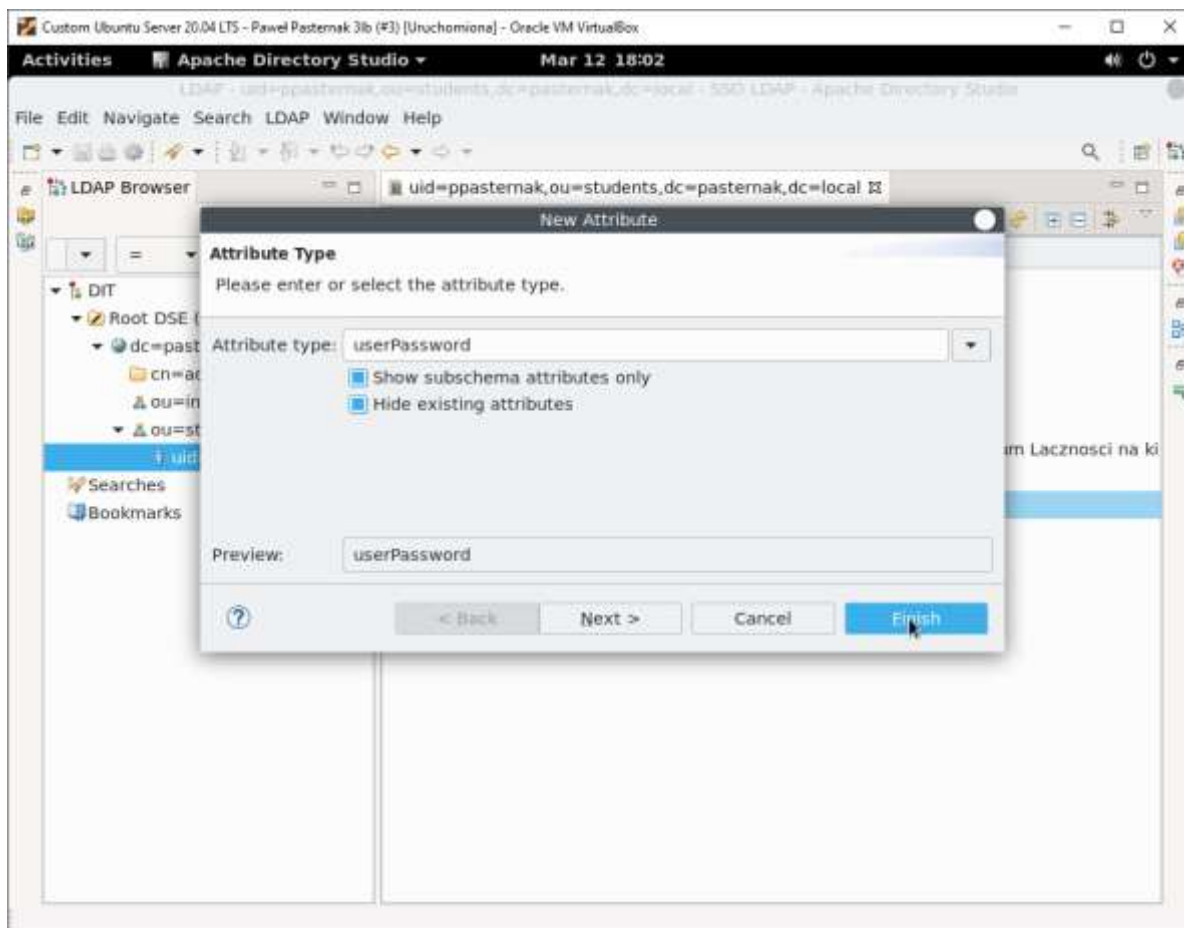
DN: uid=ppasternak,ou=students,dc=pasternak,dc=local

Attribute Description	Value
objectClass	inetOrgPerson (structural)
objectClass	organizationalPerson (structural)
objectClass	person (structural)
objectClass	posixAccount (auxiliary)
objectClass	shadowAccount (auxiliary)
objectClass	top (abstract)
cn	Paweł Pasternak
gidNumber	11000
homeDirectory	/home/ppasternak
sn	Pasternak
uid	ppasternak
uidNumber	11000
loginShell	/bin/sh

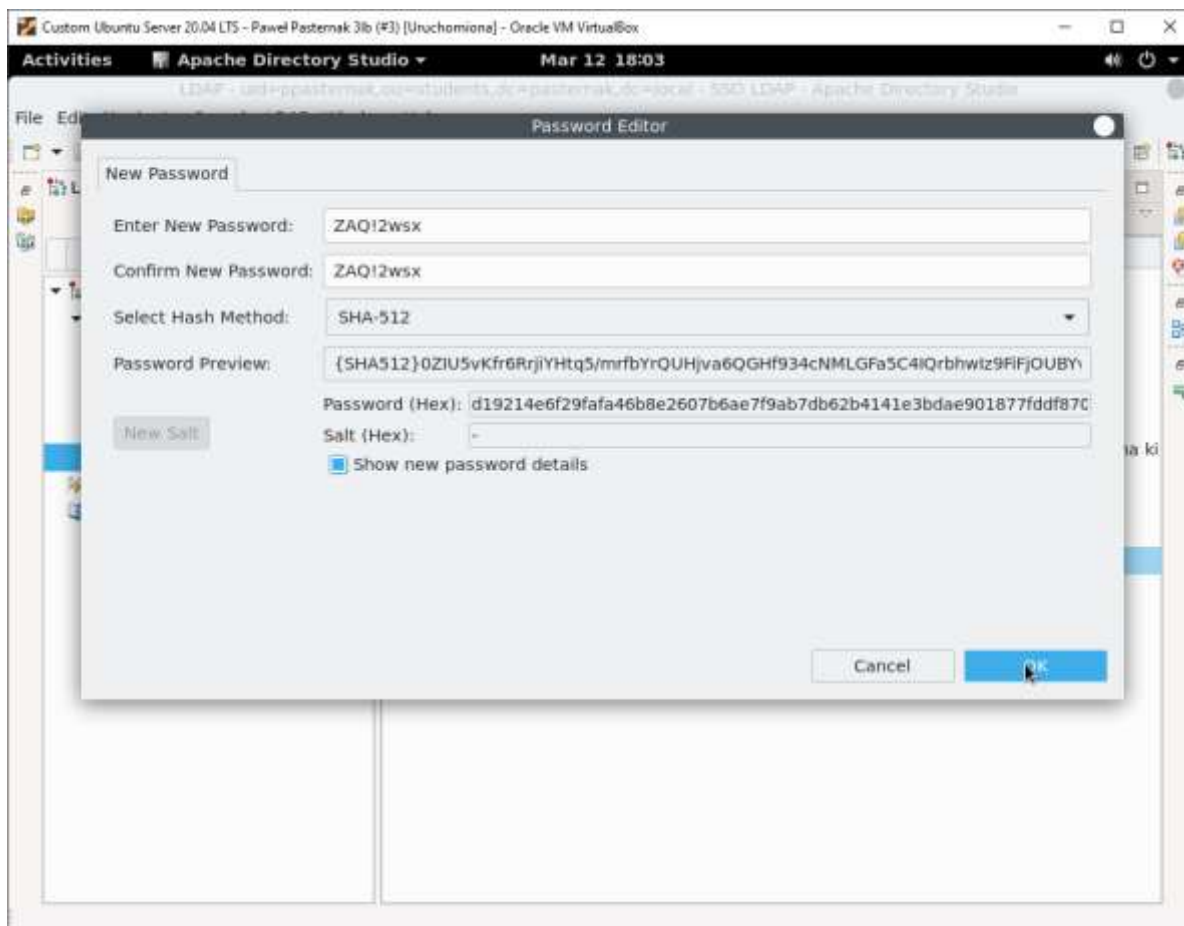
Zrzut Ekranu 46 - wyświetlenie wpisu

Paweł Pasternak 31b - LDAP

Dodanie hasła

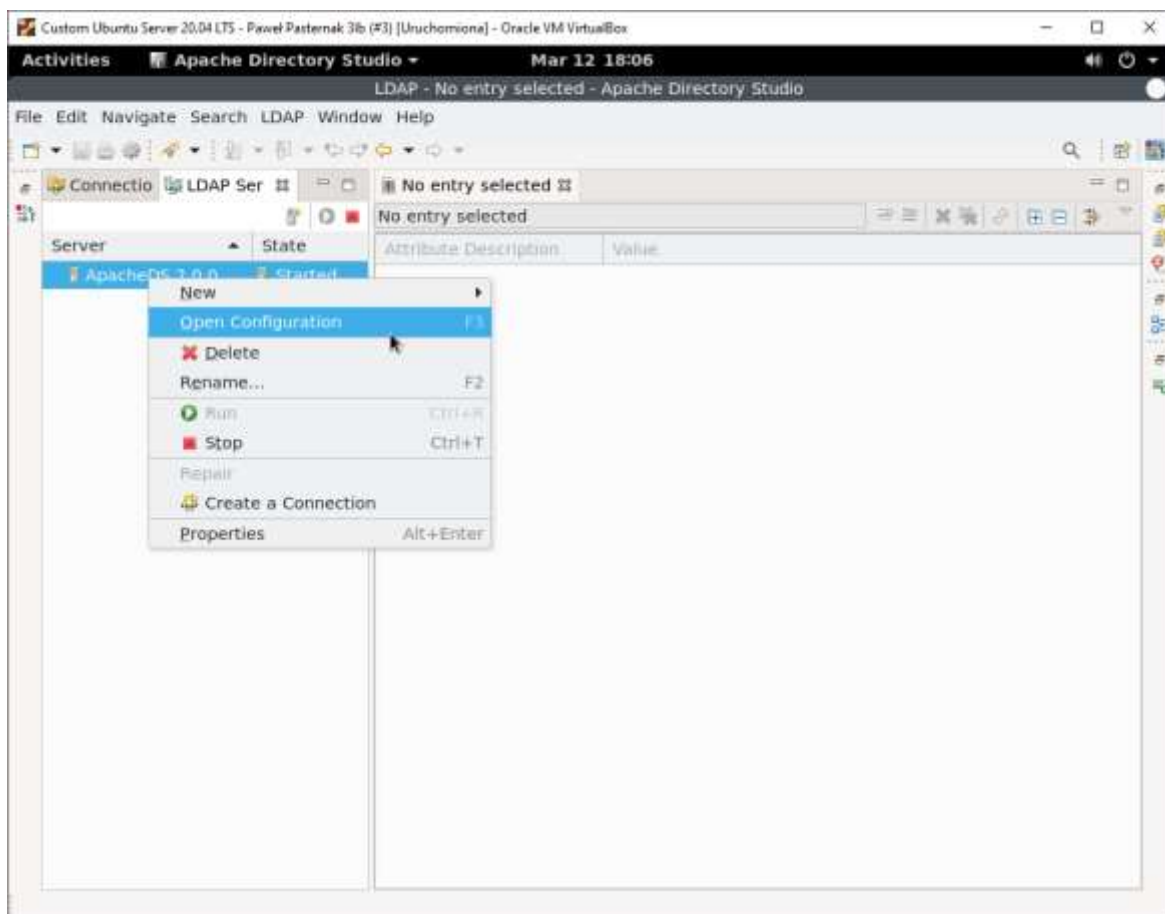


Zrzut Ekranu 47 - dodanie hasła

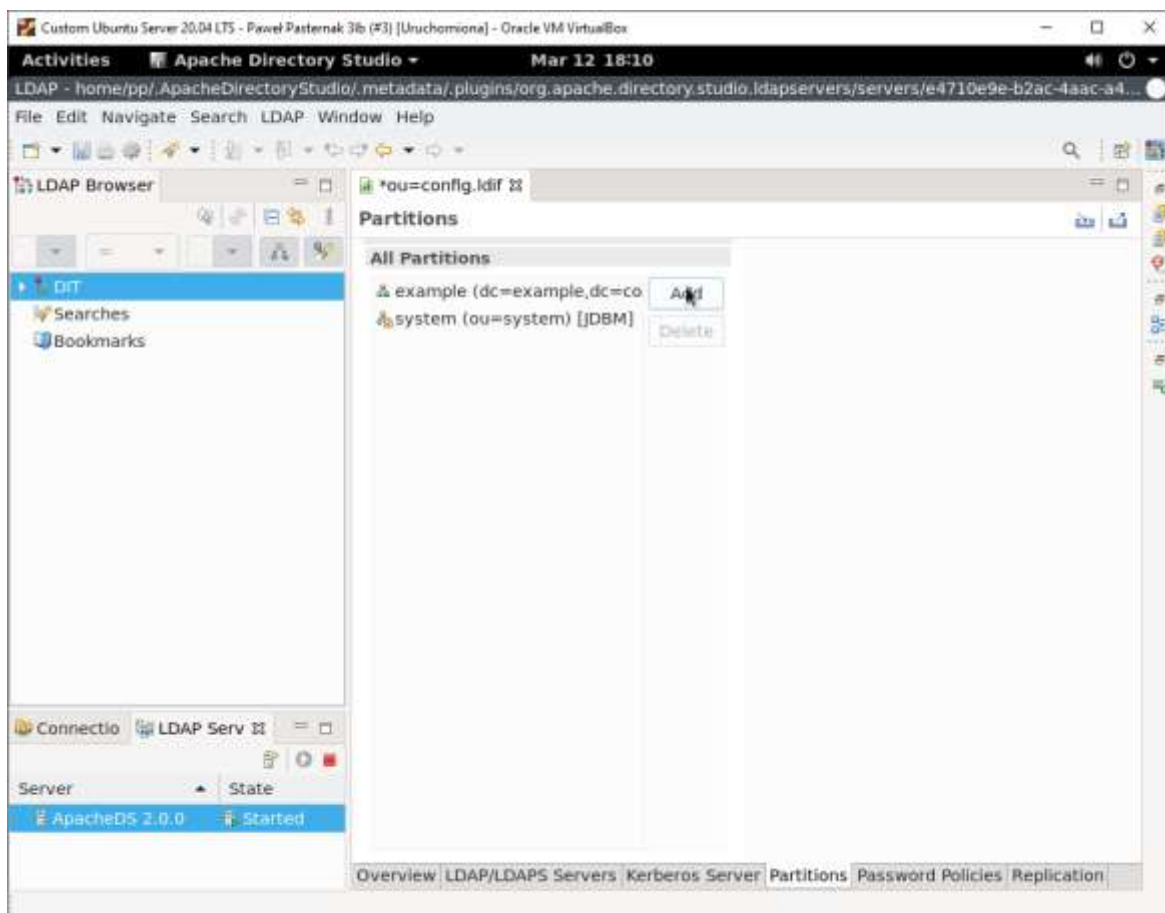


Zrzut Ekranu 48 - ustawienie hasła i metody hashowania

4. Dodatkowa konfiguracja: tworzenie dodatkowej domeny



Zrzut Ekranu 49 - otworenie panelu konfiguracyjnego serwera ApacheDS



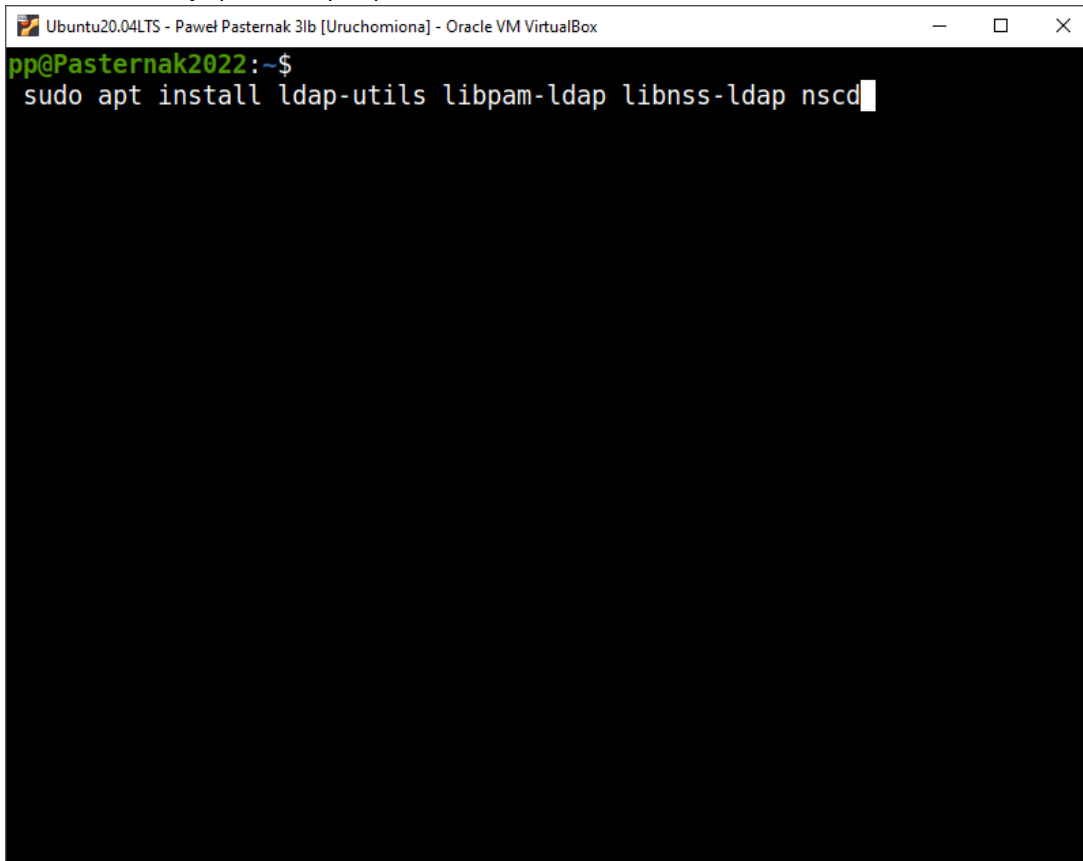
Zrzut Ekranu 50 - Dodanie nowej domeny

Część IV – Zastosowanie w praktyce

1. Logowanie do systemu za pomocą kont LDAP:

Przygotowanie: klienta (Linux)

- Instalacja potrzebnych paczek

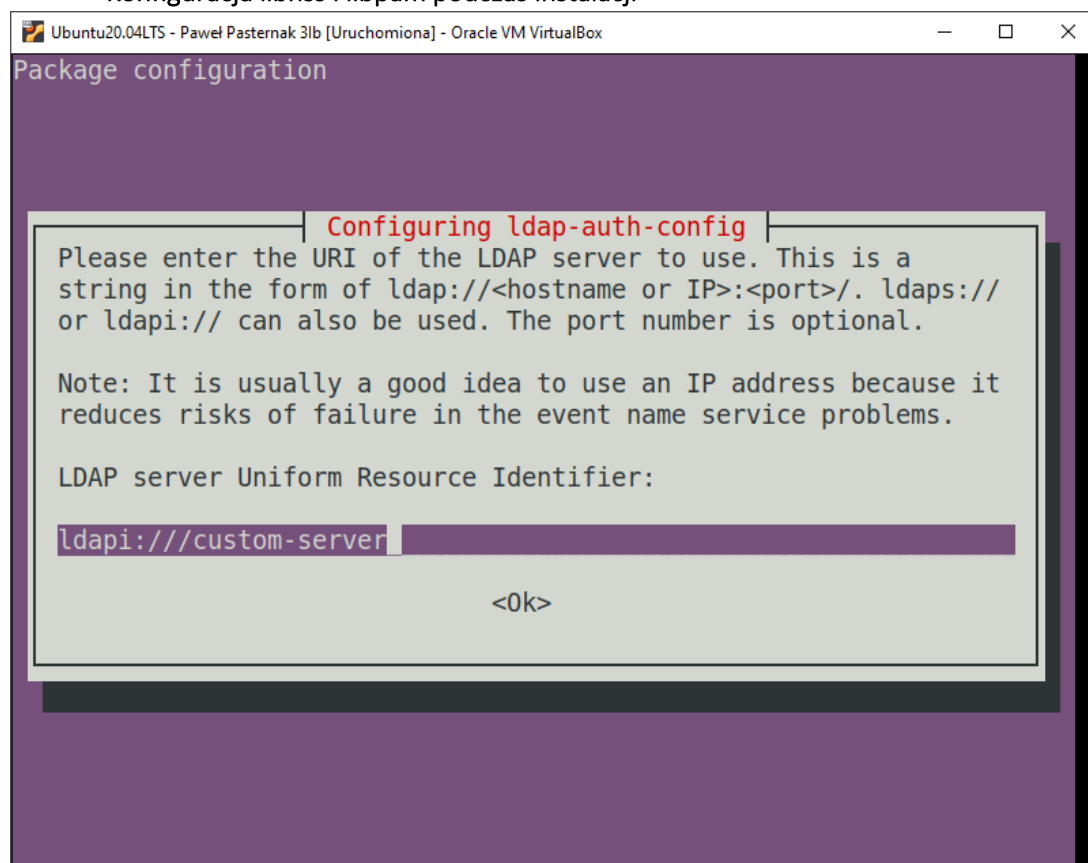


The screenshot shows a terminal window titled "Ubuntu20.04LTS - Paweł Pasternak 31b [Uruchomiona] - Oracle VM VirtualBox". The prompt is "pp@Pasternak2022:~\$". The command entered is "sudo apt install ldap-utils libpam-ldap libnss-ldap nscd".

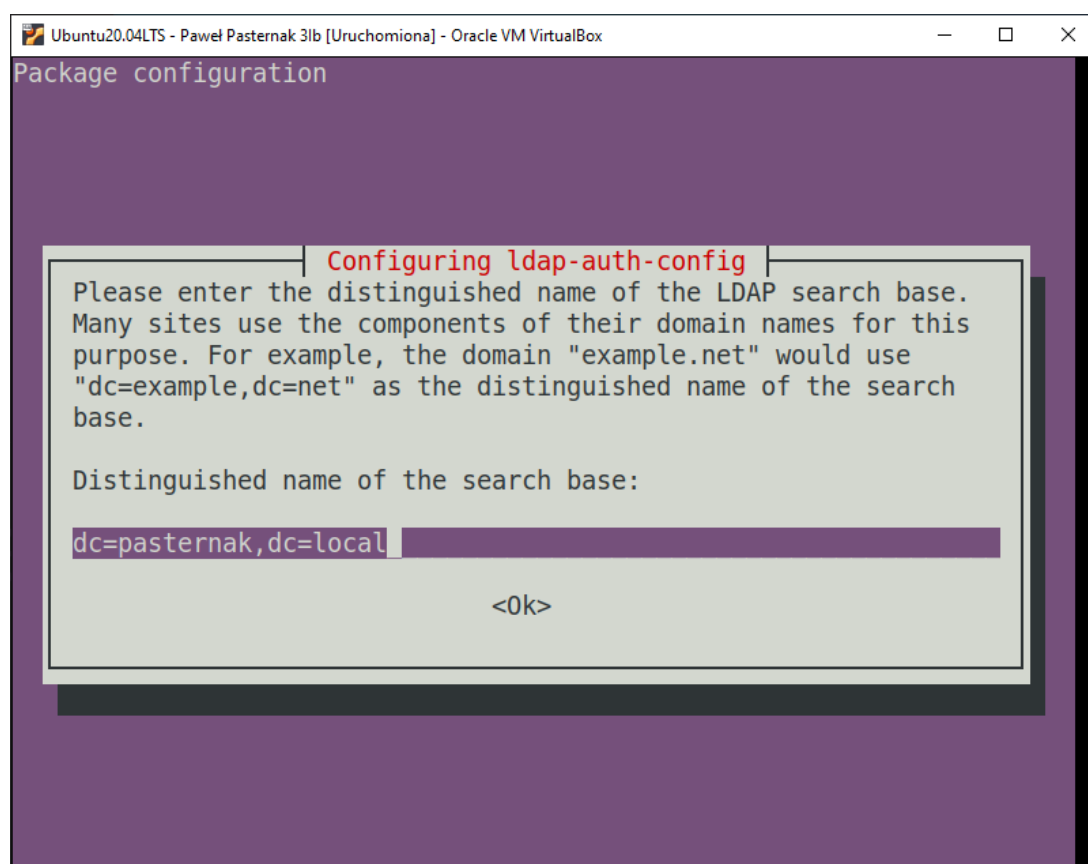
```
pp@Pasternak2022:~$ sudo apt install ldap-utils libpam-ldap libnss-ldap nscd
```

Zrzut Ekranu 51 - instalacja potrzebnych pakietów do uwierzytelniania na kliencie

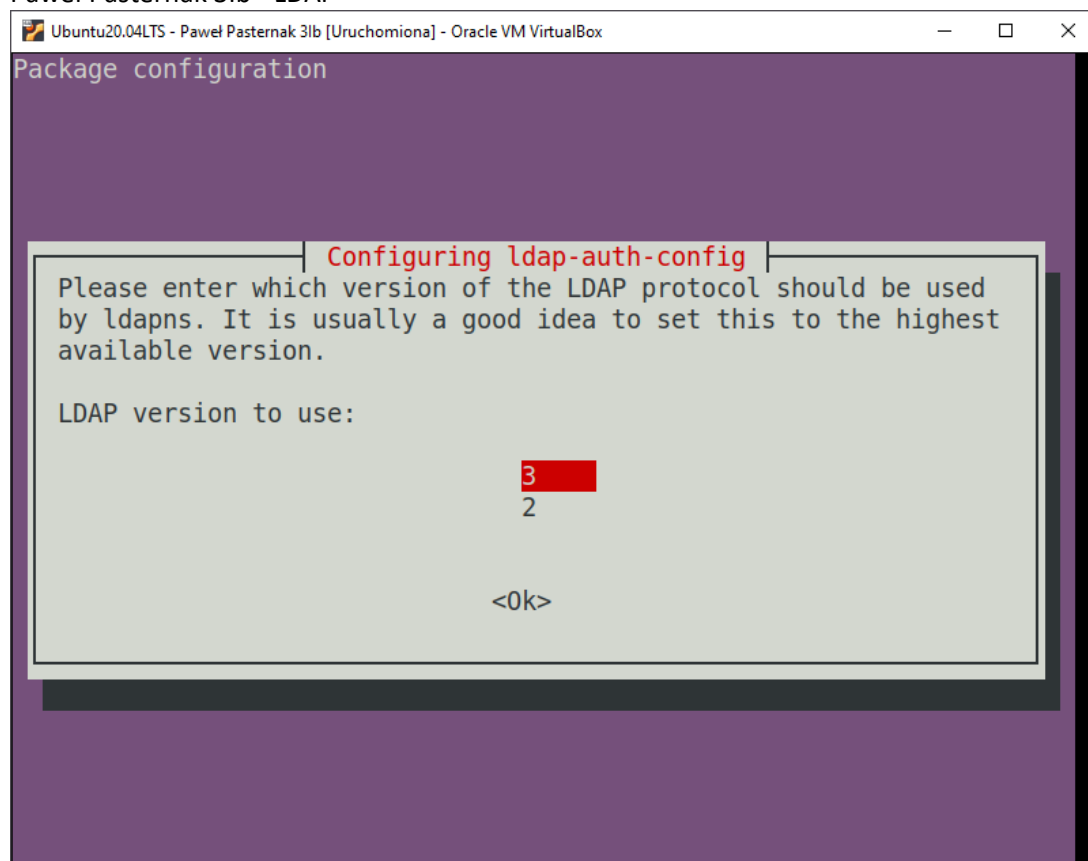
- Konfiguracja libnss i libpam podczas instalacji



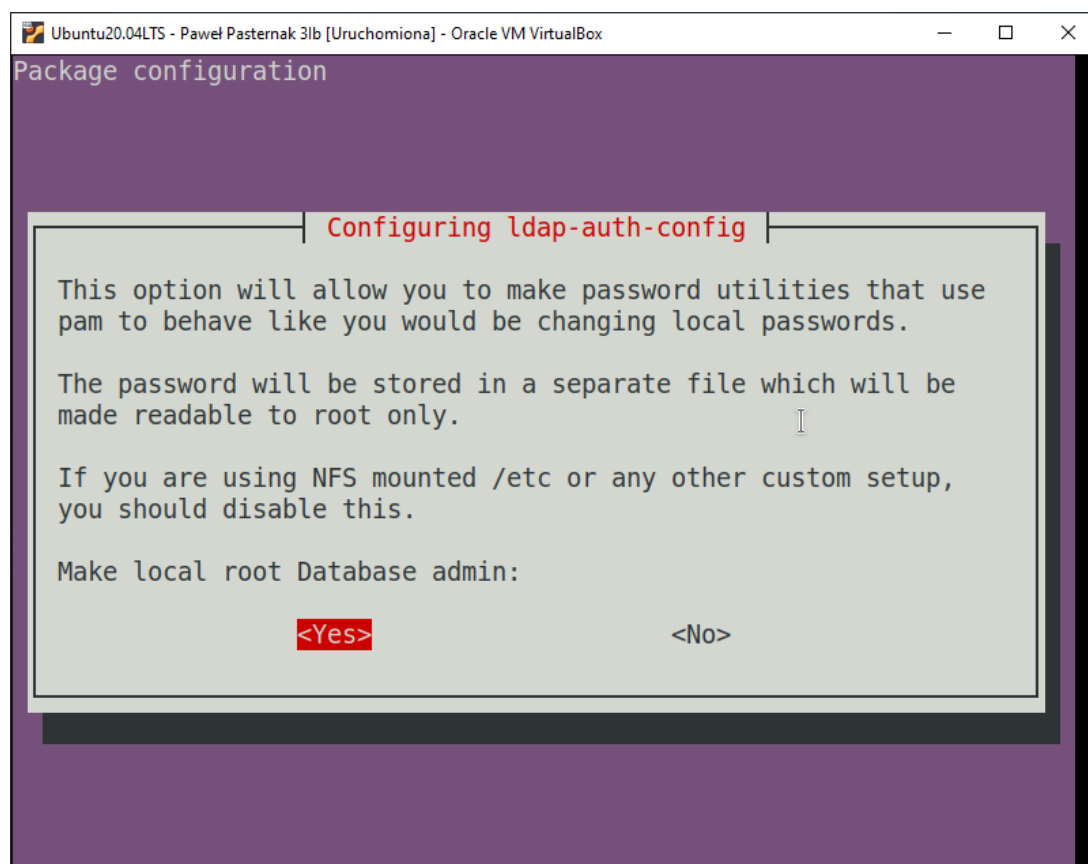
Zrzut Ekranu 52 - wprowadzenie nazwy serwera LDAP



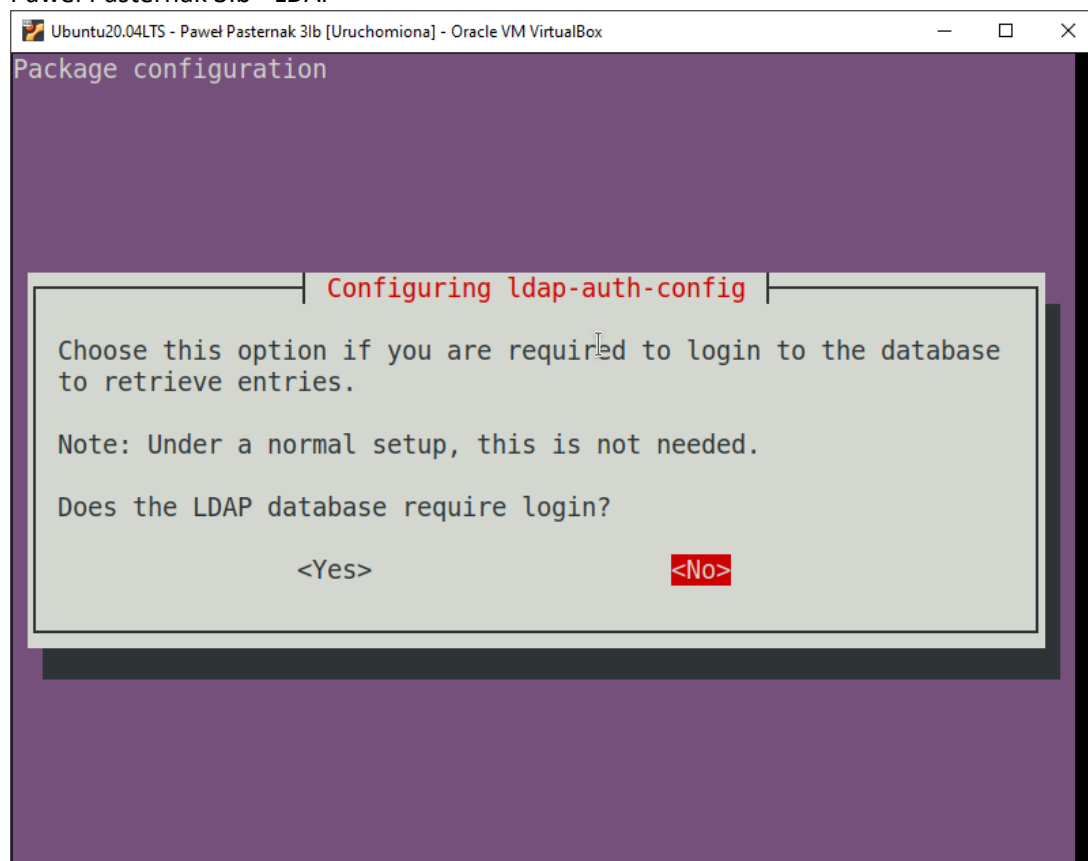
Zrzut Ekranu 53 - wprowadzeni dn serwera LDAP



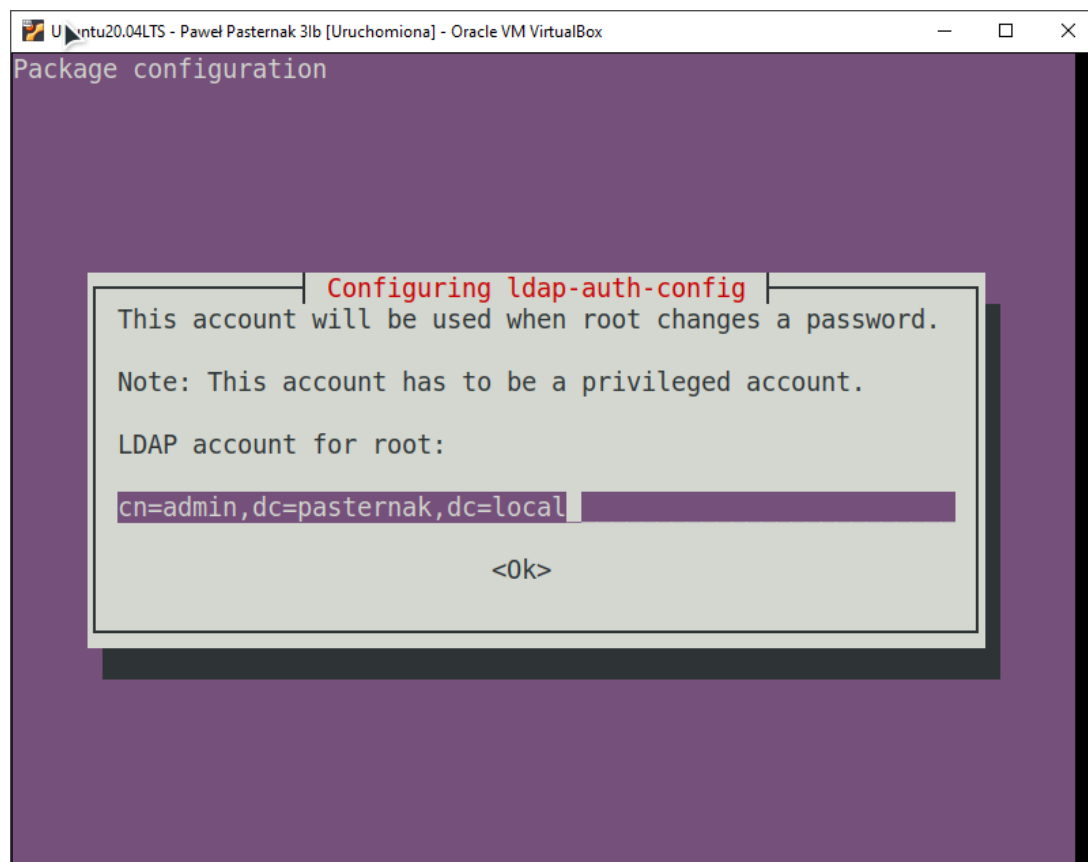
Zrzut Ekranu 54 - ustawienie wykorzystywanej wersji LDAP

Zrzut Ekranu 55 - umożliwienie zmieniania hasła dla użytkowników LDAP za pomocą linuxowych poleceń, np. *passwd*

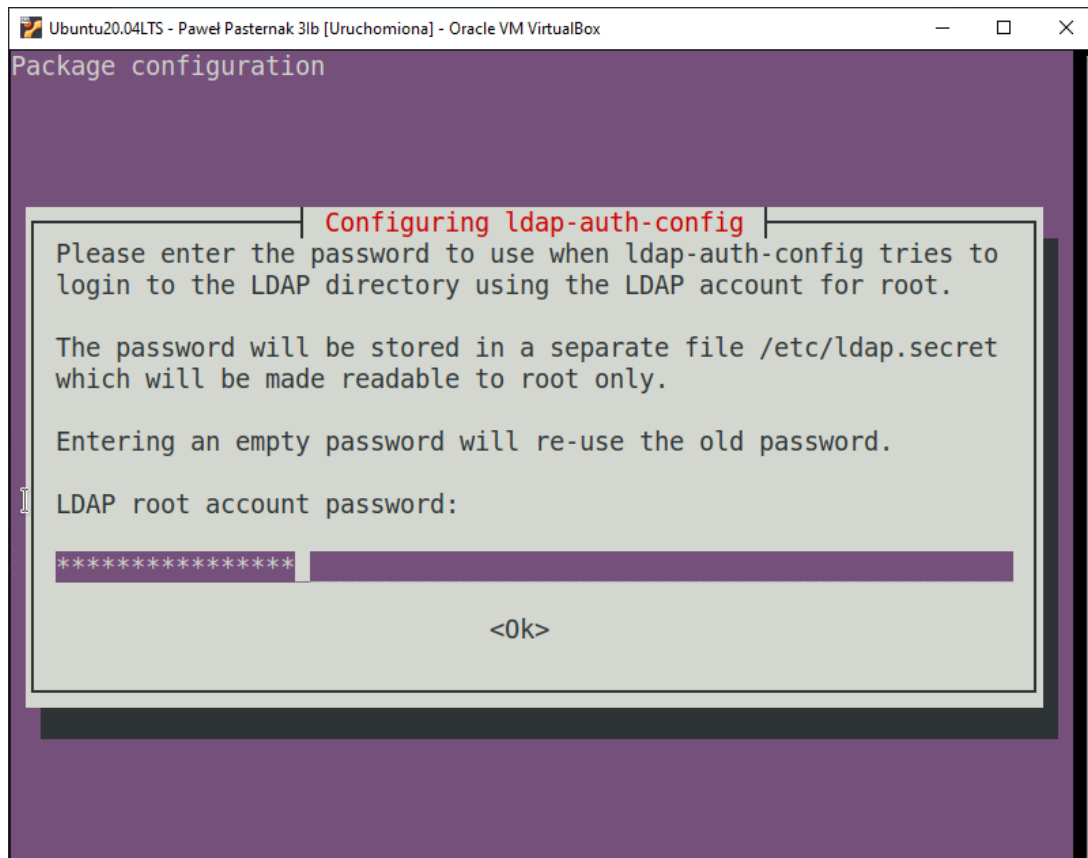
Paweł Pasternak 3lb - LDAP



Zrzut Ekranu 56 - ustawienie czy serwera potrzebuje hasła do odczytu wpisów

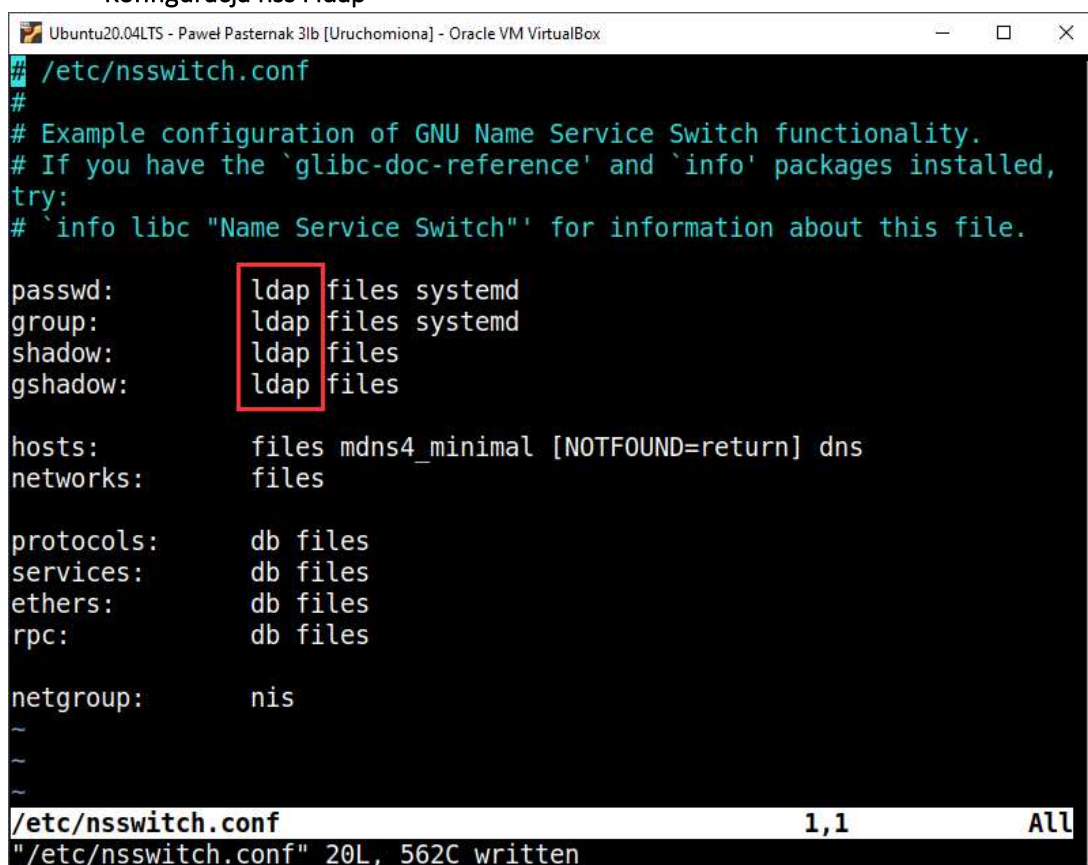


Zrzut Ekranu 57 - wprowadzenie nazwy administratora, do użycia w przypadku zmiany hasła



Zrzut Ekranu 58 - podanie hasła administratora LDAP

- Konfiguracja nss i ldap



Zrzut Ekranu 59 - dodanie ustawień, umożliwiających autoryzację za pomocą kont LDAP, do pliku /etc/nsswitch.conf

☒ Odnosnik do nss

Paweł Pasternak 3lb - LDAP

```
Ubuntu20.04LTS - Paweł Pasternak 3lb [Uruchomiona] - Oracle VM VirtualBox
#
# LDAP Defaults
#
# See ldap.conf(5) for details
# This file should be world readable but not world writable.

BASE      dc=pasternak,dc=local
URI        ldap://custom-server

#SIZELIMIT      12
#TIMELIMIT      15
#DEREF          never

# TLS certificates (needed for GnuTLS)
TLS_CACERT      /etc/ssl/certs/ca-certificates.crt
~
~
~
~
~
~
/etc/ldap/ldap.conf 17,0-1 All
"/etc/ldap/ldap.conf" 17L, 296C written
```

Zrzut Ekranu 60 - dodanie serwera LDAP w pliku `/etc/ldap/ldap.conf`, dzięki czemu będziemy mogli wykorzystać aplikacje z pakietu `ldap-utils`

- Logowanie 😊

```
Ubuntu20.04LTS - Paweł Pasternak 3lb [Uruchomiona] - Oracle VM VirtualBox
pp@Pasternak2022:~$
su ppasternak
Password:
$ cd
sh: 1: cd: can't cd to /home/ppasternak
$ id
uid=11000(ppasternak) gid=20000(group1) groups=20000(group1)
$
```

Zrzut Ekranu 61 - zalogowanie za pomocą użytkownika LDAP do maszyny, możemy zauważyć, że użytkownik nie posiada folderu domowego.

Najlepszym sposobem na rozwiązanie takiego problemu było by użycie zasobu sieciowego, z folderami domowymi wszystkich użytkowników, przez co moglibyśmy uzyskać coś na kształt mobilnych profili. Do montowania takich folderów moglibyśmy użyć pakietu `aufofs`, który montowałby taki katalog domowy lub moglibyśmy montować cały `/home` dzięki wpisowi w `/etc/fstab`.

Przygotowanie: (Windows)

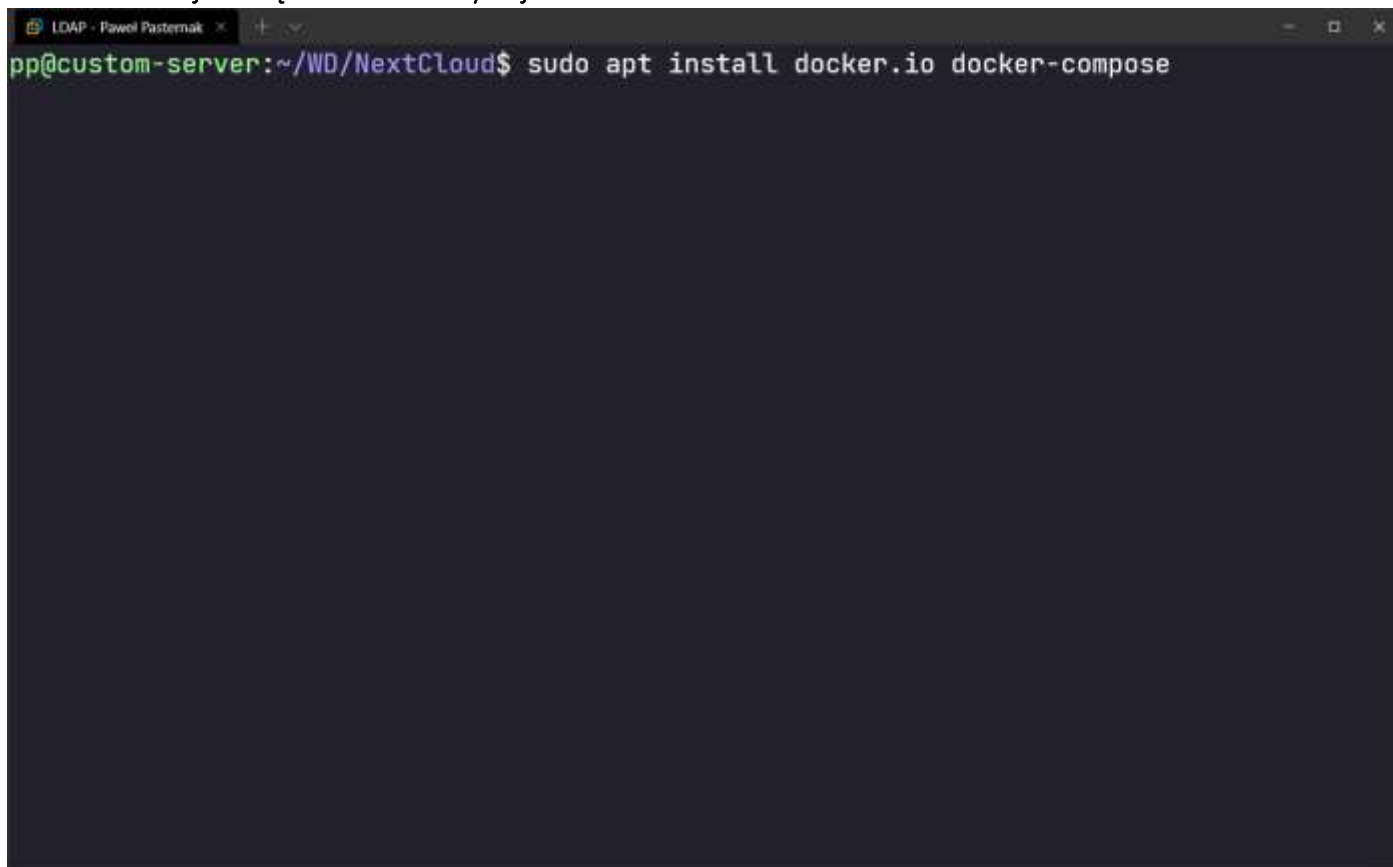
Można to osiągnąć za pomocą Samby w wersji 3, gdzie możemy użyć openLDAP jako backend albo Samby 4 z wbudowanym serwerem LDAP.

Ustawienie czegoś takiego jest znacznie trudniejsze niż w przypadku Linuxa.

2. Logowanie do aplikacji za pomocą integracji z LDAP (na przykładzie Nextcloud).

Przygotowanie i instalacja Nextcloud-a

- Instalacja narzędzi do konteneryzacji

A screenshot of a terminal window with a dark background. The window title is "LDAP - Paweł Pasternak". The prompt is "pp@custom-server:~/WD/NextCloud\$". The command entered is "sudo apt install docker.io docker-compose". The terminal is mostly empty, suggesting the command has been executed and the output is not visible.

```
pp@custom-server:~/WD/NextCloud$ sudo apt install docker.io docker-compose
```

Zrzut Ekranu 62 – instalacja oprogramowanie potrzebnego do konteneryzacji

☒ Odnosnik do konteneryzacji

- Utworzenie pliku docker-compose o treści:

```
# docker-compose.yaml

version: '3.2'

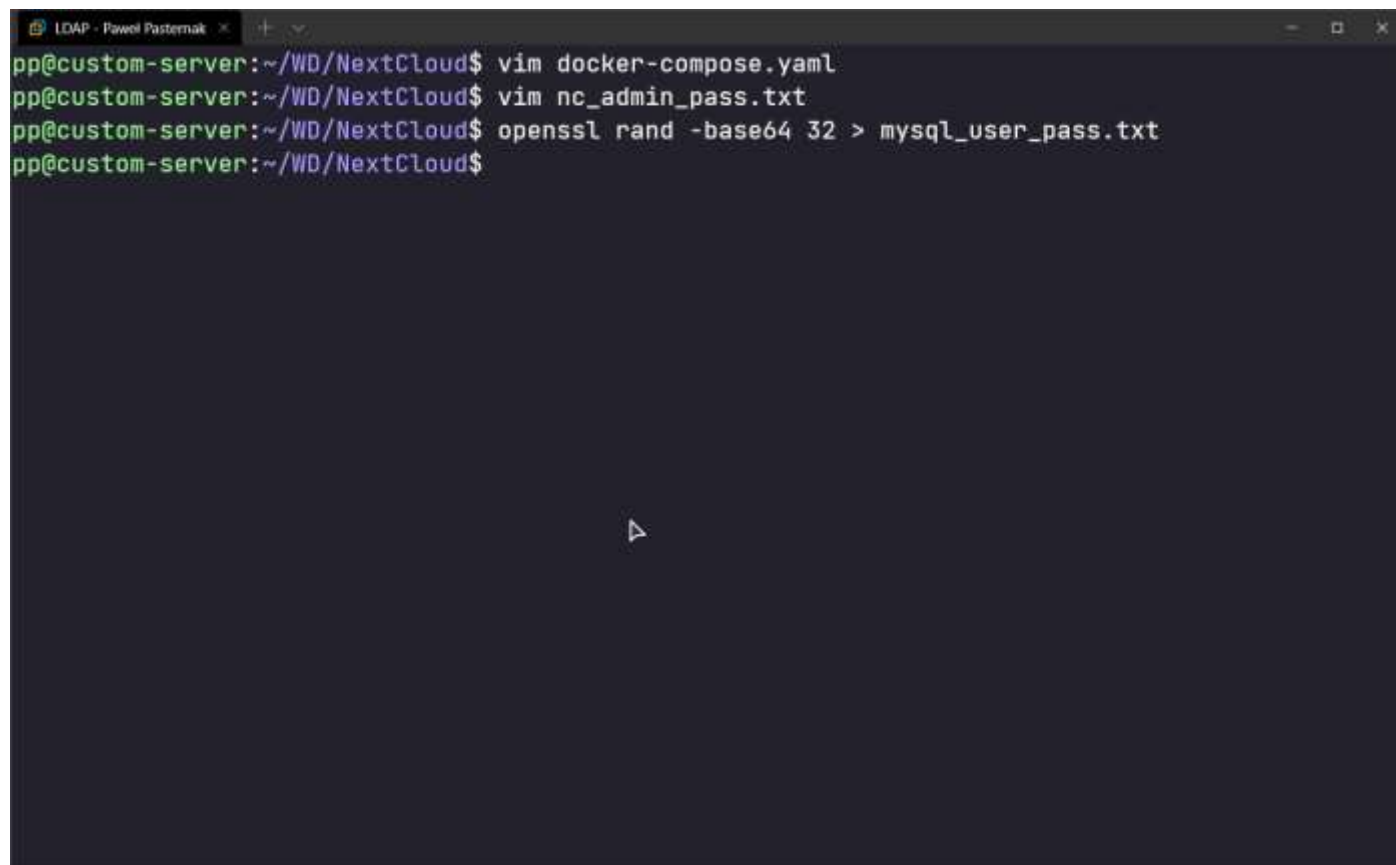
services:
  db:
    image: mariadb
    restart: always
    command: --transaction-isolation=READ-COMMITTED --binlog-format=ROW
    volumes:
      - db:/var/lib/mysql
    environment:
      - MYSQL_RANDOM_ROOT_PASSWORD=yes
      - MYSQL_USER=nextcloud_user
      - MYSQL_PASSWORD_FILE=/run/secrets/mysql_user_password
      - MYSQL_DATABASE=nextcloud
    secrets:
      - mysql_user_password

  app:
    image: nextcloud
    restart: always
    ports:
      - 80:80
      - 443:443
    links:
      - db
    volumes:
      - nextcloud:/var/www/html
    environment:
      - NEXTCLOUD_ADMIN_USER=pp
      - NEXTCLOUD_ADMIN_PASSWORD_FILE=/run/secrets/nextcloud_admin_password
      - MYSQL_USER=nextcloud_user
      - MYSQL_PASSWORD_FILE=/run/secrets/mysql_user_password
      - MYSQL_DATABASE=nextcloud
      - MYSQL_HOST=db
    secrets:
      - nextcloud_admin_password
      - mysql_user_password

volumes:
  nextcloud:
  db:

secrets:
  nextcloud_admin_password:
    file: ./nc_admin_pass.txt
  mysql_user_password:
    file: ./mysql_user_pass.txt
```

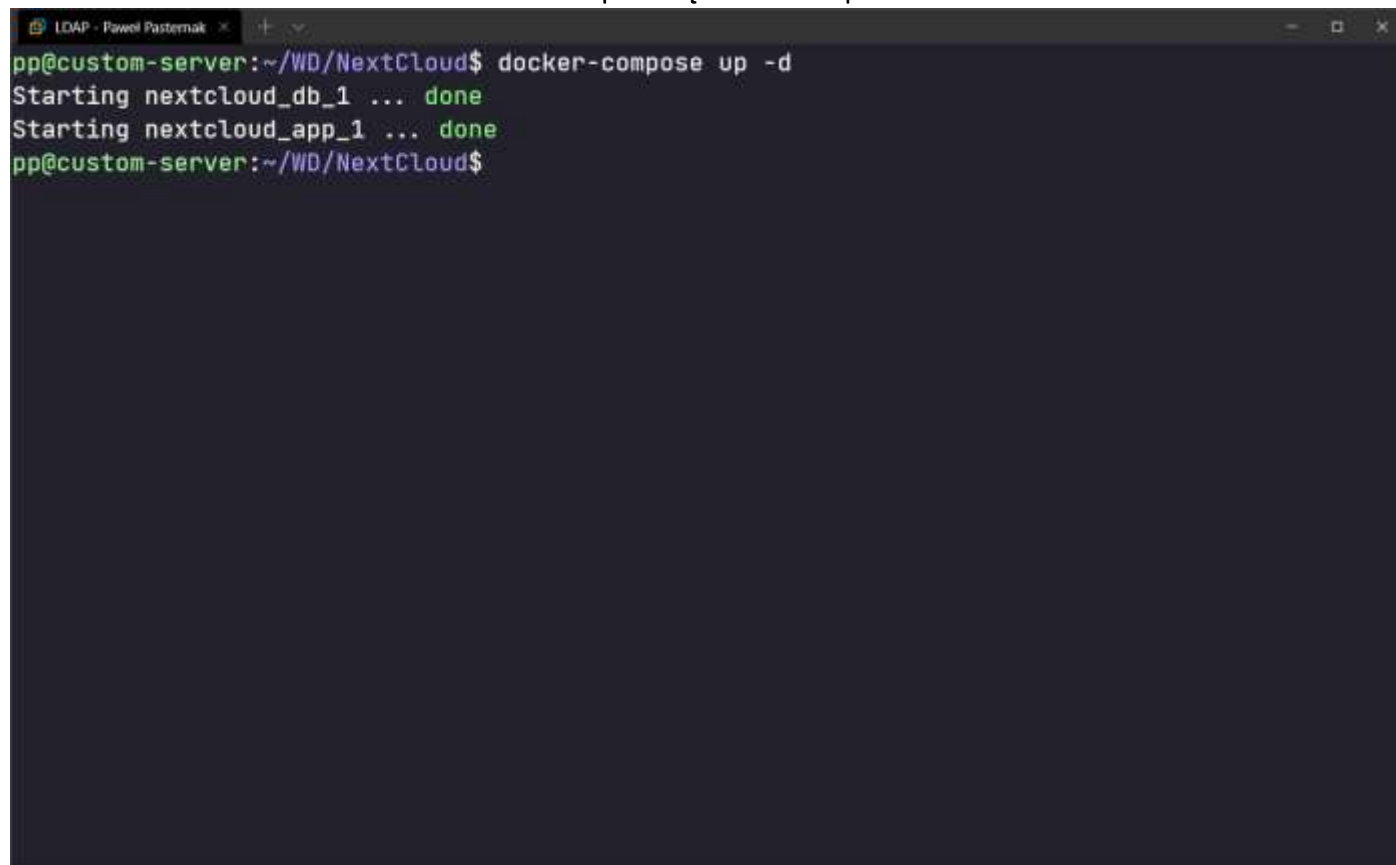
- Utworzenie sekretów z hasłami



```
pp@custom-server:~/WD/NextCloud$ vim docker-compose.yml
pp@custom-server:~/WD/NextCloud$ vim nc_admin_pass.txt
pp@custom-server:~/WD/NextCloud$ openssl rand -base64 32 > mysql_user_pass.txt
pp@custom-server:~/WD/NextCloud$
```

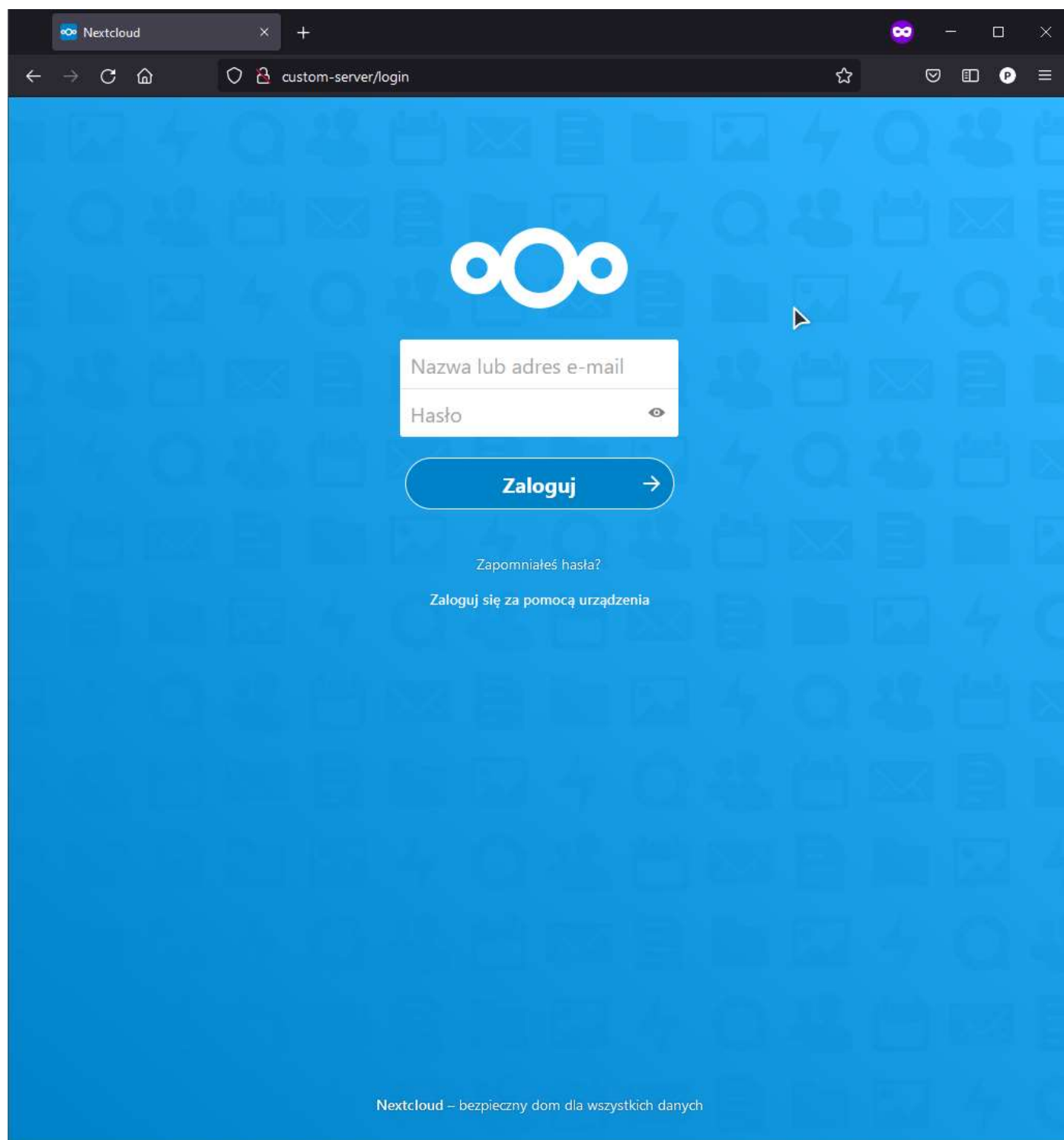
Zrzut Ekranu 63 – podanie hasła dla administratora i wygenerowanie losowego hasła dla użytkownika bazy danych

- Utworzenie i uruchomienie kontenerów z pomocą docker-compose



```
pp@custom-server:~/WD/NextCloud$ docker-compose up -d
Starting nextcloud_db_1 ... done
Starting nextcloud_app_1 ... done
pp@custom-server:~/WD/NextCloud$
```

Zrzut Ekranu 64 – pobranie obrazów i utworzenie działających kontenerów, wolumenów na dane, sekretów i sieci wewnętrznej w której będą działać kontenery



Zrzut Ekranu 65 - wejście na stronę i zalogowanie się za pomocą ustawionego loginu i hasła

The screenshot shows the Nextcloud application settings page. The left sidebar contains a list of application categories. The main area displays a table of installed applications. The 'LDAP user and group backend' application is selected, and its status is being changed from 'Polecane' (Recommended) to 'Włącz' (Enabled). A user profile menu is open on the right side of the page.

Application Name	Version	Status	Action
Share by mail	1.13.0	✓ Polecane	
Support	1.6.0	✓ Polecane	
Text	3.4.0	✓ Polecane	
Theming	1.14.0	✓ Polecane	
Update notification	1.13.0	✓ Polecane	
Usage survey	1.11.0	✓ Polecane	
User status	1.3.1	✓ Polecane	
Versions	1.16.0	✓ Polecane	Wyłącz
Video player	1.12.0	✓ Polecane	Wyłącz
Weather status	1.3.0	✓ Polecane	Wyłącz
Auditing / Logging	1.13.0	✓ Polecane	Włącz
Default encryption module	2.11.0	✓ Polecane	Włącz
External storage support	1.15.0	✓ Polecane	Włącz
LDAP user and group backend	1.13.1	✓ Polecane	Włącz

User Profile Menu:

- pp Zobacz profil
- Ustaw status
- Ustawienia
- + Aplikacje
- O aplikacji
- Użytkownicy
- Pomoc
- Wyloguj

Zrzut Ekranu 66 - Włączenie logowania za pomocą LDAP

- Konfiguracja integracji z LDAP

The screenshot shows the 'Integracja z LDAP/AD' configuration page in Nextcloud. The left sidebar contains two main sections: 'Osobiste' (Personal) and 'Administracja' (Administration). The 'Osobiste' section includes links for 'Informacje osobiste', 'Bezpieczeństwo', 'Powiadomienia', 'Mobilne i stacjonarne', 'Dostępność', 'Udostępnianie', 'Praca grupowa', 'Przepliw', and 'Prywatność'. The 'Administracja' section includes links for 'Przegląd', 'Wsparcie', 'Ustawienia podstawowe', 'Udostępnianie', 'Bezpieczeństwo', 'Integracja z LDAP/AD' (which is currently selected), 'Motyw', 'Praca grupowa', 'Uprawnienia administratora', and 'Aktywność'.

The main content area is titled 'Integracja z LDAP/AD' and features a tabbed interface with tabs for 'Serwer', 'Użytkownicy', 'Atrybuty logowania', 'Grupy', and 'Zaawansowane'. The 'Serwer' tab is active, showing a list of LDAP servers. The first server is '1. Serwer: 192.168.100.58'. Below this, there are input fields for the server address (192.168.100.58), the number of users (389), the search filter (cn=admin,dc=pasternak,dc=local), and the base DN (dc=pasternak,dc=local). There is also a checkbox for 'Ręcznie wprowadzaj filtry LDAP (zalecane dla dużych katalogów)'. At the bottom of the form, a green dot indicates 'Konfiguracja poprawna' (Configuration correct), and a blue 'Kontynuuj' button is visible.

On the right side of the screen, a user profile dropdown menu is open, showing options like 'Zobacz profil', 'Ustaw status', 'Ustawienia', 'Aplikacje', 'O aplikacji', 'Użytkownicy', 'Pomoc', and 'Wyloguj'.

Zrzut Ekranu 67 - Ustawianie połączenia z serwerem LDAP

Ustawienia - Nextcloud

custom-server/settings/admin/ldap

Integracja z LDAP/AD

Serwer **Użytkownicy** Atrybuty logowania Grupy Zaawansowane Eksperckie

Wyświetlanie i wyszukiwanie użytkowników jest ograniczony tymi kryteriami:

Tylko te klasy obiektów: **inetOrgPerson,**

Najbardziej wspólną klasą obiektów dla użytkowników jest `organizationalPerson`, `person`, `user` i `InetOrgPerson`. Jeśli nie wiesz, którą klasę obiektów wybrać, skonsultuj to ze swoim administratorem usługi katalogowej.

Tylko z tych grup: **Wybierz grupy**

[Edytuj zapytanie LDAP](#)

Filtr LDAP `((objectclass=inetOrgPerson)(objectclass=posixAccount))`

Sprawdź ustawienia i policz użytkowników 1 znaleziony użytkownik

Konfiguracja poprawna **Wstecz** **Kontynuuj** **Pomoc**

Zrzut Ekranu 68 - Ustawienie jak pobierać użytkowników

Ustawienia - Nextcloud

custom-server/settings/admin/ldap

Integracja z LDAP/AD

Server Użytkownicy **Atrybuty logowania** Grupy Zaawansowane Eksperckie

Podczas logowania, Nextcloud znajdzie użytkownika na podstawie następujących atrybutów:

Nazwa użytkownika LDAP/AD: ☒

Adres e-mail LDAP/AD: ☐

Inne atrybuty: **Wybierz atrybuty**

[Edytuj](#)

[zapytanie LDAP](#)

Filtr LDAP (&(|(objectclass=inetOrgPerson)(objectclass=posixAccount))(uid=%uid))

Testowa nazwa użytł Weryfikuj ustawienia

Konfiguracja poprawna ● **Wstecz**

Kontynuuj **Pomoc**

- Osobiste**
 - Informacje osobiste
 - Bezpieczeństwo
 - Powiadomienia
 - Mobilne i stacjonarne
 - Dostępność
 - Udostępnianie
 - Praca grupowa
 - Przepływ
 - Prywatność
- Administracja**
 - Przegląd
 - Wsparcie
 - Ustawienia podstawowe
 - Udostępnianie
 - Bezpieczeństwo
 - Integracja z LDAP/AD**
 - Motyw
 - Praca grupowa
 - Uprawnienia administratora
 - Aktywność

Zrzut Ekranu 69 - Ustawienie atrybutów logowania dla użytkowników

The screenshot shows the Nextcloud administration interface for LDAP integration. The left sidebar contains navigation links for personal settings, security, notifications, mobile and desktop, availability, sharing, group work, workflow, and privacy. The main content area is titled 'Integracja z LDAP/AD' and has several tabs: 'Serwer', 'Użytkownicy', 'Atrybuty logowania', 'Grupy' (selected), 'Zaawansowane', and 'Eksperckie'. Under the 'Grupy' tab, it states 'Grupy spełniające te kryteria są dostępne w Nextcloud:' and provides two filters: 'Tylko te klasy obiektów:' set to 'posixGroup' and 'Tylko z tych grup:' set to 'Wybierz grupy'. Below these filters are links for 'Edytuj' and 'zapytanie LDAP', and the LDAP filter is shown as '(&(!((objectclass=posixGroup)))'. At the bottom, a confirmation message says 'Zweryfikuj ustawienia i policz grupy' with '1 znaleziona grupa'. A green status indicator shows 'Konfiguracja poprawna', and there are buttons for 'Wstecz' and 'Pomoc'.

Osobiste

- Informacje osobiste
- Bezpieczeństwo
- Powiadomienia
- Mobilne i stacjonarne
- Dostępność
- Udostępnianie
- Praca grupowa
- Przepływ
- Prywatność

Administracja

- Przegląd
- Wsparcie
- Ustawienia podstawowe
- Udostępnianie
- Bezpieczeństwo
- Integracja z LDAP/AD**
- Motyw
- Praca grupowa
- Uprawnienia administratora
- Aktywność

Integracja z LDAP/AD

Serwer Użytkownicy Atrybuty logowania **Grupy** Zaawansowane Eksperckie

Grupy spełniające te kryteria są dostępne w Nextcloud:

Tylko te klasy obiektów: **posixGroup**

Tylko z tych grup: **Wybierz grupy**

[↓ Edytuj](#)
[zapytanie LDAP](#)

Filtr LDAP (&(!((objectclass=posixGroup)))

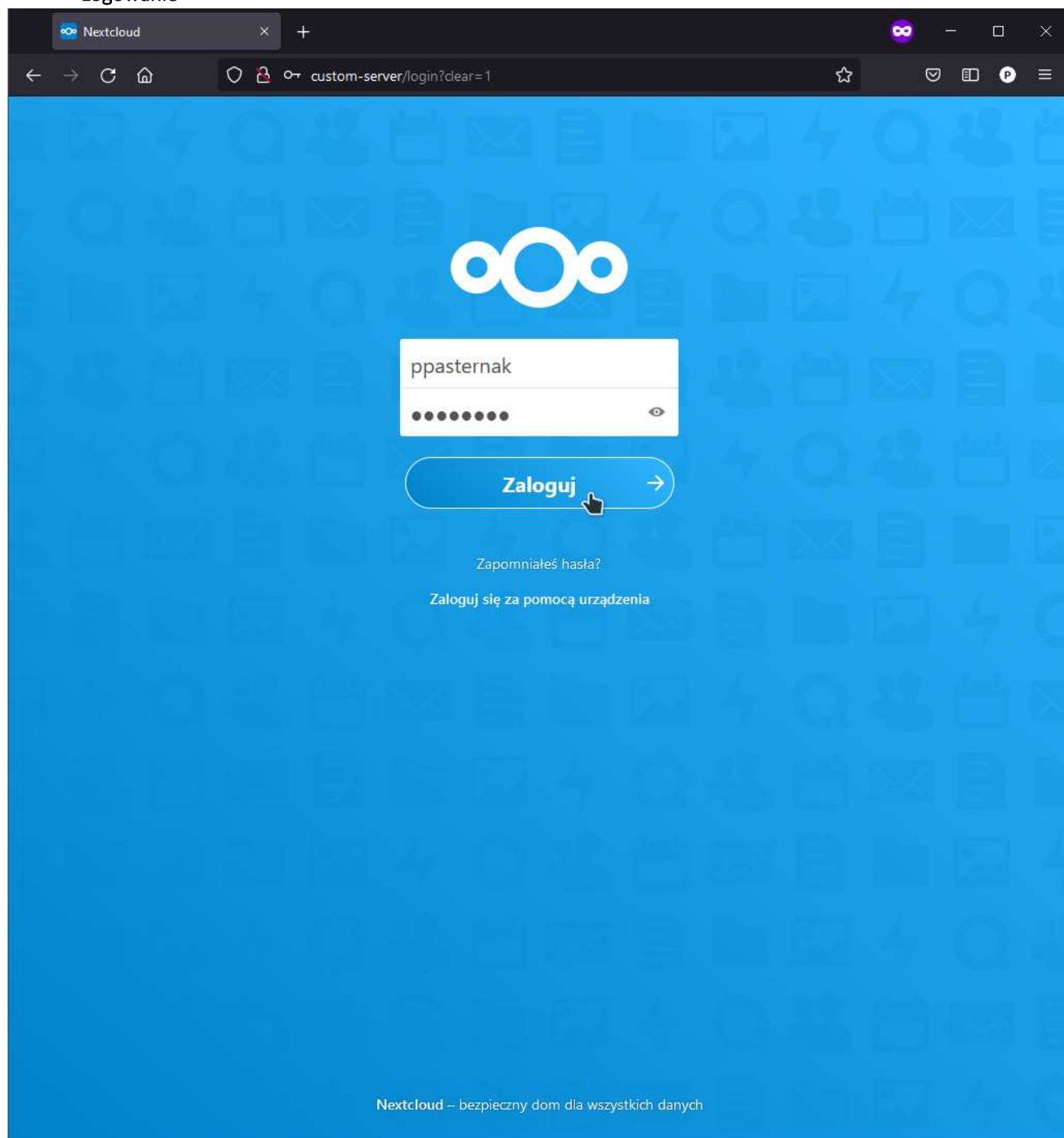
Zweryfikuj ustawienia i policz grupy 1 znaleziona grupa

Konfiguracja poprawna **Wstecz**

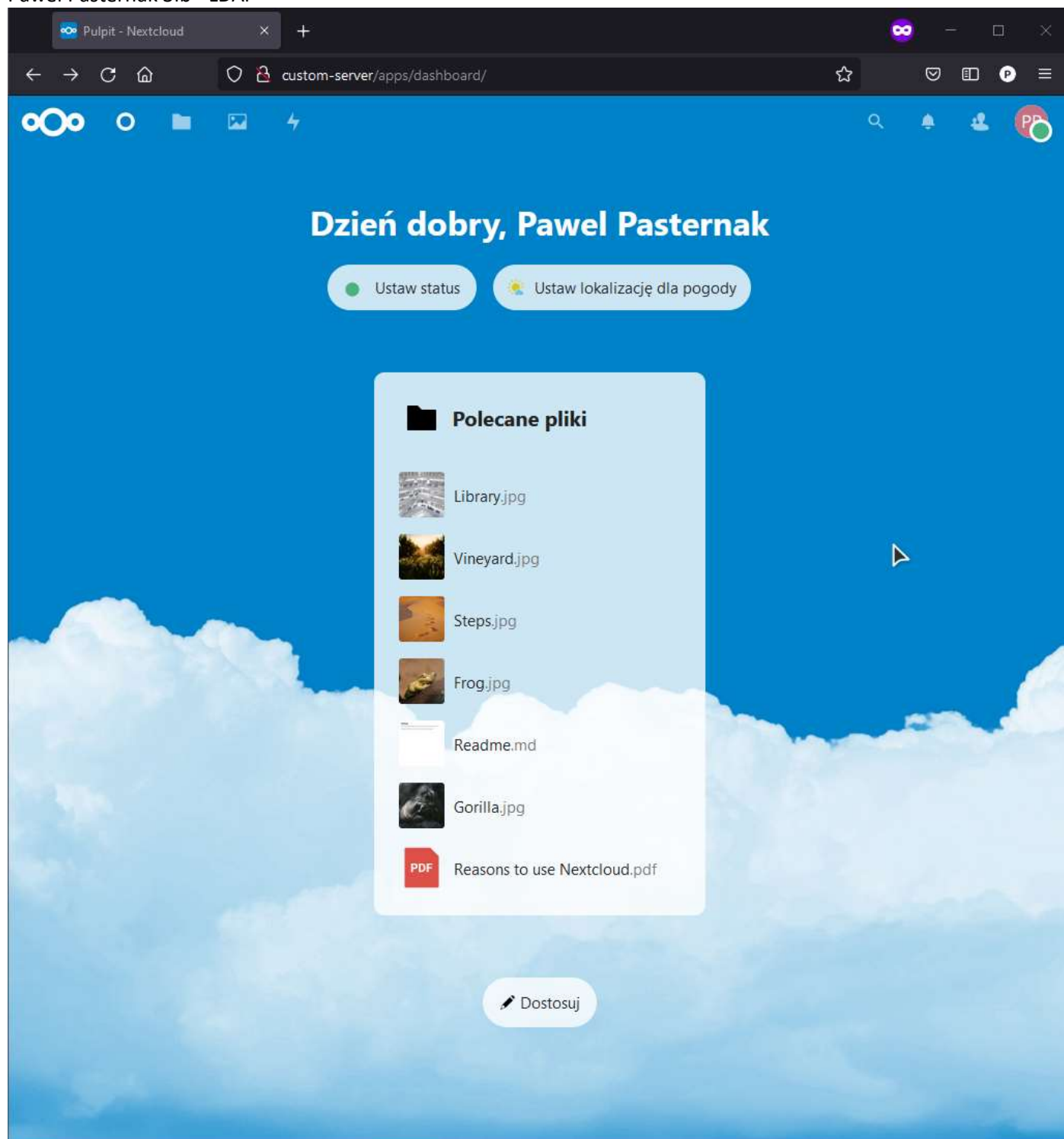
i Pomoc

Zrzut Ekranu 70 - Dodanie grup (posixGroup)

- Logowanie



Zrzut Ekranu 71 - Logowanie na użytkownika LDAP



Zrzut Ekranu 72 - Ekran po zalogowaniu użytkownika (jako pełną nazwę jest wykorzystane cn)

Zagadnienia uzupełniające

1. NSS – Name Service Switch (przełącznik usługi nazw)

Przełącznik usługi nazw (NSS) łączy komputer z różnymi źródłami typowych baz danych konfiguracji i mechanizmów rozpoznawania nazw. Źródła te obejmują lokalne pliki systemu operacyjnego (takie jak /etc/passwd, /etc/group i /etc/hosts), system nazw domen (DNS), Network Information Service (NIS, NIS+) i LDAP.

Ten mechanizm systemu operacyjnego, używany w miliardach komputerów, w tym we wszystkich uniksopodobnych systemach operacyjnych, jest niezbędny do funkcjonowania jako część sieciowej organizacji i Internetu. Jest on wywoływany między innymi za każdym razem, gdy użytkownik komputera kliknie lub wpisze adres strony internetowej w przeglądarce internetowej lub odpowie na wezwanie do hasła, aby uzyskać autoryzację dostępu do komputera i Internetu.

[▲ Powrót](#)

2. Konteneryzacja

Wirtualizacja na poziomie Systemu Operacyjnego (ang. OS-level virtualization) jest to wirtualizacja, w której jądro systemu pozwala na istnienie wielu izolowanych od siebie przestrzeni użytkowników.

Inne nazwy tych przestrzeni użytkowników (i ich przedstawiciele) to m.in.:

- Kontenery (LXC containers, Docker, Podman)
- Strefy (Solaris containers)
- Wirtualne serwery prywatne (OpenVZ)
- Partycje
- Środowiska wirtualne (VE)
- Wirtualne jądra (DragonFly BSD)
- Więzienia (FreeBSD jail, chroot jail)



Takie instancje mogą wyglądać jak prawdziwe komputery z punktu widzenia uruchomionych na nich programów. Program komputerowy działający w zwykłym systemie operacyjnym może zobaczyć wszystkie zasoby (podłączone urządzenia, pliki i foldery, udziały sieciowe, moc procesora, wymierne możliwości sprzętowe) tego komputera. Jednak programy działające wewnątrz kontenera widzą tylko zawartość kontenera i urządzenia przypisane do kontenera. Konteneryzacja jest znacznie lżejsza niż pełna wirtualizacja, a funkcjonalność kontenerów jest jednocześnie bardziej i mniej ograniczona niż maszyn wirtualnych.

[▲ Powrót](#)