

## Ubuntu serwer

Ubuntu jest systemem opensourcowym, współtworzonym przez użytkowników.

### Instalacja Ubuntu Server

Wymagania systemowe to procesor 2 rdzeniowy 2GHz oraz 4GRAM, 25G przestrzeni dyskowej.

Zarówno system Ubuntu kliencki jak i serwer wykorzystują to samo repozytorium, komendy w wierszu poleceń też działają zamiennie. Serwer nie posiada interfejsu graficznego. Instalując Ubuntu (serwer) na maszynie wirtualnej upewnij się czy masz włączoną wirtualizację w BIOS/UEFI. Pobieramy obraz systemu kopiując go na pen drive, w BIOS/UEFI zmieniamy kolejność bootowania na pen drive jako 1. Rusza instalator. Instalacja daje nam do wyboru rodzaj języka, aktualizacja systemu (można pominąć) układ klawiatury, konfigurację karty sieciowej, wybór partycji do zainstalowania, proxy, nazwa użytkownika i hasło itp. Większość ustawień zostawiamy domyślnie. Nawet jeśli ich nie skonfigurujemy przy instalacji możemy do tego wrócić w trakcie użytkowania systemu. Część komend nawet wpisywana we właściwym trybie może nie działać – bierze się to z tego że trzeba zainstalować paczkę w terminalu.

Komendy w terminalu co do zasady uniwersalne na kliencie i serwerze. W praktyce problemy pojawiają się już na samym etapie instalacji systemu, podczas którego często trzeba odłączyć się od WAN, by instalacja powiodła się. W niektórych wersjach Ubuntu Server np. 23.10 są liczne błędy, które uniemożliwiają instalację narzędzi pakietów (tzw. APT – Advanced Packaging Tool) takich jak „net-tools” czy „isc-dhcp”. W miarę pewną opcją jest instalacja Ubuntu Server 24.04 LTS, która zawiera ponad 800 stron manuala i na której poprawione są błędy poprzedników.

Warto więc na starcie wpisać `sudo apt update`, by zaktualizować pakiety serwera a następnie `sudo apt upgrade` (uaktualnimy pakiety). Może dojść do sytuacji że część pakietów jest starsza a część nowsza – by rozwiązać problem nieścisłości możemy wpisać `sudo apt dist-upgrade`.

W terminalu w systemach LINUX używamy często `sudo`, które pozwala na przejście na uprawnienia administratora, czyli także instalacji jakiegoś pakietu APT.

Jeśli będą problemy z rozpoznawaniem komend sieciowych w Ubuntu klient należy zainstalować w terminalu: `apt install net-tools`. Polecenie „ctrl c” przerywa polecenie w terminalu.

Inne pojęcia związane z Linuxem to:

demon - program pracujący w tle i nieprzyłączony do terminalu,

superdemon – narzędzie kontrolujące wybrane porty i uruchamiające usługi tylko w razie potrzeby.

```

admin1@admin1-VirtualBox:~$ sudo passwd root
[sudo] hasło użytkownika admin1:
Proszę podać nowe hasło UNIX:
Proszę ponownie podać hasło UNIX:
passwd: password updated successfully
admin1@admin1-VirtualBox:~$ su
Hasło:
root@admin1-VirtualBox:/home/admin1# ifconfig

Command 'ifconfig' not found, but can be installed with:

apt install net-tools

root@admin1-VirtualBox:/home/admin1# apt install net-tools
E: Nie udało się uzyskać blokady /var/lib/dpkg/lock-frontent - open (11: Zasoby chwilowo niedostępne)
E: Unable to acquire the dpkg frontend lock (/var/lib/dpkg/lock-frontent), is another process using it?
root@admin1-VirtualBox:/home/admin1# ps -a
  PID TTY          TIME CMD
 1607 pts/1        00:00:00 su
 1608 pts/1        00:00:00 bash
 1641 pts/1        00:00:00 ps
root@admin1-VirtualBox:/home/admin1# ps -aw
  PID TTY          TIME CMD
 1607 pts/1        00:00:00 su
 1608 pts/1        00:00:00 bash

```

## Komendy:

sudo apt install traceroute – instaluje traceroute - śledzi trasę (ilość routerów do serwera)

ifconfig - ipv4, ipv6, adres Mac, maska podsieci, pokazuje rodzaje interfejsów, adres pętli zwrotnej

iwconfig - wersja if config tylko dla bezprzewodowej karty sieciowej

ping - weryfikacja komunikacji z innym hostem lub stroną

history – wyświetla komendy wpisane wcześniej w terminalu

sudo su – przejście na konto na prawach roota

sudo passwd – zmiana hasła roota, wyłączenie hasła roota – sudo passwd -l root

ls – wyświetla zawartość katalogu/nazwy plików:

```

root@marek-1-2:/home/marek# ls /etc/ppp
chap-secrets  ip-pre-up  ip-up.d    ipv6-up    options.pptp
ip-down       ip-pre-up.d  ipv6-down  ipv6-up.d  pap-secrets
ip-down.d     ip-up       ipv6-down.d  options    peers
root@marek-1-2:/home/marek# ls -lt
total 36
drwxr-xr-x 3 marek marek 4096 Sep  8 16:35 Pictures
drwx----- 4 marek marek 4096 Sep  8 16:03 snap
drwxr-xr-x 2 marek marek 4096 Sep  8 15:57 Desktop
drwxr-xr-x 2 marek marek 4096 Sep  8 15:57 Documents
drwxr-xr-x 2 marek marek 4096 Sep  8 15:57 Downloads
drwxr-xr-x 2 marek marek 4096 Sep  8 15:57 Music
drwxr-xr-x 2 marek marek 4096 Sep  8 15:57 Public
drwxr-xr-x 2 marek marek 4096 Sep  8 15:57 Templates
drwxr-xr-x 2 marek marek 4096 Sep  8 15:57 Videos
root@marek-1-2:/home/marek#

```

ls / - wyświetla pliki root directory (odpowiednik mojego komputera w Windows)

ls -lS /etc/ssh („S” jest do filtrowania, ta komenda wyświetla konkretnie ssh)

ls -lSh /etc/ssh – wyświetla to samo co powyżej tylko w bardziej przystępnej formie (human readable)

ls -l sample – tworzy katalog:

```
sysadmin@localhost:~$ ls
Desktop Documents Downloads Music Pictures Public Templates
Videos
sysadmin@localhost:~$ touch sample
sysadmin@localhost:~$ ls -l sample
-rw-rw-r-- 1 sysadmin sysadmin 0 Nov  9 16:48 sample
sysadmin@localhost:~$ ls
Desktop Downloads Pictures Templates sample
Documents Music Public Videos
```

Usuwanie katalogu:

```
sysadmin@localhost:~$ ls
Desktop Downloads Pictures Templates sample
Documents Music Public Videos
sysadmin@localhost:~$ rm sample
sysadmin@localhost:~$ ls
Desktop Documents Downloads Music Pictures Public Templates
Videos
```

man – komenda z podpowiedziami (skrót od manual, wpisz np. man ls)

info – wyświetla informację do czego służy komenda, wpisz np. info ls

lspci – wyświetla urządzenia peryferyjne wpięte do PCI

lsusb – wyświetla urządzenia wpięte to magistrali USB

free –m – wyświetla ilość pamięci wykorzystanej i wolnej

top – wyświetla procesy komputera w danej chwili

host – sprawdza DNS danej strony:

```
root@marek-1-2:/home/marek# host wp.pl
wp.pl has address 212.77.98.9
wp.pl mail is handled by 0 mx.wp.pl.
wp.pl mail is handled by 5 mx5.wp.pl.
root@marek-1-2:/home/marek#
```

view /etc/hosts – wyświetla hosty i ich adresy IP

sudo nano /etc/hostname – zmieniamy nazwę komputera

sudo nano /etc/passwd – tworzymy nazwę użytkownika

cat /etc/hostname oraz cat /etc/hosts – sprawdza użytkownika i nazwę PC

sudo user add „marek”/sudo adduser „marek” dodaje użytkownika marek i hasło, sudo deluser „marek” – usuwa użytkownika o nazwie marek

sudo groupadd .../sudo addgroup - dodaje grupę, groupdel (clerks) – usuwa grupę o nazwie clerks, sudo adduser (nazwa użytkownika, nazwa grupy) – dodaje użytkownika do grupy

sudo usermod -G sudo -a (nazwa użytkownika) – dodajemy użytkownika do grupy sudo

cat /etc/group |grep sudo – sprawdza przynależność do grupy

ls -ld /home/username – sprawdza uprawnienia danego użytkownika

ss – pokazuje statystyki gniazda tj. numery portów, status połączenia, adresy serwerów i lokalne

cat /etc/resolv.conf – ustawienia dotyczące DNS

view /etc/passwd – zawiera informacje o użytkownikach i kontach

cat /etc/shadow – pokazuje nazwę konta i zaszyfrowaną postać hasła danego konta

view /etc/group – zawiera informacje o użytkownikach i grupach, do których należą

id – jak wyżej

groupmod -n (clerks managers) – zmienia nazwę grupy

who albo w – wyświetla informację kto jest aktualnie zalogowany

chage -l (username) sprawdza ustawienia hasła użytkownika (chage oznacza change age)

chage age – zmienia ustawienia hasła użytkownika

## Zarządzanie strukturą dysku

fdisk /dev/sda – narzędzie do zarządzania partycjami, wpisując „m” uzyskamy wykaz zadań:

```
Command (m for help): m
Help:
  GPT
  M   enter protective/hybrid MBR

Generic
d   delete a partition
F   list free unpartitioned space
l   list known partition types
n   add a new partition
p   print the partition table
t   change a partition type
v   verify the partition table
i   print information about a partition

Misc
m   print this menu
x   extra functionality (experts only)

Script
I   load disk layout from sfdisk script file
O   dump disk layout to sfdisk script file

Save & Exit
w   write table to disk and exit
q   quit without saving changes

Create a new label
g   create a new empty GPT partition table
G   create a new empty SGI (IRIX) partition table
o   create a new empty MBR (DOS) partition table
s   create a new empty Sun partition table

Command (m for help): F
Unpartitioned space /dev/sda: 1.48 MiB, 1555968 bytes, 3039 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes

   Start      End  Sectors  Size
363333632 363336670    3039   1.5M

Command (m for help):
```

Przy pomocy fdisk możemy dodać nową partycję czy ją usunąć oraz sprawdzić pojemność dysku.

view /etc/resolv.conf – zawiera informacje o DNS aktualnie używanych

arp - wyświetla tablicę adresów IP i mac, arp -a

netstat - wyświetlenie połączeń i podłączonych portów

netstat - ano - aktywne połączenia sieciowe, rodzaj połączenia, numery portów

netstat – r działa jak komenda „route” natomiast netstat -tln pokazuje otwarte porty

route - wyświetla tablice routingu, pokazuje bramę domyślną dzięki czemu możliwy NAT

traceroute + adres strony/nazwa domeny strony - bada przeskokki tj. ilość routerów do celu

ip address show lub ip a - wyświetla interfejs sieciowy

sudo lshw –class network – wyświetla informacje o interfejsach sieciowych np. przepustowość, sterowniki kart sieciowych

sudo ethtool (nazwa karty sieciowej) - wyświetla m.in. tryb pracy karty:

```
marek@marek:~$ sudo ethtool enp0s3
Settings for enp0s3:
  Supported ports: [ TP ]
  Supported link modes:  10baseT/Half 10baseT/Full
                        100baseT/Half 100baseT/Full
                        1000baseT/Full
  Supported pause frame use: No
  Supports auto-negotiation: Yes
  Supported FEC modes: Not reported
  Advertised link modes:  10baseT/Half 10baseT/Full
                        100baseT/Half 100baseT/Full
                        1000baseT/Full
  Advertised pause frame use: No
  Advertised auto-negotiation: Yes
  Advertised FEC modes: Not reported
  Speed: 1000Mb/s
  Duplex: Full
  Auto-negotiation: on
  Port: Twisted Pair
  PHYAD: 0
  Transceiver: internal
  MDI-X: off (auto)
  Supports Wake-on: umbg
  Wake-on: d
  Current message level: 0x00000007 (7)
                        drv probe link
  Link detected: yes

marek@marek:~$
```

sudo ip addr add 165.18.6.1/24 dev enp0s8 – tymczasowo zmienia adres IP karty sieciowej o nazwie enp0s8 na 165.18.6.1 z maską /24, na 1 karcie możemy dodać kilka adresów IP (na serwerze, wtedy numer portu decyduje jaka konkretna strona się wyświetli), adresy będą aktywne do ponownego uruchomienia systemu, możemy je wpisać ręcznie w GUI,

ip addr show enp0s8 – sprawdza adresację karty o nazwie enp0s8

sudo ip route add default via 192.168.66.1 - ustawia adres bramy domyślnej o adresie 192.168.66.1

ip route albo ip route show – sprawdza ustawienia bramy domyślnej

nameserver – 8.8.8.8 – dodaje DNS o adresie 8.8.8.8

ip addr flush enp0s8 – czyści adresację karty enp0s8, potrzeba reboota

ip address show lo – wyświetla informację o pętli zwrotnej

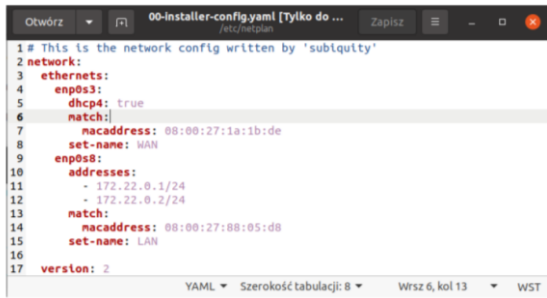
sudo nano/etc/netplan/\* .yaml - uruchomienie netplan do konfiguracji interfejsów sieciowych

```
GNU nano 2.9.3 /etc/netplan/01-network-manager-all.yaml
Let NetworkManager manage all devices on this system
network:
  version: 2
  renderer: NetworkManager
  ethernets:
    ens33:
      dhcp4: no
      addresses: [192.168.72.150/24]
      gateway4: 192.168.72.2
      nameservers:
        addresses: [8.8.8.8,8.8.4.4]
```

/etc/netplan/01-network-manager-all.yaml - ustawienia konfiguracyjne sieci, po konfiguracji należy wpisać komendę sudo netplan try i sudo netplan apply. W nowszych Ubuntu: nano /etc/netplan/50-cloud-init.yaml

Komenda „sudo ip addr add 192.168.5.5/24 brd + dev enp0s3” przypisze adres IP i maskę dla konkretnego interfejsu oraz broadcast.

sudo nano /etc/netplan/00-installer-config.yaml – dodaje kartę sieciową do edycji jeśli nie ma jej w pliku konfiguracyjnym, konfigurujemy kartę w netplan i zatwierdzamy sudo netplan apply  
zmiana nazwy karty sieciowej na serwerze:



```
1 # This is the network config written by 'subiquity'
2 network:
3   ethernets:
4     enp0s3:
5       dhcp4: true
6     match:
7       macaddress: 08:00:27:1a:1b:de
8       set-name: WAN
9     enp0s8:
10      addresses:
11        - 172.22.0.1/24
12        - 172.22.0.2/24
13      match:
14        macaddress: 08:00:27:88:05:d8
15        set-name: LAN
16
17 version: 2
```

Komenda `sudo systemctl restart NetworkManager.service` – uruchomienie ponowne by system odczytał zmienione ustawienia interfejsu.

Zmiana nazwy karty sieciowej na desktopie na LAN:

```
/etc/udev/rules.d/70-persistent-net.rules
```

```
ATTR{address}=="08:00:27:fe:e8:3b",NAME="LAN"
```

gdzie 08:00:27:fe:e8:3b to adres MAC karty sieciowej której nazwę chcemy zmienić. Uruchamiamy system ponownie.

Reset netplanu:

```
sudo rm -rf /etc/netplan/*
```

```
touch /etc/netplan/config.yaml
```

```
netplan apply
```

Reset network manager:

```
nmcli con, kopiujemy UUID,
```

```
nmcli con delete (kopiujemy UUID),
```

```
rm -r /etc/udev/rules.d/70-persistent-net.rules, reboot.
```

```
cat /etc/resolv.conf lub resolvectl – sprawdza w pliku adresy serwerów DNS, z których korzysta system
```

## Protokół dynamicznej konfiguracji hosta (DHCP)

To usługa sieciowa, która umożliwia automatyczne przypisywanie ustawień do komputerów hostów z serwera, zamiast ręcznej konfiguracji każdego hosta sieciowego. Komputery skonfigurowane jako klienci DHCP nie mają kontroli nad ustawieniami otrzymywanymi z serwera DHCP, a konfiguracja jest transparentna dla użytkownika komputera.

Najczęstsze ustawienia udostępniane klientom DHCP przez serwer DHCP to:

- Adres IP i maska sieci
- Adres IP bramy domyślnej
- Adresy IP serwerów DNS

Serwer DHCP może jednak również dostarczać właściwości konfiguracyjne, takie jak:

- Nazwa hosta
- Nazwa domeny
- Serwer czasu
- Serwer wydruku

Zaletą korzystania z DHCP jest to, że zmiany w sieci, na przykład zmiana adresu serwera DNS, wymagają jedynie zmiany na serwerze DHCP, a wszystkie hosty sieciowe zostaną ponownie skonfigurowane, gdy ich klienci DHCP następnym razem odpytają serwer DHCP. Dodatkową zaletą jest łatwiejsze integrowanie nowych komputerów z siecią, ponieważ nie ma potrzeby sprawdzania dostępności adresu IP. Konflikty w przydzielaniu adresów IP są również ograniczone. Serwer DHCP może udostępniać ustawienia konfiguracyjne za pomocą następujących metod:

- Alokacja ręczna (adres MAC)

Ta metoda polega na użyciu protokołu DHCP do identyfikacji unikalnego adresu sprzętowego każdej karty sieciowej podłączonej do sieci, a następnie ciągłym dostarczaniu stałej konfiguracji za każdym razem, gdy klient DHCP wysyła żądanie do serwera DHCP za pomocą tego urządzenia sieciowego. Gwarantuje to automatyczne przypisanie określonego adresu do danej karty sieciowej na podstawie jej adresu MAC.

- Alokacja dynamiczna (pula adresów)

W tej metodzie serwer DHCP przydziela adres IP z puli adresów na określony czas lub dzierżawę, która jest skonfigurowana na serwerze lub do momentu, gdy klient poinformuje serwer, że nie potrzebuje już danego adresu. W ten sposób klienci będą otrzymywać swoje właściwości konfiguracyjne dynamicznie i na zasadzie „kto pierwszy, ten lepszy”. Gdy klient DHCP nie jest już w sieci przez określony czas, konfiguracja wygasa i wraca do puli adresów, aby mogli z niej korzystać inni klienci DHCP. W ten sposób adres może zostać wydzierżawiony lub używany przez określony czas. Po tym czasie klient musi renegotjować dzierżawę z serwerem, aby utrzymać adres.

- Automatyczne przydzielanie

Za pomocą tej metody DHCP automatycznie przypisuje adres IP urządzeniu na stałe, wybierając go z puli dostępnych adresów. Zwykle DHCP jest używany do przydzielania klientowi adresu tymczasowego, ale serwer DHCP może zezwolić na nieograniczony czas dzierżawy.

Dwie ostatnie metody można uznać za „automatyczne”, ponieważ w każdym przypadku serwer DHCP przypisuje adres bez dodatkowej interwencji. Jediną różnicą między nimi jest czas dzierżawy adresu IP, innymi słowy, czy adres klienta zmienia się w czasie. Serwer DHCP udostępniany przez Ubuntu to `dhcpd` (demon protokołu dynamicznej konfiguracji hosta), który jest łatwy w instalacji i konfiguracji i uruchamia się automatycznie przy uruchomieniu systemu.

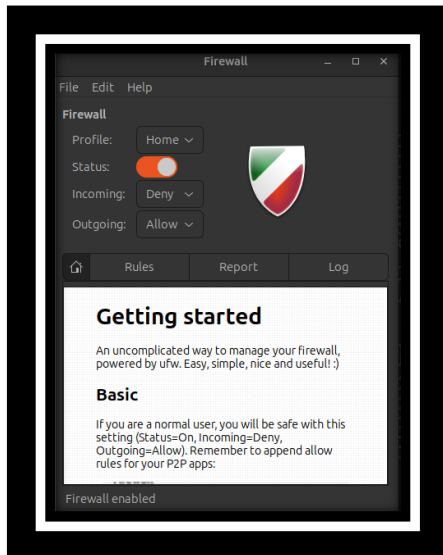
- a) `sudo apt install isc-dhcp-server` – instaluje, uruchamia DHCP, `sudo service isc-dhcp-server start` i `sudo service isc-dhcp-server restart` do włączenia usługi.
- b) `nano /etc/default/isc-dhcp-server` – wpisujemy nazwę karty sieciowej, na której chcemy wdrożyć dhcp,

- c) `nano /etc/dhcp/dhcpd.conf` (usuwamy # z 2 serwerów domenowych), edytujemy pulę,
- d) pod „a slightly different... usuwamy # z subnet i range -> wpisujemy adres podsieci, maskę, range adresów IP, na końcu nawiasu usuwamy #
- e) `sudo systemctl restart isc-dhcp-server -> sudo systemctl status isc-dhcp-server`

`ufw enable` – włączanie firewall, `ufw disable` wyłącza, `ufw status` – sprawdza status zapory.

`ufw allow 22` lub `ufw deny 22` - włącza i wyłącza port SSH

`sudo apt install gufw` – instaluje firewalla, którego można znaleźć w menu:



### Instalacja telnetu:

`sudo apt install telnetd` – instaluje telnet -> `systemctl status inetd` – sprawdza status telnetu

`netstat -tulpn | grep :23` – sprawdzanie czy port telnetu jest nasłuchiwany

teraz podłączamy urządzenie do serwera, poleceniem ip a sprawdzamy adres IP naszej karty sieciowej i wpisujemy go do Putty (other -> adres IP Serwera)

### Instalacja SSH:

`sudo apt install ssh` – instaluje ssh, `sudo /etc/init.d/ssh restart` – ponownie uruchamia ssh by działał, `sudo /etc/init.d/ssh stop` – zatrzymuje ssh, `sudo /etc/init.d/ssh start` – uruchamia demona ssh, `ssh nazwa_użytkownika@adres IP`

### Firewall

`sudo ufw allow proto tcp from 192.168.0.2 to any port 22` – daje dostęp do portu konkretnym hostom bądź albo sieciom. W tym przypadku host o adresie 192.168.0.2 daje dostęp każdemu adresowi IP na tym hoście przez SSH. Gdy zamienimy 192.168.0.2 na 192.168.0.0 to wtedy cała podsieć będzie miała dostęp.

### DNS

DNS tłumaczy nazwy w sieciach na adresy IP. Posiada on 2 strefy wyszukiwania do przodu (domena -> IP) i do tyłu (IP-> nazwa domeny). Najczęściej konfigurujemy podstawowy serwer nazw (primary name server), który posiada kopię bazy danych z nazwami wszystkich hostów w strefie/rekordy dla wszystkich poddomen oraz zapasowy serwer (secondary name server), który zawiera kopię baz danych z rekordami dla domeny i poddomeny.

`sudo apt install bind9` – uruchomienie serwera DNS, `dig` (adres strony www do testowania),

W pliku `named.conf.local` można dodać strefę wyszukiwania do przodu i wstecz.

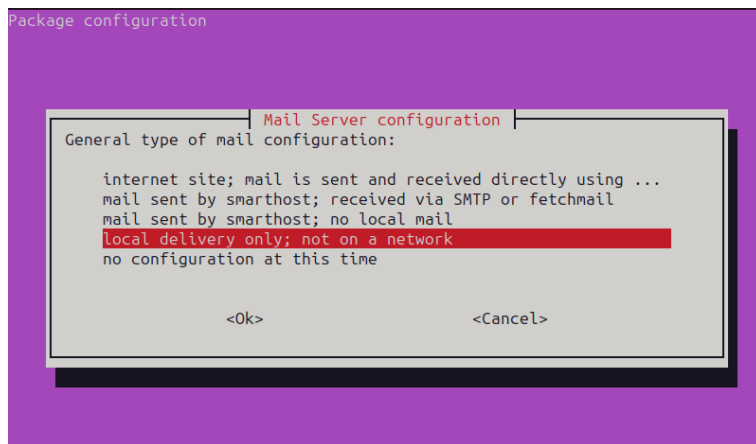
## FTP

Dość wydajnym i szybkim serwerem FTP jest VSFTPD (very secure). Konfiguracja:

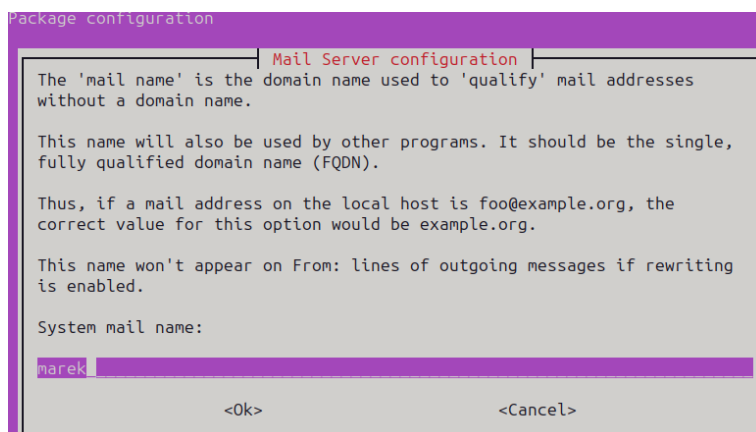
`apt-get install vsftpd -> service vsftpd start` (uruchamiamy usługę) -> `nmap localhost` (sprawdzamy czy usługa jest uruchomiona). Głównym plikiem konfiguracyjnym serwera FTP jest `view /etc/vsftpd.conf`. By serwer FTP był dostępny dla lokalnych użytkowników należy w tym pliku ustawić wartość opcji „`local_enable=YES`.” Potem zapisujemy zmiany i restartujemy: `service vsftpd restart`. By umożliwić logowanie się użytkownikom anonimowym procedura jest taka sama jak lokalnie tylko zamiast „`YES`” wprowadzamy „`NO`”.

## Email

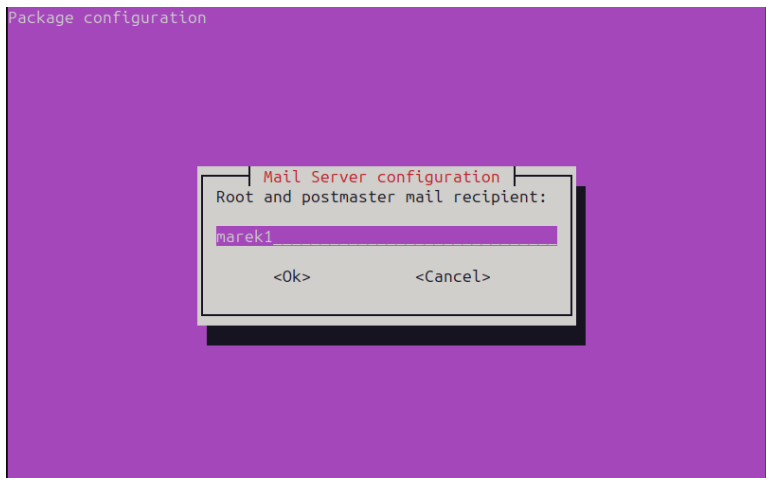
`sudo apt install exim4` – tworzenie poczty lokalnie, `sudo dpkg-reconfigure exim4-config` (uruchamia kreatora konfiguracji serwera), później wybieramy bez dostępu do sieci:



Wprowadzamy nazwę domeny, adres IP do nadchodzących połączeń i klikamy ok:



Wprowadzamy listę domen, dla których serwer jest miejscem docelowym. Przy zapytaniach DNS klikamy „nie”. Format: mbox w /var/mail. Nie dzielić konfiguracji na małe pliki – nie. W polu odbiorca poczty dla kont root:



Na koniec `sudo service exim4 restart`.

Wysyłanie maila: zalogować się na konto użytkownika, połączyć się telnetem przez port 25, później `helo „marek”`, wprowadzić nazwę nadawcy wiadomości np. `mail from marek@zstie.edu.pl`, piszemy nazwę odbiorcy: `rcpt to: marek1@zstie.edu.pl`, wpisać data. Piszemy wiadomość zakończoną kropką w linii poniżej. Kończymy sesję przez „quit”. Wiadomość można odczytać przez zainstalowanie `sudo apt install mailutils`, logujemy się na konto np. `su marek1`, wywołać polecenie „mail”. Wpisać numer wiadomości i enter. Kończymy wpisując „q”.

### **Instalacja strony www – apache2**

W większości dystrybucji Linuxa serwer www jest zainstalowany domyślnie. Jeśli nie, możemy go doinstalować.

`sudo apt update` – aktualizacja paczek

`sudo apt install apache2` – instalacja serwisu www apache2

`apache2 -v2` – weryfikacja czy apache2 został zainstalowany poprawnie

`sudo service apache2 restart`

`nmap localhost` – sprawdzamy adres IP hosta, który jednocześnie będzie adresem strony www

W przeglądarce wpisujemy adres IP hosta i powinna wyświetlić się strona.

## Windows Server 2022 – wprowadzenie

Zarówno standard jak i datacenter wspierają 48TB RAM oraz 2048 logicznych rdzeni. W tej wersji systemu możemy otrzymywać żądania DNS poprzez HTTPS a nie tylko HTTP. Procesor serwera jest chroniony na poziomie sprzętowym, oprogramowania i w przy użyciu sterowników.

W Windows Server 2022 ograniczono rozmiar kontenera by system ładował się 30% szybciej od swoich poprzedników. Przeglądarka Edge została dodana jako domyślna dla systemu.

Mamy 2 główne wersje Windows Server 2022: Server Core i Server Desktopowy. Ten ostatni jest bardziej przyjazny dla użytkownika – np. role serwera w Server Core mogą być zainstalowane poprzez powershella, ale zużywają mniej RAM i mają zwiększoną stabilność. Po instalacji systemu warto sprawdzić w menadżerze urządzeń aktualizacje sterowników.

Pod tym linkiem możemy pobrać obraz ISO po rejestracji czy wykorzystać go w środowisku wirtualnym: <https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2022>

Na maszynie wirtualnej mamy też opcje instalacji obrazu ISO do ewaluacji.

### Active Directory

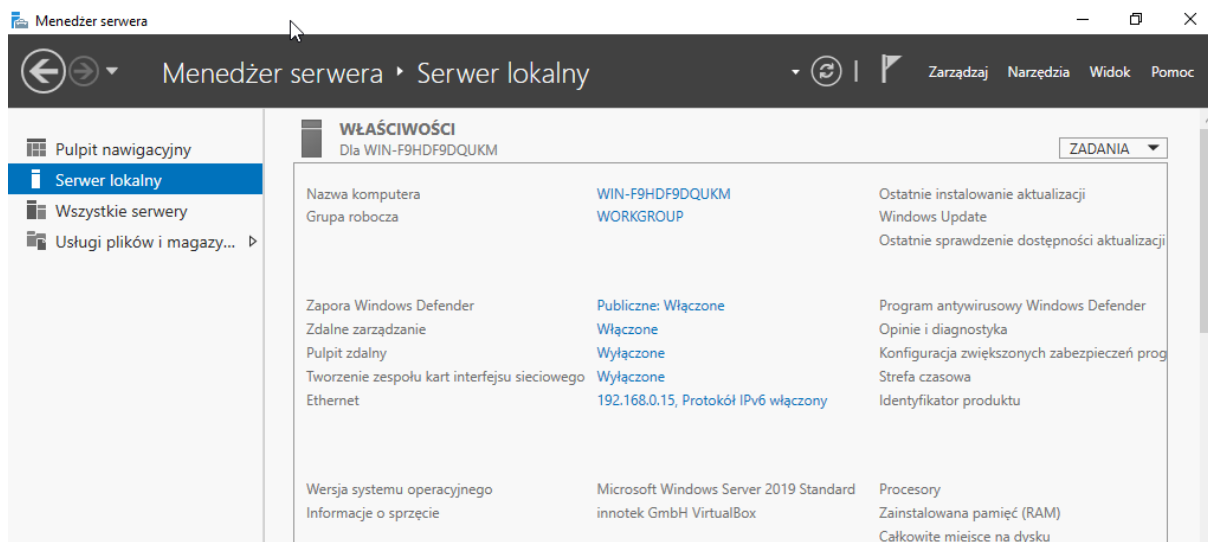
Active Directory DS służy do instalowania kontrolera domeny do istniejącej domeny. Kontroler domeny to komputer, na którym zainstalowano AD. Przechowuje informacje o użytkownikach, komputerach i innych urządzeniach w sieci. Pozwala to administratorom bezpiecznie zarządzać i ułatwia udostępnianie zasobów.

W Active Directory podstawowym elementem konstrukcji jest domena, która jest grupą komputerów połączoną w jedną sieć (serwer jako kontroler domeny i stacji roboczych). Domena jest częścią drzewa, czyli związku wielu domen mających ten sam schemat, konfigurację i hierarchiczną przestrzeń nazw.

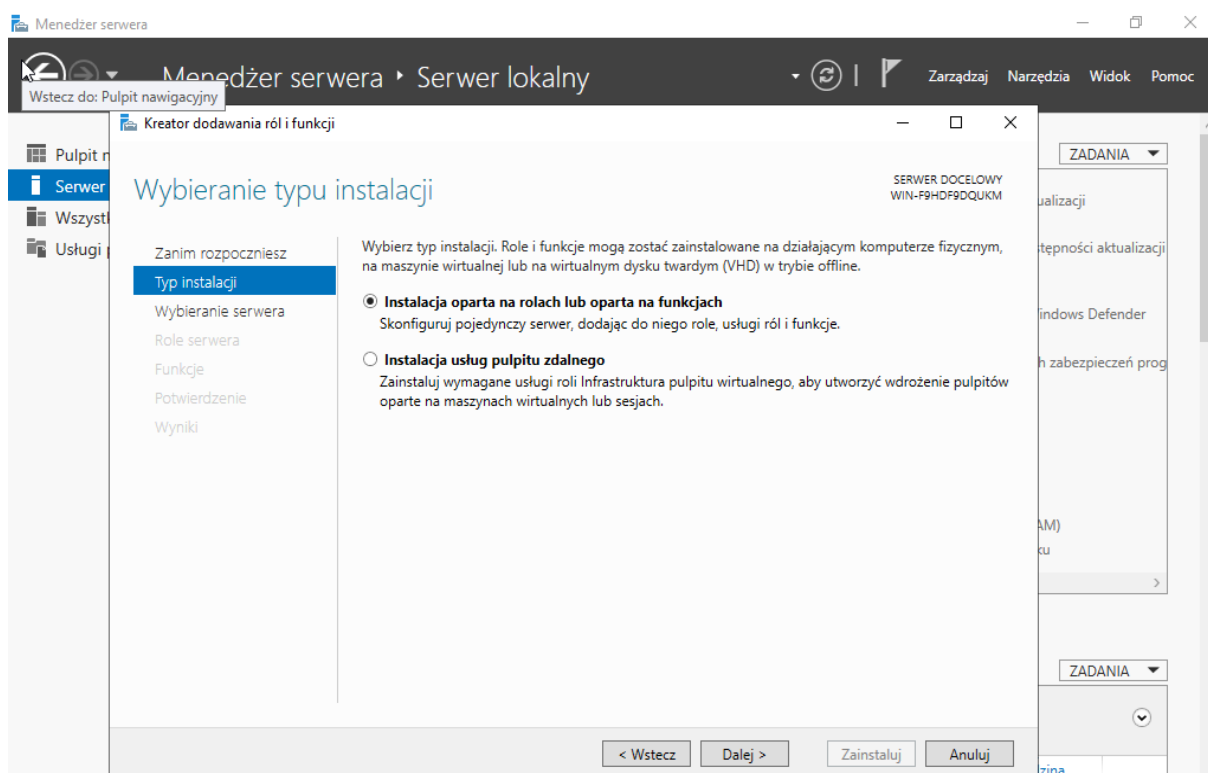
Las to struktura złożona z wielu drzew tylko niemająca ciągłej przestrzeni nazw.

### Instalacja

Uruchamiamy Windows Serwer 2022 dashboard, lecz zanim zainstalujemy rolę upewniamy się że serwer ma statyczny adres IP.

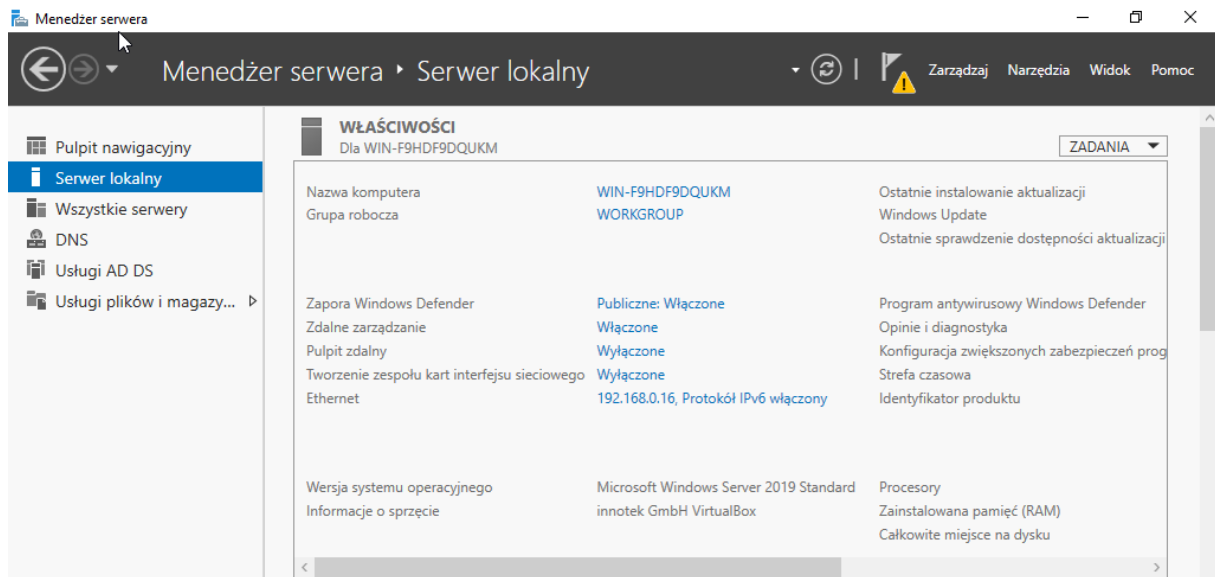


Klikamy zarządzaj -> dodaj role i funkcje a potem:



Potem wybieramy serwer, na którym chcemy AD DS zainstalować. W większości przypadków będziemy wybierać serwer lokalny. Wybieramy Active Directory -> z pop-upu dodaj funkcje -> usługi domenowe Active Directory -> zaznaczamy DNS, który umożliwia rozpoznawanie nazw w sieciach TCP/IP oraz kojarzy nazwę z adresem IP, zapewnia też hierarchiczną strukturę nazw, gwarantującą że każda nazwa hosta będzie unikatowa -> dalej -> dalej->zainstaluj.

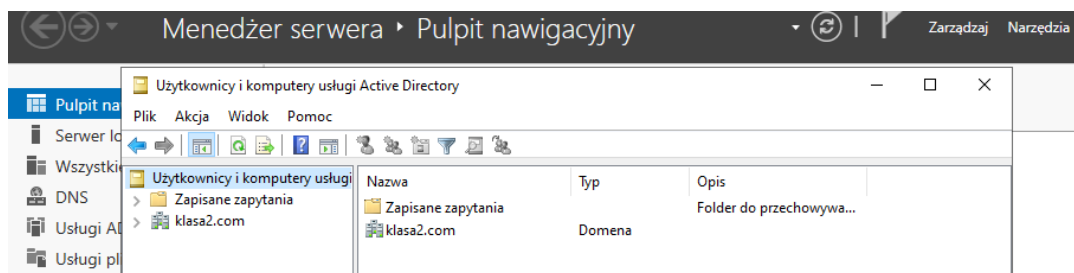
Jeśli AD DS się zainstaluje, promujemy nasz serwer jako kontroler domeny. U góry zobaczymy żółte ostrzeżenie:

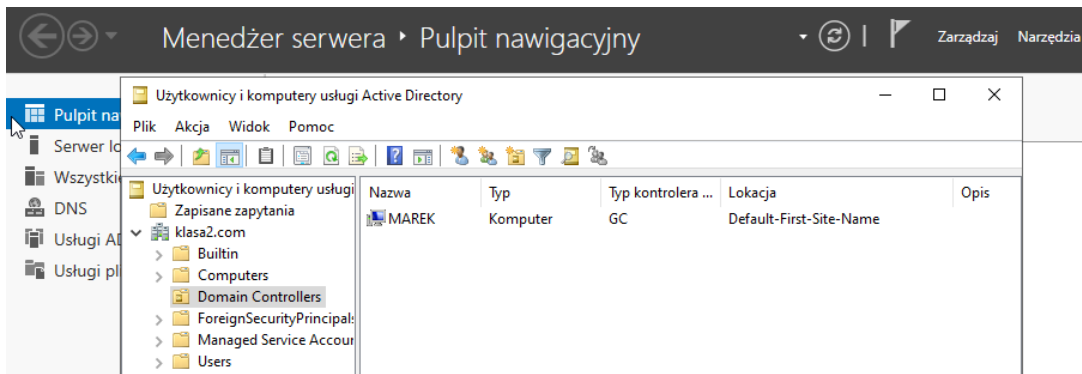


Klikamy promuj serwer. W zależności od tego jak chcemy ten kontroler skonfigurować wpisujemy różne opcje. Jeśli chcemy utworzyć las z domeną typu root o nazwie „klasa2.com” to wpisujemy te informacje we właściwym miejscu. Później ustalamy m.in. jaki system ma być kontrolowany przez kontroler domeny. Zostawiamy wszystko domyślnie i ustalamy hasło. Ignorujemy ostrzeżenie o DNS. Nazwa NETBIOS domeny w tym przypadku to „klasa2” (sam się uzupełnia). NetBIOS (Network Basic Input/Output System) na serwerze to interfejs programowania aplikacji (API) i protokół sieciowy, który umożliwia komunikację między komputerami w sieci lokalnej, w szczególności na urządzeniach korzystających z protokołu TCP/IP. Ułatwia wymianę danych między aplikacjami, np. udostępnianie plików czy drukarek.

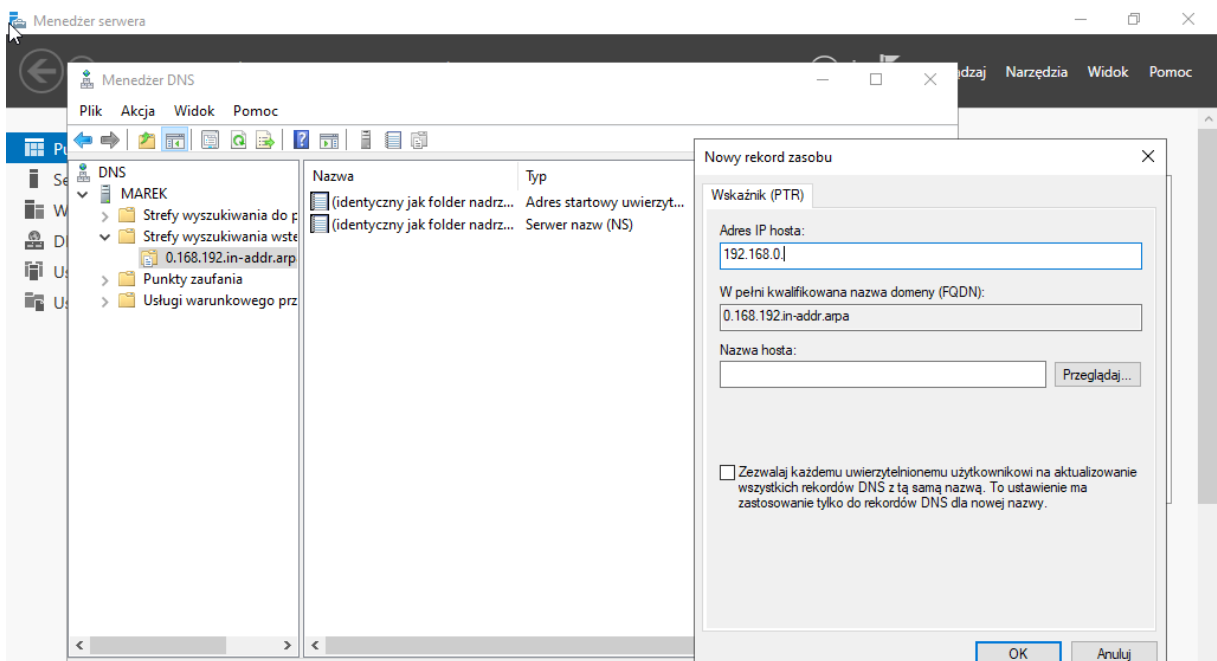
Zostawiamy bazę danych z ustawieniami domyślnymi. Później wyświetla się podsumowanie naszych czynności, klikamy zainstaluj. Serwer po zakończeniu uruchomi się ponownie. Po ponownym uruchomieniu będziemy logować się już do utworzonej domeny. W menadżerze serwera -> narzędzia sprawdzamy czy Active Directory zostało poprawnie zainstalowane, czy nazwa domeny się zgadza. Analogicznie w zakładce narzędzia -> DNS.

W zakładce narzędzia -> użytkownicy Active Directory możemy sprawdzić co stworzyliśmy:

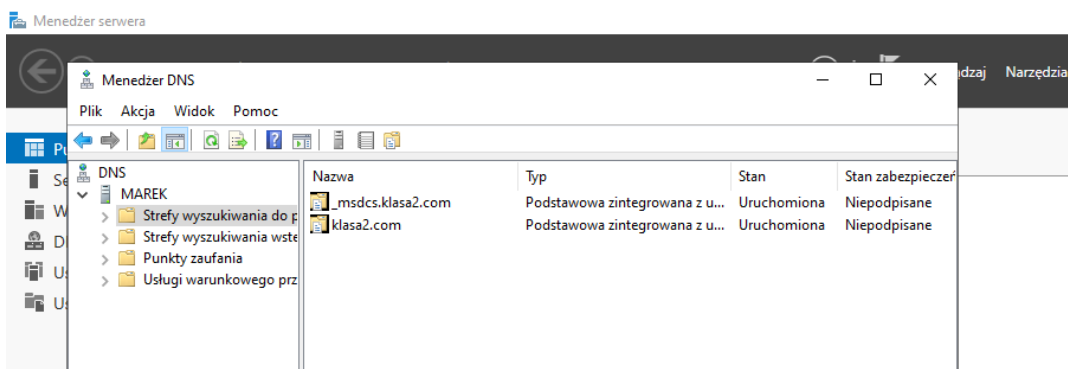




By usunąć Active Directory wchodzimy w menadzerze serwera „usuń rolę i funkcje” -> odznaczamy AD DS. (untick) -> obniżamy poziom -> ponownie uruchamiamy serwer.



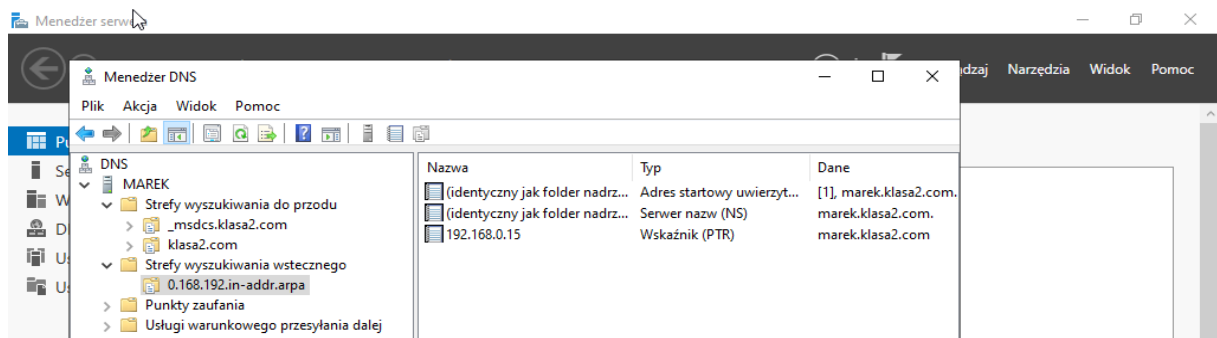
## DNS



Strefa wyszukiwania do przodu zapewnia rozpoznawanie nazwy hosta na adres IP a strefa do tyłu – odwrotnie. By stworzyć strefę wyszukiwania do tyłu klikamy DNS-> strefa wyszukiwania do tyłu -> akcja/prawym przyciskiem myszy: dodaj nową -> 4x dalej -> wpisujemy adres IP sieci -> zakończ.

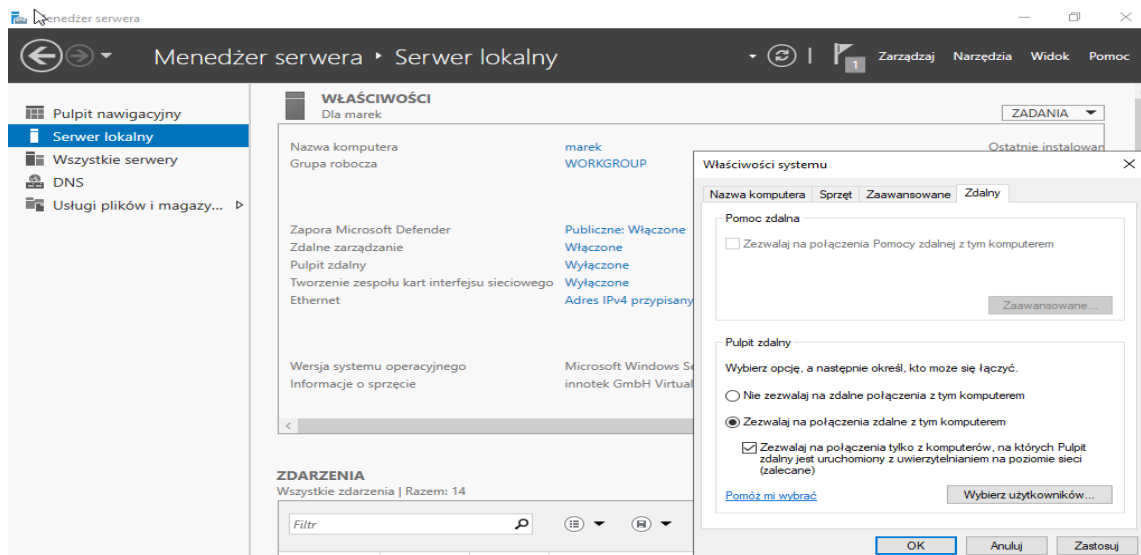
Teraz skonfigurujemy nowy wskaźnik.

Klikamy przeglądamy -> 2x Marek -> 2x strefy wyszukiwania do przodu -> wybieramy klasa2.com -> klikamy nasz serwer marek -> ok:



Teraz w karcie sieciowej serwera możemy wpisać adres DNS naszego hosta.

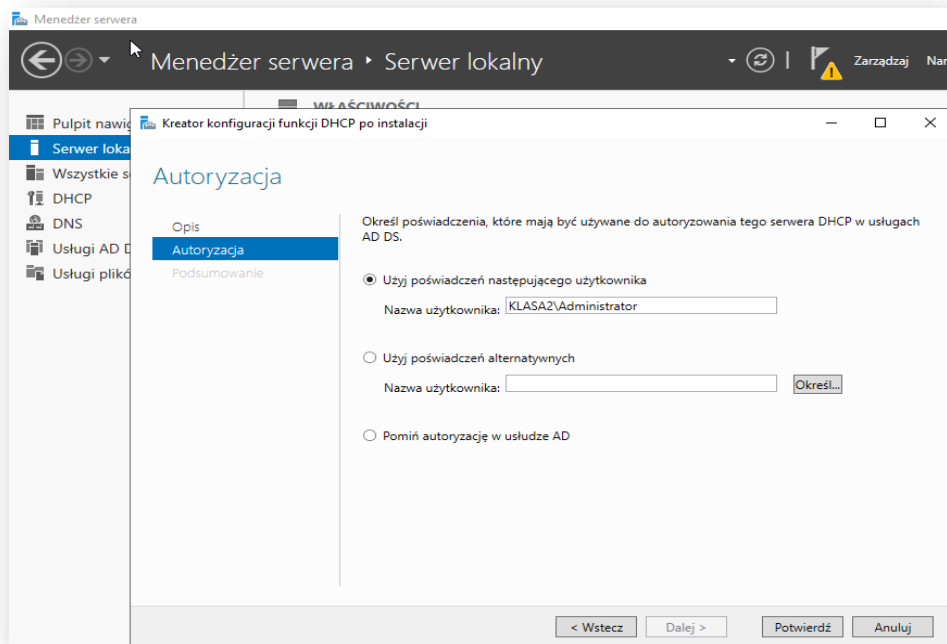
Pulpit zdalny włączamy w serwerze lokalnym klikając na niebieskie pole (z wyłączone na włączone) a później:



## Instalacja roli DHCP

DHCP przypisuje automatycznie nie tylko adresy IP, ale także bramę domyślną, maskę podsieci oraz serwery DNS klientowi w sieci. Instrukcja:

Klikamy: zarządzaj -> dodaj role i funkcje, 3x dalej, zaznaczamy Serwer DHCP -> dodaj funkcje -> 3x dalej -> zainstaluj (nie jest wymagany restart serwera) -> zamknij. Klikamy w wykrzyknik u góry -> dokończ konfigurację funkcji DHCP -> teraz musimy dodać grupy zabezpieczeń oraz autoryzować serwer DHCP na komputerze docelowym. W tym przypadku jesteśmy zalogowani jako administrator więc zostaniemy przy ustawieniach domyślnych i klikamy potwierdź i zamknij:



Teraz otwieramy konsolę do zarządzania serwerem DHCP. Klikamy narzędzia -> DHCP -> klikamy po lewej w nazwę domeny -> ipv4 -> klikamy prawym na ipv4 -> nowy zakres -> wpisujemy nazwę i opis -> wpisujemy pulę adresów i maskę -> teraz określamy jakie adresy mogą być wykluczone z puli (można zostawić puste) -> definiujemy czas dzierżawy -> klikamy dalej -> dodajemy adres IP routera -> nazwa domeny powinna uzupełnić się automatycznie -> serwer WINS już nie jest obecnie używany więc można go pominąć -> aktywujemy zakres i zakończ. Teraz jeśli DHCP mamy aktywowane, serwer będzie automatycznie przydzielał adresy IP automatycznie.

### **Przyłączanie stacji roboczej do domeny**

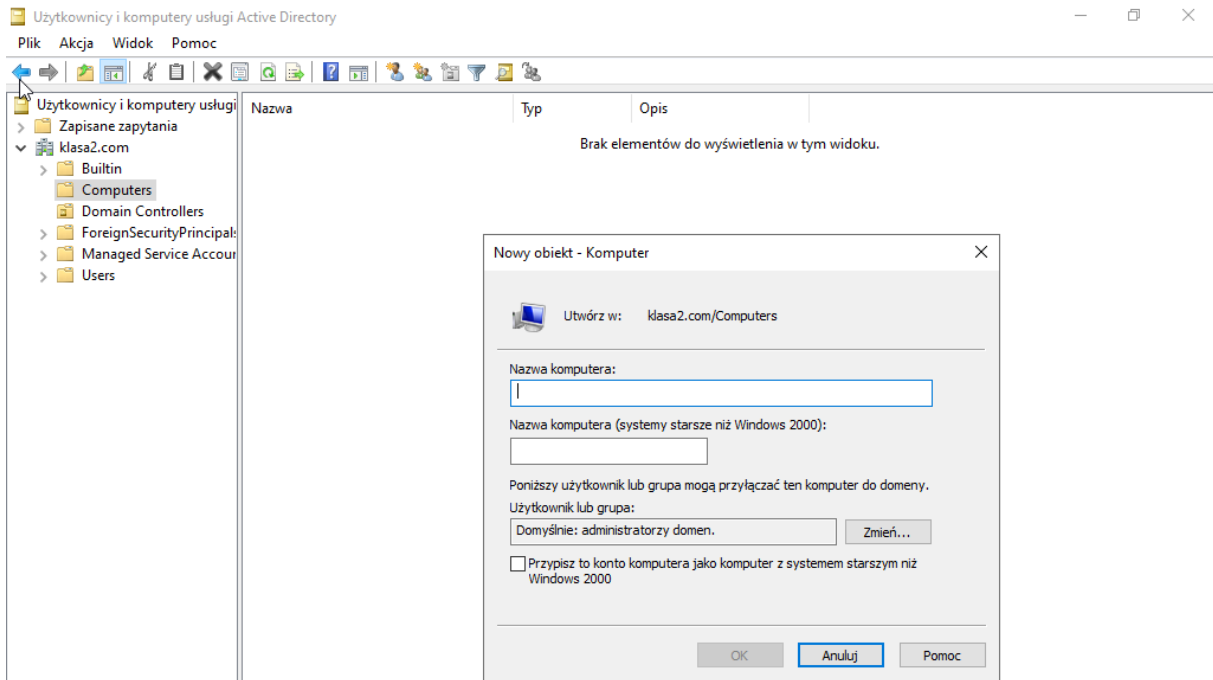
Nie ma możliwości przyłączenia Windows 11 Home do domeny lokalnej.

Najpierw należy zsynchronizować czas na Windows 11 z serwerem dla uwierzytelnienia Kerberos, które weryfikuje tożsamość użytkowników za pomocą systemu „biletów”. Wykorzystuje kryptografię z kluczami tajnymi i zaufaną stroną trzecią do weryfikacji tożsamości użytkowników i uwierzytelniania aplikacji typu klient-serwer.

Uruchamiamy Windows 11 lokalnie z skonfigurowaną obsługą DHCP serwer. Uruchamiamy CMD i pingujemy nazwę domeny. Po pingu DNS powinien odzwierciedlić w komunikacie właściwy adres IP.

Na kliencie klikamy ustawienia -> konta -> access work or school -> u góry po prawej „połącz” -> połącz to urządzenie z lokalną domeną -> wpisujemy nazwę domeny -> dalej -> wpisujemy login i hasło admina -> pomiń -> uruchamiamy ponownie -> na kliencie logujemy się do konta domenowego.

Możemy też dodać klienta z serwera. Klikamy w „użytkownicy i komputery usługi AD”:



Podczas konfiguracji delegujemy uprawnienia dla tego komputera. Na kliencie logujemy się lokalnie, zmieniamy nazwę komputera, z grupy roboczej przyłączamy do domeny i wpisujemy jej nazwę.

### **Dodawanie klienta do domeny Windows 10**

Na serwerze w zakładce użytkownicy i komputery usługi AD klikamy na „computers”, prawym nowy -> komputer -> wpisujemy nazwę komputera klienta.

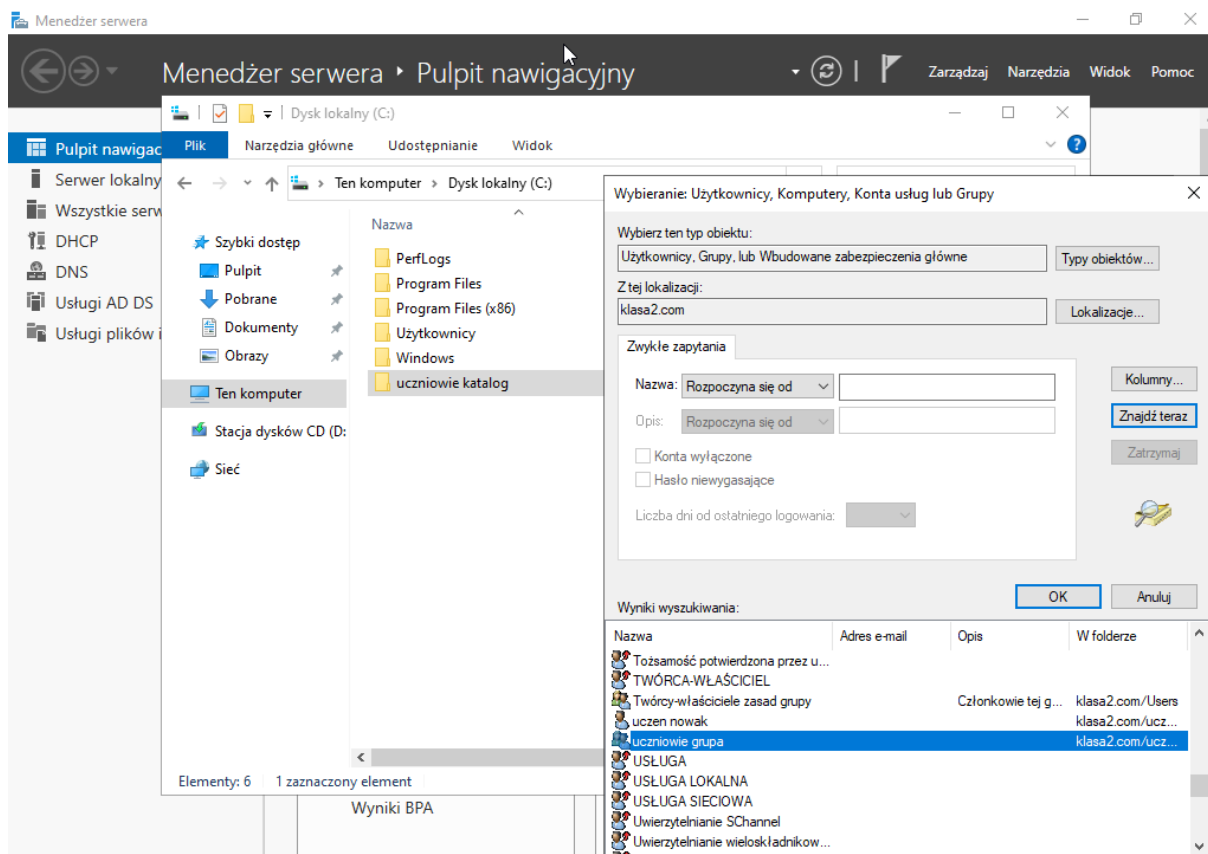
Na kliencie: w zmień nazwę komputera (zaawansowane) zmieniamy z grupa robocza na domena -> wpisujemy nazwę domeny -> jeśli na karcie sieciowej klienta nie ma adres DNS serwera to należy go wpisać, uruchamiamy ponownie klienta.

### **Tworzenie grup i użytkowników**

By utworzyć grupę lub użytkownika w AD wchodzimy w narzędzia -> użytkownicy i komputery AD -> prawym kliknięciem w nazwę domeny -> nowy -> jednostka organizacyjna -> wpisujemy nazwę np. uczniowie -> ok. By stworzyć użytkownika w tym katalogu klikamy prawym -> nowy -> użytkownik -> wpisujemy nazwę i określamy zasady hasła. Jeśli dołączyłeś już stację roboczą do serwera to możesz zalogować się jako nowy użytkownik.

Tworzenie grupy. Klikamy prawym na utworzony katalog „uczniowie” -> prawym -> nowy -> grupa -> np. grupa uczniowie -> ok. Możemy na partycji :C serwera utworzyć katalog o nazwie „uczniowie”

i ustalić by tylko użytkownicy o nazwie „uczniowie” mieli dostęp do katalogu -> klikamy prawym właściwości -> udostępnianie -> udostępnianie zaawansowane -> udostępnij ten folder -> uprawnienia -> wszyscy (usuń) -> dodaj -> zaawansowane -> znajdź teraz -> grupa uczniowie -> 2x ok -> ustalamy uprawnienia.



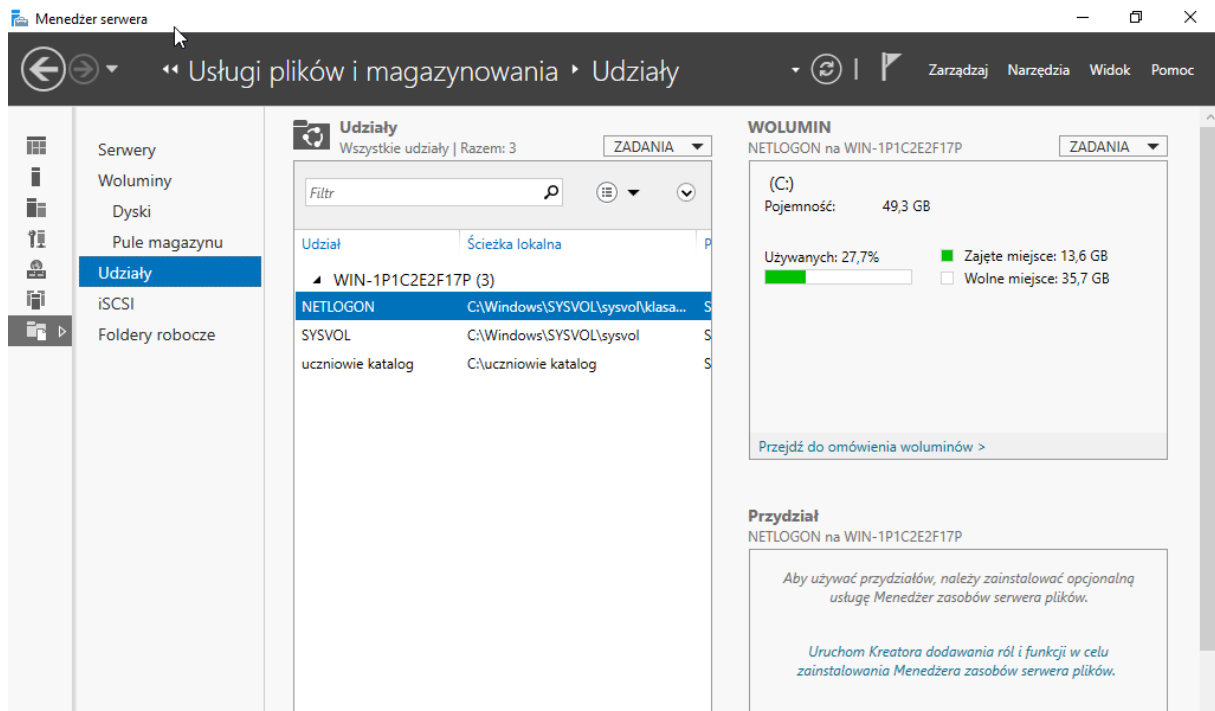
Następnie, logując się z klienta -> wpisując w CMD \\nazwę użytkownika domenowego sprawdzamy czy katalog będzie dostępny. Nie mamy dostępu. Musimy wrócić do serwera i użytkowników

i komputerów Active Directory -> prawym -> uczniowie grupa -> właściwości -> członkowie (jest pusto) -> dodaj -> zaawansowane -> znajdź teraz -> dodajemy „uczen nowak”, 2x ok i zastosuj. Na kliencie należy ponownie zalogować się jako „uczen nowak” i sprawdzić czy mamy dostęp do katalogu.

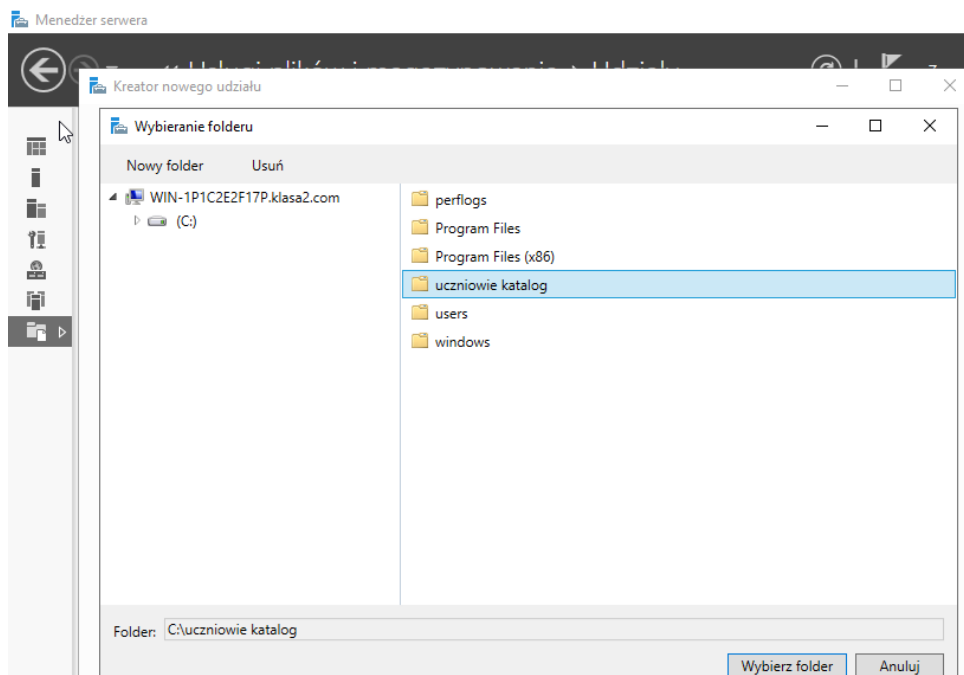
## Tworzenie współdzielonego katalogu

Możemy utworzyć katalog na 1 komputerze, do którego będą mieli dostęp użytkownicy w tej samej sieci pracując na innych komputerach. By to zrobić na Windows Server 2022 możemy użyć eksplorator plików, menadżer serwera, PowerShell lub komendy w wierszu poleceń. Tym razem

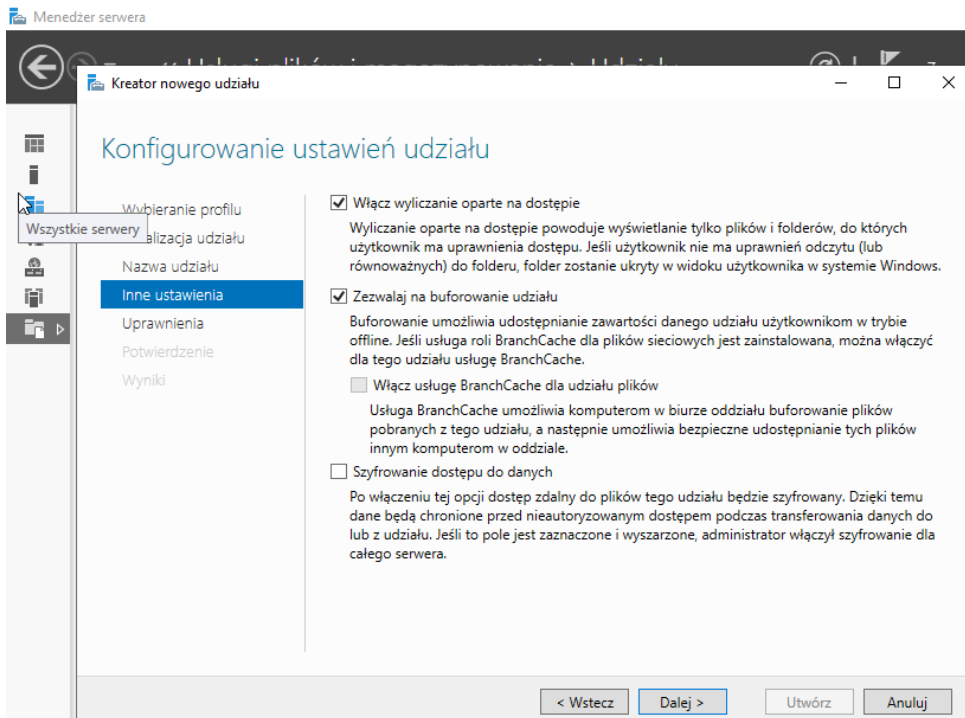
w menadżer serwera -> narzędzia -> użytkownicy i komputery usługi Active Directory -> sprawdzamy jakich użytkowników utworzyliśmy i jakie mają uprawnienia. Później wchodzimy znowu w menadżer serwera -> po lewej usługi plików i magazynowania -> klikamy w udziały -> teraz widzimy aktualnie używane foldery:



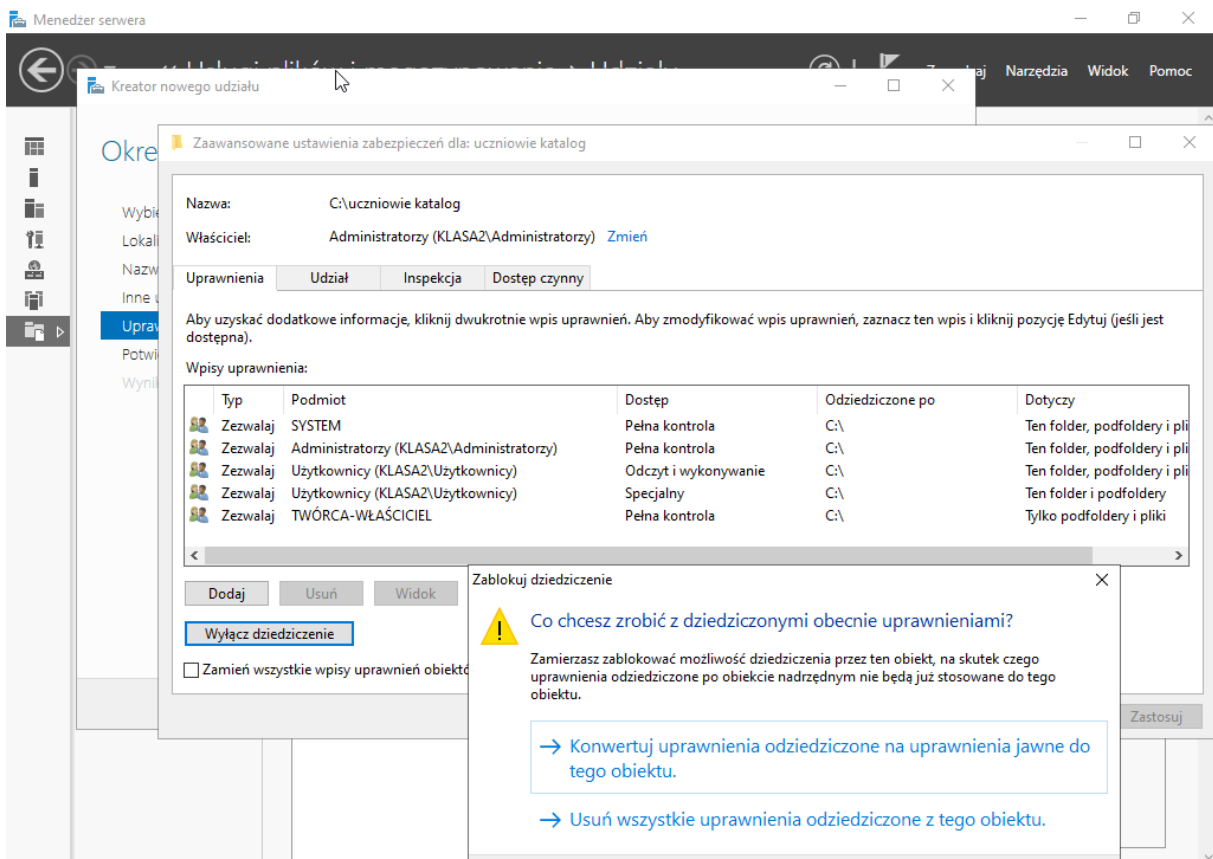
Jako że jest to serwer domenowy mamy 3 współdzielone pliki NETLOGON, Sysvol i uczniowie katalog. Klikamy w zadania -> nowy udział -> udział SMB szybkie -> dalej -> wpisz ścieżkę niestandardową (przełącznik) -> wybieramy katalog, który ma być udostępniony -> albo po lewej możemy utworzyć nowy folder do udostępniania:



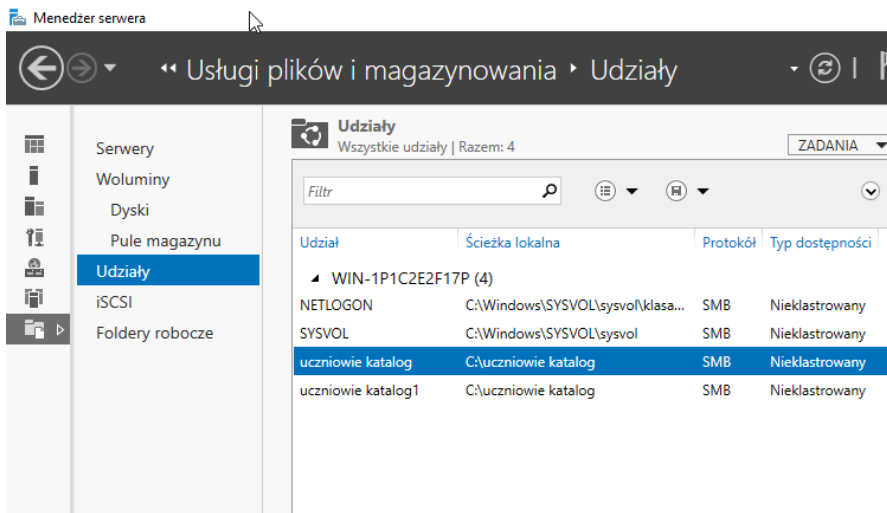
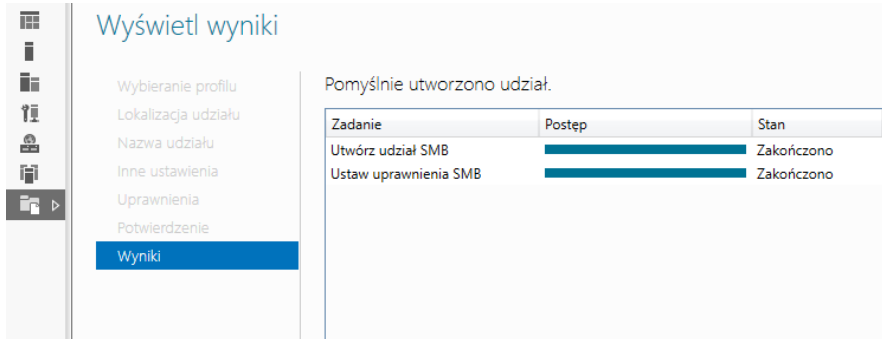
Jak klikniemy wybierz katalog klikamy dalej. Zobaczymy ścieżkę lokalną i zdalną do tego katalogu. Zaznaczamy pierwsze 2 opcje:



Klikamy dalej. Domyślnie serwer ustawia dzielenie plików jako pełną kontrolę. Klikamy w dostosowanie uprawnień a potem wyłącz dziedziczenie a potem konwertuj uprawnienia odziedziczone... a potem usuwamy obu użytkowników.



Teraz klikamy w dodaj by ustalić uprawnienia konkretnej grupy do katalogu -> wybierz podmiot zabezpieczeń -> wpisz nazwę użytkowników i grup, którym chcesz przydzielić dostęp – najlepiej to zrobić poprzez sprawdzenie nazwy, by format był zgodny z AD. Klikamy ok i określamy rodzaj uprawnienia i ok, zastosuj i ok. Klikamy dalej by kontynuować -> klikamy utwórz. Nasz katalog został utworzony i jest gotowy do użycia:

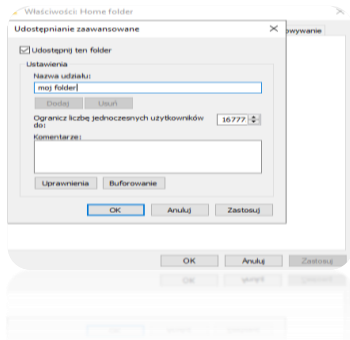


By sprawdzić czy to działa przejdź do systemu klienckiego Win 10 lub Win11. Zaloguj się jako ten użytkownik domeny (w tym przypadku uczeń nowak). W CMD wpisz adres IP serwera lub \\nazwę serwera.

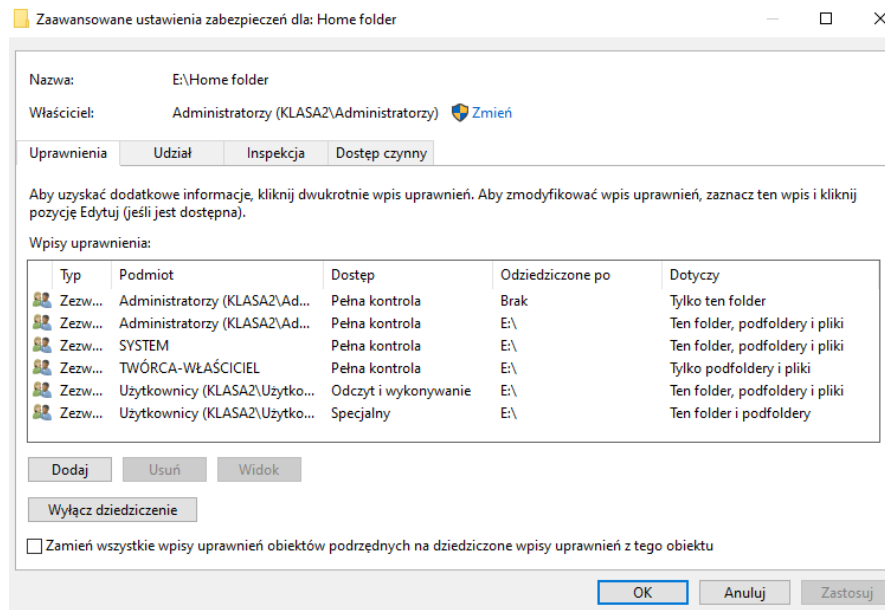
## Folder macierzysty w Active Directory

Folder macierzysty jest prywatną lokalizacją użytkowników, gdzie mogą przechowywać pliki osobiste. Są one przechowywane na serwerze i z definicji nie powinny być dostępne dla innych użytkowników.

Zaczynamy od utworzenia na serwerze katalogu, najlepiej na partycji niesystemowej. Klikamy w niego prawym przyciskiem myszy -> właściwości -> udostępnianie -> udostępnianie zaawansowane -> udostępni folder (jeśli na końcu nazwy udziału mamy „\$” - stanie się niewidoczny dla użytkowników):



Klikamy w uprawnienia w tym samym okienku. Zaznaczmy pełną kontrolę dla wszystkich użytkowników. Zastosuj -> ok ->ok. Następnie klikamy w zabezpieczenia-> zaawansowane:



Klikamy w wyłączyć dziedziczenie -> konwertuj... Usuwamy domyślnych użytkowników, w tym przypadku „Użytkownicy (Klasa2...)”. Zastosuj -> ok.

Wracamy do zakładki udostępnianie i tam kopiujemy ścieżkę sieciową katalogu.

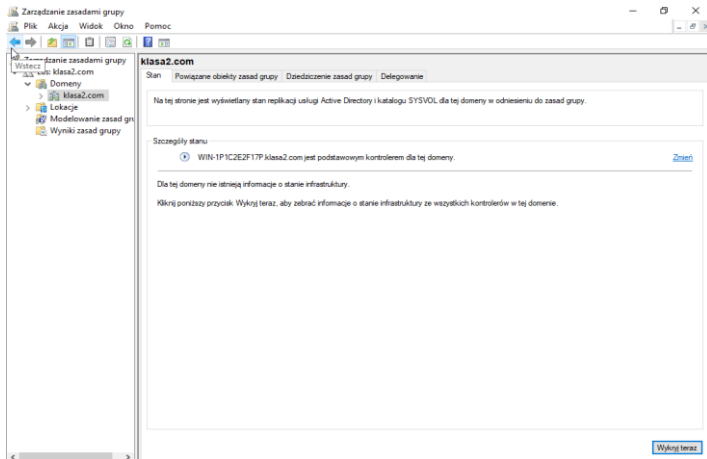
W menadżerze serwera wchodzimy w narzędzia -> użytkownicy i komputery AD. W moim przypadku w grupie uczniowie zaznacz użytkowników, którzy mają mieć dostęp do folderu macierzystego i kliknij prawym -> właściwości. Wchodzimy w zakładkę „profil” -> podłącz -> z listy „h” by zachować porządek (h od home folder) -> do -> wklejamy skopiowaną ścieżkę z \$ i dopisując %username% na końcu. Sprawdź w użytkownikach AD-> właściwości -> profil czy ścieżka tego katalogu jest widoczna.

Wchodząc na eksploratorze plików w nasz folder powinna być widoczna nazwa użytkownika, która ma do niego dostęp.

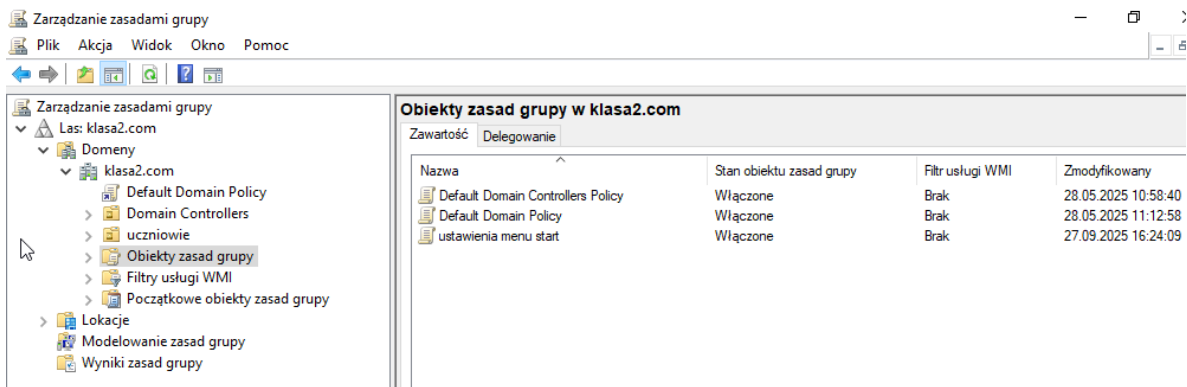
**Zarządzanie zasadami grupy w AD** (w tym wyłączenie na kliencie opcji z pola start: wyłącz i restart)

Zarządzanie zasadami grupy określa sposób grupy użytkowników i komputerów będą się zachowywać, może być wdrożona na stronach www, domenach czy jednostkach

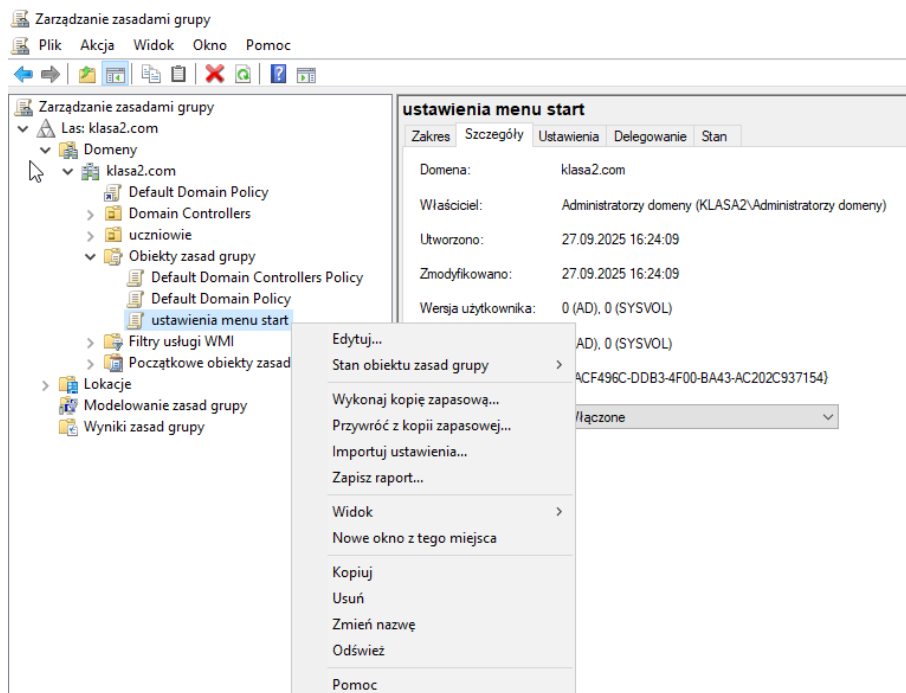
organizacyjnych (OU). By to skonfigurować wchodzimy w narzędzia -> zarządzanie zasadami grupy. Po lewej stronie okienka rozwijamy domenę (w tym przypadku klasa2.com):



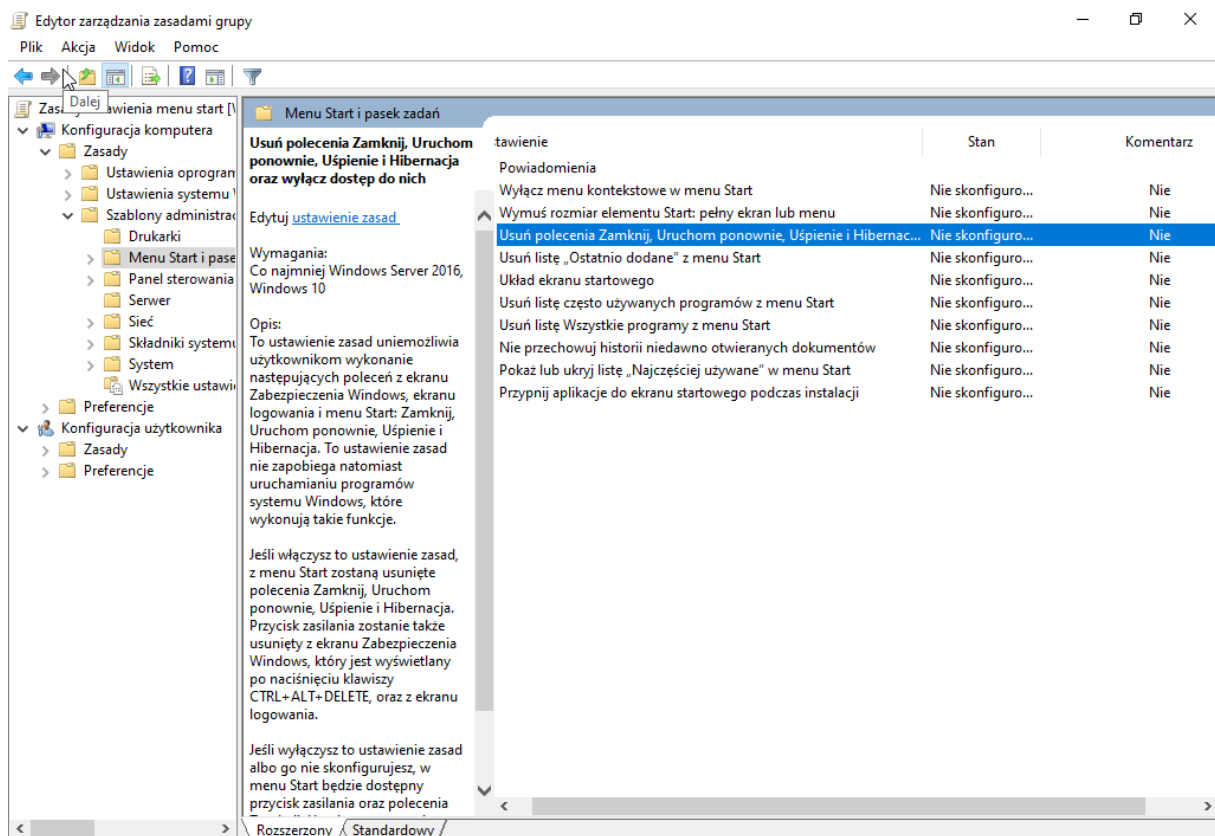
Po 2-krotnym kliknięciu w domenę, klikamy w obiekty zasad grupy. Te zasady dotyczą wszystkich użytkowników tej domeny. By utworzyć nowe zasady grupy klikamy prawym przyciskiem myszy w obiekty zasad grupy -> nowe -> określamy nazwę (tutaj ustawienia menu start) -> ok.



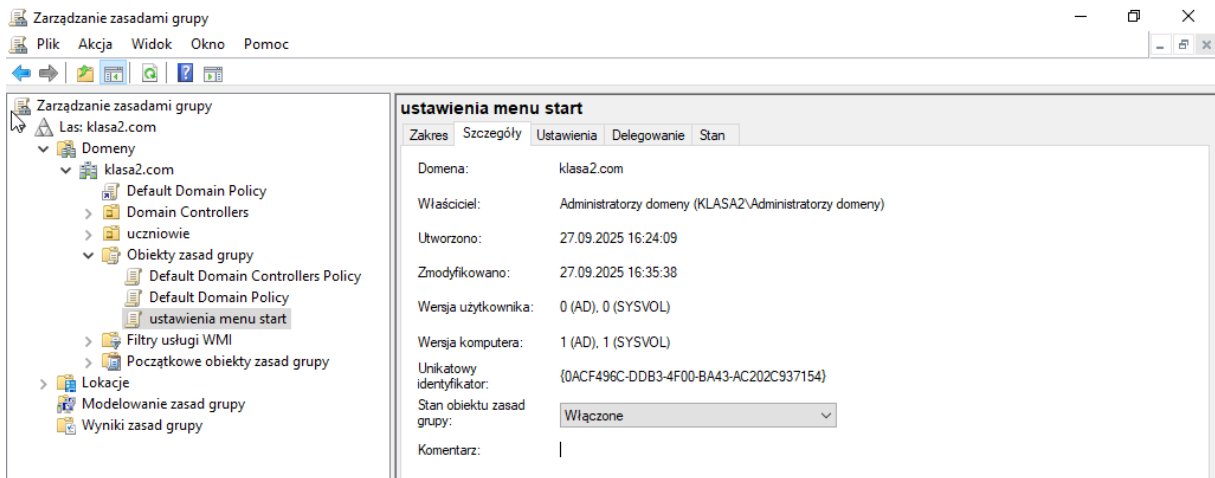
Dwukrotnie klikamy w obiekty zasad grupy a potem w nowoutworzone zasady grupy. By zmodyfikować nasze zasady klikamy prawym -> edytuj:



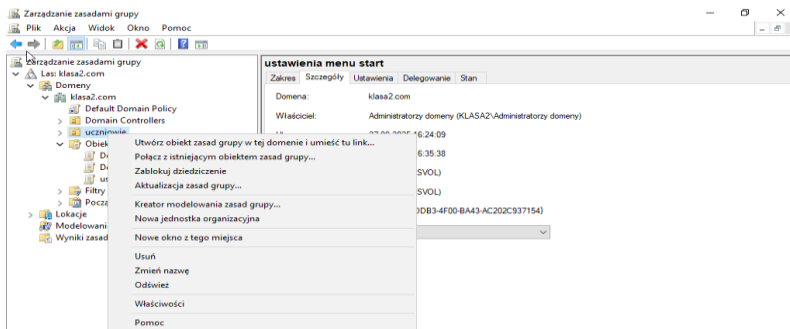
Mamy tutaj 2 rodzaje konfiguracji: użytkownika (gdy loguje się użytkownik) lub komputera (gdy uruchamia się system). By zrobić to co chcemy pierwotnie klikamy w konfigurację komputera -> zasady -> szablony administracyjne -> menu start i pasek zadań -> usuń polecenia zamknij... Możemy tutaj stosować różne zasady grupy. W tym konkretnym przykładzie usuwamy użytkownikowi możliwość wyłączenia PC:



Klikamy dwukrotnie w niebieskie pole -> włączone -> zastosuj -> ok. gdy odświeżymy u góry przycisk, zobaczymy że nasza zasady grupy została wdrożona:



Łączymy grupę uczniowie z utworzonym obiektem zasad grupy:



Później klikamy „ustawienia menu start” – w moim przypadku. Ok.

Przejdź do klienta, zaloguj się do domeny. Jeszcze powinna być opcja wyłączenia PC z menu start. Wdrożenie zajmuje 90 minut – możemy wymusić akcję wpisując w CMD na PC komendę gpupdate /force