

MikroTik router

Linux Server | Domain Controller | Active Directory | DNS | DHCP

Windows client

TARTALOMJEGYZÉK

1. MikroTik router.....	1
1.1 A MikroTik router konfigurálása	1
2. Linux Server Domain Controller Active Directory DNS DHCP	1
2.2 A szerver kezdeti konfigurálása	3
2.2.1 Az IP címzés beállítása.....	3
2.2.2 Hosts fájl konfigurálása.....	4
2.2.3 Hostname beállítása.....	4
2.2.4 Az IP címzés ellenőrzése.....	6
2.2.5 A Sudo beállítása.....	6
2.2.6 A „Guest Additions” kiegészítő telepítése	6
2.3 Fájlrendszer paraméterek beállítása	7
2.4 Időzóna konfigurálása	8
2.5 Samba Active Directory telepítése és konfigurálása	8
2.6 DHCP szolgáltatás telepítése, konfigurálása.....	10
3. Windows kliens	10
3.1 A Windows kliens tartományba léptetése	11
3.2 Remote Server Administration Tools (RSAT) telepítése és használata	11
3.3 A DNS szolgáltatás konfigurálása.....	12
3.4 Active Directory szervezeti egységek felhasználók csoportok felvétele	12
4. A Samba Domain Controller működésének ellenőrzése	13

A telepítéseknél az operációs rendszerek újabb, próba (trial) verzióit is használhatjuk!

Mindig ellenőrizzük, hogy a hivatalos letöltési oldalakon vannak-e újabb megjelenések!

A segédletet a készítő engedélye és beleegyezése nélkül felhasználni és másolni szigorúan tilos!

1. MikroTik router

Telepítsük a MikroTik router-t a már tanult módon!

1.1 A MikroTik router konfigurálása

```
interface/print
```

```
ip/dhcp-client/add disabled=no interface=ether1
```

```
ip/address/add interface=ether2 address=172.16.0.1/16
```

```
ip/dhcp-client/add disabled=no interface=ether3
```

```
ip/address/print
```

```
ip/firewall/nat/add chain=srcnat action=masquerade out-interface=ether1
```

```
ip/firewall/nat/add chain=dstnat action=dst-nat in-interface=ether3 dst-port=2222 to-addresses=172.16.0.254 to-ports=22 protocol=tcp
```

(Az SSH kapcsolat használatához engedélyezzük a 22-es port-ot, így a szerverhez tudunk majd a 2222-es porton keresztül kapcsolódni terminálemulátor szoftveren keresztül)

```
ip/firewall/nat/print
```

2. Linux Server | Domain Controller | Active Directory | DNS | DHCP

Hozunk létre a VirtualBox-ban egy új virtuális gépet az alábbiak szerint:

Name: linux_server_dc_ad_dns_dhcp

Type: Linux

Version: Debian 12 Bookworm (64 bit)

Base Memory: 8GB

Processors: 2

A memória mennyisége és a CPU magok száma a gazdagépben lévő fizikai RAM mennyiségének és CPU magok számának függvénye!

Disk Size: 20 GB

A virtuális gép konfigurálása:

System/Motherboard → Boot Order: floppy-t vegyük ki a boot sorrendből

Storage: helyezzük be az optikai meghajtóba a Debian ISO-t, a vdi lemezképre kapcsoljuk be a „Solid-state Drive”-ot (amennyiben SSD-re telepítünk)

Network/Adapter 1: NAT kártya

Indítsuk el a virtuális gépet, és telepítsük az alábbiak szerint:

Install

Select a language | Language: *English*

Select your location | Country, territory or area: *United Kingdom*

Configure the keyboard | Keymap to use: *Hungarian*

Configure the network | Hostname: *linuxserverdc*

Configure the network | Domain name: *xycompany.xy*

Set up users and passwords

Root password: *#Aa123456789@*

Full name for the new user: *LinuxServerDCAdmin*

Username for your account: *linuxserverdcadmin*

Choose a password for the new user: *#Bb123456789@*

Partition disks | Partitioning method → *Manual*

1. New partition size: 15 GB | Type: Primary | Location: Beginning | Use as: Ext4 | Mount point: / | Label: linuxserverdc | Bootable flag: on

2. New partition size: 3.25 GB | Type: Logical | Location: Beginning | Use as: Ext4 | Mount point: /home | Label: home | Bootable flag: off

3. New partition size: 3.2 GB | Type: Logical | Use as: swap area | Bootable flag: off

Configure the package manager

Scan extra installation media? → *No*

Debian archive mirror country → *United Kingdom*

Debian archive mirror: *deb.debian.org*

HTTP proxy information (blank for none): hagyjuk üresen → *Continue*

Configuring popularity-contest | Participate in the package usage survey? → *No*

Software selection | Choose software to install:

- *SSH server*

- *standard system utilities*

Configuring grub-pc | Install the GRUB boot loader to your primary drive? → *YES*

Configuring grub-pc | Device for boot loader installation: */dev/sda*

Finish the installation → *Continue*

2.2 A szerver kezdeti konfigurálása

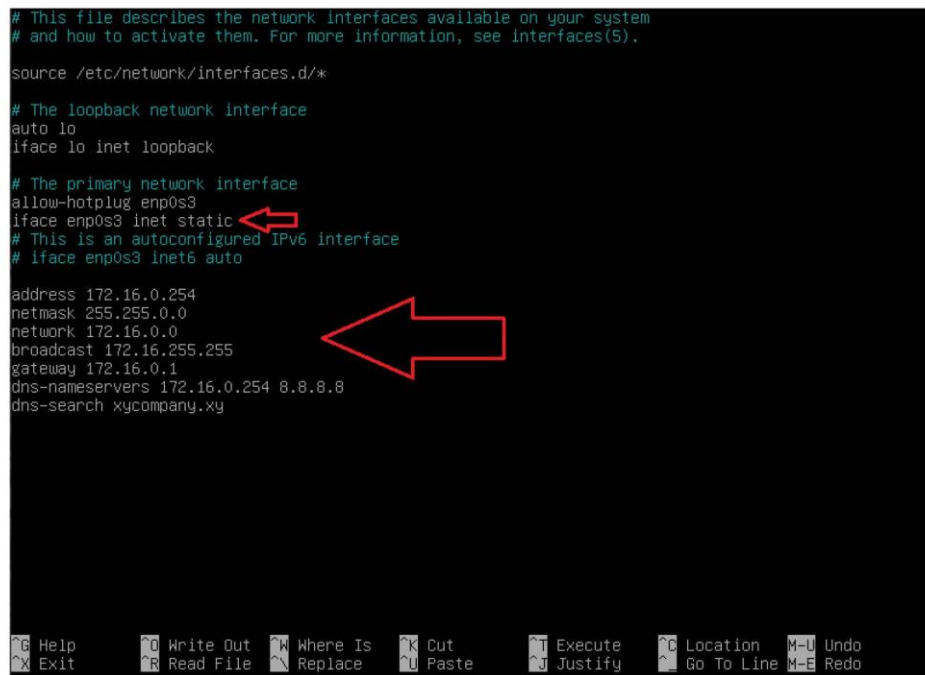
A rendszer újraindulása után jelentkezzünk be a **root** felhasználóval!

2.2.1 Az IP címzés beállítása

Az IP címeket az `/etc/network/interfaces` fájlban tudjuk konfigurálni:

`nano /etc/network/interfaces`

```
iface enp0s3 inet static
address 172.16.0.254
netmask 255.255.0.0
network 172.16.0.0
broadcast 172.16.255.255
gateway 172.16.0.1
dns-nameservers 172.16.0.254 8.8.8.8
dns-search xycompany.xy
```



```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug enp0s3
iface enp0s3 inet static
# This is an autoconfigured IPv6 interface
# iface enp0s3 inet6 auto

address 172.16.0.254
netmask 255.255.0.0
network 172.16.0.0
broadcast 172.16.255.255
gateway 172.16.0.1
dns-nameservers 172.16.0.254 8.8.8.8
dns-search xycompany.xy
```

Mentsük a fájlt és lépünk ki!

2.2.2 Hosts fájl konfigurálása

A gazdagép/tartományneveket IP címekké fordítani az */etc/hosts* fájlban tudjuk:

`nano /etc/hosts`

```
127.0.0.1 localhost
172.16.0.254 linuxserverdc.xycompany.xy linuxserverdc
```

```
127.0.0.1      localhost
172.16.0.254   linuxserverdc.xycompany.xy   linuxserverdc

# The following lines are desirable for IPv6 capable hosts
::1           localhost ip6-localhost ip6-loopback
ff02::1       ip6-allnodes
ff02::2       ip6-allrouters
```

Mentsük a fájlt és lépünk ki!

2.2.3 Hostname beállítása

A gép hostnevét a */etc/hostname* fájlban tudjuk megadni:

`nano /etc/hostname`

```
linuxserverdc
```

```
linuxserverdc
```

Mentsük a fájlt és lépünk ki!

Állítsuk le a szerveret!

`systemctl poweroff`

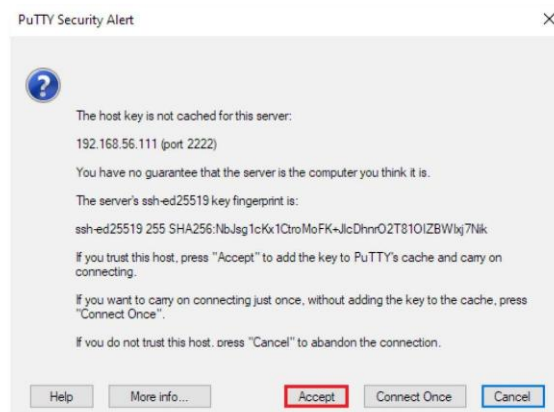
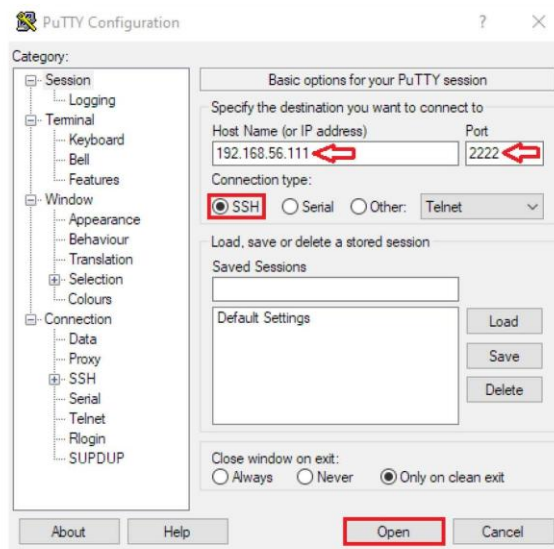
A virtuális gépben konfiguráljuk a hálózati kártyát: a "NAT" kártyát állítsuk "Internal Network"-re!

Indítsuk el újra a szerveret és lépünk be Putty-val SSH-n keresztül a **linuxserverdcadmin** felhasználóval!

A Putty-ba a MikroTik-ben az **ether3** interfészre DHCP-ről kapott IP címet **(természetesen mindenki a sajátját)** kell beírunk az alábbiak szerint:

```
[admin@MikroTik] > ip/address/print
Flags: D - DYNAMIC
Columns: ADDRESS, NETWORK, INTERFACE
# ADDRESS NETWORK INTERFACE
0 172.16.0.1/16 172.16.0.0 ether2
1 D 10.0.2.15/24 10.0.2.0 ether1
2 D 192.168.56.111/24 192.168.56.0 ether3
[admin@MikroTik] > ip/firewall/nat/print
Flags: X - disabled, I - invalid; D - dynamic
0 chain=srcnat action=masquerade out-interface=ether1

1 chain=dstnat action=dst-nat to-addresses=172.16.0.254 to-ports=22
protocol=tcp in-interface=ether3 dst-port=2222
[admin@MikroTik] >
```



login as: **linuxserverdcadmin**

password: **#Bb123456789@**

2.2.4 Az IP címzés ellenőrzése

`ip address`

2.2.5 A Sudo beállítása

`su -`

`apt install sudo`

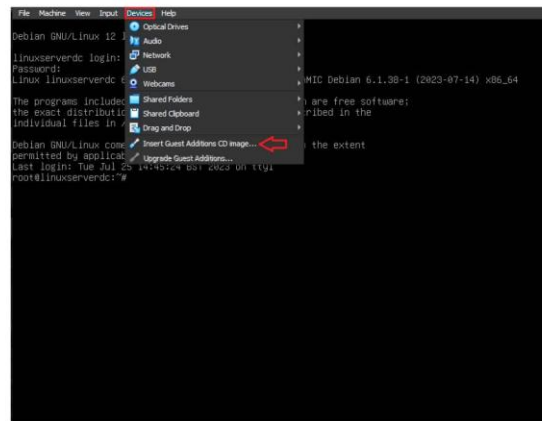
`usermod -aG sudo linuxserverdcadmin`

`getent group sudo`

Maradjunk a root felhasználónál a telepítés további folytatásához!

2.2.6 A „Guest Additions” kiegészítő telepítése

`apt install build-essential dkms linux-headers-$(uname -r) -y`



helyezzük be a virtuális gépbe a „Guest Additions” iso állományát

`mkdir /mnt/cdrom`

`mount /dev/cdrom /mnt/cdrom`

`cd /mnt/cdrom`

`sh ./VBoxLinuxAdditions.run --nox11`

`systemctl reboot`

Lépünk vissza a **linuxserverdcadmin** felhasználóval.

(a Putty címsorára jobb klikk, "Restart session")

Váltsunk a **root** felhasználóra!

2.3 Fájlrendszer paraméterek beállítása

Ha azt szeretnénk, hogy a fájlrendszer automatikusan rendelkezésre álljon a rendszer újraindulása után is, akkor fel kell venni az adatait a `/etc/fstab` nevű fájlban. A fájl 6 db, szöközőkkel, tabulátorokkal határolt mezőből álló sorokat tartalmaz, egy sor egyetlen fájlrendszer leírására szolgál.

Megadhatunk egyéb paramétereket is, pl.:

- Kiterjesztett felhasználói attribútumok (user_xattr)
- Hozzáférési lista (acl)
- Ha a bármilyen hiba fordul elő, és újramountolásra kerül a lemez, az read only (csak olvasható) lesz (errors=remount-ro)

`nano /etc/fstab`

Az alábbi paramétereket kell megadnunk (vigyázzunk a szöközőkre, felesleges vesszőkre stb.):

UUID=xyzxyzxy-xyzx-xyzx-xyzx-xyzxyzxyzxyzxy / ext4 user_xattr,acl,errors=remount-ro 0 1

```
# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# systemd generates mount units based on this file, see systemd.mount(5).
# Please run 'systemctl daemon-reload' after making changes here.
#
# <file system> <mount point> <type> <options> <dump> <pass>
# / was on /dev/sda1 during installation
UUID=1f70e47-74e5-44f5-8730-237c0ba6d57c / ext4 user_xattr,acl,errors=remount-ro 0 1
# /home was on /dev/sda5 during installation
UUID=f1a75dd8-95ed-4d61-96b1-03b29e4d0592 /home ext4 defaults 0 2
# swap was on /dev/sda6 during installation
UUID=4d205a1d-6ed2-4fd6-9b98-e637dc4ff70f none swap sw 0 0
/dev/sr0 /media/cdrom0 udf,iso9660 user,noauto 0 0
```

Mentsük a fájlt és lépünk ki!

`systemctl reboot`

Az újraindítás után jelentkezünk vissza Putty-n keresztül és **lépünk át a root felhasználóba!**

Ha jól konfiguráltuk az fstab fájlt, kihagyhatjuk ezt a lépést!

Ha elégtelened az fstab paramétereit és írásvédetté válik a fájlrendszer, a következő a teendő:

`lsblk` (megkeresni a partíció azonosítóját)

`mount -o remount,rw /dev/sda1 /` (az sda1 az azonosító)

Lépünk be újra az `fstab` fájlba, és javítsuk a hibát.

Mentsük a fájlt és lépünk ki!

`systemctl reboot`

2.4 Időzóna konfigurálása

```
timedatectl set-timezone Europe/Budapest  
date
```

2.5 Samba Active Directory telepítése és konfigurálása

```
apt install samba krb5-user krb5-config winbind libpam-winbind libnss-winbind -y
```

samba: Lehetővé teszi az olyan alapvető Windows hálózati protokollok használatát a Linux rendszerben, mint például az SMB/CIFS (Server Message Block/Common Internet File System), mellyel létrehozhatunk Samba-fiókot, megoszthatjuk fájlokat és nyomtatókat a hálózaton.

krb5-user: Alapvető programok az MIT (Massachusetts Institute of Technology) Kerberos használatával történő hitelesítéshez.

krb5-config: Konfigurációs fájlokat és eszközöket tartalmaz a Kerberos rendszerhez.

winbind: A Windows hálózati bejelentkezési információk kezelését végzi.

libpam-winbind és a libnss-winbind: A Samba-val együttműködve teszik lehetővé a Linux rendszernek, hogy a Windows bejelentkezési rendszert használja a PAM (Pluggable Authentication Modules) és a NSS (Name Service Switch) keretrendszeren keresztül.

Default Kerberos version 5 realm:

```
XYCOMPANY.XY
```

Kerberos servers for your realm:

```
linuxserverdc
```

Administrative server for your kerberos realm:

```
linuxserverdc
```

A Samba konfigurálása előtt állítsuk/tiltsuk le a háttérben futó Samba szolgáltatásokat:

```
systemctl stop samba-ad-dc.service smb.service nmbd.service winbind.service  
systemctl disable samba-ad-dc.service smb.service nmbd.service winbind.service
```

Nevezzük át a Samba eredeti konfigurációs állományát:

```
mv /etc/samba/smb.conf /etc/samba/smb.conf.orig
```

Telepítsük a tartományi szolgáltatást interaktív módon:

```
samba-tool domain provision --use-rfc2307 --interactive
```

Enterekkel haladjunk, a **DNS forwarder**-t és a **jelszót** adjuk meg a megfelelő sorokban:

Realm [XYCOMPANY.XY]:

Domain [XYCOMPANY]:

Server Role (dc, member, standalone) [dc]:

DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE)
[SAMBA_INTERNAL]:

DNS forwarder IP address (write 'none' to disable forwarding) [8.8.8.8]: **8.8.8.8**

Administrator password: **#Aa123456789@**

Nevezzük át a Kerberos fő konfigurációs fájlját a /etc könyvtárban, majd linkeljük a helyére a /var/lib/samba/private mappában lévő Kerberos fájlt:

krb5.conf biztonsági mentése (átnevezése):

```
mv /etc/krb5.conf /etc/krb5.conf.orig
```

Linkeljük a Samba által használatos Kerberos konfigurációs fájlt az előző helyre:

```
ln -sf /var/lib/samba/private/krb5.conf /etc/krb5.conf
```

Nyissuk meg a /etc/resolv.conf fájlt, és a következőkre cseréljük a tartalmát:

```
nano /etc/resolv.conf
```

```
domain xycompany.xy  
search xycompany.xy  
nameserver 172.16.0.254  
nameserver 8.8.8.8
```

Mentsük a fájlt és lépünk ki!

Indítsuk el a Samba szolgáltatásokat:

```
systemctl unmask samba-ad-dc.service  
systemctl start samba-ad-dc.service  
systemctl enable samba-ad-dc.service
```

2.6 DHCP szolgáltatás telepítése, konfigurálása

```
apt install isc-dhcp-server -y  
systemctl stop isc-dhcp-server
```

```
mv /etc/dhcp/dhcpd.conf /etc/dhcp/dhcpd.conf.orig
```

```
nano /etc/dhcp/dhcpd.conf
```

Másoljuk a fájlba az alábbi konfigurációt:

```
default-lease-time 86400;  
max-lease-time 86400;  
option subnet-mask 255.255.0.0;  
option broadcast-address 172.16.255.255;  
option routers 172.16.0.1;  
option domain-name-servers 172.16.0.254;  
option domain-name "xycompany.xy";  
subnet 172.16.0.0 netmask 255.255.0.0 {  
    range 172.16.0.100 172.16.0.150;  
}
```

Mentsük a fájlt és lépünk ki!

Nyissuk meg a következő fájlt és egészítsük ki a következőképpen:

```
nano /etc/default/isc-dhcp-server
```

INTERFACESv4="enp0s3" (meg kell adnunk a hálózati kártya azonosítóját)

Mentsük a fájlt és lépünk ki!

Indítsuk újra a DHCP szolgáltatást:

```
systemctl restart isc-dhcp-server
```

Ellenőrizzük, hogy a DHCP szolgáltatás megfelelően fut-e:

```
systemctl status isc-dhcp-server
```

3. Windows kliens

Telepítsük és konfiguráljuk a Windows klienst a már tanult módon!

Telepítsük a „Guest Additions” kiegészítőt!

A virtuális gép újraindulása után lépünk vissza a **winadmin** felhasználóval!

3.1 A Windows kliens tartományba léptetése

Újraindítás után lépünk vissza a **winadmin** felhasználóval!

Adjunk leírást és nevet a kliens gépnek, és **léptessük tartományba**, a már tanult módon:

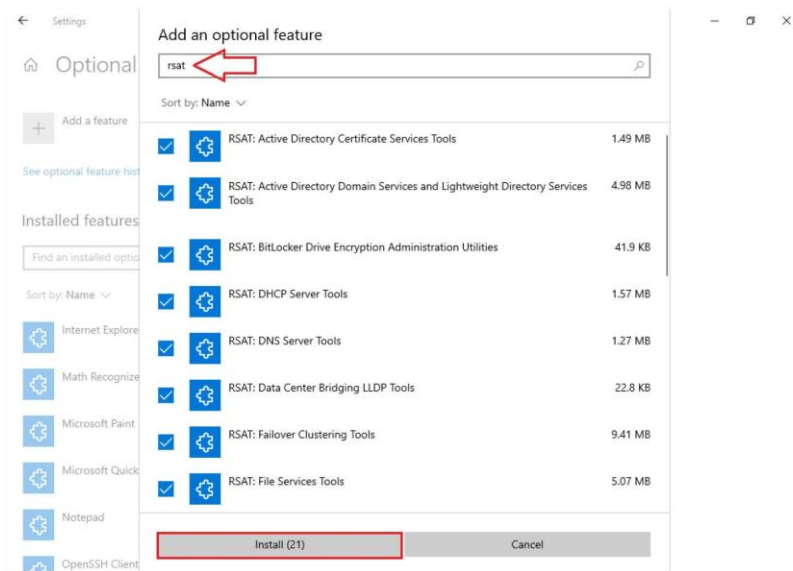
Computer description: **winclient**

Computer name: **winclient**

3.2 Remote Server Administration Tools (RSAT) telepítése és használata

A kliens gép tartományba léptetése után az újraindulást követően **tartományi adminisztrátorként** lépünk vissza:

Start menü → jobb klikk → Apps and Features → Optional features → Add a feature → a keresőbe: rsat → jelöljük ki az összes összetevőt → install



Telepítés után az alábbi helyen találjuk az egyes szolgáltatásokat/szerepköröket:

Control Panel → Administrative Tools → Active Directory - Users and Computers

Control Panel → Administrative Tools → DHCP

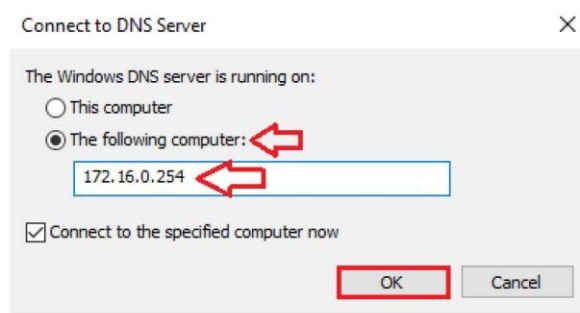
Control Panel → Administrative Tools → DNS

Control Panel → Administrative Tools → Group Policy Management

Control Panel → Administrative Tools → Computer Management

3.3 A DNS szolgáltatás konfigurálása

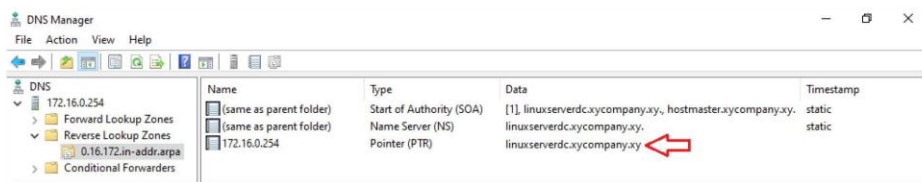
Control Panel → Administrative Tools → DNS



Hozzunk létre a „Reverse Lookup Zones” alatt egy zónát (Network ID: 172.16.0) és vegyük fel az alábbi pointer-t (PTR):

Host IP Address: 172.16.0.254

Host name: linuxserverdc.xycompany.xy



3.4 Active Directory | szervezeti egységek | felhasználók | csoportok felvétele

Control Panel → Administrative Tools → Active Directory - Users and Computers

Hozzuk létre az alábbi szervezeti felépítést a már tanult módon! Vegyük fel szervezeti egységeket, felhasználókat, csoportokat! A felhasználókat tegyük bele a megfelelő csoportba!

xycompany

managing_director (1 fő) → Michael Smith | michael_s → jelszó: #Cc123456789@

finance_department (1 fő)

personnel_department (2 fő)

marketing_department (2 fő)

secretariat (1 fő)

programmers (2 fő) 2/1 → William Johnson | william_j → jelszó: #Cc123456789@

4. A Samba Domain Controller működésének ellenőrzése

Indítsuk újra a Windows klienst, majd jelentkezünk be egy, az Active Directory-ban létrehozott felhasználóval.

Ellenőrizzük az IP címzést és az internet elérhetőségét:

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.19044.1288]
(c) Microsoft Corporation. All rights reserved.

C:\Users\michael>ipconfig /all
Windows IP Configuration

Host Name . . . . . : winclient
Primary Dns Suffix . . . . . : xycompany.xy
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : xycompany.xy

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . . : xycompany.xy
Description . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Physical Address. . . . . : 00-00-27-7B-F7-BC
Dhcp Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::8c75:e89e:a3:34f1%7 (Preferred)
IPv4 Address. . . . . : 172.16.0.100 (Preferred)
Subnet Mask . . . . . : 255.255.0.0
Lease Obtained. . . . . : Friday, July 22, 2022 4:44:12 PM
Lease Expires . . . . . : Saturday, July 23, 2022 4:04:35 AM
Default Gateway . . . . . : 172.16.0.1
Dhcp Server . . . . . : 172.16.0.254
Dhcpv6 IAID . . . . . : 101187623
Dhcpv6 Client DUID . . . . . : 00-01-00-01-2A-6C-62-E2-00-00-27-7B-F7-BC
DNS Servers . . . . . : 172.16.0.254
NetBIOS over Tcpip. . . . . : Enabled

C:\Users\michael>
```

```
C:\Windows\system32\cmd.exe

C:\Users\michael>ping 8.8.8.8
Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=11ms TTL=58
Reply from 8.8.8.8: bytes=32 time=10ms TTL=58
Reply from 8.8.8.8: bytes=32 time=10ms TTL=58
Reply from 8.8.8.8: bytes=32 time=9ms TTL=58

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 9ms, Maximum = 11ms, Average = 10ms

C:\Users\michael>ping cisco.com
Pinging cisco.com [72.163.4.185] with 32 bytes of data:
Reply from 72.163.4.185: bytes=32 time=169ms TTL=234
Reply from 72.163.4.185: bytes=32 time=169ms TTL=234
Reply from 72.163.4.185: bytes=32 time=169ms TTL=234
Reply from 72.163.4.185: bytes=32 time=164ms TTL=234

Ping statistics for 72.163.4.185:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 164ms, Maximum = 169ms, Average = 167ms

C:\Users\michael>
```