**Balmero Romero**

**Okos Iroda**

**Készítette**

**Felkészítő tanár: Jankó Krisztina**

Tartalom

[**Okos Iroda** 5](#_Toc194069849)

[Feladatfelosztás 7](#_Toc194069850)

[Topológia 8](#_Toc194069851)

[Tárgyaló 9](#_Toc194069852)

[VLSM 9](#_Toc194069853)

[Irodahelyiség 10](#_Toc194069854)

[VLSM 10](#_Toc194069855)

[Server Terem 11](#_Toc194069856)

[VLSM 11](#_Toc194069857)

[FTárgyaló 12](#_Toc194069858)

[VLSM 12](#_Toc194069859)

[Recepció 13](#_Toc194069860)

[VLSM 13](#_Toc194069861)

[Pihenő 14](#_Toc194069862)

[VLSM 14](#_Toc194069863)

[Parancsok 15](#_Toc194069864)

[R1 alapkonfigurációs parancsok: 15](#_Toc194069865)

[DHCP 15](#_Toc194069866)

[VPN 15](#_Toc194069867)

[Portok + IP címek 15](#_Toc194069868)

[OSPF 16](#_Toc194069869)

[NAT 16](#_Toc194069870)

[NTP 17](#_Toc194069871)

[R2 parancsok 17](#_Toc194069872)s

[DHCP 17](#_Toc194069873)

[VPN 17](#_Toc194069874)

[Portok + IP címek 18](#_Toc194069875)

[OSPF 19](#_Toc194069876)

[NAT 19](#_Toc194069877)

[IP Route 20](#_Toc194069878)

[NTP 21](#_Toc194069879)

[R3 parancsok 21](#_Toc194069880)

[Portok + IP címek 21](#_Toc194069881)

[IP Route 22](#_Toc194069882)

[R4 parancsok 22](#_Toc194069883)

[Portok + IP címek 22](#_Toc194069884)

[IP Route 23](#_Toc194069885)

[SW1 parancsok 24](#_Toc194069886)

[Spanning-tree 24](#_Toc194069887)

[IP címek 24](#_Toc194069888)

[NTP 25](#_Toc194069889)

[SW2 parancsok 25](#_Toc194069890)

[Feszitőfa protocoll 25](#_Toc194069891)

[TRUNK 25](#_Toc194069892)

[IP 26](#_Toc194069893)

[NTP 27](#_Toc194069894)

[SW3 parancsok 27](#_Toc194069895)

[SSH 27](#_Toc194069896)

[Feszitőfa protocoll 27](#_Toc194069897)

[TRUNK + 2. és 3. rétegbeli redundancia 27](#_Toc194069898)

[IP 28](#_Toc194069899)

[NTP 29](#_Toc194069900)

[SW4 parancsok 29](#_Toc194069901)

[SSH 29](#_Toc194069902)

[Feszítőfa protocoll 29](#_Toc194069903)

[TRUNK + 2. és 3. rétegbeli redundancia 29](#_Toc194069904)

[IP 30](#_Toc194069905)

[NTP 31](#_Toc194069906)

[SW5 parancsok 31](#_Toc194069907)

[SSH 31](#_Toc194069908)

[Feszítőfa protocoll 32](#_Toc194069909)

[TRUNK + 2. és 3. rétegbeli redundancia 32](#_Toc194069910)

[NTP 33](#_Toc194069911)

[SW6 parancsok 33](#_Toc194069912)

[Feszitőfa protocoll 33](#_Toc194069913)

[TRUNK 33](#_Toc194069914)

[NTP 34](#_Toc194069915)

[SW7 parancsok 34](#_Toc194069916)

[Feszítőfa protocoll 34](#_Toc194069917)

[IP 35](#_Toc194069918)

[MS parancsok 35](#_Toc194069919)

[Routing engedélyezés 35](#_Toc194069920)

[TRUNK 35](#_Toc194069921)

[IP 36](#_Toc194069922)

[NTP 36](#_Toc194069923)

[ASA tűzfal parancsok 37](#_Toc194069924)

[IP + NAT 37](#_Toc194069925)

[TELNET + SSH 38](#_Toc194069926)

[Vezeték nélküli Router 39](#_Toc194069927)

[IP+DHCP 39](#_Toc194069928)

[WIFI 40](#_Toc194069929)

[40](#_Toc194069930)

[40](#_Toc194069931)

[Windows Server 41](#_Toc194069932)

[51](#_Toc194069933)

[Linux Server 56](#_Toc194069934)

# **Okos Iroda**

Ha egy vállalat egy telephelyi hálózatot szeretne kiépíteni, számos szempontot figyelembe kell vennie. Természetesen a kivitelezés az egyik alapvető szempont, de nem elhanyagolható az sem, hogy a hálózat technológiai elvárásoknak eleget tevő, megfelelően skálázható, biztonságos és hatékony legyen. A telephelyi hálózatok tervezésénél csak olyan jövőbiztos megoldásokat érdemes használni, amelyek lehetővé teszik a zökkenőmentes fejlesztéseket és a folyamatos üzleti igények kielégítését.

A következő dokumentáció részletesen bemutatja egy háromszintes irodaépület hálózatának kialakítását, amely 20 alkalmazott számára biztosít munkakörnyezetet. Az irodaépület hálózata magába foglal két szervert, egy tűzfalat, telephelyenként egy-egy forgalomirányító eszközt (router), switcheket és hat munkaállomást. Az épület földszintjén recepció, pihenő és egy kisebb tárgyaló kapott helyet, az első emeleten egy irodahelyiség és egy szerverterem került kialakításra. A második emeleten egy tárgyalóterem került kialakításra.

A telephely hálózati topológiája csillag formában került kialakításra, amely az egyik legelterjedtebb megoldás az üzleti környezetekben. A csillag topológia egyik legnagyobb előnye, hogy az összes eszköz közvetlen kapcsolatban áll a központi switch-el, így egyetlen eszköz meghibásodása nem érinti a teljes hálózat működését. Ez biztosítja a hálózat stabilitását és megbízhatóságát, miközben az eszközök közvetlenül hozzáférnek a központi erőforrásokhoz, például a szerverekhez és más kritikus adatforrásokhoz. Csillag topológia különösen karbantartható és bővíthető magas fokú egyszerűsége miatt; emiatt dinamikusan fejlődő telephelyek, vagyis az olyan telephelyek, ahol időről-időre megnövekedhet a munkaállomások vagy egyéb hálózati eszközök száma, számára ez kiváló választás lehet.

Az irodai hálózatban alkalmazott IP-címzési séma az VLSM (Variable Length Subnet Mask) technológia segítségével történik. Ennek előnye, hogy az IP-címek hatékonyan kerülnek kiosztásra, miközben biztosítva van, hogy minden eszköz számára elegendő cím álljon rendelkezésre. Emellett a címzési rendszer rugalmas, így lehetővé teszi, hogy új eszközöket integráljunk a rendszerbe anélkül, hogy túl sok felesleges címet kellene kiosztani.

Ezek közül kiemelt helyet foglalnak el a nagy teljesítményű routerek az internetkapcsolat biztosítása és a helyi hálózatok közötti adatforgalom irányítása érdekében. A routerrel könnyen szegmentálható a hálózat, és a vállalati e-mailhez, fájlmegosztáshoz és a videókonferenciákhoz eltérő sávszélesség biztosítható. A switch-ek a helyi eszközök összekapcsolásáért felelnek, így biztosítva, hogy minden munkaállomás és eszköz a legnagyobb sebességgel kommunikálhasson a hálózaton belül. Access Point-ok biztosítják a megfelelő Wi-Fi lefedettséget az irodai területeken, lehetővé téve a mobil eszközök és laptopok számára is az internethez való hozzáférést.

A helyi szerverek biztosítják az adatok tárolását és megosztását az alkalmazottak számára, miközben a tűzfal feladata a külső fenyegetésektől való védelem. A tűzfal nemcsak a külső támadások, hanem a nem kívánt belső adatforgalom blokkolásában is kulcsszerepet játszik, így megakadályozza a hálózat összeomlását. A tűzfal szoros együttműködésben működik a VPN megoldással, amely titkosítja a hálózaton keresztül áramló adatokat, így biztosítva, hogy az adatkommunikáció ne legyen kiszolgáltatva a lehallgatásnak. A VPN segítségével a távmunka-végzés is biztonságosan valósítható meg, hiszen alkalmazottjaik titkosított csatornákon keresztül férhetnek hozzá a vállalati rendszerekhez, és eközben a hálózat védelme nem sérül.

A rendszeres adatmentés biztosítja, hogy minden fontos információ védve legyen az esetleges adatvesztéssel szemben. A napi mentések a helyi szerveren tárolódnak, hetente pedig automatikusan egy felhőalapú tárolóba is szinkronizálódnak. Ennek a lépcsőzetes mentési stratégiának az lesz a vége, hogy a vállalati adatok minden körülmények között visszaállíthatók lesznek, akkor is, ha a hardverhiba vagy a kiberbiztonsági támadás váratlanul következik be. A biztonsági mentések kezelését a hálózati adminisztrátorok látják el, akik folyamatosan figyelemmel kísérik a rendszer állapotát és szükség esetén módosítanak a mentési folyamatokon.

Nagy hangsúlyt fektettünk a skálázhatóságra a hálózati infrastruktúra tervezésénél, lehetővé téve ezáltal a jövőbeni bővítést akár további eszközök, akár nagyobb sávszélesség biztosítása révén. A tűzfal és a VPN technológiának köszönhetően a biztonság, az alkalmazottak által folyamatosan végzett karbantartás és monitorozás pedig a megbízhatóság garantált. A telephelyi hálózat válaszai tehát nemcsak a jelenlegi, hanem a jövőbeli kihívásokra is megfelelőek, amely biztosítja a cég hosszú távú sikeres működését.

# Feladatfelosztás

A feladatfelosztáshoz a projekt elkészítéséhez, megtervezéséhez és véghezviteléhez a Trello

alkalmazást használtuk. Egy közös megbeszélés után az alábbiak szerint alakultak a feladat felosztások:

Rolinak a feladatai a Linux server elkészítése, a fődokumentáció angol nyelvre fordítása és a Linux server dokumentációja volt. Továbbá a Packet Tracer-ben beállította és konfigurálta a Linux servert, az OSPF-t, és a Wi-Fi-t.

Bálintnak a feladatai a Windows server és a VLSM táblázat elkészítése, illetve a Windows server dokumentálása a fődokumentációban. Ezenfelül a Packet Tracer-ben beállította és konfigurálta a Windows servert, a NAT-ot, az ASA tűzfalat, a VPN-t és végezetül az ipv6-ot.

Mendelnek a feladatai közé tartozott a fődokumentációban a Packet Tracer dokumentálása és a tesztelési dokumentáció elkészítése. A Packet Tracerben pedig elkészítette az alapkonfigurációt, beállította az IP címeket, és DHCP segítségével további IP címeket osztott ki a megfelelő eszközöknek. Ezenkívül konfigurálta a 2. és 3. rétegbeli redundanciát, az NTP-t, a VLAN-okat, és a biztonsági beállításokat.

A képen szöveg, kerék, gumiabroncs, Szárazföldi jármű látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

# Topológia

Az okos irodánk 6 fő részből áll. A földszinten található a recepció, az Ftárgyaló és a Pihenő. A recepció egy nyomtatóból, két PC-ből, egy Switchből, és egy Routerből áll. Az Ftárgyaló egy Routerből, egy switchből és egy Multilayer Switchből, illetve 6 PC-ből áll,amiből 3 statikusan 3 pedig DHCP-vel kapott IP címet. A következő szinten található a Server terem, ahol 2 server (1 Windows és 1 Linux) található, illetve egy tűzfal és egy router. A fő telephely az irodahelység, itt található 6 PC, 3 Switch és egy Router. A legfelső szinten található egy Tárgyaló amiben 8 PC és 2db Switch található.

A képen képernyőkép, Színesség, művészet, tervezés látható

Automatikusan generált leírás

# Tárgyaló

A képen képernyőkép, sor, kék, Acélkék látható

Automatikusan generált leírásA tárgyalóban 10 darab eszköz kapott helyet, ezek közül 8db PC található amik DHCP-vel kaptak IP címet. A switchek között trunk vonalakat állítottunk be amin keresztül történik a kommunikáció. Ezekben a switchekben szintén állítottunk IP címeket. Portbiztonságot állítottunk a Router felé néző portra. Végezetül a switcheken biztonsági üzenetet állítottunk be jelszóval hogy az illetéktelenek ne tudjanak belépni.

## VLSM

A képen szöveg, képernyőkép, szám, Betűtípus látható

Automatikusan generált leírás

# Irodahelyiség

Az irodahelyiségben 6db PC található amelyeken statikusan állítottunk be IP címeket. A PC-k 3 db switch-hez kapcsolódnak, amelyeken 2. és 3. rétegbeli redundanciát valósítottunk meg. Ezek közül az egyik switch csatlakozik egy Routerhez. Ezen a routeren statikus útvonallal (IP Route) felvettük a többi hálózatok alhálózati címét és a következő ugrási címet(next hop). A switch-eken feszítőfa-protokollt alkalmaztunk. A router DHCP beállításainak köszönhetően kapnak az eszközök IP címeket. Továbbá VPN beállítások is megtalálhatóak ezen az eszközön.

A képen képernyőkép, diagram, sor, térkép látható

Automatikusan generált leírás

## VLSM

A képen szöveg, képernyőkép, szám látható

Automatikusan generált leírás

# Server Terem

A server teremben 2db szerver található (Linux és Windows). A Windows és Linux szerverben a következő szolgáltatásokat engedélyeztük:

* DHCP
* TFTP
* DNS szolgáltatások
* NTP
* FTP
* HTTP
* HTTPS

A képen lila, képernyőkép, Színesség, sor látható

Automatikusan generált leírásTovábbá a hálózatban található egy tűzfal és egy router is. A tűzfalban NAT-ot, VLAN-okat és TELNETET + SSH-t állítottunk be. A routeren statikus útvonallal felvettük a többi hálózatok alhálózati címét és a következő ugrási címet.

## VLSM

A képen szöveg, képernyőkép, Betűtípus, sor látható

Automatikusan generált leírás

# FTárgyaló

A képen képernyőkép, sor, diagram látható

Automatikusan generált leírásAZ Ftárgyalóban 6db PC található ebből 3db statikus IP címet kapott a másik 3db pedig DHCP-vel kapta a címet. A Multilayer Switchben NTP serverhez csatlakoztunk, majd SSH-t és trunköket állítottunk be. A másik Switchben szintén trunköt illetve feszítőfa protokollt alkalmaztunk. A router osztja ki a DHCP beállításainak köszönhetően IP címeket, illetve VPN-t állítottunk be.

## VLSM

A képen szöveg, képernyőkép, szám, Betűtípus látható

Automatikusan generált leírás

# Recepció

A képen képernyőkép, térkép, piros, diagram látható

Automatikusan generált leírásA recepcióban 2db PC található és 1 db nyomató, amelyeknek statikusan állítottunk IP címet. Található 1 switch és egy router is. A Routeren statikus útvonallal felvettük a többi hálózatok alhálózati címét és a következő ugrási címet.

## VLSM

A képen szöveg, képernyőkép, Betűtípus, sor látható

Automatikusan generált leírás

# Pihenő

A pihenőben 1 Wireless Router található, amely DHCP elérést biztosít a többi eszköz számára illetve a WIFI biztonságos csatlakoztathatóságáért is felel. A Laptop és 3db okostelefon ezeknek a beállításoknak köszönhetően kaptak IP címet és csatlakoznak WIFI-vel.

A képen szöveg, képernyőkép, diagram, Grafika látható

Automatikusan generált leírás

VLSM

A képen szöveg, képernyőkép, Betűtípus, szám látható

Automatikusan generált leírás

# Parancsok

## R1 parancsok

hostname R1

login on-failure log

login on-success log

enable secret class

enable password cisco

username admin privilege 15 secret cisco

banner motd ^CBelepes csak engedellyel!^C

### DHCP

ip dhcp pool targyalo

network 192.168.0.0 255.255.255.192

default-router 192.168.0.1

dns-server 8.8.8.8

### VPN

crypto isakmp policy 10

encr aes 256

authentication pre-share

group 5

crypto isakmp key cisco address 192.168.0.221

crypto ipsec transform-set TSET esp-aes 256 esp-sha-hmac

crypto map CMAP 10 ipsec-isakmp

set peer 192.168.0.221

set pfs group5

set security-association lifetime seconds 86400

set transform-set TSET

match address 100

ip domain-name okosiroda.hu

### Portok + IP címek

interface GigabitEthernet0/0

ip address 192.168.0.1 255.255.255.192

ip nat outside

duplex auto

speed auto

!

interface GigabitEthernet0/1

ip address 192.168.0.213 255.255.255.252

duplex auto

speed auto

crypto map CMAP

!

interface GigabitEthernet0/0/0

ip address 192.168.0.65 255.255.255.192

!

interface GigabitEthernet0/1/0.10

encapsulation dot1Q 10

no ip address

!

interface GigabitEthernet0/1/0.20

encapsulation dot1Q 20

no ip address

ip nat inside

### OSPF

router ospf 1

log-adjacency-changes

network 192.168.0.208 0.0.0.3 area 0

network 192.168.0.212 0.0.0.3 area 0

network 192.168.0.216 0.0.0.3 area 0

network 192.168.0.64 0.0.0.63 area 0

### NAT

ip nat inside source static 192.168.0.75 192.168.0.209

ip nat inside source static 192.168.0.75 192.168.0.217

ip nat inside source static 192.168.0.75 192.168.0.213

ip classless

ip route 192.168.0.160 255.255.255.240 192.168.0.214

ip route 192.168.0.128 255.255.255.224 192.168.0.214

ip route 192.168.0.176 255.255.255.240 192.168.0.214

!

line con 0

password 7 0822455D0A16

login

!

line vty 0 4

password cisco

login

privilege level 15

line vty 5 15

password cisco

login

privilege level 15

### NTP

ntp server 192.168.0.163

ntp update-calendar

!

## R2 parancsok

service password-encryption

!

hostname R2

!

login on-failure log

login on-success log

!

enable secret class

enable password cisco

### DHCP

ip dhcp pool ftargyalo

network 192.168.0.128 255.255.255.224

default-router 192.168.0.129

dns-server 8.8.8.8

username admin privilege 15 secret cisco

### VPN

crypto isakmp policy 10

encr aes 256

authentication pre-share

group 5

crypto isakmp key cisco address 192.168.0.213

crypto ipsec transform-set TSET esp-aes 256 esp-sha-hmac

crypto map CMAP 10 ipsec-isakmp

set peer 192.168.0.213

set pfs group5

set security-association lifetime seconds 86400

set transform-set TSET

match address 100

!

ip domain-name okosiroda.hu

!

### Portok + IP címek

interface FastEthernet0/0

ip address 192.168.0.129 255.255.255.224

duplex auto

speed auto

!

interface FastEthernet0/0.10

encapsulation dot1Q 10

no ip address

!

interface FastEthernet0/0.20

encapsulation dot1Q 20

ip address 192.168.0.249 255.255.255.252

ip nat inside

!

interface FastEthernet0/1

ip address 192.168.0.229 255.255.255.252

duplex auto

speed auto

!

interface Ethernet0/0/0

ip address 192.168.0.221 255.255.255.252

ip nat outside

duplex auto

speed auto

crypto map CMAP

!

interface Ethernet0/1/0

ip address 192.168.0.225 255.255.255.252

ipv6 traffic-filter incoming in

ipv6 traffic-filter outgoing out

ip nat outside

duplex auto

speed auto

ipv6 address 2001:4::2/64

!

interface Vlan1

no ip address

ipv6 address 2001:3::1/64

no shutdown

!

### OSPF

router ospf 1

log-adjacency-changes

network 192.168.0.220 0.0.0.3 area 0

network 192.168.0.224 0.0.0.3 area 0

network 192.168.0.228 0.0.0.3 area 0

network 192.168.0.128 0.0.0.31 area 0

### NAT

ip nat inside source static 192.168.0.138 192.168.0.221

ip nat inside source static 192.168.0.138 192.168.0.25

ip classless

### IP Route

ip route 192.168.0.176 255.255.255.240 192.168.0.222

ip route 192.168.0.160 255.255.255.240 192.168.0.222

ip route 192.168.0.64 255.255.255.192 192.168.0.222

ip route 192.168.0.0 255.255.255.192 192.168.0.222

ip route 0.0.0.0 0.0.0.0 192.168.0.193

!

ip flow-export version 9

!

ipv6 route ::/0 2001:4::1

!

banner motd ^CBelepes csak engedellyel!^C

!

line con 0

password cisco

login

!

line aux 0

!

line vty 0 4

password cisco

login

privilege level 15

line vty 5 15

password cisco

login

privilege level 15

!

### NTP

ntp server 192.168.0.163

ntp update-calendar

## R3 parancsok

hostname R3

!

login on-failure log

login on-success log

!

spanning-tree mode pvst

!

### Portok + IP címek

interface GigabitEthernet0/0

ip address 192.168.0.161 255.255.255.240

duplex auto

speed auto

!

interface GigabitEthernet0/1

ip address 192.168.0.214 255.255.255.252

duplex auto

speed auto

!

interface GigabitEthernet0/2/0

ip address 192.168.1.6 255.255.255.252

!

interface GigabitEthernet0/3/0

no ip address

shutdown

!

interface Vlan1

no ip address

shutdown

ip classless

### IP Route

ip route 192.168.0.176 255.255.255.240 192.168.1.5

ip route 192.168.0.128 255.255.255.224 192.168.1.5

ip route 192.168.0.64 255.255.255.192 192.168.0.213

ip route 192.168.0.0 255.255.255.192 192.168.0.213

!

ip flow-export version 9

!

banner motd ^C Idegeneknek belepni tilos! ^C

!

line con 0

!

line aux 0

!

line vty 0 4

login

line vty 5 15

login

## R4 parancsok

hostname R4

### Portok + IP címek

interface FastEthernet0/0

ip address 192.168.0.177 255.255.255.240

duplex auto

speed auto

!

interface FastEthernet0/1

no ip address

duplex auto

speed auto

!

interface Ethernet0/0/0

ip address 192.168.0.222 255.255.255.252

duplex auto

speed auto

!

interface GigabitEthernet0/1/0

ip address 192.168.1.5 255.255.255.252

!

interface Vlan1

no ip address

shutdown

!

router rip

!

### IP Route

ip classless

ip route 192.168.0.160 255.255.255.240 192.168.1.6

ip route 192.168.0.128 255.255.255.224 192.168.0.221

ip route 192.168.0.64 255.255.255.192 192.168.1.6

ip route 192.168.0.0 255.255.255.192 192.168.1.6

!

ip flow-export version 9

## SW1 parancsok

hostname SW1

!

enable secret cisco

enable password class

!

ip domain-name okosiroda.hu

!

username admin secret cisco

### Spanning-tree

spanning-tree mode pvst

spanning-tree extend system-id

**TRUNK**

interface FastEthernet0/1

switchport mode access

switchport port-security mac-address sticky

interface GigabitEthernet0/1

switchport mode trunk

### IP címek

interface Vlan1

ip address 192.168.0.2 255.255.255.192

!

interface Vlan10

no ip address

!

ip default-gateway 192.168.1.9

!

banner motd ^CBelepes csak engedellyel!^C

!

!

!

line con 0

password cisco

login

!

line vty 0 4

password cisco

login

privilege level 15

line vty 5 15

password cisco

login

privilege level 15

### NTP

ntp server 192.168.0.163

## SW2 parancsok

hostname SW2

!

enable secret cisco

enable password class

!

ip domain-name okosiroda.hu

!

username admin secret cisco

### Feszitőfa protocoll

spanning-tree mode pvst

spanning-tree extend system-id

### TRUNK

interface FastEthernet0/1

switchport mode access

switchport port-security mac-address sticky

!

interface GigabitEthernet0/1

switchport mode trunk

### IP

interface Vlan1

ip address 192.168.0.2 255.255.255.192

!

interface Vlan10

no ip address

!

ip default-gateway 192.168.1.9

!

banner motd ^CBelepes csak engedellyel!^C

!

line con 0

password cisco

login

!

line vty 0 4

password cisco

login

privilege level 15

line vty 5 15

password cisco

login

privilege level 15

### NTP

ntp server 192.168.0.163

## SW3 parancsok

hostname SW3

enable secret class

enable password cisco

### SSH

ip ssh authentication-retries 2

ip ssh time-out 90

ip domain-name okosiroda.hu

!

username admin secret cisco

### Feszitőfa protocoll

spanning-tree mode pvst

spanning-tree extend system-id

spanning-tree vlan 1 priority 0

### TRUNK + 2. és 3. rétegbeli redundancia

interface GigabitEthernet2/1

switchport mode access

switchport port-security mac-address sticky

!

interface GigabitEthernet3/1

switchport trunk native vlan 99

switchport mode trunk

switchport nonegotiate

storm-control broadcast level 50

!

interface GigabitEthernet4/1

switchport trunk native vlan 99

switchport mode trunk

switchport nonegotiate

storm-control broadcast level 50

!

interface GigabitEthernet5/1

switchport trunk native vlan 99

switchport mode trunk

switchport nonegotiate

storm-control broadcast level 50

!

interface GigabitEthernet6/1

switchport trunk native vlan 99

switchport mode trunk

switchport nonegotiate

storm-control broadcast level 50

### IP

interface Vlan1

ip address 192.168.0.66 255.255.255.192

!

banner motd ^CBelepes csak engedellyel!^C

!

line con 0

password cisco

login

!

line vty 0 4

exec-timeout 5 0

password cisco

login local

transport input ssh

privilege level 15

line vty 5 15

password cisco

no login

privilege level 15

!

### NTP

ntp server 192.168.0.163

## SW4 parancsok

service password-encryption

hostname SW4

!

enable secret cisco

enable password class

### SSH

ip ssh authentication-retries 2

ip ssh time-out 90

ip domain-name okosiroda.hu

!

username admin secret cisco

### Feszítőfa protocoll

spanning-tree mode pvst

spanning-tree extend system-id

spanning-tree vlan 1 priority 0

### TRUNK + 2. és 3. rétegbeli redundancia

interface GigabitEthernet2/1

switchport mode trunk

switchport port-security mac-address sticky

!

interface GigabitEthernet3/1

switchport trunk native vlan 99

switchport mode trunk

switchport nonegotiate

storm-control broadcast level 50

!

interface GigabitEthernet4/1

switchport trunk native vlan 99

switchport mode trunk

switchport nonegotiate

storm-control broadcast level 50

!

interface GigabitEthernet5/1

switchport trunk native vlan 99

switchport mode trunk

switchport nonegotiate

storm-control broadcast level 50

!

interface GigabitEthernet6/1

switchport trunk native vlan 99

switchport mode trunk

switchport nonegotiate

storm-control broadcast level 50

### IP

interface Vlan1

ip address 192.168.0.67 255.255.255.192

!

banner motd ^CBelepes csak engedellyel!^C

!

line con 0

password cisco

login

!

line vty 0 4

password cisco

login

privilege level 15

line vty 5 15

password cisco

no login

privilege level 15

### NTP

ntp server 192.168.0.163

## SW5 parancsok

service password-encryption

!

hostname SW5

!

enable secret cisco

enable password class

### SSH

ip ssh authentication-retries 2

ip ssh time-out 90

ip domain-name okosiroda.hu

!

username admin secret cisco

### Feszítőfa protocoll

spanning-tree mode pvst

spanning-tree extend system-id

spanning-tree vlan 1 priority 0

### TRUNK + 2. és 3. rétegbeli redundancia

interface GigabitEthernet3/1

switchport trunk native vlan 99

switchport mode trunk

switchport nonegotiate

storm-control broadcast level 50

!

interface GigabitEthernet4/1

switchport trunk native vlan 99

switchport mode trunk

switchport nonegotiate

storm-control broadcast level 50

!

interface GigabitEthernet6/1

switchport trunk native vlan 99

switchport mode trunk

switchport nonegotiate

storm-control broadcast level 50

!

interface Vlan1

ip address 192.168.0.68 255.255.255.192

!

banner motd ^CBelepes csak engedellyel!^C

!

line con 0

password cisco

login

!

line vty 0 4

password cisco

login

privilege level 15

line vty 5 15

password cisco

no login

privilege level 15

### NTP

ntp server 192.168.0.163

## SW6 parancsok

hostname SW6

!

enable secret class

enable password cisco

!

ip domain-name okosiroda.hu

!

username admin secret cisco

### Feszitőfa protocoll

spanning-tree mode pvst

spanning-tree extend system-id

### TRUNK

interface FastEthernet0/4

switchport trunk allowed vlan 1

switchport mode access

switchport port-security mac-address sticky

!

interface Vlan1

ip address 192.168.0.131 255.255.255.224

!

ip default-gateway 192.168.2.42

!

banner motd ^CBelepes csak engedellyel!^C

!

line con 0

password cisco

login

!

line vty 0 4

password cisco

login

privilege level 15

line vty 5 15

password cisco

login

privilege level 15

### NTP

ntp server 192.168.0.163

## SW7 parancsok

hostname SW7

### Feszítőfa protocoll

spanning-tree mode pvst

spanning-tree extend system-id

### IP

interface Vlan1

ip address 192.168.0.181 255.255.255.240

## MS parancsok

!

hostname MS

!

!

enable secret cisco

enable password class

### Routing engedélyezés

ip routing

!

no ipv6 cef

!

username admin privilege 15 secret cisco

!

ip domain-name okosiroda.hu

!

spanning-tree mode pvst

!

### TRUNK

interface GigabitEthernet1/0/5

switchport trunk allowed vlan 1

switchport mode access

### IP

interface Vlan1

ip address 192.168.0.130 255.255.255.224

!

interface Vlan10

mac-address 0060.70bb.ca01

no ip address

!

ip default-gateway 192.168.1.41

ip classless

!

ip flow-export version 9

!

banner motd ^CBelepes csak engedellyel!^C

!

line con 0

password 7 0822455D0A16

login

!

line aux 0

!

line vty 0 4

password 7 0822455D0A16

login

privilege level 15

line vty 5 15

password 7 0822455D0A16

login

privilege level 15

### NTP

ntp server 192.168.0.163

## ASA tűzfal parancsok

!

hostname ciscoasa

!

interface Ethernet0/0

switchport access vlan 2

### IP + NAT

interface Vlan1

nameif belso

security-level 100

ip address 192.168.0.162 255.255.255.240

!

interface Vlan2

nameif kulso

security-level 0

ip address 192.168.0.237 255.255.255.252

!

interface Vlan3

no nameif

security-level 50

ip address 192.168.0.241 255.255.255.252

!

object network DMZ-SERVER

host 192.168.2.1

object network INSIDE-NET

subnet 192.168.0.160 255.255.255.240

nat (belso,kulso) dynamic interface

!

route kulso 0.0.0.0 0.0.0.0 192.168.0.161 1

!

aaa authentication ssh console LOCAL

!

username admin password cisco

!

class-map INSPECTION-DEFAULT

match default-inspection-traffic

!

policy-map GLOBAL-POLICY

class INSPECTION-DEFAULT

inspect icmp

!

service-policy GLOBAL-POLICY global

### TELNET + SSH

telnet timeout 5

ssh 192.168.0.160 255.255.255.240 belso

ssh timeout 5

!

dhcpd auto\_config outside

!

dhcpd enable belso

!

## Vezeték nélküli Router

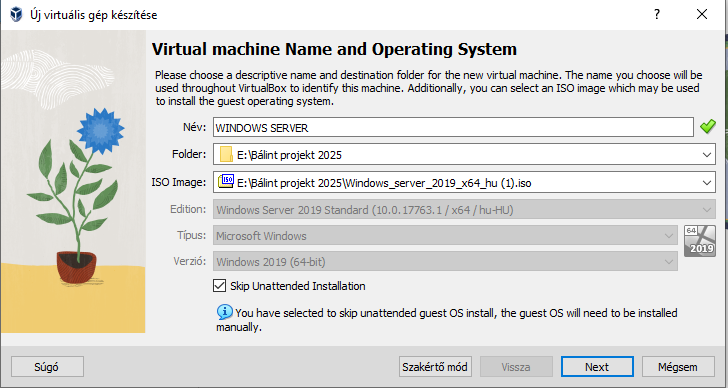
### IP+DHCP

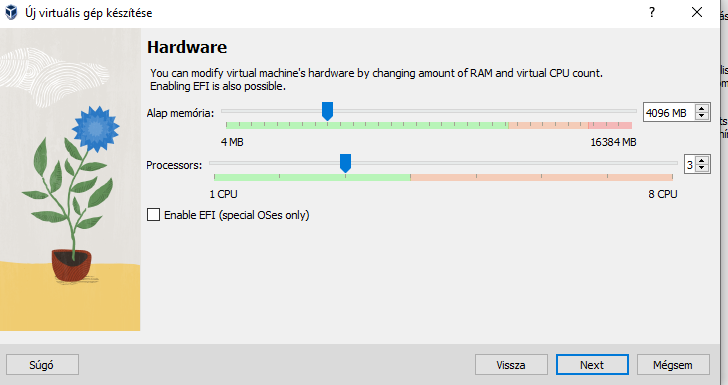
### WIFI

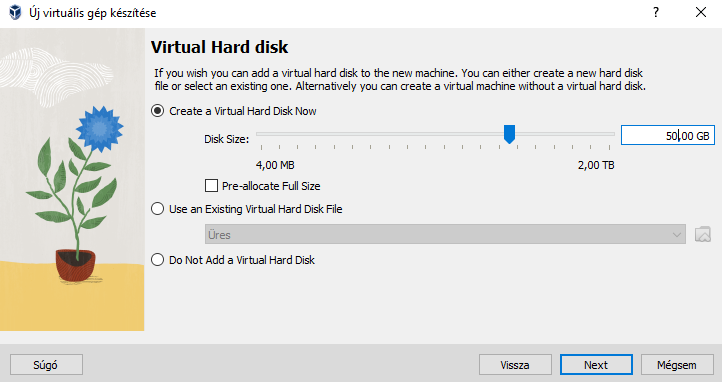
### 

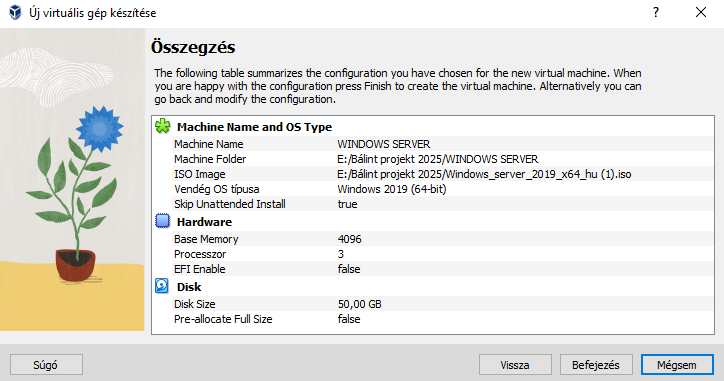
### 

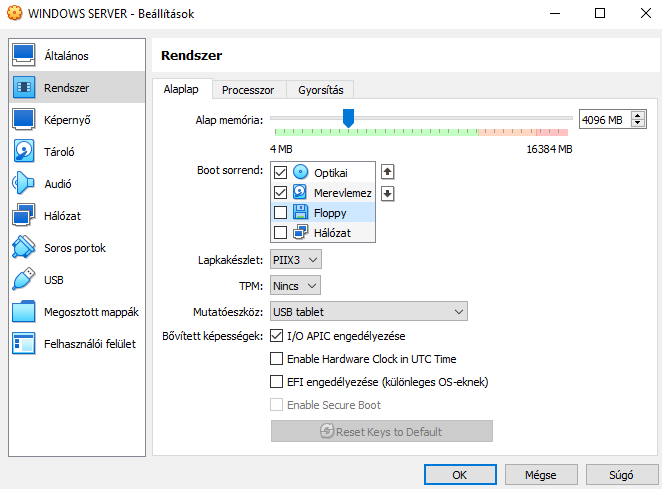
# Windows Server

Létrehoztunk egy virtuális gépet, megadtuk a gép nevét és a verzióját (Windows server 2019).

Ezt követően megadtuk a memória méretét (4096MB) és a processzorok számát: 3.

Megadtuk a virtuális merevlemez méretét: 50GB.

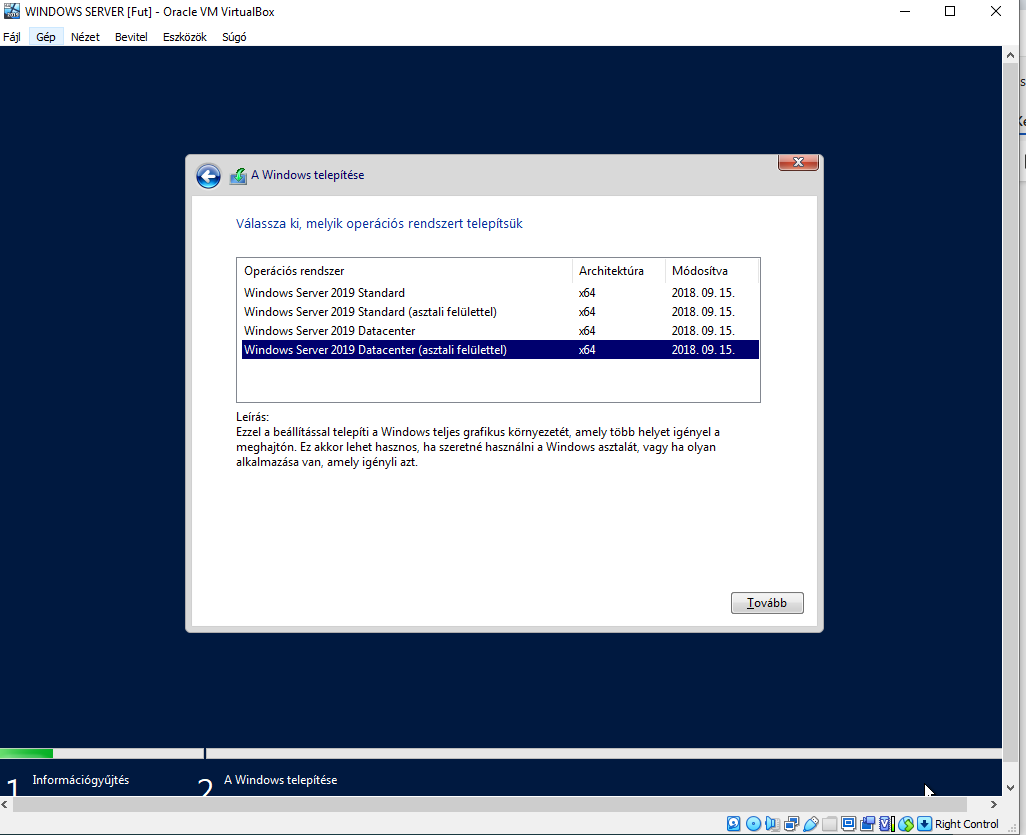
A létrehozás előtt leellenőriztük a virtuális gép alaptulajdonságait.

Ezután a beállításoknál kivettük a boot sorrendből a floppy-t.

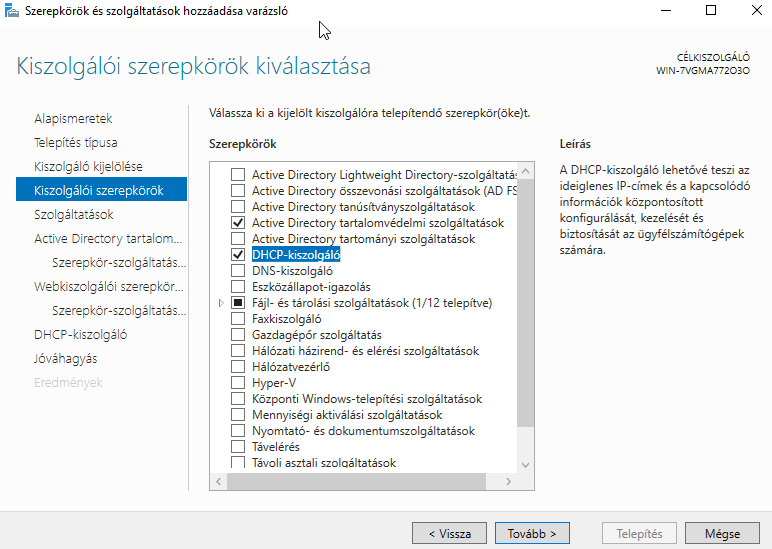
A beállítások után elindítottuk a virtuális gépet és elkezdtük a Windows telepítését.



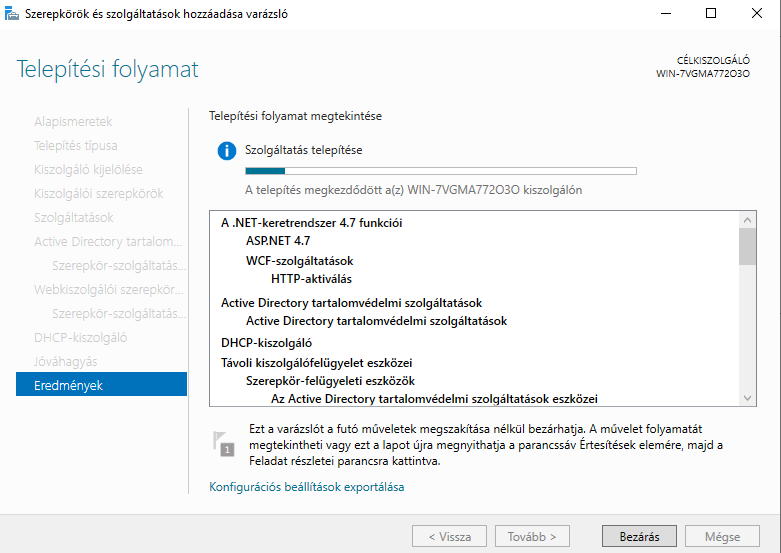
Kiválasztottuk az operációs rendszert Windows Server 2019 Datacentert asztali felülettel.

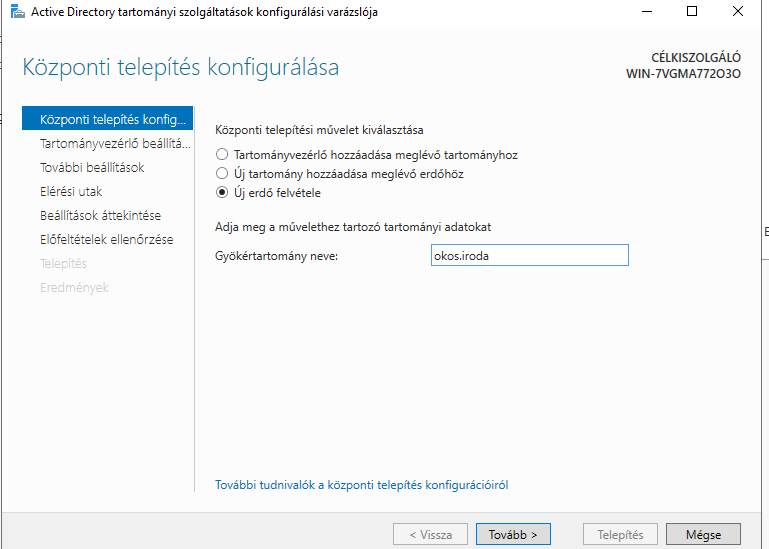


A sikeres telepítés után kiszolgálói szerepköröket adtunk hozzá a szerverünkhöz.

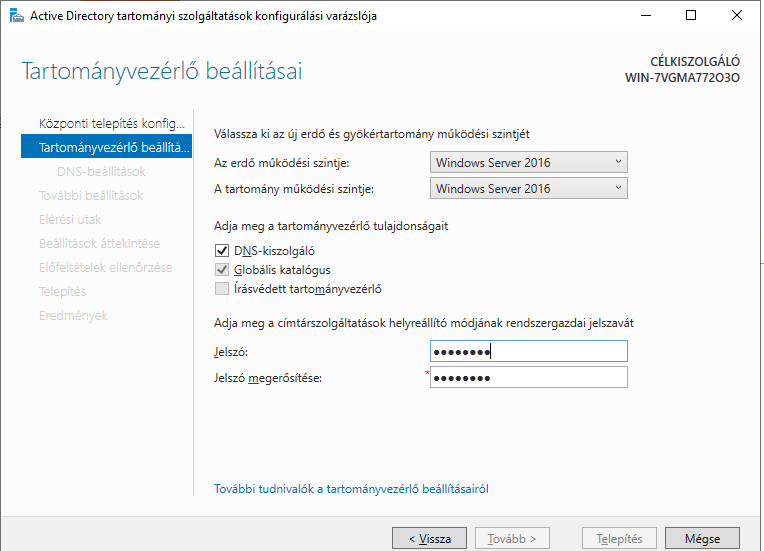


Először a DHCP kiszolgálót és a Active Directory tartalomvédelmi szolgáltatásait telepítettük le.



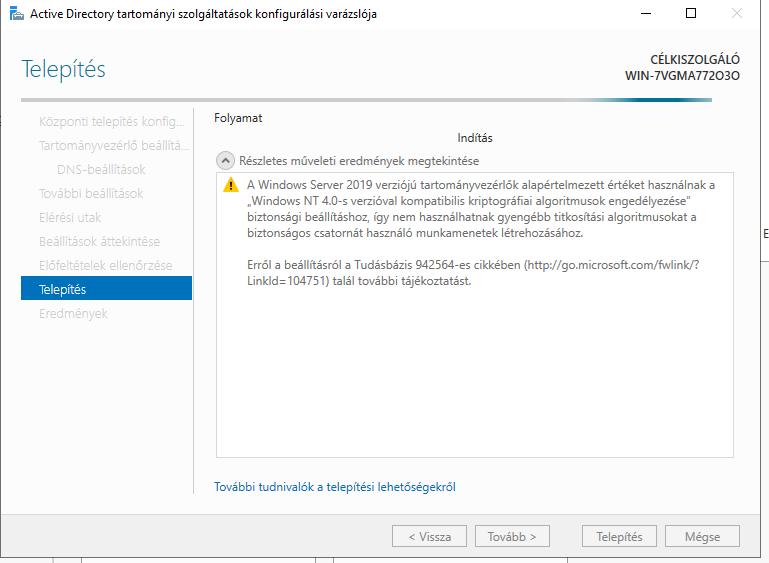
A sikeres telepítés után új erdőt vettünk fel.

Ezután tartományvezérlővé léptettük elő a szervert.

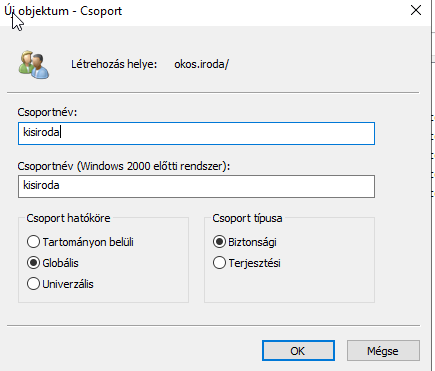


A további beállításoknál a NetBIOS-tartománynevet a szerver automatikusan kitöltötte.

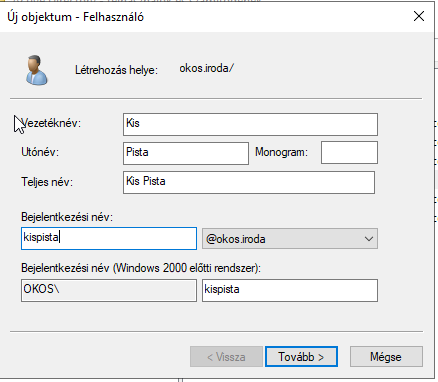
Itt a sikeres telepítése látható a tartományi szolgáltatások konfigurálása után.



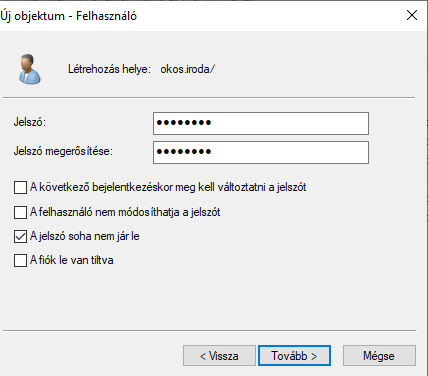
Új objektum csoportot hoztunk létre, ahol megadtuk a csoport nevét.

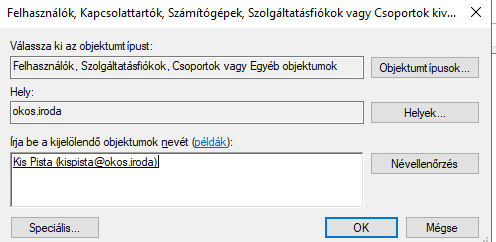


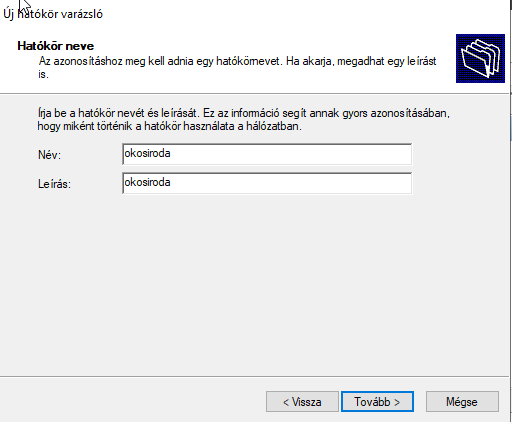
Ezután felvettünk egy új felhasználót.



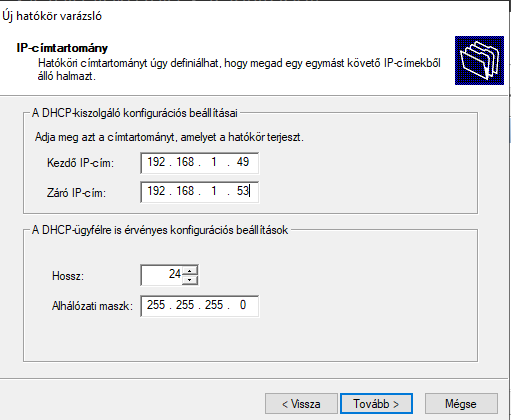
Jelszót adtunk neki és kijelöltük, hogy a jelszó soha ne járjon le.



Ezután az új felhasználót hozzáadtuk a csoporthoz.

Új hatókört hoztunk létre okosiroda néven.

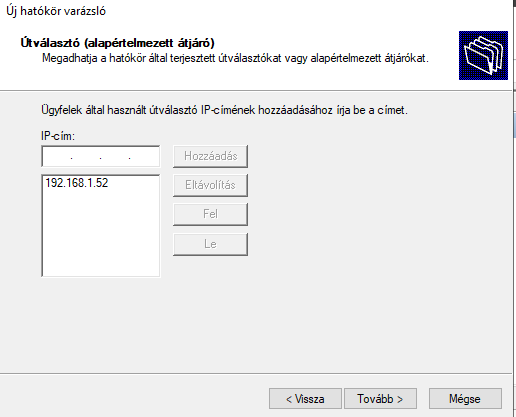
A dhcp kiszolgálónál megadtuk a kezdő és záró ip címet.



Ezután kizártuk a képen látható ip címeket. (Miért?)



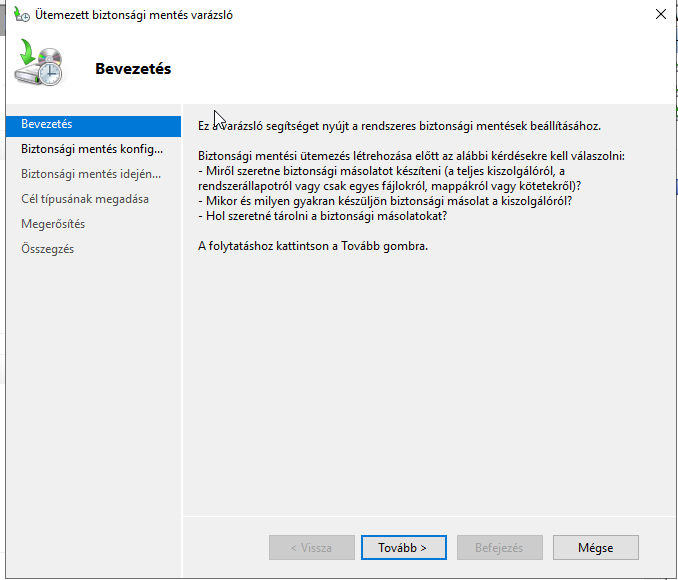
Alapértelmezett átjárót hoztunk létre.

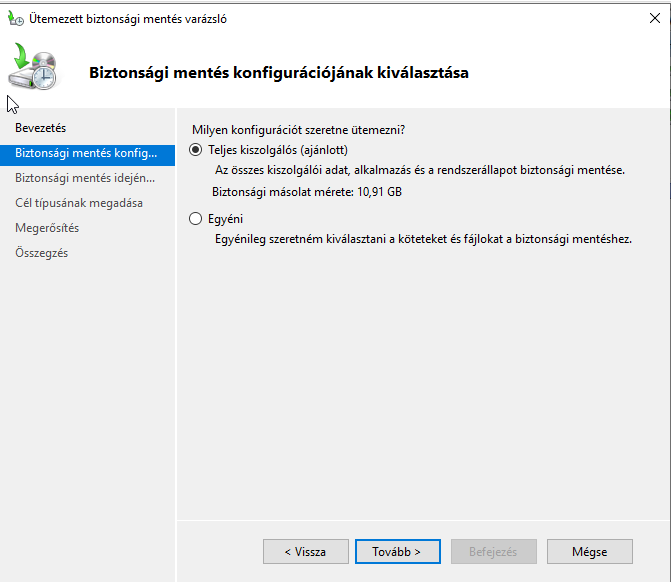


A szolgálatásoknál kiválasztottuk a biztonsági másolatot a szerveren.

# 

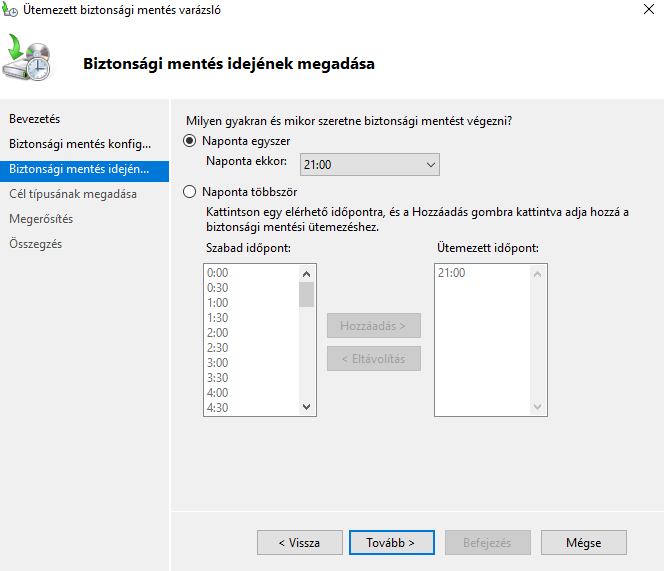
Miután letelepült elkezdtük a biztonsági mentés beállításait a szerveren.



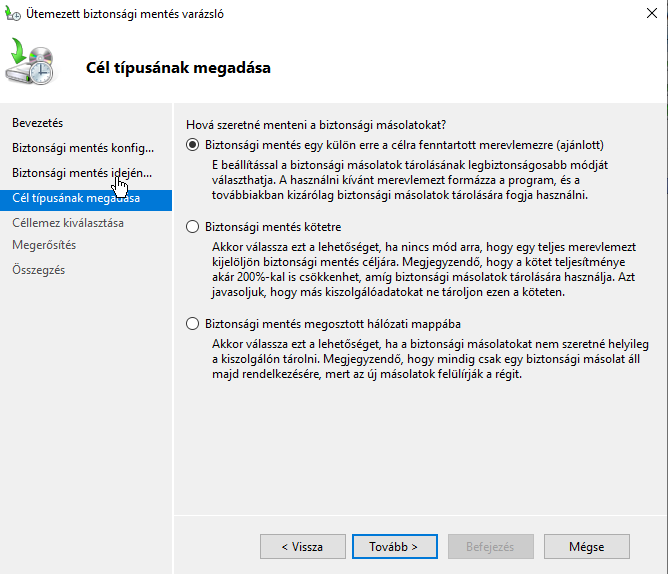


Beállítottuk a biztonsági mentés konfigurációját.

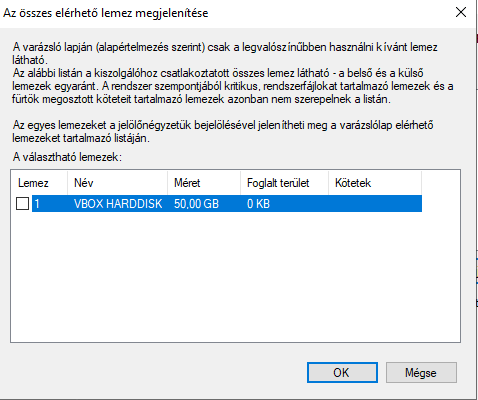
Ezután megadtuk a biztonsági mentés idejét.



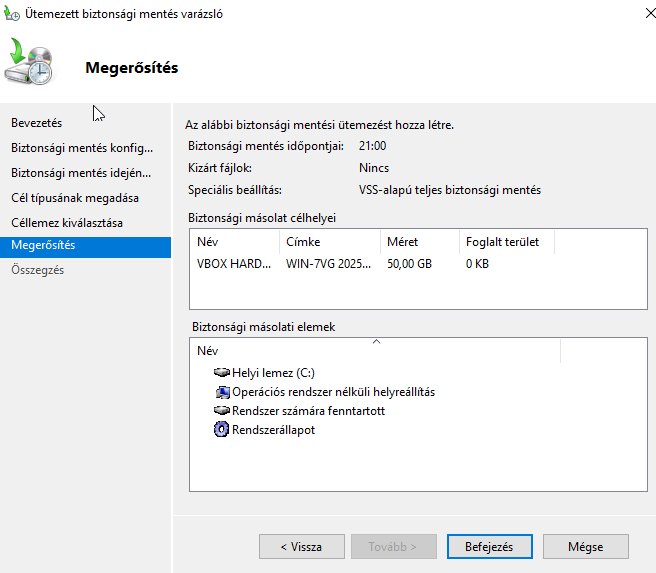
Kiválasztottuk hova szeretnénk menteni a biztonsági másolatot.



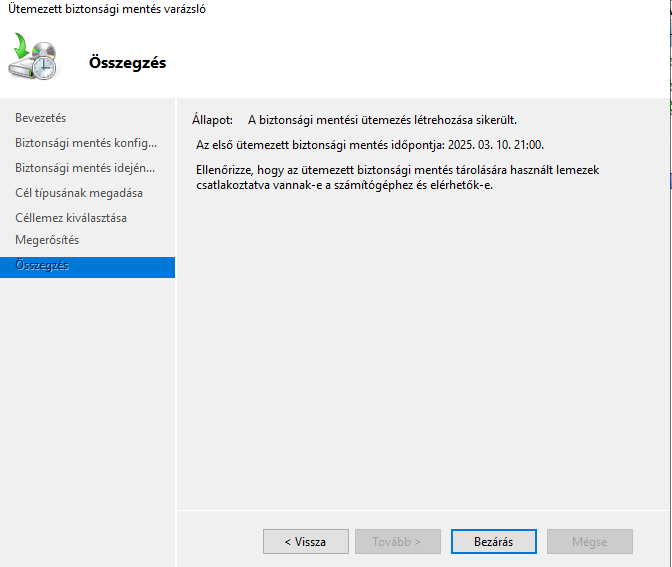
Kiválasztottuk melyik lemezre szeretnénk a biztonsági másolatot



Leellenőriztük az eddigi beállításokat a biztonsági mentés konfigurációja befejezése előtt.



A biztonsági mentés sikeresen megtörtént.

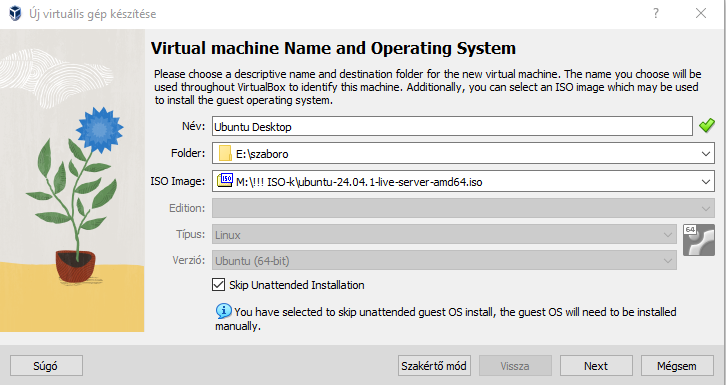


# Linux Server

Ubuntu Server telepítése

Megadtuk a virtuális gép nevét.

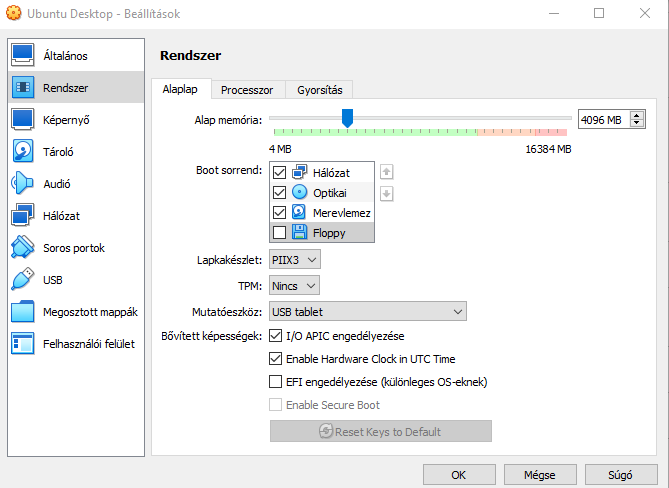
Megadtuk a virtuális gép tárolására szolgáló könyvtár nevét.



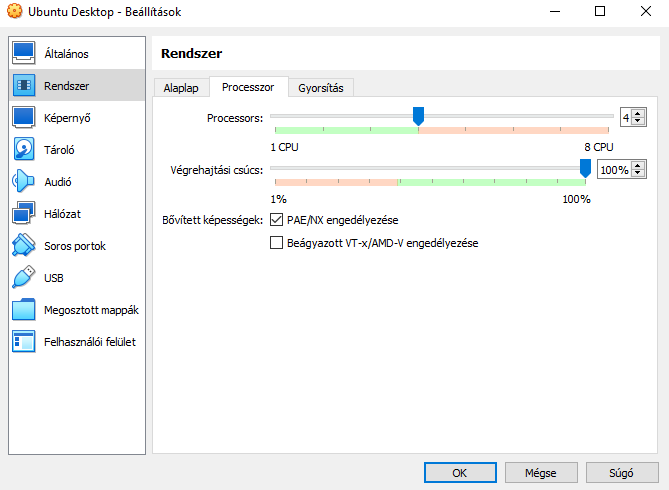
Megadtuk a Virtuális gép által felhasználható memória méretét.

A létrejött virtuális gép korábban megadott paraméterei is módosíthatók a beállításokban.

Megadtuk a bootolási források és sorrendeket.

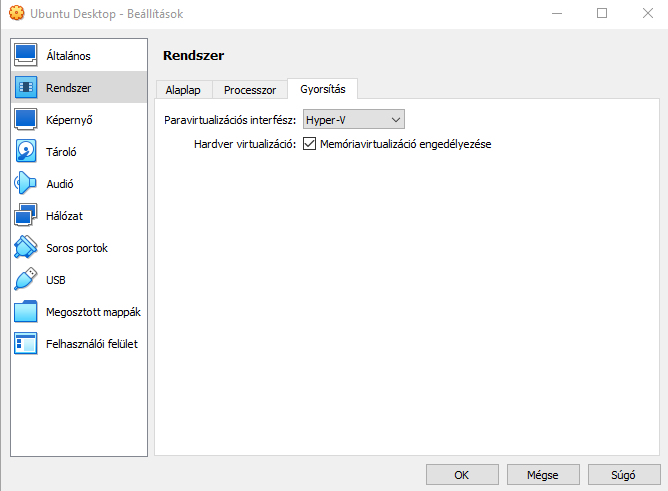


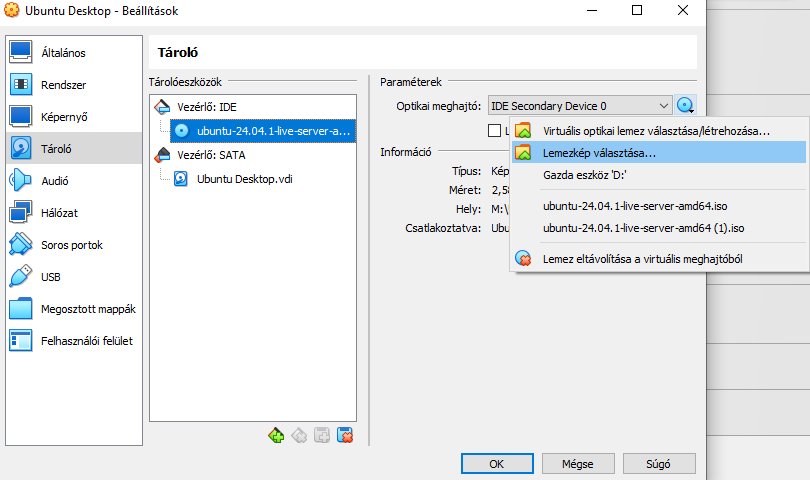
A bővített lehetőségek ha elérhetőek, gyorsítják a működést, ezért ezt bepipáltuk.

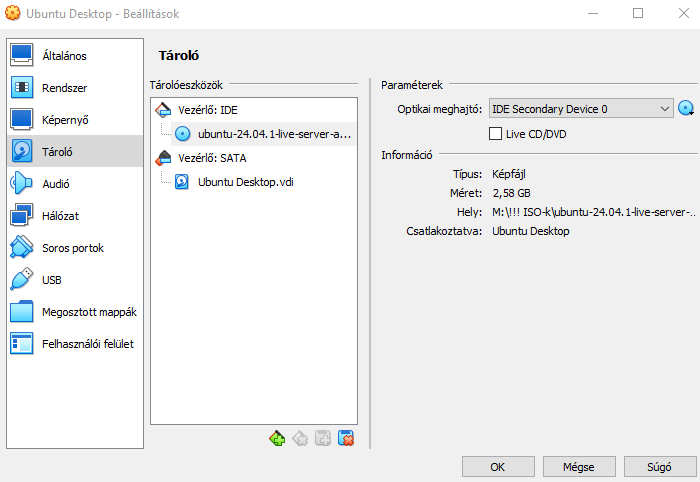


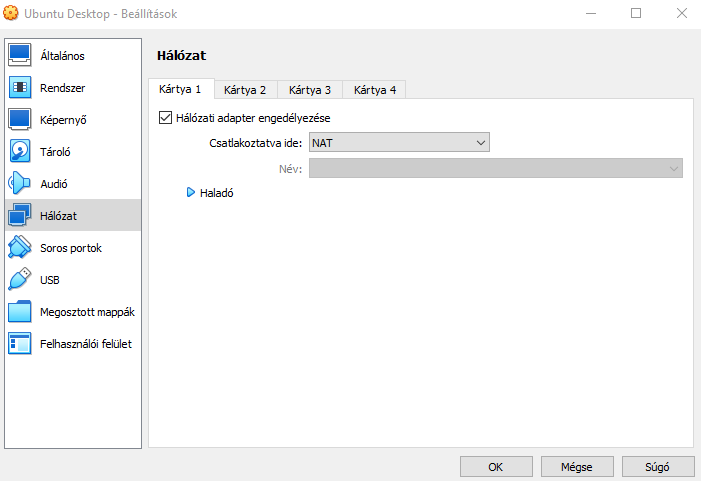
Mivel az Intel CPU-k Hyper-V technológiát használnak, ezért azt választottuk ki

A memória virtualizációnak a fizikai gépen elérhetőnek kell lenni, ezért azt ki pipáltuk.









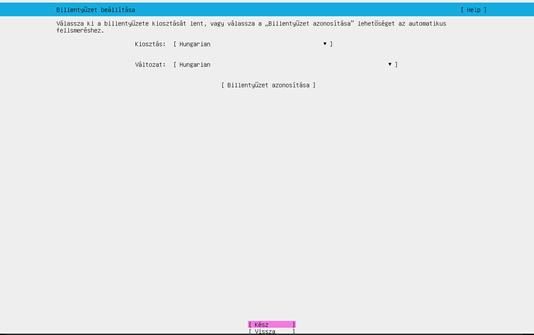
Operációs rendszer telepítése

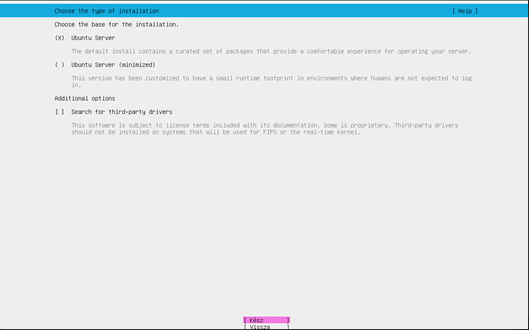
Kiválasztottuk a magyar nyelvet.

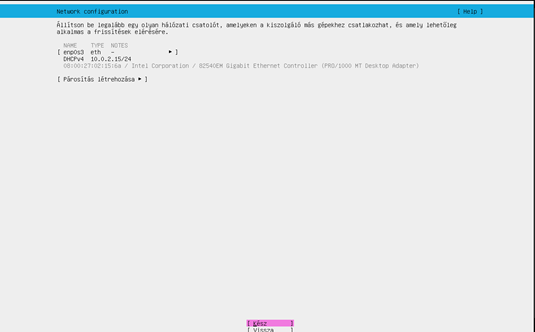


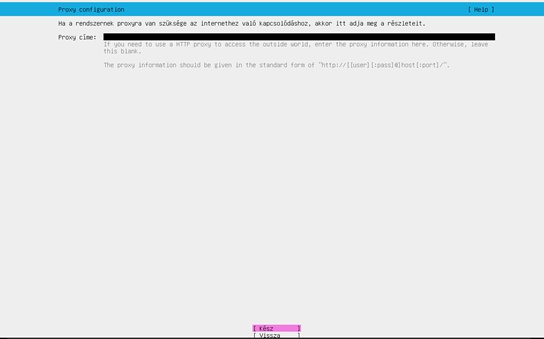


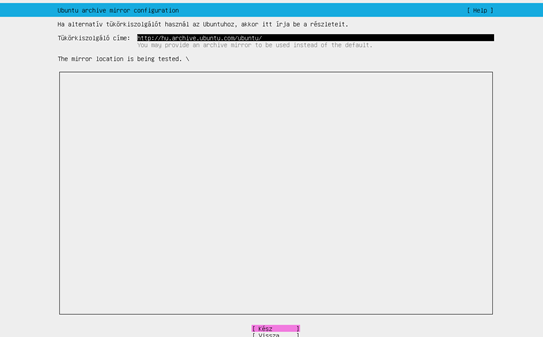
Billentyűzet beállításánál, kiválasztottuk a billentyűzet kiosztására a Magyar nyelvet.

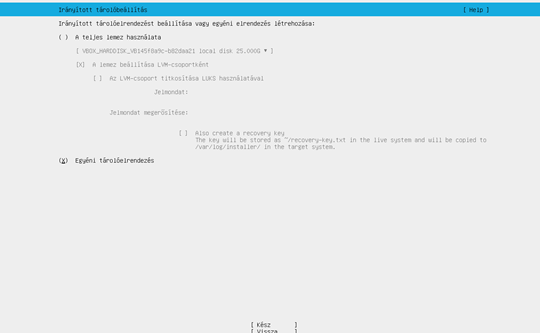








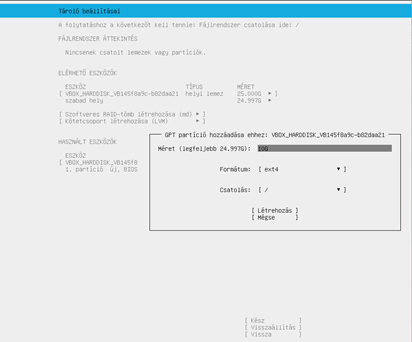
Az archívumtükör beállításánál beállítottunk egy alternatív archívum-tükörkiszolgálót, melyet az alapértelmezett helyett használhat.

Irányított tárolóbeállításnál egyéni tárolóberendezést választottunk.

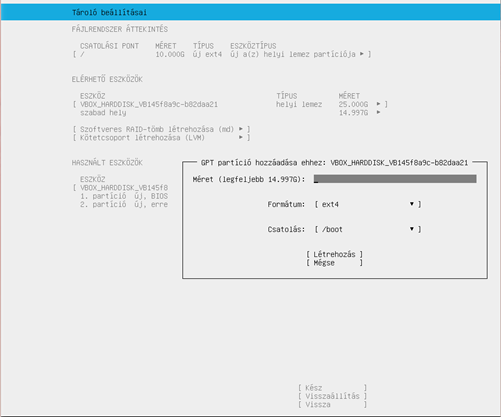
Tároló beállításánál hozzáadtunk egy GPT partíciót.



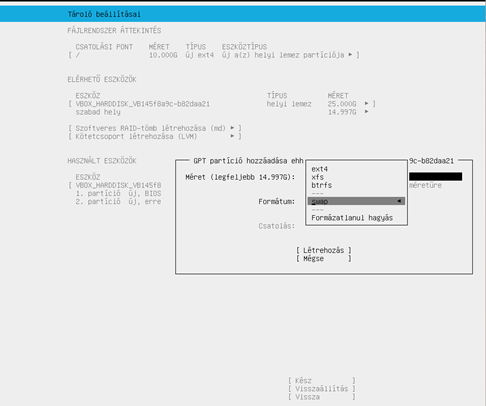
Amelynek 10G-ot adtunk meg.



Csatolásnak Boot-ot választottunk ki.



Formátumnál Swap-et választottunk ki.





Profilbeállításnál Az ön nevéhez Szabó Roland-ot adtunk meg.

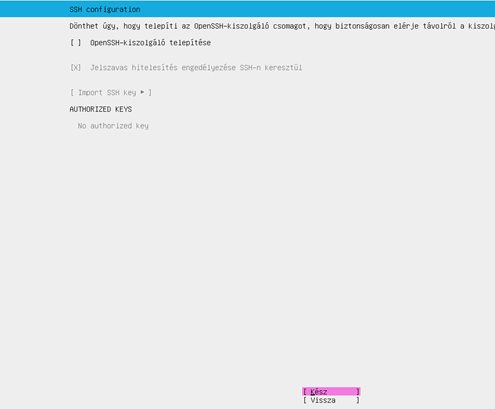
A kiszolgáló nevének server-t adtunk meg.

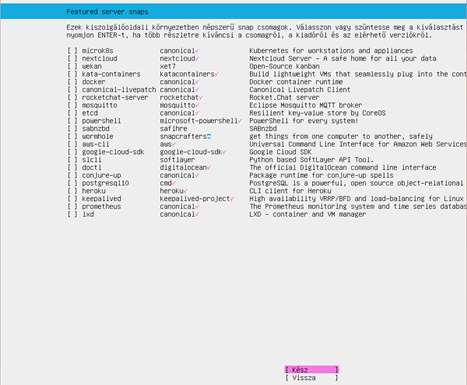
Felhasználónévnek roli-t adtunk meg.

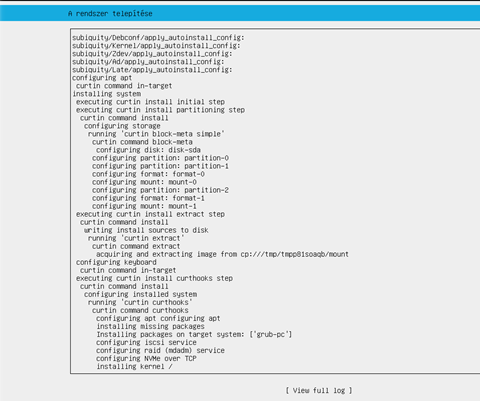
Majd jelszónak 12345-et adtunk meg.





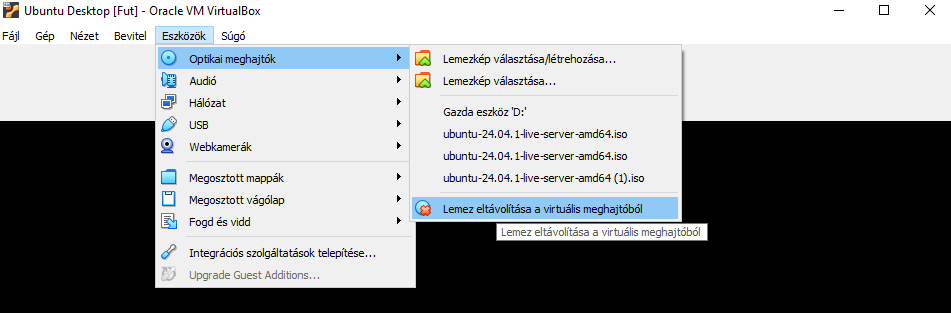




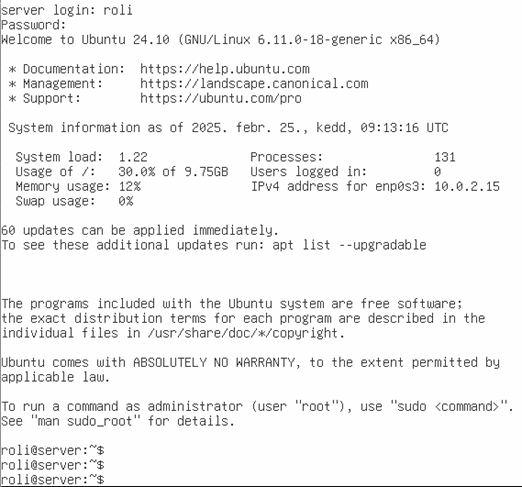


Az eszközöknél az Optikai meghajtókon belül a

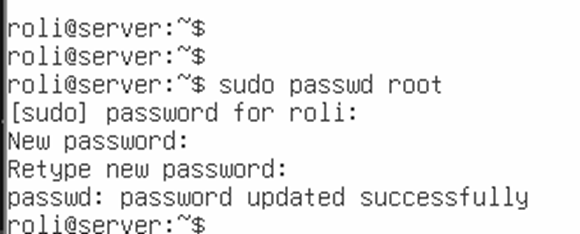
„Lemez eltávolítása a virtuális meghajtóból”-ra nyomtunk.



Bejelentkezés



Rendszergazdai fiókot aktiváltuk.

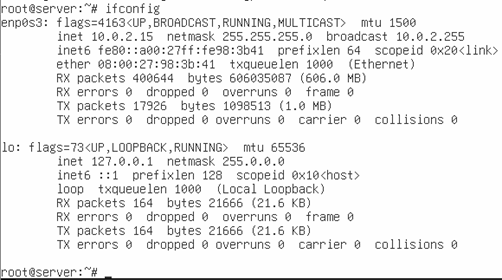


root password:12345

roli server:123456

TFTP kiszolgáló telepítése

Ellenőriztük, hogy van-e működő internet kapcsolata a gépnek.

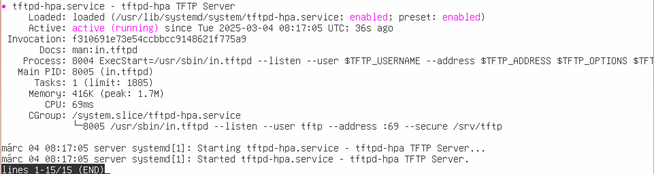


Telepítettük a tftp-hpa csomagot.





Meggyőződtünk, hogy sikeresen elindult a TFTP kiszolgáló



Beállítottuk, hogy a rendszer indulásakor a TFTP kiszolgáló induljon el.

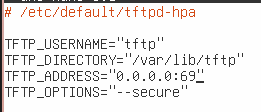


Megnyitottuk a nano szövegszerkesztővel a TFTP kiszolgáló konfigurációs állományát.



Módosítottuk a TFTP kiszolgáló könyvtárát, ahova a fájlok kerülnek.

Illetve módosítottuk, hogy milyen porton figyeljen a TFTP kiszolgáló.



Létrehoztuk a könyvtárat, amit a konfigurációs állományban beállítottunk.



Beállítottuk, hogy könyvtár ne legyen senki tulajdona.



Beállítottuk, hogy a könyvtár bárki számára írható, olvasható és tallózható legyen





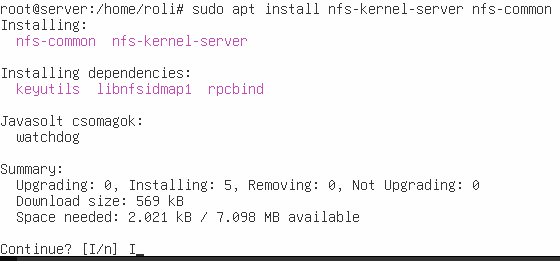




Megosztás Linux kliensek számára

Telepítettük a megosztáshoz szükséges szolgáltatásokat.





Létrehoztuk a megosztandó mappát.



Teljes jogosultságot adtunk.



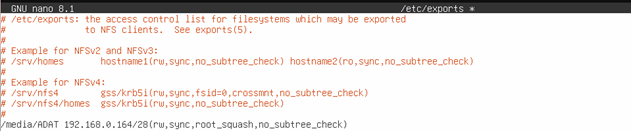
Létrehoztunk egy szöveges fájlt a teszt kedvéért.



Exports fájlt szerkesztettük.



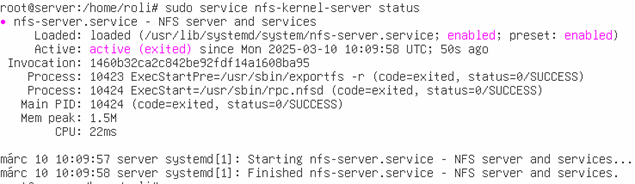
A képen látható módon szerkesztettük az exports fájlt.



Újraindítottuk az nfs-kernel szervert.



Ellenőriztük a szerver aktuális állapotát.

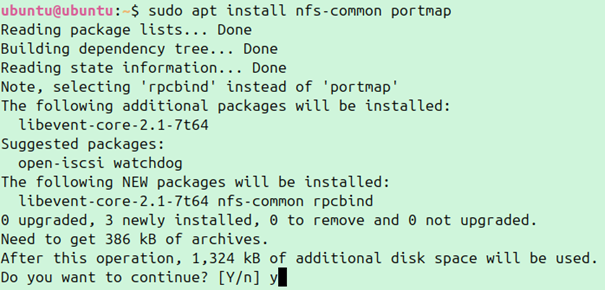


Hálózatot hírdettünk.



Folytatás Ubuntu kliensen.

A terminált használva letöltöttük az nfs-common portmap szolgáltatást.



Létrehoztuk a mappát



Felcsatoltuk a megosztást.

