Windows Server

Kiadások

1., **Standard** - Ideális KKV környezetekben, ahol kevésbé szükségesek a nagy teljesítményű és skálázható szolgáltatások – jelenleg 1176 $. 2 virtuális gépet lehet telepíteni

2., **DataCenter** - Támogatja a nagy teljesítményű és skálázható szolgáltatásokat, ideális nagyobb vállalatok és adatközpontok számára – jelenleg 6771 $. Tetszőleges számú virtuális gépet lehet telepíteni

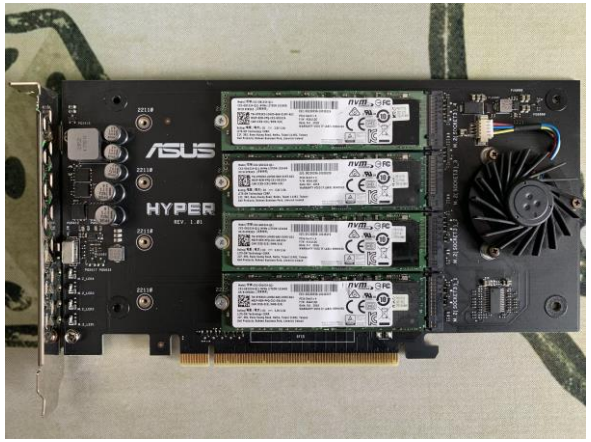
3., **DataCenter Azure** – 6771 $-tól felfelé de változó. A Microsoft ügyfélmenedzserének (account manager) a bevonásával történik többnyire

Hardverkövetelmények

- Processzor: 1.4 GHz x64, NX, DEP, CMPXCHG16b, LAHF/SAHF, PrefetchW, másodlagos címfordítás (EPT vagy NPT), SSE4.2, POPCNT instrukciók
- RAM: ajánlott 2GB
- Tárhely: 32 GB, PCI-E architektúra
- Hálózati adapter: 1 Gb/s

Speciális hardverek

4 processzoros alaplap



PCIe NVMe SSD adattároló

Fájlrendszerek

- **NTFS** (New Technology File System)

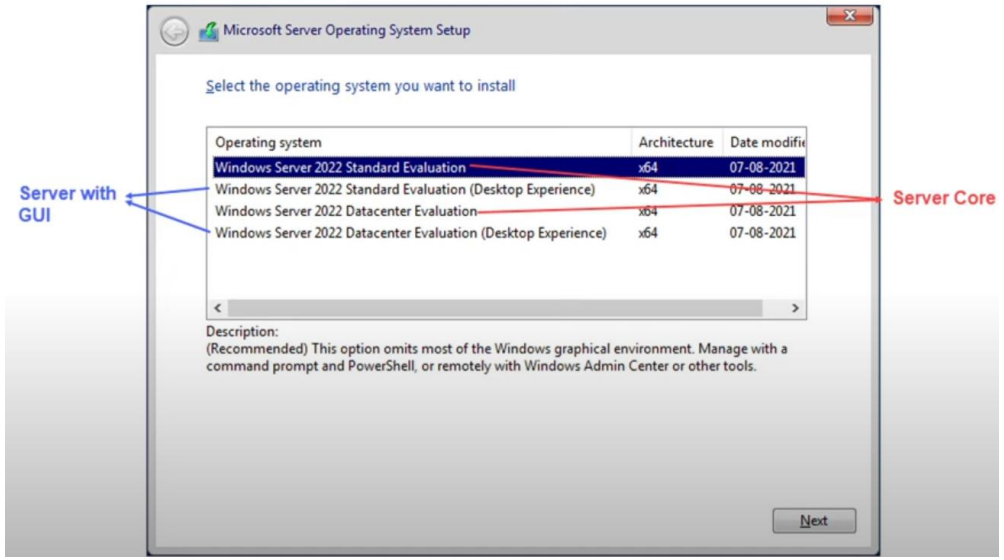
  Előnyei: Naplózás, biztonság (ACL – access control list), nagyméretű file, Bitlocker
  Hátrányai: Teljesítmény, komplexitás, nagy filerendszer nehéz kezelése

- **ReFS** (Resilient File System)

  Előnyei: Integritás, megbízhatóság, Storage Space (pool, hibáknál automatikus javítás), nagy teljesítmény, skálázhatóság
  Hátrányai: kompatibilitás, bonyolultabb hibaelhárítás

Telepítés

A Windows Server telepítője alapból 2 beállítást teszt lehetővé mint a Standard, mint pedig a DataCenter verzióra. Ha nem akarunk ablakkezelőt, és elég a sima parancssor, akkor válasszuk a “**sima**” telepítést (ún. “Server Core” 1., 3., eset) . Ha viszont ablakkezelővel szeretnénk, akkor válasszuk a “**Desktop Experience**” opciót (ún. “Server with GUI” - 2., 4., eset).



Magyar nyelv telepítése

Mivel alapból nem telepíti fel a Windows Server a magyar nyelvi csomagot, ezért nekünk kell ezt megtennünk a következő képp:

1., a beállításoknál keressük meg a **Language Settings**-et

2., a **Preferred Languages**-nél kiválasztjuk a **Hungarian** opciót (ami **Magyar**)

3., a magyar nyelv **beállításánál töltsük le az összes opciót**.

4., a **Prefferred Language**-t most már **átállíthatjuk magyarra**

5., **Újraindítás** után megjelenik a magyar kezelőfelület

Ha valami miatt azt írja ki, hogy nincs internet csatlakozás, közben meg mégis működik az Edge pl., akkor a Network Troubleshooterrel orvosolhatjuk, majd újraindítás után már működnie kell

Kiszolgálókezelő
(Server Manager)

A Kiszolgálókezelő a Windows Server egyik központi konzolja, amely lehetővé teszi a rendszergazdák számára, hogy különféle feladatokat végezzenek a szerveren.

A Kiszolgálókezelő funkciói:

1., Szerepkörök és szolgáltatások kezelése: (pl. DNS, DHCP, AD DS)

2., Szerverek állapotának ellenőrzése

3., Konfigurációs feladatok

4., Távoli kezelés lehetősége – megkönnyíti a rendszergazdák munkáját

5., Eseménynapló megtekintése

Active Directory (AD)

- A Windows Server központi adatbázisa, amely kezeli a hálózati erőforrásokat (felhasználók, számítógépek, nyomtatók, egyéb eszközök).

- Fő célja, hogy egyszerűsítse a hálózati erőforrások kezelését és biztonságossá tegye a hozzáférést.

A Címtárszolgáltató (AD DS) telepítése és előléptetése tartományvezérlővé

A Windows Server Címtárszolgáltató (AD DS - Active Directory Domain Services) egy olyan szolgáltatás, amely lehetővé teszi a felhasználói fiókok, számítógépek ill. egyéb elemek központi kezelését. Emellett a címtár hierarchikus struktúráját kezeli és biztosítja.

Az AD DS telepítése és előléptetése Tartományvezérlővé:

1., Az Active Directory Címtárszolgáltató telepítése (AD Domain Service, **AD DS**) a Szerepkörök és Szolgáltatásoknál.

2., Az Active Directory **tartományvezérlővé történő előléptetése** – kiválasztjuk az ide illő opciót: pl. **Erdő** felvétele (forest).

* A telepítés folyamán hagyjuk bekapcsolva a DNS opciót is, hogy ne kelljen külön telepíteni.

A Címtárszolgáltató (AD DS) felosztása

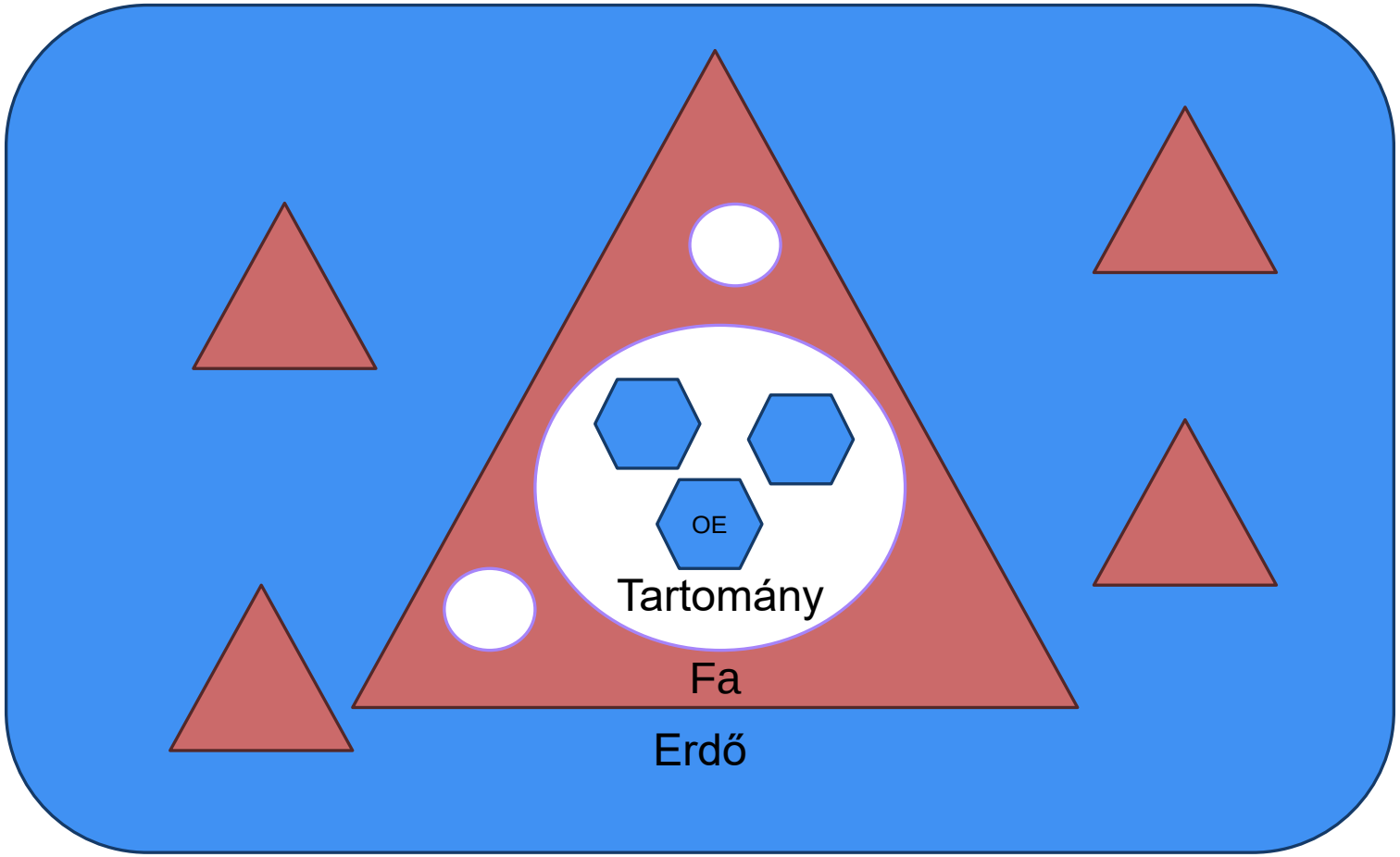
1. **Erdő** (Forest) - Az AD legmagasabb szintű tárolóegysége, amely tartalmazhat egy vagy több tartományt

2. **Fa** (Tree) - Az erdőn belül található, és egy közös DNS névtérrel rendelkező tartományok hierarchikus struktúrája. Több fa is lehet egy erdőn belül.

3. **Tartomány** (Domain) - Az AD alapvető egysége, amely egy biztonsági határt képez a felhasználók, számítógépek és erőforrások között. Minden tartomány rendelkezik egyedi DNS névvel (például: example.com).

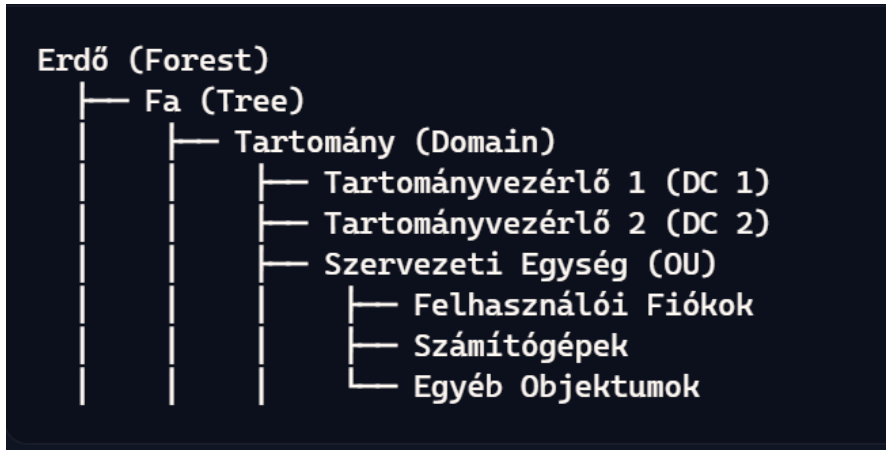
4. **Szervezeti Egység** (Organization unit - OU) - Logikai tárolóegységek, amelyek csoportosítják a felhasználói fiókokat, csoportokat, számítógépeket és egyéb objektumokat

A Címtárszolgáltató (AD DS) ábrázolása



A Tartományvezérlő (DC)

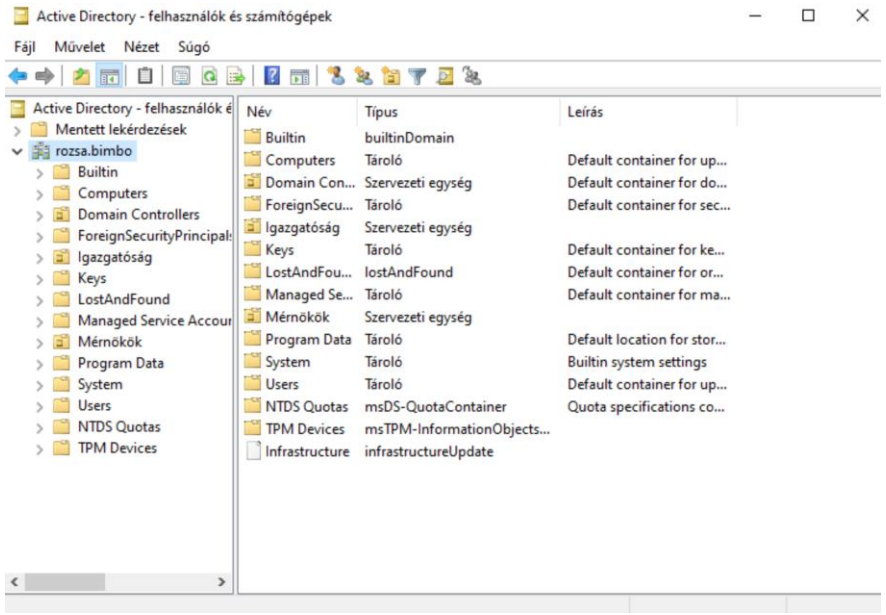
A **tartományvezérlő** (Domain Controller, DC) - Felelős a felhasználók és gépek hitelesítéséért, valamint a hálózati erőforrásokhoz való hozzáférés kezeléséért az adott tartományban



A Címtárszolgáltató Felhasználók és számítógépek

A címtárszolgáltató alatti **Active Directory – Felhasználók és Számítógépek** modulban történik

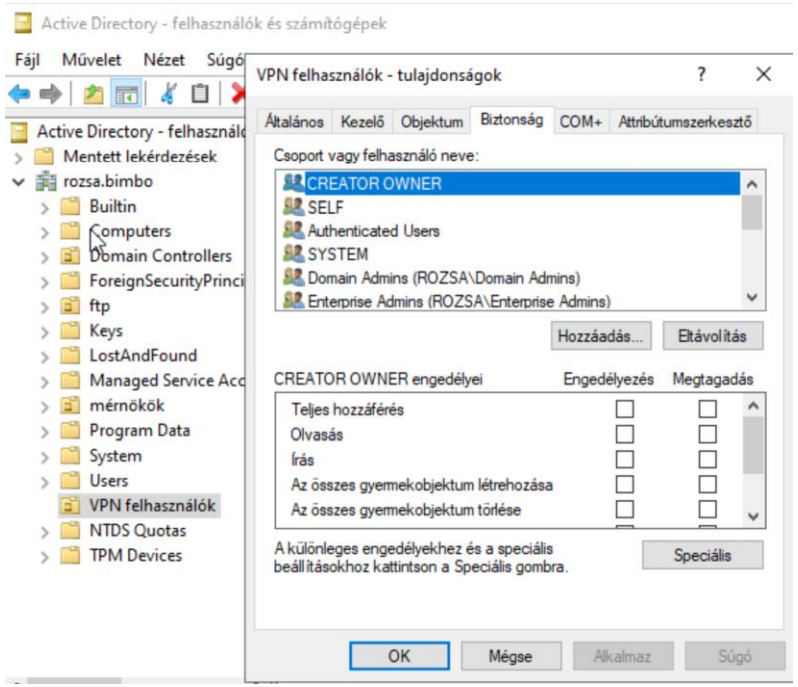
Itt az adott tartományunkhoz felvehetünk új szervezeti egységet (OU), csoportot (G), felhasználót, számítógépet, nyomtatót, stb.



A Címtárszolgáltató Jogosultságok

Ahhoz, hogy a címtárszolgáltató alatti **Active Directory – Felhasználók és Számítógépek** modulban elő tudjuk hívni az egyes objektumokra vonatkoztatott jogosultságokat (Biztonság fül), be kell kapcsolnunk a **Nézet** menüben a **Speciális beállítások**at

Ezen a fülön engedélyezhetjük a teljes hozzáférést, az olvasást, írást, ill. a gyermekobjektumokra vonatkoztatott szabályokat az adott AD objektum számára



A Címtárszolgáltató
Csoportok létrehozása

A címtárszolgáltatóban (AD DS) ugyanitt a Felhasználók és számítógépek moduljában történik többek közt a csoportok létrehozása, amelyhez a következő feltételeket kell meghatározni:

- **Csoportnév** (name)
- **Hatókör** (scope) – a., globális b., tartományon belüli, c., univerzális
- **Típus** a., biztonsági (secgrp), b., terjesztési (levelező)

Ezután az egyes már meglévő és jövőbéli felhasználókhoz hozzárendeljük a csoporttagságot. Másik módszer, hogy a csoportokhoz adjuk hozzá a tagokat – akár egy egész szervezeti egységet is!

A Címtárszolgáltató
Paracssor (Command Prompt)

Parancssorban felhasználót/csoprtot/szervezeti egységet a **dsadd** parancs segítségével adunk hozzá. A felhasználónév az a **samid**, a hatókör a **scope**, ami lehet g (globális), l (helyi tartomány), u (univerzális), a biztonsági csoport pedig a secgrp (yes/no), a tagokat pedig a **members** paranccsal adjuk hozzá. Törölni a **dsrm** paranccsal lehet. A cspoportházirendet a **gpupdate** paranccsal frissítjük (group policy update)!

Példa 1., Adjuk hozzá attila felhasználót a tanárok szervezeti egységébe, amely a szixi szervezeti egység alá tartozik. A bejelentkezési név atti legyen!
dsadd user “CN=attila,OU=tanárok,OU=szixi,DC=rozsa,DC=bimbo” -samid atti@rozsa.bimbo

Példa 2., Adjuk hozzá a külsősök biztonsági csoportot a tanárok szervezeti egységébe és Ugyanide is adjuk hozzá az előzőekben létrehozott attila felhasználót:
dsadd group “CN=külsősök,OU=tanárok,OU=szixi,DC=rozsa,DC=bimbo” -scope g -secrgp yes -members “CN=attila,OU=tanárok,OU=szixi,DC=rozsa,DC=bimbo”

Példa 3., töröljük az attila felhasználót:
dsrm "CN=attila,OU=tanárok,OU=szixi,DC=rozsa,DC=bimbo"

A Címtárszolgáltató
Paracssor – egyéb parancsok

dcdiag – a tartományvezérlő állapotának lekérdezése

dsquery user -name "attila" – felhasználónév lekérdezés

dsget user "CN=attila,OU=tanárok,OU=szixi,DC=rozsa,DC=bimbo" -display -email -tel – az AD objektum tulajdonságát jeleníti meg

dsmod user "CN=attila,OU=tanárok,OU=szixi,DC=rozsa,DC=bimbo" -pwd szixi123 – az AD objektum tulajdonságát módosítja

dsmove user "CN=attila,OU=tanárok,OU=szixi,DC=rozsa,DC=bimbo" -newparent "OU=külsősök,OU=tanárok,OU=szixi,DC=rozsa,DC=bimbo” – Az AD objektumok áthelyezésére szolgál

dsmove user "OU=tanárok,OU=szixi,DC=rozsa, DC=bimbo" –newname “teachers” – Az AD objektumok átnevezésére szolgál

dsrm "CN=attila,OU=külsősök,OU=tanárok,OU=szixi,DC=rozsa,DC=bimbo" – AD objektumok törlése

És amire nincs az AD-ben külön paracs, pl. felhasználó letiltása/engedélyezése: **net user attila active:no** és **net user attila:yes**

A Címtárszolgáltató PowerShell - példák

A PowerShell egy konfigurációs és feladat-automatizálási eszköztár. Főbb tulajdonságai: objektumorientált, parancsmagokat használ (cmdlets), automatizál ill. cross-platform működik (Core verzió).

Első lépésként telepíteni kell az címtárszolgáltató modulját a következő parancssal:
Import-Module ActiveDirectory

New-ADUser -Name ”Alexovcs Attila" -GivenName “Attila" -Surname “Alexovics" -SamAccountName “attila" -UserPrincipalName “attila@rozsa.bimbo" -Path "OU=tanárok,DC=rozsa,DC=bimbo" -AccountPassword (ConvertTo-SecureString „szixi123" -AsPlainText -Force) -Enabled $true – felhasználó hozzáadása, és engedélyezése

Disable-ADAccount -Identity “attila” – felhasználó letiltása
Enable-ADAccount -Identity "attila” – felhasználó engedélyezése

Get-Help New-ADUser -Detailed - részletes segítség kérése a parancsról PowerShell-ben

A Címtárszolgáltató Tartalomvédelmi Szolgáltatások 1

Az címtárszolgáltató tartalomvédelmi szolgáltatásai (**AD RMS**, Active Directory Rights Management Services) lehetővé teszi **az információk védelmét és kezelését a vállalatokban** - a dokumentumokat, e-maileket és más információkat titkosítják, hogy csak jogos felhasználók érheték el és használhassák

1., Telepítése a Kiszolgálókezelőből (Server Manager) történik. Ezután rákattintunk a sárga háromszögre, és **gyökérfürtöt** (cluster) kell létrehoznunk, amely lehet tanusítványkezelésre és licenszelésre vagy csak licenszelésre.

2., A következő lépésben létre kell hozni a **konfigurációs adatbázist** (SQL, vagy Windows belsős adatbázist használjuk).

3., Eztán nem szakítjuk félbe a konfigurálást, hanem **AD DS**-ben felvesszük a tartalomvédelemért felelős admint a felhasználók mappába (csinálunk egy “**rmsadmin**” felhasználót). A felhasználó tulajdonságainál felvesszük a A “**következő tagjá**”ba mint **Domain Admin** –t is.

4., visszatérünk az RMS konfigurálásba, majd a szolgáltatásfióknál megadjuk a **ROZSA\rmsadmint** –t és a jelszót, a kriptográfiai módot (2048-bit RSA), a fürtkulcstárolót és annak a jelszavát

A Címtárszolgáltató Tartalomvédelmi Szolgáltatások 2

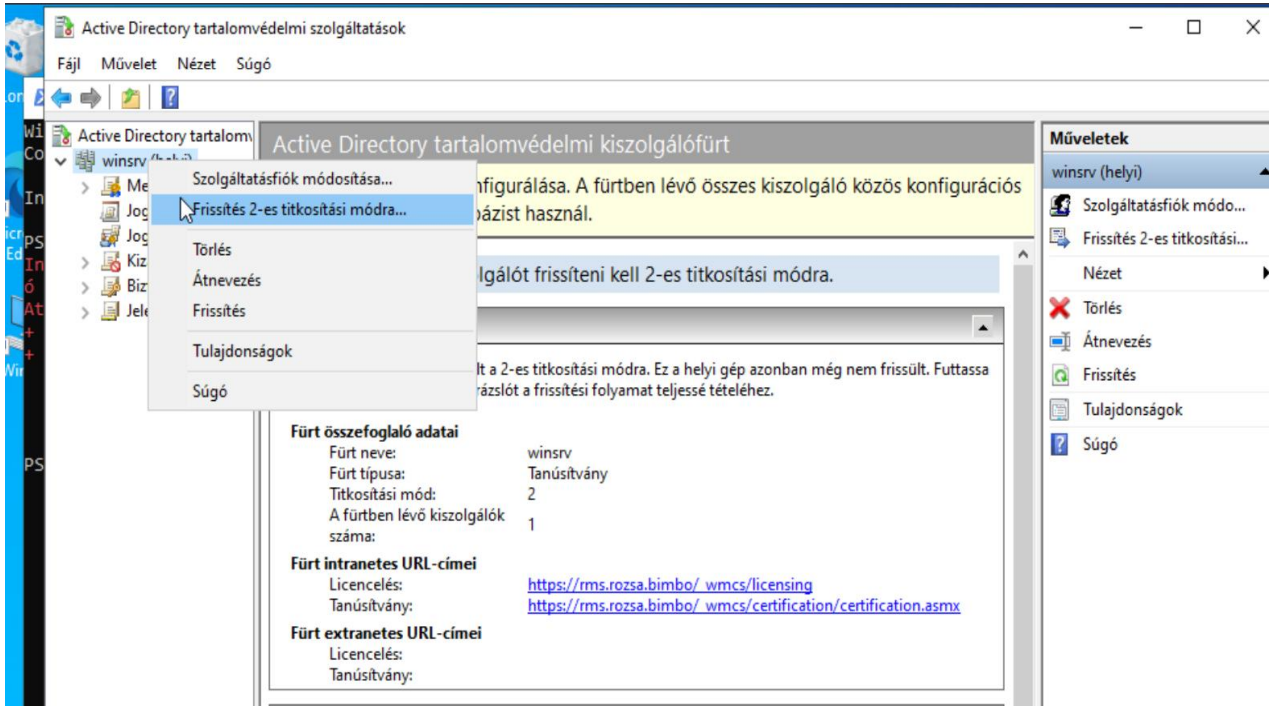
5., A fürt webhelye default, majd a fürt címe **SSL** opció és ott: **rms.rozsa.bimbo**, 443-as port

6., **Tanusítványok** (CA általi betöltés, vagy önaláírt tanusítvány)

7., **A szolgáltatás** kapcsolódási pontjának **regisztrációja most**

8., Felvesszük a megosztani kívánt **mappát** (pl. a C meghajtón Secret), ahol a “megosztás” és a “biztonság” fülön felvesszük az Admint és a “Domain Users”-t az engedélyekkel, az “Everyone”-t eltávolítjuk! Ebbe a mappába helyezzük majd a tartalomvédelmi célból menedzselni kívánt dokumentumokat

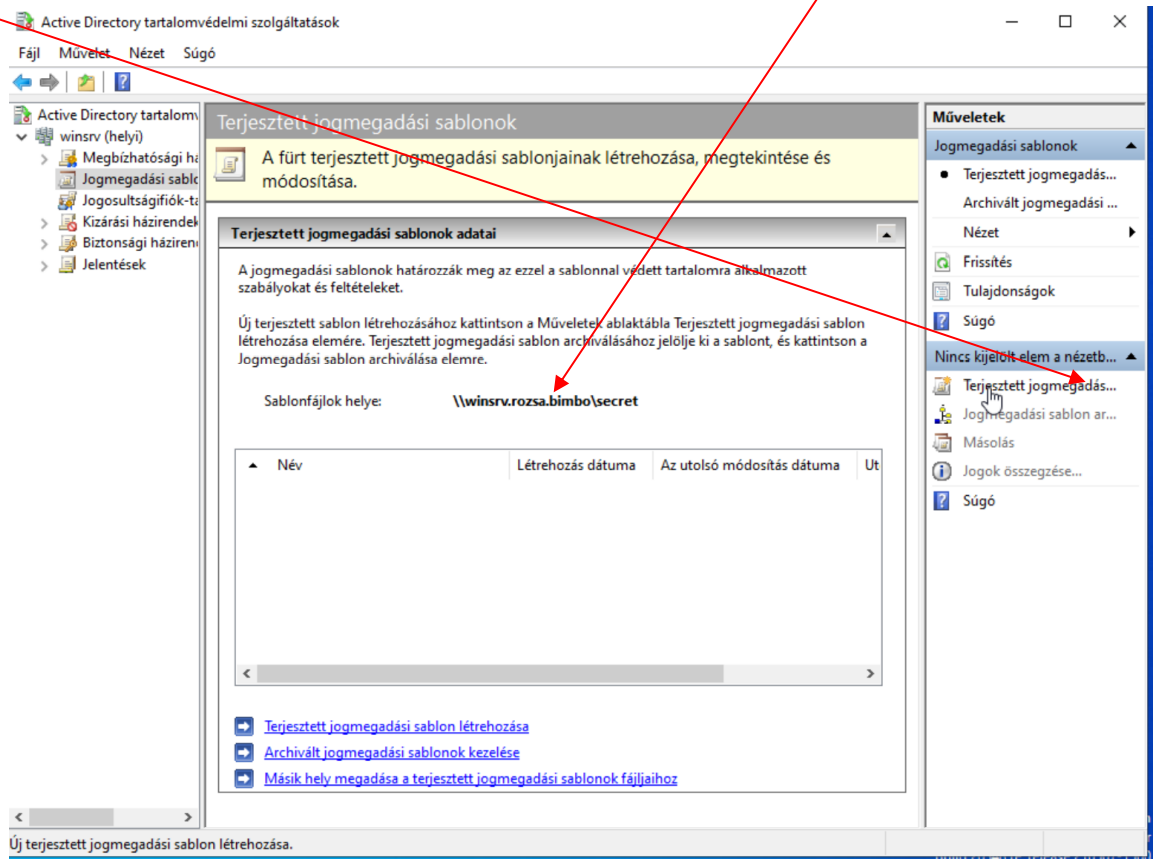
9., Elindítjuk a tartalomvédelmi szolgáltatásokat, majd frissítünk a 2-es titkosítási módra (varázsló), majd elfogadjuk az önaláírt tanusítványt



A Címtárszolgáltató Tartalomvédelmi Szolgáltatások 3

10., A jogmegadási sablonokban felvesszük tartalomvédelmi mappánkat

11., Terjesztett jogmegadási sablont hozunk létre



A Címtárszolgáltató
Tartalomvédelmi Szolgáltatások 4

A Címtárszolgáltató Tanusítványkezelő

A címtárszolgáltató tanusítványkezelő szolgáltatásai (**AD CS**, Active Directory Certification Services) lehetővé teszi, hogy **digitális tanúsítványokat állítsanak ki és kezeljenek**. Ezek a tanúsítványok számos feladatot végezhetnek el, beleértve a következőket: hitelesítés, adatvédelem, digitális aláírás, integritás, hálózat hitelesítés. Cégek és szervezetek esetében saját “hitelesítő intézményt” hoz létre, amely digitális tanúsítványokat állít ki és kezel a belső és külső biztonsági igények kielégítése érdekében. Telepítése a Kiszolgálókezelőből (Server Manager) történik – Active Directory Certification Services

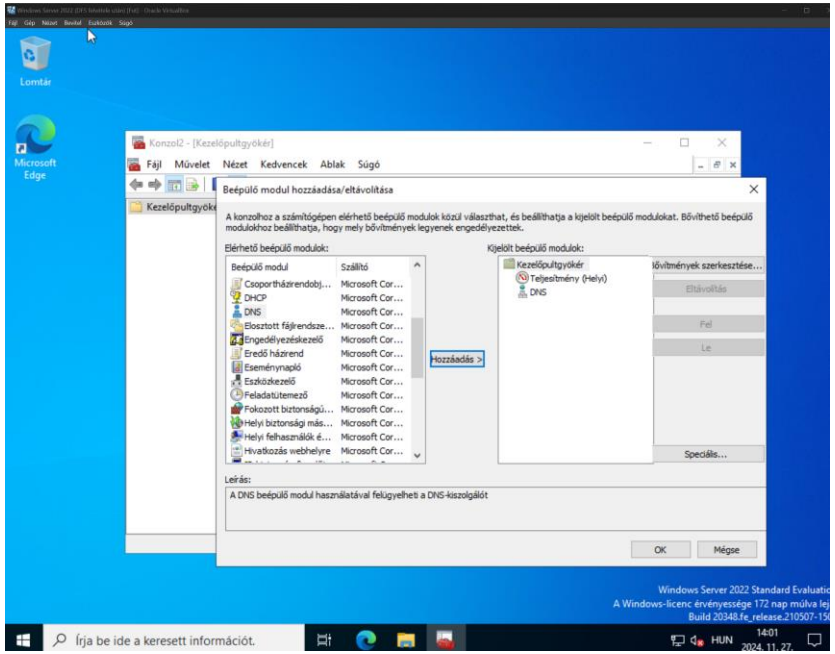
Rendszerfelügyelet (MMC)

A rendszerfelügyeleti (adminisztratív) eszközök Windows Server alatt az **MMC (Microsoft Management Colsole)**. Ez egy keretrendszer, amely lehetővé teszi a rendszergazdáknak a különböző adminisztratív eszközök (snap-ins) közös kezelőfelület alatti futtatását és kezelését – pl. DNS, tejesítményfigyelő, eseménynapló, szolgáltatások, eszközkezelő stb.

- Már telepítve van, nem kell telepíteni. A keresősor aljára beírjuk, hogy **mmc.exe**

- Bepakoljuk a figyelni kívánt eszközöket pl. DNS, teljesítményfigyelő stb.

- Elmentjük sablonba, hogy bármikor megnyitható legyen



A csoportházirend (Group Policy)

A **csoportházirend** (Group Policy) egy hatékony eszköz, amely lehetővé teszi a rendszergazdáknak, hogy szabályozzák a felhasználók és számítógépek beállításait Active Directory (AD) környezetben

Kezelésére a **Csoportházirend kezelése** konzol (Group Policy Management Console, GPMC) szolgál. Vagy a keresőből **gpmc.msc**, vagy a Kiszolgálókezelő (Server Manager) Eszközök menüből indíthatjuk el

A csoportházirendek lehetővé teszik a felhasználói és a számítógép konfigurációt:

- **Felhasználói konfiguráció**: azon beállításokat jelenti, amelyeket egy adott felhasználóra alkalmaznak. Pl. automatikusan induló programok, hozzáférési jogok és szabályok

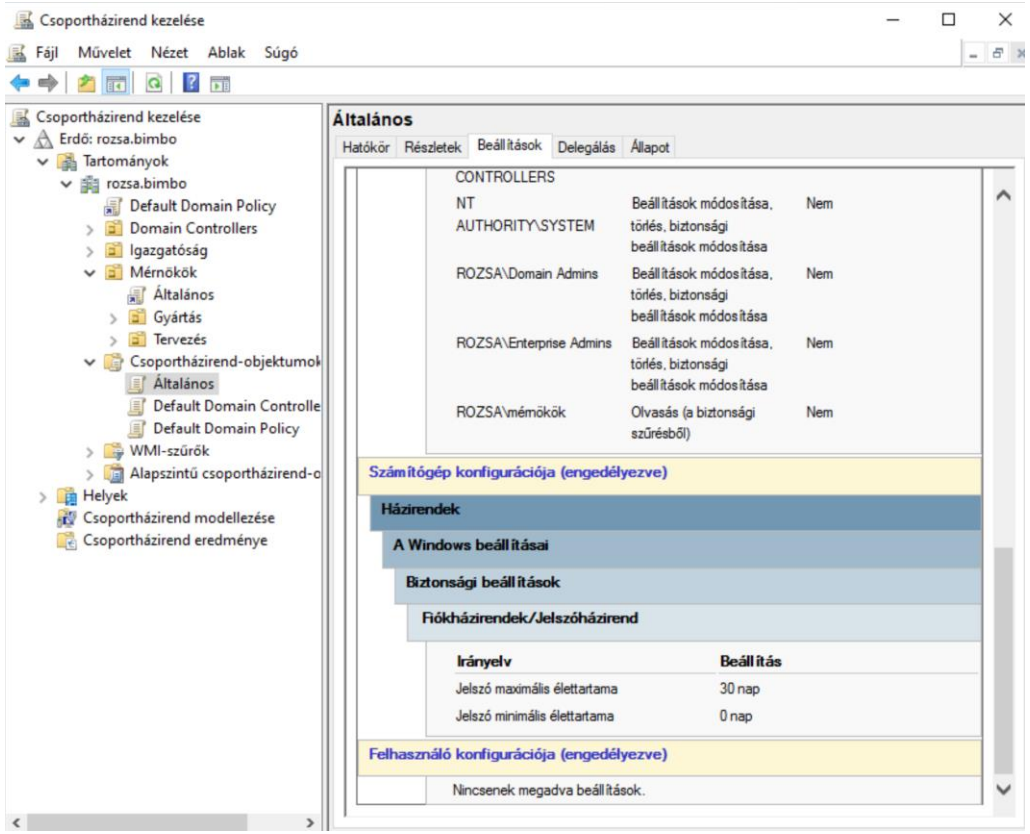
- **Számítógép konfiguráció**: azon beállításokat jelenti, amelyeket egy adott számítógépre alkalmaznak. Hozzáférés az erőforrásokhoz, hálózati beállítások, biztonsági szabályok

A csoportházirend alapok (Group Policy)

Az újonnan felvett házirendhez **hozzáadjuk a felhasználókat/csoportokat (vagy magán az objektumon hozunk létre új csoportházirendet)**, majd egér jobb gombbal megnyitjuk a **Szerkesztés**-t. Itt kiválaszjuk hogy felhasználóra, vagy a számítógépre vonatkozzon a csoportházirend. Szoftvereket telepíthetünk automatikusan, ill. Windows beállítások ->Biztonsági beállítások->fiókházirend-nél beállíthatjuk a jelszó élettartalmát pl..

A csoportházirend változásainak **érvénybe léptetés**éhez a tartományunkra kattintva (rozsa.bimbo) jobb gombbal Frissítés, vagy ki kell adni parancssorban a **gpupdate /force** parancsot.

A létrehozott csoportházirend összefoglalója



Az érvénybe léptetett csoportházirend konzolnak Beállítások fülén összefoglalót készítünk, majd megjelennek a változások (ez esetben a jelszó max. élettartama)

Csoportházirend példa
regedit tiltás klienseknek

Válasszuk ki azt az objektumot, amelyre érvényes lesz az új házirend

Itt hozzunk létre **új csoportházirend**et (Jobb gomb, csoportházirend-objektum létrehozása….)

Megadjuk a nevet “regedit tiltás”, OK, majd ezt a csoportházirendet jobb gomb, **Szerkesztés**…

Felhasználó konf. → Házirendek → Felügyeleti sablonok → **Minden beállítás**

A Beállításjegyzék szerkesztőeszközeihez való hozzáférés megakadályozása –ra kattintunk

Itt **engedélyezzük**, OK, majd bezárjuk az újonnan létrehozott csoportházirend ablakát

Windows Serveren érvénybe léptetjük **gpupdate /force**

A kliens gépen is érvénybe léptetjük **gpupdate /force**

Csoportházirendek érvényesítése kliensen – CP/PS

gpupdate /force – parancssorban a csoportházirend késleltetés nélküli érvénybe léptetése

Ha sok kliens gépünk van, és nem akarunk ezzel bajlódni minden egyes alkalommal - távolról is kiadhatjuk a parancsot. Ehhez engedélyeznünk kell:

- kliens oldalon a távoli PowerShell elérést: **Enable-PSRemoting -Force**,

- majd a Windows Serveren a csoportházirend azonnali érvényesítését:
  (pl. IP-cím alapján) **Invoke-GPUpdate -Computer „192.168.0.33" -Force**
  (vagy NetBIOS név…) **Invoke-GPUpdate -Computer „ATTIPC" –Force**
  (vagy FQDN tartománynév…) **Invoke-GPUpdate -Computer „atti.rozsa.bimbo" -Force**

- Ha az összes klienst akarjuk egyszerre felfrissíteni, akkor:

Get-ADComputer -Filter * | ForEach-Object { Invoke-GPUpdate -Computer $_.Name -Force }

Csoportházirendek érvényesítése a kliensen szkripttel

Harmadik módszerként pedig megírunk egy parancssori (powershell) scriptet, majd elmentjük pl. **gpupdate.bat** név alatt:

@echo off
gpupdate /force

Elindítjuk a szerverünkön a csoportházirend kezelőt, majd a kiválasztott objektumhoz rendelt csoportházirendet szerkesztjük (megnyitjuk)

Felhasználó konf. → Házirendek → Windows beállítás → Parancsfájlok → **Bejelentkezés**

Itt hozzáadjuk a scriptet, majd OK, kilépünk

Felfrissítjük a csoportházirendet a szerveren: **gpupdate /force**

Csoportházirendek – szoftverek automatikus indítása példa

Azt akarjuk, hogy induljon el a jegyzetfüzet - megírjuk rá a parancssori scriptet, majd elmentjük pl. **notepad.bat** név alatt:
@echo off
start notepad.exe

Vagy megírunk egy powershell scriptet, majd elmentjük pl. **notepad.ps1** név alatt:
Start-Process notepad.exe

Elindítjuk a szerverünkön a csoportházirend kezelőt, majd a kiválasztott objektumhoz rendelt csoportházirendet szerkesztjük (megnyitjuk)

Felhasználó konf. → Házirendek → Windows beállítás → Parancsfájlok → **Bejelentkezés**

Itt hozzáadjuk az elmentett scriptet, majd OK, kilépünk

Felfrissítjük a csoportházirendet a szerveren: **gpupdate /force**

Megjegyzés: Automatikusan indítható alkalmazások pl. paint (mspaint.exe), feladatkezelő (taskmgr.exe), számológép (calc.exe), fájlkezelő (explorer.exe)

Csoportházirendek – szoftverek automatikus indítása útvonallal

Azt akarjuk, hogy induljon el alkalmazás - megírjuk rá a parancssori scriptet, majd elmentjük pl. **notepad.bat** név alatt:

@echo off
start "" "C:\Windows\System32\notepad.exe"

Vagy megírunk egy powershell scriptet, majd elmentjük pl. **notepad.ps1** név alatt:
Start-Process "C:\Windows\System32\notepad.exe"

A többi lépés az előző példa alapján történik, mint bejelentkezési szkript (logon script), majd csoportházirend frissítés (gpupdate /force)

Csoportházirendek – szoftverek automatikus telepítése

Kiválasztjuk a vonatkoztatott csoportházirendet (vagy létrehozunk egyet), majd szerkesztés

Számítógép konf. → Házirendek → Szoftverbeállítások → Szoftverek telepítése

Jobb gomb → Új → Csomag

Itt kiválasztjuk a szoftver útvonalát és a szoftvert (MSI installer / ZAP alacsony szintű csomag), amelyet a szerverünkről a kliens gépre kívánunk feltelepíteni, majd OK, kilépünk

Felfrissítjük a csoportházirendet a szerveren: **gpupdate /force**

statikus IP-cím felvétele

1., Ellenőrizzük a parancssorban a jelenlegi automatikusan kiosztott IP-t (**ipconfig**)

2., A hálózati kapcsolatoknál (Network Connections) kiválasztjuk a hálózati adaptert, és a tulajdonságainál az **IP4 protokoll**nál megadjuk a statikus értékeket:

Az esetemben az Ipconfig értékeit beírtam az IP4 protokollba, ahogy a /24-es almaszkot is:
IP address: 192.168.0.10
Subnet mask: 255.255.255.0
Default Gateway: 192.168.0.1

DNS server address-re meg a szerverük lesz, tehát 192.168.0.10 (és nem a google 8.8.8.8)

3., A Windows Server **újraindítása**

4., Ellenőrizzük a parancssorban az IP címet (**ipconfig**)

A tartománynévrendszer - DNS

A **DNS (Domain Name System)** egy hierarchikus és decentralizált névadó rendszer, amely az interneten és más IP-hálózatokon használt **domain neveket IP-címekké alakítja át**. A DNS teszi lehetővé, hogy az emberek könnyen megjegyezhető neveket használjanak IP helyett.

Funkciói:

a., **névrendszer** - domain neveket IP-címekhez rendel

b., **hierarchia** = gyökérzóna + országkód/legfelsőbb szintű domének (LTD)
pl. szixi.hu

c., **zónák és rekordok**: A DNS adatatbázisa ezekből áll. A zónák a tartományt lefedő adatokat tartalmaznak, addig a rekordok egyedi leképezések

- A record – IP4 cím leképezése a domainhez
- AAAA record – IP6 cím leképezése a domainhez
- CNAME – canonical (kanonikus, hivatalos) rekord, ami egy másik domain nevére utal pl. atti.szixi.hu IN CNAME attila.szixi.hu
- MX – exchange record
- PTR – pointer, mutató – visszafelé keresés rekord

A DNS működése

1. **Lekérdezés** - Amikor beírunk egy domain nevet a böngészőbe, egy DNS lekérdezés indul el, hogy megtalálja az IP-címet.

2. **Feloldás** (Resolving) - A lekérdezés először a lokális DNS cache-ben keres, majd ha ott nem találja, továbbítja a megfelelő DNS szerverekhez a hierarchián keresztül (gyökér, TLD)

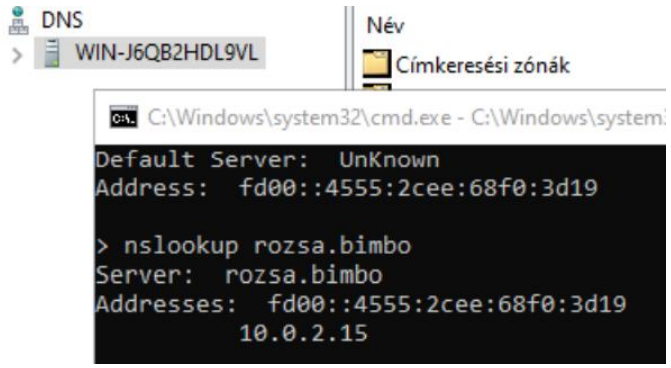
3. **Visszaadás** - Ha megtalálta az IP-címet, a böngésző csatlakozik a megfelelő szerverhez az IP-cím segítségével

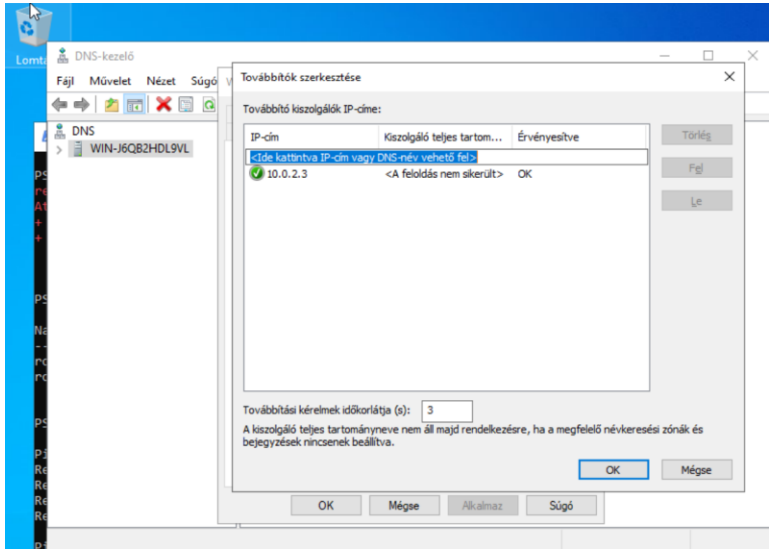
DNS konfigurálása

1., A DNS manager-ben ha üres a címkeresési zóna (**forward lookup zone**) adjunk hozzá varázslóval egy újat, AD-integrációval, alapbeállításokkal

2., A DNS manager-ben ha üres a névkeresési zóna (**reverse lookup zone**) adjunk hozzá varázslóval egy újat, AD-integrációval, alapbeállításokkal

3., Bridge módban a DNS managernél a szerverünk tulajdonságainál a továbbítók-nál (forwarder) adjuk hozzá a DNS szerverünk IP-jét – esetemben 192.168.0.1, hogy menjen az internetes névfeloldás. NAT módban a Virtualbox erőszakol egy ún. DNS szerver default-t (10.0.2.3 – zöld pipa), amelyet nem tudunk átírni majd a 10.0.2.15 –re a továbbítóknál, de ettől még a belső DNS szerver 10.0.2.15 lesz!

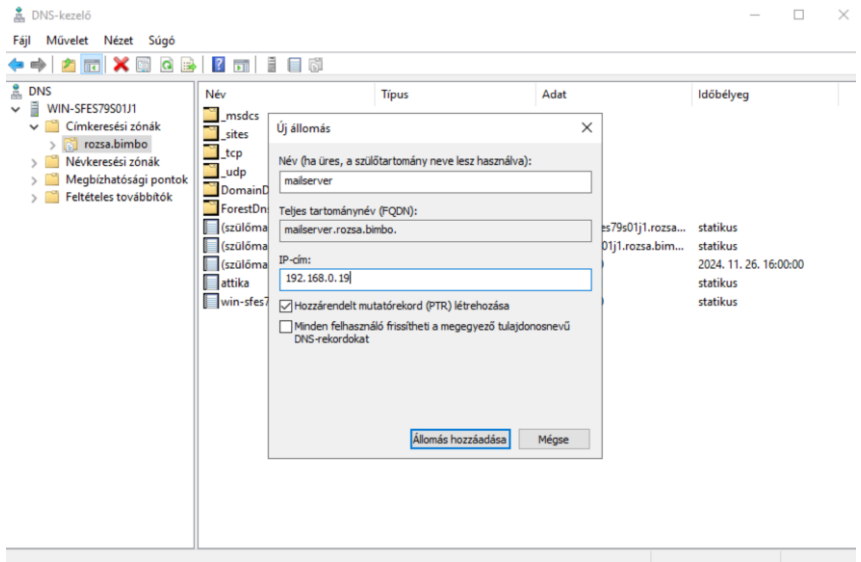




DNS konfigurálása - példa

Állítsuk be a DNS szolgáltatást a szerveren úgy, hogy a adjunk hozzá egy új állomást, ahol a gép neve “mailserver”, és az IP címe 192.168.0.19 legyen

Megoldás: A DNS manager **címkeresési zónák** megadott tartományához adjunk hozzá egy új állomást, és oda írjuk be a megadott értékeket. Esetemben a megadott tartomány rozsa.bimbo.



DHCP szerver telepítése

A DHCP (Dynamic Host Configuration Protocol) egy hálózati protokoll, amely automatikusan kiosztja az IP-címeket és más hálózati konfigurációs adatokat a számítógépek és egyéb eszközök számára egy adott hálózaton egy adott ideig.

A telepítés menete:

1., Szerepkörök és szolgáltatások hozzáadásánál a **DHCP** opció kiválasztása.

2., Az újraindítást (**restart**) bepipáljuk a telepítés folyamán

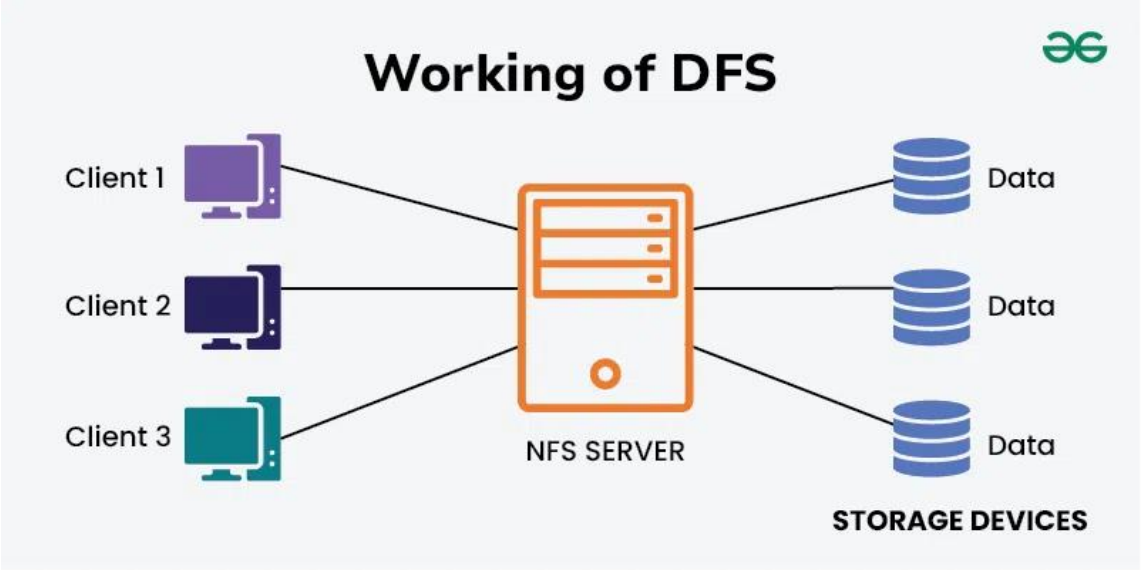
3., Az Eszközöknél megjelenik a DHCP opciójánál, kibontva az IPv4-nél **felvesszük az új hatókört** (New Scope)

4., Beállítjuk a **kiválasztott tartományt** (range) és a **kizárandó tartományt** (exclusion)

Kliens oldalon kiadjuk a Windows gépeken a frissítő parancsokat:
ipconfig /release - a számítógép "elengedi" az IP-címet, és többé nem használja azt
ipconfig /renew - lekéri az új IP-t a DHCP szervertől

Elosztott Fájlrendszer - DFS

Az elosztott fájlrendszer **DFS (Distributed File System)** lehetővé teszi, hogy a fájlok több kiszolgáló között eloszlassák, és mindezt úgy kezeljék, mintha az összes fájl egy helyen lenne tárolva



DFS szerver telepítése

A telepítés menete:

1., Szerepkörök és szolgáltatások hozzáadásánál **File and Storage Services-t** szétbontva bepipáljuk a **DFS Namespaces**-t.

2., Az újraindítást (**restart**) bepipáljuk a telepítés folyamán

3., Elindítjuk az Elosztott fájlrendszer kezelőjét vagy a keresőablakból, vagy a kiszolgálókezelő eszközei közül (Server Manager >> Tools- ból)

4., Hozzáádjuk a virtuális gépünk nevét, ellenőrizve természetesen
(az én esetemben WIN-SFES79S01J1…), majd az útvonalat, ahol fizikailag megjelenik.

5., Ha kvótákat is hozzá akarunk rendelni, akkor telepítenünk kell a File Server Resource Manager-t is a szétbontott **File and Storage Services**-ből

RAID – Alapfogalmak

A **RAID** (Redundant Array of Independent Disks) egy olyan technológia, amely több fizikai merevlemezt kombinál egy logikai egységgé, hogy javítsa az adatvédelmet, a teljesítményt vagy mindkettőt.

A **redundancia** olyan adatokat vagy rendszereket jelent, amelyek **másolatot tartalmaznak** egy eredeti adat vagy rendszer helyett, hogy növeljék a megbízhatóságot és az adatvédelmet. Amikor egy rendszer redundanciával működik, az azt jelenti, hogy az adatok több példányban is tárolva vannak, így ha egy példány elveszik vagy megsérül, az adat másolatok segítségével helyreállítható.. Pl. RAID 1

A **paritás** egy olyan hibaellenőrzési módszer, amely segítségével az adatok hibás bitjeit lehet azonosítani és helyreállítani. A paritás egy **extra bit vagy információ, amelyet az adatokkal együtt tárolnak**, és amely segít az adatvesztés vagy adatkárosodás felismerésében és kijavításában. Pl. RAID 5

RAID felosztás

RAID 0 (Stripping)
Előny: Kiváló teljesítmény, az adatokat párhuzamosan írják és olvassák a lemezekről
Hátrány: Nincs adatvédelem

RAID 1 (Mirroring)
Előny: Adatvédelem
Hátrány: költséges, kétszer annyi lemez szükséges, mint a tárolni kívánt adatok mennyisége.

RAID 5 (Stripping with parity)
Előny: Növeli az adatvédelmet paritásblokkal,
Hátrány: legalább 3 lemez szükséges, teljesítménycsökkenés

RAID 6 (Stripping with double parity)
Előny: Növeli az adatvédelmet dupla paritásblokkal, két lemez meghibásodását is képes kezelni
Hátrány: legalább 4 lemez szükséges, teljesítménycsökkenés

RAID 10 (1+0, Mirroring and Stripping)
Előny: RAID 0 és RAID 1 kombinációja, kiváló teljesítményt és adatvédelmet kínál.
Hátrány: költséges, legalább 4 lemez szükséges

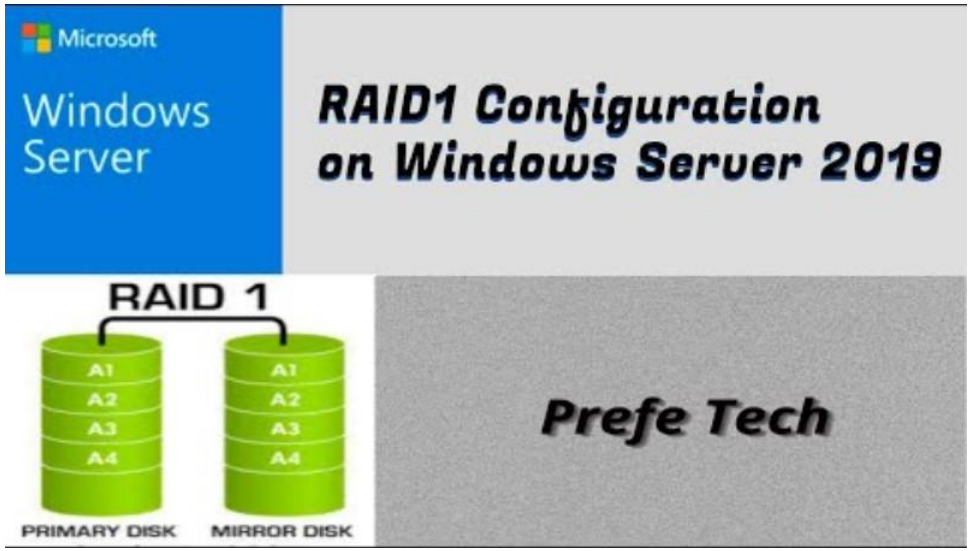
RAID - szemléltetés

a RAID megvalósítása

Windows Serveren RAID megoldás létrehozásához eszközt kétféleképp tudjuk megnyitni

- Kiszolgálókezelő → Eszközök → Számítógép-kezelés → Lemezkezelés
- Vagy a keresősoron beírjuk, hogy **diskmgmt.msc**

Konkrét példa. RAID 1: Adott két üres lemez, azonos gyártótól, azonos típus és paraméter. A lemezkezelőben a lemezre kattintva jobb gomb, Új Tükrözött Kötet… (New Mirrored Volume), majd elindul ennek a telepítővarázslója.



WINS szerver telepítése

A WinS kiszolgáló a NetBIOS nevek és az IP címek közötti leképezéseket tárolja egy adatbázisban – Microsoft fejlesztette. **Már a DNS-t használják helyette**.

A NetBIOS (Network Basic Input/Output System) egy hálózati protokoll, amely lehetővé teszi a hálózati alkalmazások számára, hogy kommunikáljanak egymással egy helyi hálózaton (LAN). IBM fejlesztett ki régen. Névszolgáltatás, üzenetküldés-fogadás, munkamenet-kezelés.

Mivel az újabb rendszerekben és hálózatokban kifejezetten nem ajánlott a DNS végett, a Windows Server 2022-es kiadása már nem is tartalmazza alapból, csak a Microsofttól lehet letöltetni, vagy eröltetve a **PowerShell**-ből: **Install-Package -Name WINSInstaller -Force**

Web szerver (IIS) telepítése

Windows Server alatt a webservert az **IIS (Internet Information Service)** szolgáltatás segítségével lehet telepíteni. Az interneten keresztül szolgáltat weboldalakat és egyéb digitális tartalmakat a felhasználóknak.

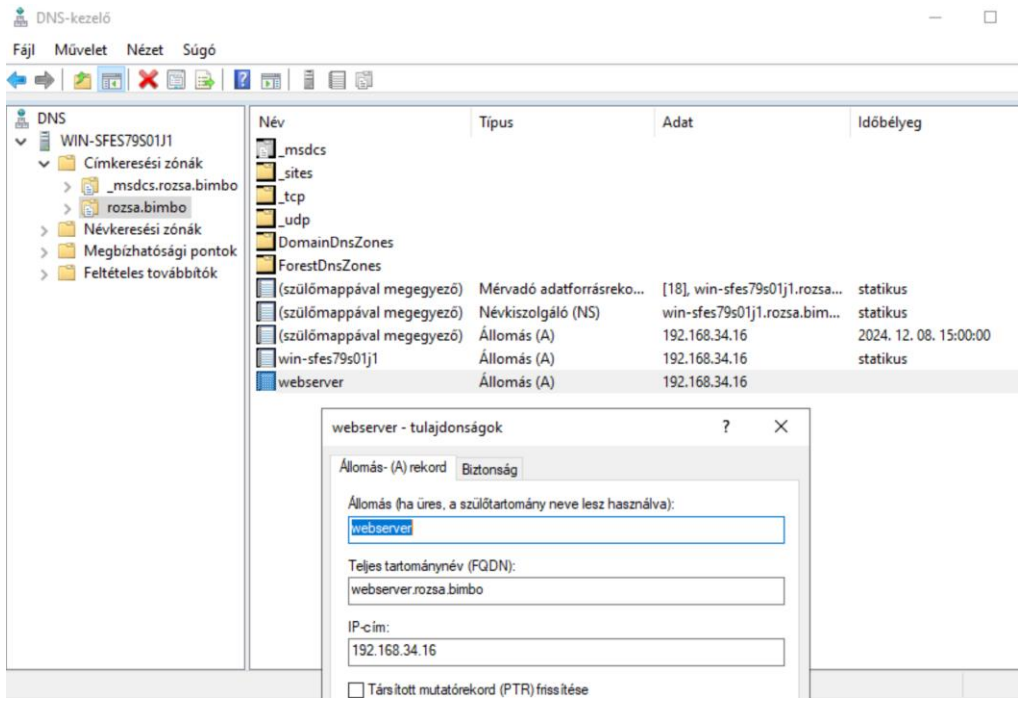
A kiszolgálókezelőben (Server Manager) a Szerepkörök és szolgáltatásoknál kiválasztjuk a Web Server (IIS) opciót.

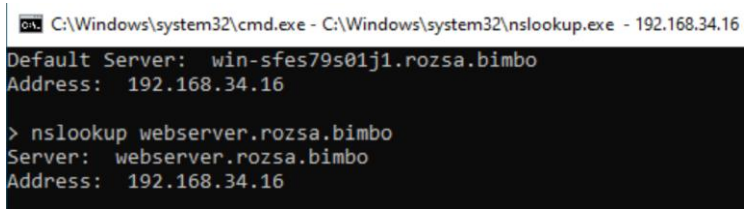
Telepítés után a Kiszolgálókezelőben (Server Manager) Eszközök (Tools) Internet Information Service (IIS)-re kell kattintani, vagy a keresősorba beírjuk, hogy **iis**. A default website helye a **C:\inetpub** mappában van.

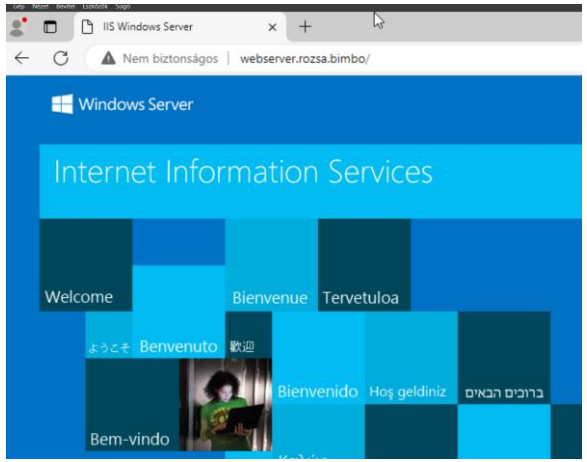
Web szerver (IIS) DNS

Leelenőrizzük a böngészőben a webszerverünk IP-jét. Esetemben http://192.168.34.16

A DNS managerben a címkereső zónában (forwarding zone) hozzáadjuk új állomásként (A-record) mutató nélkül (PTR pointer nélkül) – az én esetemben a “webserver” nevet az 192.168.34.16 IP-címemhez, majd az nslookup paranccsal ill. a böngészőben ellenőrizzük a webserver.rozsa.bimbo –t.







FTP szerver telepítése

Windows Server alatt az FTP kiszolgálót a **Web Server (IIS)** szolgáltatásban lévő **FTP Server** segítségével lehet telepíteni. A fájlok átvitelére szolgál a hálózaton keresztül az FTP (File Transfer Protocol) protokoll segítségével.

A kiszolgálókezelőben (Server Manager) a Szerepkörök és szolgáltatásoknál szétnyitjuk a Web Server (IIS) menüjét, majd ott kiválasztjuk az FTP Server opciót.

Telepítés után a Kiszolgálókezelőben (Server Manager) Eszközök (Tools) Internet Information Service (IIS)-re kell kattintani, vagy a keresősorba beírjuk **iis**. Szétbontva a kapcsolatoknál a “Helyek” mappára jobb gombbal kattintva megjelenik, hogy **“FTP-hely hozzáadása…”**

FTP szerver beállítása

Az IIS-ben szétbontva a kapcsolatoknál, mikor hozzáadjuk a helyekhez az új FTP-helyet, akkor megadjuk a nevét és a tartalomkönyvtárat (itt létrehozunk egy könyvtárat a tárolónkon)

A kötésnél (binding) beírjuk az IP-címet – esetemben a saját IP-t. 192.168.34.16, port 21, majd kiválasztjuk a megfelelő SSL opciót - **amelyről bővebben is szót ejtünk majd a tananyag SSL, TSL, HTTPS, és tanusítványok részeinél**.

Kiválasztjuk a minden felhasználó (all users opciót), és bepipáljuk az írást és olvasást (read+write) opciókat.

Megjegyzés: Kliens gépről az FTP szerverhez a Filezilla / “Commander” jellegű programokat használunk

FTP szerver beállítása

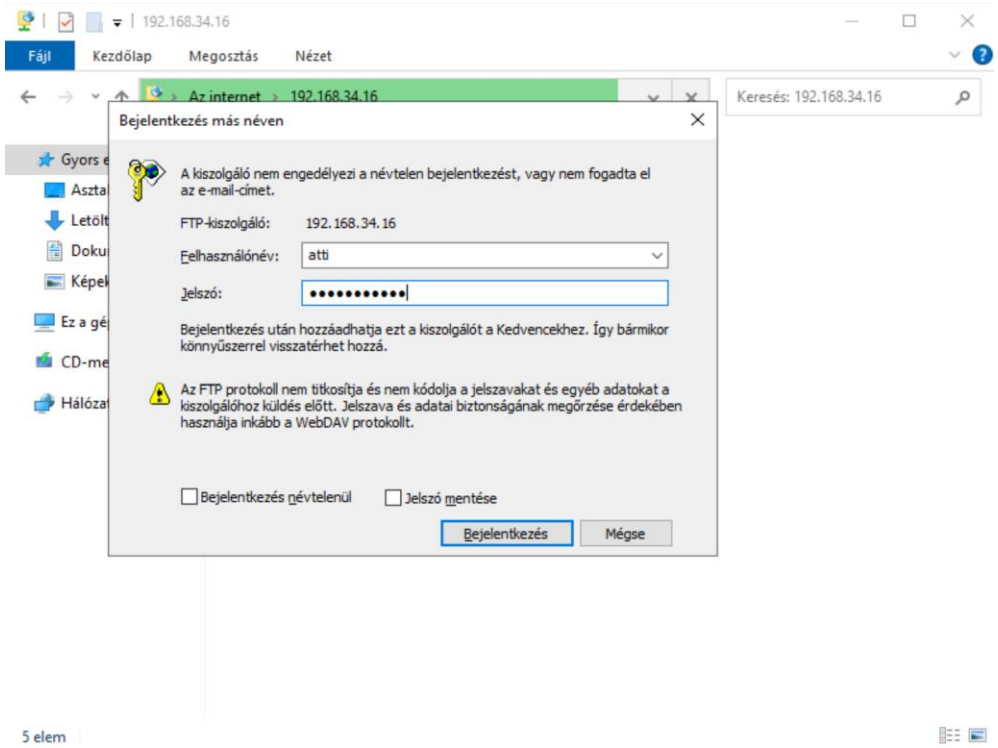
Az IIS-ben szétbontva a kapcsolatoknál, mikor hozzáadjuk a helyekhez az új FTP-helyet, akkor megadjuk a nevét és a tartalomkönyvtárat (itt létrehozunk egy könyvtárat a tárolónkon)

A kötésnél (binding) beírjuk az IP-címet – esetemben a saját IP-t. 192.168.34.16, port 21, majd kiválasztjuk a megfelelő SSL opciót - **amelyről bővebben is szót ejtünk majd a tananyag SSL, TSL, HTTPS, és tanusítványok részeinél**.

Kiválasztjuk a minden felhasználó (all users opciót), és bepipáljuk az írást és olvasást (read+write) opciókat.

Csatlakozás FTP szerverhez

Megjegyzés: Kliens gépről az FTP szerverhez a Filezilla / “Commander” jellegű programokat használunk, viszont alapból ha megnyitjuk az fájlkezelőt (explorer) tudunk csatlakozni az FTP protokoll segítségével. Itt alapesetben egy címtárszolgáltatóban (Active Directory) felvett felhasználót használtam az **ftp://192.168.34.16** paranccsal



Biztonságos kapcsolat
HTTPS / FTPS

Az interneten keresztül küldött adatok védelme érdekében ún. biztonságos kapcsolati protokollokat vezettek be amelyek lényege, hogy az alapprotokollok titkosítást is alkalmaznak.

Web: **HTTPS** = HTTP + SSL/TLS

File: **FTPS** = FTP + SSL/TLS

- **Kapcsolat létrehozása**: A kliens böngésző egy HTTPS kérést küld a szervernek

- **Kézfogás**: A szerver és a kliens SSL/TLS kézfogást hajt végre, amely során megegyeznek a titkosítási algoritmusokban és cserélik a titkosítási kulcsokat

- **Titkosított adatátvitel**: Az adatok titkosítva kerülnek átvitelre a böngésző és a szerver között, védve azokat a lehallgatás és a manipuláció ellen

SSL / TLS

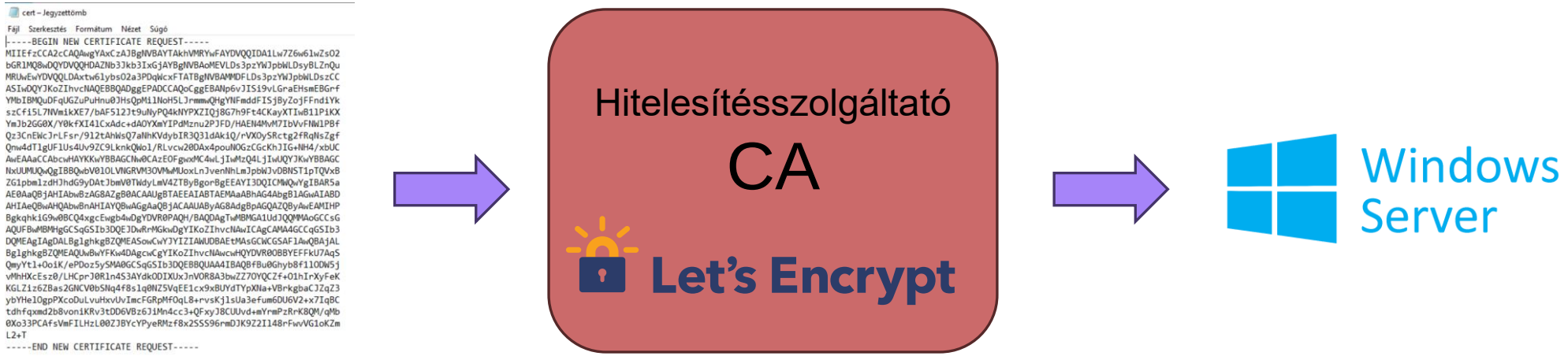
Az SSL (Secure Sockets Layer) egy biztonsági technológia, amely titkosítást alkalmaz az interneten keresztül küldött adatok védelmére. A TLS (Transport Layer Security) ennek egy új verziója.

Harmadik féltől ún. **Hitelesítésszolgáltatótól (CA) kérhetnek SSL tanúsítványt**, amelyet telepítünk a szerverünkre - Let's Encrypt (ingyenes), Comodo SSL, DigiCert, GoDaddy… **de önmagunk is aláírhatjuk.**

Tanusítványok (Certificate)

Az SSL/TLS protokollok megkövetelik ún. tanúsítványok használatát az adatátvitel titkosításához és hitelesítéséhez. Mint említettük a **hitelesítésszolgáltatók** (**CA**, Certification Authority-k) állítják ki a tanúsítványokat, így a felhasználók bízhatnak a tanúsítvánnyal rendelkező szerverekben.

Windows Server-en az IIS managerben a szerverünkön az IIS tábla Kiszolgálói tanusítványok ikonjára kattintva felugrik egy jobb oldali menü, ott elindítjuk a **Tanusítványkérelmet**. A kitöltés után kiválasztjuk a kódolás típusát és a bithosszt, majd megajuk a fájl nevét és elmentjük. Ezt feltöltve a hitelesítőszogáltatóra (CA) készítünk egy tanusítványt a megfelelő paraméterekkel, majd letöltjük és telepítjük Windows Serveren (az IIS kiszolgálói tanusítványoknál importáljuk, mint pfx file).



Tanusítványok – ACME protokoll

Az **ACME (Automated Certificate Management Environment)** egy protokoll, amelyet arra terveztek, hogy automatizálja az SSL/TLS tanúsítványok kiadásának és megújításának folyamatát.

A Let’s Encrypt honlapjáról letölthető a Documentationban a Windows / IIS-ben található WIN-ACME, vagy közvetlenül a **https://www.win-acme.com** -ról

VPN kapcsolat

A VPN (Virtual Private Network) egy technológia, amely lehetővé teszi, hogy biztonságosan csatlakozz a hálózatra, és titkosítva küldj és fogadj adatokat az interneten keresztül. Egy privát, titkosított csatornát hoz létre egy nyilvános vagy megosztott hálózaton belül.

Lehetővé teszi, hogy más országokban elérhető tartalmak hozzáférését, amelyeket földrajzi korlátozásokkal védtek - hozzáférés külföldi streaming szolgáltatásokhoz vagy weboldalakhoz

A nyilvános Wi-Fi hálózatokat használói a VPN segítségével megvédhetik az adataikat a lehetséges veszélyektől.

A VPN elrejti az IP címet, így a tevékenység anonimebbé válik. Az internetszolgáltató és más harmadik felek kevésbé tudják nyomon követni a tevékenységet.

Távelérés (Remote Access) szerver telepítése

VPN-kapcsolatot a Windows Serveren a Távelérésben (**Remote Access**) található VPN komponens biztosítja

A Kiszolgálókezelőben (Server Manager) hozzáadjuk a Szerepkörök és szolgáltatásoknál a Remote Access-t, majd bepipáljuk a telepítés során a **DirectAccess and VPN (RAS)** és a **Routing** opciót.

Konfigurálás előtt meg kell nyintunk a **Tűzfal**on (Windows Defender Firewall) a megfelelő portokat a speciális beállításoknál. A **bejövő szabályoknál engedélyezni kell** a Secure Socket Tunneling Protocol-t (**SSTP-In**).

Visszakapcsolva a VPN telepítése utáni beállító-varázslójára (Server Manager-ben zászló), kiválasztjuk a harmadik “CSAK A VPN telepítése opciót” (Deploy VPN only). Nem pipáljuk be a DirectAccest (A DirectAccess lehetővé teszi, hogy a felhasználók automatikusan csatlakozzanak a hálózathoz anélkül, hogy manuálisan be kellene kapcsolni a VPN-t).

Távelérés (Remote Access) konfigurálása szerver - 1.rész

Az **útválasztó és távelérés** (keresősor: **rras** - routing and remote access) **konzol**on konfiguráljuk a szerverünket úgy, hogy jobb kiválasztjuk, majd jobb egérgombbal előhívjuk a telepítővarázslót. Kiválasztjuk az egyéni konfigurációt (custom) – itt bepipáljuk a VPN (virtuális magánhálózat), és a NAT-ot (hálózati címfordítás). Végezetül indítsuk el a szolgáltatást!

A szerverünk-re kattintva jobb gombbal a tulajdonságainál az első táblán ellenőrizzük, hogy az IP4 útválasztó LAN módban, ill. az IP4 távelérésen van pipa, majd magán az IP4 fülön adjuk hozzá az IP-cím tartományt

Az IP4-et szétbontva a hálózati címfordítás(NAT)-nál hozzáadunk egy új Ethernet-et. Itt nyilvánosra állítjuk és bepipáljuk a hálózati címfordítást (NAT)-ot. Alkalmazzuk majd OK.

Ennek az új Ethernet kapcsolatnak beállítjuk a szolgáltatásait és a portjait úgy, hogy a privát címet home-ra állítjuk (127.0.0.1). A következő szolgáltatásokról van szó: 2db IP-biztonság (kulcscsere ill. NAT), Távoli asztal, HTTPS, HTTP, VPN átjárók (PPTP, L2TP/IPSec – Layer2 Tuneling Protocol).

Újraindítjuk a VPN szerverünket (jobb gomb, összes feladat, újraindítás),
vagy Powershell: **Restart-Service rras**

Távelérés (Remote Access) konfigurálása szerver - 2.rész

A címtárszolgáltató felhasználók és számítógépeinél (AD) létrehozunk egy “VPN felhasználók” nevű szervezeti egységet, majd ebbe egy VPN Teszt felhasználót (**vpnteszt@rozsa.bimbo**)

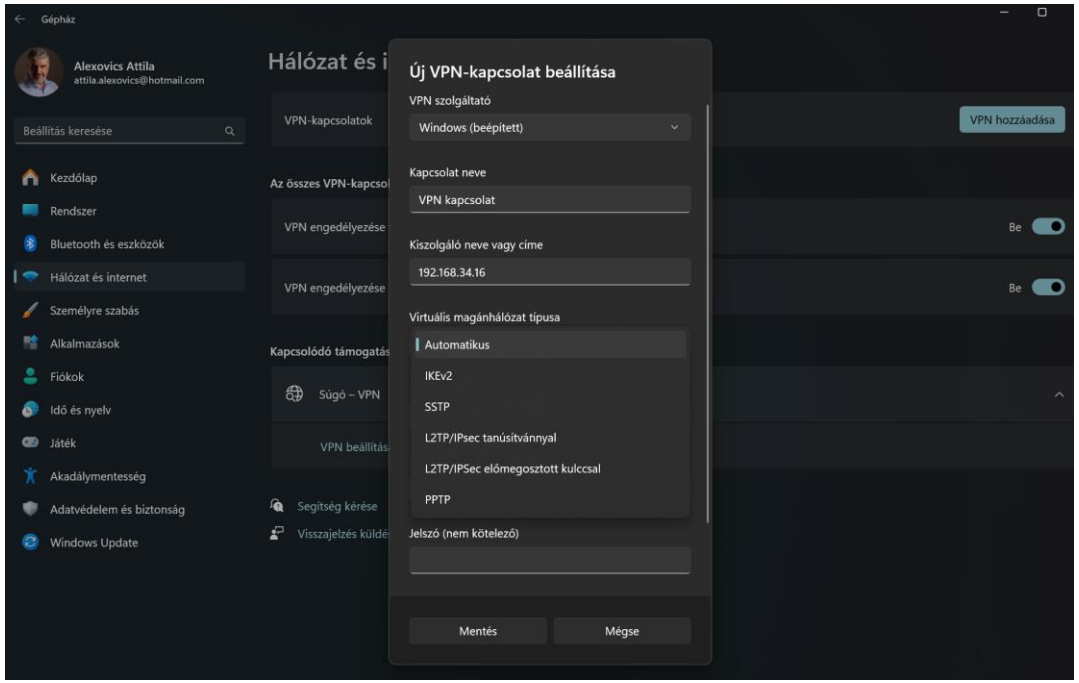
A felhasználó tulajdonságainál a “következő tagja…”-nál hozzáadjuk a Remote Desktop Users-t (hozzáadás, speciálist kinyitva, majd a keresés most opció). Alkalmazzuk.

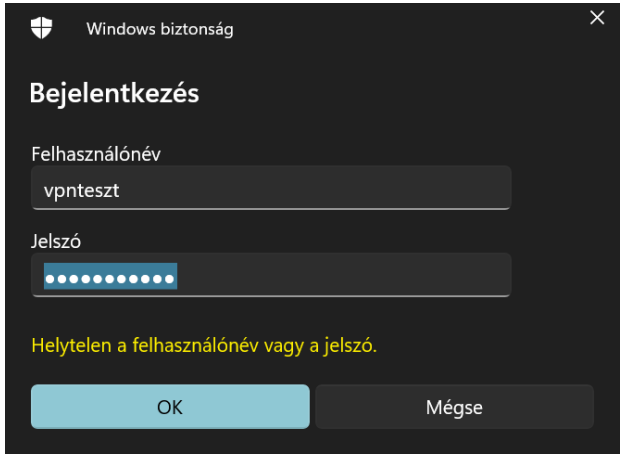
Ugyanitt a behívás fülön engedélyezzük a hálózati hozzáférést. Alkalmazzuk, majd OK.

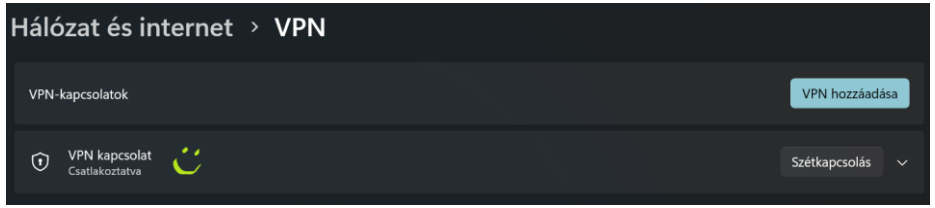
A kliens gépen beállítjuk az internetbeállításoknál a VPN-t Windows Beépitett, Automatic opcióval (de lehet szinte bármelyik biztonságos csatlakozással):

Távelérés (Remote Access) konfigurálása a kliensen

A kliens gépen beállítjuk az internetbeállításoknál a VPN-t Windows Beépitett, Automatic opcióval (de lehet szinte bármelyik biztonságos csatlakozással):

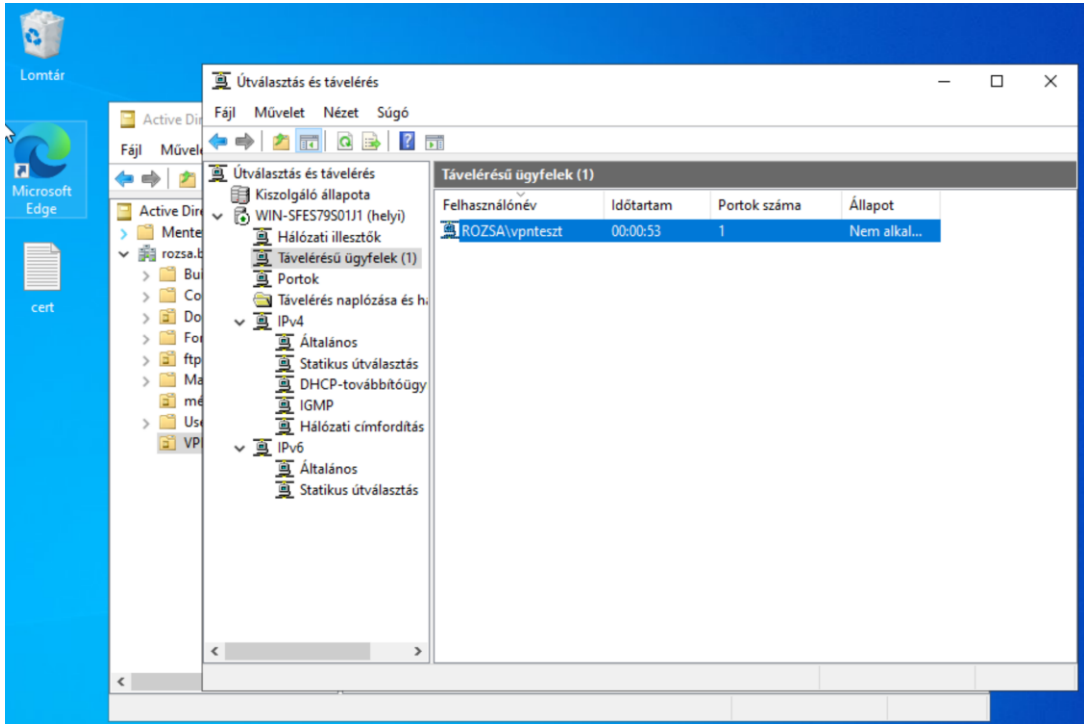






Távelérés (Remote Access) ellenőrzése

A kapcsolódó kliens gépet a Windows Server-en az **Útválasztás és Távelérés** konzolján úgy ellenőrizhetjük, hogy a szerverünket megnyitjuk, és megnézzük a **Távelérésű ügyfelek**-nél, hogy jelen van-e a csatlakozott gép



Szerverek távoli menedzselése (RSAT)

Ha Windows Servert távolról akarjuk irányítani pl. egy Windows 11 gépről, akkor ehhez fel kell telepíteni az RSAT-ot (Remote Desktop Administrative Tools)-t a következőképp:

A Windows 11 Pro-n a Rendszer → Választható funkciók → Funckiók megtekintésénél kiválasztjuk az **RSAT: Active Directory Services és a Lightweight Directory szolgáltatás eszközei** –t, ami feltelepül. Elvileg csak a Pro verzió tudja, és átkerült az Alkalmazásoktól a Rendszer menüpontba

A Windows 11 Pro-n megyitjuk a Kiszolgálókezelőt, majd az eszközöknél csatlakozunk az **Active Directory Felhasználók és számítógépek** konzoljához, amelyen látjuk a szerverünket. Megnyitva távolról irányíthatjuk azt, felvehetünk felhasználókat, lekérdezhetünk stb. **Ha nincs ott a szerver, akkor a Kiszolgálókezelőben hozzá kell adni.**

Szerverek távoli menedzselése (RSAT) tutorial

Figyelem, a legújabb Windows-on az RSAT telepítése átkerült az Alkalmazásoktól a Rendszer menüpontba!

Windows Server Backup (WSB)

Lehetővé teszi a Windows Server adatok és állapotának **biztonsági mentését és visszaállítását**.

Telepítése a Kiszolgálókezelőben (Server Manager) található Kezelés – Szerepkörök, első telepítési ablakot átugorva (nem pipálunk semmit), a következő **Szolgáltatások** ablaknál pipáljuk be a **Windows Server Backup** szolgáltatást.

Indítása a Kiszolgálókezelő Eszközeinél a Windows Server Biztonsági Másolat, vagy a keresősorban **wbadmin.msc**

A WSB Funkciói:

- **Teljes szervermentés** - Az összes adat, alkalmazás és rendszerállapot biztonsági mentése
- **Kiválasztott kötetek és fájlok**
- **Rendszerállapot mentés**
- **“Bare Metal” visszaállítás**
- **Automatikus ütemezés**

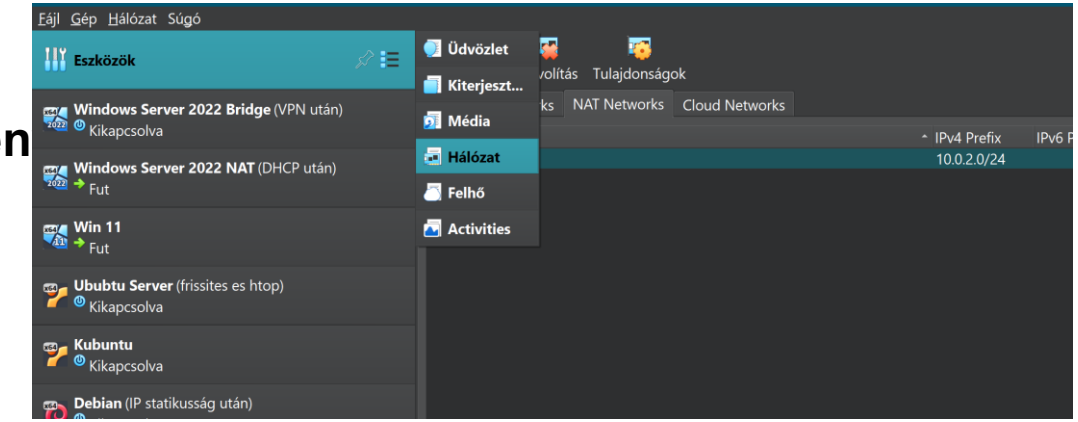
Virtuális gépek párhuzamos futtatása és kapcsolata VirtualBox alatt

Adott a feladat, hogy VirtualBox alatt futó **Windows Serverhez kapcsolódjunk** az ugyancsak ezen virtuális környezet alatt futó **Windows 11** klienssel a célból, hogy szimuláljuk egy majdani valós hálózatot, topológiát stb. Ez akkor fordul elő, amikor valami oknál fogva nem elég a külső SSH konzol (pl. Putty).

VirtualBox Bridge üzemmódjában “csak” tartományba kell léptetni a klienst (esetünkben rozsa.bimbo, és a Windows Server AD-jében létrehozott entitásos szabályok szerint). Ilyen esetekben a **Belső hálózat** üzemmódot használjuk. NAT-ban viszont alapból két külön hálózatnak tekinti a két virtuális gépet a VirtualBox, és a portok forwardja ki és a be a gazdagépre sem oldja meg igazán a helyzetet. Megoldás ilyenkor, hogy mindkét gépet ún. **NAT Network** módban indítjuk el. Mivel alapból a VirtualBox nem kínálja fel a lehetőséget, egy rejtett opciónál kell bekapcsolnunk és nevet adni neki.

A Belső hálózat előnye (nagyvállalat):
- Szervezeten belüli teljesítmény, irányítás
- Alapos tűzfalkonfigurációt és védelmet igén

A NAT Network (tesztkörnyezet) előnye:
- BIZTONSÁG a külső fenyegetések ellen,
- ANONIMITÁS

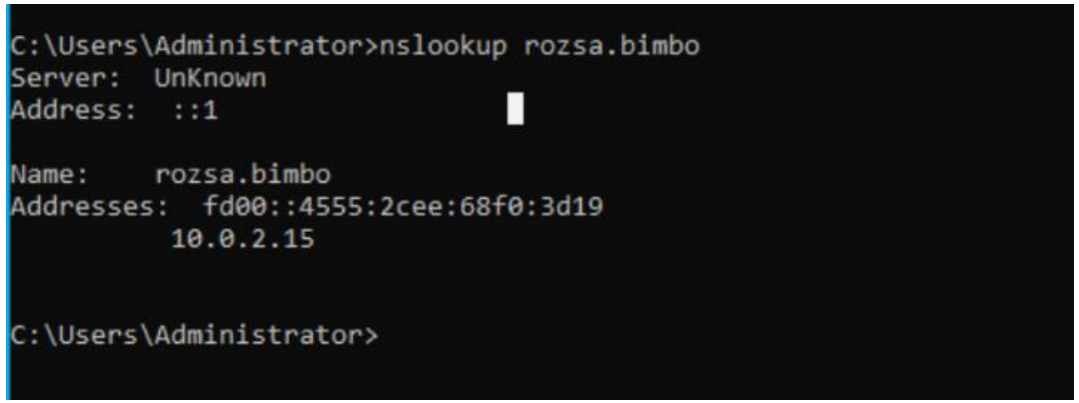


Windows Server és Win11 kapcsolata VirtualBox alatt 1.

0., Előfeltétel: Bizonyosodjunk meg arról, hogy a virtuális gépeink képesek-e fele annyi memóriával ill. processzorral működni, vagy a gazdagépünk képes-e dupla erőforrás kihelyezésére !!

1., A **Windows 11** Home edition-nel, ahol privát Microsoftos fiókot választ valaki telepítéskor nem engedi állítólag átrakni vállalati/szervezeti fiókra, csak a **Pro verziót**

2., A **Windows Server**t tartományvezérlővé előléptetjük, majd **megcímezzük az interfészünket** a hálózatunkra, és DNS managerben a továbbítóknál az átjáró (10.0.2.2) helyett **10.0.2.3**-at adunk neki, amit nem enged megváltoztatni - kényszerített VirtualBox NAT DNS szerver. Ettől függetlenül a DNS szerverünk az interfészen megadott **10.0.2.15** lesz. nslookup próba ez legyen:



3., a Win11 is alapból ezt a 10.0.2.15 -tel erőszakoskodik a hálózati interfészen, hogy ne legyen ütközés ott írjuk át a saját IP-jét a **Win11-nek 10.0.2.16**-ra

Windows Server és Win11 kapcsolata VirtualBox alatt 2.

4., **Engedélyezzük a szerver és a win11 tűzfalán is az 53-as port**ot bemenőre és kimenőre (szabályok felvétele, bemenő, port 53, majd kimenő szabályként ugyanez…)

5., Megpingetjük Windows Server-ről a Win11 klinest (**ping 10.0.2.16**) – mennie kell

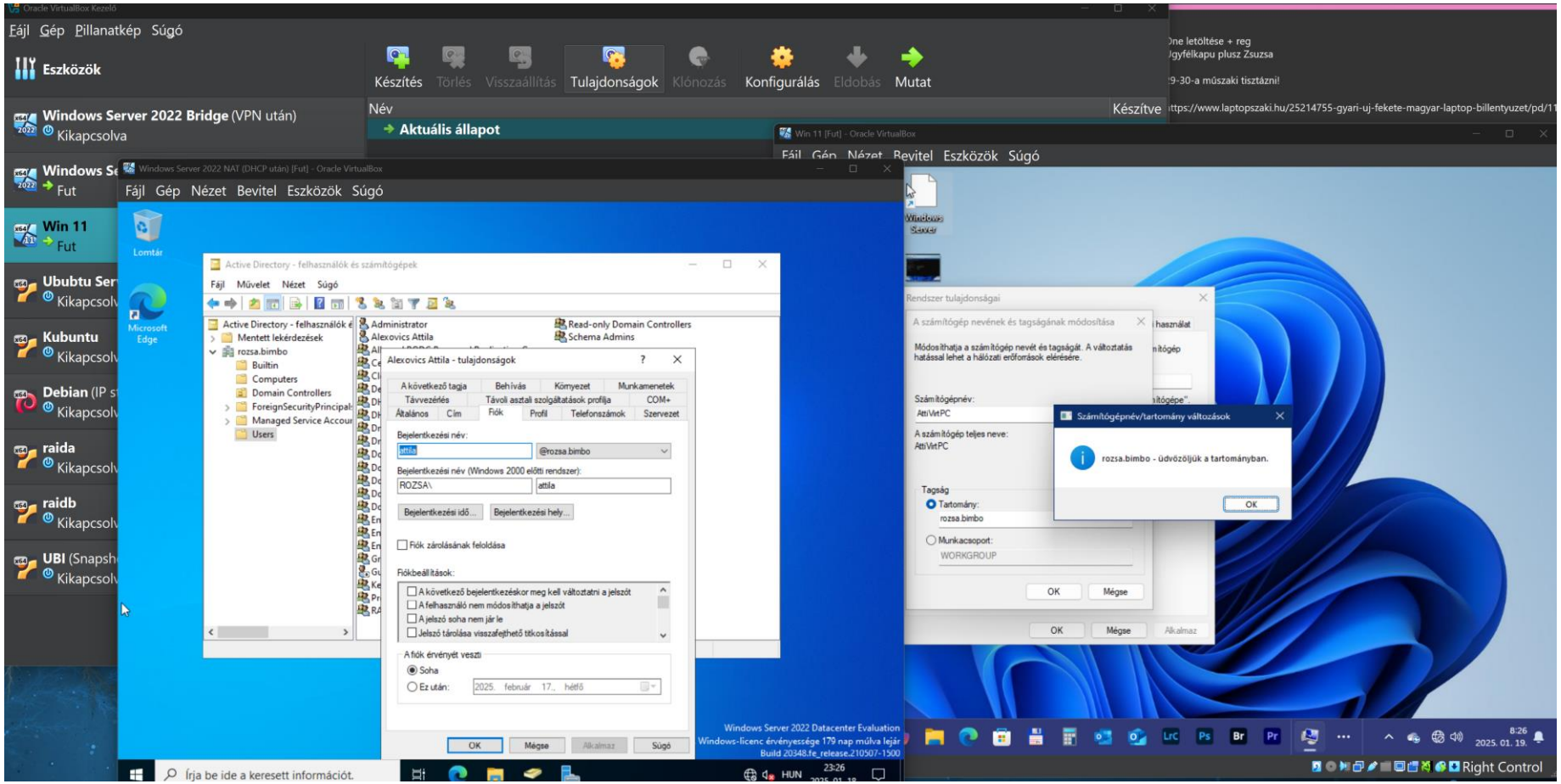
6., **Engedélyezzük a szerver tűzfalán at ICMP v4 protokollt** a bejövő szabályoknál (mert nem fogad pinget), tehát bejövő szabályok -> Új szabály -> Egyéni -> Minden program -> Protokoll tipusnál meg válaszd ki az ICMP v4-et., majd engedélyezd, OK a végén. Ez által mennie kell a kliens Win11 oldalról is a ping a ping a szerver felé (ping 10. 0. 2. 15) – tehát **kétirányú a kommunikáció**

7. A szerveren az **Active Directoryba felveszünk egy felhasználót**. Jelszónál pipák nélkül. Ha nem engedi, akkor csak csináljuk meg, majd később a felhasználó tulajdonságainál szedjük ki a jelszóra vonatkozó pipákat.

10. **Win 11-ben** a Rendszer tulajdonságai -> Számitógép nevének és tagságának módosításánál a ""**tartomány**-ra kell kattintani, majd ott beirni a tartományt (esetemben: rozsa.bimbo)

11. Miután csatlakozott a kliens Win11, akkor a szerver **Active Directory-jában meg kell jelennie a kliens gép nevének** egy refresh után

Windows Server és Win11 kapcsolata VirtualBox alatt 3.



Windows Server és Win11 kapcsolata VirtualBox alatt 4.