

BProf-Témalabor

AD_DS Üzemeltetés

(DOKUMENTÁCIÓ)

0. Előkészületek

A rendszerek feltelepítéséhez **Oracle VM VirtualBox** környezetét használtam fel. **Windows 2022 Server ENG + Major updates ISO** lemezképet használtam fel a környezetek feltelepítéséhez!

VM Specifikáció:

- 2vCPU
- 4GB RAM
- 80GB meghajtó
- Belső hálózati csatoló (INTEL PRO/1000 MT Szerver)
- 128MB VRAM

1. Pilot rendszer telepítése

1.1. MS Windows 2022 AD_DS szerver telepítése

A szerver feltelepítésekor, **felcsatoltam a lemezket a VM gépre**. VM gépre csatlakoztatva, majd a VM gépet elindítva elindul a telepítő! **A lemezkep csak az angol nyelvet tartalmazza**, így igazából teljesen mindegy, hogy az első lépésekben mit is csinálunk.

- „Next” gombot elég megnyomni, majd...
- „Install now” gombra elindítom a telepítőt...

Licenc kulcs beírását, a jelen helyzetben nem tudjuk megtenni.
(Hiszen nem rendelkezünk licenc kulccsal)

- „I don't have a product key” gombra nyomunk...

A feltelepítendő verzió kiválasztásakor, ahogyan a feladat kérte, számunkra a „**Desktop Experience**” lesz a fontos. És azon belül is a „**Standard**” verzió.

→ „**Windows Server 2022 Standard Evaluation (Desktop Experience) x64**” lehetőséget kiválasztjuk, majd a „**Next**” gombra kattintunk.

Az ekkor feljövő „**Terms of Services**” részt elfogadjuk, természetesen előtte, mindenki mindenki előtt elolvassuk.

A következő alkalommal „**Custom**” telepítést kellene választanunk, hiszen még a meghajtón nincsen semmiféle rendszer. A VM által létrehozott 80GB-s merevlemez kiválasztom, majd a „**Next**” gombra elindul a teljes telepítési folyamat. Innentől kezdve csak idő kérdése, s felkerül a rendszer.

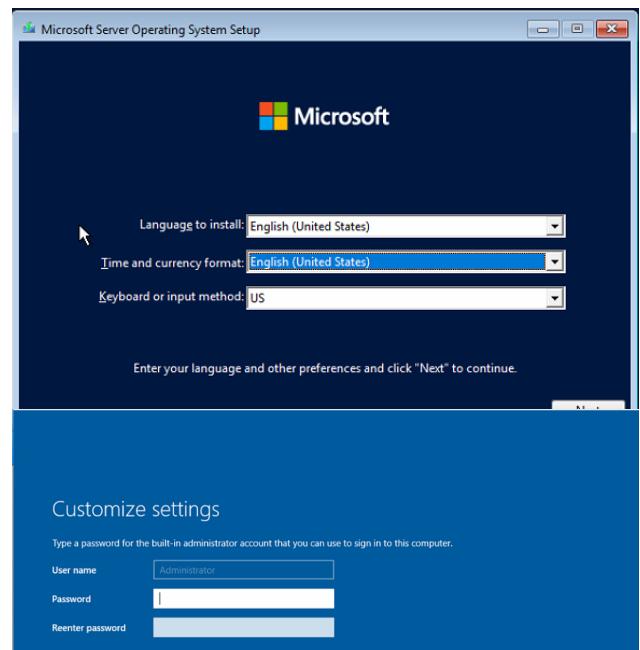
Ha minden jól megy, a Windows Server majd magától szépen újraindul és néhány utólagos konfigurálás után beállíthatjuk a szervert.

Felhasználót, majd a későbbiekben állítjuk. Most egyenlőre elég a jelszót megadni. Majd ezután nyomhatunk a „**Finish**” gombra.

Ekkor már megkapjuk a kezünkbe az irányítást! **CTRL+ALT+DEL** kombinációval elérhetjük a bejelentkezési panelt. Be is jelentkezünk.

Bejelentkezéskor még lefut a „**Personalized Settings**”-s kis ablakcska, ami szépen a fiókot beállítja.

Majd ezek után, **megnyílik szépen a Service Manager alkalmazás a gépen**. Fel is raktam a rendszert!



1.2. MS Windows 2022 MEMBERS szerver telepítése

A telepítés módszere teljesen megegyezik azzal, mint amit fentebb leírtam. Kezdődhet a „Privát hálózat” beállítása.

1.3. Privát hálózat beállítása a 2 szerver között

Első lépésként, mindenképpen legyen leállítva minden két virtuális számítógép! Majd, miután minden két szerver leállt, utána szépen beállítjuk minden két szervernél a hálózati csatolót! Ehhez egyszerűen az alábbi lépéseket kell megtenni. (VBOX panelen)
 → Adott VM esetében „Configure” → „Network” → Majd a „Connection to” részét „Internal Network” -re állítjuk! Mindkét VM esetében „TÉMALAB” a név.

Ha ez megvan, akkor szépen elkezdjük konfigurálni minden két szervert! A lépések tehát a következők!

- minden két VM gép esetében megnyitjuk a „Control Panel”-t (Vezérlőpult)
 - „Network and Sharing Centers” megnyitása, majd „Change Adapter Settings” oldalsó menüre rákattintunk.
 - Jobb klikk a „Network” hálózati kapcsolatra, majd „Properties” gombra rákattintunk
 - „Internet Protocol Version 4” menüpontra rákattintunk majd a „Properties” gombra rákattintunk
 - DHCP opcióról manuálisra térünk át (szervereknél érdemes statikus IP címet beállítani)
 - **AD_DS SERVER**
 - IP: 192.168.7.1
 - MASK: 255.255.255.0
 - DEFAULT-GTW: 192.168.7.101 + DNS: 192.168.7.1
 - **MEMBER SERVER**
 - IP: 192.168.7.2
 - MASK: 255.255.255.0
 - DEFAULT-GTW: 192.168.7.101 + DNS: 192.168.7.1
- A két szerver Windows Firewall szabályok miatt nem érik el egymást, így „Private” Network miatt most minden két oldalt kikapcsolom! Ezt kikapcsolva minden két szerver tudni fog egymással kommunikálni!
 - minden két szerveren megnyitjuk a „Windows Defender Firewall with Advanced Security” alkalmazást.
 - „Properties” fülre rákattintunk
 - „Private Profiles” fülre kattintunk tovább
 - „Protected Network Connections” fülön kiszedjük a pipát a „Network” hálózati csatolóról.
- A két szervernek ekkor már látnia kellene egymást! Parancssorban érdemes pillantást venni még arra, hogy ténylegesen belettek-e állítva az IP címek! (ipconfig /all, de nem árt egy ipconfig /release és egy ipconfig /renew)
- Pingeljük meg minden két oldalt a szertvert.:

```
Pinging 192.168.7.1 with 32 bytes of data:
Reply from 192.168.7.1: bytes=32 time<1ms TTL=128

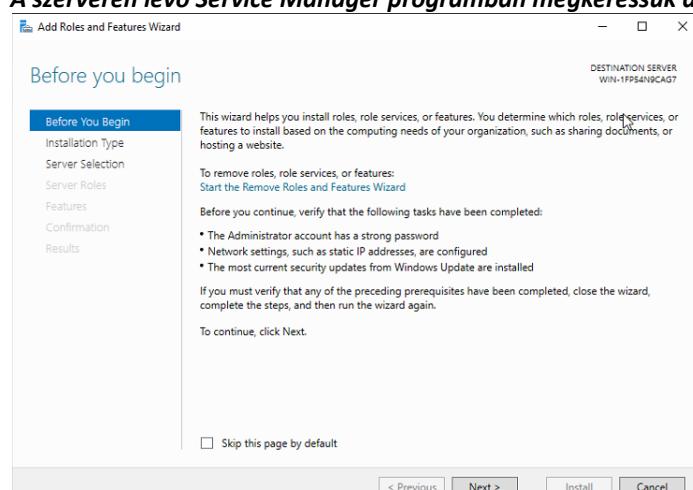
Ping statistics for 192.168.7.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
Pinging 192.168.7.2 with 32 bytes of data:
Reply from 192.168.7.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.7.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

1.4. AD_DS feltelepítése

A szerveren lévő Service Manager programban megkeressük a „Add Roles and Features” menüpontot.



Ezen az oldalon csak szól nekünk a „Wizard” bizonyos dolgokról! Mint például arról, hogy az Adminisztrátor fiókjának jelszava erősnek kell lennie. A Biztonsági frissítések telepítve vannak. És stb, stb...

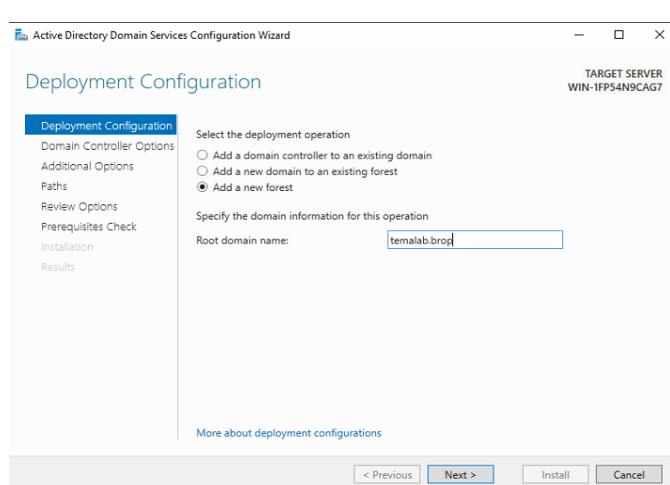
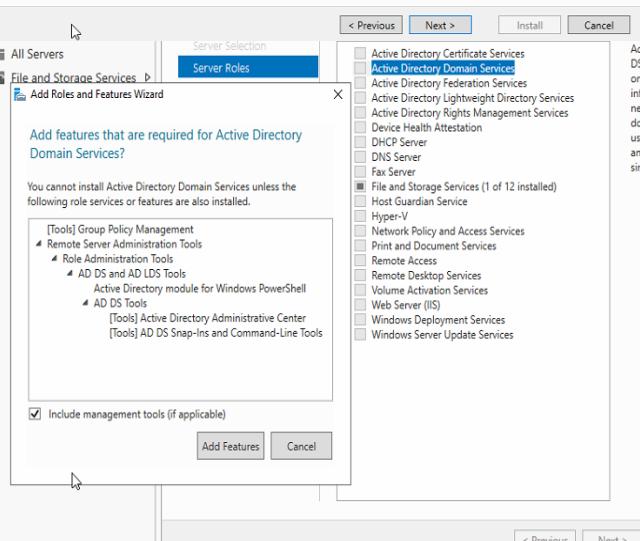
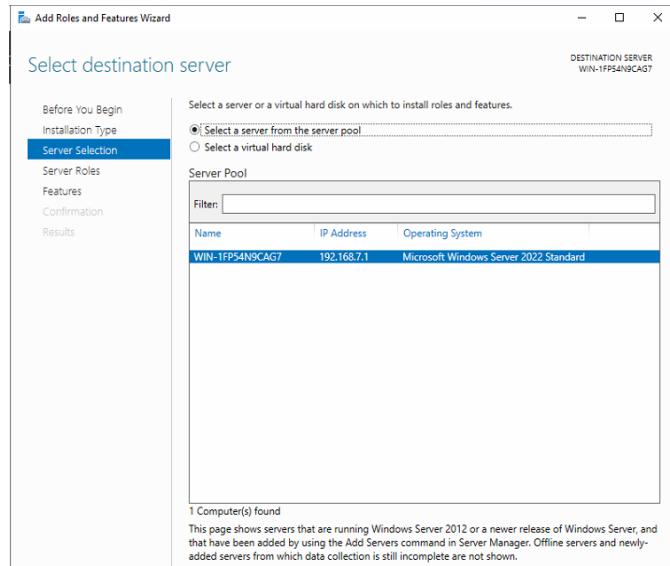
Ennél a pontnál, azért érdemes a leírtakat ellenőrizni.

Ha megvagyunk, akkor a „Next” gombra kiválaszthatjuk a telepítés típusát!

(Lehetséges itt, kikapcsolni ezt az oldalt, alapértelmezetten, ha már többet nem szeretnénk látni ezt az oldalt)

Számunkra a „Role-based or Feature-based installation” fog kelleni, hiszen szeretnénk egy új funkciót felrakni az AD_DS szerverünkre! Ezt kiválasztva, lépjünk tovább.

Ki kell választanunk most azt a szervert, ahova most ezt a funkciót felszeretnénk telepíteni.



Egyedül, akkor a „**Prerequisites Check**” rész maradt, ahol megvizsgálja a rendszert, hogy minden átmentünk-e. Ha ezzel megvagyunk az „**Install**” gombra nyomva, elkezdődik a telepítés. Majd a szerver újraindul.

Jelen helyzetben, most csak a saját szerverünk van itt.
(A másik szerver azért nincsen itt, mert nincsen hozzáadva ehhez a szerverhez, mint aki menedzselni tudná)

Tehát, ebben az esetben itt most csak elegendő a „**Next**” gombra kattintani. Ha több szerverünk lenne, akkor kellene jobban figyelembe venni a kilistázott szervereket, hogy biztosan olyan szerverre legyen feltelepítve a feltelepítendő funkció, ahova tényleg szeretnénk felrakni a kívánt funkciót.
(Érdekességeképpen a Virtual Disk-t is lehet választani)
Itt kiválasztjuk szépen az „**Active Directory Domain Services**” pontot.

A pont kiválasztásakor felszólít minket a rendszer, hogy ehhez a funkcióhoz szeretne még további funkciókat/szolgáltatásokat felrakni, hiszen azok szükségesek lennének az AD_DS szolgáltatáshoz!

Jelen esetben elég csak az „**Add Features**” gombra kattintanunk!

A további lépésekben megtekinthetjük, milyen Szolgáltatásokat rakhattunk fel a szerverre, mint például a **Group Policy**-t és társait. (**előbbi, felrakja mert kell az AD_DS-hez**) És az AD_DS fülnél pedig információt kapunk a szolgáltatásról, valamint arról, hogy milyen szempontokat lenne még érdemes figyelembe vennünk! Ha végeztünk mindenkel a „**Confirmation**” fülnél akkor nyomjunk az „**Install**” gombra! Ezzel elindítjuk a szolgáltatás telepítését.

A telepítés végefelé az AD_DS feltelepítésekor szól a szerver, hogy beavatkozásra van szükség! A Service Manager alkalmazásnál a „**zászló**” ikonnál megjelenik egy értesítés! Ezt megnyitva az AD_DS-nek szüksége van arra, hogy ezt a szervert DC-nek állítsuk be! Ehhez kattintsunk a „**Promote this server to Domain Controller**” lehetőségre!

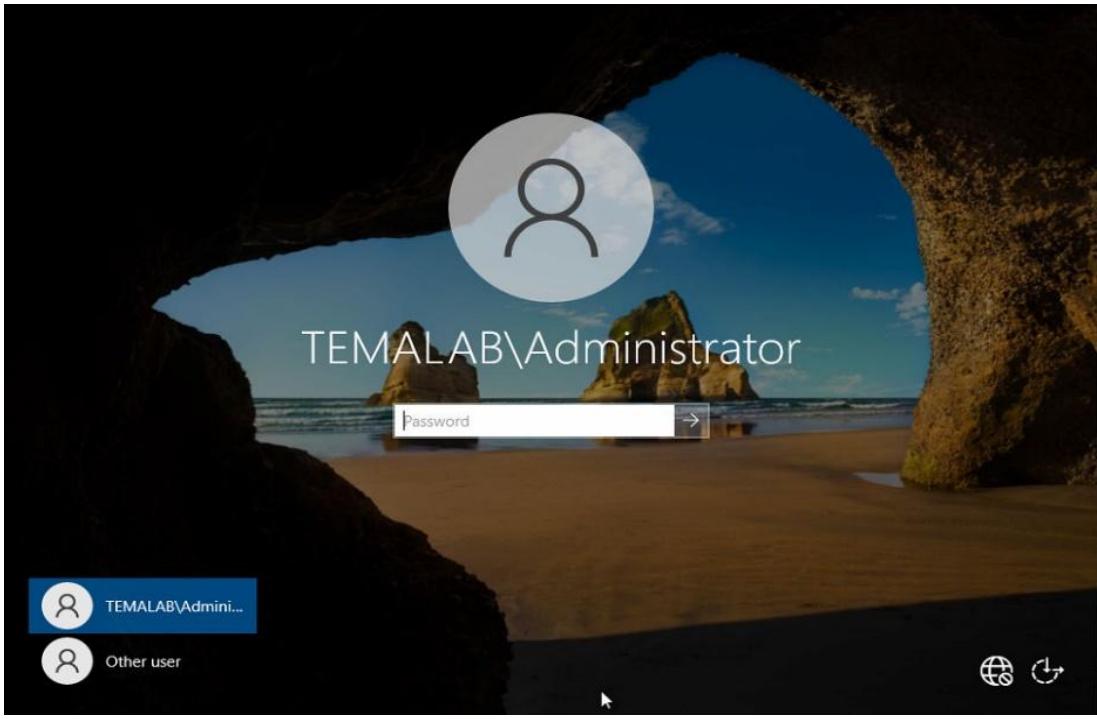
Mivel nincsen se, már létező „**Forest**”-ünk, valamint nem is létezik „**Domain**”-ünk, így nekünk az „**Add a new forest**” opción fog kelleni!

Root domain name → temalab.bprof (**én, ezt elírtam... majd egy következő szakaszban, nekiugrok a javításnak**)

Domain Controller Option résznél a „**Functional level**” részét nem kell állítanunk, mert minden szerverünk a 2016-hoz képest újabb lesz! Csak a DSRM jelszót kell beállítani, majd tovább lépnünk.

„**Additional Options**” résznél a **NETBIOS** nevet lehet beállítani. Én alapértelmezés szerint hagytam (TEMALAB) „**Paths**” résznél az alapértelmezett útvonalakat meghagytam. Ehhez nem kellett nyúlni.

Ami talán érdekes lehet, az a „**Review Options**” rész lehet, hiszen itt meg tudjuk nézni az elkészült „**Scriptet**”. Ezt a PowerShell scriptet, akár mi is ki tudjuk adni a programban!



Ha minden jót csináltunk, ez a képernyő fog fogadni!

Ha ezzel megvagyunk, bejelentkezve a szerverre, mindennek problémamentesnek kellene lennie.

Valamint a Dashboard bal oldalán megjelenik az AD_DS menüpont is!

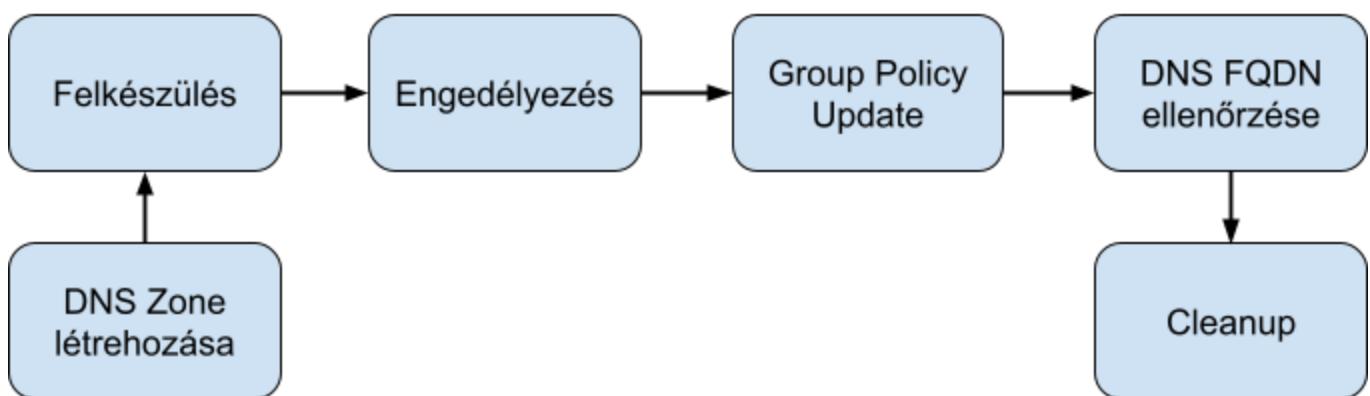
Akkor, most itt lenne az idő arra, hogy beléptessük a másik gépet erre a tartományra!

Ehhez, nekünk a másik szerver fog kelleni.

1.5. AD_DS szerver Domain Name elírásának javítása

Sajnálatos módon, hibát vétettem a Domain név beírásakor. Ezt pedig valahogy orvosolni kellene... Sok esetben ez nem jelent gondot. De egy gép tartományba léptetésekor sok fejfájást tud okozni az, amikor a gép azért nem tud felcsatlakozni, mert véletlenül elgépelték azt a szerver beállításakor..... Kezdjük is el a probléma javítását! Min is kellene végig mennünk?

Domain átnevezésének lépései



1.5.1. DNS Zone létrehozása

Ehhez nyissuk meg a DNS alkalmazást, majd adjunk hozzá a szerverhez egy új DNS Zone-t!

- A zóna típusa "**Primary**" (ehhez a szerverhez szeretnénk hozzáadni)
- "**To all DNS Servers running on domain controllers in this subdomain: temalab.brop**" kiválasztása
- "**Forward Lookup Zone**" lehetőség választása, hiszen DNS nevet szeretnénk IP-re alakítani
- "**Zone name: temalab.bprof**" legyen
- Dynamic update maradjon alapértelmezett (AD miatt)

FINISH gombra kattintva készen van a DNS Zone-nk amit használni fogunk!

1.5.2. Felkészülés fázis

Ebben a fázisban felkészítjük a szervert a Domain átnevezéséhez! Ehhez meg kell adnunk az alábbi parancsokat! Nyissunk meg egy CMD-t!

Generáljuk le a DomainList.xml file-t! Ebben megtalálható maga a Forest struktúrája. Majd szerkessük a file-t és amit elírtunk, azt írjuk át!

rendom /list

Ezzel a parancssal megnézhetjük a beállított fájl új értékét. Itt meggyőződhetünk arról, hogy most tényleg jól írtuk le a Domain nevét!

rendom /showforest

Ha minden jól ment, akkor töltök fel a változtatásokat! Ez megfagyaszta a későbbi változtatásokat az AD-n!

rendom /upload

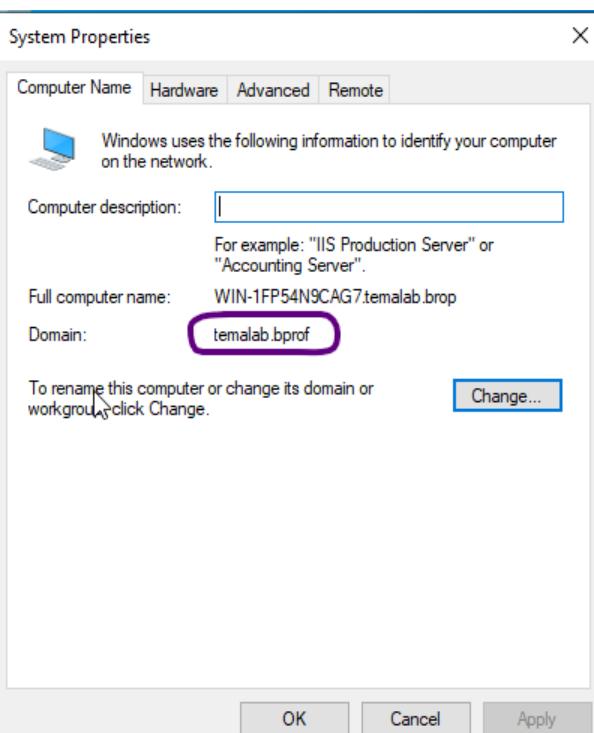
A most következő parancs felkeresi az összes DC-t és szól a változásokról! minden DC-t előkészítjük a folyamathoz

rendom /prepare

1.5.3. Engedélyezés fázis

Ebben a fázisban az összes Domain Controllernek megmondjuk, hogy vigyék véghez ezeket a változtatásokat! A következő parancsot adjuk ki a CMD-ben!

rendom /execute



Ekkor minden DC szerveren végbemegy a változás, majd szónak egy felugró ablakban, hogy a rendszer újra fog indulni! Ha minden változtatás végbement ezt az ablakot kellene látnunk.

Mint jól látható a "**Full computer name**" és társai még nincsenek rendesen átnevezve! A FCN az majd a végző fázisban fog végbemenni!

Jelen helyzetben most az NT4-t és a GP-t kellene helyrerakni! (NT4 = NETBIOS, GP = GROUP POLICY / FQDN nevet)

```
C:\Users\Administrator>rendom /execute
Waiting for DCs to reply.
Waiting for DCs to reply.
The script was executed successfully on WIN-1FP54N9CAG7.temalab.brop
1 server contacted, 0 servers returned Errors

The operation completed successfully.

C:\Users\Administrator>
```

1.5.4. Group Policy Update fázis

A mostani fázisban (ha lennének kliensek) a kliensekre vonatkozóan a változtatások tényleges lefutása után 2x kellene Őket újraindítani!

Most azt fogjuk megoldani, hogy a GP-n is helyesen jelenjen meg a tényleges domain nevünk! Ehhez vegyük elő újra a CMD-t!

A domain, az egy dolog hogy megváltozott... De az NT4 és a DNS név az nem változott meg! Kezdjük el, ezeknek a beállítását! (Az alsó parancs lefuttatása nem fontos, mert a NETBIOS name az jó!)

```
gpfixup /olddns:temalab.brop /newdns:temalab.bprof
gpfixup /oldnb:TEMALAB /newnb:TEMALAB
```

1.5.5. DNS FQDN ellenőrzése

Mi is ez pontosan? Ez a **"Full Qualified Domain Name"** ami lényegében az-az azonosító, amivel azonosítjuk a gépünket abban a Domain-ben! Most ezt is állítsuk be, hogy helyesen jelenjen meg!

Előtte, kérjük le a jelenlegi FQDN nevünket! (Ez feloldja a gépnek az FQDN nevét)

```
ping -a <ip>
```

Majd az FQDN nevet kimásolva, már le is futtathatjuk a parancsot!

```
netdom computername WIN-XXXX.temalab.brop /add:WIN-XXXX.temalab.bprof
netdom computername WIN-XXXX.temalab.brop /makeprimary:WIN-XXXX.temalab.bprof
```

Ezután a parancssor szépen visszaír, hogy a változtatások érvényesítéséhez, újra kell indítani az OS-t! Ezt tegyük is meg!

1.5.6. Cleanup fázis

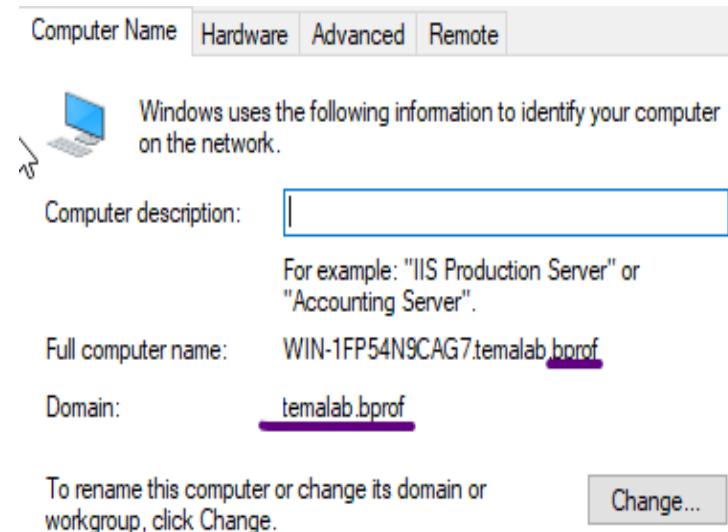
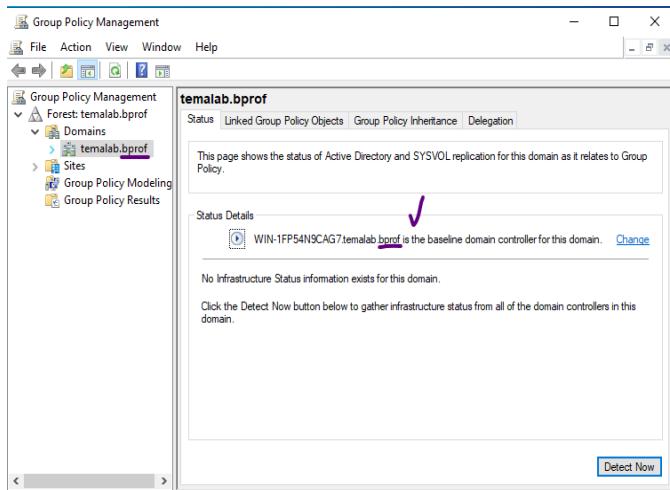
Mint minden módosítás után, el kell dobnunk a régi Domain referenciait! Ehhez megint nyissunk meg egy CMD-t! Valamint az upload fázist, le kell zárnunk!

Jöjjön, egy kis cleanup!

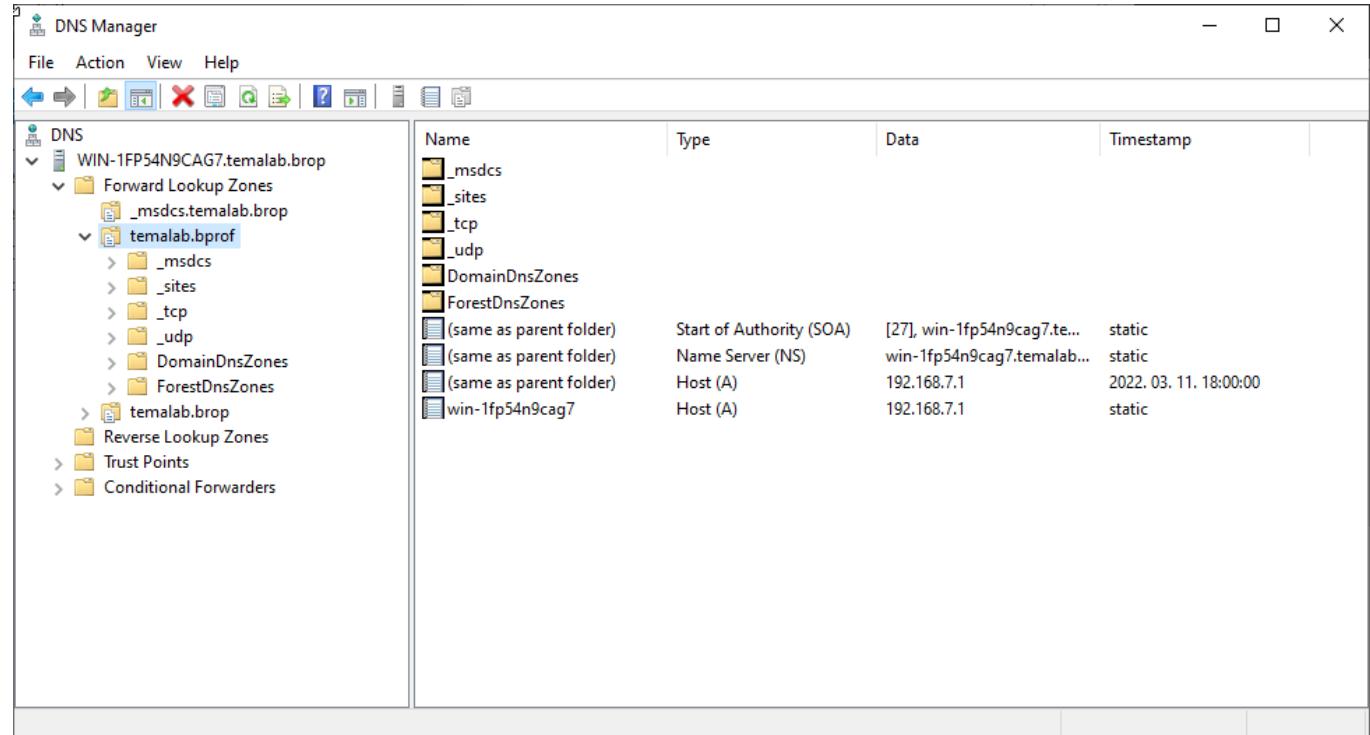
```
rendom /cleanup
```

Majd vegyük le a lezárást a feltöltésről!

```
rendom /end
```

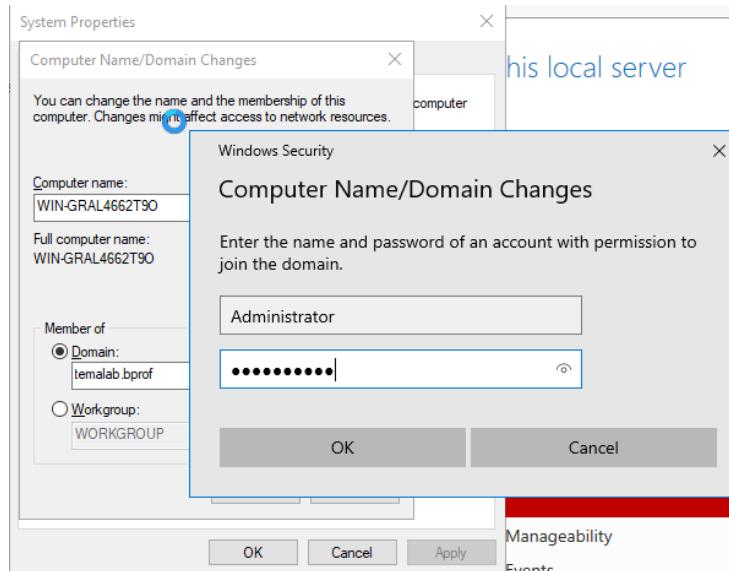


Ha minden jól ment, akkor a DNS alatt már látnunk kellene szépen minden!



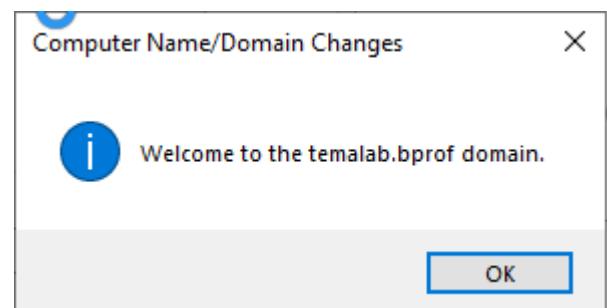
1.6. MEMBERS szerver tartományba léptetése

Nyissuk meg a MEMBERS szerveren a System alkalmazást. Megnyitásakor menjünk az “*Advanced System Settings*” menüpontra majd a “*Computer Name*” fülönél, nyomunk a “*Change*” gombra. A domain lehetőséget választva, írjuk be a “*temalab.bprof*” domain nevét a mezőbe. Miután ezt megtettük a megjelenő ablakban adjuk meg a fiók nevét és jelszavát!



Ha az adatok megegyeznek, akkor sikeresen fel tudunk lépni a megadott tartományba!

Újraindítva a gépet, bejelentkezve már láthatjuk azt, hogy a tartományban van a gépünk! (**másik szervernél a DNS alkalmazásban már láthatóvá válik**)
De AD_UC alatt láthatónak kell lennie a szervernek.



tcp	Start of Authority (SOA)	[28], win-1fp54n9cag7.te...	static
udp	Name Server (NS)	win-1fp54n9cag7.temalab...	static
DomainDnsZones	Host (A)	192.168.7.1	2022. 03. 11. 18:00:00
ForestDnsZones	Host (A)	192.168.7.1	static
(same as parent folder)	Host (A)	192.168.7.2	2022. 03. 11. 19:00:00
(same as parent folder)	Host (A)	192.168.7.2	2022. 03. 11. 19:00:00
win-1fp54n9cag7	Host (A)	192.168.7.2	2022. 03. 11. 19:00:00
WIN-GRAL4662T90			

1.7. ADDS menedzsment eszközök telepítése MEMBERS szerverre

Ahhoz, hogy a DCdiag Utility programot lefutathassuk, szükségünk lesz az azt tartalmazó "Feature"-ra. Erre két lehetőségünk van. Az első lehetőség, hogy felrakjuk az AD_DS-t erre a szerverre is! De ez nem lenne jó ötlet! Helyette az RSAT szolgáltatást fogom felrakni! (**Remote Server Administration Tools**) ami már egy FEATURE. Az AD_DS az egy ROLE.



Igy az "Add Roles and Features Wizard" programban a ROLES résznél nem kell kiválasztanunk semmit sem! Ennél a résznél viszont az alábbi "feature"-t fel kell tennünk! Az AD DS and AD LDS Tools az tartalmazza a DCdiag Utility-t!

1.8. DCdiag Utility és Összegzés

Gépet újraindítva, bejelentkeztem a tartományi fiókba (Administrator), majd a PowerShellben a "**dcdiag /s:temalabor.bprof**" parancsot lefuttatva kapunk egy állapotot, hogy működik-e a dolog.

```

language support are loaded
PS C:\Users\Administrator.TEMALAB> dcdiag /s:temalabor.bprof

Directory Server Diagnosis

Performing initial setup:
 * Identified AD Forest.
 Done gathering initial info.

Doing initial required tests

Testing server: Default-First-Site-Name\WIN-1FP54N9CAG7
Starting test: Connectivity
..... WIN-1FP54N9CAG7 passed test Connectivity

Doing primary tests

Testing server: Default-First-Site-Name\WIN-1FP54N9CAG7
Starting test: Advertising
..... WIN-1FP54N9CAG7 passed test Advertising
Starting test: FrsEvent
..... WIN-1FP54N9CAG7 passed test FrsEvent
Starting test: DFSREvent
There are warning or error events within the last 24 hours after the SYSVOL has been shared. Failing SYSVOL
replication problems may cause Group Policy problems.
..... WIN-1FP54N9CAG7 failed test DFSREvent
Starting test: SysVolCheck
..... WIN-1FP54N9CAG7 passed test SysVolCheck
Starting test: KccEvent
..... WIN-1FP54N9CAG7 passed test KccEvent

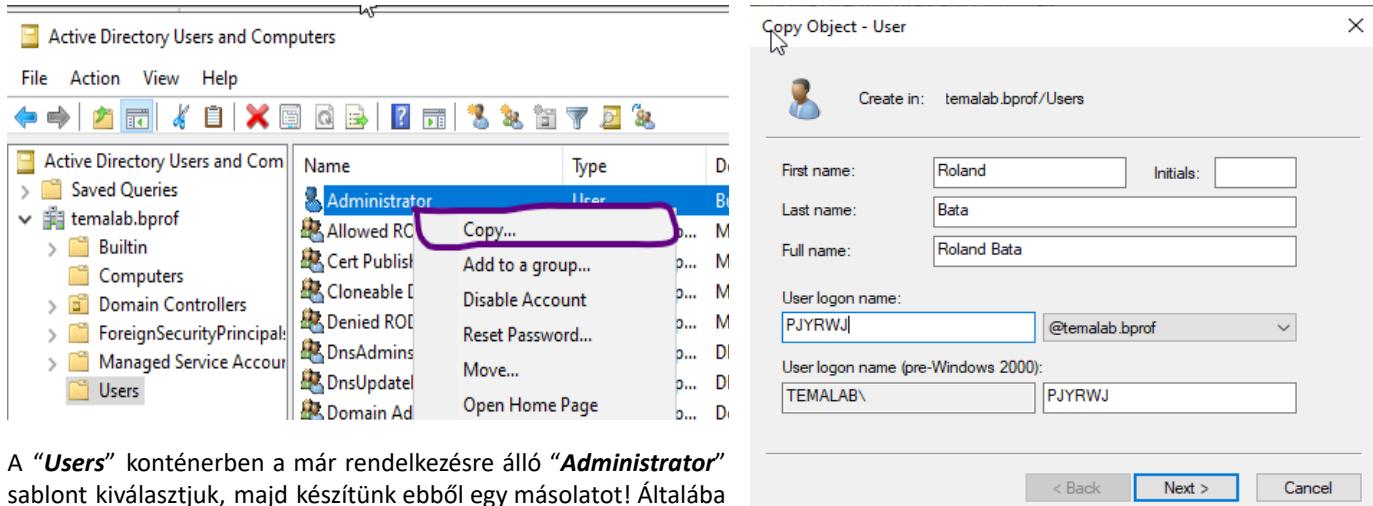
```

2.Címtár objektumok létrehozása

2.1. Saját tartományi rendszergazdai fiók létrehozása

Ebben a fejezetben egy tartományi rendszergazdát fogunk létrehozni, majd a későbbi fejezetben a beépített letiltásával!

Első lépésként, nyissuk meg az "Active Directory Users and Computers" alkalmazást! Majd a saját tartományunkat válasszuk ki! A saját tartományunkon belül pedig a "Users" konténert.



A "Users" konténerben a már rendelkezésre álló "Administrator" sablont kiválasztjuk, majd készítünk ebből egy másolatot! Általában véve a sablonokat be szokták úgy állítani, hogy ne lehessen használni, úgy egzakt. Ezt majd a következő fejezetben tesszük meg, hogy ne lehessen ezt használni. Majd, ahogyan a fenti képen látható módon, kitöljük az adatainkat, amivel használni fogjuk ezt a fiókot!

A "Next" gomb megnyomására a megjelenő ablakban meg kell adnunk valamilyen jelszót. És emellett lehetőségünk van további lehetőségek beállítására. Mint például arra, hogy a felhasználó nem változtathat jelszót, fiókja le van tiltva, a jelszava sohasem jár le, valamint arra lehetőséget, hogy a következő bejelentkezéskor jelszót kell változtatni. (**Remote Desktop-t kinyírja, mert nem tudnak ekkor jelszót változtatni**) Ha mindenkel megvagyunk, akkor "Next" gombra kattintunk, majd ha minden leellenőriztünk, akkor a "Finish" gombra kattintunk.

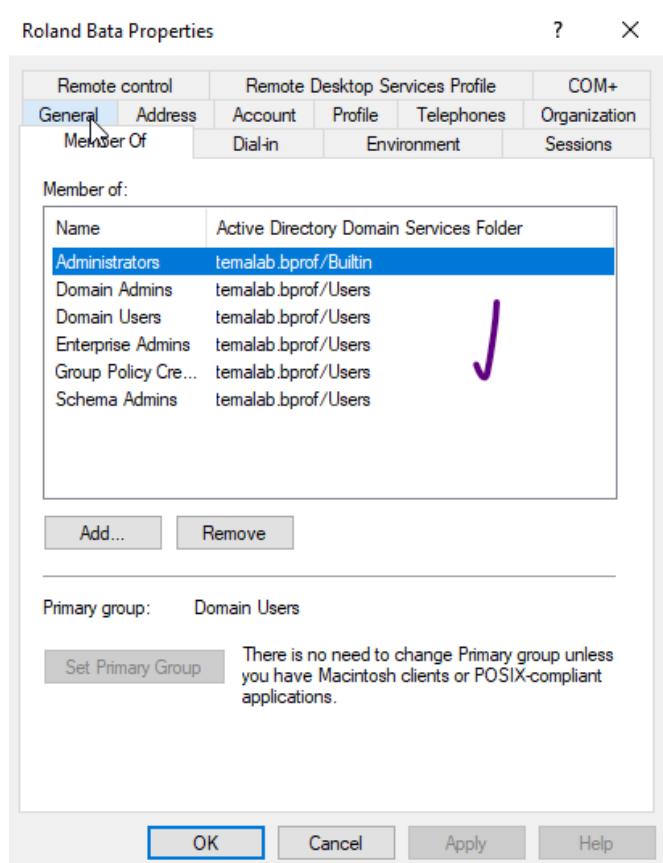
A fiókunk beállításait már ekkor is ellenőrizhetjük! Jobb klikk az imént létrehozott fiókunkra és utána a "Properties" lehetőség kiválasztásakor, már több lehetőséget láthatunk.

Mint az jól látható a képen, ténylegesen Adminisztrátor jogosultságokkal rendelkezik a fiókunk. De természetesen ha esetleg valamilyen jogosultság még hiányozna, akkor azt akár itt is megtehetjük (vagy a csoportban). (**pl Remote Desktop**)

Sok lehetőségünk akad egy felhasználó testreszabására vagy csoportok testreszabására. Mint például a "Session"-ben meg lehet adni, hogy mennyi ideig tarthat egy User Session Time-ja. Mennyit tölthet "Idle"-ben és stb...

Ami még érdekesebb lehet az a "Home Folder" beállítása. Megtehetjük azt, hogy a felhasználók vagy a csoportok "Home" mappája mondjuk nem a gépen van, hanem mondjuk egy szerveren RAID-ve. Vagy egy meghajtóként is felcsatolhatjuk ezeket.

A mostani szakaszban tehát azt amit kellett, elvégeztem. A következő szakaszban a beépített rendszergazdát (sablont) fogom letiltani!

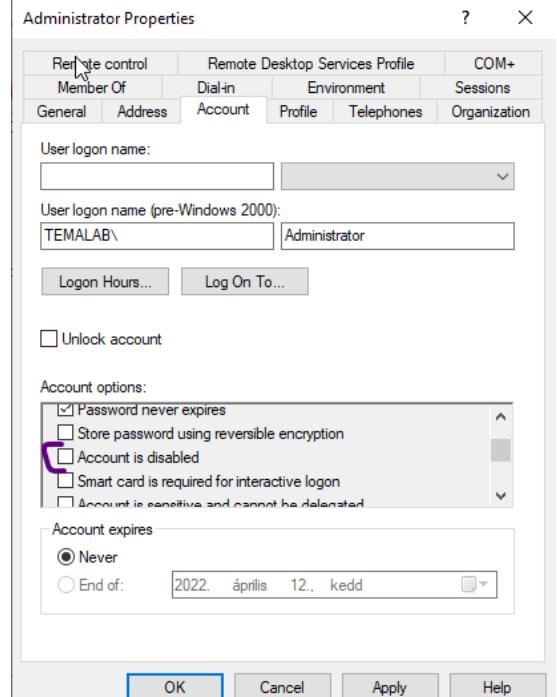


2.2. Beépített rendszerelődai fiók letiltása

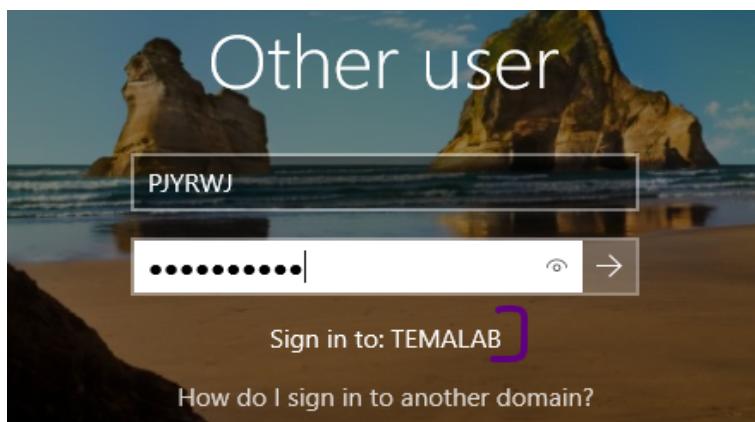
A mostani szakaszban a beépített rendszerelődai fiókot fogom tiltani. Ehhez a "Active Directory Users and Computers" alkalmazást fogjuk használni!

Kiválasztjuk a saját tartományunkat, majd el navigálunk a "Users" konténerbe majd az "Administrator"-re jobb klikk és válasszuk ki a "Properties" lehetőséget!

Itt az "Account" fülre kattintunk, majd az "Account Options" szekcióban kijelöljük az "Account is disabled" lehetőséget! (Végül "Apply")



Jelentkezzünk ki a fiókból és próbálunk meg újra bejelentkezni! Ha minden jól csináltunk, akkor ez az ablak fog minket fogadni! (MEMBERS szerver esetén is)



Próbálunk bejelentkezni az új fiókba!

Ha minden jól csináltunk, akkor szépen ezzel az új fiókkal be tudunk lépni!

Ezt a lehetőséget a MEMBERS szerveren is kipróbáltam és ugyanúgy betudtam ott is jelentkezni, valamint az "Administrator" fiókkal már nem tudtam bejelentkezni.

A következő szakaszban elkezdünk a PowerShell-el foglalkozni! Amivel Címtár objektumokat fogunk létrehozni!

2.3. Címtár objektumok létrehozása PowerShell segítségével (IGDLA)

A most következendő fejezetben egy fontos fogalommal fogunk foglalkozni, amit úgy hívnak, hogy IGDLA! Megmondom őszintén, hogy amikor olvastam ezt a feladatot, nem értem, hogy miért is kellene nekem így csinálnom a dolgokat. Már mint a szövegkörnyezetben leírt dolgok számomra akkoriban nem tűntek nekem elégé egyértelműnek. Már mint, nem az IGDLA fogalmával volt a gondom. Hanem ami a szövegkörnyezetben volt leírva. Ez nagyban megnehezítette a munkámat az, hogy magyarul voltak kiírva a dolgok. Szerintem sok helyen ezt továbbra is angolul kellene, "illene" használnunk. Már a szakmai angol értelmében. De ebbe nem szeretnék belekötni a továbbiakban. Én ahogyan az elején is, azokat a részeket, szakmai szavakat, továbbra is angolul fogom leírnivalni!

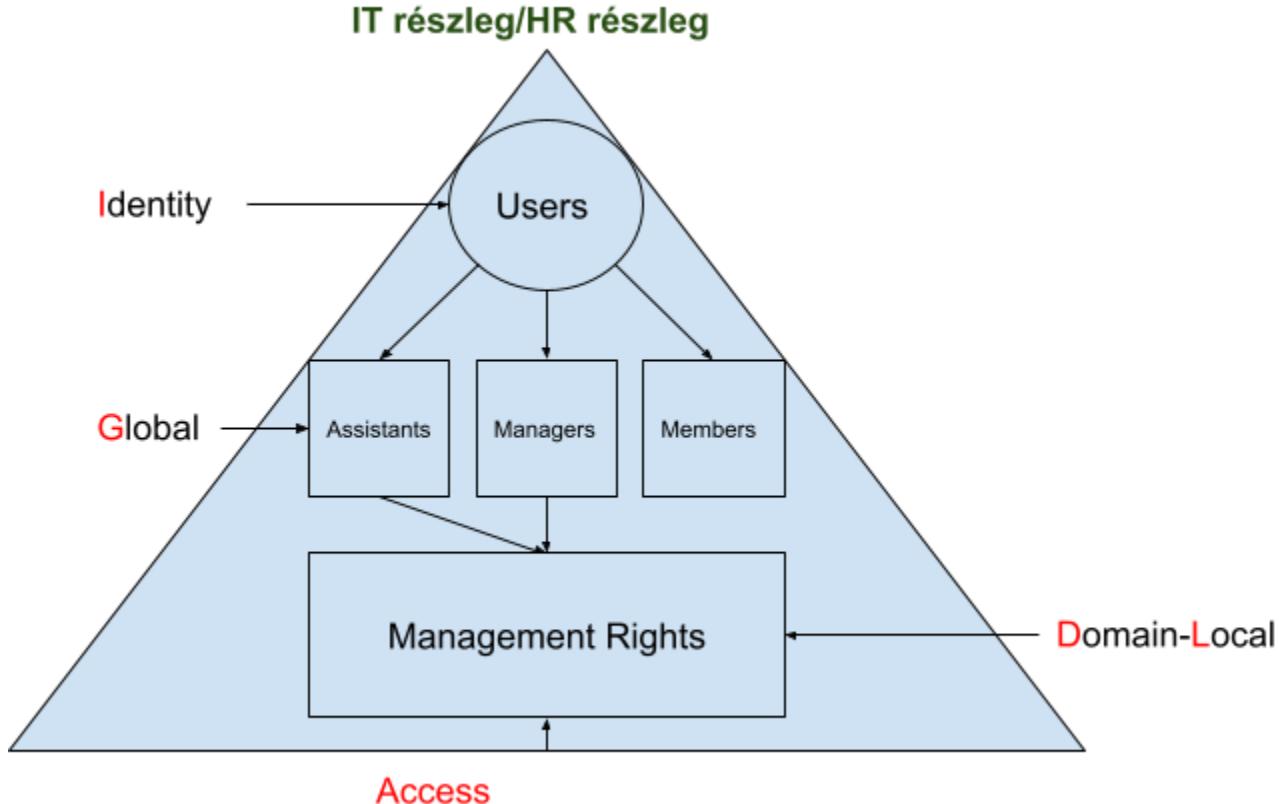
Mi is az-az IGDLA? Az alábbi szavakat alkotja az IGDLA.:

- Identity
- Global
- Domain Local
- Access

A feladat kritériumai ezek voltak.:

- Minimum 10 felhasználó legyen
 - 1 vezető
 - 1 asszisztens (vezető helyettes)
- Kettő OU létrehozása (Organization Unit = Szervezeti egység)
- Egy OU az egyik OU alá → Ennek nem láttam értelmét, de tudom azt, mikor lehetne használni és más hogyan esináltam meg
- 1-1 Group az OU-knak (Tagoknak és a Vezetőknek)

Az alábbi séma szerint építettem fel a feladatot!



Ezen séma alapján már könnyű volt elindulni az alapokon. De előtte érdemes tisztázni néhány fogalmat.

- Mi is az az Identity? (Identitások) (IT_User1)
 - Felhasználói és Számítógépes fiókok amelyek egy szervezeten belül bizonyos szerepet képviselnek!
 - Bárminely csoportnak a tagja lehet, de más tartományokban csak Univerzális és Globális csoportoknak lehet a tagja
- Mi is az a Global? (Szerepcsoportok) (IT_Members)
 - A Domain-Local csoport tagjai
 - A szerepkör alapján hasonló jogosultságokkal rendelkező Identitások csoportosításával képviselik a kezelési szabályokat
- Mi is az a Domain-Local? (Szabálycsoportok) (IT_ManageRight)
 - A helyi tartomány házirendjei alapján biztosítanak hozzáférést a tagoknak az erőforrásokhoz
 - Egy DL csoport hozzáadásával egy fájl ACL-jéhez (Access Control List) az egész csoportnak engedélyt adhat a hozzáférésre, függetlenül a szervezetben betöltött szerepkörtől. Ezt ellenőrzi a...
- Mi is az a hozzáférés?
 - Egy erőforráshoz való hozzárendelés, ami a hierarchiában lefelé halad, amíg meg nem találjuk az azt igénylő Identitásokat

Most, hogy az alap fogalmakat tisztáztam (ezzel magamnak is sokat segítve), nekiálltam ezeknek az elveknek alapján létrehozni a scripteket. Ezen sémből, már egész határozottan meg lehet írni a PowerShell scripteket!

Elöljáróban annyit, hogy én nem olvastam el az 1300 oldalas PowerShell könyvet. Csak belenéztem. Nekem, az interneten lévő MS DOCS segített és a PowerShell ISE program, ami segített abban, hogy egyes AD parancsok-hoz milyen változók szükségesek. Akkor elemezzük végig azt, hogy a feladat mit is kért pontosan.

Nyissunk meg egy PowerShell ISE alkalmazást.

Elsősorban hozzuk létre az igényelt **Organization Unit**-kat! Amik így néznek ki: (**Organizational Unit**)

```
New-ADOrganizationalUnit "IT" -Path "DC=temalab,DC=bprof" #OU
New-ADOrganizationalUnit "HR" -Path "DC=temalab,DC=bprof" #OU
New-ADOrganizationalUnit "Users" -Path "OU=IT,DC=temalab,DC=bprof" #OU
New-ADOrganizationalUnit "Users" -Path "OU=HR,DC=temalab,DC=bprof" #OU
```

Ezzel létrehoztam az IT és a HR Organization Unit-t! Fontos, hogy minden OU-ban még van egy OU, amiben a sima felhasználókat fogjuk csoportosítani!

- **New-ADOrganizationalUnit:** Létrehozunk egy új AD OU-t
- **-Path:** Itt adjuk meg azt, hogy melyik
 - **DC-hez** → Domain Component-hez
 - **OU-hoz** → Organizational Unit-hoz hozzuk létre

Miután ezzel meg voltunk, hozzuk létre a Domain Local csoportot a részlegekhez! Ami pedig így fog kinézni: (**Domain-Local**)

```
New-ADGroup -GroupScope DomainLocal -Name IT_ManageRight -Path "OU=IT,DC=temalab,DC=bprof"
```

Fontos megadnunk a csoportnak a Scope-ját, ez a mi esetünkben "**DomainLocal**" lesz!

- **-Name:** Itt adjuk meg a csoportnak a nevét
- **-Path:** Itt pedig az elérést

Most jöhetnek a szerep csoportok (Global)

```
#Global (szerepkörök)
New-ADGroup -GroupScope Global -Name IT_Managers -Path "OU=IT,DC=temalab,DC=bprof"
#Global
New-ADGroup -GroupScope Global -Name IT_Assistants -Path "OU=IT,DC=temalab,DC=bprof"
#Global
New-ADGroup -GroupScope Global -Name IT_Members -Path "OU=IT,DC=temalab,DC=bprof"
```

Definiáltam a vezetőnek, vezetőhelyetteseknek és a tagoknak egy csoportot. (szerintem ezeknek a paraméterei már egyértelműek)

Most, behúzhatjuk a jogosultságokat: (**Access**)

```
#Access (EHHEZ A OBJEKTUMHOZ)
Set-ADOrganizationalUnit -Identity "OU=IT,DC=temalab,DC=bprof" -ManagedBy "CN=IT_ManageRight,OU=IT,DC=temalab,DC=bprof"
#Access (nyilak)
Add-ADPrincipalGroupMembership -Identity "CN=IT_Managers,OU=IT,DC=temalab,DC=bprof" -MemberOf "CN=IT_ManageRight,OU=IT,DC=temalab,DC=bprof"
Add-ADPrincipalGroupMembership -Identity "CN=IT_Assistants,OU=IT,DC=temalab,DC=bprof" -MemberOf "CN=IT_ManageRight,OU=IT,DC=temalab,DC=bprof"
```

- **Set-ADOrganizationalUnit:** Beállítunk valamit az OU-ban
- **-Identity:** Akit beállítunk
- **-MemberOf:** Akinek a tagjai vagyunk (ez beállítódik a másik oldalt arra hivatkozva, hogy kik a tagjai ennek a csoportnak)

Ha ezzel megvagyunk, hozzuk is létre az **Identitásokat**, valamint állítsuk be egyes identitásokhoz azt, hogy pontosan melyik csoporthoz tartoznak: (**Identity**)

```
#Identity (USERS)
New-ADUser -Name IT_User1 -AccountPassword $passwd -DisplayName "User Name 1" -Path "OU=Users,OU=IT,DC=temalab,DC=bprof" -Enabled $true
New-ADUser -Name IT_User2 -AccountPassword $passwd -DisplayName "User Name 2" -Path "OU=Users,OU=IT,DC=temalab,DC=bprof" -Enabled $true
New-ADUser -Name IT_User3 -AccountPassword $passwd -DisplayName "User Name 3" -Path "OU=Users,OU=IT,DC=temalab,DC=bprof" -Enabled $true
New-ADUser -Name IT_User4 -AccountPassword $passwd -DisplayName "User Name 4" -Path "OU=Users,OU=IT,DC=temalab,DC=bprof" -Enabled $true
New-ADUser -Name IT_User5 -AccountPassword $passwd -DisplayName "User Name 5" -Path "OU=Users,OU=IT,DC=temalab,DC=bprof" -Enabled $true
New-ADUser -Name IT_Manager -AccountPassword $passwd -DisplayName "User Name 6" -Path "OU=IT,DC=temalab,DC=bprof" -Enabled $true
New-ADUser -Name IT_Assistant -AccountPassword $passwd -DisplayName "User Name 7" -Path "OU=IT,DC=temalab,DC=bprof" -Enabled $true
Add-ADPrincipalGroupMembership -Identity "CN=IT_Manager,OU=IT,DC=temalab,DC=bprof" -MemberOf "CN=IT_Managers,OU=IT,DC=temalab,DC=bprof"
Add-ADPrincipalGroupMembership -Identity "CN=IT_Assistant,OU=IT,DC=temalab,DC=bprof" -MemberOf "CN=IT_Managers,OU=IT,DC=temalab,DC=bprof"
Add-ADPrincipalGroupMembership -Identity "CN=IT_User1,OU=Users,OU=IT,DC=temalab,DC=bprof" -MemberOf "CN=IT_Members,OU=IT,DC=temalab,DC=bprof"
Add-ADPrincipalGroupMembership -Identity "CN=IT_User2,OU=Users,OU=IT,DC=temalab,DC=bprof" -MemberOf "CN=IT_Members,OU=IT,DC=temalab,DC=bprof"
Add-ADPrincipalGroupMembership -Identity "CN=IT_User3,OU=Users,OU=IT,DC=temalab,DC=bprof" -MemberOf "CN=IT_Members,OU=IT,DC=temalab,DC=bprof"
Add-ADPrincipalGroupMembership -Identity "CN=IT_User4,OU=Users,OU=IT,DC=temalab,DC=bprof" -MemberOf "CN=IT_Members,OU=IT,DC=temalab,DC=bprof"
Add-ADPrincipalGroupMembership -Identity "CN=IT_User5,OU=Users,OU=IT,DC=temalab,DC=bprof" -MemberOf "CN=IT_Members,OU=IT,DC=temalab,DC=bprof"
```

Felhasználók esetén, mivel mi adunk meg jelszót, meg kell azért azt adnunk, hogy a fiók engedélyezve lehessen. A jelszavak SecureString-é konvertálást végző kód részlet pedig ez lenne.:

```
$passwd = "Password1" | ConvertTo-SecureString -AsPlainText -Force
```

Itt megfigyelhető egy "**Pipeline**". Ezt használjuk arra, hogy ennek a tartalmát továbbvisszük a következő kifejezésnek!

A teljes kód így néz ki:

```
$passwd = "Password1" | ConvertTo-SecureString -AsPlainText -Force

New-ADOrganizationalUnit "IT" -Path "DC=temalab,DC=bprof" #OU
New-ADOrganizationalUnit "HR" -Path "DC=temalab,DC=bprof" #OU
New-ADOrganizationalUnit "Users" -Path "OU=IT,DC=temalab,DC=bprof" #OU
New-ADOrganizationalUnit "Users" -Path "OU=HR,DC=temalab,DC=bprof" #OU

#Domain Local (JOGOK) (szabálycsoporthoz)
New-ADGroup -GroupScope DomainLocal -Name IT_ManageRight -Path "OU=IT,DC=temalab,DC=bprof"
#Global (szerepkörök)
New-ADGroup -GroupScope Global -Name IT_Managers -Path "OU=IT,DC=temalab,DC=bprof"
#Global
New-ADGroup -GroupScope Global -Name IT_Assistants -Path "OU=IT,DC=temalab,DC=bprof"
#Global
New-ADGroup -GroupScope Global -Name IT_Members -Path "OU=IT,DC=temalab,DC=bprof"
#Access (EHEZ A OBJEKTUMHOZ)
Set-ADOrganizationalUnit -Identity "OU=IT,DC=temalab,DC=bprof" -ManagedBy "CN=IT_ManageRight,OU=IT,DC=temalab,DC=bprof"
#Access (nyilak)
Add-ADPrincipalGroupMembership -Identity "CN=IT_Managers,OU=IT,DC=temalab,DC=bprof" -MemberOf "CN=IT_ManageRight,OU=IT,DC=temalab,DC=bprof"
Add-ADPrincipalGroupMembership -Identity "CN=IT_Assistants,OU=IT,DC=temalab,DC=bprof" -MemberOf "CN=IT_ManageRight,OU=IT,DC=temalab,DC=bprof"

#Identity (USERS)
New-ADUser -Name IT_User1 -AccountPassword $passwd -DisplayName "User Name 1" -Path "OU=Users,OU=IT,DC=temalab,DC=bprof" -Enabled $true
New-ADUser -Name IT_User2 -AccountPassword $passwd -DisplayName "User Name 2" -Path "OU=Users,OU=IT,DC=temalab,DC=bprof" -Enabled $true
New-ADUser -Name IT_User3 -AccountPassword $passwd -DisplayName "User Name 3" -Path "OU=Users,OU=IT,DC=temalab,DC=bprof" -Enabled $true
New-ADUser -Name IT_User4 -AccountPassword $passwd -DisplayName "User Name 4" -Path "OU=Users,OU=IT,DC=temalab,DC=bprof" -Enabled $true
New-ADUser -Name IT_User5 -AccountPassword $passwd -DisplayName "User Name 5" -Path "OU=Users,OU=IT,DC=temalab,DC=bprof" -Enabled $true
New-ADUser -Name IT_Manager -AccountPassword $passwd -DisplayName "User Name 5" -Path "OU=IT,DC=temalab,DC=bprof" -Enabled $true
New-ADUser -Name IT_Assistant -AccountPassword $passwd -DisplayName "User Name 5" -Path "OU=IT,DC=temalab,DC=bprof" -Enabled $true
Add-ADPrincipalGroupMembership -Identity "CN=IT_Manager,OU=IT,DC=temalab,DC=bprof" -MemberOf "CN=IT_Managers,OU=IT,DC=temalab,DC=bprof"
Add-ADPrincipalGroupMembership -Identity "CN=IT_Assistant,OU=IT,DC=temalab,DC=bprof" -MemberOf "CN=IT_Assistants,OU=IT,DC=temalab,DC=bprof"
Add-ADPrincipalGroupMembership -Identity "CN=IT_User1,OU=Users,OU=IT,DC=temalab,DC=bprof" -MemberOf "CN=IT_Members,OU=IT,DC=temalab,DC=bprof"
Add-ADPrincipalGroupMembership -Identity "CN=IT_User2,OU=Users,OU=IT,DC=temalab,DC=bprof" -MemberOf "CN=IT_Members,OU=IT,DC=temalab,DC=bprof"
Add-ADPrincipalGroupMembership -Identity "CN=IT_User3,OU=Users,OU=IT,DC=temalab,DC=bprof" -MemberOf "CN=IT_Members,OU=IT,DC=temalab,DC=bprof"
Add-ADPrincipalGroupMembership -Identity "CN=IT_User4,OU=Users,OU=IT,DC=temalab,DC=bprof" -MemberOf "CN=IT_Members,OU=IT,DC=temalab,DC=bprof"
Add-ADPrincipalGroupMembership -Identity "CN=IT_User5,OU=Users,OU=IT,DC=temalab,DC=bprof" -MemberOf "CN=IT_Members,OU=IT,DC=temalab,DC=bprof"

#Domain Local (JOGOK)
New-ADGroup -GroupScope DomainLocal -Name HR_ManageRight -Path "OU=HR,DC=temalab,DC=bprof"
#Global
New-ADGroup -GroupScope Global -Name HR_Managers -Path "OU=HR,DC=temalab,DC=bprof"
#Global
New-ADGroup -GroupScope Global -Name HR_Assistants -Path "OU=HR,DC=temalab,DC=bprof"
#Global
New-ADGroup -GroupScope Global -Name HR_Members -Path "OU=HR,DC=temalab,DC=bprof"
#Access (nyilak)
Set-ADOrganizationalUnit -Identity "OU=HR,DC=temalab,DC=bprof" -ManagedBy "CN=HR_ManageRight,OU=HR,DC=temalab,DC=bprof"
#Access (nyilak)
Add-ADPrincipalGroupMembership -Identity "CN=HR_Managers,OU=HR,DC=temalab,DC=bprof" -MemberOf "CN=HR_ManageRight,OU=HR,DC=temalab,DC=bprof"
Add-ADPrincipalGroupMembership -Identity "CN=HR_Assistants,OU=HR,DC=temalab,DC=bprof" -MemberOf "CN=HR_ManageRight,OU=HR,DC=temalab,DC=bprof"

New-ADUser -Name HR_User1 -AccountPassword $passwd -DisplayName "User Name 1" -Path "OU=Users,OU=HR,DC=temalab,DC=bprof" -Enabled $true
New-ADUser -Name HR_User2 -AccountPassword $passwd -DisplayName "User Name 2" -Path "OU=Users,OU=HR,DC=temalab,DC=bprof" -Enabled $true
New-ADUser -Name HR_User3 -AccountPassword $passwd -DisplayName "User Name 3" -Path "OU=Users,OU=HR,DC=temalab,DC=bprof" -Enabled $true
New-ADUser -Name HR_User4 -AccountPassword $passwd -DisplayName "User Name 4" -Path "OU=Users,OU=HR,DC=temalab,DC=bprof" -Enabled $true
New-ADUser -Name HR_User5 -AccountPassword $passwd -DisplayName "User Name 5" -Path "OU=Users,OU=HR,DC=temalab,DC=bprof" -Enabled $true
New-ADUser -Name HR_Manager -AccountPassword $passwd -DisplayName "User Name 5" -Path "OU=HR,DC=temalab,DC=bprof" -Enabled $true
New-ADUser -Name HR_Assistant -AccountPassword $passwd -DisplayName "User Name 5" -Path "OU=HR,DC=temalab,DC=bprof" -Enabled $true
Add-ADPrincipalGroupMembership -Identity "CN=HR_Manager,OU=HR,DC=temalab,DC=bprof" -MemberOf "CN=HR_Managers,OU=HR,DC=temalab,DC=bprof"
Add-ADPrincipalGroupMembership -Identity "CN=HR_Assistant,OU=HR,DC=temalab,DC=bprof" -MemberOf "CN=HR_Assistants,OU=HR,DC=temalab,DC=bprof"
Add-ADPrincipalGroupMembership -Identity "CN=HR_User1,OU=Users,OU=HR,DC=temalab,DC=bprof" -MemberOf "CN=HR_Members,OU=HR,DC=temalab,DC=bprof"
Add-ADPrincipalGroupMembership -Identity "CN=HR_User2,OU=Users,OU=HR,DC=temalab,DC=bprof" -MemberOf "CN=HR_Members,OU=HR,DC=temalab,DC=bprof"
Add-ADPrincipalGroupMembership -Identity "CN=HR_User3,OU=Users,OU=HR,DC=temalab,DC=bprof" -MemberOf "CN=HR_Members,OU=HR,DC=temalab,DC=bprof"
Add-ADPrincipalGroupMembership -Identity "CN=HR_User4,OU=Users,OU=HR,DC=temalab,DC=bprof" -MemberOf "CN=HR_Members,OU=HR,DC=temalab,DC=bprof"
Add-ADPrincipalGroupMembership -Identity "CN=HR_User5,OU=Users,OU=HR,DC=temalab,DC=bprof" -MemberOf "CN=HR_Members,OU=HR,DC=temalab,DC=bprof"
```

Térmeztetesen az egész kódon lehet finomítani! Ha lesz rá időm, alkalmam, akkor még elgondolkozok azon, hogy pícit átirom a dolgokat. Sőt, elvileg automatizálni is lehetne a dolgokat, de nem vagyok PowerShell szakértő, valamint ezt a nyelvet nem annyira szeretem. Azt díjazom, hogy a PowerShell ISE éppen annyit segít, hogy ne neked kelljen rájönnöd a dolgokra.

Az eredmény pedig így néz ki!

The screenshot shows the Windows Active Directory Users and Computers (ADUC) management console. On the left, the navigation pane displays the tree structure of the Active Directory forest, including Active Directory Users and Computers, Saved Queries, and various organizational units like temalab.bprof, HR, and IT. The IT and HR organizational units contain sub-OU's such as Users, Keys, LostAndFound, Managed Service Accounts, Program Data, System, Users, NTDS Quotas, and TPM Devices. The HR organizational unit also contains a security group named HR_Managers.

The main pane displays a list of objects under the HR_Managers security group. The columns are Name, Type, and Description. The objects listed are:

Name	Type	Description
Users	Organizational Unit	
HR_Assistant	User	
HR_Assistants	Security Group - Global	
HR_Manager	User	
HR_ManageRight	Security Group - Domain Local	
HR_Managers	Security Group - Global	
HR_Members	Security Group - Global	

On the right, a detailed properties window for the HR_Managers security group is open. It shows the 'Members' tab, which lists the member of the group. The member listed is 'HR_Manager' from the temalab.bprof/HR OU. There are 'Add...' and 'Remove' buttons at the bottom of the members list.

The image shows two side-by-side Windows dialog boxes. On the left, the 'HR_Managers Properties' window displays the 'Members' tab, showing 'HR_ManageRight' as a member of the 'HR' group. On the right, the 'HR_User5 Properties' window displays the 'Member Of' tab, showing 'Domain Users' and 'HR_Members' as groups the user belongs to.

A következő feladat az alapvető biztonsági beállítások kezelése lesz.

3. Alapvető biztonsági beállítások kezelése

Első feladatunk beállítani azt tartomány szintjén, hogy a jelszavak, azok 180 napig legyenek a jelszavak használhatóak!

Elhez az AD_DS szerveren nyissuk meg a "**Group Policy Management**" alkalmazást! Válasszuk ki a saját erdőket! (*Forest*) Majd a domain nevet lenyitva a "**Default Domain Policy**" lehetőségnél jobb klikk, majd "**Edit**" gombra kattintunk.

Navigálunk el a... **Policies** → **Windows Settings** → **Security Settings** → **Account Policies** → **Password Policy** lehetőségre.

Majd itt a "**Maximum password age**" lehetőséget átírjuk az alapértelmezett értékéről, akkor **180 napra**!

Ennek elmentésekor, indítsuk el a MEMBERS szervert, majd nézzük meg azt, hogy valóban frissültek-e a Policy-k! (Biztosan, hiszen bejelentkezés előtt, ezeket ellenőri a rendszer)

```
C:\Users\HR_User1>net user /domain HR_User1
The request will be processed at a domain controller for domain temalab.bprof.
```

```
User name          HR_User1
Full Name          User Name 1
Comment
User's comment
Country/region code    000 (System Default)
Account active      Yes
Account expires     Never

Password last set   3/14/2022 6:07:43 AM
Password expires    9/10/2022 6:07:43 AM
Password changeable 3/15/2022 6:07:43 AM
Password required    Yes
User may change password Yes

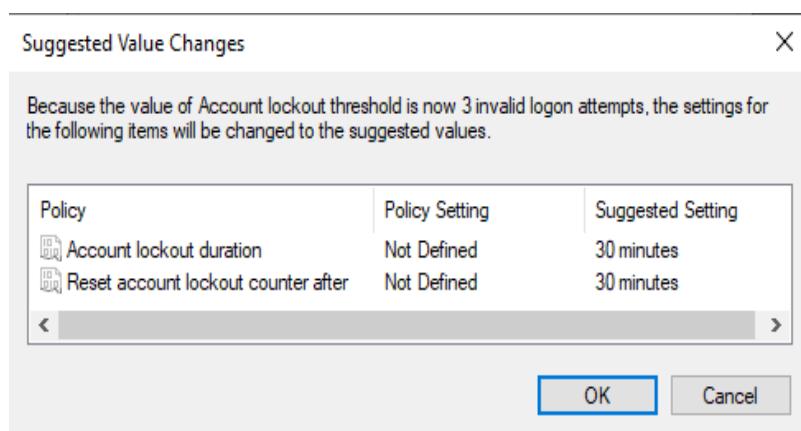
Workstations allowed All
Logon script
User profile
Home directory
Last logon         3/17/2022 4:06:02 AM
Logon hours allowed All

Local Group Memberships
Global Group memberships *HR_Members           *Domain Users
The command completed successfully.
```

Mint a képen jól látható, a HR_User1 fiók esetében a "**Password expires**" és a "**Password last set**" **között 180 nap különbség van!** Az-az sikeresen beállítódtak a Policy-k!

Állítsunk be még 1-2 dolgot!

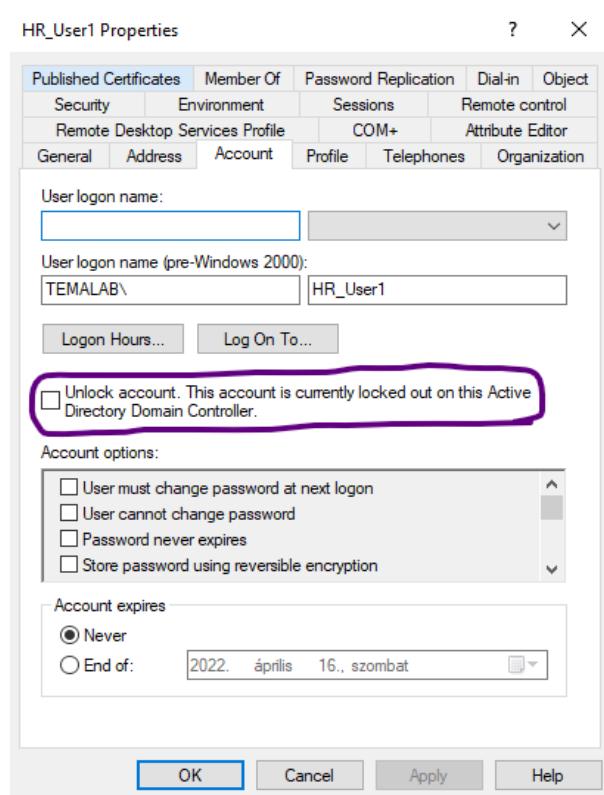
- Fiókbezárás 3 próbálkozás után : Account Lockout Policy → Account Lockout threshold



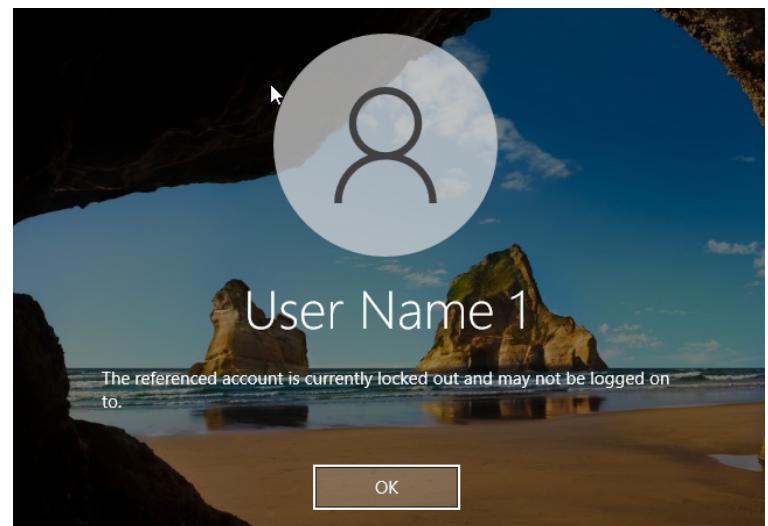
Ekkor felajánl nekünk egy "**Suggested Value Changes**" ablakban számunkra egy lehetőséget, hogy ezekre a beállításokra lenne érdemes beállítani az "**Account lockout duration**"-t, azaz hogy mennyi ideig legyen lezártva a fiók. Valamint azt, hogy a "**Reset account lockout counter after**" aminek az a lényege, hogy mennyi idő múlva állítsa vissza a "**bad logon**" számlálót! Ezt érdemes azonos beállításokra állítani.

De természetesen, ha nekünk ezek az értéket majd nem lesznek megfelelők, ezeket majd felülbírálhatjuk.

- 2 jelszóváltoztatás után lehessen újra használni a régi jelszót : Password Policy → Enforce Password History
- Ezeket beállítva, jelentkezzünk ki a MEMBERS szerveren bejelentkezett fiókból. Majd próbálkozzunk 3x téves jelszó beírásával! Ezt az ablakot kell kapni.:



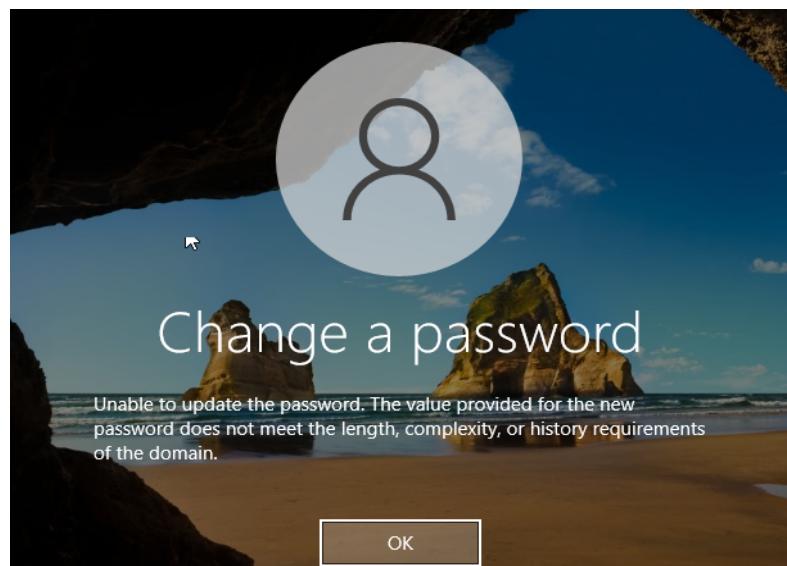
Mint jól látható, 3. próbálkozásra valóban sikerült lezárnunk a fiókunkat!



AD_UE alkalmazásban is látható, hogy jelenleg a fiókunk le lett zárt az AD_DC-ból! Nyissuk fel a fiókot a jelszóváltoztatási teszteléshez.

Bár, megtéhetném azt, hogy ezt a fiókot itt hagyom. De tesztelünk le minden szépen!

Ehhez kapcsoljuk ki a "**Password must meet complexity requirements**" lehetőséget a Password Policy-ben!



Tehát, első alkalommal "**Password2**"-re írtam át a jelszót, majd pedig megpróbáltam "**Password1**"-re visszairni a jelszót! És nem is engedte! A bal oldali képen ez teljesen jól látható!

Majd írjuk vissza 3.-ra a jelszavunkat! Apró megjegyzés arra, ha nem engedi a jelszót többször egymás után megváltoztatni!

Ehhez egy további policy beállítást kell átírnivalni! Pontosabban a "**Minimum password age**" lehetőséget! Ennek átírásakor lehetőségünk van

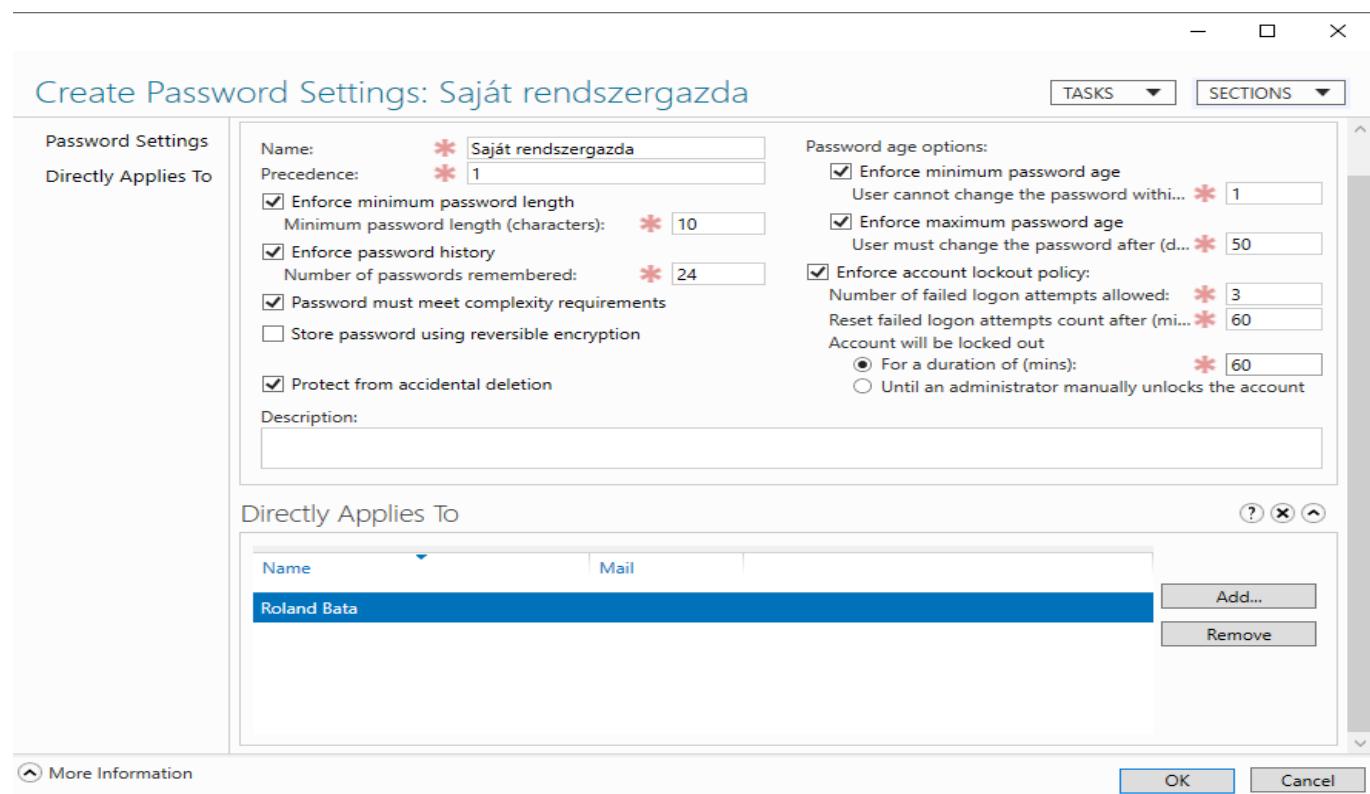
azonnal jelszót változtatni! Állítsunk vissza, most minden lehetőséget, amit kézzel beállítottunk! Fontos megjegyzés, hogyha a MEMBERS szerverre nem jutnak el a változások, akkor érdemes újraindítani a gépet. (VAGY CMD-ben “gupdate /force”)

A következő feladatunk egy eltérő jelszó házirend létrehozása lesz. A rendszergazdáknak állítsunk be egy erőset, a létrehozott csoportnak pedig alacsonyabb szintű jelszó házirendet fogunk kialakítani!

Elsősorban nyissuk meg az AD_AC alkalmazást (**Active Directory Administrative Center**)! Válasszuk ki a saját domain konténerünket! Ha ez nem létezne, akkor mint Node-t hozzá kellene adnunk. De a lokális minden látni fogjuk! Jelen esetben, ezzel tehát akkor nem kell foglalkoznunk!

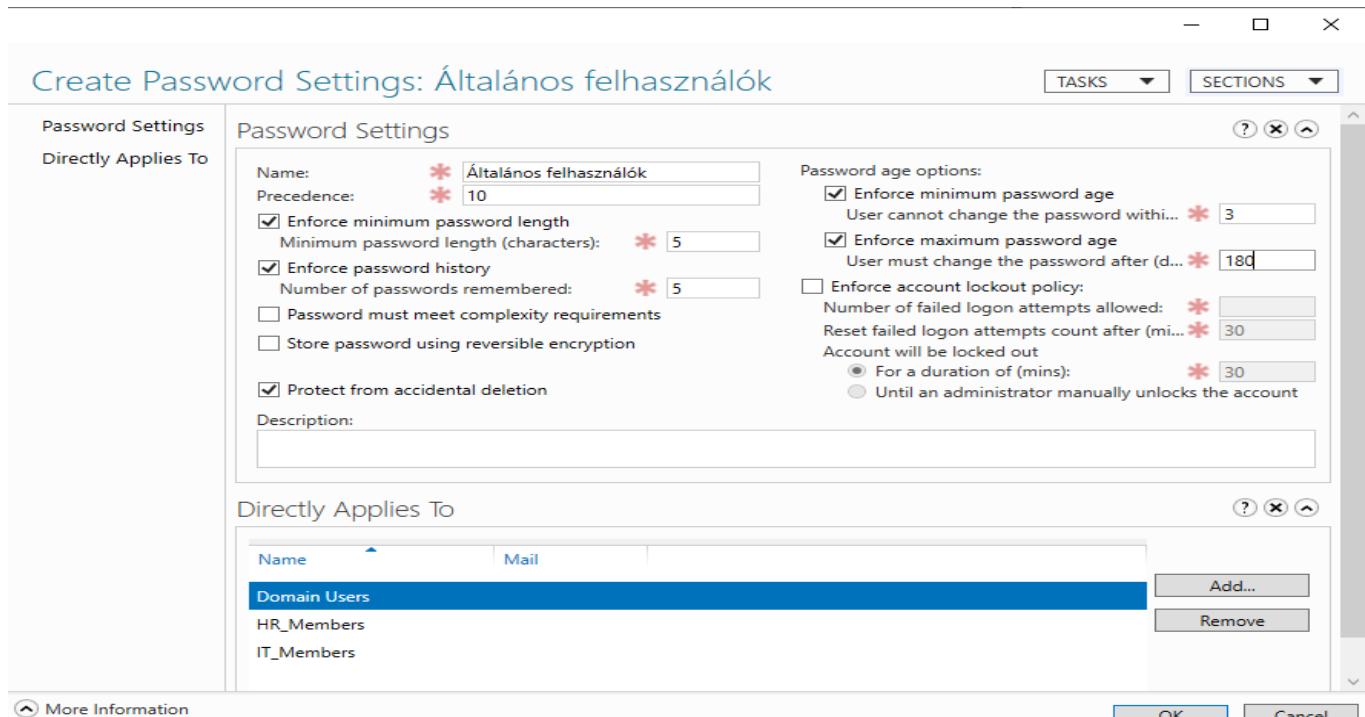
Nyissuk meg a **“System”** konténert, majd válasszuk ki a **“Password Settings”** konténert ezen a konténeren belül! Ha minden igaz, ez most jelen esetben teljes mértékben üres. Itt fogjuk létrehozni a házirendeket szépen elszeparálva! A jobb oldalt lévő **“Task”** fülön kattintsunk a **“New”** gombra és azon belül a **“Password Settings”** lehetőségre! Ekkor lehetőségünk van beállítani a paramétereket!

Elsőként a saját rendszergazdai fiókunknak hozzunk létre egy FGPP-t! *Lényegében arról van itt szó, hogy tudjuk definiálni felhasználó illetve csoport szinten azt, hogy milyen jelszó policy-k lesznek az érvényesek! Az-az tehetem azt, hogy egy csoport tagja vagyok, amely csoportnak a precedencia értéke nagyobb az én értékemhez képest. Ez azt jelenti, hogy az én értékem, kisebb, aminek révén az én jelszó policy-m fog érvényre jutni! (ha van) Ez teljesen más hogy lenne, ha mondjuk a csoport precedenciája sokkal kisebb az enyémhez képest! Ekkor a csoporthoz tartozó jelszó policy lesz érvényben az én nevemben is!*



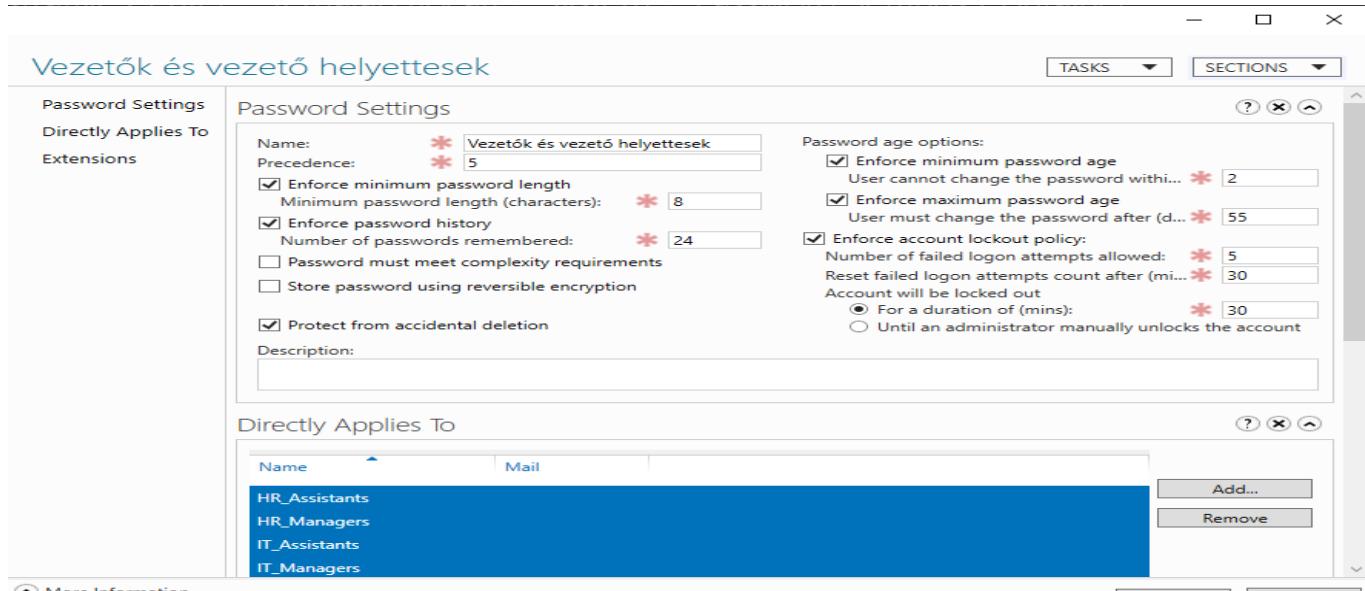
A rendszergazdai fiókunk precedence értéke legyen a legkisebb! A fenti beállításokat alkalmaztam a fiókomhoz!

A következő feladatunk az általános felhasználói fiókokhoz is egy jelszó házirend létrehozása! Ehhez továbbra is a “**Task**” fülön található “**New**” gombon belül a “**Password Settings**” lehetőséget kell választanunk! Ezeket a beállításokat alkalmaztam a felhasználókra!



A precedence értéket elég magasra állítva, belátható az, hogy a mi rendszergazdai fiókunk az ugyanúgy tagja a Domain Users csoportnak! Ez nem fog gondot jelenteni, hiszen a mi rendszergazdai fiókunknak kisebb a precedencia értéke, az-az az Ő jelszó házirendje fog érvényre jutni! Ehhez hozzáadtam a HR_Members és az IT_Members felhasználókat! (Igen, az IT_Managerek és az IT_Assistant-ek és a HR viszonylatban az fog történni, hogy rájuk a Domain Users jelszó házirendje lesz érvényben... Ezt fogom most majd korrigálni! Ellenőrizni fogjuk a Precedence hatását!)

Ehhez hozunk létre egy újabb sablont! És vegyük bele az IT/HR_Managers és az IT/HR_Assistants csoportokat!



Nyilván a beállításokkal is szeretném érzékeltetni, hogy a vezetők és a vezető helyettesek csoportjának beállítási szintje megközelítőleg közel van a saját fiókomhoz! De természetesen meg lehet azt oldani, hogy ezeknél a beállításoknál sokkal lazábbra vesszük a dolgokat és azonnal a legkisebb precedenciára állítom! De így, most a vezetőkre és a vezető helyettesekre ez a keményebb jelszó házirend lesz érvényben! (És nem a Általános felhasználók jelszó házirendje fogja dominálni a vezető és a vezetőhelyettes csoportjának jelszó házirendjét!)

A következő feladatunk a jelszó házirendek ellenőrzése! Ehhez most a MEMBERS szerveren jelentkezzünk be, most egy általános felhasználói fiókba! (Pl.: HR_User1)

```
PS C:\Windows\system32> Get-ADUserResultantPasswordPolicy HR_User1

AppliesTo : {CN=HR_Members,OU=HR,DC=temalab,DC=bprof, CN=IT_Members,OU=IT,DC=temalab,DC=bprof, CN=Domain Users,CN=Users,DC=temalab,DC=bprof}
ComplexityEnabled : False
DistinguishedName : CN=Általános felhasználók,CN=Password Settings Container,CN=System,DC=temalab,DC=bprof
LockoutDuration : 00:30:00
LockoutObservationWindow : 00:30:00
LockoutThreshold : 0
MaxPasswordAge : 180.00:00:00
MinPasswordAge : 3.00:00:00
MinPasswordLength : 5
Name : Általános felhasználók
ObjectClass : msDS-PasswordSettings
ObjectGUID : 90e56b2d-eaea-4384-b28a-b5018b2bc0b8
PasswordHistoryCount : 5
Precedence : 10
ReversibleEncryptionEnabled : False
```

Egy IT_Manager fiók esetén?

```
PS C:\Windows\system32> Get-ADUserResultantPasswordPolicy HR_Manager

AppliesTo : {CN=HR_Assistants,OU=HR,DC=temalab,DC=bprof, CN=IT_Assistants,OU=IT,DC=temalab,DC=bprof, CN=IT_Managers,OU=IT,DC=temalab,DC=bprof}
ComplexityEnabled : False
DistinguishedName : CN=Vezetők és vezető helyettesek,CN=Password Settings Container,CN=System,DC=temalab,DC=bprof
LockoutDuration : 00:30:00
LockoutObservationWindow : 00:30:00
LockoutThreshold : 5
MaxPasswordAge : 55.00:00:00
MinPasswordAge : 2.00:00:00
MinPasswordLength : 8
Name : Vezetők és vezető helyettesek
ObjectClass : msDS-PasswordSettings
ObjectGUID : 71000cae-07fb-42a4-9e5f-2a7b72ed6225
PasswordHistoryCount : 24
Precedence : 5
ReversibleEncryptionEnabled : False
```

Mint az jól látható, ránk nem lesz érvényes az Általános felhasználók jelszó házirendje! Pedig mi is a Domain_Members tagjai vagyunk! Ez a precedencia miatt van!

4. NTFS és fájlmegosztási jogosultságok tesztelése

4.1. Fájlmegosztás létrehozása a MEMBERS szerveren

A MEMBERS szerveren hozunk létre a "C" meghajtóra egy *Shares* folder-t! És a feladat alapján, hozunk létre egy "IT" és egy "HR" mappát!

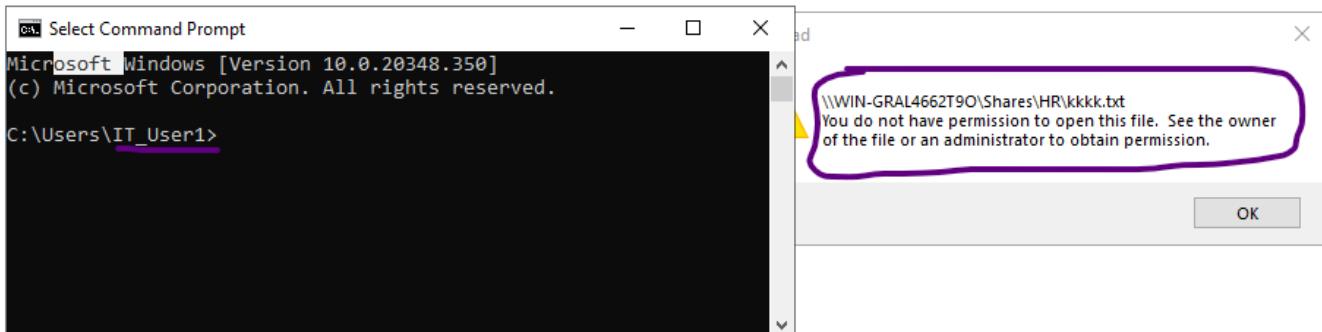
Majd menjünk el a "Shares" mappa "Properties" részére és a "Security" fülön nyomjunk az "Advanced" gombra!

A kettő mappának az alábbi beállításokat adtam meg.:

Type	Principal	Access	Inherited from	Applies to
Deny	IT_Managers (TEMALAB\IT_Manag...)	Special	None	This folder, subfolders and files
Deny	IT_Assistants (TEMALAB\IT_ASSISTANT...)	Special	None	This folder, subfolders and files
Deny	IT_Members (TEMALAB\IT_Memb...)	Special	None	This folder, subfolders and files
Allow	IT_Managers (TEMALAB\IT_Manag...)	Read & execute	None	This folder, subfolders and files
Allow	IT_Assistants (TEMALAB\IT_ASSISTANT...)	Read & execute	None	This folder, subfolders and files
Allow	IT_Members (TEMALAB\IT_Memb...)	Read & execute	None	This folder, subfolders and files
Allow	HR_Managers (TEMALAB\HR_Man...)	Full control	None	This folder, subfolders and files
Allow	HR_Assistants (TEMALAB\HR_ASSISTANT...)	Full control	None	This folder, subfolders and files
Allow	HR_Members (TEMALAB\HR_Memb...)	Full control	None	This folder, subfolders and files
Allow	SYSTEM	Full control	C:\	This folder, subfolders and files
Allow	Administrators (WIN-GRAL4662T9...)	Full control	C:\	This folder, subfolders and files

Mint a képen jól látható most a HR mappának az ACL részét állítjuk! A HR_Managers,Members,Assistants csoportoknak teljes jogosultságot állítunk be, de az IT_Managers,Assistants,Members esetében ez egy picit más hogyan fog kinézni. Csak arra

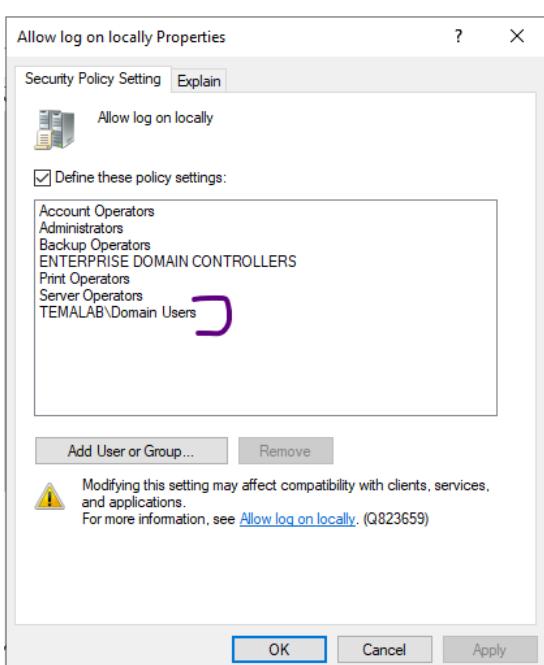
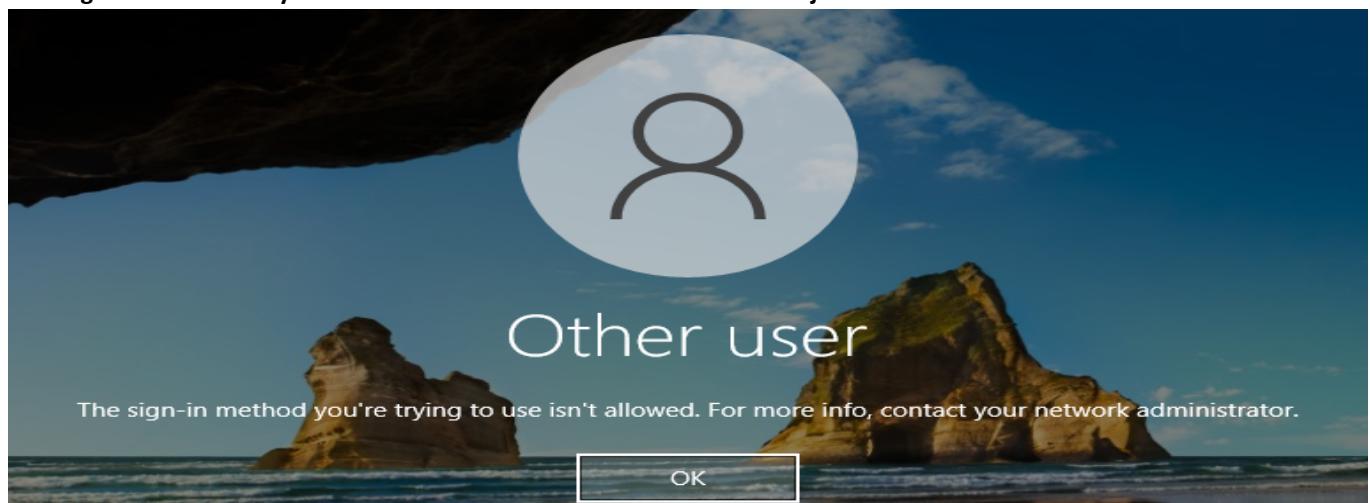
adunk nekik jogosultságot, hogy olvasni tudjanak! Emellett letiltjuk nekik azokat a dolgokat, amikkel módosításokat tudnának végrehajtani a mappában lévő tartalmakkal, vagy akár saját maguk tudnának létrehozni tartalmakat. Hiszen a feladat csak annyit kért, hogy az egyik részleg a saját mappájához teljes jogosultsága legyen, míg a másik részlegnek csak olvasási joga lehessen! Ezeket a beállításokat tükröztem az IT mappára is! Csak azzal a különbséggel, hogy ott az IT csoportoknak állítottam be ezeket a tiltásokat ACL szinten! (Access Control List)



Mint az a fenti képen látható, nem tudjuk elmenteni a létrehozott TXT állományt IT_User1 felhasználóként a HR mappába! Ami azt jelenti, hogy a beállított ACL teljes egészében úgy működik, ahogyan azt beállítottam!

4.2. DU bejelentkezések engedélyezése a DC-n

Jelenleg a tartományvezérlő szerverünkön nem tudunk bejelentkezni a létrehozott felhasználóinkkal!



Ehhez be kell jelentkeznünk a tartományvezérlő szerverünkre, majd nyissuk meg a "**Group Policy Management**" alkalmazást, majd nyissuk le a saját domain-keket! A saját domain-ünk alatt a "**Domain Controllers**" részt nyissuk le, majd a "**Default Domain Controllers Policy**" részre "**Edit**"-ünk.

Policies → Windows Settings → Security Settings → Local Policies → User Rights and Managements lehetőséget kiválasztva válasszuk ki a "**Allow log on locally**" lehetőséget! Itt tudjuk azt beállítani, hogy lokálisan is be tudunk jelentkezni a tartományvezérlő szerverre! Adjuk hozzá a Domain Users csoportot és ezzel most már sikeresen be tudunk lépni a Domain Userek-kel!

Így, most már csak egy dolgot kell megtennünk! Nyissunk meg egy CMD-t, majd írjuk bele az alábbi parancsot.: **gpupdate /force**
Ezzel azt érjük el, hogy ráerőltetjük a csoportházirendre azt, hogy frissítse a beállításokat.

Jelentkezzünk ki és próbálunk meg bejelentkezni egy DU fiókkal!

4.3. Egyszerűsített fájlmegosztási beállítások áttekintése

Ezen a módon tudjuk beállítani, hogy kik férhetnek hozzá a megosztott mappához! Jelenlegi helyzetben mindenkinél olvasási és írási jogai vannak! Ezt beállíthatjuk akár az IT/HR részlegre is, így csak azok fognak tudni ehhez a megosztott mappához hozzáérni, akikhez ezt a mappát hozzárendeltük! A mostani példában most csak a HR felhasználóknak adtam jogot, így amikor megpróbáltam elérni a megosztott mappát (IT userrel), ezt a hibát kellett kapnom!

The screenshot shows a Windows Network Error dialog box on the left and a file permissions table on the right.

Network Error

Windows cannot access \\WIN-GRAL4662T9O\Shares

You do not have permission to access \\WIN-GRAL4662T9O\Shares. Contact your network administrator to request access.

For more information about permissions, see [Windows Help and Support](#)

Close

Name	Permission Level
HR_Assistants	Read/Write ▾
HR_Managers	Read/Write ▾
HR_Members	Read/Write ▾
Roland Bata	Owner

Ha most hozzáadjuk az IT részleghez a jogokat, akkor az IT részleg is most már, hozzáfog tudni férni a megosztott mappához! Annyi viszont fontos, hogy a beállított mappai jogosultságok módosítását kérő ablaknál azt a lehetőséget válasszuk ki, hogy ne nyúljon a beállított értékekhez! (így nem fogja felülcsapni a beállított ACL-keket a mappákon, így továbbra sem fog tudni fájlt mappát, etc-t létrehozni egy IT-s egy HR-s mappában! (csak olvasni fog tudni)

4.4. FSRM feltelepítése a MEMBERS szerverre

A mostani feladatban egy File Server Resource Manager szolgáltatást fogunk feltelepíteni a fájlszerverre, jelen esetben a MEMBERS szerverre!

A "Server Manager" alkalmazásban válasszuk ki az "Add roles and features" ágát!

A "Server Roles" kiválasztásakor, a "File and Storage Services" fület nyissuk le, valamint a "File and iSCSI Services" lehetőséget is nyissuk tovább, majd ott az FSRM lehetőséget jelöljük be! Majd szépen, kezdjük el feltelepíteni a kért szolgáltatást!

The screenshot shows the "Add Roles and Features Wizard" window during the installation process.

Add Roles and Features Wizard

Installation progress

DESTINATION SERVER: WIN-GRAL4662T9O.temalab.bprof

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results

View installation progress

Feature installation

Installation started on WIN-GRAL4662T9O.temalab.bprof

File and Storage Services

- File and iSCSI Services
- File Server Resource Manager**

Remote Server Administration Tools

- Role Administration Tools
- File Services Tools
- File Server Resource Manager Tools

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

[Export configuration settings](#)

< Previous Next > Close Cancel

Ekkor a tools menüpontban megjelenik egy új alkalmazás, "File Server Resource Manager", ezt most nyissuk meg!

4.4.1. Quota Management (Kvóta menedzsment)

A kvóta menedzsment használatával lehetőségünk van, úgynevezett korlátokat felállítani egy köteten, vagy egy mappára. Emellett értesítést tudunk generálni adott elérte kvóta kúszóbszintek esetén, amikor azt a kvóta határt elértük vagy túlléptük!

A kvóta menedzsmentben kétféle kvótázási módszert definiáltak

- **"Hard" Quote** : A felhasználók nem léphetik túl a megadott kvótázási szintet! Ha 100MB a kvóta, ha az betek, nincsen további erőforrás megosztás!
- **"Soft" Quote** : A felhasználók túl léphetik a megadott kvótázási limitet, egy bizonyos határig. (120%) De törölni kellene a felesleges fájlokat, hogy az adott korlántról beljebb maradjanak.

A kvóta menedzsmentnek kettő menüpontja van

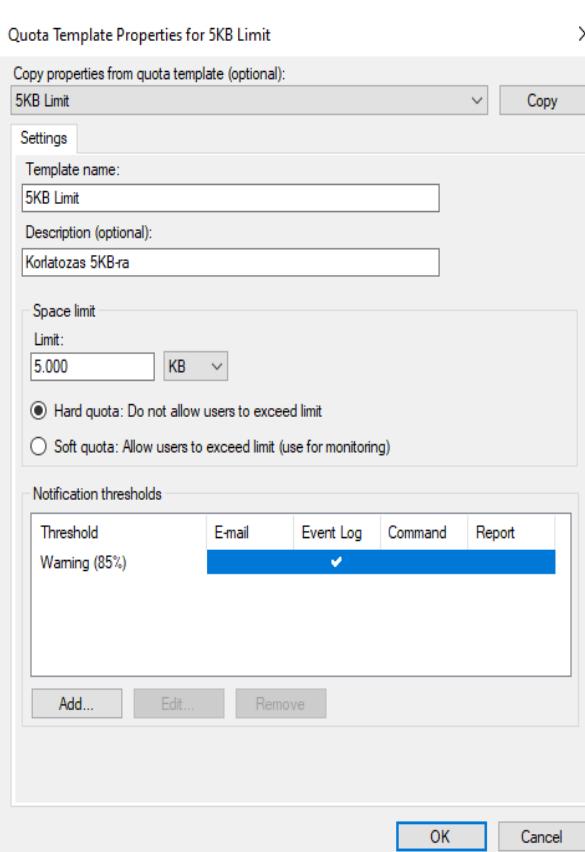
- **Quotas** → A beállított kvóták gyűjteménye
- **Quota Templates** → Kvótázási sablonok, amiket egyes kvótára beállíthatunk

4.4.1.1. Quota Templates

Egy kvóta séma létrehozásakor az alábbi lehetőségeket állíthatjuk be!

- **Copy Properties from Quota Template (optional)** → Lemásolhatjuk egy másik séma beállításait! Ez nem kötelező lépés, csak opcionális!
- **Template Name** → Séma neve, pl : 5KB LIMIT (A szóval jelzem, hogy ez bizony HARD Quote stílus lesz)
- **Description** → Séma leírása, pl: 5KB-s limit
- **Space Limit** → Beállíthatjuk KB/MB/GB/TB lépcsoik közül kiválasztva, mekkora legyen a limit/usage!
 - Hard quota / Soft quota opción kijelölése
- **Notifications Thresholds** → Adott kvótahatár elérésekor, a rendszer hogyan reagáljon
 - **email kiküldése (mindkettőt is lehet)**
 - email küldése egy adminisztrátor felé
 - email küldése a user felé, aki túllépte a korlátot
 - **esemény naplózása**
 - hibajelzés küldése az eseménynaplóba
 - testreszabható log entry-vel! (amikor bekerül a log, annak formázását állíthatjuk) → MONITORING
 - **command**
 - parancs futtatása amikor valaki elér egy limitet
 - **reports**
 - riportokkal kapcsolatos beállítások

4.4.1.2. Quotas



Egy kvótát itt hozhatunk létre! Az alábbi lehetőségeket állíthatjuk be rajta!

- **Quota Path** → A megadott helyre kvóta beállítása, pl A Shares mappa!
 - Create quote on path → megosztási kvóta
 - Auto Apply template and create quotas on existing and new subfolders → felhasználói kvóta
- Kiválaszthatjuk a template-t amit használni szeretnénk rajta, vagy mi magunk módosítjuk ott!

Eredmények:

Filter: Show all: 1 items					
Quota Path	% Us...	Limit	Quota Ty...	Source Template	Match Temp...
Source Template: 5KB Limit (1 item)					
C:\Shares\HR	60%	5.00 KB	Hard	5KB Limit	Yes

Teszteljük le az adott beállításokat! Nyissuk meg a másik szervet és kezdjünk el fájlokat létrehozni! Most jelenleg csak a HR részlegre érvényes a kvóta! Nézzük meg, mit tudunk elérni!

Mint az a lenti képen jól látható 4 mappa létrehozása után, már meg is telt a tárhely... (Egy picit feljebb fogom tenni a kvótahatárt, mert jegyzettömbre sem tudtam menteni)

The screenshot shows two windows. On the left, a 'Disk Space' dialog box titled 'Out of Disk Space' indicates there is not enough space on 'Shares (\WIN-GRAL4662T9O)'. It shows a yellow folder icon labeled 'Shares' with the path '\WIN-GRAL4662T9O', type 'File folder', and date modified '2022. 03. 19. 8:14'. Below it, a green recycle bin icon is shown with the text 'Free up space from this disk and try again: Shares'. At the bottom are 'Try Again' and 'Cancel' buttons. On the right, the Windows Event Viewer shows an 'Application' log with 692 events. One specific event is highlighted: 'Event 12325, SRMSVC' under the 'General' tab, which details a quota exceeded warning for user 'TEMALAB\HR_User1' on share 'C:\Shares\HR'.

Level	Date and Time	Source	Event ID	Task Category
Warning	3/20/2022 5:06:40 PM	SRMSVC	12325	None
Warning	3/20/2022 5:02:51 PM	SRMSVC	12325	None
Information	3/20/2022 4:56:05 PM	SceCli	1704	None
Warning	3/20/2022 4:50:40 PM	SRMSVC	12317	None
Error	3/20/2022 4:43:17 PM	SRMSVC	12344	None
Error	3/20/2022 4:25:06 PM	SRMSVC	12344	None
Error	3/20/2022 4:07:27 PM	SRMSVC	12344	None
Information	3/20/2022 3:55:12 PM	HHCTRL	1904	None
Information	3/20/2022 3:55:12 PM	HHCTRL	1904	None
Information	3/20/2022 3:55:12 PM	HHCTRL	1904	None
Information	3/20/2022 3:55:12 PM	HHCTRL	1904	None
Information	3/20/2022 3:55:12 PM	HHCTRL	1904	None

Nézzük meg az "**Event Viewer**"-t hogy lássuk azt, hogy ténylegesen elkezdte logolni a kvótát! Mint az a fenti képen is látható **SRMSVC** kódnéven (*ServerResourceManagerService*). Mint a figyelmeztetésnél látható, jelez nekünk, hogy ezen felhasználó túllépte a megadott kvóta küszöböt! Az-az a beállítások működnek!

Ha a másik kvótázási metódust választjuk "**Auto Apply template and create quotas on existing and new subfolders**" akkor a "Shares" mappát kiválasztva végigpásztázza a mappa tartalmát, majd külön külön beállít rájuk 500KB-s kvótát! (IT és HR mappára)

Quota Path	% Used	Limit	Quot...	Source Templ...	Match Te...	Description
Source Template: 500KB Limit (3 items)						
C:\Shares*	---	500 KB	Hard ...	500KB Limit	Yes	
C:\Shares\HR	41%	500 KB	Hard	500KB Limit	Yes	
C:\Shares\IT	0%	500 KB	Hard	500KB Limit	Yes	

4.4.2. File Screening Management (Fájl szűrés menedzsment)

4.4.2.1. File Groups

Itt tudjuk megmondani a fájl csoportokat. Az-az mi számít pl audió és videó fájlnak. (kiterjesztések)

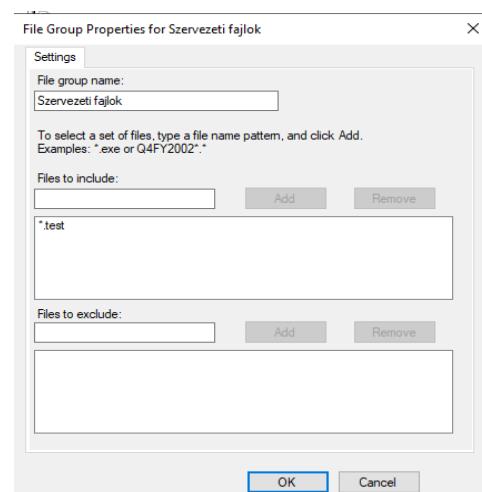
File Groups	Include Files	Exclude Files
Audio and Vid...	*.aac, *.aif, *.aiff, *.ASF, *.ASX, *.AU, *.avi, *.f...	
Backup Files	*.bak, *.bck, *.bkf, *.old	
Compressed F...	*.ace, *.arc, *.arj, *.bhx, *.bz2, *.cab, *.gz, ...	
E-mail Files	*.eml, *.idx, *.mbox, *.mbx, *.msg, *.oft, *...	
Executable Files	*.bat, *.cmd, *.com, *.cpl, *.exe, *.inf, *.js,...	
Image Files	*.bmp, *.dib, *.eps, *.gif, *.img, *.jfif, *.jpe...	
Office Files	*.accdb, *.accde, *.accdr, *.accdt, *.adn, *...	
System Files	*.acm, *.dll, *.ocx, *.sys, *.vxd	
Temporary Files	*.temp, *.tmp, ~*	
Text Files	*.asc, *.text, *.txt	
Web Page Files	*.asp, *.aspx, *.cgi, *.css, *.dhtml, *.hta, *....	

Mi magunk is definiálhatunk file groupokat. Amiknek a tartalmuk a következő.

- **File Group Name** → Amivel jellemizzük a fájlcsoportot
- **Files to include** → Mik azok a kiterjesztések, amik bele tartoznak ebbe a csoportba
- **Files to exclude** → A fenti állításnak az ellentetje

Ennél a pontnál érdemes szerintem rengeteg időt rászánni arra, hogy ténylegesen végig gondoljuk mik azok a dolgok, amiket majd be fogunk állítani.

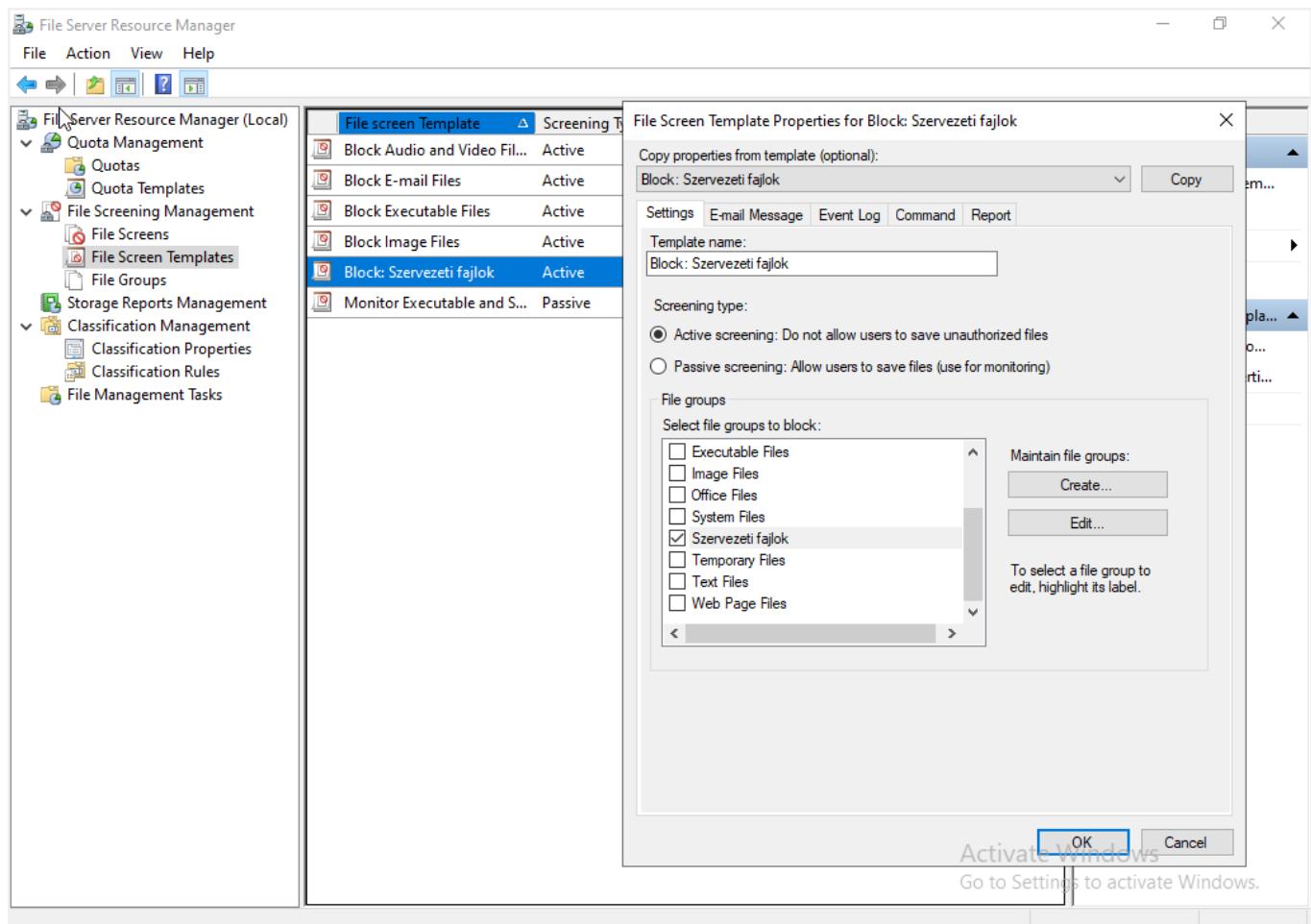
Általában véve az exclude files részét nem szokták kitölteni, csak ha az include files résznél úgy írjuk meg a parancsokat, hogy esetlegesen úgy is tudja értelmezni a dolgokat. Az-az ha pl *.t*t írok be, akkor a txt, text és társait is ebbe a csoportba tenném bele, ami nem lenne jó ötlet! Inkább írjuk bele szépen mik azok a kiterjesztések, amik ténylegesen ide tartoznak.



4.4.2.2. File Screen Templates

Ennél a lehetőségnél sémákat hozhatunk létre. Pl blokkoljuk az email típusú fájlokat! De mi magunk is létrehozhatunk egyet, amiknél ezeket állíthatjuk be

- **Settings fülön**
 - **Template Name** → Séma típusa, pl Block: Szervezeti fajlok
 - **Screening type** → Maga a szűrés típusa
 - **Active Screening** → Aktív szűrés (Ne engedjük a felhasználókat ezen fájlok létrehozására)
 - **Passive Screening** → Passzív szűrés (Engedjük a felhasználókat ezen fájlok létrehozására → monitorozás szempontjából ez hasznos)
 - **File Groups** → Itt választhatjuk ki a sémára illő fájl csoportokat, pl szervezeti fájlok
- Email-message, event log, command, report fülök egyeznek a kvóta menedzsmentben leírtakkal, így ezt most tükröztem ide is! (Csak logolom az eseményeket!)

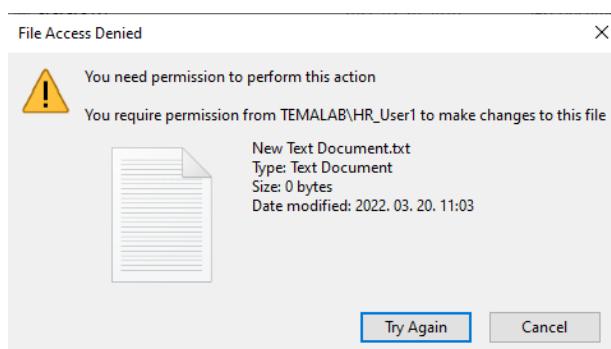


4.4.2.3. File Screens

Itt tudunk hasonló módon, úgy mint a kvótánál létrehozni szűrési képeket! Itt kétféleképpen tudunk létrehozni fájlszűrést. Ennek kétféle módja van.:

- **Create File Screen → Fájlszűrés létrehozása**
- **Create File Screen Exception → Fájlszűrési kivétel létrehozása**

A két lehetőség között csak annyi a különbség, hogy ha mondjak létrehozom a Shares mappára azt a szűrési feltételt, hogy blokkolom a szervezeti fájlokat és emellé a HR→TEST mappára állítok egy másik szűrési módot, akkor azon a mappán belül a .test kiterjesztű fájlokat létre fogom tudni hozni! Az előbbi képen a HR mappában próbáltam egy .test file-t létrehozni!



Az alsó képnél pedig a TEST mappában létre tudunk hozni szervezeti fájlokat! Az-az működött a FSM beállításunk! :)

Ezeket a beállításokat elég szépen lehet kombinálni akár, ezzel egészen szép ökoszisztemát lehet teremteni.

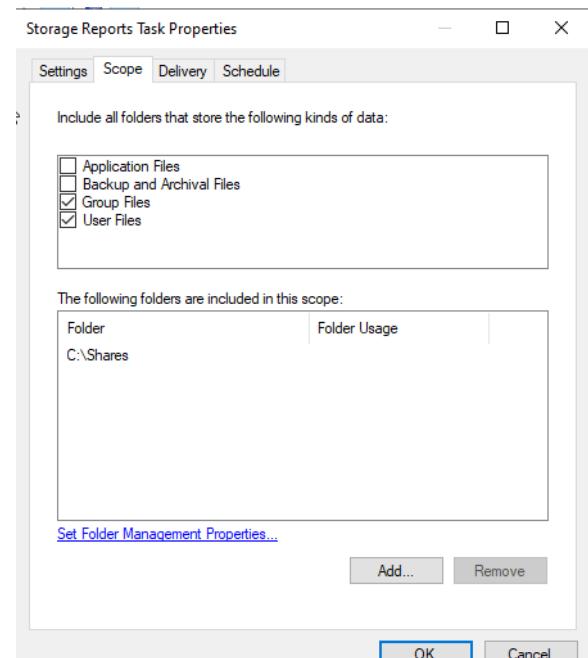
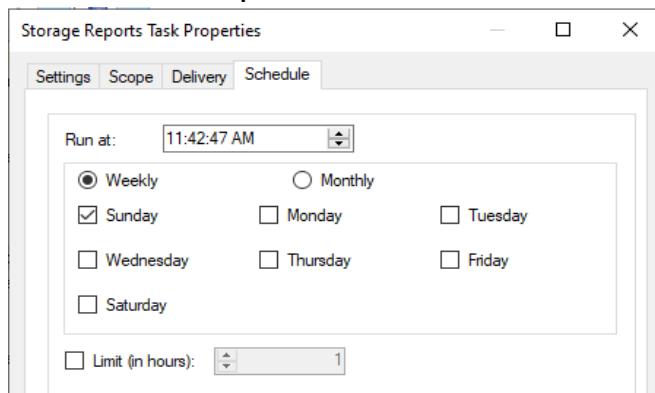
File Explorer View			
Name	Date modified	Type	Size
New Text Document.test	2022. 03. 20. 11:04	TEST File	0 KB

4.4.3. Storage Reports Management (Riport menedzsment)

Itt tudunk kimagasztásokat generálni. Ez monitorozási szempontból egész hasznos! Hiszen nem fogunk minden áldott nap a szerver teremben tevékenykedni, hogy megnézhessük, hogy mondjuk a beállított kvóta esetében ki hogyan halad, vagy a fájlszűrési beállítások, hogyan működnek most, jelen esetben.

Schedule a new report task lehetőséget választva hozzunk létre egy riportot, amiben a kvótákat figyelhetjük meg!

- **Settings fülön**
 - **Report Name** → Riport neve, pl Quota riport
 - **Report Data** → Amilyen adatokat szeretnénk riportolni, azaz információkat gyűjteni, pl kvótáról, fájl szűrésekről stb...
 - **Report Formats** → Amilyen típusban elkészíti a riportokat
- **Scope fülön**
 - Mik azok a mappák, amiket a látókörünkbe tesszük
 - Miket vegyük figyelembe
 - Alkalmazás fájlok
 - Mentések és archivált fájlok
 - Csoport fájlok
 - Felhasználói fájlok
- **Deliver fül az teljesen megegyezik a fenti két módszerben lévő információkkal**
- **Schedule fülnél adhatjuk meg, hogy milyen időközönként fusson le a riport!**



Az eredmény pedig itt látható:

Quota Usage Report Generated at: 3/20/2022 11:27:11 AM	
Report Description:	Lists the quotas that exceed a certain disk space usage level. Use this report to quickly identify quotas that may soon be exceeded so that you can take the appropriate action.
Machine:	WIN-GRAL4662T90
Report Folders:	'Group Files ()', 'User Files ()', 'C:\Shares'
Parameters:	Minimum Quota used percent: 0%

[Quota Usage Report Table of Contents](#)

[Report Totals](#)
[Report statistics](#)

Report Totals					
Quotas shown in report		All quotas matching report criteria			
Quotas	Total Usage	Quotas	Total Usage		
2	0.21 MB	2	0.21 MB		

[To top of the current report](#)

Report statistics						
Folder	Owner	Quota	Usage	Used	Peak Usage	Peak Usage Time
c:\shares\HR	TEMALAB\PJYRWJ	0.49 MB	0.20 MB	41.80 %	0.40 MB	3/20/2022 10:01:57 AM
c:\shares\IT	TEMALAB\PJYRWJ	0.49 MB	0.00 MB	0.20 %	0.00 MB	3/20/2022 10:01:13 AM

[To top of the current report](#)

Az eredményről teljes egészében leolvashatóak az eredmények! Azok a dolgok, amiket beállítottunk a kvóta menedzsment részénél, annak az eredménye itt is megjelent! :) Így ezzel a feladattal is készen vagyunk!

5. Group Policy szolgáltatások

Mi is az a GP?

A Group Policy az egy olyan szolgáltatás, amelyen belül szabályozhatjuk a felhasználók és a számítógépek munkakörnyezetét. Az-az itt kezelhetjük és konfigurálhatjuk a beállításokat.

Mi is az a GPO?

A Group Policy Object az egy olyan csoportházirend objektum/konténer ami több policy beállításokat tartalmat. Ez a GPO társítható/csatolható (link) (létrehozásakor, vagy már létezőt is csatolhatunk) AD konténerekhez, webhelyekhez, tartományokhoz, OU-khoz.

Hogyan kerül érvényre a GPO, az-az hogyan néz ki a GPO hierarchikus sorrendje? LSDOU

- Local GPO-k
- Site-level GPO-k
- Domain-level GPO-k
- OU GPO-k, beleértve az al OU-kat

Ezen hierarchikus sorrend alapján kerül feldolgozásra a GP!

Alkalmazhatunk Policy beállításokat ugye számítógépekre és felhasználókra! Ezeknek az érvényre jutása így néz ki.:

Computer Configuration → Rendszer Indulásakor, majd 90-120 percenként frissül

User Configuration → Bejelentkezéskor, majd 90-120 percenként frissül

A GPO tartalma 2 helyre kerül eltárolásra:

- **GPC** → *Group Policy Container*
 - Egy olyan konténer, ami az AD_DS-n keresztül kerül tárolásra, ami tartalmazza a verzió információkat
- **GPT** → *Group Policy Template*
 - A SYSVOL könyvtárban kerül elmentésre, ami tartalmazza a GP beállításokat

GPCM segítségével (Group Policy Management Consol) tudjuk a GPO-kat

- *Lementeni (Backup)*
- *Visszaállítani (Restore)*
- *Másolni (Copy)*
- *Importálni (Import)*

Tudjuk szabályozni pl az OU-ra a precedencia sorrendet, hogy melyik GPO jusson érvényre, ha számunkra a default hierarchia sorrend éppen nem megfelelő. (LSDOU)

Tudunk blokkolni, esetleg erőltetni is GPO-t! Az erőltetett GPO felülírja a blokkolt GPO-t! Valamint az erőltetett GPO, az alacsonyabb rendű GPO-kat felülbírálja!

Mi is az a Loopback Policy?

Lehetővé teszi a felhasználói csoportházirend-beállítások alkalmazását a számítógép alapján, amelyre a felhasználó bejelentkezett. Ennek két módja van

- **Replace Mode**
 - A felhasználói beállítások felülírásra kerülnek
 - Magyarán, amikor egy user bejelentkezik, akkor az Ő-hozzá tartozó GPO-k nem fognak érvényre jutni, hanem a számítógép fogja a felhasználói policy-keket betölteni, a saját számítógép objektumából.
- **Merge Mode**
 - A felhasználói beállítások összevonásra kerülnek
 - Magyarán, amikor egy user bejelentkezik, akkor az Ő-hozzá tartozó GPO-k és a Számítógép Objektumából származó GPO-k kerülnek érvényre (összevonásra). → User GPO nyer általában

Mitől is más? Ugye alapértelmezetten a felhasználói GPO-k jutnak érvényre, a felhasználók esetében. Itt viszont megoldhatjuk azt, hogy egy számítógép alapú GPO legyen érvényben a felhasználói helyett.

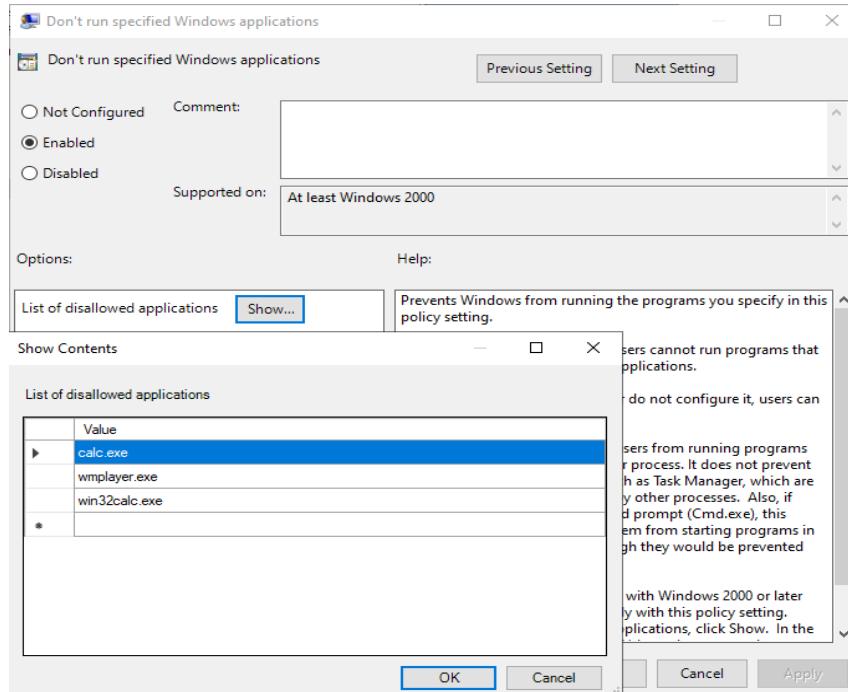
5.1. Media Player és a Calculator letiltása GP alatt

Hozzunk létre egy GPO-t a GPM-ben! A Group Policy Objects konténernél hozzuk létre az “Új” GPO-t!

A neve, legyen.:.

- **Media Player and Calculator Disable Policy**

Majd a létrejött GPO esetében az “Edit” gombra kattintva, állítsuk be azt, hogy az MediaPlayer és a Calculator-t ne lehessen elindítani! Ehhez, navigálunk... User Configuration → Administrative Templates (ADMX files) → System majd válasszuk ki a “Don’t run Specified Windows Applications”, majd az alábbi adatokat állítsuk be!



Miután beállítottuk ezt a GPO-t rendeljük hozzá a Tartományhoz!

The screenshot shows the 'Media Player and Calculator Disable Policy' delegation dialog in the Group Policy Management Editor. The 'Scope' dropdown is set to 'temalab.bprof'. The 'Group Policy objects' list contains several policies: 'Calculator only Policy', 'Default Domain Controllers Policy', 'Default Domain Policy', 'Media Player and Calculator Disable Policy', 'StartMenu Design HR Policy', and 'StartMenu Design HR Policy'. A purple arrow points from the 'temalab.bprof' entry in the left navigation pane to the 'Select GPO' dropdown in the dialog.

Jogosultsága! Ennek révén fogják tudni csak a Userek felvenni a GPO-t! A Scope alatt nézzük meg, hogy ténylegesen ott van ez a felhasználó! Bár, akire feladjuk az “**Apply Group Policy**” jogot, az biztosan bekerül a “**Security Filtering**”-be!

Fontos lépés, hogy engedélyezzük ezt az opciót! Annyit megjegyezlek, hogy az AppLock számonra nem akart működni... Akárhogyan is próbálkoztam, de nem akarta. Azt tudom, hogy lehet benne pl olyat is csinálni, hogy adott típusú EXE fájlokat ne lehessen futtatni. Pl installer!

A “**List of disallowed applications**” résznél, a “**Show...**” lehetőséget kiválasztva, szépen beleírjuk azokat az alkalmazásokat, amiket mi nem szeretnénk, hogy a felhasználó futtathassa! Fontos megjegyezni, hogy “**path**” azért nem fog ide kelleni, mert az OS a folyamatokat figyeli és annak alapján, ha mi megpróbálnánk egy ilyen exe fájlt elindítani, akkor azt nagyon magas eséllyel nem fogja engedni, mert tiltólistán van!

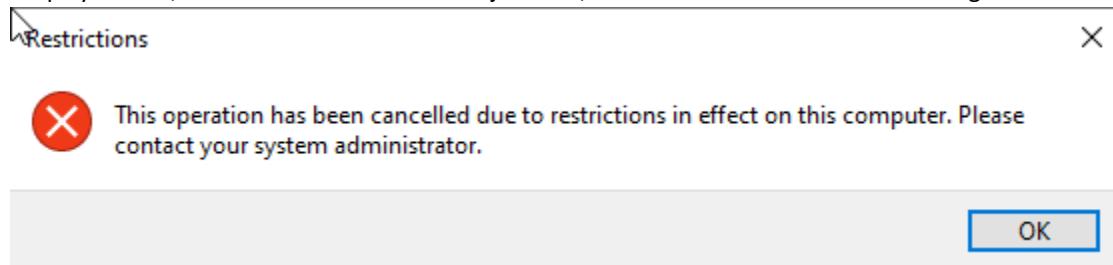
Fontos megjegyeznem, hogy ez a lehetőség nem működne telepítőkkel! Erre tényleg az AppLocker lenne a megoldás!!! Ebben az esetben, viszont pedig ez! (Elvileg)

Azért ide kellene rendelnünk, mert számunkra nagyon fontos lenne az, hogy ez a beállítás TARTOMÁNY szinten alkalmazódjon! Ez azt jelenti, hogy hierarchikusan lefelé, minden egyes OU-nak, Sites-nak belekerül! Az-az mindenire érvényre jut!

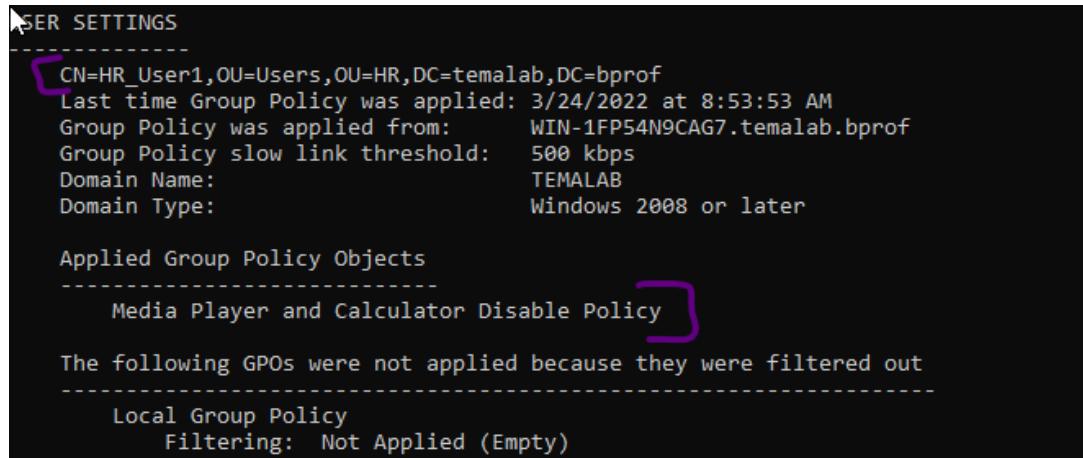
A következő lépésekben foglalkozunk kell a jogokkal! Már mintazzal, hogy a delegálást beállítjuk! Sajnos előfordulhat olyan eset, hogy nem kerül valami rendesen beállításra!

Ehhez a Delegation fülön ellenőrizzük le, hogy az Authenticated Users-nek van olvasás és apply group policy

Teszteljük le! Ehhez elindítottam a másik szervert, majd HR_User1 fiókba belépve próbáljuk meg elindítani a cal.exe-t, wmpplayer.exe-t, win32calc.exe-t! Ha minden jól ment, akkor ennek az ablaknak kellene fogadnia!



Ha ezt az ablakot kapjuk, akkor valóban sikerült a beállítás. (sikerült, ezzel a módszerrel) De, ha nem vagyunk biztosak abban, hogy a sors miatt nem engedte-e elindítani, akkor egy cmd program megnyitásával ezeket az adatokat kellene vissza kapnunk a **gpresult /r** parancssal!



Mint az jól látható, az "Applied Group Policy Objects" résznél valóban megjelenik az a GPO amit beállítottunk! Tehát, nem történt hallucinálás!

GUI alternatívaként a rsop.msc alkalmazást kell megnyitni!

(Ha a beállítások nem lennének aktívakkor a "**gpupdate /force**" parancsot írjuk be!)

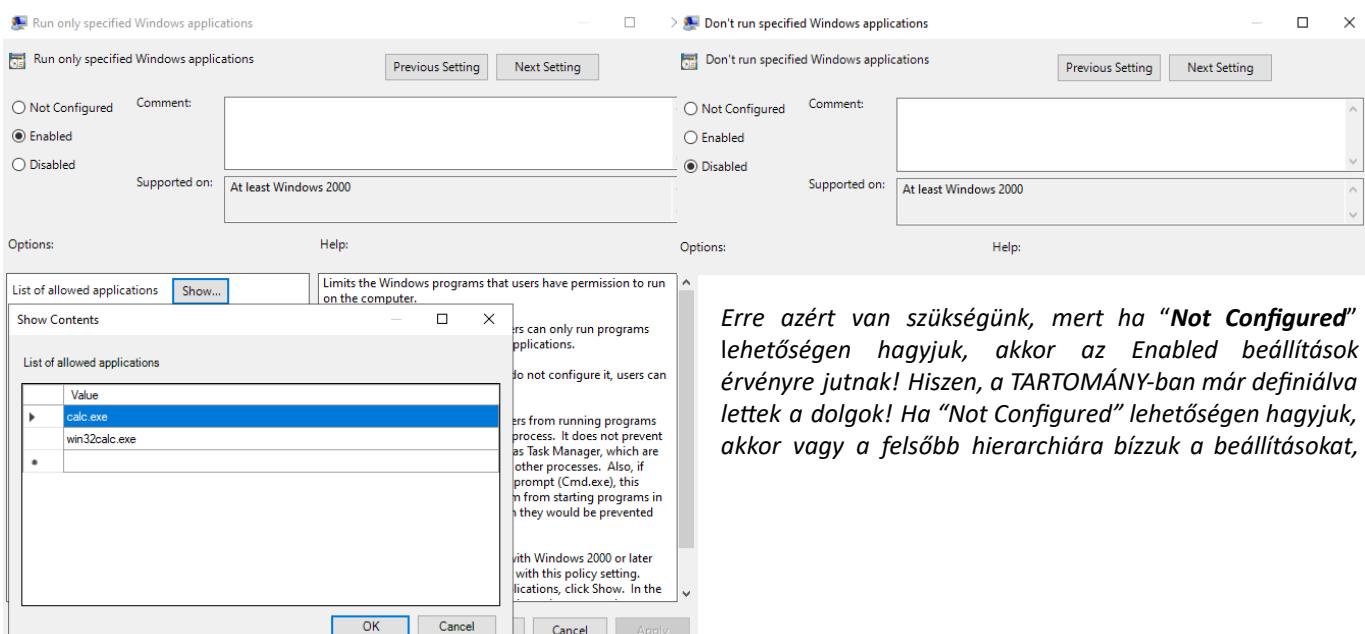
5.2. Calculator Only felhasználói

Állítsuk be, mondjuk a HR_User2-nek azt, hogy Ő egy Calculator Only felhasználó! Az-az ezen felhasználó csak a számológép alkalmazását nyithatja meg! Semmi más!

Ehhez nyissuk meg a Group Policy Manager alkalmazást. A Group Policy Objects konténernél hozzuk létre az "Új" GPO-t!

A neve, legyen.:

- **Calculator Only Policy**
- Majd a létrejött GPO esetében az "**Edit**" gombra kattintva, állítsuk be azt, hogy a Calculator-t lehessen CSAK elindítani! Ehhez, navigálunk... **User Configuration** → **Administrative Templates (ADMX files)** → **System** majd válasszuk ki a "**Run Only Specified Windows Applications**" lehetőséget, majd az alábbi adatokat állítsuk be! És a "**Don't run Specified Windows Applications**" tiltsuk le!



Erre azért van szükségünk, mert ha "Not Configured" lehetőségen hagyjuk, akkor az Enabled beállítások érvényre jutnak! Hiszen, a TARTOMÁNY-ban már definiálva lettek a dolgok! Ha "Not Configured" lehetőségen hagyjuk, akkor vagy a felsőbb hierarchiára bízzuk a beállításokat,

vagy ha nem volt a felsőbb hierarchiában, akkor letiltásra kerül! Számunkra, azért kell tehát ezt a funkciót kikapcsolni, mert nem szeretnénk azt, hogy a felsőbb hierarchia beleszóljon a futtatható alkalmazásokba, mert így ha "Not Configured" lenne, akkor sem tudnánk elindítani a calc.exe-t a win32calc.exe-t! Szóval, állítsuk be "Enabled"-re és akkor biztosan a mi GPO-nk fog dominálni! (LSDOU)

Most, a Delegation oldalt módosítanunk kell! Azt nem szeretnénk, hogy minden Authentikált felhasználó felvehesse ezt a GPO-t, hiszen azt mondta, hogy most HR_User2 lesz a Calculator Only fiók! Ehhez a Authenticated Users-től el kell venni azt a jogot, hogy felvehetik ezt a GPO-t! Adjuk hozzá ellenben HR_User2-t és adjuk meg neki ezeket a jogokat! (Scope → Security Filtering-ben így csak Ő LESZ BENNE) Valamint a HR → Users OU-ba rendeljük hozzá ezt a GPO-t! Az eredmény, tehát...

The screenshot shows the Group Policy Management console. On the left, under 'Forest: temalab.bprof', there's a tree view with 'Domains' expanded, showing 'temalab.bprof' which contains 'Default Domain Policy', 'Media Player and Calculator Disable Policy', 'Domain Controllers', 'HR' (which contains 'Users' and 'Calculator only Policy'), 'IT' (which contains 'Users'), and 'Group Policy Objects' (which contains 'Calculator only Policy', 'Default Domain Controllers Policy', 'Default Domain Policy', and 'Media Player and Calculator Disable Policy'). A purple bracket highlights the 'Calculator only Policy' node under 'HR'. On the right, a detailed view of the 'Calculator only Policy' is shown. It has tabs for 'Scope', 'Details', 'Settings', 'Delegation', and 'Status'. Under 'Scope', it says 'These groups and users have the specified permission for this GPO'. Under 'Groups and users:', there's a table:

Name	Allowed Permissions
Authenticated Users	Read
Domain Admins (TEMALAB\Domain Admins)	Edit settings, delete, modify security
Enterprise Admins (TEMALAB\Enterprise Admins)	Edit settings, delete, modify security
ENTERPRISE DOMAIN CONTROLLERS	Read
SYSTEM	Edit settings, delete, modify security
User Name 2 (TEMALAB\HR_User2)	Read (from Security Filtering)

Ha megnézzük HR_User1-t számára akkor tehát erre a GPO-ra "Denied" kellene írnia, hiszen Ő nem veheti fel! Az eredmény...

```

CN=HR_User1,OU=Users,OU=HR,DC=temalab,DC=bprof
Last time Group Policy was applied: 3/24/2022 at 8:59:43 AM
Group Policy was applied from: WIN-1FP54N9CAG7.temalab.bprof
Group Policy slow link threshold: 500 kbps
Domain Name: TEMALAB
Domain Type: Windows 2008 or later

Applied Group Policy Objects
-----
    Media Player and Calculator Disable Policy

The following GPOs were not applied because they were filtered out
-----
    Local Group Policy
        Filtering: Not Applied (Empty)

    Calculator only Policy
        Filtering: Denied (Security)

```

Most lépjünk át a HR_User2-be! (Mivel sajnos, tényleg minden letiltottam ott, és csak a calculator indul el, így sajnos nem tudok cmd-s ablakot mutatni, ahol tényleg beállítódik a GPO erre, de erre is van egy b lehetség, ezt majd lentebb leírom!) Ott tényleg elindul a calculator. Azért nem fogok képet lőni róla, mert erre már nem fontos! Csinálunk egy GPR-t! (Group Policy Results)

Ez arra lesz jó nekünk, hogy megbizonyosodjunk arról, hogy tényleg az adott GPO került alkalmazásra! A Group Policy Results Wizard-ban kiválasztjuk a másik számítógépet és a HR_User2 felhasználót. Ekkor az eredmény...

The screenshot shows the 'Settings' tab of the Group Policy Results wizard. Under 'Policies', 'Administrative Templates' is selected. In the 'System' section, there's a table:

Policy	Setting	Winning GPO
Don't run specified Windows applications	Disabled	Calculator only Policy
Run only specified Windows applications	Enabled	Calculator only Policy
List of allowed applications	Source GPO	
calc.exe	Calculator only Policy	
win32calc.exe	Calculator only Policy	

Mint látható, az LSDOU miatt, itt a "Winning GPO" a "Calculator only Policy" lesz! Az-az szépen beállítottuk a dolgokat!

5.3. Start Menu konfiguráció Calculator Only fiókra

A feladat annyit kér, hogy a Start Menü-t szabjuk testre! Jelen esetben én csak annyit tettem meg, hogy A Calculator ki lett Pin-ve a HR_User2-nek!

Nyissunk egy PowerShell-t a AD_DS szerveren, majd adjuk ki ezt a parancsot.:

- **Export-StartLayout -Path C:\Users\PJYRWJ\Desktop\desktop.xml**

Ekkor az asztalra desktop.xml fájlnévként kerül elmentésre! Én, erre állítottam be a file-t!



```
<LayoutModificationTemplate xmlns:defaultlayout="http://schemas.microsoft.com/Start/2014/FullDefaultLayout" xmlns:start="http://schemas.microsoft.com/Start/2014/Start ^
<LayoutOptions StartTileGroupCellWidth="6" />
<DefaultLayoutOverride>
<StartLayoutCollection>
<defaultlayout:StartLayout GroupCellWidth="6">
<start:Group Name="Calculating">
<start:DesktopApplicationTile Size="2x2" Column="0" Row="0" DesktopApplicationLinkPath="%windir%\system32\win32calc.exe" />
</start:Group>
</defaultlayout:StartLayout>
</StartLayoutCollection>
</DefaultLayoutOverride>
</LayoutModificationTemplate>
```

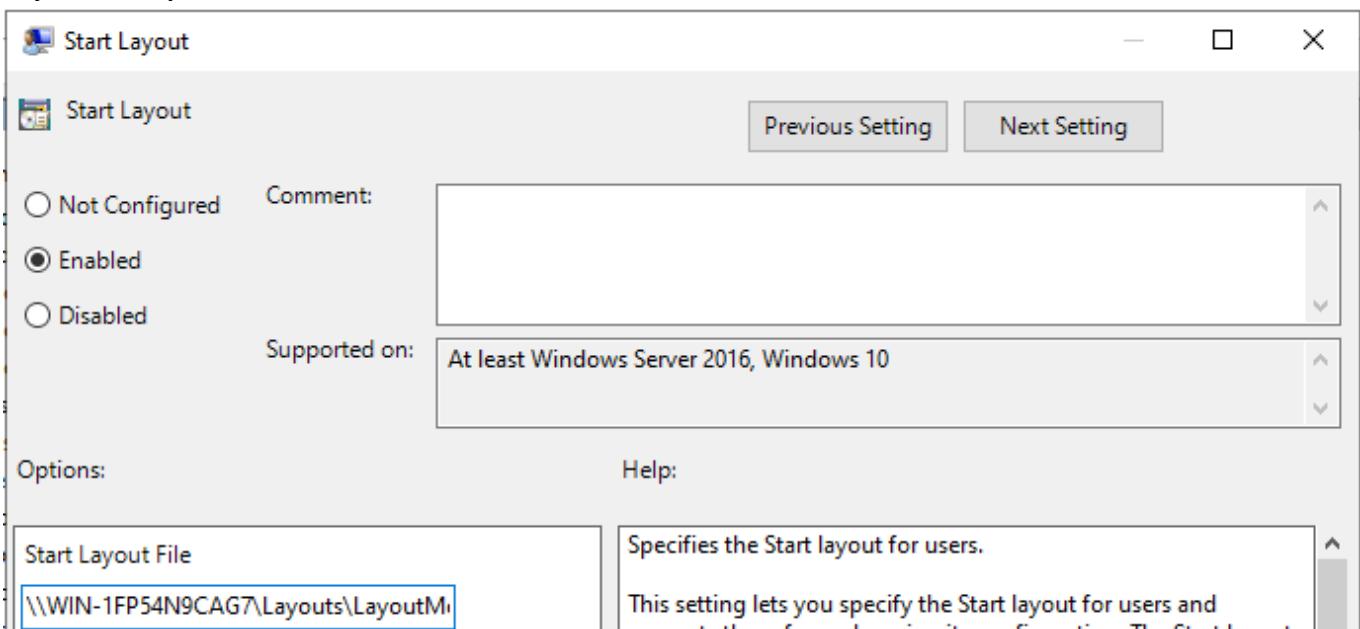
Így a Calculator alkalmazás kerül ki pinelve a felhasználó Start Menüjére! Természetesen a tálcára is lehetne pinelni. Valamint még 1-2 dolgot testre lehet szabni, de számomra ennyi is elég volt...

Elmentés után, menjünk vissza a GPM-hez és szeressük a “**Calculator Only**” GPO-t! Navigálunk a

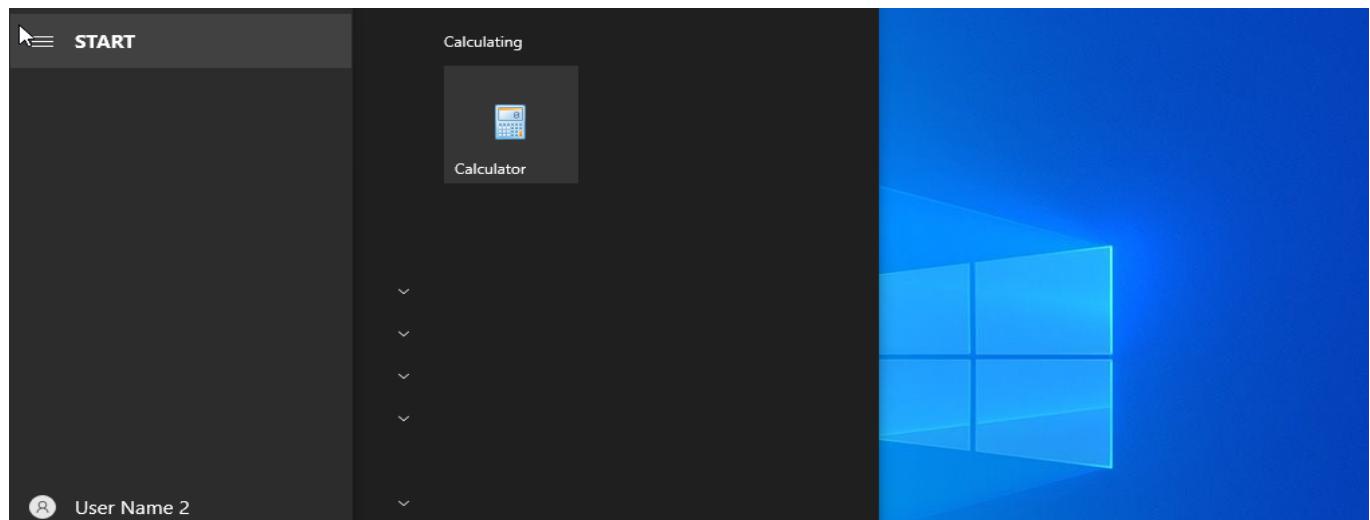
- **User Configuration → Administrative Templates → Start Menu and Taskbar → Start Layout** lehetőségre, majd

Hozzunk létre egy Layouts folder-t egy tetszőleges helyen az AD_DS-n, majd osszuk meg a mappát, hogy ehhez hozzá tudjon majd férni a másik fél! (CSAK OLVASÁSRA)

Majd a Start Layout-t eszerint állítsuk be.:



Ekkor, bejelentkezve a HR_User2 fiókba, ha minden jól csináltunk, akkor csak ennek kell megjelennie!



5.4. Loopback Policy működése

A definíciót, már fentebb definiáltam. Tesztelni azért nem tudom, mert bármit létrehozok, arra már nem szeretne történni semmi sem! Ezt a részt, emiatt nem tudtam tesztelni.

6. Group Policy Preferences szolgáltatások

6.1. Miért használjuk? Mit tud?

Sok IT karrieres ember esetében előfordulhat olyan eset, amikor hálózati meghajtót csatolunk fel a felhasználóknak! Ezt meg lehet oldani "**Logon Scriptekkel**". Ehhez viszont az IT szakembernek meg kell írnia, valamint debuggálnia kell, tárolnia azt a scriptet egy központi helyen, valamint azt futtatni User GPO-k által. Most ezeket az eseteket is, amik ehhez hasonlók, gondoljuk ide! (PolicyPak)

Egy egyszerű, központi rendszer amiben konfigurálhatjuk és telepíthetjük ezeket a módosításokat anélkül, hogy a könnyen elfejezhető és a rögtön dokumentált, elszórt változtatásokkal foglalkoznánk, hiszen minden bizonnal ez a módszer segítene csökkenteni a költségeket és megkönnyítené az IT-s munkáját.

- Nehezebb programkódot írni és debuggálni, de ez leginkább az újoncoknak okozhat problémát
- Moderált szintű kódolás és logikai szint szükséges, hogy bizonyos beállításokat beállíthassunk egyes emberekre vagy számítógépekre
- Szkriptek alkalmazásához szükséges kijelentkeztetni a felhasználókat
- GP-k periodikusan kerülnek érvényre! (fentebb leírva, mennyi időközönként vagy esetben frissül / "gpupdate /force" kényszerítés, ami lehetne REMOTE IS)
- Group Policy Preferences beállítások már akkor érvényre jutnak, amikor megírod a változtatásokat!
- A GPP lehet aközben is, miközben a felhasználó be van jelentkezve (bármilyen biztonsági kontextusban)
- Könnyebben állítható GUI alatt

Minden egyes beállítás esetében 4 alapműveletet tudunk definiálni a preferences beállításakor!

- **Create** → Létrehozás
- **Update** → Frissítés
- **Delete** → Törlés
- **Replace** → Cserélés

6.2. Group Policy Preferences vs Group Policy Settings (Policies)

Group Policy Preferences

- A preferenciák nem érvényesülnek
- UI nem letiltott
- Könnyen elkészíthető preferencia elemek a registry beállításokról, fájlokról és még sok egyéb másról
- Lehetőséget biztosít registry beállítások vagy egy egész registry ágak importálására lokálisan vagy remote hozzáférésen keresztül
- Nem elérhető a Local Group Policy-n
- Egy egészen barátságos GUI-t kínál
- Felhasználó belenyúlhat

Group Policy Settings (Policies)

- A beállítások érvényesülnek
- UI tiltott
- Policy hozzáadása alkalmazás támogatást és adminisztratív template-k létrehozását igényli
- Nem lehet Policy beállításokat létrehozni ahhoz, hogy fájlokat, mappákat menedzseljünk
- Elérhető Local Group Policy-n
- Alternatív UI-t biztosít a legtöbb Policy beállításokhoz
- Felhasználó nem nyúlhat bele

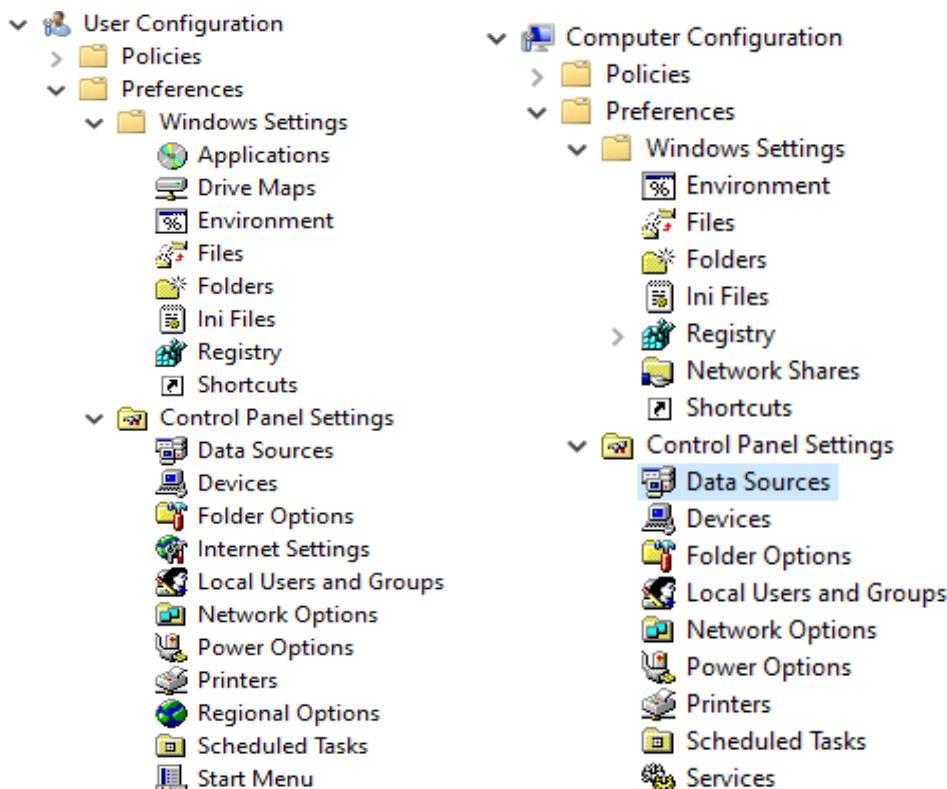
6.3. Group Policy Preferences lehetőségek

A GPP-t két oldalról lehet konfigurálni! Lehetséges ugyanúgy felhasználói illetve számítógép szinten GPP-t beállítani!

Nézzük meg, röviden, hogy milyen lehetőségeink vannak a felhasználói oldalról.:

- **Windows beállítások**
 - Applications : Alkalmazások → Erről nincsen információm
 - Drive Maps : Csatolt mappa → Konfigurálhatjuk a megosztott mappákat
 - Environment : Környezeti változó → Definiálhatjuk a környezeti változókat felhasználók és számítógép szintjén
 - Files : Fájlok → Fájlokkal való műveletek (erről majd később)
 - Folders : Mappák → Mappákkal való műveletek
 - Ini Files : Inicializálós fájlok → Ez komolyabb téma, de ebbe most nem megyek bele
 - Registry → Registry beállítások kezelése
 - Shortcuts : Parancsikonok → Parancsikkal való beállítások
- **Control Panel Settings : Vezérlőpult beállítások**
 - Data Sources : Adatforrások → Nem megyek bele
 - Devices : Eszközök → Eszközökkel kapcsolatos beállítások (mit használhat, mit nem)
 - Folder Options : Mappa beállítások → (rejtett fájlok, kiterjesztés stb...)
 - Internet Settings : Internetes beállítások → (IEexplorer)
 - Local Users and Groups : Lokális felhasználók és csoportok és beállításaik
 - Network Options : Hálózati beállítások → VPN és Dial Up beállítások
 - Power Options : Energiaellátási Beállítások → Ismerős? Teljesítménycentrikus stb...
 - Printers : Nyomtatók → Megosztott, Lokális nyomtatók stb beállítása
 - Regional Options → Regionális beállítások (nyelv stb)
 - Scheduled Tasks → Ütemezett feladatok beállítása
 - Start Menu → Start menüvel kapcsolatos beállítások

Van még számítógépes oldal is, de azt most nem részletezném! Helyette itt is lenne a két lista felhasználói és számítógépes oldalról!



A kiválasztott vizsgálandó elemek.:

User Configuration részből.:

- Power Options (Control Panel Settings)
- Shortcuts (Windows Settings)

Computer Configuration részt nem tudom tesztelni, mert nincsen Computer objektumom.

6.4. Power Options a HR-eseknek

Hozzunk létre a HR felhasználóknak egy Teljesítmény beállítást! Az alábbiakat állítsuk be!

- Név.: **HR_SUPER_ENERGY_SETTINGS_FOR_USERS**
- Set as the active Power Plan → **Beállítjuk aktív Teljesítménynek!**
- Additional Settings
 - Require Password on Wakeup (kelljen-e jelszó ha felébresztjük a gépet)
 - On battery : NO → Akkumulátorról
 - Plugged : NO → Áramellátásról
- Display
 - Turn off Display After (mennyi idő múlva kapcsoljon ki a kijelző)
 - On battery : 0 minutes (az-az soha)
 - Plugged : 0 minutes (az-az soha)

Egy ugyanilyen POWER OPTION-t létrehoztam véletlenül! **HR_SUPER_ENERGY** néven! (Hiszen "Create" módban módosítottam, így ezzel létrehozta újra, más névvel)

Az eredmény a másik szerveren!

The screenshot shows the Windows Control Panel under 'Power Options'. The main window title is 'Power Options'. The left sidebar lists options like 'Choose what the power buttons do', 'Create a power plan', and 'Choose when to turn off the display'. The central area is titled 'Choose or customize a power plan' and describes power plans as collections of hardware and system settings. It shows three plans:

- HR_SUPER_ENERGY_SETTINGS_FOR_USERS** (selected): Described as 'Automatically balances performance with energy consumption on capable hardware.'
- High performance**: Described as 'Favors performance, but may use more energy.'
- Balanced (recommended)**: Described as 'Automatically balances performance with energy consumption on capable hardware.'

At the bottom, there's a 'Tix' watermark. On the far left, a tree view shows 'User Configuration' and 'Control Panel Settings' expanded, with 'Power Options' selected. A small window titled 'Power Plan (At least Windows 7) Properties' is open at the bottom, showing 'Advanced settings' tab with various power management options like 'Stop processing items in extension on error' and 'Run in user's context'.

Mint az jól látszik, teljes mértékben egy hagyományos GUI-t látunk! Lényegében illeszünk tudunk beállítani akár magunknak is egy személyi számítógépnél, amikor hozzáadunk egy Power Options-t!

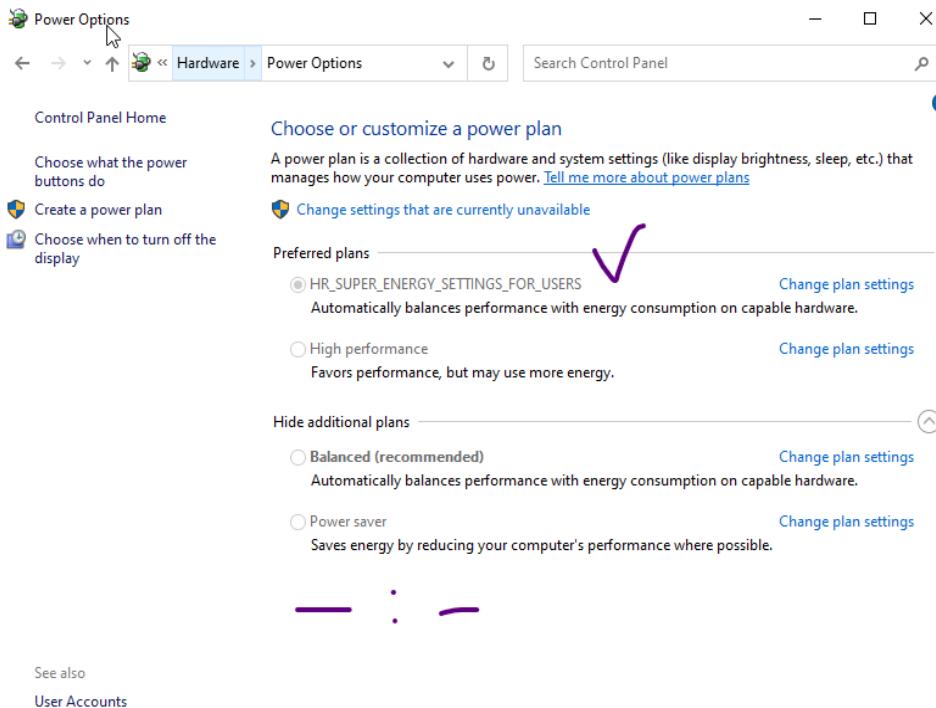
Minden egyes menüpont esetében ugyanilyesmi panel-t láthatunk! Tehát ténylegesen egy egyszerű,

tiszta felületet kapunk! (Bár, generálható ebből XML kód is)

Javítsuk ki a problémát! Azaz, hogy létrehozunk egy power options-t DE “**DELETE**”-re állítjuk! Majd ezeket állítsuk be még!

- Név.: **HR_SUPER_USERS** → Ezt szeretnénk törölni!

Majd a másik gépnél gpupdate /force paranccsal ezt az eredményt kell látnunk!



Az-az sikerült a törlésünk a gépről!

Igazából innentől kezdve törölhető az a Preferences! És elég csak ezt megtartanunk!

Bár, elvileg megtehetnénk azt, hogy egy Preferences-re beállítjuk azt, hogy csak 1x futassa le ezt a Preferences-t, majd többször már ne! így nem fog lefutni minden egyes login után fölöslegesen ez a preferences!

Ezt a Policy-t a HR OU-ban helyeztem el! A Policy neve pedig.: **HR_USERS_POWER_PLAN POLICY**

A következő feladatban, Shortucot fogunk beállítani mondjuk az IT Usereknek! Tételezzük fel, hogy szeretik az “logout.hu” szaki oldalt!

6.5. Shortcuts az IT-soknak

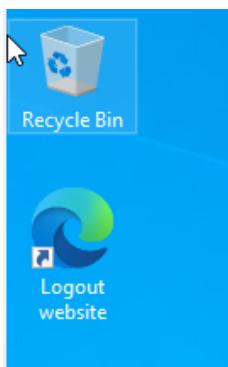
Hozzuk létre ezt a User GPO-t az alábbi adatokkal és dolgokkal...

- GPO neve → **IT_USERS_SHORTCUT POLICY**
- Majd a GPO-t linkeljük a IT OU-hoz!

Szerkessük ezt a Policy-t majd a **User Configuration → Preferences → Windows settings → Shortcuts** résznél adjunk hozzá egy új “**Shortcut**”-t és az alábbi adatokat adjuk meg!

- Action típusa → Create
- Name → Logout website
- Target Type → Legyen URL
- Location → Legyen Desktop
- Target URL → <https://logout.hu>
- Shortcut key → Shift + L
- Common fűl
 - *Apply once and do not reapply* lehetőség kiválasztása → Egyszer alkalmazza ezt a lehetőséget, többször nem. minden felhasználónál egyszer lefut, többször nem! Ha letörököm, akkor soha nem kapom vissza... :(
 - *Ha viszont azt szeretnénk, hogy mindig ott maradjon, akkor a fenti opción ne pipáljuk be!*

Eredmény:



Mint az jól látható, létrejött a Shortcut az asztalon, azzal a névvel amivel mi szerettük volna! Sőt, még “**Shortcut Key**” kombinációra is reagál!

Tehát a Group Policy Preferences-ben illesmi lehetőségeket tudunk beállítani! Nyilván, ennél mélyebben is el lehet mélyedni ezekben a funkciókban, de én próbáltam olyan funkciókat megmutatni, amiket jobban lehet demonstrálni és könnyebb is!

A Computer Configuration részét, azért nem tudom megcsinálni, mert az OU-khoz nincsen rendelve Számítógépes Objektum! Ez önmagában nem azt jelenti, hogy az adott Userek nem jelentkezhetnek be

az adott gépeken, hanem csak annyit, hogy nem tudunk így csatolni Computer Configuration GPO-kat, hiszen nem tagja ezeknek a OU-knak! (Nincsenek abban a hierarchiákban a Computer Objectek)

7. Biztonsági naplózás (AUDIT)

7.1. User Login/out AUDIT Policy létrehozása

A mostani feladatban azt fogjuk beállítani, hogy amikor egy felhasználó, vagy bárki más, aki bejelentkezik a gépre, vagy kijelentkezik, arról szóló információ az megjelenjen!

Hozzunk létre a Group Policy Management felületén egy új GPO-t! Majd az alábbi helyen állítsuk be a dolgokat.:)

Computer Configuration → Policies → Windows Settings → Security Settings → Advanced Audit Policy Configuration → Audit Policies résznél az alábbi dolgokat állítsuk be.:)

- **Account Logon → Audit Kerberos Service Ticket Operations** : Ezt a jegyet kérjük el a felhasználóktól, majd naplózzuk ezeket, csak ami sikeresen létrejött : Success
- **Account Logon → Audit Kerberos Authentication Service** : Felhasználói fiók authentikálásakor keletkezett logokat naplózzuk. (ez más eszköz miatt fog nekünk kelleni, majd lentebb kifejtem) Success, Failure
- **Logon/Logoff → Audit Logoff** : Success
- **Logon/Logoff → Audit Logon** : Success, Failure

Majd, miután ezt megcsináltuk, teszteljük le a bejelentkezést a másik gépen! Próbálunk meg hibásan belépní többször és be és kijelentkezni sikeresen! A fő gépen az **Event Viewer → Windows Logs → Security** résznél ezt kellene látnunk!

The screenshot shows three windows from the Event Viewer:

- Windows Logs - Security**: A list of audit events. The first event (Event ID 4771) is highlighted. It details a Kerberos pre-authentication failure for user 'IT_User3' on service 'krbtgt/TEMALAB'. The event includes account information, service information, network information, additional information, and certificate information.
- Event 4771, security-Auditing**: A detailed view of the selected event. It shows the same information as the list, with 'IT_User3' circled in purple.
- Windows Logs - Security**: Another list of audit events. The second event (Event ID 4768) is highlighted. It details a Kerberos authentication ticket (TGT) request for user 'IT_User3' on service 'krbtgt/TEMALAB'. The event includes account information, service information, and network information.
- Event 4768, security-Auditing**: A detailed view of the selected event. It shows the same information as the list, with 'IT_User3' circled in purple.

Mint az a képeken látható. A DC szerveren sikeresen naplózásra került a 4 hibás bejelentkezási kísérlet a KAS segítségével! És szépen megjelenik a sikeres bejelentkezés is! A kérdés az, hogy miért nem ment a sima “**Logon Events**” segítségével? Miért nem jelenik meg?

7.2. Logon Events és Account Logon Events

Logon Events.:

- A ticketek a lokális gépen kerülnek auditálásra → Így a DC szervernek SOHA sem lesz rálátása a lokális ticketekre! (Kivéve ha ezt Event Subscription-nel kezeljük! Erre majd lesz egy példa)
- Így az olyan logok, mint a 4624,4625 (sikeres/sikertelen bejelentkezés) csak a LOKÁLIS GÉPEN KERÜLNÉK AUDITÁLÁSRÁ!
- ITT NEM JELENIK MEG A KERBEROS SZOLGÁLTATÁS, ÍGY SOHA NEM TUD KIJUTNI A LOG KÍVÜLRE!

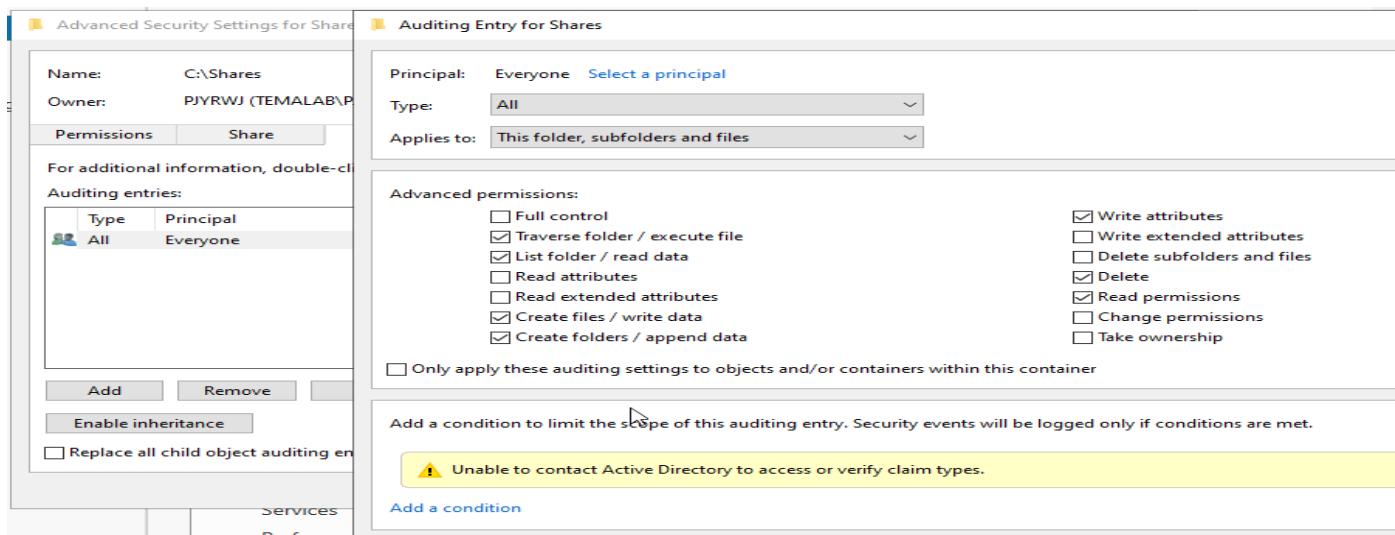
Account Logon Events.:

- A ticketek egy úgynevezett Kerberos szolgáltatás hatáskörébe fognak tartozni, az-az minden olyan eszközről, amin bejelentkezések fognak történni, azokat elküldi a DC szerverre! Úgynevezett Kerberos ticketek kerülnek kicserélésre! Ezen eventek konfigurálásakor, amikor egy kliens megpróbál bejelentkezni egy fiókba, vele együtt elküldi az Ő által generált eventet! Ez fog majd megjelenni a DC server Event Viewer felületén!

7.3. Megosztott mappán lévő műveletek AUDITálása

Fontos megjegyezni, hogy itt a megosztott mappán lévő műveleteket csak a MEMBERS szervernek kellene auditálnia! (De lehetőség szerint egy Event Subscription hatására bármikor gyűjthetjük ezen Eventeket!)

Lépjünk be a MEMBERS szerverre és jelentkezzünk be egy rendszergazdai fiókkal! (Én ezt a saját rendszergazdai fiókkal tettem meg)



Nyissuk meg a Shares mappának a “Properties” részét, majd menjünk el a “Security” fülre, majd az “Advanced” gombra nyomjunk rá, majd az “Auditing” fülönél állítsuk be a fenti dolgokat!

- Principal: Everyone → mindenkit szeretnénk auditálni
- Applies to → erre a mappára és az alsóbb mappákra és filek-ra! (Az egész fa struktúrán végig!)
- Advanced Permissions → mit szeretnénk auditálni!
 - Traverse folder / execute file → Amikor mappákon keresztül végig haladunk vagy fájlokat megnyitunk
 - List folder / read data → Amikor mappának a tartalmát listázzuk vagy az adatokat olvassuk
 - Create files / write data → Amikor fájlt hozunk létre vagy adatot írunk
 - Create folders / append data → Amikor mappát hozunk létre vagy adatot fűzünk hozzá valamihez
 - Write attributes → írási attribútumok
 - Delete → törlés
 - Read permissions → Olvasási jogok (granted ...)
- Amik nem lettek bekapcsolva, de érdekes lehet
 - Take ownership → Amikor valaki használati jogot elveszi
 - Change permissions → Amikor valaki jogokat állít (mappára, file-ra)
 - Delete subfolders and files → Nagyobb mappák esetén, a mellék mappák és fájlok törlésénél jelenik meg

A feladatunk az, hogy ha egy felhasználó (4. feladatban a shares mappa megosztásra került) valamelyen műveletet végrehajt a megosztott mappán belül az kerüljön auditálásra! (Olvasás, Írás, Módosítás, Törlés → CRUD)

Nyissuk meg a "gpedit.msc"-t vagy a "**Local Group Policy Editor**"-t és navigáljunk el a

- Computer Configuration → Windows Settings → Security Settings → Local Policies → Audit Policy
 - Audit Object Access → Success-re és Failure-re állítása!
- Computer Configuration → Windows Settings → Security Settings → Advanced Audit Policy Configuration → System Audit Policies ... → Object Access
 - Audit File System → Success-re és Failure-re állítása!
 - Ha egy objektum lezárásra kerül → **ID4658**
 - Ha egy objektumhoz hozzáférést kért valaki → **ID4656**
 - Ha egy objektumhoz hozzáférés történt → **ID4663**
 - Audit Handle Manipulation → Success-re és Failure-re állítása!
 - Ha egy objektumhoz magasabb hozzáférési szintet adunk → **ID4690**
 - Elvileg ezt nem kellene a mostani feladat szerint naplózni, de ha egy alacsonyabb szintű biztonsági szál vagy folyamat kapja meg az objektumhoz a jogot, akkor ezt zajnak kell vennünk!

Tesztelés képpen az AD_DS szerverre jelentkezzünk be, mondjuk "IT_User4" felhasználóval, majd lépjünk fel a megosztott mappára! (Elvileg már ilyenkor is generál logot, én ezt törltem kezdésként)

Első esetben hajtsunk végre mappa olvasást, majd fájl olvasást!

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	4/24/2022 7:08:27 AM	Microsoft Win...	4658	File System
Audit Success	4/24/2022 7:08:27 AM	Microsoft Win...	4656	File System
Audit Success	4/24/2022 7:08:27 AM	Microsoft Win...	4658	File System
Audit Success	4/24/2022 7:08:27 AM	Microsoft Win...	4690	Handle Manipulation
Audit Success	4/24/2022 7:08:27 AM	Microsoft Win...	4656	File System
Audit Success	4/24/2022 7:08:27 AM	Microsoft Win...	4658	File System

Event 4656, Microsoft Windows security auditing.

General Details

A handle to an object was requested.

Subject:

- Security ID: TEMALAB\IT_User4
- Account Name: IT_User4
- Account Domain: TEMALAB
- Logon ID: 0x2AC5D5

Object:

- Object Server: Security
- Object Type: File
- Object Name: C:\Shares\HR\asasasa.txt
- Handle ID: 0x212c
- Resource Attributes: -

Process Information:

- Process ID: 0x4
- Process Name: -

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	4/24/2022 7:22:54 AM	Microsoft Win...	4656	File System
Audit Success	4/24/2022 7:22:54 AM	Microsoft Win...	4658	File System

Event 4656, Microsoft Windows security auditing.

General Details

Access Request Information:

- Transaction ID: {00000000-0000-0000-0000-000000000000}
- Accesses:
 - SYNCHRONIZE
 - ReadAttributes
- Access Reasons:
 - 3820042577-1371130825-1255: SYNCHRONIZE: Granted by D:(A;ID;0x1200a9;;S-1-5-21-2864606760-3820042577-1371130825-1255)
 - 3820042577-1371130825-1255: ReadAttributes: Granted by D:(A;ID;0x1200a9;;S-1-5-21-2864606760-3820042577-1371130825-1255)
- Access Mask: 0x100080
- Privileges Used for Access Check: -
- Restricted SID Count: 0

Audit Failure 4/24/2022 7:31:09 AM Microsoft Win... 4656 File System

Audit Success 4/24/2022 7:31:03 AM Eventlog 1102 Log clear

Keywords	Date and Time	Source	Event ID	Task Category
Audit Failure	4/24/2022 7:31:09 AM	Microsoft Win...	4656	File System
Audit Success	4/24/2022 7:31:03 AM	Eventlog	1102	Log clear

Event 4656, Microsoft Windows security auditing.

General Details

Access Request Information:

- Transaction ID: {00000000-0000-0000-0000-000000000000}
- Accesses:
 - DELETE
 - SYNCHRONIZE
 - ReadAttributes
- Access Reasons:
 - 3820042577-1371130825-1255: DELETE: Denied by D:(D;ID:DCLCRPDTCRSDWDWO;;S-1-5-21-2864606760-3820042577-1371130825-1255)
 - 3820042577-1371130825-1255: SYNCHRONIZE: Unknown or unchecked
 - 3820042577-1371130825-1255: ReadAttributes: Granted by ACE on parent folder D:(A;OICI;0x1200a9;;S-1-5-21-2864606760-3820042577-1371130825-1255)

Mint az a képen is jól látszik, a fenti képen lévő HR mappában lévő fájlra, megkapjuk, hogy milyen jogaink is vannak ahhoz a fájlhoz! Mint az szemmel látható, tudjuk szinkronizálni és olvasni ezt a fájlt! Így ha ezen a fájlon én most valamelyen módosítást próbálnék végrehajtani, vagy azt a fájl törlni, akkor mivel ezen a két jogon kívül nemek nincsen jogom törlni és módosítani így azt én nem tehetem meg!

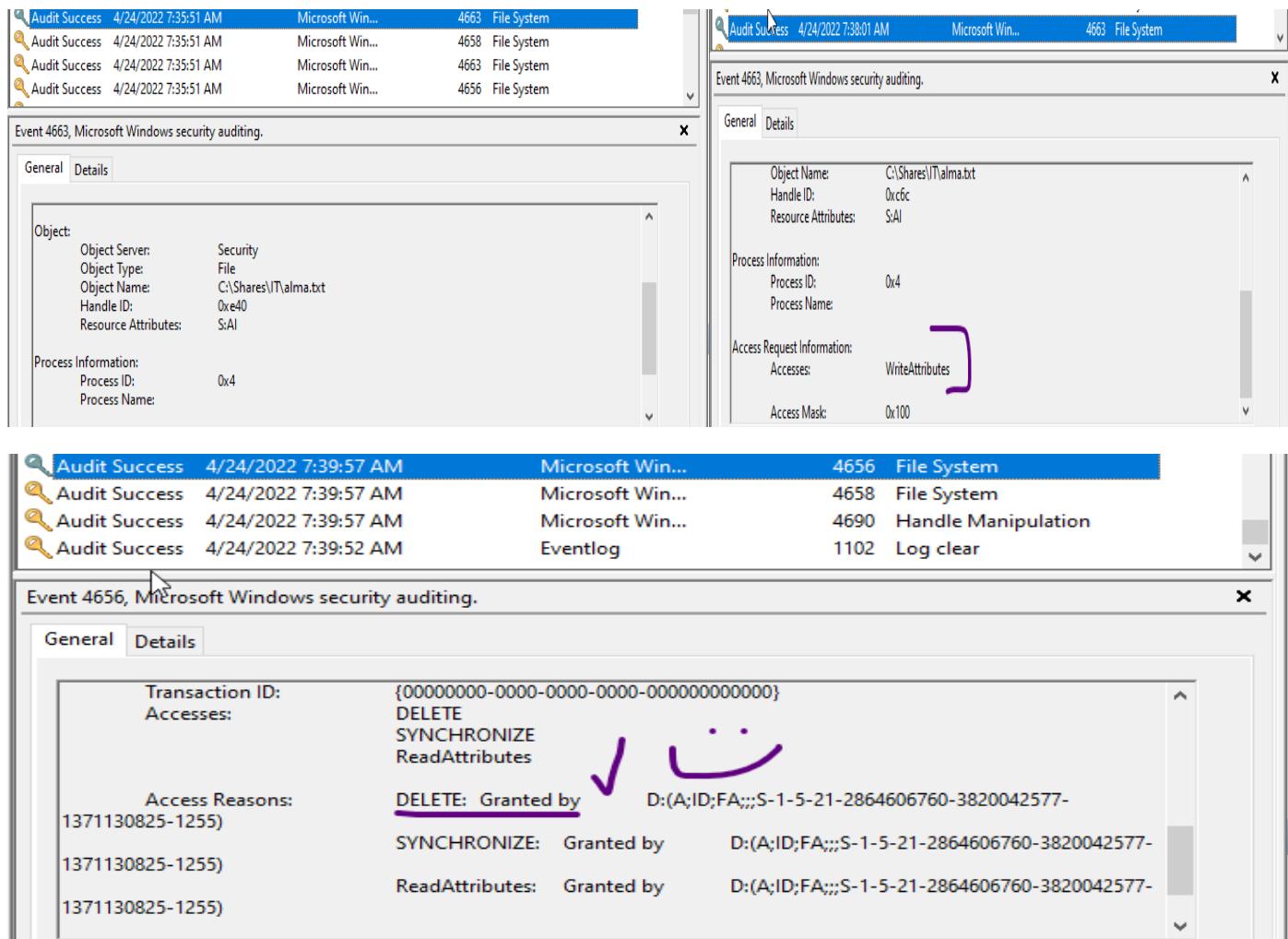
Ez nyilván egy HR felhasználó számára nem így nézne ki, hiszen Ő tudja módosítani és törlni is a saját mappájában lévő adatokat!

A következő feladat legyen az, hogy próbáljuk meg törlni ezt a fájlt!
Itt már tisztábban látható az, amiről fentebb beszéltem!

Mint az látható, megjelenik az “**Accesses**” részén a “**DELETE**” tag is! Ami lényegében azt jelenti, hogy a mi felhasználónk megpróbálta törölni azt a fájlt, amihez nincs is jog!

Ez már az “**Access Reasons: DELETE: Denied by**” résznél már le is olvasható, hogy MEG LETT TAGADVA A JOGUNK A FÁJL TÖRLÉSÉHEZ!

A következő feladatban az IT mappában fogok fájlt létrehozni, módosítani, törölni!



The screenshot shows the Windows Event Viewer interface. At the top, there are two event details windows. The left one is for Event ID 4663, titled "Event 4663, Microsoft Windows security auditing." It shows audit success logs for creating and modifying files in the C:\Shares\IT\ directory. The right one is for Event ID 4656, also titled "Event 4656, Microsoft Windows security auditing." It shows audit success logs for clearing the log and deleting files. Below these are the main log lists for each event type.

Event Type	Date	User	Process ID	File System
Audit Success	4/24/2022 7:35:51 AM	Microsoft Win...	4663	File System
Audit Success	4/24/2022 7:35:51 AM	Microsoft Win...	4658	File System
Audit Success	4/24/2022 7:35:51 AM	Microsoft Win...	4663	File System
Audit Success	4/24/2022 7:35:51 AM	Microsoft Win...	4656	File System

Event Type	Date	User	Process ID	File System
Audit Success	4/24/2022 7:39:57 AM	Microsoft Win...	4656	File System
Audit Success	4/24/2022 7:39:57 AM	Microsoft Win...	4658	File System
Audit Success	4/24/2022 7:39:57 AM	Microsoft Win...	4690	Handle Manipulation
Audit Success	4/24/2022 7:39:52 AM	Eventlog	1102	Log clear

Itt most törlök az IT mappából az alma.txt-t!

Mint a képen is lehet látni, itt már nem a denied by részt olvashatjuk le az eventről, hanem a “**DELETE: Granted by**” feliratot

7.4. Megosztott mappán lévő műveletek AUDITálása (Virtuális gépek gazdagépe szerint)

A gond ezzel a feladattal, a saját windows-unk! Vagyis a gazdagépen a “**Host Only Adapter**”-t a Windows az “**Public**”-nak veszi, amit módosítani sem tudunk, így bizonyos esetekben nem tudjuk elérni a virtuális gépeket!

Ehhez 2 dolgot kell tennünk, hogy publikus hálózatként is tudjuk használni a VM gépeket! (Jelen esetben elérni a SHARED folder!)

- Fokozott Biztonságú Windows Defender Tűzfal szabályokban egy bejövő szabályt létrehozni!
- Megbizonyosodni, hogy a VM gépek fel tudják oldani a gazdagép NETBIOS nevét! (Ezt meglépve, biztosan tudnak kommunikálni a VM gépek a gazdagéppel!)

Nyissuk meg a gazdagépen a Fokozott Biztonságú Windows Defender Tűzfal alkalmazást! Majd hozzunk létre itt egy bejövő szabályt!

- Egyéni szabály legyen
- minden programra terjedjen ki
- Bármely protokollra terjedjen ki
- A hatókör részén az alábbi dolgokat állítsuk be
 - Melyik “Helyi IP” címre vonatkozzon a szabály? (Ide a gazdagép “Host Only” kártyájának az IP címét kell beírni ÉS NEM A DHCP SZERVER CÍMÉT!)
 - Ez jelen esetben 192.168.7.101
 - Melyik “Távoli IP” címekre vonatkozik ez a szabály? (Ide a VM gépek IP címét kell beírni)
 - 192.168.7.1
 - 192.168.7.2
- Művelet részében az “**Engedélyezze a kapcsolatot**” lehetőség kiválasztása
- A szabály, minden profilra legyen érvényes (tartomány, személyes, nyilvános)
- Majd adjunk ennek a szabálynak valamelyen nevet! (Majd mentés)

Ellenőrizzük a VM gépeken, hogy sikerül-e feloldaniuk a VM gazdagép címét!

```
C:\Users\PJYRWJ>nbtstat -a 192.168.7.101
Ethernet:
Node IpAddress: [192.168.7.2] Scope Id: []
               NetBIOS Remote Machine Name Table

      Name        Type      Status
-----+-----+-----+
SMILE-ROLANDB <00>  UNIQUE   Registered
WORKGROUP     <00>  GROUP    Registered
SMILE-ROLANDB <20>  UNIQUE   Registered

MAC Address = 0A-00-27-00-00-08

C:\Users\PJYRWJ>
```

Mint az a képen látható, a nbtstat parancsot használtam a számítógépem NetBIOS nevének a feloldására! Látható, hogy teljesen más munkacsoportba tartozik, a VM-k által használt munkacsoportjához képest! (A feladat szempontja szerint a gépünk alkalmas arra, hogy teszteljük azt, hogy ha mi módosítunk valamit a Shared folderben az hogyan kerül auditálásra!)

Természetesen csináltam egy egyszerű pingelést a fő gépéről, hogy ez a másik irányban is ténylegesen működik és mind a 192.168.7.1 és a 192.168.7.2-s kliens-t is élérem! Kezdődjön akkor a megosztott mappához való felcsatlakozás!

Ehhez a gazdagépen nyissunk meg egy “**Fájlkezelőt**” majd írjuk be a megosztott mappához az elérési utat!
Ekkor a rendszer kér tőlünk azonosítást! Próbálunk meg mondjuk egy rendszergazdai fiókkal belépni!

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	4/24/2022 8:45:49 AM	Microsoft Win...	4690	Handle Manipulation
Audit Success	4/24/2022 8:45:49 AM	Microsoft Win...	4658	File System
Audit Success	4/24/2022 8:45:49 AM	Microsoft Win...	4656	File System
Audit Success	4/24/2022 8:45:49 AM	Microsoft Win...	4654	File System
Audit Success	4/24/2022 8:45:49 AM	Microsoft Win...	4690	Handle Manipulation
Audit Success	4/24/2022 8:42:30 AM	Eventlog	1102	Log clear

Event 4690, Microsoft Windows security auditing.

General Details

An attempt was made to duplicate a handle to an object.

Subject:

- Security ID: TEMALAB\PJYRWJ
- Account Name: PJYRWJ
- Account Domain: TEMALAB
- Logon ID: 0x388390

Source Handle Information:

- Source Handle ID: 0x2154
- Source Process ID: 0x4

Log Name: Security
Source: Microsoft Windows security
Event ID: 4690
Level: Information
User: N/A

Logged: 4/24/2022 8:45:49 AM
Task Category: Handle Manipulation
Keywords: Audit Success
Computer: WIN-GRAL4662T9O.temalab.bprof

Lényegében ugyanazt tudom tenni, mintha egy VM gépnél kezdeném el az adatokat módosítani!

Mint az a képen látható, ugyanazon dolgok fognak itt is megjelenni, mint amikor az IT_User4-el teszteltem a lépéseket!

Megjegyzés: Gyakran használnak “**Host Only**” adaptort VM alatt, hogy a gazdagép és a virtuális kliens között lehessen kapcsolatot felépíteni! Mint például webszerverek esetén. (apache és társai)

8. AD_DS Snapshot

8.1. Mi is az a Snapshot?

A Snapshot lényege az, hogy egy úgynévezett pillanatnyi képet készítsünk a rendszer adott állapotáról! (AD_DS) Általában ezt akkor szokták alkalmazni, ha valamilyen módosítást hajtunk végre az AD_DC-n!

Az alábbiakban az alábbi adatok kerülnek mentésre "Snapshot" létrehozásakor... Ilyen alkalommal csinál a rendszer egy "Shadow" copy-t azon meghajtóról, amin ezek megtalálhatóak:

- Adatbázis adatok
- Log adatok

A SNAPSHOT NEM ALKALMAS TÖRÖLT ADATOK VISSZAÁLLÍTÁSÁRA! Csak egy célra szolgál, hogy ezt a fát, visszafejthessük és az esetlegesen törölt dolgokat, mi magunk visszarakhassuk!

8.2. Snapshot létrehozása

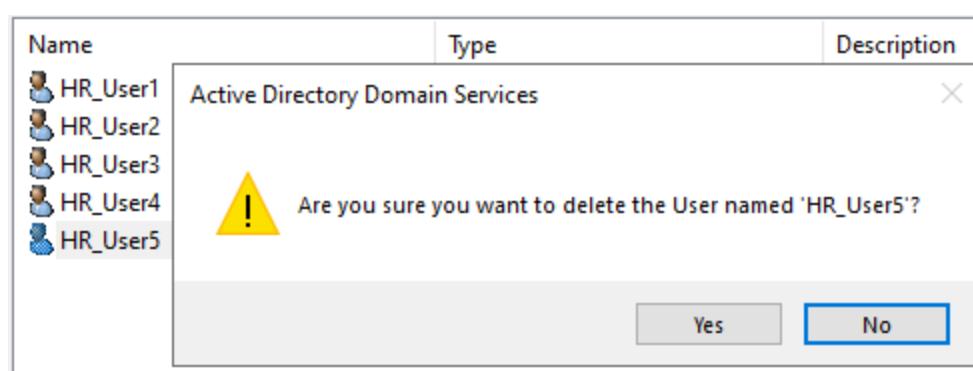
Ahhoz, hogy snapshotot tudunk készíteni, nézzünk át, 1-2 fontos dolgot. Nyissunk meg egy parancssort és írjuk be az ntdsutil.exe parancsot! Majd írjuk be a "snapshot" kulcsszót!

Majd futassuk le az alábbi parancsokat.:

- activate instance ntds → Az NT Directory Services részéről fogunk képet csinálni
- create → ezzel létre is hozzuk a snapshotot

```
snapshot: activate instance ntds
Active instance set to "ntds".
snapshot: create
Creating snapshot...
Snapshot set {5466ef48-cbf2-446c-8d93-5af2b9b3c9be} generated successfully.
snapshot: list all
1: 2022/04/10:11:20 {5466ef48-cbf2-446c-8d93-5af2b9b3c9be}
2: C: {afded583-2585-40e8-a153-cbcc5aad83c6}

snapshot:
```



Töröljünk le egy HR felhasználót a teszteléshez!

Majd pedig menjünk vissza a parancssorhoz és adjuk ki az alábbi parancsokat! Fontos megjegyezni, hogy a snapshotokat nem lehet visszatölteni! Csak megnézni lehet a tartalmukat! Elsősorban csatoljuk fel az elkészült snapshotot!

A további parancsok, tehát.:

- **mount <UID>** → Felcsatoljuk az azonosítóval ellátott "Snapshotot", {5466ef48-cbf2-446c-8d93-5af2b9b3c9be}

```
snapshot: mount {5466ef48-cbf2-446c-8d93-5af2b9b3c9be}
Snapshot {afded583-2585-40e8-a153-cbcc5aad83c6} mounted as C:\$SNAP_202204101120_VOLUMEC$\
```

```
File: $SNAP_202204101120_VOLUMEC$ 2022. 04. 10. 11:32 File folder 83 245 052 ...
```

Most pedig, hogy az AD_UC lássa egy porthoz felcsatoljuk a "Shadow" snapshotot!

Az alábbi parancshoz nyissunk egy másik CMD-t, majd adjuk ki az alábbi parancsot.:

- **dsamain /dbpath C:_\<datetime_volume>\windows\ntds\ntds.dit /ldapport 10048** → Hiszen ntds-ről csináltunk copy-t.

```
C:\Windows\system32>dsamain /dbpath C:\\$SNAP_202204101120_VOLUME\\$\\Windows\\NTDS\\ntds.dit /ldapport 10048  
EVENTLOG (Warning): NTDS General / Security : 3051  
The directory has been configured to not enforce per-attribute authorization during LDAP add operations.
```

For more information about the study, please contact Dr. Michael J. Hwang at (310) 794-3000 or via email at mhwang@ucla.edu.

For more information, please see <https://go.microsoft.com/fwlink/?linkid=2174022>

EVENTLOG (Warning): NTDS General / Security : 3054
The directory has been configured to allow implicit owner privileges when initially setting or modifying the nTSecurityDescriptor attribute during LDAP add and modify operations. Warning events will be logged, but no requests will be blocked.

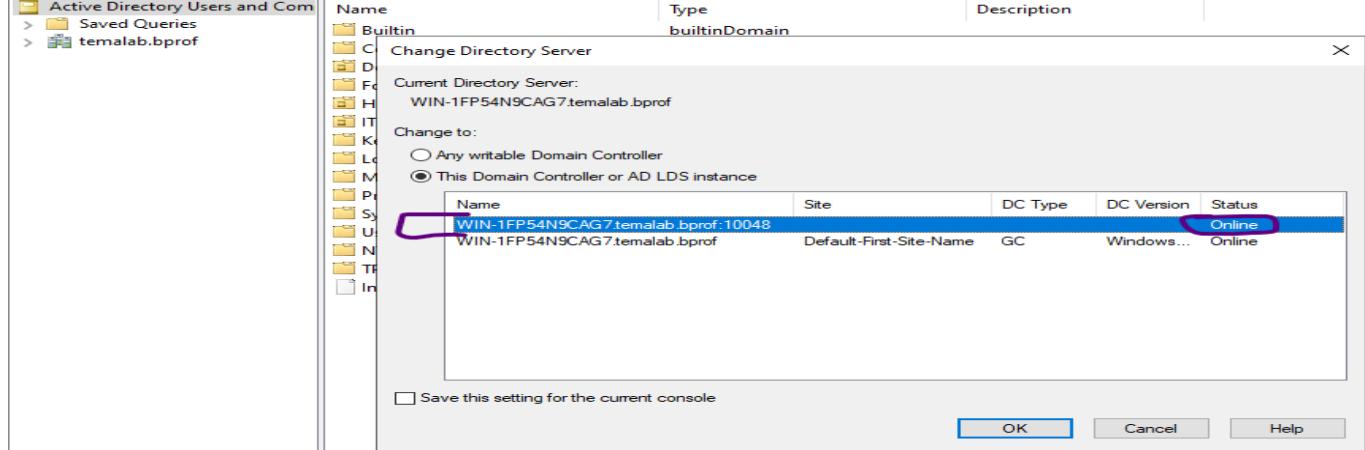
This setting is not secure and should only be used as a temporary troubleshooting step. Please review the suggested mitigations in the link below.

For more information, please see <https://go.microsoft.com/fwlink/?linkid=2174032>.

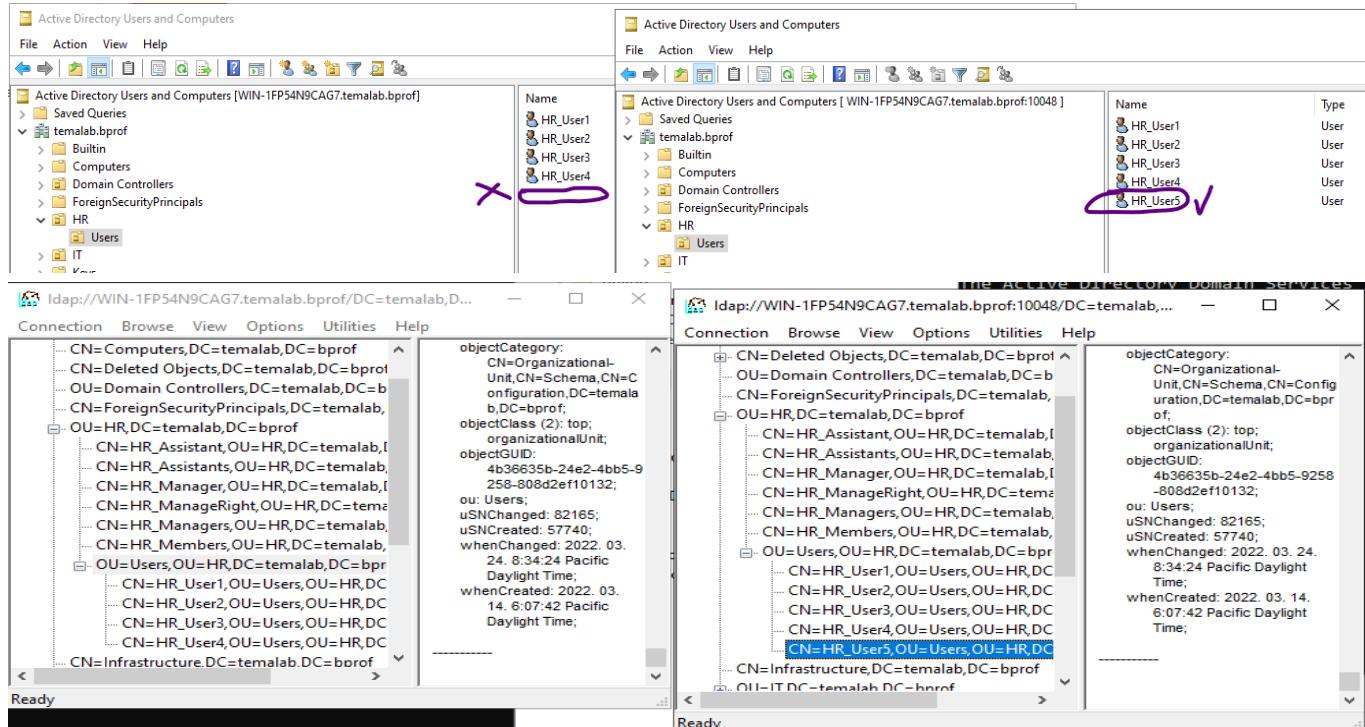
EVENTLOG (Informational): NTDS General / Service Control : 1000
Microsoft Active Directory Domain Services startup complete

Lépiünk át az AD-HC-re! És váltunk "Domain Controlers"-ek.

Lépjunk át az AD_UC-ra! Es valtsunk "**Domain Controller**" → Jobb kíkk az AD_UC-re!



Mint az alábbi képen látható, a snapshot, amit készítettünk, tényleg elmentette a dolgokat! Az-az visszaolvasható!



LDAP program segítségével ugyanazt a képet lehet látni. Itt mondjuk bonyolultabb az adat visszanyerése, de lényegében csak ennyit tudunk tenni.

9. Event Forwarding

9.1. Event Forwarding lényege

Az itt leírtak, csak a beállítás menetét tartalmazzák! A PPT-n kerül minden demonstrálásra! Részletesebben bemutatva!

Mi is az "Event Forwarding"? Mi ennek a lényege?

Az "Event Forwarding" lényege, hogy egy központosított, vagy "Collector" számítógép felé kerüljenek továbbításra a forrás, vagy "Source" számítógépek felől érkező, "Collector" által definiált "Subscription" beállítások révén kijelölt "Eventek".

Lényegében a "Source" számítógépek továbbítják a "Subscription"-k által definiált "Event"-ket (logokat) a Collector szerver felé!

- **Collector Server** → Aki begyűjt a források "Event"-it a "Subscription"-k segítségével!
- **Source's** → Azon kliensek/szerverek akik feliratkoznak egy "Subscription"-re, majd a feliratkozás hatására továbbítják a "Subscription" által definiált "Event"-ket

Az Event Forwarding az alábbi lépésekkel áll:

- WinRM szolgáltatás beállítása
- GPO létrehozása az "Event"-ek megfelelő továbbításához
- Event Log Readers csoporthoz felhasználók hozzárendelése
- Event Subscription beállítása
 - Login/out AUDIT begyűjtés
 - Shared folder CRUD AUDIT begyűjtés
- Event Subscription finomhangolása

9.2. WinRM szolgáltatás beállítása

Első lépésként állítsuk be a "Collector"-t! Nevezük ki az AD_DS szerverünket erre a szerepre! Nézzük meg, hogy a WinRM aktív-e!

Nyissunk meg egy PowerShell alkalmazást! Majd az alábbi parancsot adjuk ki!

```
PS C:\Windows\system32> Test-WSMan

wsmid          : http://schemas.dmtf.org/wbem/wsman/identity/1/wsmanidentity.xsd
ProtocolVersion : http://schemas.dmtf.org/wbem/wsman/1/wsman.xsd
ProductVendor   : Microsoft Corporation
ProductVersion  : OS: 0.0.0 SP: 0.0 Stack: 3.0
```

Mint a képen látható, a WinRM szolgáltatás fut! És a MEMBERS szerveren is ezt a parancsot kiadva, ugyanazt adja ki!

```
PS C:\Windows\system32> winrm qc
WinRM service is already running on this machine.
WinRM is already set up for remote management on this computer.
PS C:\Windows\system32>
```

Még a QuickConfig is szól nekünk arról, hogy ez konfigurálva van! Viszont régebbi szervereken előfordulhat az, hogy ezen szolgáltatás nem aktív!

Teszteljük le a WinRM szolgáltatást a MEMBERS szerverről! Adjuk ki az alábbi parancsot!

Viszont a következő lépésekben biztosan beállítjuk a WinRM-t is!

```
PS C:\Windows\system32> Invoke-Command -ComputerName WIN-1FP54N9CAG7 -ScriptBlock {1}
1
PS C:\Windows\system32>
```

Mint látható visszakapjuk eredményként az 1-t! (ScriptBlock) segítségével! Ha viszont a WinRM nem futna egyik/másik oldalról, akkor az alábbi képet kapjuk!

```
PS C:\Windows\system32> Invoke-Command -ComputerName WIN-1FP54N9CAG7 -ScriptBlock {1}
[WIN-1FP54N9CAG7] Connecting to remote server WIN-1FP54N9CAG7 failed with the following error message : Access is denied. For more information, see the about_Remote_Troubleshooting Help topic.
+ CategoryInfo          : OpenError: (WIN-1FP54N9CAG7:String) [], PSRemotingTransportException
+ FullyQualifiedErrorId : AccessDenied,PSSessionStateBroken
PS C:\Windows\system32>
```

Másik gép

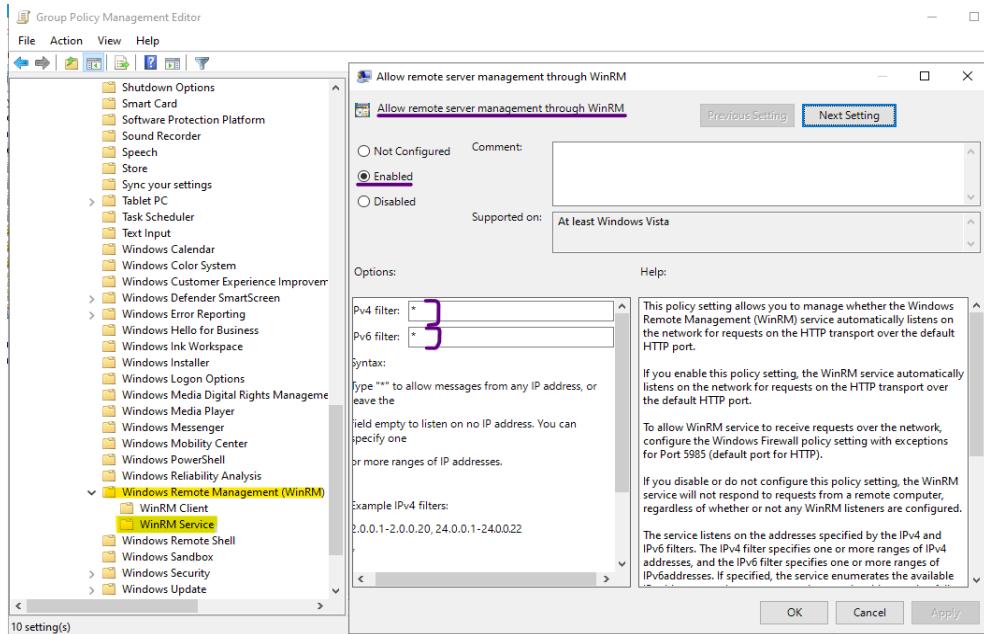
Ha a Remote Be rende lehetséges

9.3. GPO létrehozása az “Event”-ek megfelelő továbbításához

Nyissuk meg a “Collector” szerveren a Group Policy Management szolgáltatást! Majd hozzunk létre egy GPO-t! És linkeljük a Domain-hez!

Az alábbi helyeken állítsuk be a dologokat.:

- Computer Configuration > Policies > Administrative Templates > Windows Components > Windows Remote Management (WinRM) > WinRM Service



Itt azt állítjuk be, hogy a WinRM az IPv4 és IPv6-s kapcsolaton keresztül is működjön.

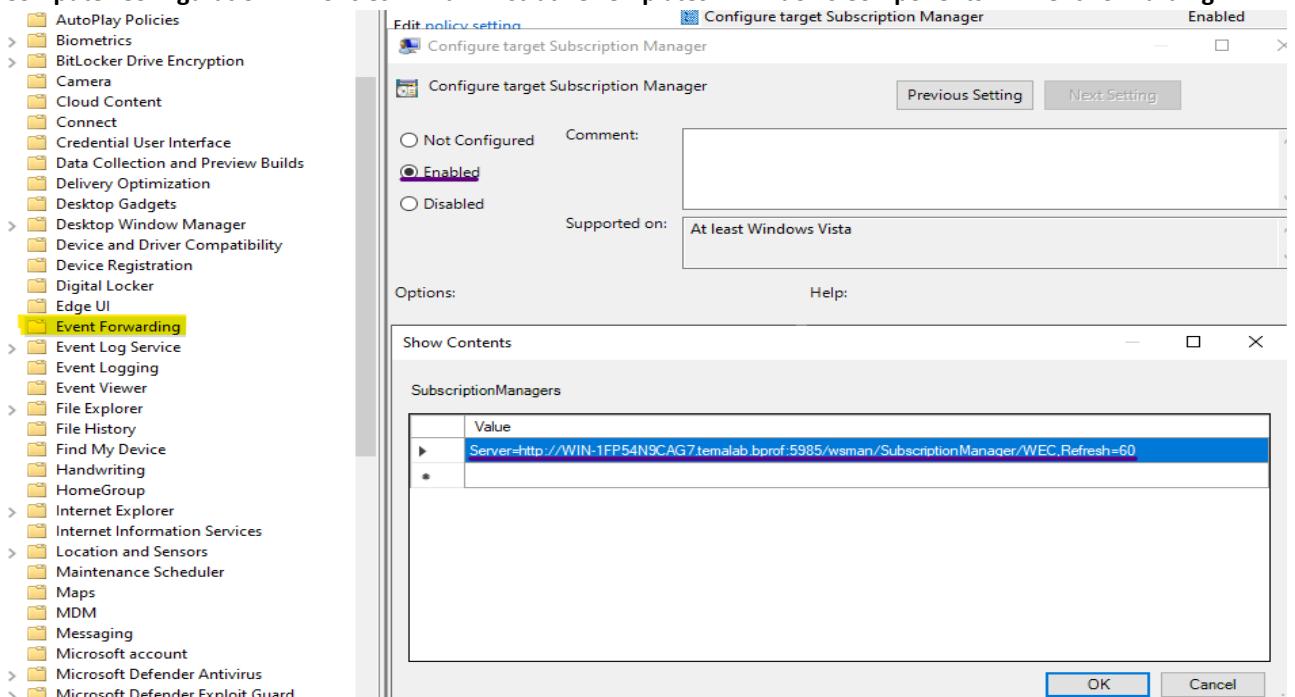
Ha mi mondjuk nem szeretnénk IPv6-t akkor mindenképpen definiálnunk kell egy GPO-t arra, hogy akkor az IPv6 ne legyen engedélyezve! Ekkor az “IPv6 filter” részénél a “*”-t ki kell vennünk és hagyjuk üresen azt a mezőt!

Le is tudjuk ellenőrizni, hogy a folyamat fut-e!

```
C:\Windows\system32>netstat -aon | find "5985"
TCP      0.0.0.0:5985          0.0.0.0:0              LISTENING      4
TCP      [::]:5985            [::]:0              LISTENING      4
```

Mint látható még elégü üres, s az IPv6 még nincs is itt! Majd a későbbiekben majd ha lesznek “Source”-k nagyobb lesz!

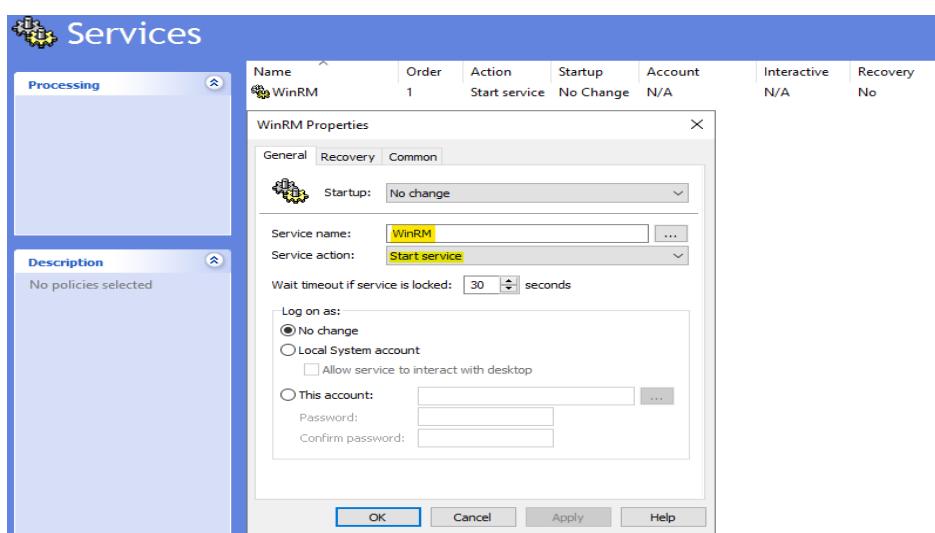
- Computer Configuration > Policies > Administrative Templates > Windows Components > Event Forwarding



Itt fontos, hogy az FQDN-t (Fully Qualified Domain Name) adjuk meg! Ezt megtudhatjuk ha pingeljük a saját

gépünket! A port az 5985! Ha lenne CERT, akkor menne HTTPS-n is, ekkor 5986 lenne a PORT! Az elérési útvonal pedig adott! Ide lesz elküldve minden “**Source**” eventje! A Refresh pedig, hogy mennyi időközönként figyeljük ezt a helyet!

- Computer Configuration > Preferences > Control Panel Settings > Services



Igaz, erre nem nagyon van szükségünk, de szeretnénk mindenképpen azt elérni, hogy a WinRM szolgáltatás elinduljon, amikor elindulnak a szerverek/kliensek!

Ennek beállítása nem lényeges, de már találkoztam olyan esettel, hogy mégsem indult el a szolgáltatás az adott gépen! Ekkor várhatunk csodákat, ha az adott szolgáltatás nem indult el / nem fut!

- Computer Configuration > Policies > Windows Settings > Security Settings > Windows Firewall with Advanced Security > Windows Firewall with Advanced Security > Inbound Rules

Erre sem feltétlenül van szükségünk, hiszen elvileg a WinRM a konfigurálásakor már ezeket a szükséges portokat megnyitja!

<input checked="" type="checkbox"/> Windows Remote Management (HTTP-In)	Windows Remote Manage...	Domai...	Yes	All
<input checked="" type="checkbox"/> Windows Remote Management (HTTP-In)	Windows Remote Manage...	Public	Yes	All

De ne bízzunk semmit sem a véletlenre! Válasszuk ki az alábbi lehetőségeket!

Predefined (Windows Firewall Remote Management) → Windows Remote (HTTP-In) (Domain, Private) → Allow The Connection

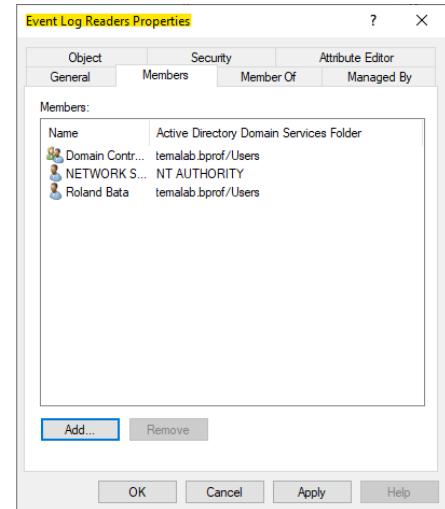
9.4. Event Log Readers csoporthoz felhasználók hozzárendelése

Ahhoz, hogy jogunk legyen az „Event”-k, pontosabban „Security”-bb dolgok olvasására, ehhez az „Event Log Readers” csoporthoz hozzá kell rendelnünk néhány „Tag”-t!

Kiket is kellene, s miért?

- **NETWORK SERVICE** → Aki bemutatja a számítógép hitelesítő adatait a távoli gépeknek! EZ KIFEJEZETTEN FONTOS, MERT CSAK VELE TUDJUK AZONOSÍTANI MAGUNKAT!!
- **Subscription User Account** → Ez azért fontos, mert valamilyen felhasználóval tudunk kell ennek a log-nak az olvasását! A távoli gépek, majd megnézzük szerepel-e az Ő „ChannelAccess” tokenükben a mi felhasználónk SID-ja!
- **Domain Controller / Maga a „Collector” gép!** → De mivel mi vagyunk maga a DC is, ezért a Domain Controller is elég!
- **Domain Computer** → Hiszen fontos a gép azonosítása is!

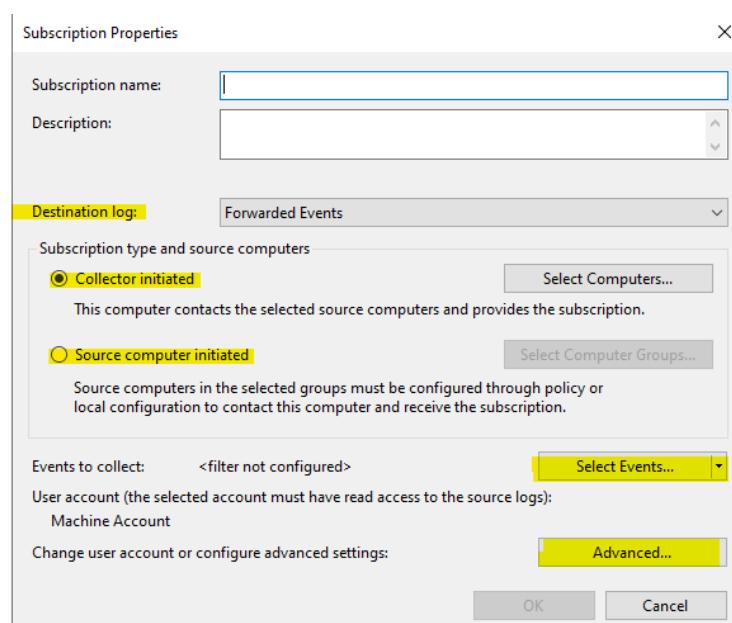
Nyissuk meg a Users and Computers lehetőséget és adjuk hozzá a „**Builtin**” résznél az „Event Log Readers” csoporthoz ezen felhasználókat!



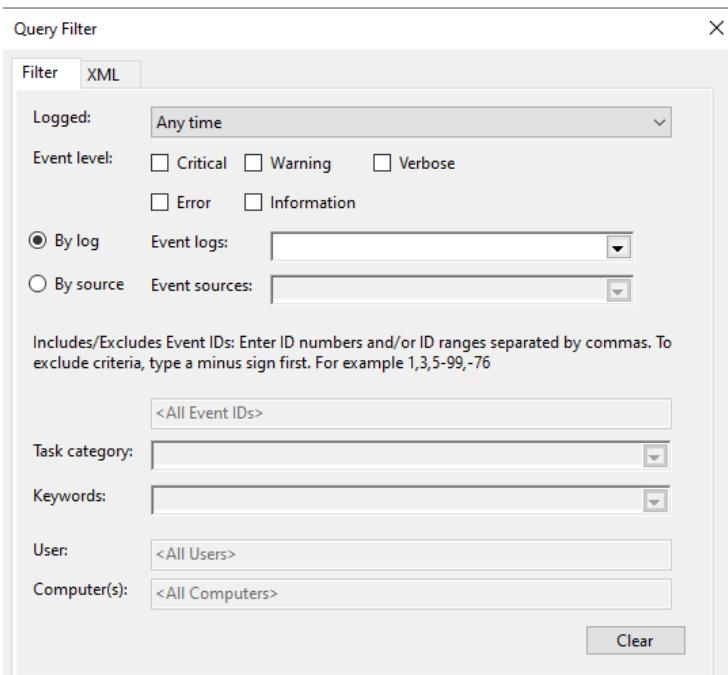
Így már majdnem a végén járunk! Most kell beállítani a „**Subscription**” részét!

9.5. Event Subscription beállítása

Nyissuk meg az „Event Viewer” alkalmazást! Majd a „**Subscription**” résznél hozzunk létre egy „**Subscription**”-t!

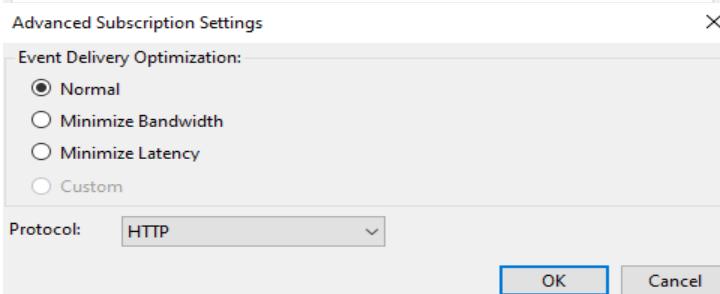


- **Subscription Name** → Amire feliratkoznak a „Source”-k!
- **Description** → Kevéske infó arról, mit is gyűjtünk!
- **Destination log** → Hova szeretnénk irányítani az „Event”-ket!
- **Subscription type and source computers**
 - **Collector Initiated** : A Collector szerver felkeresi a Source szervereket vagy a Domain Controllert és elkéri azt, ami összegyűlt! Hátránya az, hogy nehezen skálázható!
 - **Source computer Initiated** : Amint a Source gépen egy Event megérkezik, azt azonnal Forwardolja a Collector szerver felé! Ez a legjobb megoldás, jelen esetben! És ezt is fogom használni!
- **Events to collect** → Amit szeretnénk gyűjteni
- **Change user account or configure advanced settings** → Itt azt tudjuk beállítani, hogy milyen protokollon keresztül legyen elküldve, milyen gyorsan!



Itt tudjuk tehát testreszabni milyen Eventeket szeretnénk forwardolni a Collector felé!

- **Logged** → Mikor lett logolva
- **Event level** → Milyen Event típusokat szeretnénk továbbítani
- **By log** → Honnan → Security, System...
- **By source** → WinRM pl
- **<All Event IDs>** → Itt sorolhatjuk fel az Event ID-kat!
- **Task Category** → Feladat kategória
- **Keywords** → Audit Failure
- **User** → Mely felhasználókra
- **Computers** → Mely gépekre



Itt pedig be tudjuk állítani azt, hogy az Event milyen gyorsan kerüljön továbbításra

- **Normal** → Normális
- **Minimize Bandwidth** → Ha nem szeretnénk terhelni a Collector-t
- **Minimize Latency** → Ha minél gyorsabban szeretnénk megkapni
- **Custom** → PowerShell esetén (erről lesz szó!)
- **Protocol** → Amelyik protokollon szeretnénk eventet forwardolni

9.6. Event Subscription finomhangolása

Ez a beállítás azért fontos, hogy az "**Event**"-ket megkaphassuk! Ezt meg kell adni minden létrehozott "**Subscription**"-re! Elsősorban állítsuk be azt, hogy a "**ContentFormat**" az ne "**Rendered**" legyen, hanem "**Events**", ezzel gyorsabban megkapjuk az "**Event**"-ket és kíméljük a CPU Usage-t a Source gépeken! És az Event kézbesítési formája teljesen jó lesz!

```
C:\Windows\system32>wecutil gs "Login_off_collector"
Subscription Id: Login_off_collector
SubscriptionType: SourceInitiated
Description:
Enabled: true
Uri: http://schemas.microsoft.com/wbem/wsman/1/windows/EventLog
ConfigurationMode: MinLatency
DeliveryMode: Push
DeliveryMaxLatencyTime: 30000
HeartbeatInterval: 3600000
Query: <QueryList><Query Id="0"><Select Path="Security">*[System[(Level=1 or Level=2 or Level=3 or Level=4 or Level=0) and (EventID=4625 or EventID=4624 or EventID=4634 or EventID=4647 or EventID=4648)]]</Select></Query></QueryList>
ReadExistingEvents: false
TransportName: HTTP
ContentFormat: Events
Locale: hu-HU
LogFile: ForwardedEvents
PublisherName: Microsoft-Windows-EventCollector
AllowedIssuerCAList:
AllowedSubjectList:
DeniedSubjectList:
AllowedSourceDomainComputers: O:NG:BAD:P(A;;GA;;;DCS):
EventSource[0]:
  Address: WIN-GRAL4662T90.temalab.bprof
  Enabled: true
```

9.7. Event Subscription beállítása (Logon/Logoff AUDIT)

A képeken csak a beállításokat mutatom meg! Ezekről teljes mértékben látható az, hogy a beállítás menete hogyan is zajlott!

Event Viewer-ben “Subscription” létrehozása így nézett ki.:

The screenshots illustrate the step-by-step configuration of an Event Subscription in the Windows Event Viewer.

Subscription Properties - Login_off_collector (Main Window):

- Subscription name:** Login_off_collector
- Description:** (empty)
- Destination log:** Forwarded Events
- Subscription type and source computers:**
 - Collector initiated: This computer contacts the selected source computers and provides the subscription.
 - Source computer initiated: Source computers in the selected groups must be configured through policy or local configuration to contact this computer and receive the subscription.
- Events to collect:** (button: Select Events...)
- Configure advanced settings:** (button: Advanced...)
- Buttons:** OK, Cancel

Subscription Properties - Login_off_collector (Advanced Settings):

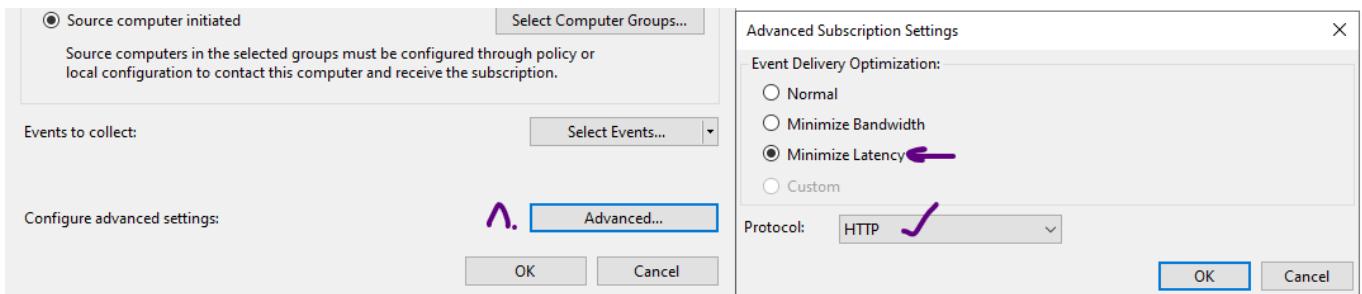
- Subscription name:** Login_off_collector
- Description:** (empty)
- Destination log:** Forwarded Events
- Subscription type and source computers:**
 - Collector initiated: This computer contacts the selected source computers and provides the subscription.
 - Source computer initiated: Source computers in the selected groups must be configured through policy or local configuration to contact this computer and receive the subscription.
- Events to collect:** (button: Select Events...)
- Configure advanced settings:** (button: Advanced...)
- Buttons:** OK, Cancel

Computer Groups Dialog (Advanced Settings):

This dialog shows the selection of computer groups for the subscription. It includes buttons for adding domain/computer groups and removing/excluding them, and a search bar for entering object names.

Subscription Properties - Login_off_collector (Final View):

- Subscription name:** Login_off_collector
- Description:** (empty)
- Destination log:** Forwarded Events
- Subscription type and source computers:**
 - Collector initiated: This computer contacts the selected source computers and provides the subscription.
 - Source computer initiated: Source computers in the selected groups must be configured through policy or local configuration to contact this computer and receive the subscription.
- Events to collect:** (button: Select Events...)
- Configure advanced settings:** (button: Advanced...)
- Advanced Settings Dialog (Visible on the right):**
 - Logged:** Any time
 - Event level:** Critical, Warning, Error, Information (checkboxes checked)
 - By log:** Event logs: Security (radio button selected)
 - Includes/Excludes Event IDs:** 4625,4624,4634,4647,4648
 - Task category:** (dropdown menu)
 - Keywords:** (dropdown menu)
 - User:** <All Users>
 - Computer(s):** <All Computers>
 - Buttons:** OK, Cancel, Clear
- Buttons:** OK, Cancel

**Eredmények ellenőrzése.:**

Name Status Type Source Co... Destination Log Description

>Login_off_collector	Active	Source Init...	1	Forwarded Eve...
----------------------	--------	----------------	---	------------------

Subscription Runtime Status - Login_off_collector

Subscription Status:
Active - : No additional status.

Source computers: 1 Total, 1 Active

Status	Computer Name
Active	WIN-GRAL4662T9O.temalab.bprof

[WIN-GRAL4662T9O.temalab.bprof] - Active - : No additional status.

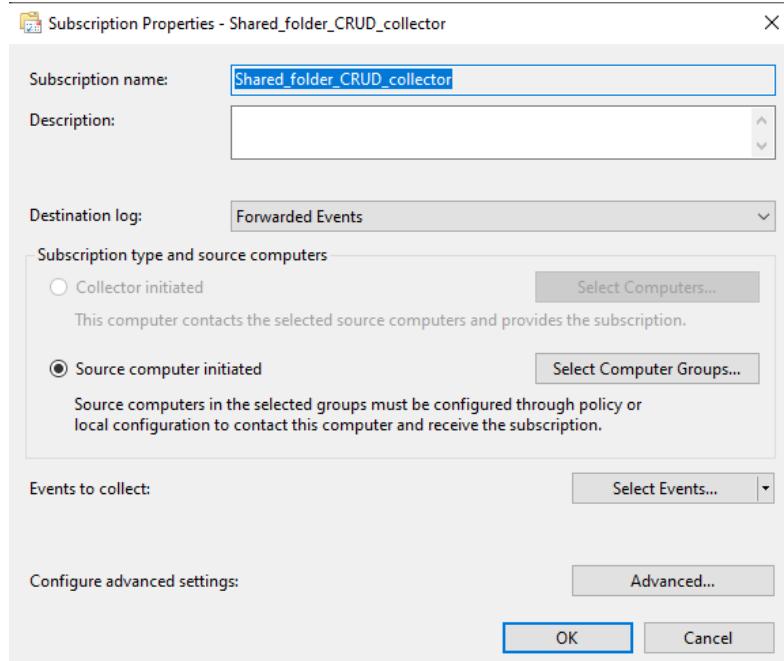
Close

Forwarded Events Number of events: 434						
Level	Date and Time	Source	Event ID	Task Category	Log	Computer
(i) Information	2022. 05. 07. 3:28:54	Microsoft Windows sec...	4624	Logon	Security	WIN-GRAL4662T9O.temalab.bprof
(i) Information	2022. 05. 07. 3:28:54	Microsoft Windows sec...	4648	Logon	Security	WIN-GRAL4662T9O.temalab.bprof
(i) Information	2022. 05. 07. 3:28:54	Microsoft Windows sec...	4634	Logoff	Security	WIN-GRAL4662T9O.temalab.bprof
(i) Information	2022. 05. 07. 3:28:54	Microsoft Windows sec...	4624	Logon	Security	WIN-GRAL4662T9O.temalab.bprof
(i) Information	2022. 05. 07. 3:28:54	Microsoft Windows sec...	4648	Logon	Security	WIN-GRAL4662T9O.temalab.bprof
(i) Information	2022. 05. 07. 3:28:53	Microsoft Windows sec...	4647	Logoff	Security	WIN-GRAL4662T9O.temalab.bprof
(i) Information	2022. 05. 07. 3:28:53	Microsoft Windows sec...	4624	Logon	Security	WIN-GRAL4662T9O.temalab.bprof
(i) Information	2022. 05. 07. 3:28:19	Microsoft Windows sec...	4624	Logon	Security	WIN-GRAL4662T9O.temalab.bprof

Event 4647, Microsoft Windows security auditing.

9.8. Event Subscription beállítása (Shared folder CRUD AUDIT)

Event Viewer-ben "Subscription" létrehozása így nézett ki.:



Select Computer Groups ugyanúgy néz ki emellett! A Select Events-nél kerülnek bele a AUDIT által ismertetett ID-k! Az Advanced rész is ugyanúgy fog kinézni!

Forwarded Events Number of events: 518						
Level	Date and Time	Source	Event ID	Task Category	Log	Computer
(i) Information	2022. 05. 07. 3:40:29	Microsoft Windows sec...	4624	Logon	Security	WIN-GRAL4662T90.bprof
(i) Information	2022. 05. 07. 3:40:28	Microsoft Windows sec...	4624	Logon	Security	WIN-GRAL4662T90.temalab.bprof
(i) Information	2022. 05. 07. 3:38:37	Microsoft Windows sec...	4658	File System	Security	WIN-GRAL4662T90.temalab.bprof
(i) Information	2022. 05. 07. 3:38:37	Microsoft Windows sec...	4656	File System	Security	WIN-GRAL4662T90.temalab.bprof
(i) Information	2022. 05. 07. 3:38:37	Microsoft Windows sec...	4658	File System	Security	WIN-GRAL4662T90.temalab.bprof
(i) Information	2022. 05. 07. 3:38:37	Microsoft Windows sec...	4690	Handle Manipulation	Security	WIN-GRAL4662T90.temalab.bprof
(i) Information	2022. 05. 07. 3:38:37	Microsoft Windows sec...	4658	File System	Security	WIN-GRAL4662T90.temalab.bprof
(i) Information	2022. 05. 07. 3:38:37	Microsoft Windows sec...	4656	File System	Security	WIN-GRAL4662T90.temalab.bprof
< Event 4624, Microsoft Windows security auditing.						

9.9. Custom Views létrehozása mindenAUDIT esetére

Erre azért van szükségünk, hogy az egész LOG halmaz ne folyjon össze arra az egy helyre! Úgynevezett nézeteket fogok definiálni!

- Custom Views → Create Custom View gombra kattintunk!

- Majd az eredményt itt láthatjuk!

Logon_Logoff_AUDIT_View Number of events: 504

Level	Date and Time	Source	Event ID	Task Category	Computer
Information	2022. 05. 07. 3:40:31	Microsoft Windows security auditing.	4624	Logon	WIN-GRAL4662T9O.temalab...
Information	2022. 05. 07. 3:40:30	Microsoft Windows security auditing.	4624	Logon	WIN-GRAL4662T9O.temalab...
Information	2022. 05. 07. 3:40:29	Microsoft Windows security auditing.	4624	Logon	WIN-GRAL4662T9O.temalab...
Information	2022. 05. 07. 3:40:28	Microsoft Windows security auditing.	4624	Logon	WIN-GRAL4662T9O.temalab...
Information	2022. 05. 07. 3:38:40	Microsoft Windows security auditing.	4634	Logoff	WIN-GRAL4662T9O.temalab...
Information	2022. 05. 07. 3:38:40	Microsoft Windows security auditing.	4624	Logon	WIN-GRAL4662T9O.temalab...
Information	2022. 05. 07. 3:38:40	Microsoft Windows security auditing.	4648	Logon	WIN-GRAL4662T9O.temalab...

Event 4624, Microsoft Windows security auditing.

- Természetesen ezt megcsinálhatjuk a másikra is, de ezt most nem részletezem, cserébe itt az eredmény!

Shared_folder CRUD_AUDIT_View Number of events: 12

Level	Date and Time	Source	Event ID	Task Category
Information	2022. 05. 07. 3:38:37	Microsoft Windows security auditing.	4658	File System
Information	2022. 05. 07. 3:38:37	Microsoft Windows security auditing.	4656	File System
Information	2022. 05. 07. 3:38:37	Microsoft Windows security auditing.	4656	File System
Information	2022. 05. 07. 3:38:37	Microsoft Windows security auditing.	4690	Handle Manipulation
Information	2022. 05. 07. 3:38:37	Microsoft Windows security auditing.	4656	File System
Information	2022. 05. 07. 3:38:37	Microsoft Windows security auditing.	4656	File System
Information	2022. 05. 07. 3:38:37	Microsoft Windows security auditing.	4658	File System
Information	2022. 05. 07. 3:38:37	Microsoft Windows security auditing.	4658	File System