Mérési jegyzőkönyv

A Windows vizsgálata 2

A mérés helyszíne:	
A mérés időpontja:	**2019. …**
A mérést végezték:	
Ennek a fájlnak a neve:	
A mérésvezető neve:	

Tudnivalók:

- Csak a sárga színnel megjelölt részre írjon.
- A <<Képernyőkép>> helyőrzőt törölje ki, és a helyére illesszen be egy, a feladat megoldását igazoló képernyőképet.
- A nehezebb feladatokat *-gal jelöltük. Ezek többségének megoldása szükséges a megajánlott jegyhez.

Otthoni felkészülés a laborra:

1. Nézze át a feladatokat! Ha nem ért egy részt, olvasson utána!

   A laborok elején a feladatokkal kapcsolatos ellenőrző kérdéseket teszünk fel.

2. Ha még nem használt Windows 10-et, telepítse egy virtuális gépben, és próbálja ki!

   A Windows10 ingyenesen letölthető a http://msdnaa.bme.hu/ weboldalról.

3. Ha még nem oldotta meg a Windows Labor 1-et, nézze át a feladatait!

   Ha nem ért valamit, járjon utána, mivel ez a labor épít az ott szerzett ismeretekre!

4. A laborfeladatok egy részét gyakorlásképpen otthon is megoldhatja!

   Ehhez az alábbi alkalmazások telepítésére van szükség:

   Sysnternals Suite és Total Commander

   Ha nem ismeri ezeket a programokat, gyakorolja a használatukat!

1. feladat: Terheltség és teljesítmény vizsgálata

1.1 Feladatkezelő (Task Manager)

Indítsuk el a *Feladatkezelőt*!

Nézzük meg a Feladatkezelő felületét! Váltsunk át a Processes nézetre, és nézzük meg, hogy hogyan lehet az aktuális erőforrás-használatot beazonosítani a hőtérképes megjelenítéssel (ehhez indítsunk el valami terhelést a háttérben, pl. játszunk le egy YouTube HD videót és mellette figyeljük a Feladatkezelőt).

1.2 Erőforrás-figyelő

Indítsuk el a *Resource Monitor*t!

A kezdőoldalon lévő számlálók alapján melyik folyamat olvasott az utóbbi időben a legtöbbet a lemezről?

Folyamat neve: perfmon.exe

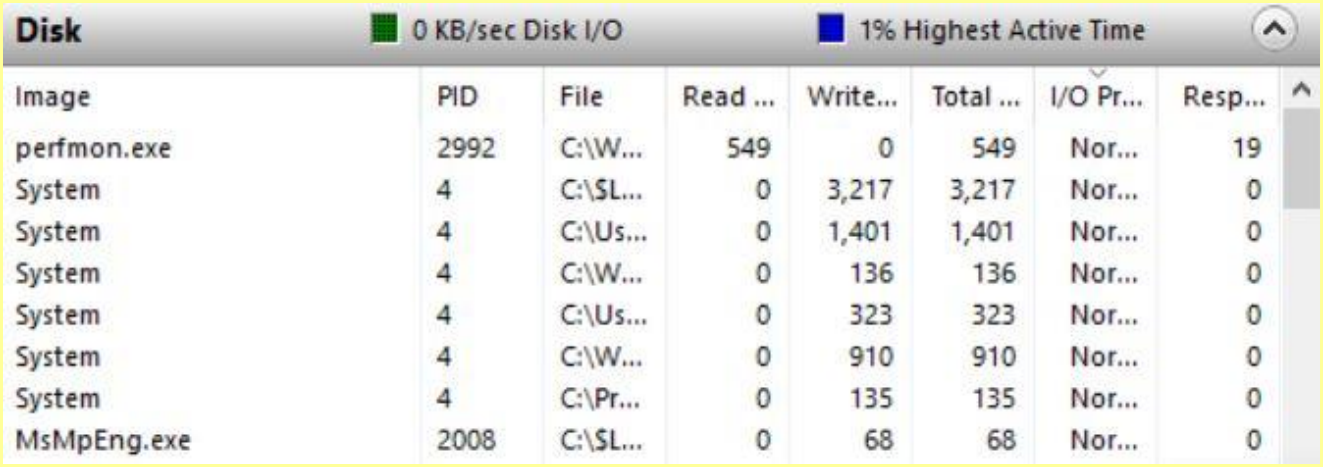
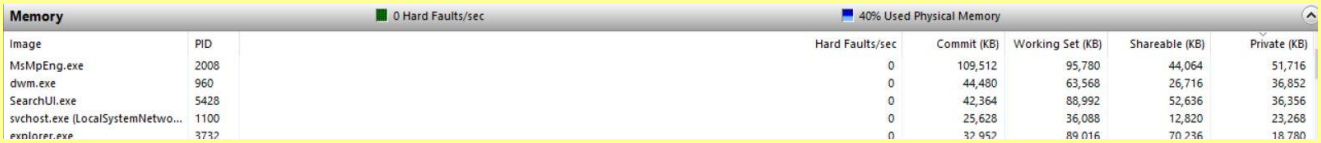


Image	PID	File	Read ...	Write...	Total ...	I/O Pr...	Resp...
perfmon.exe	2992	C:\W...	549	0	549	Nor...	19
System	4	C:\SL...	0	3,217	3,217	Nor...	0
System	4	C:\Us...	0	1,401	1,401	Nor...	0
System	4	C:\W...	0	136	136	Nor...	0
System	4	C:\Us...	0	323	323	Nor...	0
System	4	C:\W...	0	910	910	Nor...	0
System	4	C:\Pr...	0	135	135	Nor...	0
MsMpEng.exe	2008	C:\SL...	0	68	68	Nor...	0

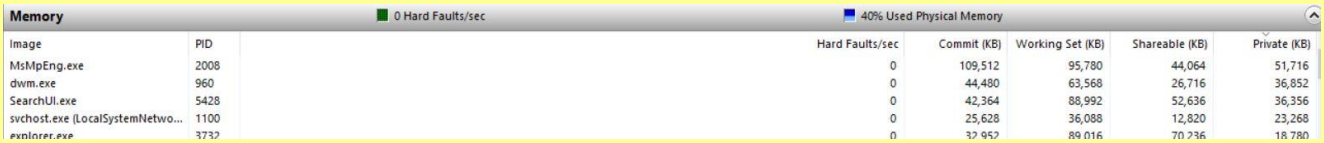
A Resource Monitorban nézzük meg, hogy jelenleg melyik folyamat használja a legtöbb fizikai memóriát!

Folyamat neve: MsMpEng.exe



Mennyi ebből az, amit megosztva használ más folyamatokkal?

Megosztott memória: 44,064 KB

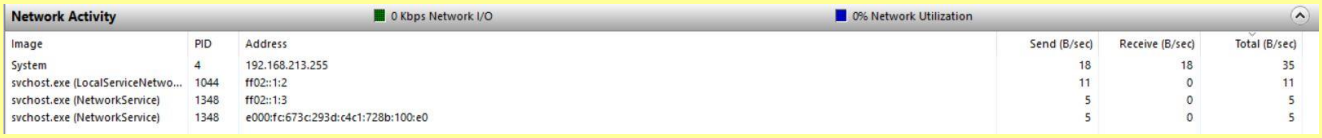


1.3 Teljesítményfigyelő

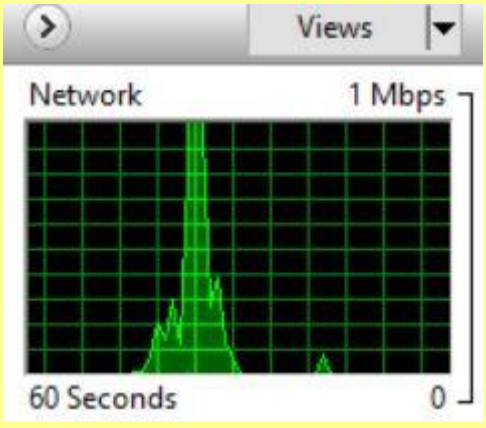
Ha ennél is részletesebb teljesítményadatokat akarunk lekérdezni, akkor a Performance Monitor (Teljesítményfigyelő) a megfelelő eszköz (`perfmon.exe` programot kell elindítani).

Indítsuk el, és adjunk hozzá egy olyan számlálót, ami a hálózati kártyán másodpercenként elküldött csomagokat méri!

Hozzáadás menete: Jobb klikk a menüsoron -> Select Columns -> Send



Generáljunk hálózati forgalmat, és készítsünk olyan grafikont, ami jelzi a hálózati forgalom alakulását!



Összefoglalás

A feladat végére tudni és érteni kell, hogy hogyan lehet az alapvető teljesítmény és terhelési adatokat lekérdezni. Ismerni kell a Feladatkezelő és az Erőforrás-figyelő lehetőségeit. Tudni kell teljesítményszámlálókat megfigyelni és rögzíteni.

2. feladat: Szolgáltatások kezelése

2.1 Szolgáltatások adatai

A *Services* kezelőfelületen[1] keresztül nézzük meg a *Security Accounts Manager* (*Biztonsági fiókkezelő)* szolgáltatást!

Mi a szerepe ennek a szolgáltatásnak?

Szerepe: Ezen szolgáltatás indítása jelzi más szolgáltatásoknak, hogy a biztonsági fiókkezelő (SAM) készen áll a kérések fogadására. A szolgáltatás letiltása megakadályozza, hogy a rendszer más szolgáltatásai értesítést kapjanak, ha a SAM készen áll, ami azt okozhatja, hogy a szolgáltatások nem indulnak megfelelően. Ezt a szolgáltatást nem ajánlott letiltani.

Mi a szolgáltatás belső neve és mi a megjelenítendő neve?

Belső név: SamSs

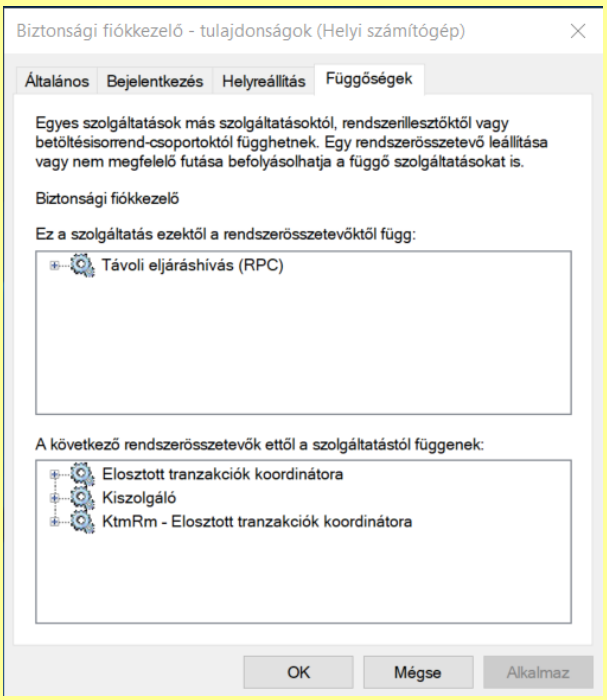
Megjelenítendő név: Biztonsági fiókkezelő

Milyen program tartozik ehhez a szolgáltatáshoz?

lsass.exe

2.2 Szolgáltatások függőségei

Milyen függőségei vannak ennek a szolgáltatásnak?



[1] Elérhető itt is: *Control Panel / System and Security / Administrative tools / Services*

2.3 Helyreállítási lehetőségek

Milyen helyreállítási lehetőségeket állíthatunk be, ha meghibásodik a *Security Account Manager* szolgáltatás?

Ha a szolgáltatás leáll, a számítógép újraindul. Ez a szolgáltatás nem támogatja a helyreállítási műveleteket.

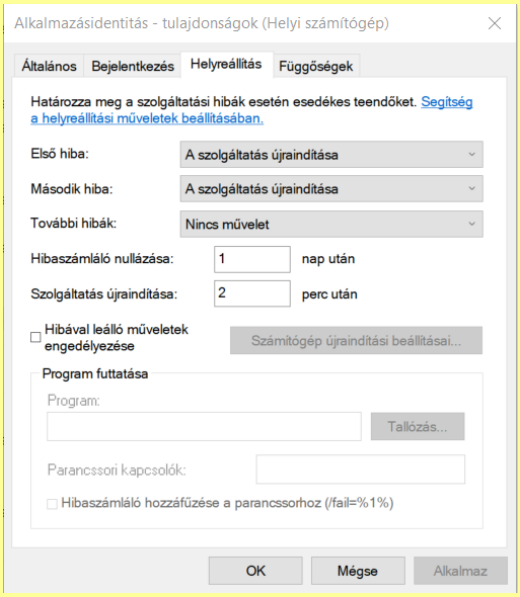
Tehát mi történik, ha meghibásodik a szolgáltatás?

A számítógép újraindul

Ezt egy másik szolgáltatáson is nézzük meg!

Helyreállítási lehetőségek:

- A szolgáltatás újraindítása
- A számítógép újraindítása



Összefoglalás

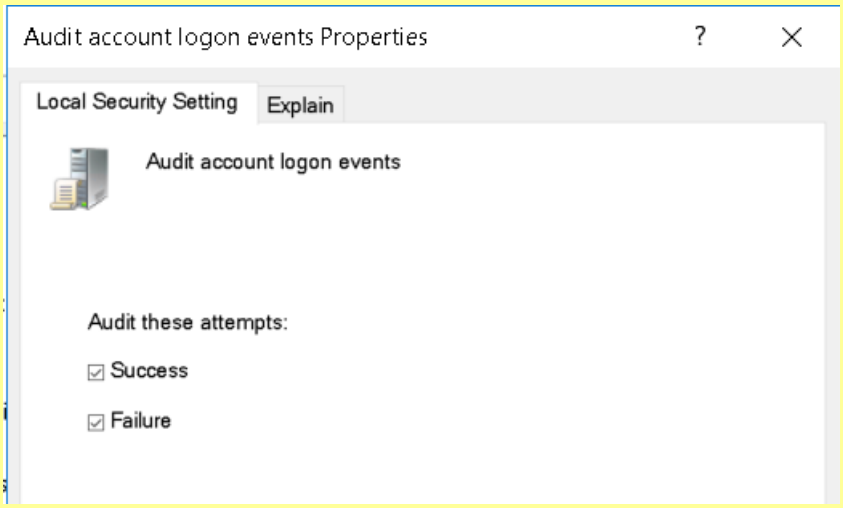
A feladat végére tudni és érteni kell, hogy milyen beállítási lehetőségeik vannak a szolgáltatásoknak.

3. feladat: Helyi biztonsági házirend

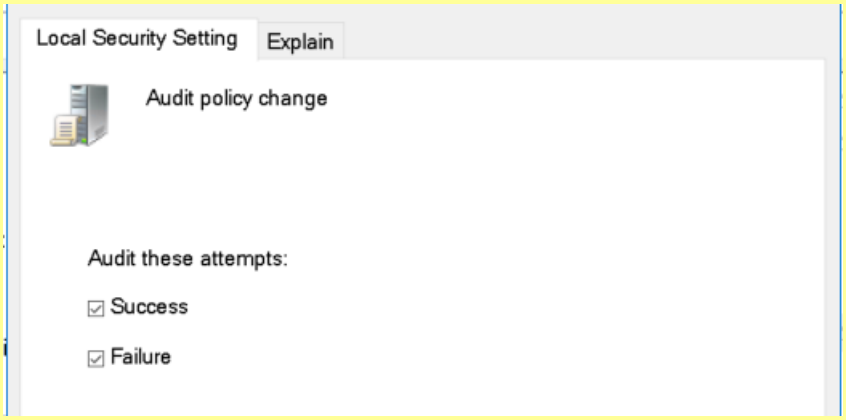
3.1 Naplózási beállítások

A helyi biztonsági házirendet a Vezérlőpult *Administrative Tools* részében érjük el *Local Security Policy* néven.

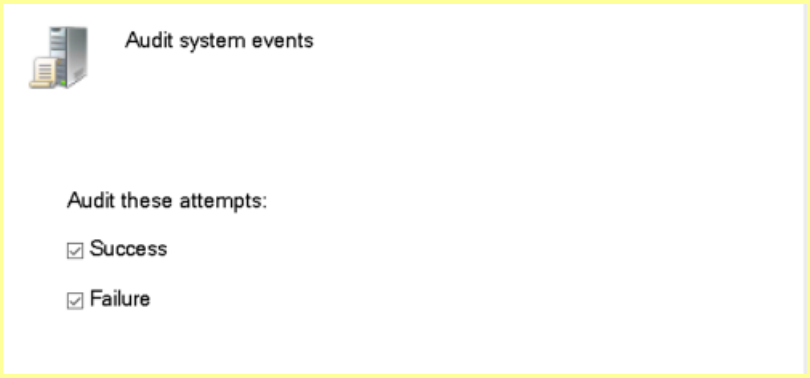
Állítsuk be a naplózási házirendben, hogy naplózza a rendszer a …
sikeres és sikertelen bejelentkezéseket!



Házirend változtatásokat!

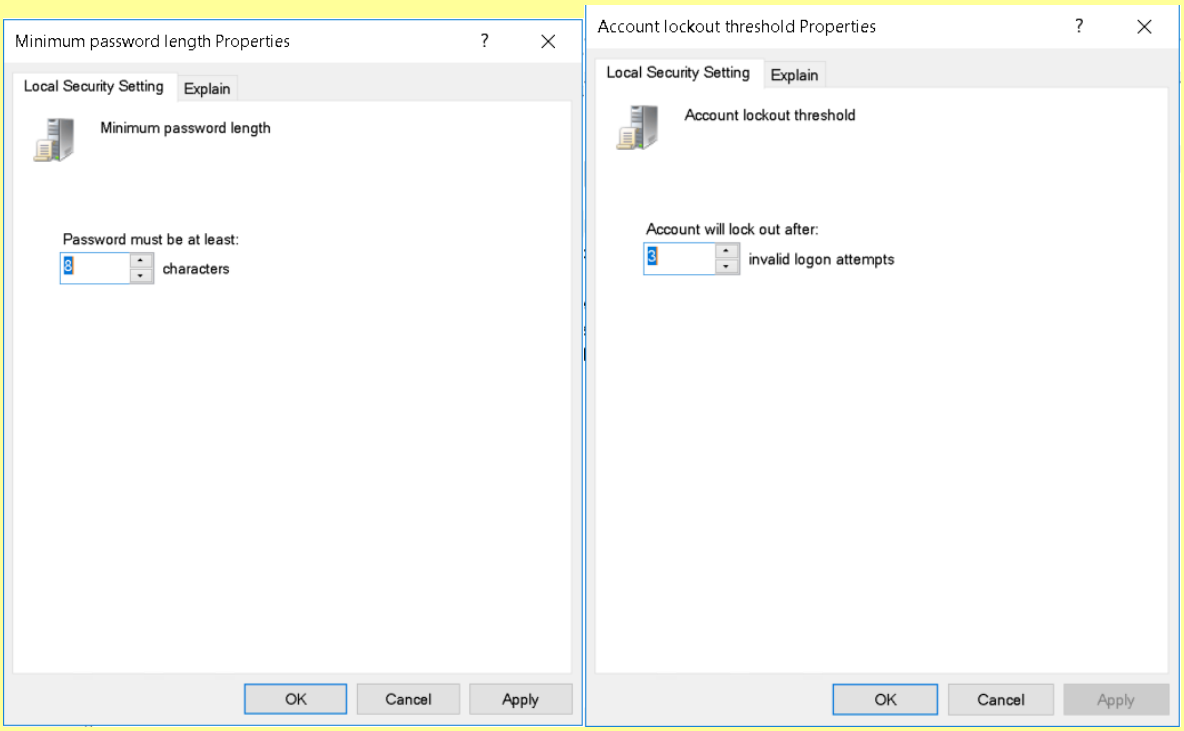


Rendszerjogok használatát!

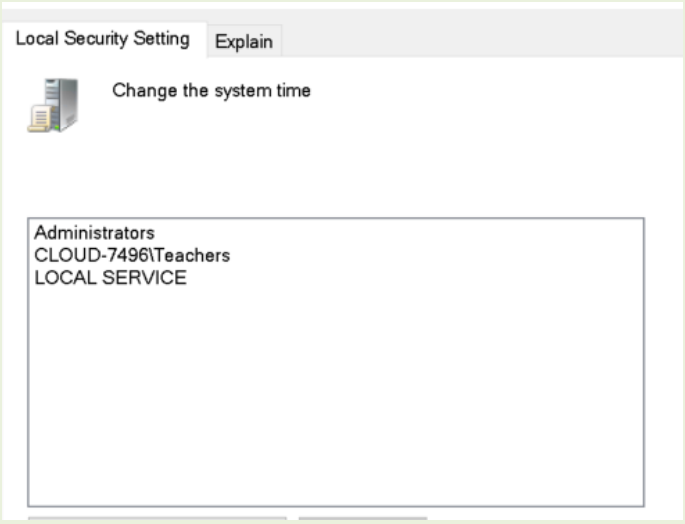


3.2 Belépéshez kapcsolódó beállítások

Állítsuk be, hogy a legrövidebb jelszó 8 karakter lehessen, és hogy 3 érvénytelen belépési kísérlet után zárolja a felhasználót a rendszer!



Hozzuk létre újra a testusert, és próbáljuk is ki, hogy kizárja-e a testuser felhasználót 3 hibás próbálkozás után (ehhez nem kell kilépnünk, elég, ha a *runas* parancs segítségével próbálkozunk)!



```
:\Program Files>runas /user:testuser hfs.exe
nter the password for testuser:
ttempting to start hfs.exe as user "CLOUD-7496\testuser" ...
UNAS ERROR: Unable to run - hfs.exe
326: The user name or password is incorrect.

:\Program Files>runas /user:testuser hfs.exe
nter the password for testuser:
ttempting to start hfs.exe as user "CLOUD-7496\testuser" ...
UNAS ERROR: Unable to run - hfs.exe
326: The user name or password is incorrect.

:\Program Files>runas /user:testuser hfs.exe
nter the password for testuser:
ttempting to start hfs.exe as user "CLOUD-7496\testuser" ...
UNAS ERROR: Unable to run - hfs.exe
326: The user name or password is incorrect.

:\Program Files>runas /user:testuser hfs.exe
nter the password for testuser:
ttempting to start hfs.exe as user "CLOUD-7496\testuser" ...
UNAS ERROR: Unable to run - hfs.exe
909: The referenced account is currently locked out and may not be logged on to.
```

Milyen eseményeket látunk ilyenkor az eseménynapló biztonsági részében?

Audit Failure, leírja, hogy mi volt az esemény, ebben az esetben a nem megfelelő jelszó bevitele

* 3.3 Emelt szintű feladat

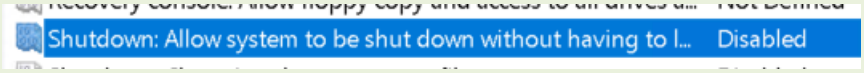
A felhasználói jogok kiosztása résznél nézzük meg, hogy milyen egyéb, rendszerszintű jogokat lehet kiosztani (ezek fiók jogok vagy privilégiumok lehetnek).

Állítsuk be, hogy a Teachers csoport is meg tudja változtatni a rendszeridőt! (A Teachers csoport hozzáadásához a felhasználót vagy csoportot kiválasztó ablakban az Objektumtípusnál be kell pipálni a csoportokat is.)

Change the system time

Administrators
CLOUD-7496\Teachers
LOCAL SERVICE

* 3.4 Emelt szintű feladat

Állítsuk be a biztonsági beállításoknál, hogy csak akkor lehessen leállítani a rendszert, ha bejelentkeztünk előtte.

Mi ennek a lépésnek a jelentősége?
Ha több User is használja a gépet, nem engedi lekapcsolni, így nem vesznek el a munkameneteink.