SZÉCHENYI ISTVÁN EGYETEM
GYŐR
TÁVKÖZLÉSI TANSZÉK

Mérési utasítás **Ismerkedés a Windows Server 2008-cal II.**

1. feladat

Telepítse a Windows Server 2008 további fontos frissítéseit a Microsoft oldaláról(kivétel IE 9). Közben nyissa meg a **Felügyeleti eszközök**nél(*Administrative Tools*) a **Számítógépkezelés**-t(*Computer Management*) és tekintse át az alábbi menüpontokat(lehetséges beállítási lehetőségeivel együtt)***:***

I. Feladat ütemező *(task scheduler)**:***
II. Eseménynaplók *(event viewer)**:***

– Készítsen az alkalmazások(*Applications*) menüpontra egy olyan szűrőt, amelyben az összes eseményforrás figyelmeztetéseit(*warning*) látja csak.
– Készítsen a rendszer(*system*) menüpontra egy olyan szűrőt, amelyben csak a rendszer hibáit(*error*) látja.

Az **Eseménynapló** a Microsoft Management Consol (MMC) beépülő modulja, amely lehetővé teszi eseménynaplók tallózását és kezelését. Ez egy elengedhetetlen eszköz a rendszer állapotának megfigyeléséhez és a felmerülő problémák azonnali elhárításához. Az Eseménynapló a következő feladatok végrehajtását teszi lehetővé:

- Több eseménynapló eseményeinek megtekintése
- Hasznos eseményszűrők mentése újra felhasználható egyéni nézetként
- Feladat egy eseményre adott válaszként történő futásának ütemezése
- Esemény-előfizetések létrehozása és kezelése

Ha az Eseménynaplót használja egy probléma elhárításához, a problémához kapcsolódó eseményeket kell keresnie, tekintet nélkül arra, hogy melyik eseménynaplóban jelennek meg. Az Eseménynapló lehetővé teszi, hogy bizonyos eseményekre több naplóban szűrjön. Ez megkönnyíti mindazon események megjelenítését, amelyek kapcsolatosak lehetnek a vizsgált problémával. Egy több naplókon átnyúló szűrő megadásához létre kell hoznia egy egyéni nézetet.

Eseménynaplók használatakor az elsődleges feladat az eseménykészlet szűkítése azokra az eseményekre, amelyek a felhasználót érdeklik. Ez néha könnyű. Máskor nagy erőfeszítést igényel, amely kárba veszhet, ha nem tudja valamilyen módon megőrizni a kemény munkával létrehozott naplónézeteket. Az Eseménynapló támogatja az egyéni nézeteket. Ha már saját szempontjai szerint lekérdezte és rendezte az elemezni kívánt eseményeket, mentheti munkája eredményét elnevezett nézetként, így az újra felhasználható lesz a későbbiekben. Exportálhatja is a nézetet, és használhatja más számítógépeken, vagy megoszthatja azt másokkal. Két általános típusú naplófájl használatos:

- Windows-naplók:
  - Alkalmazásnapló
  - továbbított események
  - biztonsági napló
  - telepítési naplófájl
  - rendszernapló

- alkalmazás- és szolgáltatás napló:
  - DFS-replikáció
  - címtárszolgáltatás
  - fájlreplikációs szolgáltatás
  - hardveresemények
  - microsoft\windows
  - windows power shell

III. Megosztott mappák***:***

IV. Helyi felhasználók és csoportok *(local users and groups)**:***

– Hozzon létre egy új **diak** nevű felhasználót (teljes név: Hallgató), amelynek jelszava **Hallgato11.** A jelszót* SOHA ne kelljen megváltoztatni, de lehessen.

– Az előző lépésben létrehozott diak felhasználót vegye fel a távoli felhasználók alapértelmezett csoportjába. Ezt követően a rendszertulajdonságok között (*System\Remote settings\Remote desktop... more safe*) a távoli használat fülön engedélyezze a távoli asztal funkciót.
Megjegyzés: Az engedélyezést követően azok, akik a távoli felhasználók csoport tagja, itt is mint felhasználók automatikusan látszódni fognak. Esetünkben 1 db. ilyen felhasználó lesz(diak).

*A jelszavakra jellemző például, hogy az ember valamilyen személyes dátumot, esetleg egy fontosabb nevet használ fel benne. Emellett sokszor előfordul, hogy értelmes szavakat, vagy azok kombinációját alkalmazzuk. A jelszótömegek ezen tulajdonságainak köszönhetően a legtöbb feltöréséhez a szótár alapú módszer elegendő. Ezen módszer esetében a szótár szavait csak meg kell próbálni néhány módosítással, és a próbálkozásokat hamar siker koronázza. Éppen ezért célszerű olyan jelszót választani, amely ellenáll a szótár alapú támadásoknak.

Ennek a kritériumnak megfelelő jelszó kiszámíthatatlan karaktereket tartalmaz, azaz megfelelően véletlenszerű. A véletlenszerűség jó, hogy ha nem csak az egymást követő karakterek változatosságában mutatkozik meg. Ugyanis az ilyen véletlenszerű jelszavaknál, ha brute force (~ nyers erő) módszerrel próbálják feltörni azokat, akkor csupán végigpróbálgatják az összes lehetséges kombinációt. Így, ha kis és nagybetűket is alkalmazunk, jelentősen meg tudjuk növelni a lehetséges kombinációk számát. Hogy még tovább növeljük a lehetőségeket, célszerű számokat és szimbólum karaktereket is alkalmazni, mint például az aláhúzás karakter (ez: _), kettőspont, pont, dollárjel, kötőjel, stb. Így az ún. jelszótér elég nagy lesz, és ha a jelszó elég hosszú, az efféle végigpróbálgatásos módszerrel kellően sokáig fog tartani a visszafejtése.

Az elfogadhatónak minősíthető jelszó legalább nyolc karakter hosszú, és valamennyi karakterosztályból tartalmaz legalább egyet.

2. feladat

V. *Teljesítménynapló (performance)*

Tekintse át a Számítógépkezelés alatt a **Teljesítménynaplók(***Performance)* típusait, beállítási lehetőségeit, majd önállóan hozza létre az alábbi **naplófájlt:**

- *(Data collector set)*a naplófájl neve: meres2 (Amennyiben az alapértelmezett könyvtár nem létezik, azt hozza létre.)
- kézi beállítást válasszunk, majd válassza a Teljesítményszámlálót (*Performance counte*r)
- a naplófájl az elindítását követően 3 percig fusson 15 másodperces időközökkel, és a helyi gép alábbi számlálóit monitorozza: processzoridő %; fájlírási sebesség, lapozófájl kihasználtság %
- A naplózás elindulása után nyissa meg a fájlt, és kísérje figyelemmel a számlálók változásait.

A Windows Teljesítményfigyelő eszköze valós időben, illetve a naplóadatok későbbi elemzéshez szánt gyűjtésével vizsgálhatja meg, hogy a futtatott programok milyen hatással vannak a számítógép teljesítményére. A Windows Teljesítményfigyelő eszköze teljesítményszámlálókat, esemény-nyomkövetési adatokat és konfigurációs adatokat használ, amelyek adatgyűjtő-csoportosítókba foghatók össze.

A **teljesítményszámlálók** a rendszer állapotát vagy tevékenységét mérik. Szerepelhetnek az operációs rendszerben vagy önálló alkalmazások részei lehetnek. A Windows Teljesítményfigyelő eszköze adott időközönként lekéri a teljesítményszámlálók aktuális értékét.

Az **esemény-nyomkövetési adatokat** a rendszer a nyomkövetési szolgáltatóktól gyűjti, amelyek az operációs rendszer vagy önálló alkalmazások olyan összetevői, amelyek műveleteket vagy eseményeket jelentenek. Több nyomkövetési szolgáltató adatait **nyomkövetési munkamenetbe** lehet egyesíteni.

A **konfigurációs információt** a rendszer a Windows beállításjegyzékében szereplő kulcsok értékeiből gyűjti. A Windows Teljesítményfigyelő eszköze a beállításkulcsok értékeit megadott időben vagy időközönként rögzítheti, a naplófájl részeként.

3. feladat

VI. Lemezkezelés(Storage)

Tekintse át a Szerverkezelés alatt a **Tárolás** lehetőségeit, majd hajtsa végre a következőket:

- a másodlagos winchesterről töröljön minden partíciót(amennyiben van)
- Hozzon létre egy 80 GB-os (81 920 MB) elsődleges partíciót úgy a másodlagos merevlemezen, hogy annak ne legyen betűjele, hanem a rendszert tartalmazó meghajtó mnt könyvtárába csatolja fel (ha a könyvtár nem létezik, azt hozza létre), NTFS fájlrendszerben gyorsformázással.
- A partíció kötetcimkéje: diak particio