

UJBÁNYI TIBOR - KATONA JÓZSEF - KŐVÁRI ATTILA

A felhasználói fiók migrációjának egy alternatív lehetősége Windows Vista/7/8 operációs rendszerekben

Bevezető

Egy új (vagy másik) számítógépre való váltáskor a felhasználó rendszerint operációs rendszert is cserél és ilyenkor bizony elég sok kényelmetlenséget okoz az új rendszer még „steril” környezete, hiszen a hónapok vagy évek alatt „belakott” felhasználói fiók nincs többé, mindent kezdhetünk előlről.

A migráció fogalma

Ahhoz, hogy megértsük a cikk témáját, mindenekelőtt a migráció fogalmának tisztázására van szükség. A migráció latin eredetű szó, amelyen a köznyelv költöztetést, vagy (lakóhely)változtatást ért. A migráció tehát lényegében valamilyen mozgást, ill. (hely)változtatást takar.

Mégis hogyan kapcsolódik ez az informatikához? Hogy egy általunk kedvelt mondást idézzünk: „Az informatika egy száguldó vonat.” – ez a mi olvasatunkban annyit jelent, hogy a technikai fejlődés irama manapság igen intenzív, ennek köszönhetően pedig – szinte napról napra új rendszerek és szoftverek jelennek meg. A technológiai újítások jobb kihasználhatóságát (és a piaci versenyt) szem előtt tartva a régi, elavult rendszereket újabb és korszerűbb rendszerek váltják fel. Ez a folyamat viszont számos problémát generál, mert ami a régi rendszeren még zökkenőmentesen működött, az új rendszeren már nem biztos, hogy gond nélkül funkcionál, legyen szó akár egy programról, vagy annak egy részéről, esetleg különböző adatbázisokról.

A felhasználói profil migrációjára az alábbi esetekben kerülhet sor:

Új számítógépre/operációs rendszerre történő váltáskor;

A felhasználói profil másik gépre való költöztetésekor.

Windows operációs rendszerben minden felhasználó külön felhasználói környezetet alakíthat ki. A testreszabott asztal és tálca, az ablakstílus, képernyőszínek, az ikonok és elrendezésük, a programjaink testreszabott beállításai – ezeknek mind búcsút inthetünk egy-egy rendszertelepítés alkalmával.

Szerencsére ez a probléma manapság már nem számít újdonságnak, ennek megfelelően számos alternatíva létezik a felhasználói fiókok migrációjának kivitelezésére (User State Migration Tool, Windows Easy Transfer). Jelen cikk keretein belül egy alternatív módszer megvalósítása kerül bemutatásra.

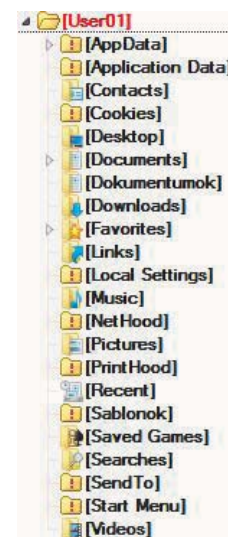
A felhasználói profil migrációja mindenféle külső segítség nélkül is elvégezhető, csupán ismerni kell az operációs rendszerünk nyújtotta lehetőségeket.

Mindenekelőtt azonban nem árt tisztázni néhány alapvető dolgot a felhasználói profillal kapcsolatban. Ismernünk kell:

- a profilkönyvtár helyét;
- a profilkönyvtár struktúráját, felépítését;
- az alkönyvtárakat és azok szerepét;
- a regisztrációs adatbázisban található felhasználói profilra vonatkozó bejegyzéseket.

A felhasználói profil könyvtárszerkezete

A felhasználó könyvtára alapértelmezettként (Windows Vista/7/8 operációs rendszerek esetén) a rendszermeghajtó gyökerében, a *Users* mappán belül helyezkedik el, azon a néven, amit a felhasználó a rendszer telepítésekor megadott. Például a *User01* felhasználó könyvtára alapértelmezetten a *C* meghajtó *Users* könyvtárán belül a *User01* almappában található. A könyvtár számos alkönyvtárat tartalmaz, amelyek különböző funkciókat töltenek be az adott felhasználói környezet működésének biztosításában.



1. ábra: a felhasználó könyvtárának mappastruktúrája

Minden felhasználói profil az alábbi könyvtárakat tartalmazza:

AppData: alkalmazás specifikus adatokat tartalmaz. Az adott program gyártó döntésének függvénye, hogy milyen adatok kerülnek ide.

Local: olyan programbeállítások kerülnek ide, amelyek állandóak, vagyis felhasználónként nem változnak.

LocalLow: funkciójában ugyanaz, mint a Local könyvtár annyi különbséggel, hogy ide csak az alacsony integritású alkalmazások írhatnak, mint például az Internet Explorer webböngésző beépülői.

Roaming: adott felhasználó alkalmazáskonfigurációs fájljai kerülnek ide. A mappa tartalma felhasználónként eltérő lehet.

Contracts: névjegytár, ide kerülnek az ún. névjegyzék fájlok, amiket például a Windows Mail használ. Egy névjegyzék fájl különféle kapcsolattartási és személyes információkat tartalmaz: leggyakrabban kép, cím és elérhetőségek (telefonszám, e-mail cím, webcím).

Cookies: az Internet Explorer webböngésző által használt „sütik” kerülnek ide.

Desktop: az asztali parancsikonokat, fájlokat és mappákat tartalmazza.

Documents: az alapértelmezett könyvtár felhasználó dokumentumai számára. Előfordul, hogy néhány alkalmazás is itt tárolja a konfigurációs beállításait, mentéseit.

Downloads: a felhasználó alapértelmezett letöltési mappája, többnyire a webböngészők használják.

Favorites: az Internet Explorer könyvjelzőit tartalmazza .url fájlokban. Az .url fájlokban internetes hivatkozások (webcímek) találhatóak.

Links: hivatkozásokat (parancsikonokat) tartalmaz az Asztal, Letöltések és a Legutóbbi helyek könyvtárakra.

Music: a felhasználó alapértelmezett Zene könyvtára. Erre a könyvtárra hivatkozik a legtöbb média-lejátszó program is az audiófájlok keresésekor.

Pictures: a felhasználó alapértelmezett Képek könyvtára.

Saved Games: a Windows beépített játékainak mentései kerülnek ide.

Searches: a Windows beépített keresőszolgáltatásának indexfájlját tartalmazza, ami elősegíti a gyorsabb keresést a rendszerben.

Videos: a felhasználó alapértelmezett Videó könyvtára, ahová alapértelmezettként a különböző videóformátumú fájlok kerülnek.

A mappastruktúrát végignézve könyvtárak mellett (és a könyvtárakon belül is) találunk ún. Junction pontokat (szimbolikus linkeket) is, amelyek – hasonlóan a parancsikonokhoz - hivatkoznak egy megadott helyre a felhasználó könyvtárán belül:

Dokumentumok: a Documents mappára mutat.

Local Settings: az AppData/Local könyvtárra hivatkozik.

Nethood: az AppData\Roaming\Microsoft\Windows\Network Shortcuts mappára hivatkozik, ahol a felhasználó hálózati helyei találhatóak.

Printhood: az AppData\Roaming\Microsoft\Windows\Printer Shortcuts mappára hivatkozik, ahol a telepített nyomtatók hivatkozásai találhatóak.

Recent: az AppData\Roaming\Microsoft\Windows\Recent mappára hivatkozik, ahol a legutóbb megnyitott dokumentumok listája található, elemenként külön hivatkozással.

Sablonok: az AppData\Roaming\Microsoft\Windows\Templates mappára hivatkozik, ahová a Microsoft Office programban létrehozott sablonfájlok kerülnek.

SendTo: az AppData\Roaming\Microsoft\Windows\SendTo mappára hivatkozik, ahol egy fájlra vagy mappára történő kattintás jobbgombos menüjének Küldés pontjában lévő elemek találhatóak.

Start Menu: az AppData\Roaming\Microsoft\Windows\Start Menu mappára hivatkozik, ahol a Windows start menüjének elemei találhatóak. Ebben a könyvtárban csak azok az elemek jelennek meg, amelyek az adott felhasználó számára is elérhetőek.

A Windows Vistától kezdődően a Microsoft új könyvtárszerkezetet vezetett be az *Application Data* könyvtárra vonatkozóan. Erre azért volt szükség, mert korábban a rendszer vegyesen tárolta az adatokat az *Application Data*-ban, ezért nehéz volt megállapítani, hogy mely adatok tartoztak a felhasználóhoz és melyek a számítógéphez.

A Windows Vistában (és annak utódaiban, a Windows 7-ben és a Windows 8-ban is) a Microsoft mérnökei megoldották a problémát azzal, hogy a felhasználói profilban az alkalmazásinformációkat az *AppData* könyvtáron belül három almappában tárolták: a *Local*, *LocalLow* és *Roaming* könyvtárakban. A *Local* és a *LocalLow* könyvtárakban olyan program információk találhatóak, amelyek felhasználónként nem változnak. Ezek általában olyan adatokat jelentenek, amelyek kifejezetten a rendszerhez tartoznak, vagy túl nagyok ahhoz, hogy a felhasználói fiókkal együtt „mozogjanak”.

Az *AppData\Roaming* a felhasználói profil könyvtáron belül Windows Vista/7/8 operációs rendszerben ugyanazt a funkciót tölti be, mint a *Local Settings\Application Data* a Windows XP-ben. Ez a mappaszerkezet váltás tette szükségessé a fent említett Junction pontok alkalmazását, a Microsoft ezzel a módszerrel tette könnyebbé az alkalmazások számára Windows XP-vel való kompatibilitást.

<i>Windows XP</i>	<i>Windows Vista/7/8</i>
Documents and Settings	Users
\$USER\$\My Documents	\$USER\$\Documents
\$USER\$\My Documents\My Music	\$USER\$\Music
\$USER\$\My Documents\My Pictures	\$USER\$\Pictures
\$USER\$\My Documents\My Videos	\$USER\$\Videos
\$USER\$\Application Data	\$USER\$\AppData\Roaming
\$USER\$\Cookies	\$USER\$\AppData\Roaming\Microsoft\Windows\Cookies
\$USER\$\Local Settings	\$USER\$\AppData\Local
\$USER\$\NetHood	\$USER\$\AppData\Roaming\Microsoft\Windows\Network Shortcuts
\$USER\$\PrintHood	\$USER\$\AppData\Roaming\Microsoft\Windows\Printer Shortcuts
\$USER\$\Recent	\$USER\$\AppData\Roaming\Microsoft\Windows\Recent
\$USER\$\SendTo	\$USER\$\AppData\Roaming\Microsoft\Windows\SendTo
\$USER\$\Start Menu	\$USER\$\AppData\Roaming\Microsoft\Windows\Start Menu
\$USER\$\Templates	\$USER\$\AppData\Roaming\Microsoft\Windows\Templates
\$USER\$\Local Settings\Application Data	\$USER\$\AppData\Local
\$USER\$\Local Settings\History	\$USER\$\AppData\Local\Microsoft\Windows\History
\$USER\$\Local Settings\Temporary Internet Files	\$USER\$\AppData\Local\Microsoft\Windows\Temporary Internet Files
All Users	ProgramData

All Users\Application Data	ProgramData
All Users\Desktop	Public\Desktop
All Users\Documents	Public\Documents
All Users\Favorites	Public\Favorites
All Users\Start Menu	ProgramData\Microsoft\Windows\Start Menu
All Users\Templates	ProgramData\Microsoft\Windows\Templates
Default User	Default

1. táblázat: a felhasználói könyvtár mappaszerkezetének differenciái a Windows XP és a későbbi Windows kiadásokban

Adatok a Registry-ben

A könyvtárstruktúra azonban csak az egyik része a felhasználói profilunknak. Az operációs rendszer a *Registry*-ben tárolja a felhasználói profilra vonatkozó információkat. A *Registry* a Microsoft Windows regisztrációs adatbázisa, amelyet a működés során használ és szükség esetén módosít. A regisztrációs adatbázisban tárolódik minden fontos beállítás és információ a rendszerről és a felhasználói programokról. A *Registry*-ben ágak (hive-ok) találhatóak. Ezek az ágak funkcionálisan és fájlrendszerbeli helyüket tekintve is különböznek egymástól. A Windows beépített regisztrációs adatbázis szerkesztőjével (regedit.exe) egységes felületen láthatjuk és szerkeszthetjük az ágakat, melyek a következők:

- HKEY_CLASSES_ROOT (HKCR)
- HKEY_CURRENT_USER (HKCU)
- HKEY_LOCAL_MACHINE (HKLM)
- HKEY_USERS (HKU)
- HKEY_CURRENT_CONFIG

A hive-ok elnevezésében a HKEY_ utáni rész jelzi a Windows API definíciójukat. Az ágak fizikailag

is megtalálhatóak a fájlrendszerben a %SystemRoot%\System32\Config könyvtárban:

SAM: HKEY_LOCAL_MACHINE\SAM
 SECURITY: HKEY_LOCAL_MACHINE\SECURITY
 SOFTWARE: HKEY_LOCAL_MACHINE\SOFTWARE
 SYSTEM: HKEY_LOCAL_MACHINE\SYSTEM
 DEFAULT: HKEY_USERS\DEFAULT

A felhasználókhoz külön hive-ok tartoznak, amik fizikailag a profil könyvtárban helyezkednek el. Az *NTUSER.DAT* a felhasználó könyvtárának gyökerében, az *USRCLASS.DAT* pedig az *AppData\Local\Microsoft\Windows* mappában található. Természetesen a fájlok tartalmának a Registry-ben is megvan a maga helye; az *NTUSER.DAT* a *HKEY_USERS\<User SID>* kulcs alatt található, a *USRCLASS.DAT* tartalma pedig a *HKEY_USERS\<User SID>_Classes* alatt látható. Harlan Carvey (2011)

A felhasználói azonosító

A felhasználói fiókhoz tartozik egy azonosító, az ún. SID (Security ID). A SID a felhasználóhoz rendelt egyedi azonosító, mint például a valós életben a személyi igazolványunk száma. A SID segítségével történik meg a felhasználó jogosultságainak ellenőrzése (többek között ezért lehetséges a felhasználók átnevezése). A Security ID-t a rendszer generálja, ami annyira egyedi, hogy egy esetleges felhasználó törlés után a már törölt felhasználó SID-jét a rendszer nem osztja ki más felhasználók részére.

Felhasználó migrációjának gyakorlati megvalósítása

Windows 7 Professional N rendszerben egy felhasználónk felhasználó migrációját szeretnénk megoldani, tehát a felhasználó költöztetését a jelenlegi operációs rendszerről egy másik telepítésre. Segítségként először engedélyezzük a rendszerben a beépített rendszergazdai fiókot.

Start menü – Futtatás – compmgmt.msc paranccsal megnyitjuk a számítógép kezelőt, majd a Helyi felhasználók és csoportok lenyíló menüben a Felhasználók csoportban keressük meg a Rendszergazda

felhasználót. A Tulajdonságok menüjében vegyük ki a „A fiók le van tiltva” opció előli pipát, majd OK. Érdemes jelszót is beállítani, mivel ez a felhasználó teljes jogkört gyakorol a rendszer felett. Ezután lépünk be a Rendszergazda felhasználóval és ott hajtjuk a migrációhoz szükséges lépéseket.

A felhasználó költöztetéséhez első lépésként egy teljes mentést kell készítenünk a felhasználó könyvtáráról, beleértve a felhasználóhoz tartozó *NTUSER.DAT* és *USRCLASS.DAT* fájlokat.

A könyvtár mentése azért lényeges, mert - mint fentebb már említésre került - a felhasználó összes alkalmazásinformációja az *AppData* almappában tárolódik, így biztosíthatjuk, hogy ne vesszenek el programjaink konfigurációs fájljai.

A mentést célszerű valamilyen fájlmenedzser program (pl.: FAR Manager) segítségével végezni, már csak azért is, mert egy későbbi lépés során szükségünk lesz olyan plusz funkciókra, amivel a Windows intéző nem rendelkezik. Ha ezzel megvagyunk, meg kell keresnünk a felhasználói profil információit tartalmazó *Registry* bejegyzéseket. A regisztrációs adatbázisban a profilinformációk jelentős (és lényegi) része a *HKEY_USERS* ágon tárolódik a felhasználóhoz tartozó SID kulcs alatt. Windows 7 operációs rendszerben az S-1-5-21-gyel kezdődő karaktersorozat alatt találjuk a számunkra fontos kulcsokat. Mint tudjuk, a Windows a felhasználóknak eltérő SID-et generál. A SID-ek szintaktikája azonban közel sem olyan bonyolult, mint azt elsőre gondolnánk. Megfigyelhető, hogy mindig csak az utolsó 4 számjegy változik, a felhasználókat a rendszer 1001-től „számozza”, minden egyes új felhasználó 1-gyel nagyobb számot kap, függetlenül attól, hogy létezik-e még a rendszerben az a felhasználó, aki az előző SID-et kapta. Ezért nem fordulhat elő, hogy egy korábbi és egy új felhasználó ugyanazt a SID-et kapja. A *HKEY_CURRENT_USER* ág alatt szintén látjuk az éppen bejelentkezett felhasználóhoz tartozó értékeket.

A szükséges információknak tehát tudjuk a helyét, azonban muszáj egy kicsit előreszaladnunk, ugyanis a *HKEY_USERS* ágon (így a *HKEY_CURRENT_USER* ágon is) mindig csak annak a felhasználónak a kulcsait, ill. a felhasználónak a SID kulcsát látjuk, akivel éppen be vagyunk jelentkezve. Ezért exportálás után, egy később létrehozott felhasználói fiókból nem tudjuk megvalósítani .reg fájl importálásával a visszaállítást, mert annak a felhasználónak már egy másik SID-et oszt ki a rendszer és a régi fiók a másik rendszeren (amire a felhasználót költöztetni akarjuk) nyilván nem lesz elérhe-

tő. Akkor mégis mi a teendő? Itt jönnek képbe a felhasználóhoz tartozó hive-ok. Tudni kell, hogy a HKEY_USERS ágon azokat az információkat látjuk, amelyeket az *NTUSER.DAT* fájl tartalmaz: a rendszer minden belépésnél onnan tölti be a felhasználóhoz kapcsolódó *Registry* bejegyzéseket.

A regisztrációs adatbázis szerkesztőben lehetőségünk van betölteni és módosítani a hive-ok tartalmát. Az *NTUSER.DAT* viszont alapértelmezetten nem látható, rejtett fájl. A rejtést fel kell oldanunk, könnyítésként akár hívhatjuk segítségül a fájlkezelőnket, amivel egyszerűen csak kivesszük a fájlattribútumok közül a rejtett és a rendszer tulajdonságokat. Ezután már a *Registry Editor* számára is láthatóvá válik a fájl, amit hive-ként betölthetünk.

Erre azért van szükség, mert a hive-okat csak így tudjuk problémamentesen módosítani, lévén hogy a módosítások a fájlban tárolódnak és a rendszer egy-egy bejelentkezéskor onnan olvassa ki az adatokat. A migráció fentiek ismeretében az alábbi lépésekből megvalósítható:

A Rendszergazda fiókkal mentés készítése a migrálni kívánt felhasználó teljes könyvtáráról.

A felhasználó *NTUSER.DAT* fájljának betöltése a regisztrációs adatbázis szerkesztőbe, majd annak exportálása .reg fájlként.

A másik rendszeren az eredetivel megegyező nevű felhasználó létrehozása, majd átjelentkezés Rendszergazda profilba.

Az új rendszeren létrehozott felhasználó *NTUSER.DAT* fájljának betöltése a regisztrációs adatbázis szerkesztőbe. Fontos, hogy a betöltött hive-nak olyan nevet adjunk, mint az eredeti felhasználó hive-jának betöltésekor tettük.

Az eredeti felhasználó adatait tartalmazó .reg fájl importálása. Ezzel a lépéssel a rendszer bele fogja írni az új rendszeren létrehozott felhasználó *NTUSER.DAT* fájljába a migrálni kívánt felhasználó adatait.

A felhasználó könyvtáráról készült teljes mentés visszamásolása a megfelelő helyre, ügyelve arra, hogy a módosított *NTUSER.DAT* fájlt ne írjuk felül.

Ha mindent jól csináltunk, az új rendszeren ugyanazt a megszokott felhasználói fiókot kapjuk vissza, mint amit a régi rendszeren is használtunk.

Összegzés

A bemutatott módszer segítségével viszonylag gyorsan és egyszerűen költöztethetünk felhasználói fiókot egyik operációs rendszerről a másikra. Ha ezt a módszert választjuk, nem árt figyelembe venni, hogy csak abban az esetben működik biztosan, ha a szoftverkörnyezet is azonos (tehát az új operációs rendszeren is telepítve kell lennie azoknak a programoknak, mint azon a rendszeren ahonnan a felhasználót migráltuk). A megoldás működik Windows Vista, Windows 7 és Windows 8 operációs rendszerek között is.

Irodalom

Harlan Carvey (2011): Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry

Kiss Balázs – Szalai Márton (2010): Windows 7 haladókönyv, SZAK KIADÓ KFT.

Nagy Gábor (2005): Útmutató a Windows Registry használatához, SZAK KIADÓ KFT.

Internetes hivatkozások

The difference between Local and LocalLow Folders (2009)

[<http://www.windowspcguy.net/?p=173>]

Forensic vizsgálatok 1. - A Windows registry elemzése (2009)

[<http://secblog.stratis.hu/2009/04/forensic-vizsgalatok-1-windows-registry.html>]

