

OPERÁCIÓS RENDSZEREK I.

A JOGOSULTSÁGI RENDSZER

```
-rw----- 1 root root 1448 szept 24 14:07 sha
-rw-r--r-- 1 root root 103 dec 4 2014 she
drwxr-xr-x 2 root root 4096 dec 4 2014 ske
-rw-r--r-- 1 root root 7096 febr 28 2014 sma
-rwxr-xr-x 1 root root 5753 febr 28 2014 sma
drwxr-xr-x 3 root root 4096 dec 5 2014 sma
drwxr-xr-x 2 root root 4096 szept 14 14:38 snm
drwxr-xr-x 2 root root 4096 febr 8 22:02 ssh
drwxr-xr-x 4 root root 4096 dec 29 00:30 ssl
-rw-r--r-- 1 root root 139 jan 12 07:49 sub
-rw----- 1 root root 117 szept 24 14:07 sub
-rw-r--r-- 1 root root 139 jan 12 07:49 sub
-rw----- 1 root root 117 szept 24 14:07 sub
-r--r----- 1 root root 745 febr 10 2014 sud
drwxr-xr-x 2 root root 4096 febr 8 17:42 sud
drwxr-xr-x 37 root root 4096 dec 29 15:33 syn
-rw-r--r-- 1 root root 2084 ápr 1 2013 sy
drwxr-xr-x 2 root root 4096 febr 16 2015 sys
drwxr-xr-x 2 root root 4096 dec 5 2014 sys
drwxr-xr-x 3 root root 4096 febr 10 23:10 sys
drwxr-xr-x 2 root root 4096 dec 4 2014 ter
-rw-r--r-- 1 root root 16 nov 15 18:13 tim
-rw-r--r-- 1 root root 1260 júl 1 2013 uc
drwxr-xr-x 4 root root 4096 febr 10 23:09 ude
drwxr-xr-x 3 root root 4096 dec 4 2014 ufw
-rw-r--r-- 1 root root 321 jún 20 2013 up
drwxr-xr-x 3 root root 4096 nov 15 18:18 upd
drwxr-xr-x 2 root root 4096 nov 15 18:18 upd
drwxr-xr-x 2 root root 4096 dec 4 2014 upd
-rw-r--r-- 1 root root 222 ápr 11 2014 up
drwxr-xr-x 2 root root 4096 dec 4 2014 vim
lrwxrwxrwx 1 root root 23 dec 4 2014 vtr
drwxr-xr-x 2 root root 4096 dec 4 2014 w3m
-rw-r--r-- 1 root root 4812 febr 7 2014 wge
-rw-r--r-- 1 root root 1343 jan 9 2007 wod
drwxr-xr-x 2 root root 4096 nov 15 18:18 wpa
drwxr-xr-x 4 root root 4096 dec 4 2014 X11
drwxr-xr-x 37 root root 4096 dec 29 15:33 syn
-rw-r--r-- 1 root root 2084 ápr 1 2013 sy
drwxr-xr-x 2 root root 4096 febr 16 2015 sys
drwxr-xr-x 2 root root 4096 dec 5 2014 sys
drwxr-xr-x 3 root root 4096 febr 10 23:10 sys
drwxr-xr-x 2 root root 4096 dec 4 2014 ter
-rw-r--r-- 1 root root 16 nov 15 18:13 tim
-rw-r--r-- 1 root root 1260 júl 1 2013 uc
```

TRADICIONÁLIS JOGOSULTSÁGI RENDSZER

UNIX

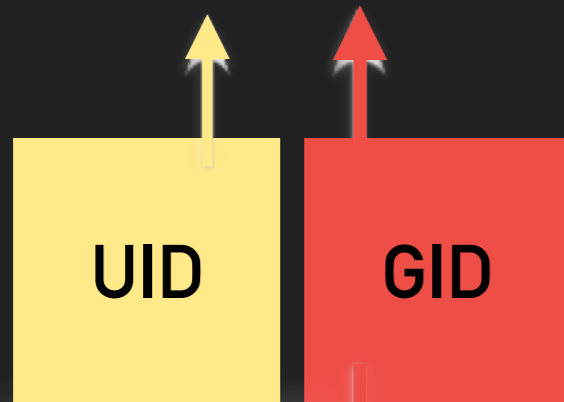
FELHASZNÁLÓK ÉS CSOPORTOK A UNIXBAN

`/etc/shadow`

```
B0QZ4Y:$1$Qh8FBkSS$NPFHHeP4naTAwy64YU0Bb/:16845:0:99999:7:::  
O3O6AB:$1$1e8L6tNV$NoF4hOShLuuWJFfdsDFax0:16845:0:99999:7:::
```

`/etc/passwd`

```
RHPY5Y:x:1918:112:Tóth Dzszenifer:/home/2016/RHPY5Y:/bin/bash  
NU70VQ:x:1919:200:Tóth Nóra:/home/2016/NU70VQ:/bin/bash  
CDAV40:x:1920:1921:Tóth Tamás:/home/2016/CDAV40:/bin/bash
```

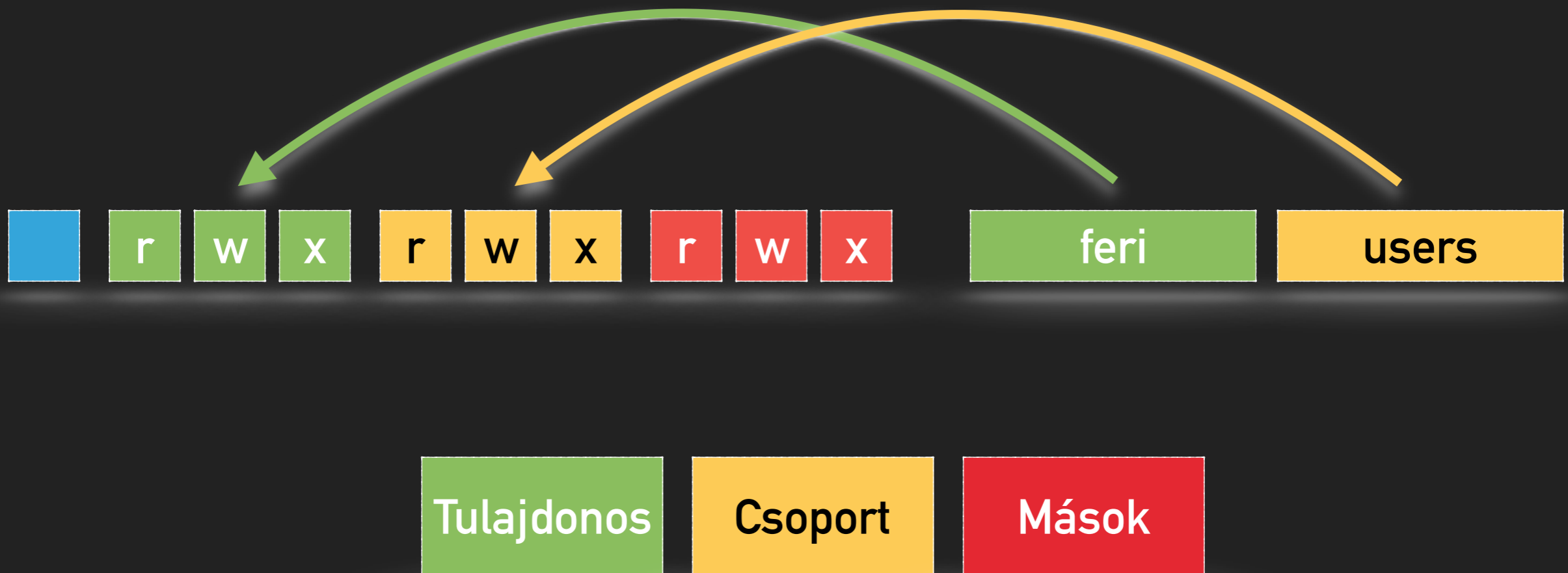


`/etc/group`

```
biciklistak:x:112:  
programozok:x:200:RHPY5Y,B6WSLG  
CDAV40:x:1921:
```

JOGOK A FÁJLRENDSZERBEN

```
-rw-r--r-- 1 feri users 1653 jan 12 07:50 dolgozat.txt
```



Fájlok esetén

r

A fájl TARTALMA olvasható a felhasználó számára.

w

A fájl TARTALMA írható a felhasználó számára.

x

A fájl tartalma egy program, melyet a felhasználó futtathat.
A program jogosultságai az őt indító felhasználóéval.

Könyvtárak esetén

r

A könyvtár TARTALMA olvasható a felhasználó számára.
Ez a tartalom a tartalomjegyzék.

w

A könyvtár TARTALMA, azaz a tartalomjegyzék írható a felhasználó számára.

x

A könyvtárba a felhasználó be tud lépni.

MIKOR TÖRÖLHETŐ EGY FÁJL VAGY KÖNYVTÁR?

Ha az azt tartalmazó könyvtár a felhasználó számára írható.

```
drwxr-xr-x 2 root root 4096 febr 11 08:56 /var/tmp/feri
```

```
-rwxrwxrwx 1 feri users 1021112 okt 7 2014 dolgozat.txt
```

JOG BEÁLLÍTÁSA

chmod **UGO** objektum [-R]

4	2	1	4	2	1	4	2	1
r	w	x	r	w	x	r	w	x

rw~~x~~: 4+2+1 = 7
r~~w~~~~x~~: 4+0+1 = 5
rw~~-~~: 4+2+0 = 6

```
chmod 750 alma.txt
```

chmod **ki** operandus jog objektum [-R]

u+r: user + read
g-w: group - write
a=rw: világ: rw-

```
chmod u+r alma.txt
```

TULAJDONOS ÉS CSOPORT CSERÉJE

```
-rw-r--r-- 1 feri users 1653 jan 12 07:50 dolgozat.txt
```

```
chown tulajdonos objektum [-R]  
chgrp tulajdonos objektum [-R]
```

Több rendszerben csak a root számára!

```
chown feri /var/tmp/alma.txt
```

```
chgrp users /var/tmp/alma.txt
```

A KVÓTA PROBLÉMA

```
drwxr-xr-x 2 root root 4096 febr 11 08:56 /var/tmp/feri
```

```
-rwxrwxrwx 1 feri users 1021112 okt 7 2014 dolgozat.txt
```


SETUID

```
-r--r----- 1 root shadow 24962 febr 18 13:24 /etc/shadow
```

```
B0QZ4Y:$1$Qh8FBkSS$NPFHHeP4naTAwy64YU0Bb/:16845:0:99999:7:::  
O3O6AB:$1$1e8L6tNV$NoF4hOShLuuWJFfdsDFax0:16845:0:99999:7:::
```

```
-rwsr-xr-x 1 root root 47032 jan 27 01:50 /usr/bin/passwd
```

r w s

A program a TULAJDONOS jogaival fut.

SETGID

```
-rwxr-sr-x 1 root root 125222 febr 18 21:26 runMe
```

r w s

A program a CSOPORT jogaival fut.

SETUID PÉLDA

```
root@columbo:/var/tmp# ls -l
-rwxr-xr-x 1 root root 14622 febr 28 13:40 setUIdDemo
```

```
root@columbo:/var/tmp# ./setUIdDemo
root:$6$nn20QLBRlcw8c6fsYJrl9HSEnkiT4S/Y7omU.kc6nUt/:16623:0:99999:7:::
daemon:*:16623:0:99999:7:::
```

```
feri@columbo:/var/tmp$ ./setUIdDemo
Unable to open file: /etc/shadow
```

```
root@columbo:/var/tmp# chmod 4755 setUIdDemo
root@columbo:/var/tmp# ls -l
összesen 16
-rwsr-xr-x 1 root root 14622 febr 28 13:40 setUIdDemo
```

```
feri@columbo:/var/tmp$ ./setUIdDemo
root:$6$nn20QLBRlcw8c6fsYJrl9HSEnkiT4S/Y7omU.kc6nUt/:16623:0:99999:7:::
daemon:*:16623:0:99999:7:::
```

```
#include <iostream>
#include <fstream>
#include <string>

#define FILENAME "/etc/shadow"

using namespace std;

int main () {
    string line;
    ifstream sf (FILENAME);
    if (sf.is_open()) {
        while (getline (sf, line) ) {
            cout << line << '\n';
        }
        sf.close();
    }
    else cout << "Unable to open file: " << FILENAME << endl;
    return 0;
}
```

STICKY BIT



C:\users\username\AppData\Local\Temp

Csak a felhasználó számára írható



/tmp

Minden felhasználó számára írható!

```
drwxrwxrwt 55 root root 12288 febr 18 21:50 /tmp
```

r w t

A könyvtárban mindenki csak a saját tulajdonában levő objektumokat törölheti!

SPECIÁLIS JOGOK BEÁLLÍTÁSA

chmod **SUGO** objektum [-R]

4	2	1	4	2	1	4	2	1	4	2	1
s	s	t	r	w	x	r	w	x	r	w	x

rw~~x~~: 4+2+1 = 7
r~~-~~x: 4+0+1 = 5
rw~~-~~: 4+2+0 = 6

```
chmod 4755 /tmp/bash
```

chmod **ki** operandus jog objektum [-R]

g+s: group setuid
u+s: user setuid
o+t: other sticky bit

```
chmod g+s /tmp/bash
```

CSOPORTJOG ÖRÖKLÉSE

Egy könyvtár csoportjogának öröklése a SetGid beállításával és az x törlésével érhető el.

4	2	1	4	2	1	4	2	1	4	2	1
-	s	-	r	w	-	r	w	-	r	w	-

```
chmod 2660 mail
```

```
drw-rwS--- 2 mail users 4096 febr 18 22:31 mail
```

```
touch mail/tesztFile
```

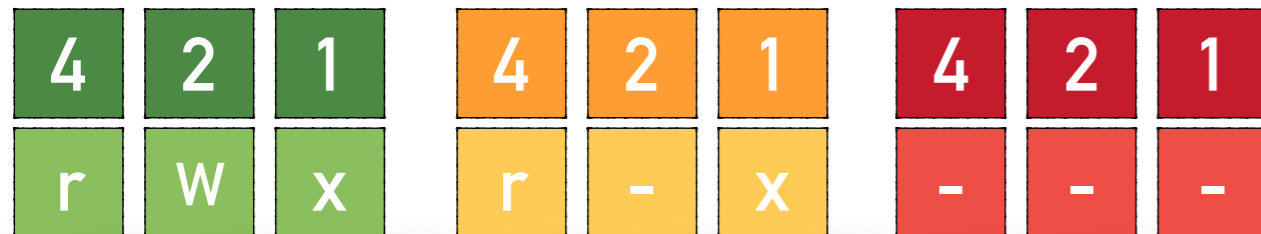
```
ls -l mail
```

```
-rw-r----- 1 root users 0 febr 18 23:32 tesztFile
```

UMASK

A umask az újonnan létrehozott fájlok és könyvtárak alapértelmezett jogosultságát határozza meg. Használata speciális: az egyes értékek meghatározása 7-érték formában történik, vagyis a meg nem adandó jogokat kell paraméterként megadnunk.

umask 027



```
umask 027
```

```
drwxr-x--- 2 root root 4096 febr 18 23:10 Adatok
-rw-r----- 1 root root 0 febr 18 23:11 zh.txt
```

ATTRIBÚTUMOK EXT4 FÁJLRENDSZERBEN

Az attribútumok az egyes fájlokhoz és könyvtárakhoz rendelt kiegészítő értékek, az egyes fájlrendszerek az attribútumok alapján további szolgáltatásokat valósíthatnak meg.

Példa: fájl módosításának és törlésének megakadályozása:

```
lsattr zh.txt
-----e-- ./zh.txt
chattr +i zh.txt

lsattr
----i-----e-- ./zh.txt

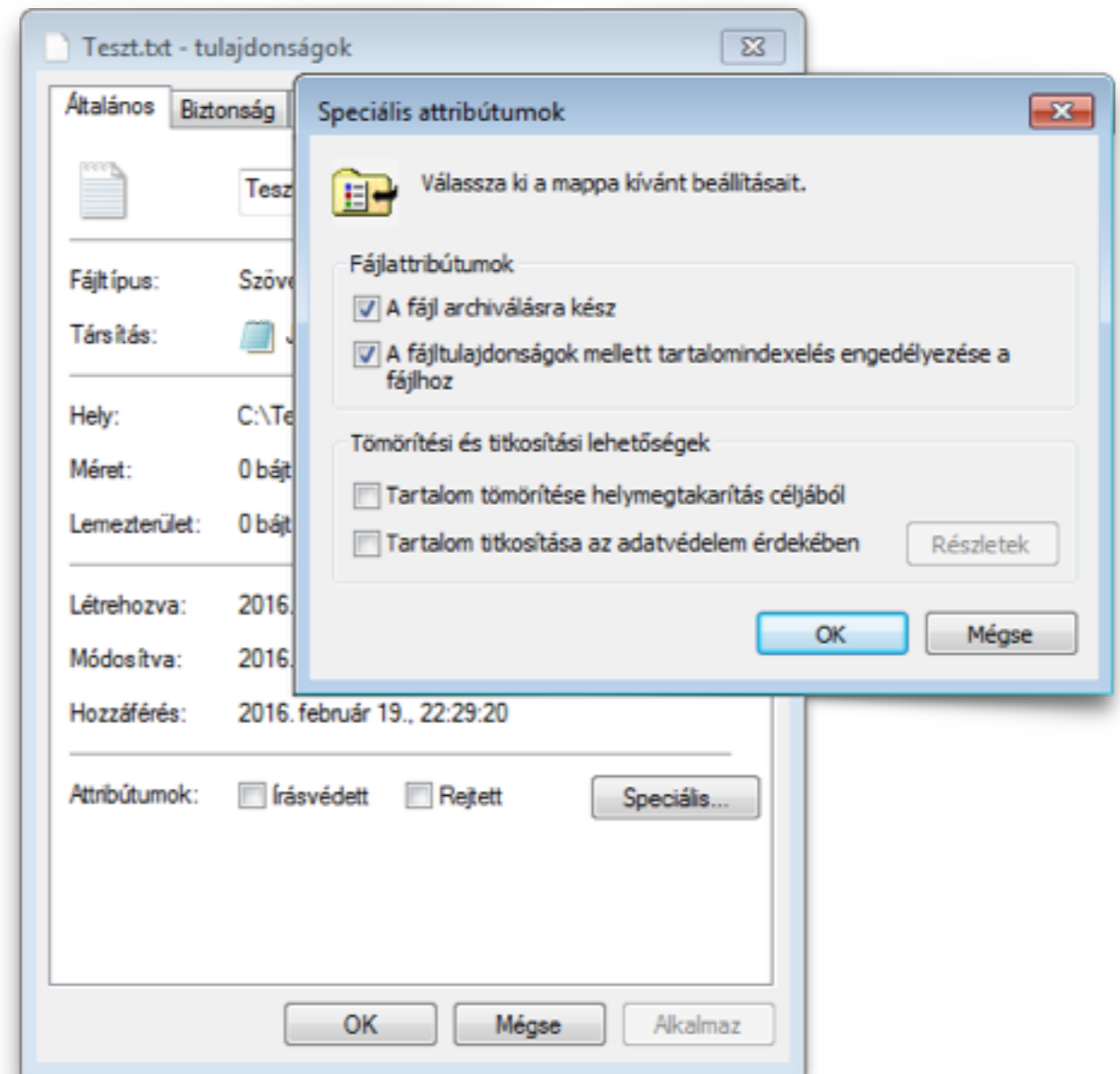
rm zh.txt
-bash: zh.txt: Engedély megtagadva
```

- ▶ append only (a)
- ▶ compressed (c)
- ▶ no dump (d)
- ▶ extent format (e),
- ▶ immutable (i),
- ▶ data journalling (j),
- ▶ secure deletion (s)
- ▶ no tail-merging (t),
- ▶ undeletable (u),
- ▶ no atime updates (A),
- ▶ no copy on write (C),
- ▶ synchronous directory updates (D),
- ▶ synchronous updates (S),
- ▶ top of directory hierarchy (T).

ATTRIBÚTUMOK A MS FÁJLRENDSZEREIBEN

Az írásvédett fájlokat nem lehet módosítani és törölni.

Az "archiválható" attribútum jelentése.

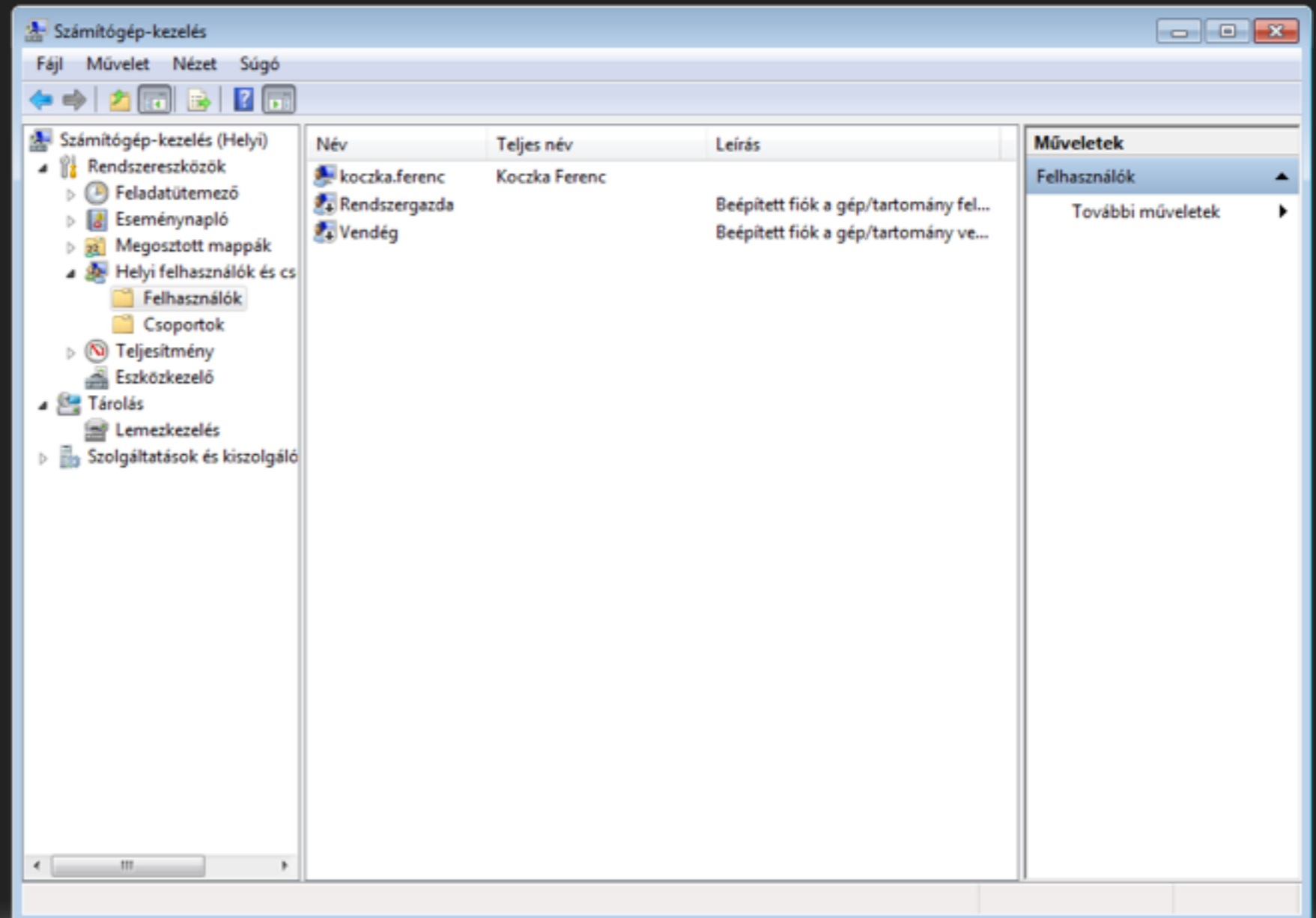


JOGOSULTSÁGI RENDSZER

WINDOWS

WINDOWS

A felhasználók felvétele, a csoportok képzése és a csoporttagság meghatározása ebben a rendszerben is alapvető feladat.



JOGOK BEÁLLÍTÁSA

NTFS alatt a jogosultságok finomabban állíthatók be.

Minden objektumhoz több felhasználó és csoport is rendelhető, és azokra egyenként megadhatók a hozzáférési jogosultságok.

Az egyes jogosultságok kifejezetten tilthatók, először a tiltás érvényesül, csak ez után az engedélyezés.

