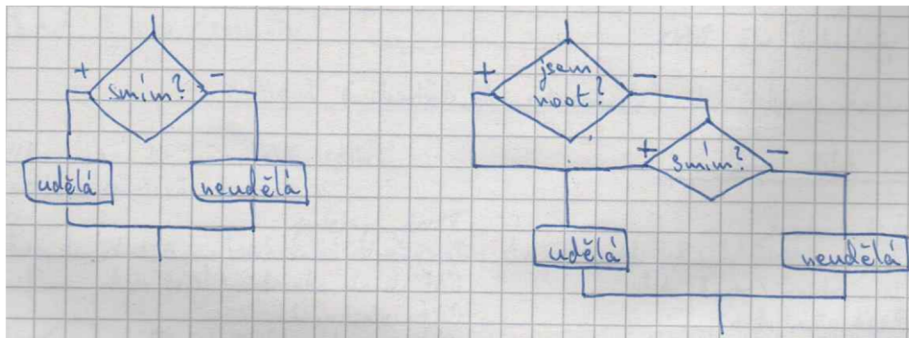


13. Uživatelé a skupiny, práva k souborům a adresářům, srovnání Windows a Linux

WINDOWS – UŽIVATELÉ A SKUPINY

Systémoví uživatelé

- Administrator (výchozí: zakázán, v edici HOME nelze povolit)
- Guest (zakázán)
- Případně + jednotky dalších
- Skrytí – nelze se za ně přihlásit
 - o Trusted installer
 - o Local system
 - o Network system



- Pod adminem je možné vytvořit další uživatele
 - o Jan Novák → jan novák → jan (A) novak (B) → = A1&"."&B1
- Přidávání a editace uživatelů:
 - o 1) Nastavení → Účty → Ostatní uživatelé
 - Pouze
 - Běžný (člen users)
 - Práva (člen administrators)
 - o 2) Start button + right click → Správa počítače → Místní uživatelé a skupiny
 - Úplná správa
 - o 3) Příkazový řádek – používáme při správě více uživatelů
 - Přidat: net user jmeno /add
 - Editovat: net user jmeno
 - Smazat: net user jmeno /delete

Systémové skupiny

- Administrators
- Users
- A další (pro spolupráci se serverem)
 - o Např.: Backup operatos

WINDOWS – PRÁVA K SOUBORŮM A ADRESÁŘŮM

Základní práva

- Norma POSIX
- RWX
 - o R(ead) → číst obsah
 - o W(rite) → vytvářet objekty
 - o (e)X(ecute) → procházet (traverse) soubor; musí být v kombinaci s R(ead)

Práva ACL (Access Control List)

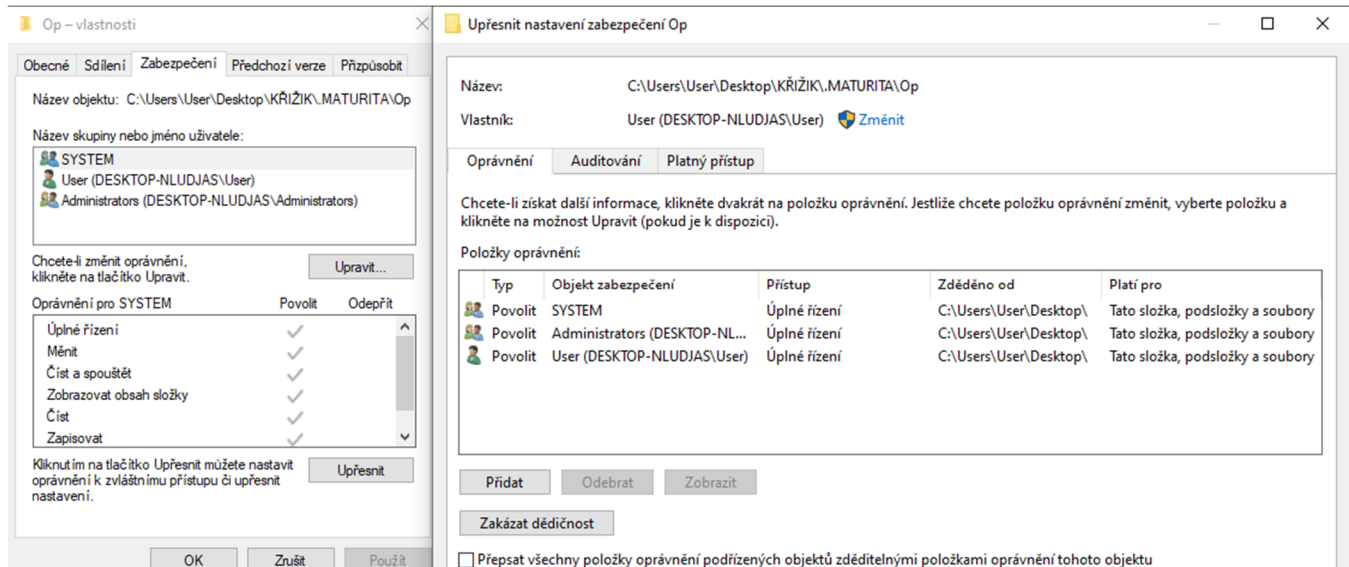
- Seznam uživatelů objektu a jejich oprávnění
- Více možností než POSIX
- Méně přehledné než POSIX
- Ve Windows součástí (v Linuxu lze doinstalovat)
- Seznam ACL oprávnění:

o Full control	=	Plný přístup
o Traverse folder / execute files	=	Procházet adresář / spouštět soubory
o List folder / read data	=	Číst obsah adresáře / číst data souboru
o Read attributes	=	Číst vlastnosti
o Read extended attributes	=	Číst rozšířené vlastnosti
o Create files / write data	=	Vytvářet soubory / zapisovat data
o Create folder / append data	=	Vytvářet adresáře / přidávat data
o Write attributes	=	Zapisovat vlastnosti
o Write extended attributes	=	Zapisovat rozšířené vlastnosti
o Delete subfolders and files	=	Mazat podadresáře a soubory
o Delete	=	Mazat
o Read permissions	=	Číst práva
o Change permissions	=	Měnit práva
o Take ownership	=	Převzít vlastnictví

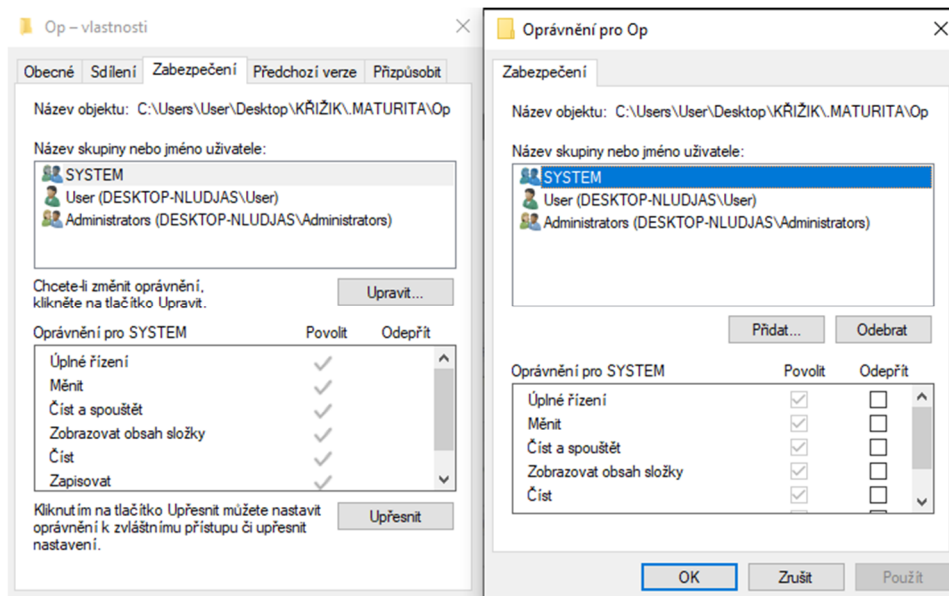
- o traverse = procházet → otevřít složku
- o read = číst → nejde otevřít, ale funguje v textu
- o vytváření souboru → vytvoření souboru
- o zápis dat → zápis dat do souboru
- o zapisovat data → nahradit, např. "Ahkj → Ahoj" (nezmění velikost souboru)
- o přidávat data → zapíše nová data, např. "x → Ahoj" (větší velikost souboru)

Dědičnost

- Objekty dědí práva podle nadřazeného adresáře
- Dědičnost
 - o lze vypnout
 - o lze vynutit



- Vlastnictví – vlastník může nakládat s právy, které má
- Deny > allow



LINUX – UŽIVATELÉ A SKUPINY

Uživatelé

- Seznam v /etc/passwd
- root UID 0
- Mnoho uživatelů systémových služeb UID 1+ (xxx)
- Mnoho uživatelů systémových služeb 3. stran UID 999-
- Vlastní uživatelé UID 1000+

Skupiny

- Každý uživatel má svou skupinu se svým jménem
 - o Pepík má jako svou primární skupinu „Pepík“
- Systémové
 - o 0 ROOT
 - o 1+ systémové
 - o 999- systémové 3. stran
- Vlastní 1000+

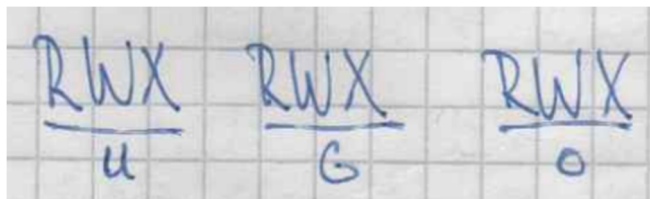
Přidávání

- Uživatelů
 - o adduser → zeptá se na všechno, na heslo apod.
 - o useradd → musíme zadat parametry
 - pokud nebudeme zadávat parametry, uživatel nebude moci nic dělat
- Skupin
 - o groupadd
 - o addgroup

LINUX – PŘÁVA K SOUBORŮM A ADRESÁŘŮM

POSIX práva

- RWX
 - o R → read content
 - o W → write files and folders
 - o X → execute (files) / traverse (folders)
- Vlastník (owner/user)
Skupina (group)
Ostatní (others)
- Soubor → -
Adresář → D
Link → L



- Příklad: -RWXR-XR- -
 - Soubor
 - Vlastník: vše
 - Skupina: číst a spouštět
 - Ostatní: číst

Příkazy pro změnu vlastností

- chown → změna vlastníka
- chgrp → změna skupiny
- chmod → změna práv
- př.:
 - chown _ petr(U):lide(G) _ /home/petr/soubor
 - chmod _ práva _ soubor(nebo adresář)
 - Práva:

RWX R-X R- -
 111 101 100
 7 5 4
 - chmod práva objekt
 - Práva:
 - 750
 - ugoa±rwx → regulární zápis
 ugoa → kdo
 ± → co (přidat/odebrat)
 rwx → právo
 - chmod ug-x soubor
 - odebral jsem vlastníkovi a skupině právo spouštět soubor

LINUX – ATRIBUTY

- Nedědičné
 - PID (Process ID)
 - PPID (Parent PID)
- Dědičné
 - UID (User ID)
 - EUID (Effective UID)
 - Číslo uživatele, pod kterým se má program spustit
 - GID (Group ID)
 - Číslo skupiny, pod kterým se má program spustit
- S – práva
 - SET UID (SUID) 4 000 (000 → práva)
 - Soubory jsou spuštěny s právy EUID
 - SET GID (SGID) 2 000
 - Spuštěny s právy GID
 - STICKY BIT 1 000 → mazat a měnit soubory může jen vlastní

SROVNÁNÍ WINDOWS A LINUX

Správa uživatelů a skupin

- Windows
 - o GUI i příkazový řádek, podpora lokálních i Microsoft účtů, skupinové politiky GPO
- Linux:
 - o Příkazový řádek, uživatelské a systémové účty, konfigurace v souborech /etc/passwd, /etc/shadow

Práva k souborům a adresářům

- Windows:
 - o ACL, práva nastavována přes GUI nebo PowerShell, hierarchické dělení práv
- Linux:
 - o Práva POSIX, správa přes chmod a chown, podpora ACL

Bezpečnostní model

- Windows:
 - o UAC (User Account Control), Active Directory, skupinové politiky
- Linux:
 - o Root uživatel, správa přes sudo, silná kontrola souborů a procesů

Tabulka srovnání

Funkce	Windows	Linux
Primární rozhraní	GUI i příkaz. řádek	Příkaz. Řádek
Správa uživatelů	Lokální i MS účty	Uživatel. a systém. účty
Formát práv	ACL	POSIX
Bezpečnostní mechanismy	UAC, Act. Directory, GPO	Sudo, root, explicitní práva
Dědění práv	Hierarchické	Explicitní, volitelné ACL
Souborové systémy	NTFS, FAT32	Ext4, XFS, Btrfs