# 11. Práce s oprávněními a s registry OS WXP (W7) a dalších OS Microsoftu, Windows – příkazový řádek (základní příkazy OS) práce se soubory

## Oprávnění

Pravidla, která se vztahují k objektům v počítači nebo síti (soubory; složky). Určují, zda má daný uživatel přístup k danému souboru / složce. Mohou být přidělovány uživatelům, skupinám a zabudovaným bezpečnostním objektům.

#### Složka/Soubor 🡪 Vlastnosti 🡪 Zabezpečení

| Úroveň oprávnění | Popis |
| --- | --- |
| Úplné řízení  Full control | Uživatelé mohou zobrazit obsah souboru nebo složky, změnit existující soubory a složky, vytvořit nové soubory a složky a spouštět programy ve složce. |
| Měnit  Modify | Uživatelé mohou měnit existující soubory a složky, ale nemohou vytvářet nové. |
| Číst a spouštět  Read & Execute | Uživatelé mohou zobrazit obsah existujících souborů a složek a mohou spouštět aplikace ve složce. |
| Číst  Read | Uživatelé mohou zobrazit obsah složky a otevírat soubory a složky. |
| Zapisovat  Write | Uživatelé mohou vytvářet nové soubory a složky a provádět změny v existujících souborech a složkách. |

### Skupiny oprávnění

* Administrators
* Power Users
* Users
* Guests

### Poznatky

* Oprávnění lze dědit
  + Složka má určitá práva 🡪 soubory a podsložky v dané složce mají stejná práva
* Pokud není stanoveno oprávnění pro určitého uživatele 🡪 použije se oprávnění skupiny
* Práva může nastavovat pouze vlastník daného souboru/složky, nebo člověk s právem na změnu
* Vlastnictví nemůže být odebráno 🡪 lze pouze předat vlastnictví někomu jinému
* Administrátor nemůže měnit práva (není vlastník) 🡪 Administrátor se může nastavit vlastníkem

## Registry

Souborová databáze, do které Windows ukládá veškerá nastavení (HW, SW, vzhled, uživatelé…). Uspořádána hierarchickou strukturou. Nachází se v „config“ složce (%systemroot%\system32\config). Z těchto souborů se při startu operačního systému zavádí do paměti.

Poprvé se registry objevily ve Windows 3.11. Měly nahradit konfigurační soubory (.ini) starších Windows OS. Registry jsou uspořádány do stromu.

Obsahují Kořenové klíče (Handle Keys; HKEY), které obsahují klíče a podklíče, které obsahují hodnoty (String, Binary, DWORD, QWORD).

### Základní větve registrů

* HKEY\_CLASSES\_ROOT
  + Informace týkající se asociace názvů souborů, tříd souborů
  + Informace nezbytné pro běh softwaru
* HKEY\_CURRENT\_USER
  + Aktivní profil uživatele, který je právě přihlášen do systému (vzhled…)
  + Mapuje se z \_USERS
* HKEY\_LOCAL\_MACHINE
  + Obsahuje hardwarové profily
  + Nastavení pro všechny uživatele a nastavení systému
* HKEY\_USERS
  + Všechny aktuální profily uživatelů
* HKEY\_CURRENT\_CONFIG
  + Konfigurační data aktuálního HW profilu (z \_LOCAL\_MACHINE)
* HKEY\_PERFORMANCE\_DATA
  + Skrytý klíč
  + Obsahuje data kernelu
* HKEY\_DYN\_DATA
  + Pouze u Win 95, 98, ME
  + Informace o HW

### Klíče HKLM

„Hives“; Klíče a podklíče slouží k snadnému organizování dat v registru, stejně jako složky a podsložky k organizování souborů.

* HKLM
  + Vytváří se při každém spuštění počítače pomocí programu ntdetect.com
* SAM
  + Security Account Manager
  + Obsahuje uživatelskou databázi
* SECURITY
  + Obsahuje bezpečnostní informace
* SOFTWARE
  + Nastavení programů instalovaných na počítači
* SYSTEM
  + Nastavení zařízení a služeb v systému

### Hodnoty

Každá hodnota je složená z 3 částí:

* Jméno hodnoty
* Typ hodnoty
* Číselná nebo textová hodnota.

Hodnot existuje víc, ale toto jsou hodnoty, které umožňuje přidat editor registru.

* REG\_BINARY (Binary Value)
  + Binární data obvykle v hexadecimální podobě (00 00 0a 03)
* REG\_DWORD
  + Data představovaná číslem o délce 4 bajty (32bit)
  + Mohou být v binárním, hexadecimálním, nebo decimálním formátu (0x278d00)
* REG\_EXPAND\_SZ
  + Expandovatelný řetězec %hodnota nahrazená aplikací %.. (%SystemRoot%\system32\ntvdm.exe)
* REG\_MULTI\_SZ
  + Vícenásobné řetězce oddělované parametrem null. (System Bus Extender SCSI miniport)
* REG\_SZ
  + Textový řetězec. (True, False,...)
* REG\_QWORD
  + Nová hodnota ve Windows Vista pro data představovaná číslem o délce 8 bajtů (64bit).

## Práce s oprávněními a s registry OS Windows

Práce s registry jsou velice nebezpečné 🡪 Nesprávné nastavení registrů může způsobit vážně chyby systému. Existuje několik programů pro práci s registry (defragmentace, editace…). Integrovaný REGEDIT, Register Crawler, Advanced Registry Tracer…

### Zakázání editace registrů

#### HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System 🡪 DWORD DisableRegistryTools 🡪 1 🡪 Restart

## Windows příkazová řádka (cmd)

Uživatelské rozhraní, ve kterém uživatel s programy nebo operačním systémem komunikuje zapisováním příkazů do příkazového řádku. Umožňuje ovládat počítač pomocí textových příkazů (bez použití myši).

### Výhody

* Nižší HW nároky
* Historie příkazů
* Tvorba skriptů (baťáků)

### Nevýhody

* Znalosti syntaxe
* Nevhodné pro začátečníky

### Syntaxe

#### prikaz [prepinace] [parametry]

### Dávkové soubory

* Textové soubory s příponou .bat
* Posloupnost příkazů
* Spuštěny a vykonány cmd
* Mohou obsahovat podmínky, cykly…

### Základní příkazy

* Interní
  + Součástí kódu příkazové řádky
  + COPY
  + REN
  + DIR
  + MD
  + CLS – clear screen
* Externí
  + Programy jako ostatní
  + Komunikují prostřednictvím cmd
  + MOVE
  + XCOPY – kopíruje adresářové struktury
  + FORMAT