Registry



Bc. Lukáš Patka

Registry

- centrální úložiště konfiguračních dat
- nastavení HW, ovladačů, konfigurace OS, aplikací, lokálních zásad, uživatelských preferencí,..
  - systémové nástroje (mmc, konfigurační dialogy) jsou jen user friendly rozhraní pro editaci registrů
- hierarchická struktura
- jednotný formát
- možnost nastavení oprávnění

Trocha historie

- MS-DOS
  - Config.sys – načtení ovladačů
    - device=c:\windows\himem.sys
      device=c:\windows\emm386.exe
      dos=umb,high,auto
      files=150
      device=c:\dos\CDromDriver.sys
      device=c:\dos\SoundDriver.sys
      device=C:\WINDOWS\COMMAND\display.sys con=(ega,,1)
      Country=042,852,C:\WINDOWS\COMMAND\country.sys
  - Autoexec.bat – spuštění programů, proměnné prostředí
    - mode con codepage prepare=((852)
      C:\WINDOWS\COMMAND\ega.cpi)
      mode con codepage select=852
      keyb cz,,C:\WINDOWS\COMMAND\keybrd2.sys
      LH c:\windows\command\mscdex.exe
      LH c:\dos\mouse.com
      PATH=C:\DOS;C:\WINDOWS
  - každá aplikace si ukládá nastavení po svém

Trocha historie

- Windows 3.0
  - *.INI – ukládání nastavení do textových souborů
    - [mysqld]
      default-character-set = utf8
      language = english
      max-connections = 60
    - plochá struktura, komplikované ukládání binárních hodnot, nestandardizované (podobná nastavení v různých aplikacích nemají jednotný formát)
- Windows 3.1
  - zrod registrů
    - vytvořeny pro ukládání informací o typech souborů, registrace OLE objektů
- Windows 95 ..
  - Registry se stávají „srdcem a duší systému“

Struktura registrů

- Subtree
  - HKEY_LOCAL_MACHINE (HKLM)
  - HKEY_USERS (HKU)
  - pro snazší orientaci jsou předdefinovány další subtrees (odkazují do výše uvedených kořenových subtrees):
    - HKEY_CLASSES_ROOT (HKCR)
      - HKLM\Software\Classes + HKCU\Software\Classes
    - HKEY_CURRENT_USER (HKCU)
      - HKU\"SID aktuálně přihlášeného uživatele"
    - HKEY_CURRENT_CONFIG (HKCG)
      - HKLM\SYSTEM\CurrentControlSet\Hardware Profiles\Current
- Key
  - obdoba složek/podsložek
- Entry
  - každý key má alespon jeden entry (default)
  - každý entry má 3 položky: název, typ, hodnota

Datové typy

- REG_SZ
  - String
- REG_BINARY
  - binární data (hexadecimálně)
- REG_DWORD
  - 1-8 hexa číslic (32b)
- REG_MULTI_SZ
  - víceřádkový String
  - null (0x00) ukončuje řádek, 2x null ukončuje celý seznam
- REG_EXPAND_SZ
  - String + expanze proměnných (%systemroot%)

Hive files, HKLM

- fyzická reprezentace registrů na disku
- HKLM
  - %SystemRoot% \System32\config

HKLM\SAM	SAM, SAM.LOG
HKLM\SECURITY	SECURITY, SECURITY.LOG
HKLM\SOFTWARE	Software, Software.log, Software.sav
HKLM\SYSTEM	System, System.log, System.sav

  - bez přípony: hive file
  - .alt: System.alt je záložní kopie System hive, ve WinXP se nepoužívá
  - .log: transakční log pro danou hive, pokud systém během updatu registrů zhavaruje, po restartu je na základě info z .log obnoven do původního stavu
  - .sav: záložní kopie dané hive vytvořená po dokončení text-mode fáze instalace systému, pokud selže graphic-mode fáze instalace -> po restartu se obnoví hive files a zopakuje se jen graphic-mode fáze instalace, updatují se pouze v případě reinstalace (opravy) systému
- HKLM\SYSTEM\CurrentControlSet\Control\hivelist

Hive files, HKU

- HKU

HKU\SID	%UserProfile% \NTUSER.DAT
HKU\SID_Classes	%UserProfile% \Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
HKU\.Default	%SystemRoot%\System32\config\default

- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList
  - seznam hive files všech uživatelů

HKEY_CLASSES_ROOT

- přípony souborů, asociace přípon s typem souboru
  - HKCR\.txt\(Default) = „txtfile”
  - HKCR*\OpenWithLIst
- Definice tříd
  - Úplný název typu souboru
    - HKCR\txtfile\(Default) = „Text document“
  - Příkazy pro otevření/tisk daného typu souboru
    - HKCR\txtfile\shell\open\command = „%SystemRoot%\system32\NOTEPAD.EXE %1 “
    - HKCR\txtfile\shell\print\command = „%SystemRoot%\system32\NOTEPAD.EXE /p %1 “
  - Informace pro správu embedded objektů daného typu souboru
  - přidělení ikony, povolení quick view
- CLSID (class identifier)
  - Každý OLE objekt má jedinečný class identifier
  - HKCR\CLSID
    - My Computer{20D04FE0-3AEA-1069-A2D8-08002B30309D}
    - Administrative Tools{D20EA4E1-3957-11D2-A40B-0C5020524153}
    - Run{2559A1F3-21D7-11D4-BDAF-00C04F60B9F0}
  - Samotné třídy obvykle editovat nepotřebujeme
  - jejich identifikátory můžeme využít v dalších klíčích, př: HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\HideDesktopIcons\NewStartPanel

HKEY_CURRENT_USER

- nastavení interaktivně přihlášeného uživatele
  - AppEvents- přiřazení zvuků různým událostem (otevření menu, odhlášení ..)
  - Console- nastavení konzolí (character-mode applications), včetně příkazového řádku
  - Control Panel- nastavení, která běžně konfigurujeme přes ovládací panely
  - Environment- uživatelské proměnné prostředí
  - Identities- definice identit pro MS Outlook Express
  - Keyboard Layout- přidání/odebrání rozložení klávesnice (Keyboard Layout\Preload)
  - Network- mapované sítové disky
  - Printers- uživatelské preference tiskáren
  - Software- standardizovaná struktura Software\výrobce\program\verze
    - Software\Microsoft\Windows\CurrentVersion
  - Volatile Environment- proměnné nadefinované pro danou session, neukládají se po odhlášení

HKEY_LOCAL_MACHINE

- nastavení HW, nastavení systému a aplikací vztahující se na všechny uživatele
  - HARDWARE. Stores data describing the hardware that Windows detects as it starts. The operating system creates this key each time it starts, and it includes information about devices and the device drivers and resources associated with them. This key contains information that IT professionals find useful during a network inventory.
  - SAM (Security Accounts Manager)- databáze uživatelských účtů a skupin
    - oprávnění pro čtení nemá ani skupina Administrators
    - odkazuje do HKLM\SECURITY\SAM
  - SECURITY- bezpečnostní nastavení systému
    - oprávnění pro čtení nemá ani skupina Administrators
  - SOFTWARE- nastavení SW vztahující se na všechny uživatele
    - Klíče mají stejnou strukturu jako HKCU\Software
  - SYSTÉM- konfigurace HW, služeb
    - Systém obsahuje alespon dva ControlSets (aktuální a záložní)
    - HKLM\SYSTEM\CurrentControlSet odkazuje na aktuální ControlSet
    - HKLM\SYSTEM\Select určuje role uložených ControlSets
      - Current, Default, Failed, Last known good

HKEY_USERS

- Uživatelská nastavení SW
  - .Default- nastavení, které systém použije pro zobrazení plochy předtím než dojde k přihlášení uživatele
    - Neplést s default user profile
  - SID- nastavení uživatele s daným SID
    - whoami /user /sid ..zobrazí SID přihlášeného uživatele
  - SID_Classes- uživatelské definice tříd, uživatelské asociace přípon s typem souboru

Nástroje pro správu registrů

- regedit
- reg /query /add /delete /save /restore ..
- SubInACL (http://support.microsoft.com/kb/265360)
- regmon (http://www.microsoft.com/technet/sysinternals/utilities/regmon.mspx)
- API: RegCloseKey, RegOpenKey, RegConnectRegistry, RegCreateKey, ..