Přijde programátor ke kamarádovi adminovi a hned ve dveřích vidí, že chudák sedí u stolu, všechny prsty na klávesnici a zkouší nohou vytáhnout šňůru ze zásuvky.

„Co se děje?!" „Ale stáhl jsem si nějaký program a když sem ho pustil, tak se vypsalo: Zmáčkni současně deset libovolných kláves a uvidíš super obrázky ženských. Tak jsem ty klávesy zmáčkl a objevilo se: Pusť jedinou z nich a zformátuju ti disky."

Podzim 2008

PV175 SPRÁVA MS WINDOWS I

Microsoft Management Console
Zálohování

MMC

- Microsoft Management Console
- Základní nástroj centrální správy operačních systémů Windows
- Hostitel pro jednotlivé utility – snap-iny
- V současnosti verze 3.0

Centralizace správy

- Z konzole spuštěné na lokálním počítači je možné provádět změny nastavení na lokální i vzdálené stanici
  - Stejné správcovské účty
  - RPC (port 530)
- Samo o sobě není příliš škálovatelné
- Hierarchie zásad skupiny
  - Lokální nastavení počítače jsou překryta nastaveními z domény

Hlavní MMC snap-iny

- Místní uživatelé a skupiny
- Prohlížeč událostí
- Sdílené složky
  - net share
  - Některá další přednáška
- Služby
- Správa disků
- Správa počítače
- Editor objektů Zásady skupiny

Zásady skupiny

- Group Policy (GPO)
- Položky ovlivňující vnitřní chod a požadavky na systém
- Aplikace zásad: čas / gpupdate
- Oddíly
  - Konfigurace počítače
  - Konfigurace uživatele
- Položky
  - Nastavení softwaru
  - Nastavení systému Windows
  - Šablony pro správu

GPO - Skripty

- Skripty = sekvence příkazů, které mají být vykonány
  - Soubory *.cmd, *.vbs,…
  - Spouštěcí a ukončovací (PC)
  - Přihlašovací a odhlašovací (user)
    - Při zpracování zásad skupiny není možné u počítačů nezařazených v doméně systémově odlišit jednotlivé uživatele. Rozlišení je však možné na základě proměnné %username%

GPO - Nastavení zabezpečení

- Zásady účtů
  - Zásady hesla
    - Specifikace požadavků na složitost přihlašovacích hesel a jejich změny
    - Komplexita, maximální a minimální délka hesla, minimální stáří hesla, historie hesel
  - Zásady uzamčení účtu
    - Reakce na zadání špatného hesla
    - Doba uzamčení účtu, počet pokusů, doba do vynulování čítače

GPO – Místní zásady

- Zásady auditu
  - Výchozí: stanice bez auditování
  - Necitlivě nastavené požadavky na audit mohou vážně ovlivnit výkon stanice
  - Security log
- Přiřazení uživatelských práv
  - Specifikování, kteří uživatelé mohou vykonávat určité činnosti
  - Blíže některá další přednáška

GPO – Šablony pro správu

- Nastavení především vzhledu a chování počítače nebo jeho jednotlivých aplikací
- Omezení přístupů k ovládacím panelům, položkám nabídky Start apod.

Správa disků

- Přehled o stavu fyzických disků v počítači a logických oddílů na nich
  - Inicializace disků
  - Vytváření oddílů
  - Rušení oddílů
  - Formátování oddílů
  - Změny písmena oddílu
  - Přimountování disku ke složce

Diskové kvóty

- Systémy Windows umožňují vymezení maximálního dostupného místa na disku pro každého uživatele zvlášť
- Při překročení vyhrazeného limitu je možné zakázat další zápis
  - V takovém případě disk (oddíl) nehlásí skutečnou kapacitu, ale pouze přidělenou
- Běžné je omezení velikosti uživatelského profilu

Další MMC snap-iny

- Defragmentace
  - dfrg.msc
  - Princip ukládání souborů v moderních souborových systémech (ve Windows je jím obvykle NTFS) přináší „kouskování“ (fragmentaci) velkých souborů, která může negativně ovlivňovat rychlost práce s nimi
  - Defragmentace je proces spojování jednotlivých částí do větších celků
- Výsledná sada zásad
  - rsop.msc
  - Výpis aktuálních zásad

Zálohování I

- Backupy, backupy, backupy ☺
- Zálohování
  - Data
    - Ruční / automatické kopírování
  - Systémová konfigurace
    - Export a import klíčů registru
    - Jak uchovat například účty?
  - Obojí
    - Image nástroje třetích stran
    - ntbackup

Zálohování II

- ntbackup
  - Integrace s naplánovanými úlohami
  - Zálohování na úrovni souborů (celé disky, složky nebo i jednotlivé soubory)
  - System state backup
    - Bootovací soubory
    - Databáze objektů počítače
    - Registry
  - Některé soubory nejsou nikdy zálohovány (např. pagefile.sys)

Zálohování III

- Typy záloh
  - Normální
    - Označí soubory za zálohované
  - Kopie
    - Vše, ale neoznačí soubory jako zálohované
  - Rozdílová
    - Zálohuje pouze nové soubory, ale neoznačí je za zálohované
  - Přírůstková
    - Zálohuje pouze nové soubory

Best practices

- Nastavit diskové kvóty pro profily a případně i data uživatelů
- Backupy, backupy, backupy
- Princip minimálních oprávnění
- Auditovat kritické zdroje
- Najít vhodnou rovnováhu mezi zabezpečením hesel a uživatelskou přijatelností
- Naučit se skriptovat ☺

Univerzitní počítačové studovny

- Redundantní diskové pole pro profily (2 TB kapacita)
- Kvóta pro uživatelský profil = 100 MB
- Záznam o každém přihlášení a odhlášení uživatele + přístupové body (turniket, čtečky karet u dveří)
- cca 800 centrálně spravovaných stanic, 50000 uživatelských účtů
  - Nutné je mít doménu ;-)

Dotazy?

Díky za pozornost