User: Vypnul se mi počítač, tak volám admina. Přichází admin, těžce vzdychne, něco si mumlá pod nos, asi 10 krát se otáčí na mé židli, kopne do počítače a ten se zapíná. Znova si těžce povzdychne, stále mumlá a odchází. On je prostě šaman!

Admin: Zavolali mě k uživateli… ten idiot se pořád točil na židli, až se mu na ní namotal kabel ze zástrčky. Tiše nadávám, rozmotávám kabel, odkopávám počítač co nejdál pod stůl, zapínám ho, nadávám, odcházím.

Podzim 2008

PV175 SPRÁVA MS WINDOWS I

Základní nastavení

Ovládací panely

- Obsahují nejzákladnější prvky nastavení počítače
- Obvykle soubory s příponou *.cpl uložené v %systemroot%/system32
- Mnohá nastavení jsou přístupná pouze členům skupiny Administrators
- Je možné omezit přístup pouze k těm položkám ovládacích panelů, které uživatel potřebuje

Systém

- Základní parametry počítače a operačního systému
- Zařazení do domény a pracovní skupiny
- Správce zařízení a ladění výkonu
- Aktivování Remote Desktopu
- Proměnné prostředí
  - Specifikování trvalých proměnných příkazové řádky

Vzhled

- Zobrazení
  - HW nastavení (rozlišení obrazovky, použité ovladače)
  - SW nastavení (theme plochy, pozadí plochy, vzhled oken)
  - Spořič obrazovky
- Hlavní panel a nabídka Start
  - Vzhled Start menu
  - Zobrazení ikon v systray

Naplánované úlohy

- Vytváření dávek / jobů
  - Spuštění určitého programu v daný čas s právy libovolného uživatele nebo systému
  - Tento uživatel nemusí být přihlášen
  - Probíhá na pozadí
  - Typickým využitím jsou skripty provádějící opakované úlohy (př. mazání dočasných souborů) a plánování záloh
- Složka %systemroot%/Tasks
- schtasks v příkazové řádce

Přidat nebo odebrat programy

- Přidání součástí Windows
- Převážně pro odinstalace
- Seznam aplikovaných záplat
  - Odebrání záplat je možné pouze v případě, kdy jsou uchovány záložní soubory (u unattended integrovaných patchů to není možné) a pouze pokud to umožňuje samotná záplata.
    - Windows Genuine Advantage nejde ;-)

Centrum zabezpečení

- Uvedeno v XP Service Pack 2
- Sdružuje 3 nejběžnější bezpečnostní prvky
  - Automatické aktualizace
  - Brána firewall
    - Firewall = zařízení nebo program chránící vnitřní perimetr na základě předdefinovaných pravidel
  - Ochrana proti virům
    - Monitoring antivirů (funkčnost, aktuálnost)

Brána firewall

- Od Windows XP SP2 obousměrný firewall
- Pracuje na transportní vrstvě TCP/IP modelu, rozlišení probíhá na základě IP adres a portů
- Centrální správa přes Group Policy
- Deaktivováno v případě použití firewallů třetích stran

Automatické aktualizace

- Každý počítač by měl být aktualizován
- Problematická může být instalace záplat – většinou je vyžadován (obtěžující) restart
  - V zájmu administrátora je restart vynutit
- Aktualizace probíhají proti serverům v Internetu nebo vlastnímu serveru WSUS

Možnosti složky

- Přístupné i z nabídky Nástroje otevřeného okna složky
- Zobrazení a změny asociace přípon souborů k programům
- Parametry zobrazení souborů
  - „Použít zjednodušené sdílení souborů (doporučeno)“
  - „Skrýt příponu souborů známých typů“

Služby I

- Procesy běžící (neviditelně) na pozadí
- Spouštěny bez intervence uživatele
- Pracují pod systémovými účty (system, network service) nebo prostřednictvím systémových procesů (svchost.exe,…)
- Management služeb může citelně ovlivnit výkonnost počítače a jeho funkcionalitu

Služby II

- Nástroje pro management služeb
  - Task manager
    - Ctrl+Shift+Esc
    - Zobrazení (a zabití ☺) běžících procesů.
  - msconfig
  - services.msc
  - Process explorer (SysInternals)
    - Zdokonalený task manager, umožňuje navíc zobrazit propojení systémových procesů a konkrétních služeb.

Logy I

- Event Viewer (eventvwr)
- Uchovávají záznamy o událostech
- Typy záznamů
  - Information (Informace)
    - Běžná zpráva informující o stavu.
  - Warning (Upozornění)
    - Varovná zpráva indikující problém, který zatím neovlivňuje chod systému.
  - Error (Chyba)
    - Kritická chyba
  - Success Audit + Failure Audit

Logy II

- Položky logů
  - Application
    - Informace od běžících aplikací.
  - Security
    - Záznamy o přístupech ke zdrojům.
  - Systém
    - Obecné informace systému.
  - Mnoho dalších, které jsou vytvářené pouze v případě používání dané služby (DNS, Active Directory, DHCP,…)

Logy III

- Důležitá je proaktivní kontrola
- Motto:
  - „Každý warning časem přejde buď v Information (problém vyřešen) nebo v Error (problém graduje).“
- Řešení problémů v současných Windows se často omezuje na dohledání čísla události na Google.

Best practices

- Kontrolovat pravidelně logy
- Používat v IT infrastruktuře organizace vlastní server WSUS a pravidelně aktualizovat spravované počítače
- Backupy, backupy, backupy
- Zakázat nepotřebné služby
- Používat firewall případně i antivir

Klávesové zkratky

- Win+D zobrazí plochu
- Win+E Tento počítač
- Win+F Hledat
- Win+L zamkne relaci
- Win+M minimalizuje všechna okna
- Win+R Spustit

Dotazy?

Díky za pozornost