Anonym poslal otázku na administrátora: „Nezdá se ti blbý odpovídat na anonymní otázky z internetu?“
Adminova odpověď: „Odpovídám zadavateli anonymní otázky, majiteli IP 90.176.19.53, broadband9.iol.cz, Jaroslavovi Jakubcovi, bytem v Kolíně, Kutnohorská 153, rodné číslo 881012/1254, číslo účtu 453897129/0300: NE NEZDÁ!“
(www.tuningpc.cz)

Podzim 2008

PV175 SPRÁVA MS WINDOWS I

Uživatelé a skupiny

Motivace

- K čemu potřebujeme uživatelské účty?
  - Řízení přístupu ke zdrojům
  - Auditování a právní odpovědnost
  - Vlastní nastavení, personalizace
  - Více relací zároveň

Security principal

- Jako security principal označujeme každý objekt, který má vlastní identifikátor SID (počítač, uživatelský účet, skupina,…)
- SID = řetězec znaků jednoznačně identifikující nějaký objekt
  - (př.: S-1-5-21-1559272821-92556266-1055285598-500)
- Vnitřní rozlišení probíhá na základě SID, ne jména (!!)

Pracovní skupina

- Volné uskupení počítačů v síti, všichni účastníci jsou si rovni (peer-to-peer)
- Každý počítač si udržuje vlastní databázi uživatelských účtů a skupin
- Případnou změnu je nutné provádět na několika počítačích
- Jednoduché, nevyžaduje širší znalosti
- Přijatelné do zhruba 10 spravovaných počítačů

Doména

- Logické uskupení počítačů v síti s jedním nebo více dedikovanými servery, které hostují databázi uživatelů (tzv. doménové řadiče)
- Centralizovaná správa
- Single sign-on
- Škálovatelnost
- Provázanost s dalšími službami
- Určeno do prostředí všech velikostí

Lokální a doménové účty

- Lokální účet
  - Uložen v registrech
  - Poskytuje přístup ke zdrojům lokálního počítače
- Doménový účet
  - Uložen na doménovém řadiči
  - Poskytuje přistup ke zdrojům v celé doméně (tj. ke všem počítačům v doméně zařazeným)
  - viz PV176 Správa Windows II

Autentizace

- Práce s operačním systémem je podmíněna úspěšnou autentizací
  - Něco co mám – token (čipová karta,…)
  - Něco co vím – heslo, PIN, passphrase
  - Něco co jsem – biometrika (otisk prstu,…)
- V doméně se vzájemně autentizují i počítače bez přispění uživatele.

Uživatelský účet

- Reprezentace osoby uživatele v kontextu počítače
- jméno: proměnná %username%
- Chráněný heslem / bez hesla (takový účet se nemůže připojovat vzdáleně)
- Vestavěné:
  - Administrator
  - Guest
  - Help Assistant

Skupiny

- Kontejner na uživatele
- Použití skupin zjednodušuje a zpřehledňuje správu uživatelských účtů (řízení přístupu na základě členství ve skupině)
- Klientská Windows neumožňují vnořování skupin

Built-in skupiny

- Administrators
  - Skupina správců s plným přístupem
- Backup Operators
  - Skupina osob s právem obejít NTFS oprávnění při zálohování
- Guests
  - Skupina hostů
  - Mají stejná práva jako běžní uživatelé, default: disabled
- Network Configuration Operators
  - Skupina správců nastavení sítě
- Power Users
  - Skupina uživatelů s rozšířenými právy (vytváření účtů atd.)
- Remote desktop users
  - Skupina uživatelů s právem vzdáleného připojení
- Users
  - Běžní uživatelé

Identity

- Dynamický typ built-in skupin (uživatele do / z nich umísťuje pouze systém)
- Authenticated users
  - Všichni autentizovaní uživatelé
- Anonymous logon
  - Osoby připojené bez přihlášení, již zastaralé
- Everyone
  - Všichni uživatelé
- Interactive
  - Uživatelé „sedící přímo u počítače“
- Network
  - Uživatelé připojení vzdáleně přes síť

Uživatelský profil

- Seskupení uživatelských dat a nastavení (pouze ta specifická pro každého uživatele)
- cesta: %userprofile%
- Typy:
  - Lokální – použitelné pro počítače nepropojené do sítě
  - Cestovní (roaming) – uložen centrálně, „cestuje“ s uživatelem od PC k PC

Grafické nástroje

- nusrmgr.cpl
  - Prvek Control panelu, pouze přidávání a odebírání uživatelů a změny hesel.
- control userpasswords2
  - Zařazování do skupin
  - Ctrl+Alt+Del logon
- mmc (Místní uživatelé a skupiny)
  - Nejobsáhlejší nastavení pro počítače mimo doménu, i správa Built-in security principals.
- Remote Desktop

Konzolové nástroje

- runas
  - Umožňuje provedení zadaného příkazu s právy jiného uživatele než je právě přihlášen.
- net user
  - Umožňuje přidání / odebrání uživatelského účtu přes příkazovou řádku.
- psgetsid (pstools)
  - Zobrazí SID požadovaného účtu.

Best practices

- Pracovat s právy běžného uživatele, jako administrátor se přihlásit pouze k provedení potřebného úkonu
- Používat silná hesla (…a nepsat si je na papírek přilepený na monitor)
- Bezpečnost x uživatelská přijatelnost
- Zakázat účet Administrator, přejmenovat účet Guest na Administrator (?)
- Dodržovat zásadu 1 účet = 1 člověk

Masarykova univerzita

- Nařízení rektora, že k počítačům připojeným do univerzitní sítě nelze přistupovat anonymně.
- Snaha o sjednocení – použití jediného účtu pro připojení na libovolný počítač nebo do libovolné bezdrátové sítě.
- Centrálně uložené profily (FI, UPS)

Dotazy?

Díky za pozornost