Local Policies, Audit událostí



Bc. Šimon Suchomel

Group Policy

- Centralizovaná konfigurace systému
- Používané hlavně v enterprise prostředí
- Ovšem konfigurace běžná pro počítače sloužící konkrétním účelům
- Omezení určitých akcí z hlediska bezpečnosti (knihovny, veřejná místa, kavárna, …)

Local Group Policy

- Zjednodušená verze GP pro lokální počítač
- Nelze měnit politiky pro určité uživatele, či skupiny
- Dá se obejít přes editor registrů, ?
- Windows Vista umožňuje použití Multiple Local Group Policy Objects

Konfigurace politiky hesel

- Pro zvýšení zabezpečení uživatelských účtů
- Můžeme specifikovat jak dlouho bude heslo platné
- Vynutit minimální délku hesla
- Windows Settings -> Security Settings -> Account Policies -> Password Policy

Možnosti

- Enforce Password History
  - # hesel držené v historii, 0 – 24, udává kolik nových hesel musí uživatel použít, než použije staré
- Maximum Password Age
  - # dní možnosti používat stejné heslo, 0 vypnuto
- Minimum Password Age
  - # dní po které nemůžeme heslo změnit
- Minimum Password Length
  - 0 – 14, 0 heslo být nemusí
- Passwords Must Meet Complexity Requirements
  - Musí mít splňovat výše uvedené a musí obsahovat velká písmena, čísla, speciální znaky

Account Lockout Policy

- Systém zamkne účet za určitých okolností
- Account Lockout Duration
  - 0 až 99,999 minut, 0 navždy
- Account Lockout Threshold
  - Po kolika špatných pokusech zadat heslo se účet zamkne 0 až 999, 0 = nikdy
- Reset Lockout Counter After
  - # minut, než se resetuje čítač špatných zadání, 1 až 99,999

Uživatelská práva – User Rights

- Přiřadit specifická práva uživatelům a skupinám
- Každé právo umožňuje provádět specifické akce
- Práva jsou kumulativní, přiřazovat skupinám a ne uživatelům
- Windows Settings -> Security Settings -> Local Policies -> User Right Assignments

Privilegia = Privileges

- Privilegium je uživatelské právo, které umožňuje provádět specifické úkony
- Většinou ovlivňující celý systém než konkrétní objekt
- Change The System Time
  - Umožňuje změnit interní čas počítače
- Create A Pagefile
  - Vytvoření a změna stránkovacího souboru
- Force Shutdown From A Remote System
- Shut Down The Systém
  - Členské servery Administrators, Backup Operators, and Power Users
  - Doménové řadiče Administrators, Account Operators, Backup Operators, Print Operators, a Server Operators
- Take Ownership Of Files Or Other Objects

Logon Rights

- Access This Computer From The Network
  - Připojit se k počítači přes síť
- Deny Access To This Computer From The Network
- Log On Locally
  - Přihlásit se použitím lokální klávesnice

Audit událostí

- Umožňuje sledovat aktivity systému a uživatele
- Aktivity se nazývají „events“ události
- Použitím auditu systém zapíše události do Security log, které obsahují
  - Jaká akce se stále
  - Jaký uživatel ji vyvolal
  - Úspěch nebo neúspěch a kdy se to stalo
- Politika auditu definuje jaké záznamy v logu budou
- Systém zapíše události do logu na tom počítači, kde se událost vyskytla

Co auditovat?

- Typy událostí
  - Přístup k souborům a adresářům
  - Přihlašování a odhlašování
  - Vypínaní a zapínání počítače
  - Změna uživatelů a skupin
  - Změny v objektech AD
- Úspěch / neúspěch
- Definovat užitečnou auditovací politiku
- Pravidelně kontrolovat security log

Požadavky

- Nejdříve je potřeba nastavit na každém počítači auditovací politiku a poté je možné konfigurovat audit na souborech, adresářích a tiskárnách
- Musíme mít uživatelské právo Manage Auditing And Security Log
- Pro audit souborů a adresářů musí být na NTFS svazku
- 2 fázový proces
  - Nastavit na každém počítači auditovací politiku
  - Povolit konkrétní audit

Nastavení auditovací politiky

- Windows Settings –> Security Settings -> Local Policies -> Audit Policy
- Account Logon Events
  - Ověření uživatele na DC (jen AD)
- Account Management
  - Operace s účty a skupinami, změna hesla, povolení / zakázání účtu
- Directory Service Access
  - Přístup k objektu AD, k jakým objektům se musí specifikovat

Auditovací politiky

- Logon Events
  - Přihlášení / Odhlášení, připojení / odpojení přes síť
- Object Access
  - Přístup k souboru, adresáři, tiskárně
- Policy Change
  - Změna v user security options, user rights, or audit policies
- Privilege Use
  - Uživatel uplatnil právo, např. změna systémového času (nevztahuje se na práva přihlašování a odhlašování)
- Process Tracking
  - Program provedl nějakou akci.
- System Events
  - Restart nebo vypnutí počítače. Události, které ovlivňují bezpečnost a security log

Aplikace auditu

- Po nastavení politiky je nutný restart
- Auditování souborů a adresářů
  - Záložka Security vlastností složky
  - Advanced nastavení, karta Auditing
- Auditování u tiskáren analogicky

Prohlížeč událostí = Event Viewer

- Defaultně 3 logy
  - Application log
    - Varování, chyby a informace jednotlivých programů, specifikuje vývojář programu
  - Security log
    - Úspěch či neúspěch audit událostí
  - System log
    - Varování, chyby a informace generované systémem
- Eventvwr
- Hledání, filtrování, správa logů, archivace logů