Nové politiky pro administraci Windows Vista

Ing. Bohuslav Frk

digitwins

Microsoft Certified Systems Administrator

Politiky (GPOs)

- Ve světě W2000 výše jde o dynamický zápis do registrů (Potřeba Group policy-aware aplikace)

- **Lokální**
  Na každém počítači, i když není v síti mimo řadičů domény
  Defaultně nastaveno pouze Security settings.
  Má nejnižší prioritu
  Nemá spoustu nastavení
- **Doménová**
  Vytvořena v AD a uchovávána v SYSVOLu na každém řadiči
  Minimálně Default Domain Policy a Default Domain Controller Policy
  Na stanicích se aplikují 90 +/-(0-30)minut (lze urychlit přes gpupdate nebo politikou)

Lokální politika

Uložena ve Windows\system32\GroupPolicy

Postrádají

- instalaci aplikací
- řízení lokálních skupin
- definici zabezpečení registrů
- definici zabezpečení filesystému
- definice pravidel pro systémové služby
- Preferences
- WMI, security … filtrování

Výhody

- Aspoň že jsou ☺

Doménové politiky

- Každá politika má jedinečné ID
- Předdefinované politiky:
  DDP - **{31B2F340-016D-11D2-945F-00C04FB984F9}**
  DDCP - **{6AC1786C-016F-11D2-945F-00C04fB984F9}**
- Doménová politika je umístěna v adresáři SYSVOL, ale některé její nastavení jsou součástí AD (párování ID na jméno, WMI ...)

Politiky

- Aplikování GPO na základě:
  - Příslušnosti v OU
  - prostřednictvím oprávnění k danému GPO
  - Povolení / zakázaní větve / politiky
  - WMI filtr
- Postup zpracování politik je:
  - Místní objekt zásad skupiny
  - Síť
  - Doména
  - Organizační jednotka
  - V rámci organizační jednotky podle priorit
- Existují vyjímky
  - Vynucené zpracování politiky
  - Zablokované zpracování politiky
  - Použití zpětné smyčky

Politiky – WMI filtry

Jedoduché cílení

- Podle operačních systémů a rolí

Select * from Win32_OperatingSystem Where Version like "6.1%" and ProductType = "1" - W7.
Select * from Win32_OperatingSystem Where Version like "6.0%" and ProductType = "1" - W Vista a výše.
Select * from Win32_ComputerSystem where DomainRole <> 5 – všechno kromě PDC

Version:
2008 R2 = "6.1%"
Windows Vista nebo Server 2008 = "6.0%"
Windows XP = "5.2%"
Windows 2000 = "5.0%"

Produkt Type:
Klient = "1"
DC = "2"
Member server = "3"

DomainRole:
DC = "4"
PDC = "5"

- Podle místa na disku, nainstalované aktualizace, podporu multicastu ….

Politiky – WMI filtry

- Co to znamená pro politiku:
  - Každá politika může mít pouze jeden WMI filtr.
  - Zpomaluje přihlašování počítače
  - Cílení lze provádět pouze na základě vlastností počítače.
  - Zpracovává se pouze na Windows XP a výše
  - Minimálně jeden DC musí být W2003 a výše.

Politika (GPO)

Rozdělena na dvě sekce

- User Configuration Settings – aplikují se bez ohledu na uživatele
- Computer Configuration Settings – aplikují se bez ohledu na počítač

Administrative Templates

- Definuje UI přístup k nastavením.
- ADM / ADMX se replikuje na ostatní DC = ADM - kde není potřeba, nepoužívat.
- Možné udělat si vlastní ADM / ADMX, stáhnout lze ke spoustům programů (Office, IE, FireFox, Media Player …) jednotné nastavení.

Politika – Jak vypadá na disku

- Gpt.ini – verze GPO
- Machine (povinné) – registry.pol
  - Scripts\startup
  - Scripts\shutdown
  - Applications (.aas soubory)
  - ADM
  - Preferences – adresáře se soubory XML
- USER (povinné) – registry.pol
  - Applications
  - Documents and settings – při přesměrování
  - Microsoft\IEAK – .INS, Ikony …
  - Scripts\logon
  - Scripts\logoff
  - Preferences – adresáře se soubory XML

Šablona ADM

- Každá nová Pre-Vista politika obsahuje šablony (conf, inetres, systém, wmplayer, wuau).
- Lze použít i pro Windows 7
- Umístěna u konkrétní politiky v adresáři ADM a na lokálním počítači v Windows\inf
- Je to textový soubor popisující cestu k registru a to buď přímo k nastavení apliace nebo do
  HKLM\Software\policies
  HKCU\Software\policies
- Pokud chceme využívat roll back, je třeba používat Group policy-aware aplikace.
- V editoru W7 jsou vidět jako Classic Administrative Templates

GPO pro W7

- Není potřeba W2008 server.
- K editaci je třeba Windows Vista a vyšší. (Součástí RSAT)
- Jiný systém práce s šablonami (jiné umístění, spořivější replikace, jazykově nezávislé ...)
- Mnoho nových nastavení. Některé i pro starší systémy.
- Rozdělena na Policies a Preferences

Nový group policy editor W7 + GPMC

- Spouští se buď editem v novém GPMC, nebo přes gpme.msc. (dříve gpedit.msc)
- Úžasné prohledávání a fitrování
- Možnost zobrazit všechna nastavení
- Možnosti poznámek k jednotlivým nastavením.
- Možnosti práce se skripty v Powershellu
- Instalace GPMC na stanici je součástí RSAT. Na serveru součástí Features

Šablona ADMX

- Umístěna v centrálním úložišti PolicyDefinitions na SYSVOLu, nebo na lokálním počítači ve Windows\PolicyDefinitions
- Jazykově nezávislá

- Šablony jsou potřeba pouze pro vytváření politik. Pro vlastní aplikaci na klientovi již ne.
- Staré šablony ADM lze převádět pomocí ADMX Migratoru, ve kterém můžeme vytvářet i nové

ADML

- Jazykový soubor příslušné ADMX politiky
- V adresáři PolicyDefinitions se vytvářejí poddadresáře pro určité jazyky (en-US, cs-CZ, de-DE) a do nich ADML soubory stejných názvů jako ADMX

Novinky v konfiguraci počítačře

- Brána Windows Firewall s prokročilým zabezpečením.
- Zásady řízení aplikací (Applocker)
- Upřesnit konfiguraci zásad auditování
- Technologie QoS
- Diskové quoty
- Řízení spotřeby
- Rozšířená správa IE
- Kontrola nad USB
- Diagnostika chyb
- …

Group Policy Preferences

- Nejdůležitější novinka v politikách, 20 nových rozšířeních
- Není potřeba W2008 server.
- GPP x Policy
- Nepovinná nastavení.
- GPP se aplikují na Windows 7, Windows Vista SP2 i na Windows XP SP2 a Windows 2003 SP1 (po instalaci volitelné aktualizaci KB943729 – XML parser).
- Není třeba Group policy-aware aplikace (GPP ukládá do běžných části registry nebo do .ini souborů)
- Obnova GPP probíhá zároveň s politikou (ale u každé položky lze toto vypnout).
- Možnost „user-friendly" filtrování v úrovní jednotlivých nastavení – změna oproti GPO.
- U všech polí a preferenci lze využívat proměnných (klávesa F3)

Computer preferences – Windows settings

ENVIRONMENT- Prostředí

- Vytváření proměnných prostředí
- Používá se pro definování programových proměnných, nebo proměnných cest.
- Defaultně spuštěno v kontextu počítače

Computer preferences – Windows settings

FILES - Soubory

- Práce se soubory na místním počítači.
- Podporuje wildcards i environment variables.
- NENÍ URČEN PRO KOPÍROVÁNÍ ODKAZŮ.

Computer preferences – Windows settings

FOLDERS - Složky

- Vytváření, mazání ... složky
- Nepodporuje wildcards
- Hlavní použití je v čištění TEMP adresářů

Computer preferences – Windows settings

INI FILES

- Pro konfiguraci programů, které ji mají uloženou v INI nebo INF souborech.
- Je třeba znát formát INI (INF) souboru

```
[Oddil]
Vlastnost1=hodnota
Vlastnost2=hodnota
```

Computer preferences – Windows settings

REGISTRY

- Možnost přehledného zobrazeni a jednotného cílení pomocí kolekcí.
- Průvodce registrem
- Již není potřeba ADM šablony (které navíc neumožnovaly popisky)
- Pro ne Group policy-aware aplikace …

Computer preferences – Windows settings

NETWORK SHARES

- Vytváření sdílení složek na lokálním počítači.
- Možnost definovat ABE (uživatelé nevidí podadresáře na které nemají právo)
- Práva se musí řešit politikou.
- Nejsou v preferences pro uživatele.

Computer preferences – Windows settings

SHORTCUTS

- Možnost definovat Typ (URL, Objekt - soubor)
- Bohatý výběr umístění.
- Možnost grafiky ikon.

Computer preferences – Control Panel Settings

DATA SOURCES

- Vytvoří systémové zdroje dat (ODBC)

Computer preferences – Control Panel Settings

DEVICES

- Povolení nebo zakázání používání jednotlivých zařízení
- Lepší kontrola je přes GPO (pouze pro Windows Vista dále)

Computer preferences – Control Panel Settings

FOLDER OPTIONS

- Umožňuje definovat přidruženost přípon k jednotlivým třídám.
- Neporovnatelně pohodlnější je toto defininovat v sekci pro uživatele, kde lze nastavit i chování zobrazení Exploreru.

Computer preferences – Control Panel Settings

LOCAL USERS AND GROUPS

- Práce s uživatelskými účty a skupinami na lokálních stanicích.
- U uživatele: Přejmenování, změna hesla, popisu …
- U Skupiny – Definice členů, U uživatelského nastavení možnost pracovat s aktuálně přihlášeným uživatelem

Computer preferences – Control Panel Settings

NETWORK OPTIONS

- Možnost vytvářet VPN připojení.
- Oproti CMAK méně možností, ale i méně práce.

Computer preferences – Control Panel Settings

POWER OPTIONS

- Definice možnosti napájení i pro Windows XP (Pro Windows Vista a novější je možnost definice přímo v GPO)
- Definic schámat napájení pro XP a výše.

Computer preferences – Control Panel Settings

PRINTERS

- Definice lokálních tiskáren.
- U uživatele je možné definovat tisk přes tiskový server (sdílená tiskárna).
- Možnosti směrování do úložiště ovladačů.

Computer preferences – Control Panel Settings

SCHEDULED TASKS

- Okamžitá úloha – spustí se ihned po aktualizaci zásad skupiny a potom se ihned odebere.
- Zde je krásně vidět co všechno umí nativně naplánované úlohy ve Windows Vista dále.

Computer preferences – Control Panel Settings

SERVICES

- Oproti nastavením v GPO lze definovat účet, který službu spouští a akce při selhání
- Nejsou v nastavení uživatele.

User preferences – Windows settings
APPLICATIONS

- Použití v budoucnu s dodavateli

User preferences – Windows settings

DRIVE MAPS

- Nástupce logonscriptů

User preferences – Control Panel Settings

INTERNET SETTINGS

- Možnost definovat nastavení od Internet Exploreru 5
- Domovská stránka, připojení … je to v podstatě kopie Nástroje – Možnosti v IE

User preferences – Control Panel Settings

REGIONAL OPTIONS

- Možnosti místních nastavení.
- Prozatím nepoužívat, stále lze co vylepšovat ☺

User preferences – Control Panel Settings

START MENU

- Definice menu Start
- Možno definovat vzhled ikony i pro Windows XP

Group Policy Preferences – záložka comon - Společné

- Ukončit … Ukončí pouze aktualní GPO, ostatní poběží dále
- Spustit v kontextu … Nutné pro mapování disků, tiskáren, pro přístup k proměnným uživatele …
- Odstranit … Akce se změní na nahradit (odstranit – vytvořit). Mimo obor se preference může dostat i díky cílení.
- Použít jednou … Nepřepisuje se nastavení, která následně udělají uživatelé.
- CÍLENÍ

Group Policy Preferences – Targeting – Cílení

- Možnosti cílení – WMI query, LDAP query …
- Možnosti kombinace OR a AND oeprátorů
- Možnosti negace
- Kolekce = „výraz v závorkách“. Lze u ní určovat výstup TRUE nebo FALSE

Prosím

- Uživatel s právy administrátora patří do říše pohádek.
- Odmítat mail na základě blacklistu je zločin.
- Používejte SPF záznamy.

- Pro svůj klidný spánek používejte všude limity.

Dotazy

Kdo se neptá nic se nedozví.
Líná huba, holé neštěstí
Víc hlav víc ví.
Žádný učený z nebe nespadl.
Chybami se člověk učí.
Ráno moudřejší večera.