

Serverové systémy Microsoft Windows

IW2/XMW2 2014/2015

Jan Fiedor

ifiedor@fit.vutbr.cz

Fakulta Informačních Technologií

Vysoké Učení Technické v Brně

Božetěchova 2, 612 66 Brno

Revize 18. 3. 2015

Active Directory

Zásady skupiny (uložení, šablony)

Uložení GPO objektů

- Fyzicky složeny ze 2 komponent
 - Kontejner zásad skupiny (*Group Policy Container*)
 - Šablona zásad skupiny (*Group Policy Template*)
- Každý GPO objekt obsahuje číslo verze
 - Inkrementováno při každé změně nastavení (zásady)
 - Umožňuje zjišťovat, zda byl objekt změněn od doby jeho poslední aplikace na uživatele nebo počítač

Verze GPO objektu a jeho komponent

Správa zásad skupiny

Soubor Akce Zobrazit Okno Nápověda

Správa zásad skupiny

- Doménová struktura: testing.local
 - Domény
 - testing.local
 - Default Domain Policy
 - Password Policy
 - Domain Controllers
 - Default Domain Controllers Policy
 - Objekty zásad skupiny
 - Default Domain Controllers Policy
 - Default Domain Policy**
 - Password Policy
 - Filtry rozhraní WMI
 - Objekty GPO Starter
 - Lokality
 - Default-First-Site-Name
 - Modelování zásad skupiny
 - Výsledky zásad skupiny

Default Domain Policy

Obor	Podrobnosti	Nastavení	Delegování	Stav
Doména:	testing.local			
Vlastník:	Domain Admins (TESTING\Domain Admins)			
Vytvořeno:	24. 2. 2013 21:35:51			
Změněno:	11. 3. 2013 13:25:36			
Verze uživatele:	2 (AD), 2 (SYSVOL) ←			
Verze počítače:	3 (AD), 3 (SYSVOL) ←			
Jedinečné ID:	{31B2F340-016D-11D2-945F-00C04FB984F9}			
Stav objektu GPO:	Povoleno			
Komentář:				

Kontejner zásad skupiny (GPC)

- Objekt Active Directory
 - Uložen v kontejneru Objekty zásad skupiny
 - Číslo verze GPO objektu uloženo ve formě atributu
- Neobsahuje žádná nastavení zásad skupiny
 - Slouží pouze pro určení rozsahu (*scope*) GPO objektů

Šablona zásad skupiny (GPT)

- Kolekce souborů
 - Uložena v systémovém oddíle AD (**SYSVOL**) v adresáři **<sysvol>\Domain\Policies\<gpc-guid>**
 - Číslo verze GPO objektu uloženo v souboru **GPT.ini**
- Obsahuje veškerá nastavení zásad skupiny
 - Zpracovány klientem zásad skupiny a CSE rozšířeními
 - Formát nastavení se liší podle typu nastavení zásad
 - Binární (registr, ...) nebo textový soubor (zásady účtů, ...)
 - INI (zásady účtů, ...) nebo XML formát (AppLocker, ...)
 - Různé kombinace (např. XML formát v binárním souboru)

Uložení šablon zásad skupiny

The screenshot shows a Windows Explorer window with the address bar set to `{31B2F340-016D-11D2-945F-00C04FB984F9}`. The left sidebar shows the navigation pane with 'Soubor' selected. The main pane displays a table of files:

Název	Datum změny	Typ	Velikost
MACHINE	24. 2. 2013 21:43	Složka souborů	
USER	11. 3. 2013 12:46	Složka souborů	
GPT.INI	11. 3. 2013 13:25	Nastavení konfigurace	1 kB

A blue arrow points from the GPT.INI file to a Notepad window titled 'GPT.INI – Poznámkový blok'. The Notepad window shows the following content:

```
[General]
Version=131075 => 0x00020003
```

Brackets under the hex value '0x00020003' point to 'Verze uživatele' and 'Verze počítače'.

At the bottom of the Explorer window, it shows 'Počet položek: 3' and 'Počet vybraných položek: 1; 27 bajtů'.

Replikace GPO objektů

- Odlišná replikace obou komponent GPO objektů
 - GPC kontejnery replikovány v rámci databáze Active Directory pomocí DRA (*Directory Replication Agent*)
 - GPT šablony replikovány společně s oddílem **SYSVOL**
 - Pomocí služby replikace souborů [deprecated]
 - Pomocí replikace distribuovaného souborového systému
- Oba typy replikace probíhají nezávisle na sobě
 - Komponenty nemusí být správně synchronizovány

Nekonzistence verzí GPO komponent

- Replikován pouze GPC kontejner (častější)
 - Klient zjistí neodpovídající verzi GPT šablony po jejím obdržení, neaplikuje v ní obsažená nastavení a zapíše tuto chybu do protokolu událostí
- Replikována pouze GPT šablona
 - Klient vůbec nezjistí, že došlo ke změně GPO objektu (nastavení zásad skupiny)
- Nekonzistence v synchronizaci obou komponent lze odhalit pomocí konzole Správa zásad skupiny
 - U starších verzí Windows lze použít **gpoutil.exe**

Stav replikace GPO objektů

The screenshot shows the 'Správa zásad skupiny' (Group Policy Management) console. The left pane displays the hierarchy: Doménová struktura: testing.local > Domény > testing.local > Default Domain Policy. The right pane shows the 'Stav' (Status) tab for the 'Default Domain Policy'. The status text indicates that the replication of Active Directory and SYSVOL services is successful. Below this, a table lists details about the domain controller 'wsrv2012.testing.local'. At the bottom, it shows the last refresh date as 24. 3. 2014 and a 'Rozpoznat' (Refresh) button.

Správa zásad skupiny

Soubor Akce Zobrazit Okno Nápověda

Správa zásad skupiny

- Doménová struktura: testing.local
 - Domény
 - testing.local
 - Default Domain Policy
 - Password Policy
 - Domain Controllers
 - Default Domain Controllers Policy
 - Objekty zásad skupiny
 - Default Domain Controllers Policy
 - Default Domain Policy**
 - Password Policy
 - Filtry rozhraní WMI
 - Objekty GPO Starter
 - Lokality
 - Modelování zásad skupiny
 - Výsledky zásad skupiny

Default Domain Policy

Obor Podrobnosti Nastavení Delegování Stav

Na této stránce je zobrazen stav replikace služby Active Directory a adresáře SYSVOL (služba replikace distribuovaného systému souborů) v této doméně vzhledem k zásadám skupiny.

Podrobnosti o stavu

- wsrv2012.testing.local je základní řadič domény v této doméně. [Změnit](#)

Název webu	Default-First-Site-Name
IP adresa	fe80::92c:97ac:8cd3:d00f%20
Objekty zásad s...	1

? Počet řadičů domény s probíhající replikací: 0

✓ Počet řadičů domény se synchronizovanou replikací: 0

Datum posledního shromáždění informací o stavu infrastruktury: 24. 3. 2014 [Rozpoznat](#)

Zásady šablon pro správu

- Zásady uložené pod uzlem zásad skupiny Šablony pro správu (*Administrative Templates*)
 - Lze filtrovat pomocí globálního filtru
- Slouží k modifikaci registru
 - Větve **HKEY_LOCAL_MACHINE** (HKLM) pro počítače
 - Větve **HKEY_CURRENT_USER** (HKCU) pro uživatele
- Vytvářeny na základě šablon pro správu
- Pro nastavení lze použít Starter GPO objekty
 - Obsahují nastavení zásad šablon pro správu

Nastavení zásad šablon pro správu

Editor správy zásad skupiny

Soubor Akce Zobrazit Nápověda

Default Domain Policy [WSRV2012.TESTING.L]

- Konfigurace počítače
 - Zásady
 - Nastavení softwaru
 - Nastavení systému Windows
 - Šablony pro správu: Definice zásad
 - Ovládací panely
 - Sít
 - Součásti systému Windows
 - Systém
 - Tiskárny
 - Veškerá nastavení**
 - Předvolby
- Konfigurace uživatele
 - Zásady
 - Nastavení softwaru
 - Nastavení systému Windows
 - Šablony pro správu: Definice zásad

Nastavení	Stav
Adresa URL souboru Events.asp	Není nakonfigurováno
Akce při odpojení serveru	Není nakonfigurováno
Akce při oznámení kritického stavu baterie	Není nakonfigurováno
Akce při oznámení nízkého stavu baterie	Není nakonfigurováno
Aktivovat funkci dat o stavu systému dialogového okna ...	Není nakonfigurováno
Aktivovat tisk přes Internet	Není nakonfigurováno
Aktualizovat úroveň zabezpečení	Není nakonfigurováno
Aktualizovat zóny domén nejvyšší úrovně	Není nakonfigurováno
Aplikovat nastavení proxy serveru podle počítače (nikoli...	Není nakonfigurováno
Automatické dotazování pro ovládací prvky ActiveX	Není nakonfigurováno
Automatické dotazování pro ovládací prvky ActiveX	Není nakonfigurováno
Automatické dotazování pro ovládací prvky ActiveX	Není nakonfigurováno
Automatické dotazování pro ovládací prvky ActiveX	Není nakonfigurováno
Automatické dotazování pro ovládací prvky ActiveX	Není nakonfigurováno
Automatické dotazování pro ovládací prvky ActiveX	Není nakonfigurováno
Automatické dotazování pro ovládací prvky ActiveX	Není nakonfigurováno
Automatické dotazování pro ovládací prvky ActiveX	Není nakonfigurováno

1869 nastavení

Filtrování zásad šablon pro správu

Editor s

Soubor Akce Zobrazit Nápověda

Default Domain Policy [WSRV2012.TESTING.L

Konfigurace počítače

Zásady

Nastavení softwaru

Nastavení systému Windows

Šablony pro správu: Definice zásad

Přidat nebo odebrat šablony...

Zapnout filtr

Možnosti filtru...

Znovu použít filtr

Všechny úkoly

Nápověda

Zásady

Nastavení softwaru

Nastavení systému Windows

Šablony pro správu: Definice zásad

Možnosti filtrování

Možnosti filtru

Pomocí níže uvedených možností můžete povolit a změnit, případně zakázat typy globálních filtrů, které se použijí na uzly Šablon pro správu.

Vyberte typ nastavení zásad, které chcete zobrazit

Spravované: Ano

Konfigurované: Jakýkoli

S komentářem: Jakýkoli

Povolit filtry klíčových slov

Filtrovat slova: Jakýkoli

Uvnitř: Záhloví nastavení zásad Text nápovědy Komentář

Povolit filtry požadavků

Vyberte požadované filtry pro platformu a aplikace:

Zahrňte nastavení, které se shoduje s kteroukoli z vybraných platform.

- BITS 1.5
- BITS 1.5
- BITS 2.0
- BITS 3.5
- Instalační služba systému Windows v2
- Instalační služba systému Windows v3
- Instalační služba systému Windows v4
- Internet Explorer 10

Šablony pro správu

- Umožňují přidávat nové zásady do GPO objektů
 - Možnost centralizované konfigurace aplikací třetích stran (pokud ukládají nastavení v registru)
- Textové soubory obsahující definice zásad
 - Třídu zásady (konfigurace počítače a/nebo uživatele)
 - Definici uživatelského rozhraní pro nastavení zásady
 - Informace jak pro dané nastavení modifikovat daný klíč registru (nastavit řetězec nebo číslo, smazat, ...)
 - Podporované verze operačního systému Windows
 - Název zásady, popis, komentář, ...

Komponenty šablon pro správu

- Rozděleny do dvou XML souborů
 - Oddělení definice zásad od jejich lokalizace
 - Svázání přes speciální identifikátory $\$(\langle typ \rangle.\langle id \rangle)$
- Soubor ADMX
 - Obsahuje pouze definice jednotlivých zásad
 - Vždy jediný pro každou šablonu pro správu
- Soubory ADML
 - Obsahují jazykovou lokalizaci (GUI rozhraní) zásad
 - Jeden soubor pro každý jazyk

Příklad definice zásady

```
<policy name="IW2Policy"  
  class="Both"  
  displayName="$(string.IW2Policy)"  
  explainText="$(string.IW2Policy_Help)"  
  key="Software\Policies\Examples"  
  valueName="IW2Entry">  
  <parentCategory ref="IW2" />  
  <supportedOn ref="windows:SUPPORTED_Windows7" />  
  <enabledValue>  
    <decimal value="1" />  
  </enabledValue>  
  <disabledValue>  
    <decimal value="0" />  
  </disabledValue>  
</policy>
```


Příklad lokalizace zásady

```
<stringTable>
```

```
  <string id="IW2Policy">IW2 zásada</string>
```

```
  <string id="IW2Policy_Help">
```

Příklad zásady vytvořené na základě šablony pro správu.

Při povolení zásady se nastaví hodnota IW2Entry na 1.

Při zakázání zásady se nastaví hodnota IW2Entry na 0.

```
  </string>
```

```
</stringTable>
```

Uložení šablon pro správu

- Uloženy odděleně od nastavení zásad
 - Při změně není potřeba aktualizovat GPT šablony
- Centrální úložiště
 - Distribuovaný adresář **\\<fqdn-domény>\SYSVOL\
<fqdn-domény>\Policies\PolicyDefinitions**
 - Použito prioritně (pokud je vytvořeno)
- Úložiště na lokálním počítači
 - Lokální adresář **<system>\PolicyDefinitions**
 - Obsahuje výchozí sadu šablon pro správu

Instalace softwaru

- Umožňuje centrální nasazování a správu aplikací
 - Přístup uživatelů k aplikacím kamkoliv se přihlásí
 - Transparentní instalace aplikací (bez zásahu uživatele)
 - Možnost automatické odinstalace aplikací
- Realizuje CSE rozšíření instalace softwaru
 - Využívá Instalační službu systému Windows
- Instalační soubory uloženy ve sdíleném adresáři
- Neprobíhá pokud je detekována pomalá linka
 - Lze změnit v nastavení zásad skupiny

Podporované soubory pro instalaci

- Instalační balíky Windows (**.msi** soubory)
 - Zachycují stav nainstalované aplikace
 - Obsahuje informace pro odinstalaci aplikace
- Transformační soubory (**.mst** soubory)
 - Umožňují upravovat proces instalace dané aplikace
 - Konfigurace instalátoru pro bezobslužnou instalaci
- Záplatové soubory (**.msp** soubory)
 - Umožňují aktualizovat existující **.msi** soubory
 - Aplikace aktualizovaných souborů a klíčů registru

Přiřazení (assign) aplikací

- Přiřazení aplikace uživateli
 - Zapsání nastavení aplikace do lokálního registru
 - Přidání zástupců do nabídky Start (a na plochu)
 - Nastavení asociace souborů s danou aplikací
 - Plná instalace při prvním spuštění aplikace (zástupce) nebo otevření souboru, jenž je s aplikací asociován
- Přiřazení aplikace počítači
 - Instalace aplikace při startu počítače
 - K dispozici všem uživatelům na daném počítači

Publikování (publish) aplikací

- Publikovat aplikace lze pouze pro uživatele
- Publikování
 - Umožnění instalace aplikace přes Programy a funkce (*Programs and Features*)
 - Nastavení asociace souborů s danou aplikací (pokud je povolena automatická instalace)
- Instalace
 - Manuálně přes Programy a funkce
 - Otevřením souboru, jenž je s aplikací asociován (pokud je povolena automatická instalace)

Nasazení aplikace

The image shows two overlapping windows from a Windows operating system. The background window is the 'Editor správy' (Group Policy Editor) for 'Default Domain Policy [WSRV2012.TEST]'. The left pane shows a tree view with 'Konfigurace počítače' expanded to 'Zásady' > 'Nastavení softwaru' > 'Instalace softwaru'. A context menu is open over 'Instalace softwaru', with 'Nová položka' selected. A blue arrow points from this menu to the foreground window. The foreground window is the '7-Zip 9.20 – vlastnosti' (7-Zip 9.20 – properties) dialog box, with the 'Nasazení' (Deployment) tab selected. The 'Typ nasazení' (Deployment type) section has 'Publikované' (Published) selected. The 'Možnosti nasazení' (Deployment options) section has 'Automaticky nainstalovat aplikaci při použití souboru tohoto typu' (Automatically install application when using file of this type) checked. The 'Možnosti uživatelského rozhraní instalace' (Installation user interface options) section has 'Největší' (Largest) selected. The 'Upřesnit...' (Specify...) button is visible at the bottom of the dialog box. The status bar at the bottom of the Group Policy Editor shows 'Přidá balíček.' (Adding package.).

Editor správy

Soubor Akce Zobrazit Nápověda

Default Domain Policy [WSRV2012.TEST]

Konfigurace počítače

Zásady

Nastavení softwaru

Instalace softwaru

Nová položka

Balíček...

Zobrazení

Vložit

Aktualizovat

Exportovat seznam...

Vlastnosti

Nápověda

Přidá balíček.

7-Zip 9.20 – vlastnosti

Obecné Nasazení Upgrady Kategorie Změny Zabezpečení

Typ nasazení

Publikované

Přřazené

Možnosti nasazení

Automaticky nainstalovat aplikaci při použití souboru tohoto typu

Odinstalovat tuto aplikaci, je-li mimo obor správy

Nezobrazovat balíček v ovládacím panelu Přidat nebo odebrat programy

Tuto aplikaci nainstalovat při přihlášení

Možnosti uživatelského rozhraní instalace

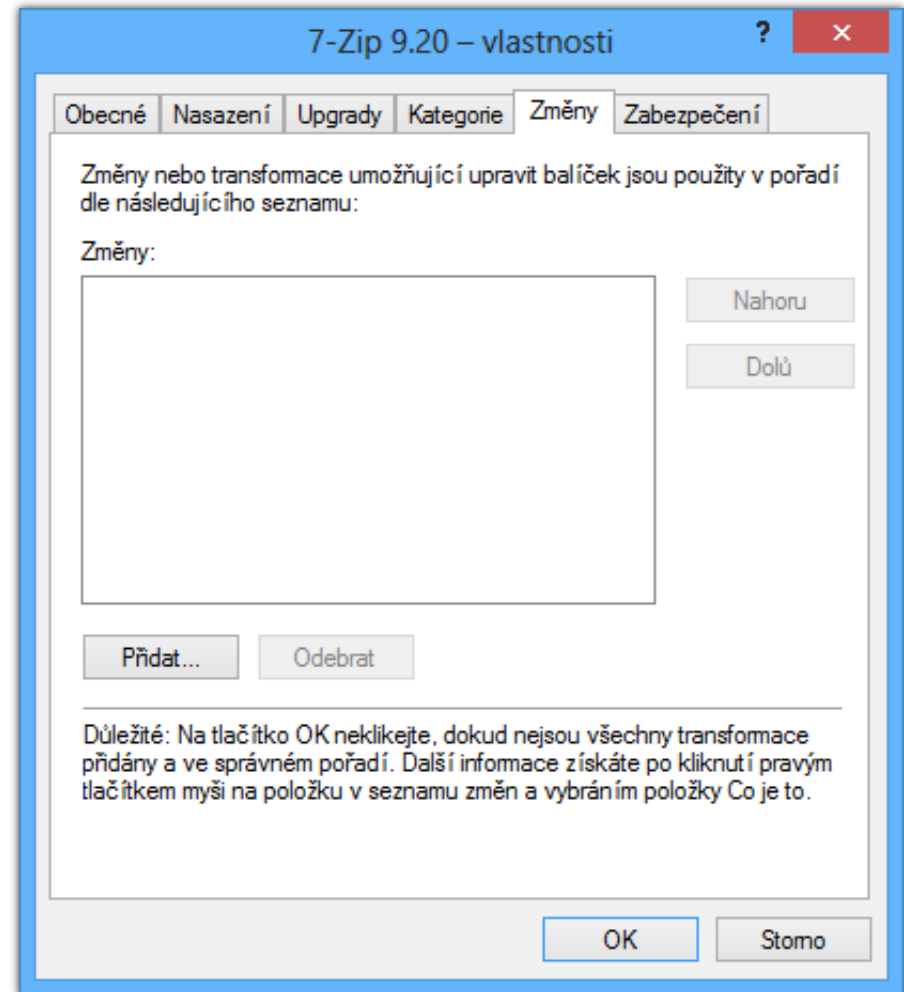
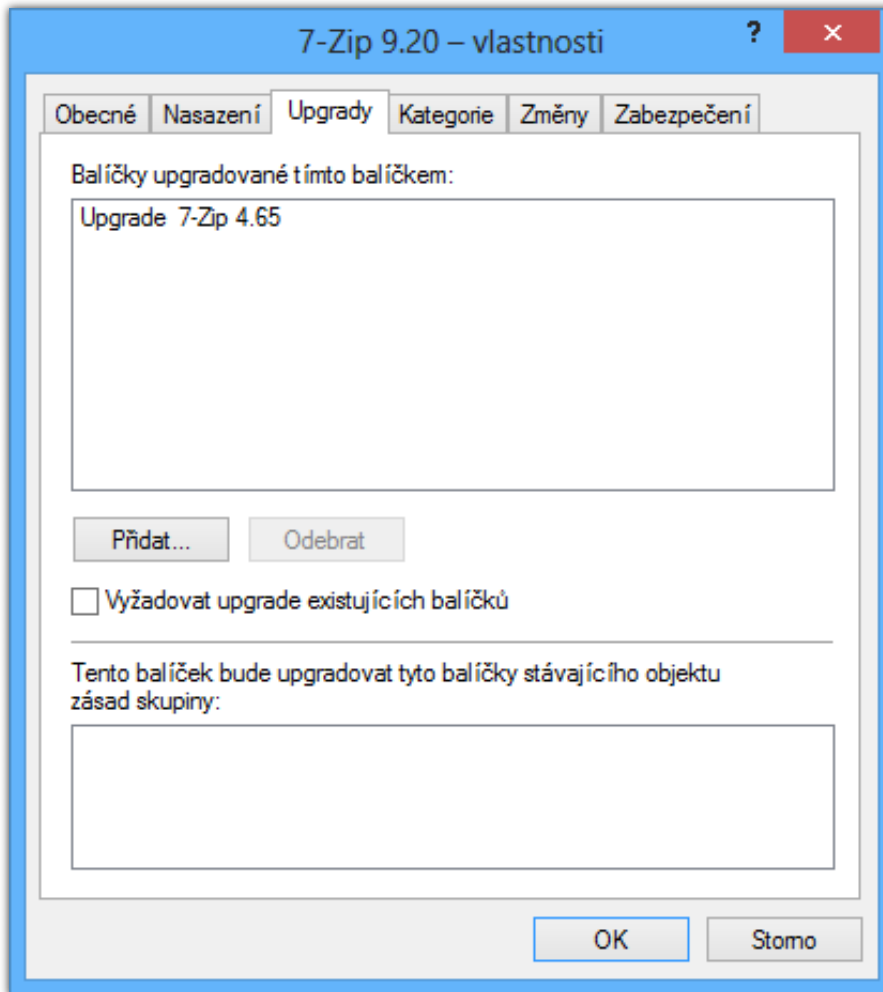
Základní

Největší

Upřesnit...

OK Storno

Upgrade a modifikace aplikace



Oinstalace aplikace

Editor správy zásad skupiny

Soubor Akce Zobrazit Nápověda

Default Domain Policy [WSRV2012.TEST]

- Konfigurace počítače
 - Zásady
 - Nastavení softwaru

Název	Verze	Stav nasazení	Zdroj
7-Zip 4.65	4.65	Publikováno	E:\7z465.msi
7-Zip 9.20	9.20	Publikováno	E:\7z920.msi

Odebrat software

Vyberte metodu odebrání:

Okamžitě odinstalovat aplikaci z počítačů a profilů uživatelů

Povolit uživatelům dále používat aplikaci, zabránit však novým instalacím

OK Storno

Přidat
Publikovat
Odebrat...
Znovu nasadit aplikaci

Automatická instalace
 Přidat
 Publikovat
 Všechny úkoly
 Aktualizovat
Vlastnosti
 Nápověda

Odebere balíček.

Předvolby zásad skupiny

- Umožňují nastavit části systému Windows, jenž bylo potřeba dříve konfigurovat pomocí skriptů
- Odlišnosti od nastavení zásad skupiny
 - Předvolby nejsou vynucené
 - Uživatel je může lokálně kdykoliv změnit nebo smazat
 - Předvolby nejsou odstraněny pokud není objekt zásad skupiny obsahující předvolby již nadále aplikován na daný počítač nebo uživatele
 - Lze zrušit (vynutit odstranění předvolby)

Nastavení předvoleb zásad skupiny

Editor správy zásad skupiny

Soubor Akce Zobrazit Nápověda

Default Domain Policy [WSRV2012.TESTI]

- Konfigurace počítače
 - Zásady
 - Předvolby
- Konfigurace uživatele
 - Zásady
 - Předvolby
 - Nastavení systému Windows
 - Aplikace
 - Mapování jednotek
 - Prostředí
 - Soubory
 - Složky
 - Soubory INI
 - Registr
 - Zástupci
 - Nastavení ovládacích panelů**

Nastavení ovládacích panelů

Zpracování

Popis

Žádné vybrané zásady

Název
Zdroje dat
Zařízení
Možnosti složky
Nastavení Internetu
Místní uživatelé a skupiny
Možnosti sítě
Možnosti napájení
Tiskárny
Místní nastavení
Naplánované úlohy
Nabídka Start

Předvolby Rozšířené Standardní

Cílení na úrovni položky

- Umožňuje specifikovat, kdy se má předvolba aplikovat na cílového uživatele nebo počítač
- Lze reagovat na
 - Hardwarové nároky (CPU, paměť RAM, volné místo)
 - Konkrétního uživatele a jeho členství ve skupinách
 - Existenci souborů a proměnných prostředí
 - Verzi operačního systému
 - Výsledek WMI dotazu
 - ...

Nastavení cílení na úrovni položky

