

# Serverové systémy Microsoft Windows

IW2/XMW2 2011/2012

**Jan Fiedor**

ifiedor@fit.vutbr.cz

Fakulta Informačních Technologií

Vysoké Učení Technické v Brně

Božetěchova 2, 612 66 Brno

Revize 11.3.2012

# 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

The screenshot shows the Group Policy Management console for a domain named 'testing.local'. The left pane displays a tree view of the domain structure, with 'Default Domain Policy' selected under 'Objekty zásad skupiny'. The right pane shows the details for this policy, including its name, owner, creation and modification dates, and version information for users and computers. Two red arrows point to the 'Verze uživatele' (User version) and 'Verze počítače' (Computer version) fields, both showing a version of 0 (AD) and 0 (sysvol).

Obor	Podrobnosti	Nastavení	Delegování
Doména:	testing.local		
Vlastník:	Domain Admins (TESTING\Domain Admins)		
Vytvořeno:	21.2.2010 14:07:52		
Změněno:	7.3.2011 1:36:52		
Verze uživatele:	0 (AD), 0 (sysvol)		
Verze počítače:	5 (AD), 5 (sysvol)		
Jedinečné ID:	{31B2F340-016D-11D2-945F-00C04FB984F9}		
Stav objektu GPO:	Povoleno		
Komentář:			

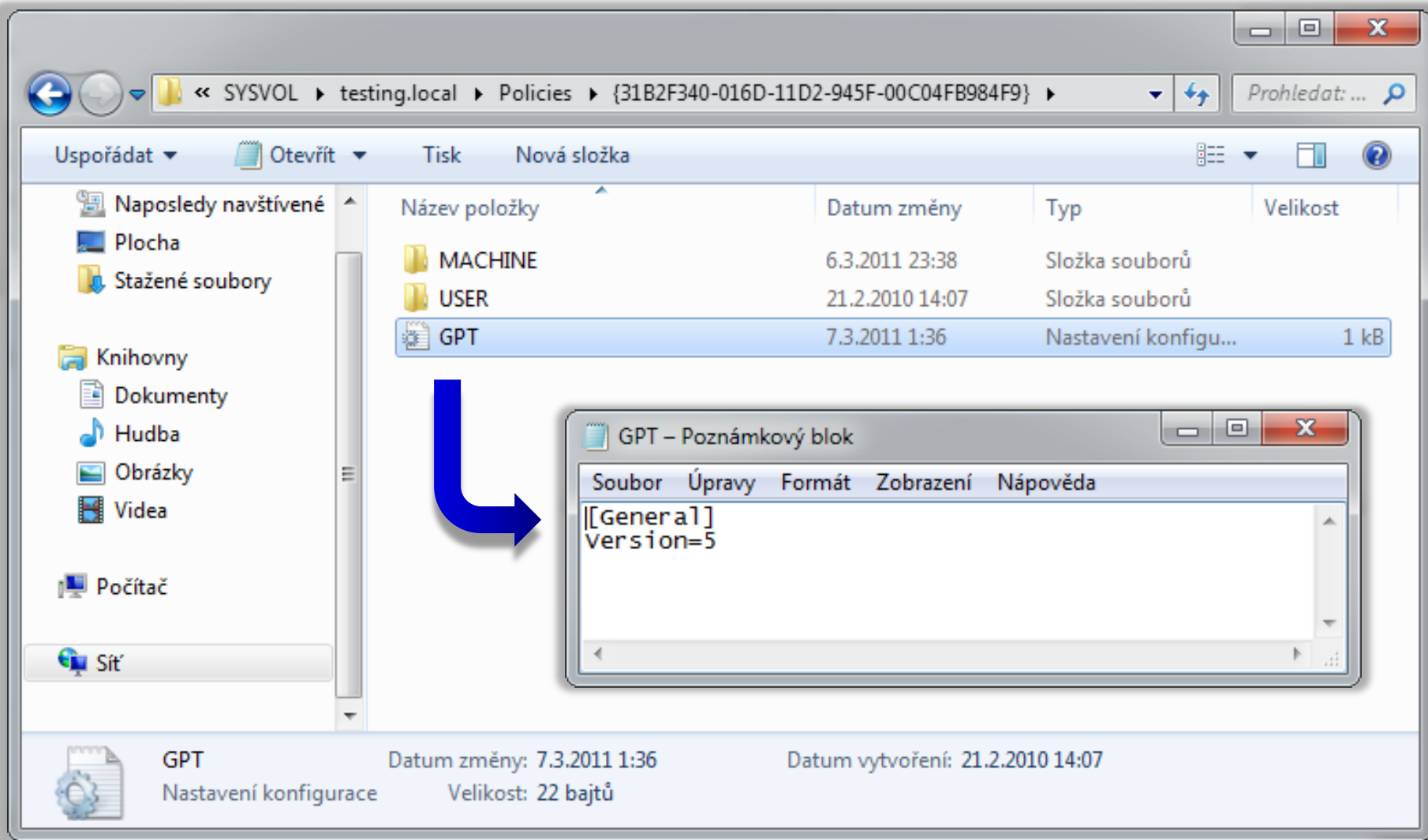
# Kontejner zásad skupiny (GPC)

- 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
  - Uložena binárně nebo v INI formátu

# Uložení šablon zásad skupiny



The screenshot shows a Windows Explorer window displaying the path: <math>\ll</math> SYSVOL > testing.local > Policies > {31B2F340-016D-11D2-945F-00C04FB984F9}. The file list shows three items: MACHINE (6.3.2011 23:38, Složka souborů), USER (21.2.2010 14:07, Složka souborů), and GPT (7.3.2011 1:36, Nastavení konfigurace, 1 kB). A blue arrow points from the GPT file to a Notepad window titled "GPT - Poznámkový blok". The Notepad window shows the following content:

```
Soubor  Úpravy  Formát  Zobrazení  Nápověda
[[General]
Version=5
```

The status bar at the bottom of the Explorer window shows: GPT (Nastavení konfigurace), Datum změny: 7.3.2011 1:36, Datum vytvoření: 21.2.2010 14:07, Velikost: 22 bajtů.

# Replikace GPO objektů

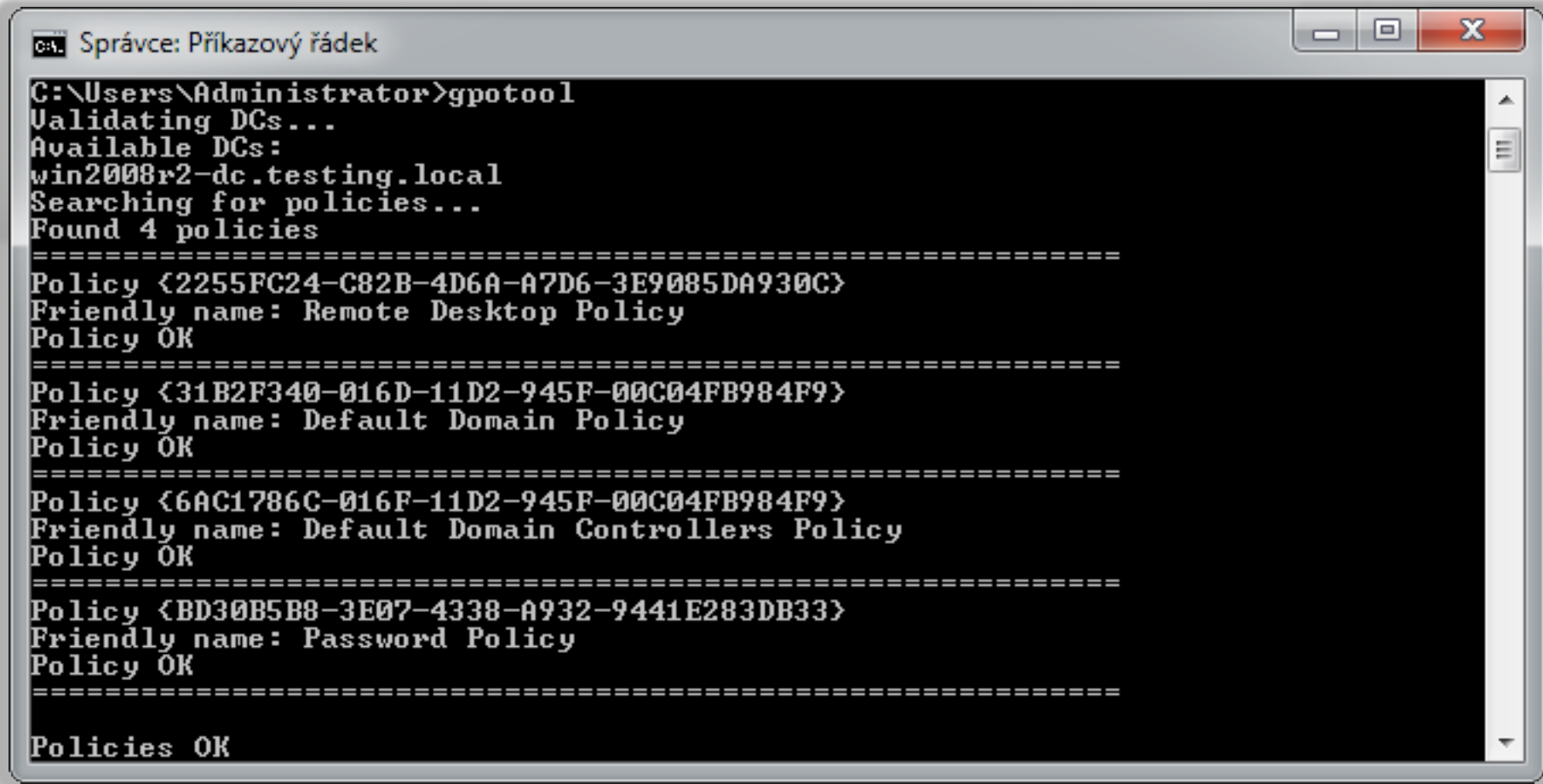
- Odlišná replikace obou komponent GPO objektů
  - GPC kontejnery replikovány v rámci databáze Active Directory pomocí DRA (*Directory Replication Agent*)
  - GPT šablony replikovány společně s oddílem SYSVOL
    - Pomocí služby replikace souborů
    - Pomocí replikace distribuovaného souborového systému
- 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 nástroje **gpoutil.exe**

# Nástroj gpoutil.exe



```
cmd Správce: Příkazový řádek
C:\Users\Administrator>gpoutil
Validating DCs...
Available DCs:
win2008r2-dc.testing.local
Searching for policies...
Found 4 policies
=====
Policy {2255FC24-C82B-4D6A-A7D6-3E9085DA930C}
Friendly name: Remote Desktop Policy
Policy OK
=====
Policy {31B2F340-016D-11D2-945F-00C04FB984F9}
Friendly name: Default Domain Policy
Policy OK
=====
Policy {6AC1786C-016F-11D2-945F-00C04FB984F9}
Friendly name: Default Domain Controllers Policy
Policy OK
=====
Policy {BD30B5B8-3E07-4338-A932-9441E283DB33}
Friendly name: Password Policy
Policy OK
=====
Policies OK
```

# 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 [WIN2008R2-DC.TESTIP]

- 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
Administrativně přiřazené soubory offline	Není nakonfigurováno
Adresa hostitele zkušebního podnikového serveru DNS	Není nakonfigurováno
Adresa URL souboru Events.asp	Není nakonfigurováno
Adresa URL určení umístění domény	Není nakonfigurováno
Akce při kritickém stavu baterie	Není nakonfigurováno
Akce při nízkém stavu baterie	Není nakonfigurováno
Akce při odpojení serveru	Není nakonfigurováno
Aktivovat funkci dat o stavu systému Přehled událostí ...	Není nakonfigurováno
Aktualizovat úroveň zabezpečení	Není nakonfigurováno
Aktualizovat zóny domén nejvyšší úrovně	Není nakonfigurováno
Aplikovat nastavení proxy serveru podle počítače (niko...	Není nakonfigurováno
Automatické dotazování na ovládací prvky ActiveX	Není nakonfigurováno
Automatické dotazování na ovládací prvky ActiveX	Není nakonfigurováno
Automatické dotazování na ovládací prvky ActiveX	Není nakonfigurováno
Automatické dotazování na ovládací prvky ActiveX	Není nakonfigurováno
Automatické dotazování na ovládací prvky ActiveX	Není nakonfigurováno

Rozšířené Standardní

1645 nastavení

# Filtrování zásad šablon pro správu

**Editor správy zásad skupiny**

Soubor Akce Zobrazit Nápověda

Default Domain Policy [WIN2008R2-DC.TESTIP]

- Konfigurace počítače
  - Zásady
    - Nastavení softwaru
    - Nastavení systému Windows
    - Šablony pro správu: Definice zásad

**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:	Konfigurované:	S komentářem:
Ano	Jakýkoli	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 2.0
- BITS 3.5
- Instalační služba systému Windows verze 2.0
- Instalační služba systému Windows verze 3.0
- Instalační služba systému Windows verze 4.0
- Internet Explorer 3.0
- Internet Explorer 4.0

Vybrat vše Vymazat vše

OK Storno

Možnosti filtrování

# Šablony pro správu

- 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 (smazat, nastavit řetězec nebo číslo, ...)
  - Podporované verze operačního systému Windows
  - Název zásady, popis, komentář, ...
- Umožňují přidávat nové zásady do GPO objektů
  - Možnost centralizované konfigurace aplikací třetích stran (pokud ukládají nastavení v registru)

# 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

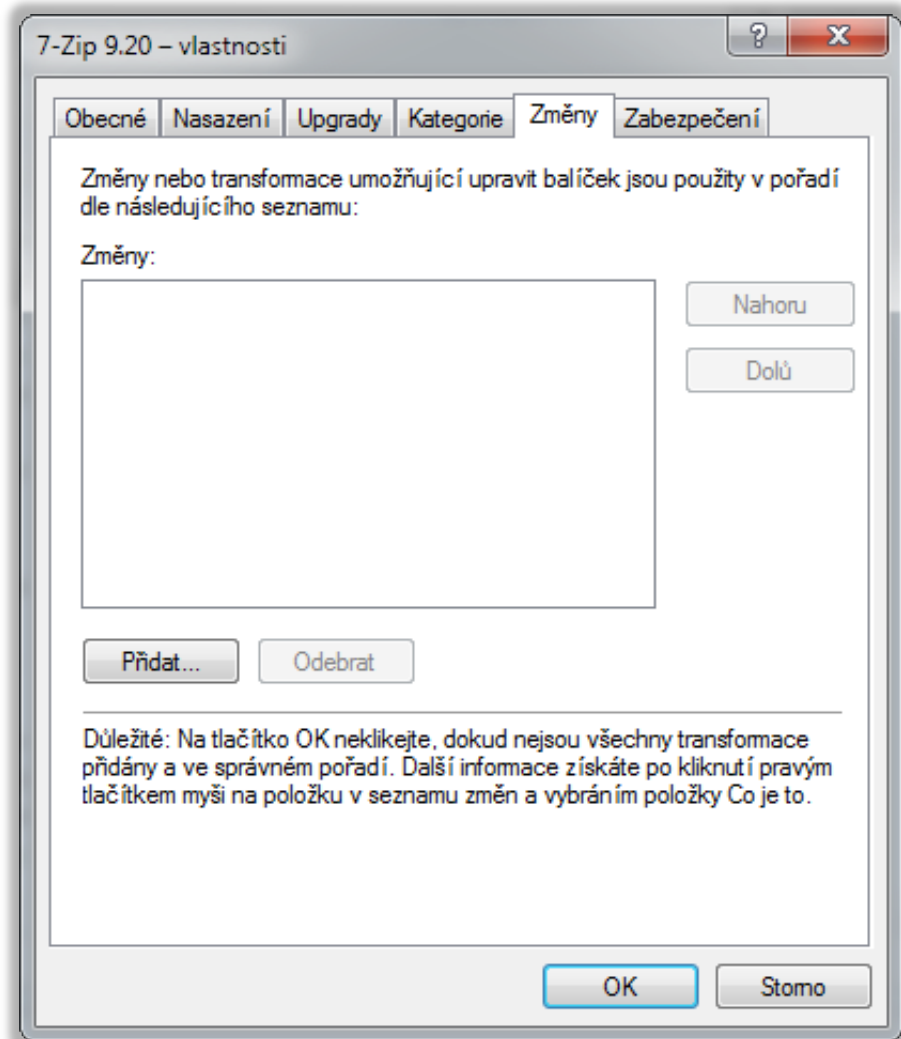
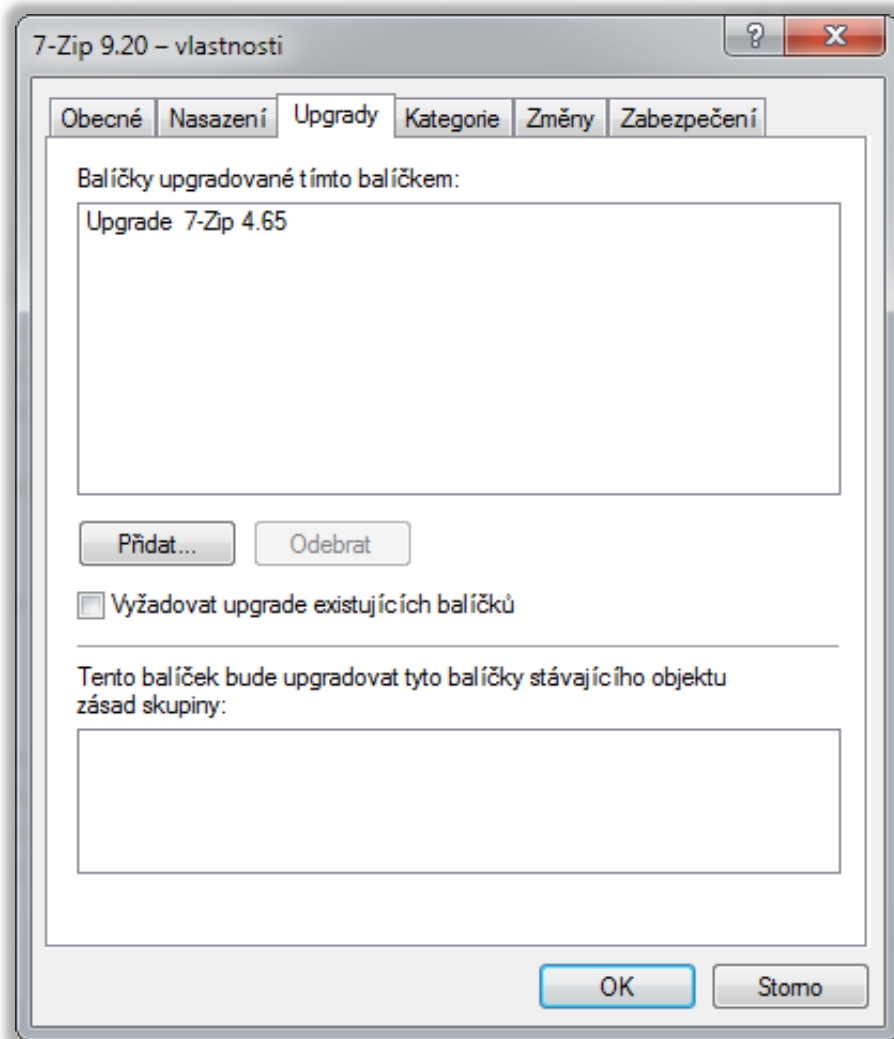
# Publikování (publish) aplikací

- 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 zásad skupiny' (Group Policy Editor) for 'Default Domain Policy [WIN2008R2-DC.]'. 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, and a sub-menu 'Balíček...' is visible. A large blue arrow points from the 'Balíček...' option to the foreground window. The foreground window is the '7-Zip 9.20 - vlastnosti' (7-Zip 9.20 - properties) dialog, with the 'Nasazení' (Installation) tab selected. The 'Typ nasazení' (Installation type) section has 'Publikované' (Published) selected. The 'Možnosti nasazení' (Installation options) section has 'Automaticky nainstalovat aplikaci při použití souboru tohoto typu' (Automatically install application when using files of this type) checked. The 'Možnosti uživatelského rozhraní instalace' (Installation user interface options) section has 'Největší' (Full) selected. The 'Upřesnit...' (Customize...) button is visible at the bottom of the dialog. The status bar at the bottom of the Group Policy Editor shows 'Přidá balíček.' (Adding package.).

# Upgrade a modifikace aplikace





# Oinstalace aplikace

Editor správy zásad skupiny

Soubor Akce Zobrazit Nápověda

Název Verze Stav nasazení Zdroj

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

Přířadit  
Publikovat  
Odebrat...  
Znovu nasadit aplikaci

Automatická instalace  
Přířadit  
Publikovat  
Všechny úkoly  
Aktualizovat  
Vlastnosti  
Nápověda

Odebere balíček.