

Serverové systémy Microsoft Windows

IW2/XMW2 2015/2016

Jan Fiedor

ifiedor@fit.vutbr.cz

Fakulta Informačních Technologií

Vysoké Učení Technické v Brně

Božetěchova 2, 612 66 Brno

Revize 14. 3. 2016

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 '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 properties for the selected 'Default Domain Policy' object.

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 displaying a Group Policy template file named GPT.INI. The file is located in the path: <code>SYSVOL >> testing.local >> Policies >> {31B2F340-016D-11D2-945F-00C04FB984F9}</code>. The file is a configuration setting file, 1 kB in size, and was last modified on 11. 3. 2013 at 13:25.

A blue arrow points from the GPT.INI file in the Explorer window to a Notepad window titled "GPT.INI – Poznámkový blok". The Notepad window shows the content of the GPT.INI file:

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

The Notepad window also includes a diagrammatic explanation of the version number: "Verze uživatele" (User version) is indicated by a red bracket under "0x0002" and "Verze počítače" (Computer version) is indicated by a blue bracket under "0003".

At the bottom of the Explorer window, the status bar shows: "Počet položek: 3 | 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.

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

Below the table, two status indicators are shown:

- ? Počet řadičů domény s probíhající replikací: 0
- ✓ Počet řadičů domény se synchronizovanou replikací: 0

At the bottom, the last refresh date is shown: Datum posledního shromáždění informací o stavu infrastruktury: 24. 3. 2014, with a 'Rozpoznat' button.

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
 - Síť
 - 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

The image shows the Group Policy Editor interface with the 'Možnosti filtru' (Filtering Options) dialog box open. The dialog box is titled 'Možnosti filtru' and contains the following sections:

- Header:** Pomocí níže uvedených možností můžete povolit a změnit, případně zakázat typy globálních filtrů, které se použijí na uzly Šablony pro správu.
- Section 1:** Vyberte typ nastavení zásad, které chcete zobrazit. This section contains three dropdown menus: 'Spravované:' (set to 'Ano'), 'Konfigurované:' (set to 'Jakýkoli'), and 'S komentářem:' (set to 'Jakýkoli').
- Section 2:** Povolit filtry klíčových slov. This section includes a text input field for 'Filtrovat slova:' (set to 'Jakýkoli') and a 'Uvnitř:' section with three checked checkboxes: 'Záhlaví nastavení zásad', 'Text nápovědy', and 'Komentář'.
- Section 3:** Povolit filtry požadavků. This section includes a dropdown menu 'Vyberte požadované filtry pro platformu a aplikace:' (set to 'Zahrňte nastavení, které se shoduje s kteroukoli z vybraných platform.') and two buttons: 'Vybrat vše' and 'Vymazat vše'. Below this is a list of items with checkboxes:
 - 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
- Buttons:** 'OK' and 'Storno' at the bottom right.

A blue arrow points from the 'Možnosti filtru...' menu item in the Group Policy Editor to the dialog box.

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

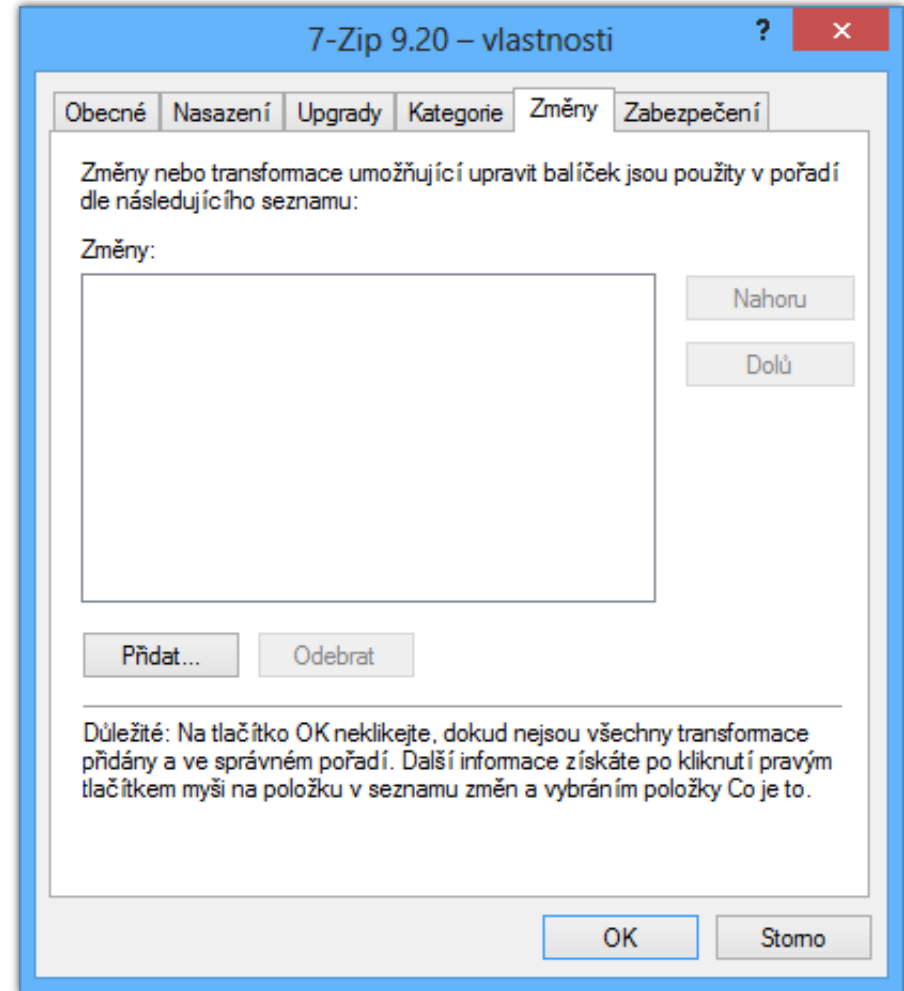
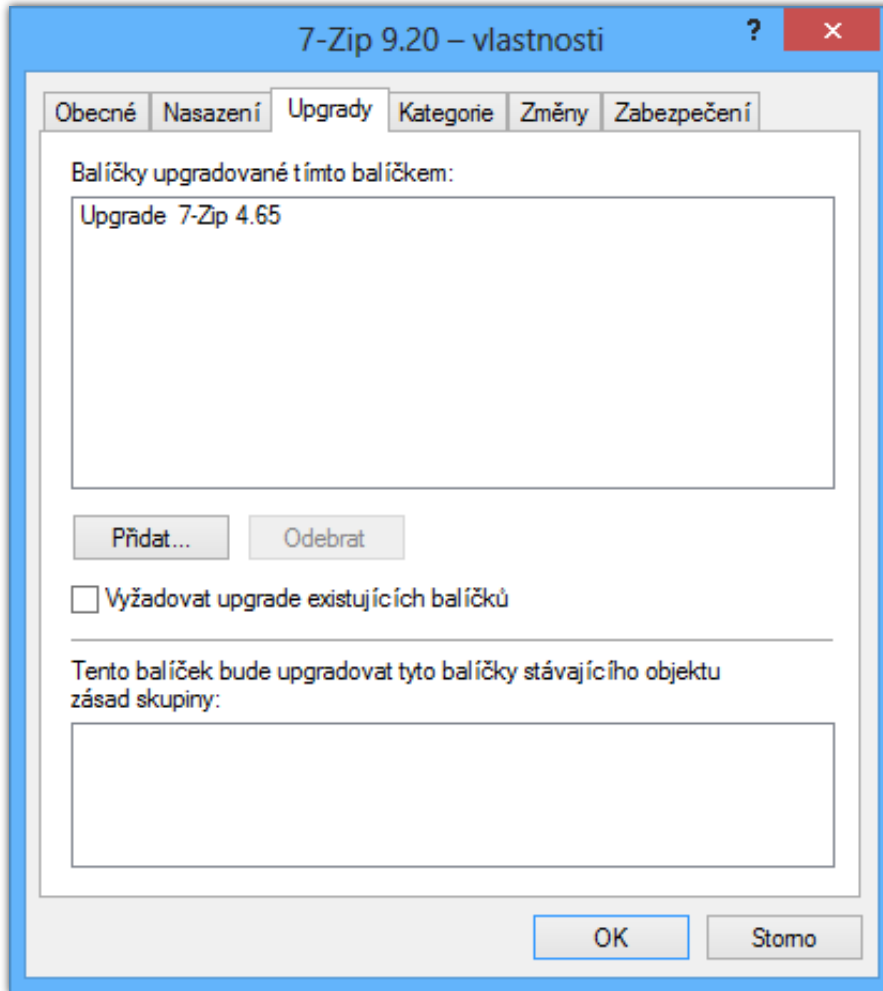
Publikování (publish) aplikací

- 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 this file 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.).

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

The image shows two overlapping Windows dialog boxes. The background dialog is titled "Nové vlastnosti jednotky" (New Volume Properties) and has tabs for "Obecné" (General) and "Společné" (Sharing). Under "Možnosti společné pro všechny položky" (Options common to all items), the checkbox "Cílení na úrovni položky" (Targeting by item) is checked. A blue arrow points from this checkbox to the foreground dialog.

The foreground dialog is titled "Editor položek cílení" (Targeting Item Editor). It contains a list of targeting conditions:

- operační systém je Windows 8 (verze Professional (64 bitů))
- A rychlost procesoru je větší než nebo rovno 2000 MHz
- A celková paměť RAM je větší než nebo rovno 8192 MB
- A volné místo na disku je větší než nebo rovno 240 GB na systémové jednotce
- A baterie je je k dispozici
- A uživatel je TESTING\Administrator (shoda SID)

Below the list, the "Uživatel" (User) field is set to "TESTING\Administrator" and the "SID" field is set to "S-1-5-21-4043651708-3049840729-1205671662-500". The "Shoda podle SID" (Match by SID) checkbox is checked.

At the bottom of the dialog, there is a note: "Položka cílení pro uživatele umožňuje použití položky předvoleb u uživatelů pouze v případě, že je uživatel provádějící zpracování shodný s uživatelem určeným v položce cílení. [Další informace...](#)"