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

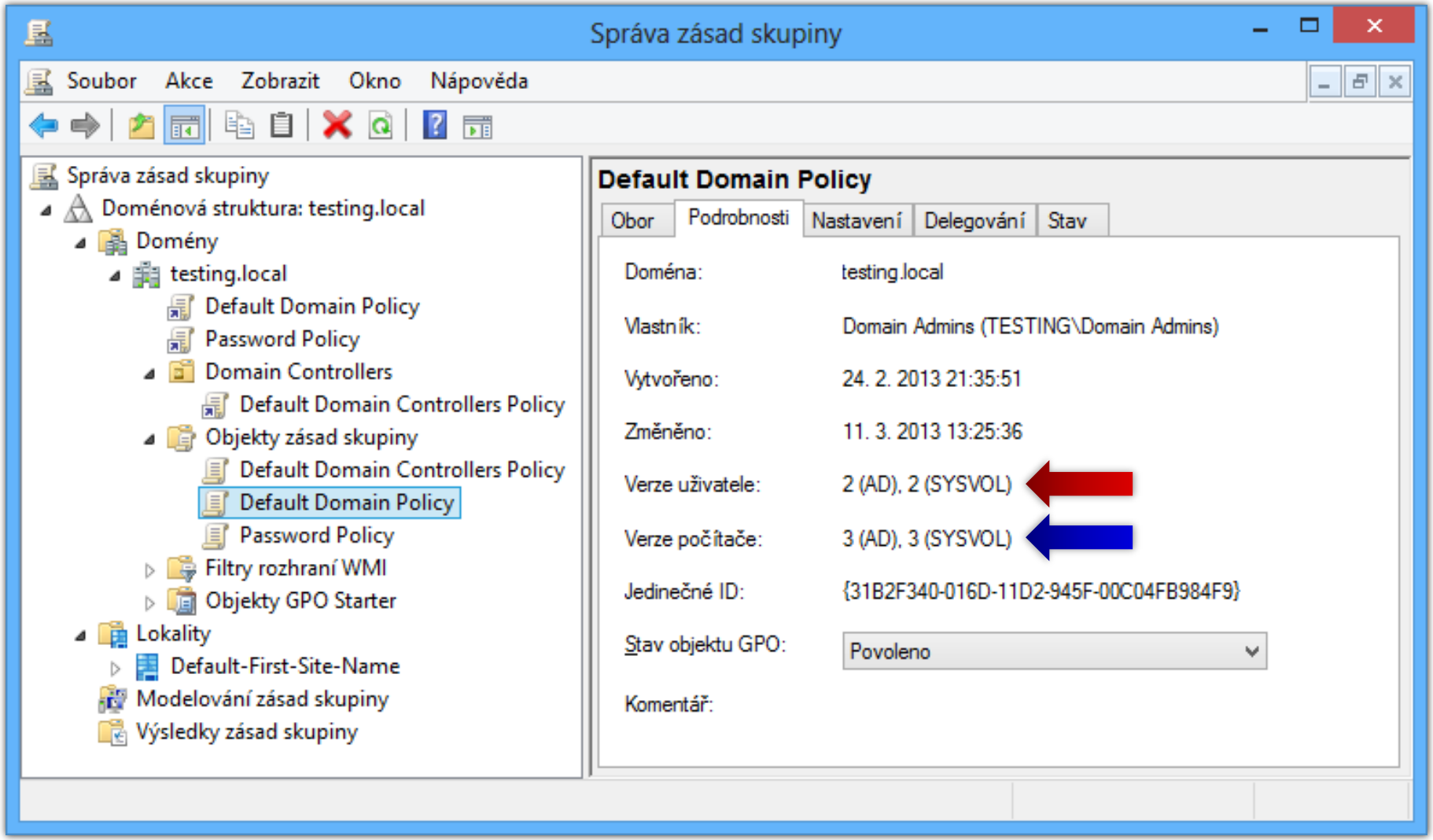
Active Directory

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



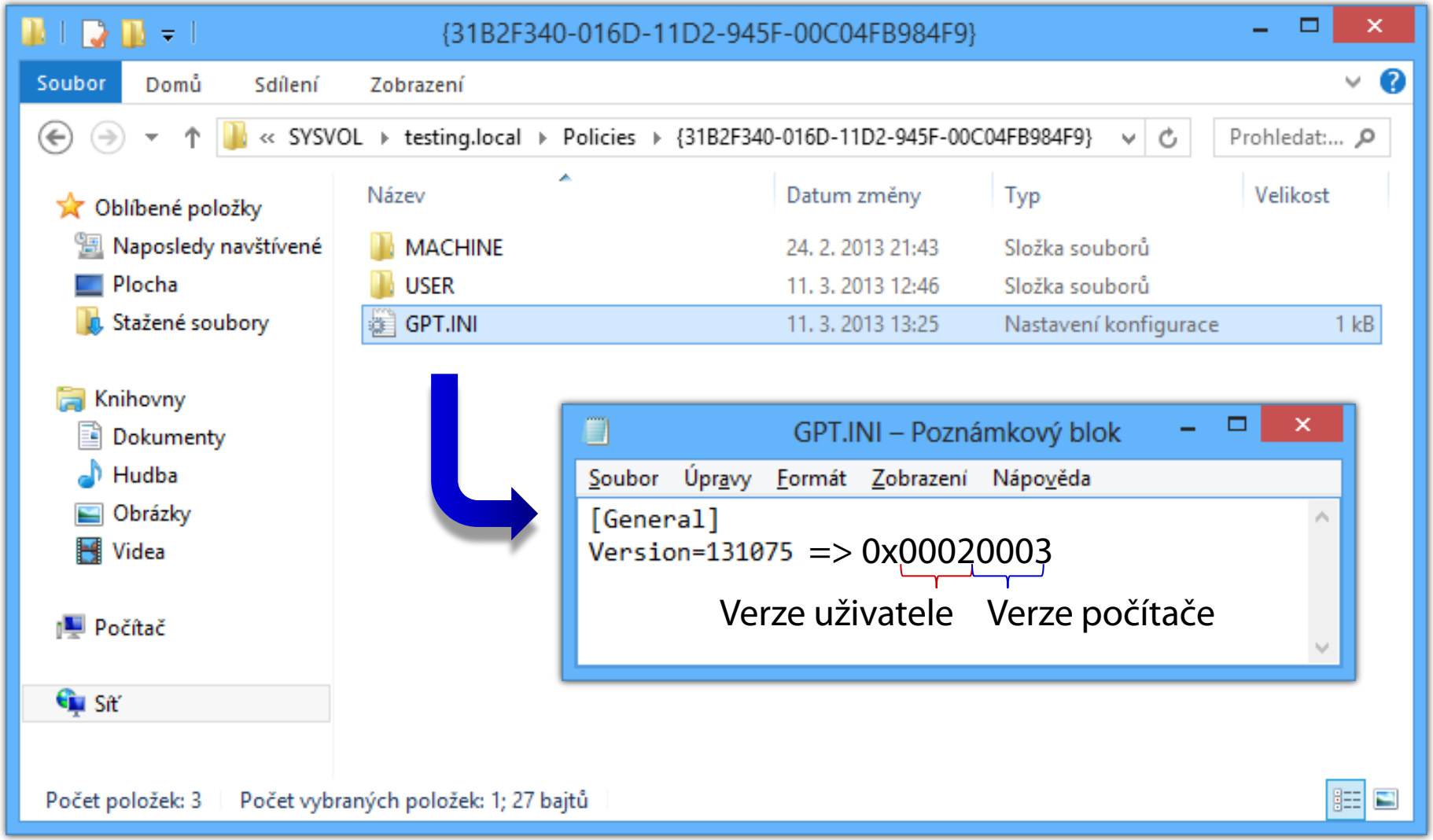
Kontejner zásad skupiny (GPC)

- 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



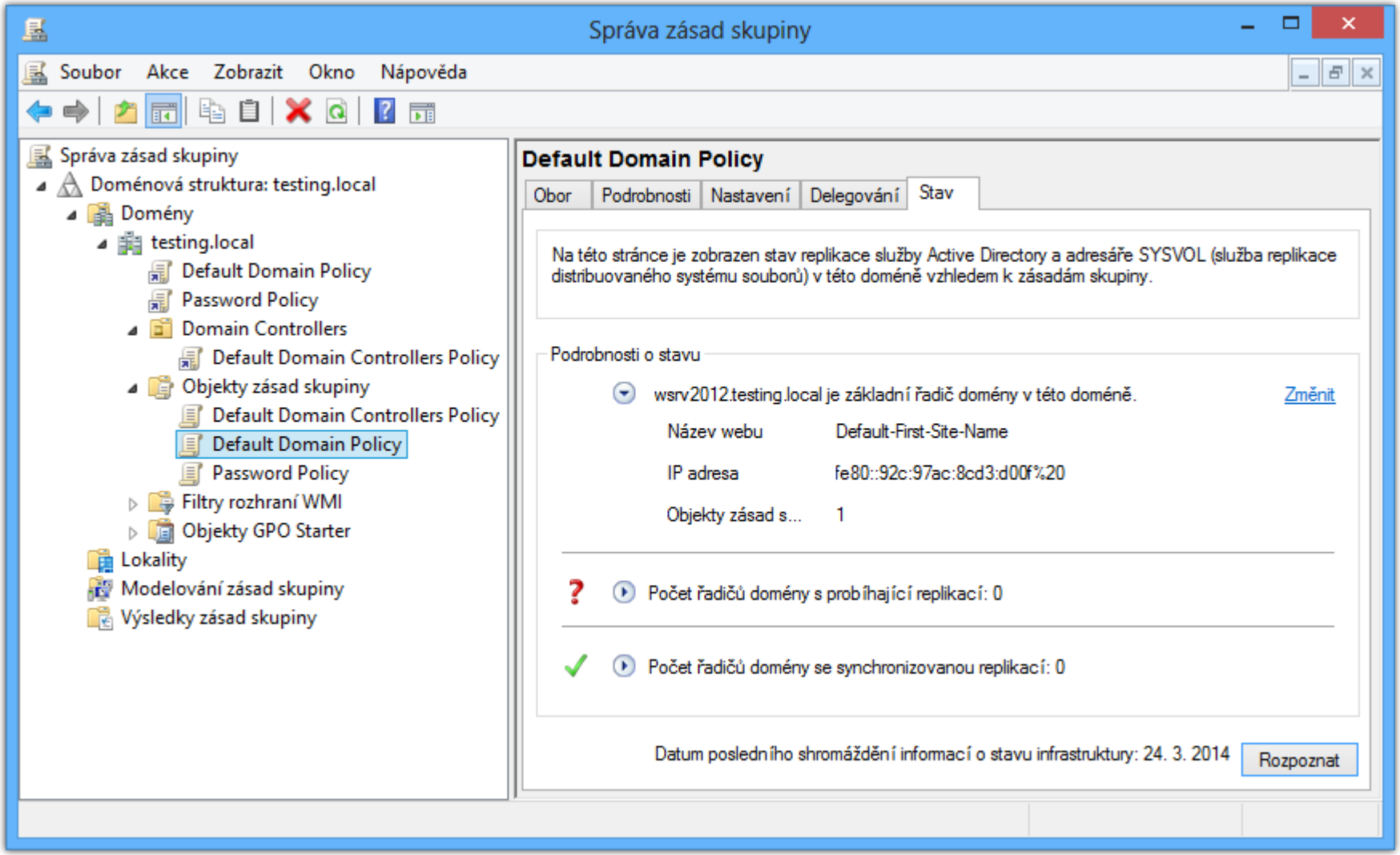
Replikace GPO objektů

- 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 **gpotool.exe**

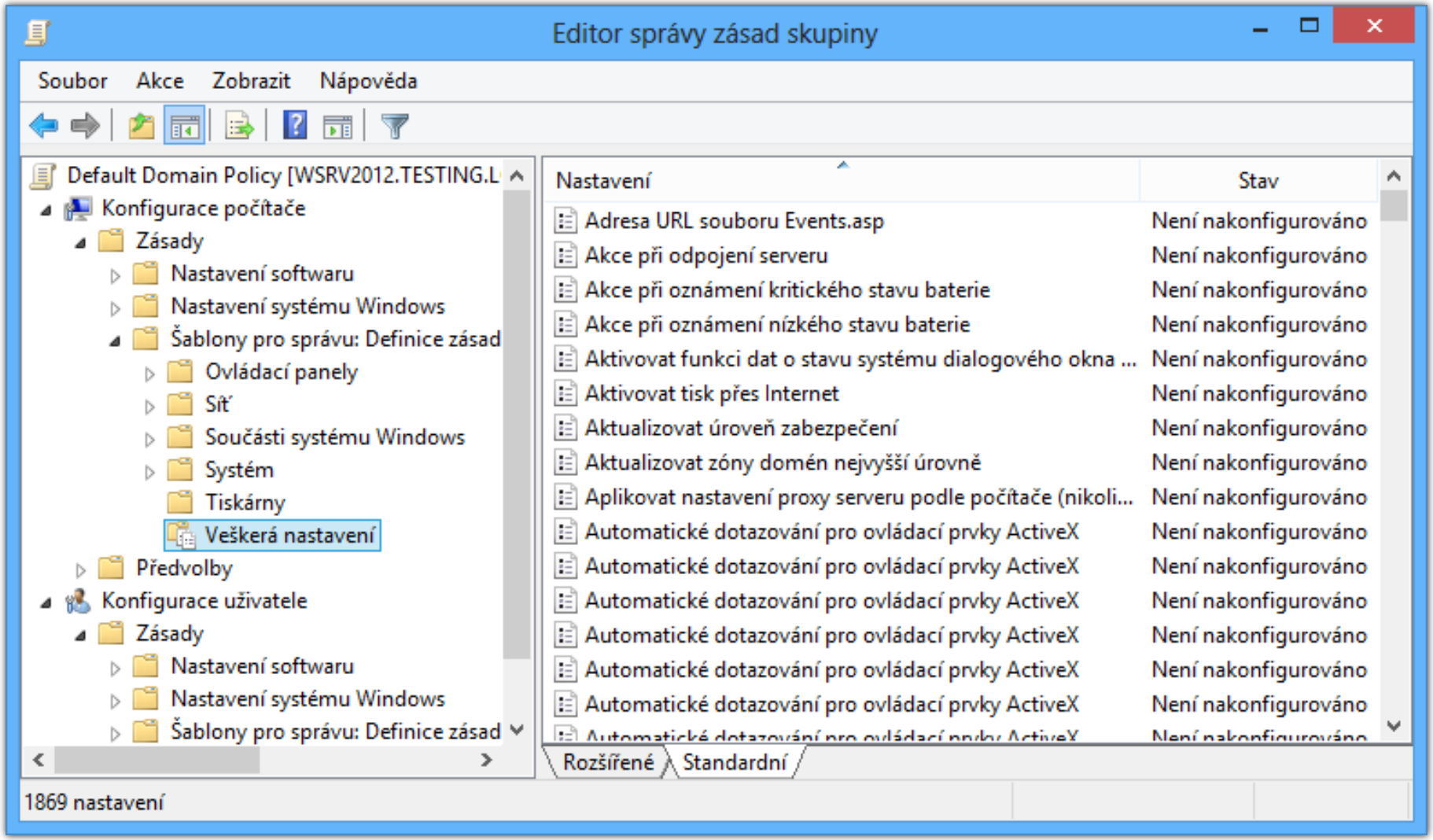
Stav replikace GPO objektů



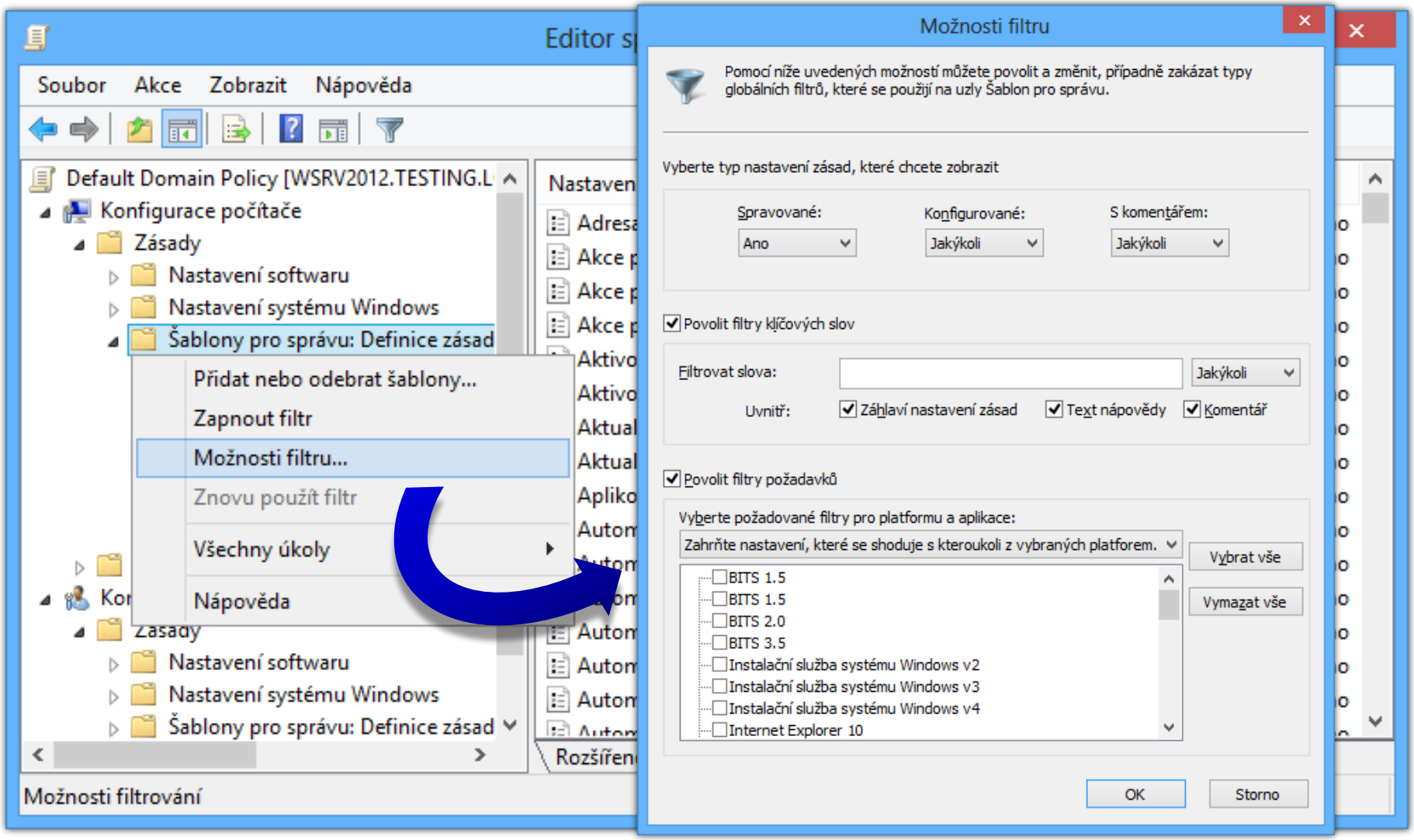
Zásady šablon pro správu

- 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



Filtrování zásad šablon pro správu



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 **$(*<typ>*.*<id>*)**
- 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 ***<systém>*\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

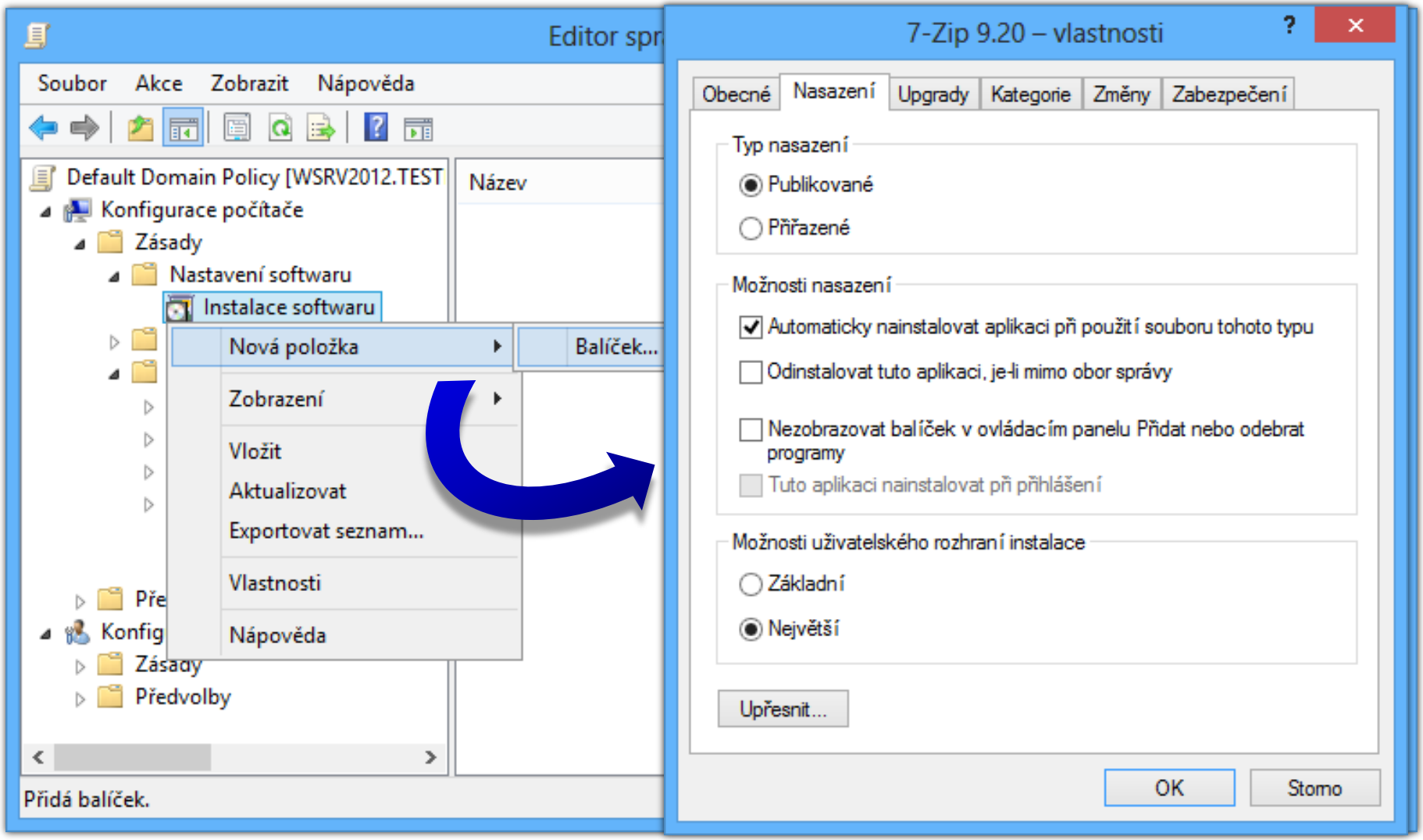
Přiřazení (assign) aplikací

- 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

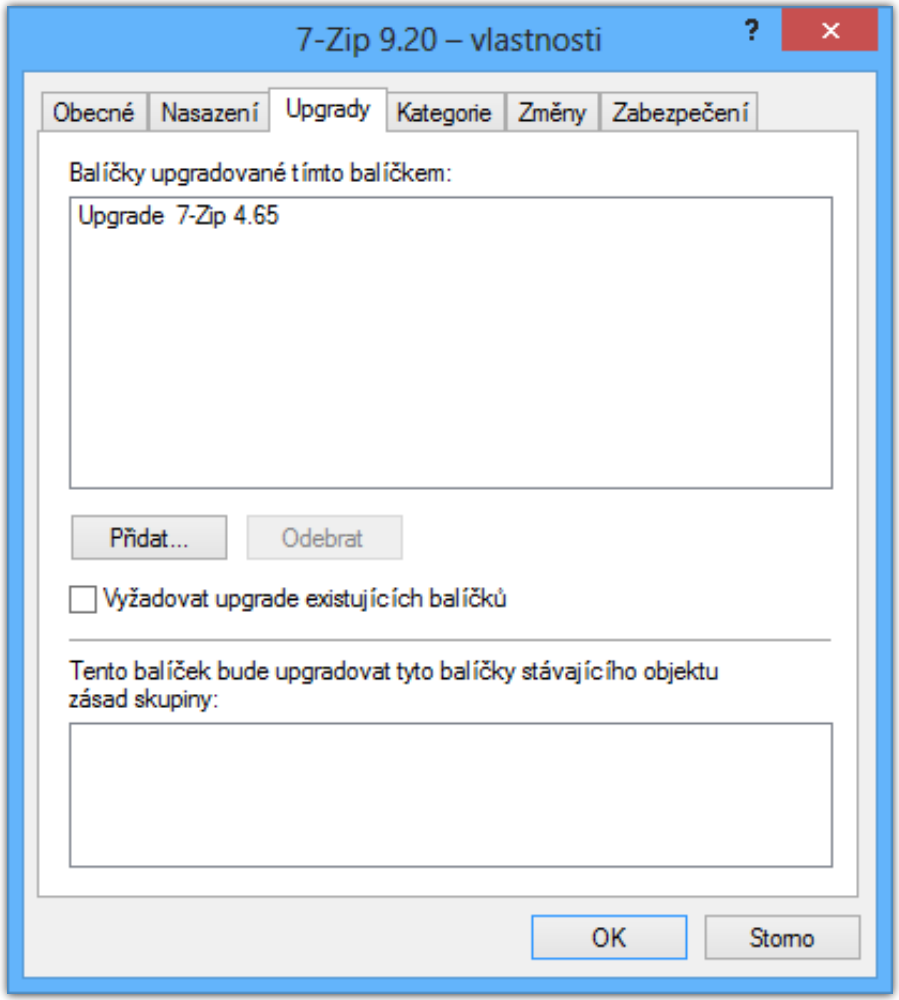
Publikování (publish) aplikací

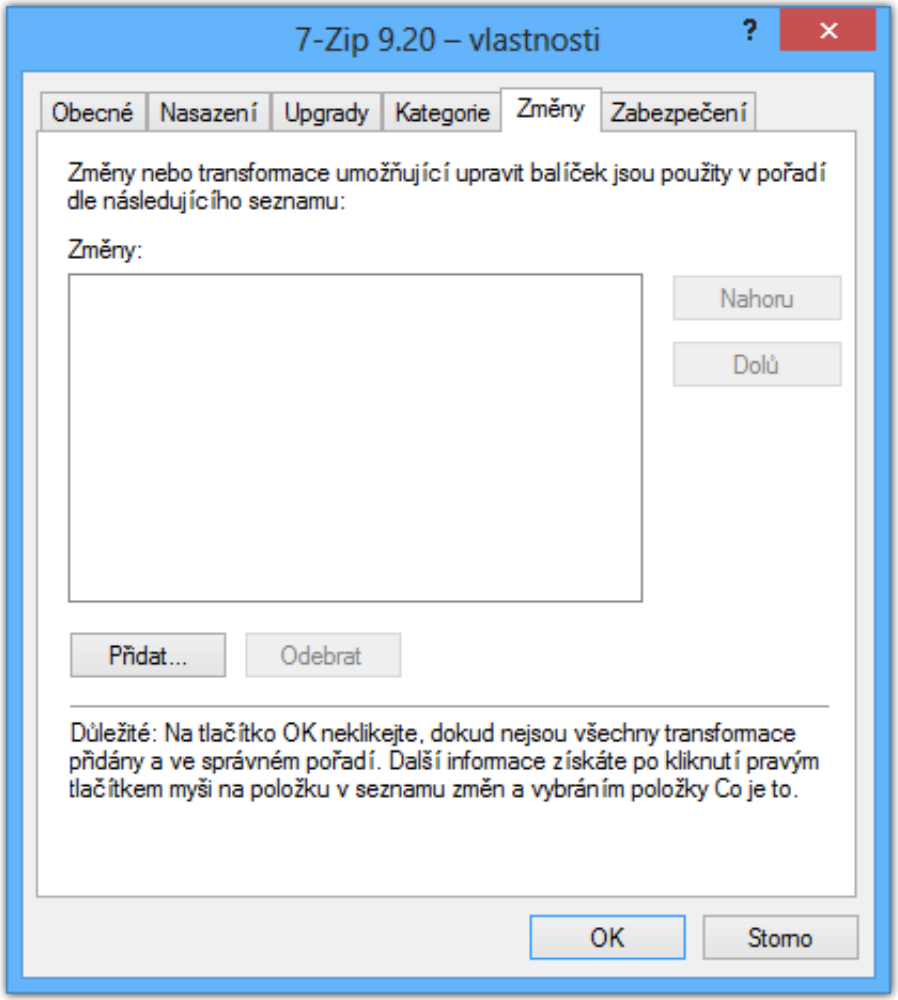
- Publikovat aplikace lze pouze pro uživatele
- Publikování
  - Umožnění instalace aplikace přes Programy a funkce (*Programs and Features*)
  - Nastavení asociace souborů s danou aplikací (pokud je povolena automatická instalace)
- Instalace
  - Manuálně přes Programy a funkce
  - Otevřením souboru,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

Nasazení aplikace

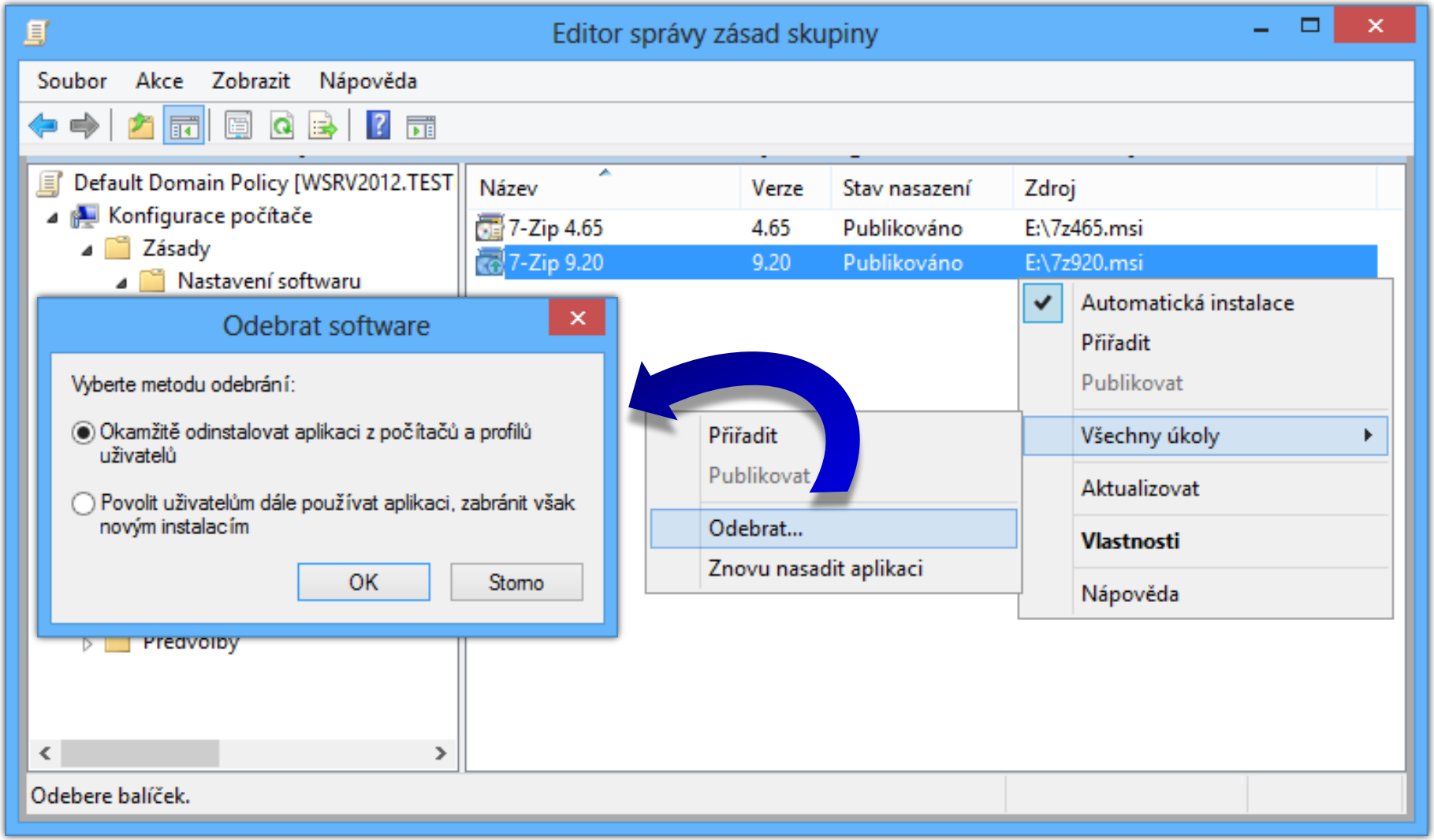


Upgrade a modifikace aplikace





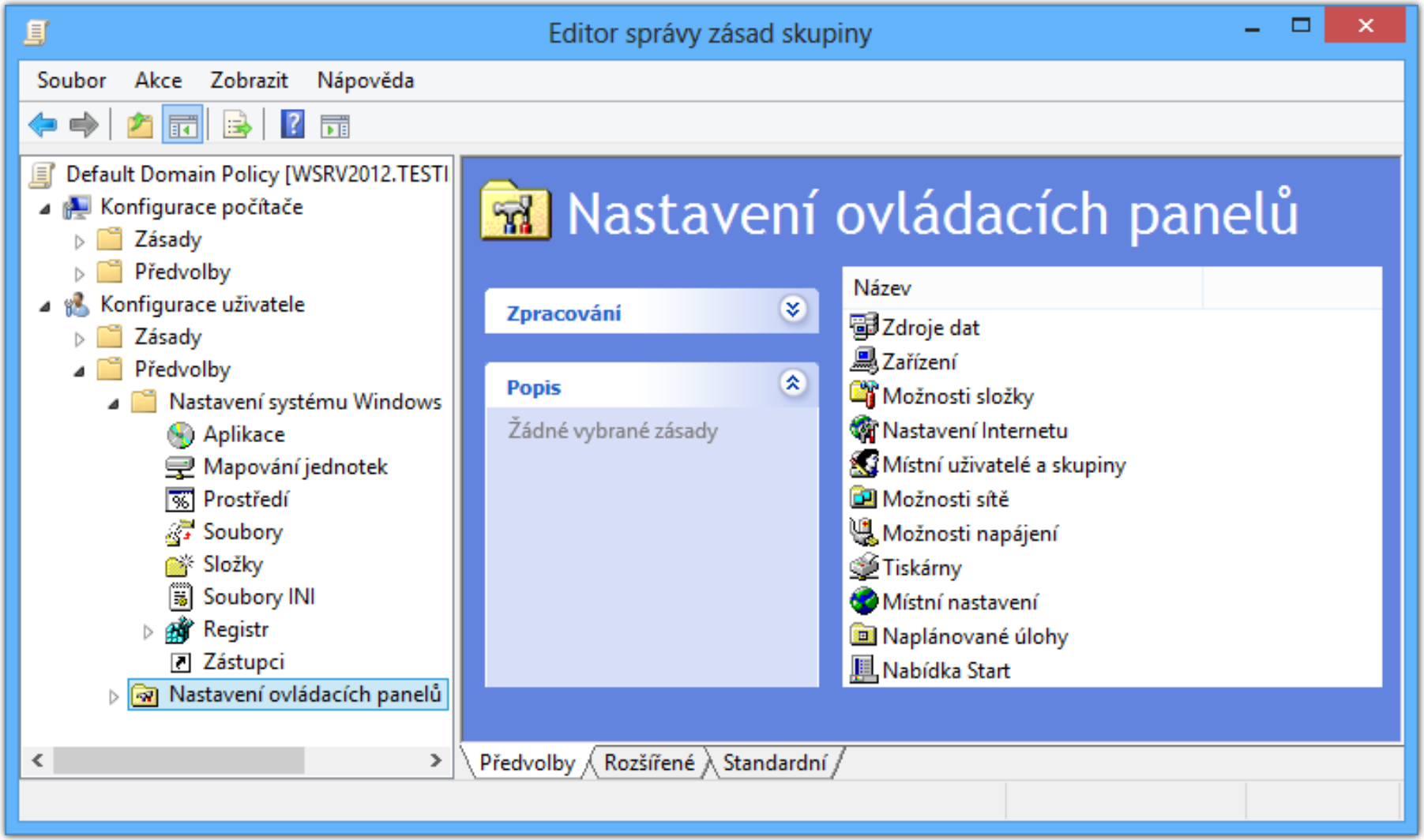
Odinstalace aplikace



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



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