Zásady skupiny

[Povinné]

Zásady skupiny (*Group policy*) jsou nedílnou součástí snad každé **Active Directory** domény. Řešení **IDA** je vhodné k zajištění bezpečnosti podnikových zdrojů. Dokáže *autentizovat* uživatele a zjistit, zda má mít daný uživatel přístup k nějakému zdroji. Neřeší ale, co vše, kromě přístupu ke zdrojům v podniku, může *autentizovaný* uživatel v doméně nebo na počítači, kde je přihlášen, provádět. Systém Windows obsahuje řadu nastavení určených pro uživatele a počítače, která umožňují velice detailně specifikovat jejich možnosti.

Z hlediska uživatele lze ovlivňovat hlavně nastavení týkající se uživatelského rozhraní, jako vzhled plochy či zobrazené položky v nabídce start, nebo nastavení systému a jeho jednotlivých služeb. Pro počítače je množství nastavení daleko bohatší, nejdůležitější jsou asi nastavení týkající se zabezpečení počítače zahrnující definici práv jednotlivých uživatelů, zásady pro účty a hesla nebo řízení aplikací či omezování softwaru. Veškerá tato nastavení je možné konfigurovat lokálně na každém počítači, což ale v doménovém prostředí není příliš vhodné.

Zásady skupiny umožňují veškerá nastavení definovat centrálně a aplikovat je na jednotlivé skupiny uživatelů či počítačů v podnikové síti. Jsou realizovány formou objektů zásad skupiny (**GPO**, *Group Policy Object*), které mohou ovlivňovat nějakou část podnikové sítě jako konkrétní doménu či místo (*site*) nebo jen objekty obsažené v určité organizační jednotce. Správné použití **zásad skupiny** výrazně snižuje administrativní nároky kladené na údržbu celé podnikové sítě a usnadňuje celkovou správu, je proto důležité vědět jak **zásady skupiny** pracují a jak mohou usnadnit práci.

Základní pojmy

[Povinné]

Nastavení zásady (*policy setting*). Jednotlivé zásady skupiny se skládají z jednoho či více nastavení zásady, často označované jako zásada (*policy*). Zásada definuje specifickou změnu v konfiguraci, jenž má být aplikována na zvolené uživatele a počítače. Zásady jsou vždy vázané na konkrétní typ objektu. Některé zásady ovlivňují pouze uživatele, nezávisle na počítači, ke kterému se tento uživatel přihlásí. Takovéto zásady se označují jako konfigurace uživatele (*user configuration settings*) nebo uživatelská nastavení (*user settings*). Jiné zásady zase naopak ovlivňují jen počítače, nezávisle na uživateli, který je k tomuto počítači přihlášen. Tyto zásady se označují jako konfigurace počítače (*computer configuration settings*) nebo nastavení počítače (*computer settings*). Každá zásada může nabývat jednoho ze tří stavů – Povoleno (*Enabled*), Zakázáno (*Disabled*) a nebo Nedefinováno (*Not defined*). Pokud není nějaká zásada definována, použije se buď nastavení specifikované na vyšší (obecnější) úrovni nebo výchozí nastavení. Některé zásady mohou vyžadovat dodatečné informace, které ovlivňují celkový dopad dané zásady na uživatele nebo počítač.

Objekt zásad skupiny (**GPO**, *group policy object*). Zásady jsou vždy definovány, a mohou existovat, pouze v rámci **GPO** objektu. **GPO** objekt je objekt **Active Directory**, jenž sdružuje jednu či více zásad a umožňuje tedy aplikovat více konfiguračních nastavení zároveň na dané uživatele a počítače.

Rozsah (*scope*). Aby se změny v konfiguraci obsažené v nějakém **GPO** objektu projevily u uživatelů nebo na počítačích v podnikové síti, je nejprve potřeba specifikovat konkrétní uživatele a počítače, na které se má tento objekt aplikovat. Tento proces je často označován jako určení rozsahu **GPO** objektu (*scoping*). Rozsah **GPO** objektu je tedy kolekce uživatelů a počítačů, na které se má daný **GPO** objekt aplikovat. Existuje několik metod jak definovat rozsah **GPO** objektu:

- **GPO odkaz** (*GPO link*). Každý **GPO** objekt může být připojen (*linked*) ke konkrétní doméně, místu (*site*) či organizační jednotce v **Active Directory**. Tato doména, místo nebo organizační jednotka pak tvoří maximální rozsah **GPO** objektu. Všichni uživatelé a počítače v dané doméně, místě či organizační jednotce, spolu se všemi uživateli a počítači v synovských organizačních jednotkách, budou ovlivněni konfigurací definovanou zásadami v daném **GPO** objektu. Jeden **GPO** objekt může být připojeno k více místům nebo organizačním jednotkám.
- **WMI filtr** (*Windows Management Instrumentation filter*). Tento typ filtru se využívá hlavně při aplikaci **GPO** objektů na počítače. Omezuje rozsah **GPO** objektu na základě charakteristiky

systému. Tedy určuje, na které počítače se má **GPO** objekt aplikovat na základě např. verze operačního systému, jenž na daném počítači běží, výkonu počítače či přítomných aplikací.

- **Bezpečnostní filtr** (*security filter*). Tento filtr definuje globální bezpečnostní (*global security*) skupiny, na které se má nebo nemá **GPO** objekt aplikovat. **GPO** objekt se tedy aplikuje nebo neaplikuje na uživatele a počítače, jenž patří do zadané skupiny.

Výsledná sada zásad (**RSoP**, *Resultant Set of policy*). Často jeden uživatel nebo počítač spadá pod rozsah více **GPO** objektů, což vede k možnostem, že nastavení určité zásady může být definováno odlišně v různých **GPO** objektech. Výsledná sada zásad zachycuje takové změny konfigurace, jenž budou nakonec aplikovány na daného uživatele nebo počítač po vyřešení všech konfliktů mezi odlišně definovanými stejnými zásadami.

Klient zásad skupiny a klientská rozšíření

[Povinné]

Klient zásad skupiny (*Group Policy Client*) je služba systému Windows, která zajišťuje aplikaci nastavení zásad definovaných v **GPO** objektech na daný počítač nebo uživatele. Samotnou aplikaci zásad ovšem vykonávají tzv. klientská rozšíření (**CSE**, *Client-Side Extensions*), což jsou procesy, jenž dokážou interpretovat konkrétní nastavení obsažená v nějakém **GPO** objektu a provádět odpovídající změny na lokálním počítači nebo u přihlášeného uživatele. Pro každou hlavní kategorii zásad skupiny existuje jedno **CSE** rozšíření, jenž tuto kategorii zpracovává. Např. existují **CSE** rozšíření pro aplikaci zabezpečení, pro modifikaci registrů, pro instalaci softwaru, pro spouštění skriptů a mnoho dalších. S každou novou verzí systému Windows samozřejmě přibývají nové zásady, jenž je možné definovat v **GPO** objektech, a tedy mohou přibývat i nová **CSE** rozšíření. Momentálně existuje několik tisíc zásad, které je možné definovat a několik desítek **CSE** rozšíření, jenž tyto zásady zpracovávají.

Je důležité vědět, že zásady skupiny jsou zaměřené na klienta (tzv. *client-driven*). Klient si stahuje (tzv. *pull* metoda) **GPO** objekty z řadiče domény a pak lokálně aplikuje nastavení na počítač nebo uživatele pomocí **CSE** rozšíření. Server v tomto nijak neparticipuje, nic sám neposílá (tzv. *push* metoda) klientovi, pouze zajišťuje uložení **GPO** objektů a jejich replikaci v rámci domény.

Chování **CSE** rozšíření může být ovlivňováno přes zásady skupiny. Standardně **CSE** rozšíření aplikují nastavení v nějakém **GPO** objektu pouze v případě, že byl tento objekt změněn, což zabraňuje zbytečné aplikaci stejného nastavení a zrychluje zpracování. Zde je vhodné si uvědomit, že řada nastavení se netýká jen zapsání hodnoty do registru a podobných jednoduchých akcí, může se jednat třeba o instalaci aplikace nebo vykonání skriptu. Také je zde problém s lokálními změnami. Většina nastavení je aplikována tak, že je normální uživatel nemůže nijak změnit. Ovšem existují i nastavení, která mohou být změněna i normálním uživatelem, navíc existuje řada nastavení, jenž mohou být změněna uživatelem s oprávněními administrátora. Pak může být výhodné změnit výchozí chování **CSE** rozšíření, aby aplikovala nastavení z **GPO** objektů i v případě, že nedošlo ke změně těchto objektů. Pokud pak nějaký uživatel změní určité nastavení lokálně tak, že je v rozporu s nastavením v **GPO** objektech, bude toto nastavení přepsáno při nejbližší aktualizaci zásad skupiny.

Typy GPO objektů

[Povinné]

Na konkrétní počítač či uživatele může být aplikováno nastavení z více **GPO** objektů. Tyto objekty mohou pocházet ze dvou zdrojů, na základě kterých se rozlišují dva typy **GPO** objektů. Prvním typem jsou lokální **GPO** objekty (*Local GPOs*), jenž jsou uloženy přímo na cílovém počítači. Druhým typem jsou doménové **GPO** objekty (*Domain-Based GPOs*), které se nacházejí na řadičích domény.

Lokální GPO objekty (*Local GPOs*). Počítače, na kterých běží systémy Windows 2000, Windows XP nebo Windows Server 2003 mají pouze jediný lokální **GPO** objekt. Tento **GPO** objekt existuje vždy, ať je počítač součástí nějaké domény, pracovní skupiny nebo vůbec není připojen k síti. Je uložen v adresáři ***<systém>*\System32\GroupPolicy**, kde *<systém>* je kořenový adresář systému Windows. Lokální **GPO** mohou ovlivňovat pouze nastavení počítače, na kterém se nacházejí. Při absenci domény jsou lokální **GPO** objekty jedinou možností, jak nastavit zásady pro nějaký počítač a jeho lokální uživatele.

V doméně se ovšem tento typ **GPO** objektů téměř nepoužívá, jelikož má nejnižší prioritu a nastavení stejných zásad obsažená v doménových **GPO** objektech vždy přepíší nastavení definovaná v lokálních **GPO** objektech.

V případě systémů Windows Vista, Windows 7 nebo Windows Server 2008 (R2) je k dispozici více lokálních **GPO** objektů, tzv. *multiple local GPOs*. Tyto objekty lze rozdělit do tří kategorií:

- **GPO místního počítače** (*Local Computer GPO*). Jediný lokální **GPO** objekt, ve kterém lze definovat nastavení počítače. Tento **GPO** objekt odpovídá lokálnímu **GPO** objektu z předchozích verzí systému Windows. Uživatelská nastavení v tomto **GPO** objektu ovlivňují všechny lokální uživatele.
- **GPO speciálních skupin**. Zde patří **GPO** objekty pro skupinu administrátorů (*Administrators*) a pro všechny ostatní uživatele (*Non-Administrators*). V těchto **GPO** objektech lze definovat pouze uživatelská nastavení, jenž budou aplikována na uživatele, jenž patří resp. nepatří do skupiny Administrators.
- **GPO místních uživatelů** (*User-Specific Local GPOs*). Tato skupina zahrnuje jeden **GPO** objekt pro každého lokálního uživatele. Opět lze definovat pouze uživatelská nastavení, která budou aplikována pouze na konkrétního uživatele.

Výsledná sada zásad, jenž bude aplikována na konkrétního uživatele, se potom získá následujícím postupem. Nejprve se na uživatele aplikují nastavení obsažené v **GPO** místního počítače. Tyto nastavení jsou pak přepsána konfliktními nastaveními v **GPO** skupiny administrátorů resp. ostatních uživatelů. Nakonec jsou na uživatele aplikována nastavení z jeho uživatelského **GPO**, jenž mohou přepsat předchozí konfliktní nastavení. Tedy čím specifičtější rozsah daný **GPO** objekt pokrývá, tím vyšší má prioritu. V případě počítače je situace jednoduchá. Pouze **GPO** lokálního počítače může obsahovat nastavení počítače, takže tento jediný objekt bude aplikován na počítač.

Doménové GPO objekty (*Domain-Based GPOs*). Doménové **GPO** objekty jsou vytvářeny v rámci **Active Directory** a jsou uloženy na všech řadičích domény. Tyto **GPO** objekty mohou být aplikovány na jakýkoliv počítač či uživatele v doméně. Každá **Active Directory** doména obsahuje po svém vzniku dva předdefinované **GPO** objekty:

- **Výchozí zásady domény** (*Default Domain Policy*). Tento **GPO** objekt je připojen přímo k doméně a ovlivňuje tedy všechny uživatele a počítače v této doméně (včetně řadičů domény). Obsahuje nastavení zásad týkajících se hesel, uzamykání účtů a služby Kerberos.
- **Výchozí zásady řadičů domény** (*Default Domain Controllers Policy*). Tento **GPO** objekt je připojen k organizační jednotce Řadiče domény (*Domain Controllers*). Jelikož všechny řadiče domény jsou přítomny v této organizační jednotce, nastavení v tomto **GPO** objektu bude aplikováno pouze na řadiče domény. Používá se hlavně pro definici zásad auditu nebo uživatelských práv.

Zpracování zásad skupiny

[Povinné]

Při zpracování zásad skupiny je dobré si uvědomit několik věcí. Vše k čemu zásady skupiny slouží je aplikace konkrétních zásad definovaných v **GPO** na cílového uživatele či počítač. **GPO** jsou aplikovány vždy v určeném pořadí, nejprve **GPO** připojené k místům, pak k doménám a nakonec k organizačním jednotkám. Nastavení zásad z **GPO**, jenž jsou aplikovány později, přepíšou nastavení stejných zásad aplikovaných dřívějšími **GPO**. Přesný postup zpracování zásad skupiny klientem je následující:

1. Naběhne počítač a síť, jsou spuštěny služby **RPCSS**[1] (*Remote Procedure Call System Service*) a **MUP**[2] (*Multiple Universal Naming Convention Provider*) a běží **Klient zásad skupiny**.

[1] Služba **Vzdálené volání procedur (RPC)** umožňuje klientovi vykonávat na serveru akce, které jsou potřeba pro obdržení všech potřebných objektů zásad skupiny (**GPO**), tedy takové akce, jenž zjistí, které **GPO** mají být na klienta aplikovány a které zajistí přenos těchto **GPO** ke klientovi

[2] Služba **Mup** zajišťuje přístup ke zdrojům na síti pomocí **UNC** (*Universal Naming Convention*) cesty

2. **Klient zásad skupiny** obdrží uspořádaný seznam všech **GPO** objektů, jejichž rozsah zahrnuje daný počítač. Uspořádání **GPO** objektů v tomto seznamu určuje také pořadí jejich zpracování. Standardně se nejprve zpracovávají lokální **GPO** objekty a pak postupně **GPO** objekty přiřazené k místu, doméně a organizačním jednotkám.
   a. **Lokální GPO objekty** (*Local GPOs*). Počítače na kterých běží Windows 2000, Windows XP nebo Windows Server 2003 mají pouze jediný **GPO** objekt a ten se tedy použije. Novější systémy jako Windows Vista, Windows 7 nebo Windows Server 2008 (R2) mají možnost definovat více lokálních **GPO** objektů (tzv. *multiple local GPOs*).
   b. **GPO objekty připojené k místu** (*Site GPOs*). Všechny **GPO** objekty, které jsou připojeny k místu, jenž obsahuje daný počítač, jsou přidány do uspořádaného seznamu nejdříve. Pokud je k danému místu připojeno více **GPO** objektů, pak pořadí připojení (*link order*) určuje pořadí jejich přidávání do seznamu. **GPO** objekty s nejnižším pořadím připojení jsou do seznamu přidány jako poslední, tedy budou aplikovány později než ostatní **GPO** objekty a přepíší nastavení **GPO** objektů, jenž byly aplikovány dříve.
   c. **GPO objekty připojené k doméně** (*domain GPOs*). Stejně jako u *site* **GPO** objektů, i zde jsou přidány jednotlivé **GPO** objekty, jenž jsou připojeny k doméně, která zahrnuje daný počítač, v pořadí určeném pořadím připojení.
   d. **GPO objekty připojené k organizačním jednotkám** (*OU GPOs*). Pořadí přidávání těchto objektů do uspořádaného seznamu závisí na hierarchii organizačních jednotek. **GPO** objekty připojené k organizačním jednotkám na nejvyšší úrovni hierarchie **Active Directory** jsou připojeny nejdříve. Pak se postupně přidávají **GPO** objekty připojené k organizačním jednotkám na nižších úrovních. Nakonec jsou pak přidány **GPO** objekty připojené k organizační jednotce, jenž obsahuje daný počítač. Pokud je ke konkrétní organizační jednotce připojeno více **GPO** objektů, přidají se opět v pořadí určeném pořadím připojení.
   e. **Vynucené GPO objekty** (*Enforced GPOs*). Tyto objekty jsou přidány až na konec uspořádaného seznamu a přepíší tedy veškerá konfliktní nastavení definovaná v **GPO** objektech v tomto seznamu dříve. Vynucené **GPO** objekty jsou přidávány v obráceném pořadí než standardní **GPO** objekty. Tedy nejprve se přidávají vynucené **GPO** objekty připojené k organizačním jednotkám, tentokrát ale v pořadí od nejnižší úrovně (**GPO** objekty připojené k OU, která obsahuje daný počítač) až k úrovni nejvyšší, pak vynucené **GPO** objekty připojené k doméně obsahující daný počítač a nakonec vynucené **GPO** objekty připojené k místu, kde je daný počítač situován. Tento postup umožňuje definovat zásady skupiny, jenž mají být vynuceny pro celou doménu. Stačí vytvořit vynucený **GPO** objekt připojený k doméně. Ten bude vždy aplikován až po aplikaci všech ostatních **GPO** objektů (kromě vynucených **GPO** objektů připojených k místu, jenž se používají málokdy) a vynutí tedy své nastavení na všech počítačích v doméně.
3. **Klient zásad skupiny** zpracuje **GPO** objekty synchronně v pořadí v jakém se vyskytují v obdrženém uspořádaném seznamu. Tedy nejprve lokální **GPO** objekty, pak **GPO** objekty připojené k místu, k doméně a k organizačním jednotkám a nakonec vynucené **GPO** objekty. Před zpracováním jednotlivých **GPO** objektů ovšem klient nejprve zjistí, zda má vůbec daný **GPO** objekt aplikovat. Nejprve ověří stav **GPO** objektu (zda má povoleno aplikovat nastavení pod uzlem konfigurace počítače) a oprávnění (zda disponuje počítač oprávněními Povolit zásady skupiny (*Allow Group Policy*)). V případě, že je na **GPO** objekt aplikován WMI filtr a pokud na počítači běží systém Windows XP nebo novější, provede klient WQL dotaz obsažený ve filtru a ověří, zda počítač splňuje požadavky tohoto filtru, aby na něj mohl být daný **GPO** objekt aplikován.
4. Pokud má být daný **GPO** objekt aplikován na počítač, **Klient zásad skupiny** spustí **CSE** rozšíření, jenž zpracují jednotlivé zásady obsažené v tomto **GPO** objektu. Nastavení zásad v daném **GPO** objektu přepíše nastavení zásad z dříve aplikovaných **GPO** objektů následovně:
   - Pokud je nějaká zásada definována (*povolena* či *zakázána*) v **GPO** objektu připojenému k nadřízenému (*parent*) kontejneru **Active Directory** (OU, doméně, místu) a zároveň je stejná zásada *nedefinována* v **GPO** objektu připojenému k podřízenému (*child*) kontejne-

ru, pak bude na počítač v podřízeném kontejneru aplikováno nastavení zásady definované v **GPO** objektu připojenému k nadřízenému kontejneru. V případě, že je na podřízeném kontejneru nastaveno blokování dědičnosti (*Block Inheritance*), nedojde k aplikaci nastavení z nadřízeného kontejneru, pokud není **GPO** objekt připojený k nadřízenému kontejneru vynucený, pak bude aplikován i přes blokování dědičnosti.

- Pokud je nějaká zásada definována (*povolena* či *zakázána*) v **GPO** objektu připojenému k nadřízenému (*parent*) kontejneru a stejná zásada je zároveň definována i v **GPO** objektu připojenému k podřízenému (*child*) kontejneru, pak nastavení v **GPO** objektu připojenému k podřízenému kontejneru přepíše nastavení v **GPO** objektu připojenému k nadřízenému kontejneru. Pokud ovšem je **GPO** objekt připojený k nadřízenému kontejneru vynucený, bude aplikováno nastavení z tohoto **GPO** objektu.
- Pokud je nějaká zásada *nedefinována* jak v **GPO** objektu připojenému k nadřízenému kontejneru, tak v **GPO** objektu připojenému k podřízenému kontejneru, pak bude použito výsledné nastavení z lokálních **GPO** objektů. Pokud ani v lokálních **GPO** objektech není daná zásada definována, použije se výchozí nastavení systému Windows.

5. Jakmile se na počítač přihlásí nějaký uživatel, jsou vykonány body 2 - 4, tentokrát ale pro uživatelská nastavení. Tedy klient opět obdrží uspořádaný seznam **GPO** objektů, jejichž rozsah zahrnuje daného uživatele, synchronně zpracuje jednotlivé **GPO** objekty v tomto seznamu a předá zásady, jenž se mají aplikovat, odpovídajícím **CSE** rozšířením.
6. Každých 90 - 120 minut po startu počítače se aktualizuje nastavení zásad daného počítače a opakují se kroky 2 - 4 pro nastavení počítače.
7. Každých 90 - 120 minut po přihlášení uživatele se aktualizuje nastavené zásad daného uživatele a opakují se kroky 2 - 4 pro uživatelská nastavení.

Pokud dojde k přerušení připojení k síti, a klient tedy nemůže kontaktovat žádný z řadičů domény, zůstávají v platnosti nastavení, jenž byla aplikována při poslední aktualizaci zásad skupiny. Jakmile je připojení obnoveno, **Klient zásad skupiny** ověří, zda již vypršel interval pro aktualizace zásad skupiny. Pokud ano, získá klient z řadiče domény nejnovější seznam **GPO** objektů pro daný počítač nebo uživatele a spustí proces aktualizace zásad skupiny.

Zpracování Loopback zásad skupiny [Povinné]

Ve výchozím nastavení budou na uživatele aplikována nastavení zásad z **GPO** objektů, jejichž rozsah zahrnuje daného uživatele. Tedy výsledná nastavení budou vždy stejná nezávisle na tom, na který počítač se daný uživatel přihlásí. Někdy je ovšem dobré tato nastavení ovlivňovat podle počítače, kde se uživatel přihlásil. Veškerá uživatelská nastavení se nacházejí pod uzlem konfigurace uživatele (*User Configuration*), jenž je při konfiguraci počítače ignorován a nastavení tedy nemohou být aplikována. Při konfiguraci uživatele zase uživatel dostane pouze **GPO** objekty, jenž ho zahrnují ve svém rozsahu, nezíská tedy **GPO** objekty, které zahrnují ve svém rozsahu daný počítač. Proto je potřeba celý proces zpracování zásad skupiny mírně pozměnit.

Loopback zpracování zásad skupiny upravuje výchozí chování algoritmu zpracování zásad skupiny při získávání uspořádaného seznamu **GPO** objektů. Namísto toho, aby se na uživatele aplikovalo nastavení obsažené v uzlu konfigurace uživatele v **GPO** objektech, jejichž rozsah zahrnuje daného uživatele, použije se nastavení obsažené v uzlu konfigurace uživatele, ovšem v **GPO** objektech, jenž zahrnují počítač, kde je uživatel přihlášen, ve svém rozsahu.

Loopback zpracování zásad skupiny se aktivuje povolením zásady **Režim zpracování Loopback uživatelských zásad skupiny** (*User Group Policy Loopback Processing Mode*). Po povolení této zásady je ještě potřeba zvolit jeden ze dvou režimů, jenž ovlivňují jak bude algoritmus modifikován:

- **Nahradit** (*Replace*). V tomto případě se místo seznamu **GPO** objektů pro daného uživatele získaného v bodě 5 použije seznam **GPO** objektů pro daný počítač, jenž byl obdržen v bodě 2. Na uživatele se pak aplikují nastavení z uzlu konfigurace uživatele obsažená v **GPO** objektech

v tomto seznamu. Všechny **GPO** objekty, které ve svém rozsahu obsahují daného uživatele, jsou tedy ignorovány.

- **Sloučit** (*Merge*). V tomto případě je seznam **GPO** objektů pro daný počítač obdržený v bodě 2 připojen na konec seznamu **GPO** objektů pro daného uživatele získaného v bodě 5. Jelikož jsou tímto **GPO** objekty pro daný počítač aplikovány později, přepíší nastavení definovaná v těchto objektech nastavení dříve provedená **GPO** objekty pro daného uživatele. Dojde tedy k dodatečné úpravě uživatelských nastavení daného uživatele podle uživatelských nastavení pro konkrétní počítač.

Uložení GPO objektů

[Povinné]

Nastavení zásad skupiny jsou v **Active Directory** reprezentována jako **GPO** objekty, tyto objekty se ovšem skládají ze dvou komponent – kontejner zásad skupiny (**GPC**, *Group Policy Container*) a šablona zásad skupiny (**GPT**, *Group Policy Template*). **GPC** kontejner je konkrétní objekt **Active Directory**, jenž je uložen v kontejneru Objekty zásad skupiny (*Group Policy Objects*). Stejně jako ostatní objekty **Active Directory** obsahuje globální unikátní identifikátor (**GUID**) a další atributy. Tento objekt ovšem neobsahuje žádná nastavení zásad skupiny. Tato nastavení jsou obsažena v **GPT** šabloně, což je kolekce souborů uložených v kořenovém adresáři **SYSVOL** na každém řadiči domény, přesněji v adresáři ***<systém>*\SYSVOL\Domain\Policies*<gpc-guid>***, kde *<gpc-guid>* je **GUID** identifikátor **GPC** kontejneru a *<systém>* je kořenový adresář systému Windows. V případě, že dojde ke změně nastavení zásad v **GPO** objektu, jsou tyto změny uloženy do **GPT** šablony na serveru, kde byl daný **GPO** objekt modifikován a replikovány s celým adresářem **SYSVOL** na ostatní řadiče domény.

Ve výchozím nastavení aplikují **CSE** rozšíření nastavení zásad v **GPO** objektu pouze pokud byl tento objekt změněn. Zjištění, zda byl daný **GPO** objekt změněn, se provádí na základě čísla verze tohoto objektu. Toto číslo je inkrementováno pokaždé, když dojde ke změně nastavení nějaké zásady obsažené v daném **GPO** objektu, a je uloženo jako atribut **GPC** kontejneru a také v souboru **GPT.ini** v **GPT** adresáři. Klient si pamatuje číslo verze každého **GPO** objektu, jenž aplikoval naposledy a při aktualizaci nejprve ověří, zda byl daný **GPO** objekt změněn a je potřeba ho tedy aplikovat.

Replikace GPO objektů

[Povinné]

Replikace **GPO** objektů mezi jednotlivými řadiči domény je komplikovanější, jelikož každá z obou komponent **GPO** objektu je replikována odlišným způsobem. Replikaci **GPC** kontejnerů zajišťuje **DRA** (*Directory Replication Agent*) s využitím topologie generované **KCC** (*Knowledge Consistency Checker*). Výsledkem je, že **GPC** kontejnery jsou replikovány v rámci daného místa (*site*) během několika sekund a mezi místy podle nastavení mezimístní (*intersite*) replikace.

Replikace **GPT** šablon je realizována jednou ze dvou technologií. Buď pomocí služby replikace souborů (**FRS**, *File Replication Service*), která je podporována i staršími systémy jako Windows 2000 nebo Windows Server 2003. Nebo lze využít novější a robustnější replikaci distribuovaného souborového systému (**DFS-R**, *Distributed File System Replication*), jenž je k dispozici od verze systému Windows Server 2008.

Jelikož jsou **GPC** kontejnery a **GPT** šablony replikovány odděleně, může nastat situace, kdy nejsou tyto komponenty synchronizovány, tedy došlo k replikaci pouze jedné z těchto částí. Zde mohou nastat dvě situace. Buď dojde pouze k replikaci **GPC** kontejneru, což je častější případ. V tomto případě klient při obdržení uspořádaného seznamu **GPO** objektů zjistí, že došlo ke změně daného **GPC** kontejneru a pokusí se získat odpovídající **GPT** šablonu. Tato šablona ovšem bude obsahovat jiné číslo verze a dojde k chybě, kterou klient zaznamená do protokolu událostí. Nebo se dříve replikuje **GPT** šablona. Zde klient vůbec nezjistí, že došlo k nějaké změně, dokud se nereplikuje také odpovídající **GPC** kontejner. Tyto nekonzistence mezi **GPC** kontejnery a **GPT** šablonami lze jednoduše identifikovat pomocí nástroje **Gpotool.exe**[3] (*Group Policy Verification Tool*).

[3] **Gpotool.exe** je k dispozici zde http://go.microsoft.com/fwlink/?linkid=27766

Šablony pro správu

[Povinné]

Zásady situované pod uzlem Šablony pro správu (*Administrative Templates*) slouží k modifikaci registru. V případě, že spadají pod uzel Konfigurace počítače (*Computer Configuration*), tak modifikují hodnoty klíčů registru ve větvi HKEY_LOCAL_MACHINE (HKLM). Pokud náleží pod uzel Konfigurace uživatele (*User Configuration*), tak modifikují hodnoty klíčů registru ve větvi HKEY_CURRENT_USER (HKCU). Tyto zásady jsou vytvářeny na základě šablon pro správu.

Šablona pro správu (*administrative template*) je normální textový soubor, jenž obsahuje definice jednotlivých zásad. Pro každou zásadu obsahuje hlavně informace o klíči registru, který tato zásada modifikuje, a podrobné informace, ze kterých se generuje uživatelské rozhraní pro nastavení této zásady. Tyto informace zahrnují např. název zásady, třídu (zásada pro počítač nebo uživatele), popis, seznam podporovaných verzí systému, ale hlavně informace definující jak se mají změnit hodnoty cílového klíče registru na základě nastavení této zásady.

Šablony pro správu umožňují přidávat nové zásady, jenž mohou modifikovat klíče registru, čehož lze s výhodou využít pro centralizovanou konfiguraci aplikací třetích stran. Stačí pouze vytvořit novou šablonu pro správu a přidat ji k uzlu Šablony pro správu. Zásady obsažené v této šabloně pak budou součástí všech **GPO** objektů. Při vytváření nových šablon pro správu lze vycházet z předdefinovaných, nebo dříve definovaných, šablon. Tyto šablony se označují jako tzv. *Starter* **GPO** objekty.

V předchozích verzích systému Windows (před Windows Vista) byly šablony pro správu **ADM** soubory (soubory s příponou *.adm*). Tyto soubory měly ovšem několik nevýhod. Veškerá lokalizace se musela provádět v rámci **ADM** souboru, tedy pro každý jazyk musel existovat jeden ADM soubor a při úpravách se musely modifikovat všechny tyto soubory. Dalším problémem bylo uložení. **ADM** soubory byly součástí **GPT** šablon, tedy každý **GPO** objekt, jenž používal danou šablonu, obsahoval v **GPT** šabloně jednu kopii **ADM** souboru této šablony. Kromě zbytečné replikace stejných dat to znamenalo také problémy při úpravách **ADM** souboru šablony, kdy musely být změněny veškeré kopie.

Od systémů Windows Vista a Windows Server 2008 jsou šablony pro správu dvojice XML souborů, jeden pro definici jednotlivých zásad (**ADMX** soubor, soubor s příponou *.admx*) a druhý pro definici uživatelského rozhraní v různých jazycích (**ADML** soubor, soubor s příponou *.adml*). **ADML** soubory pouze mapují speciální identifikátory na odpovídající prvek rozhraní nebo text v konkrétním jazyce. **ADMX** soubory pak používají místo prvků a textů jen tyto identifikátory. Při editaci zásady definované v **ADMX** souboru se pak jen vyhledá odpovídající **ADML** soubor, jenž bude použit pro generování uživatelského rozhraní.

V případě použití **ADMX**/**ADML** šablon pro správu obsahuje **GPO** objekt pouze ty informace, jenž klient potřebuje pro zpracování daného **GPO** objektu. Při editaci **GPO** objektu pak editor zásad skupiny (**GPME**, *Group Policy Management Editor*) načte **ADMX** a **ADML** soubory z lokálního počítače. Lze ale vytvořit jakési centrální úložiště (*central store*) pro tyto šablony. Centrální úložiště je speciální adresář v kořenovém adresáři **SYSVOL**, kde jsou uloženy veškeré šablony pro správu. Pokud tento adresář existuje, **GPME** bude načítat všechny šablony z tohoto adresáře, místo z lokálního počítače.

Centrální úložiště se vytvoří jednoduše. Stačí pouze vytvořit adresář **PolicyDefinitions** v adresáři ***<FQDN domény>*\SYSVOL*<FQDN domény>*\Policies** a pak do něj přesunout šablony pro správu uložené v adresáři ***<systém>*\PolicyDefinitions**, kde *<systém>* je kořenový adresář systému Windows na lokálním počítači.

Instalace softwaru pomocí zásad skupiny

[Povinné]

Instalace softwaru pomocí zásad skupiny (**GPSI**, *Group Policy Software Instalation*) se používá pro zajištění přístupu uživatelů k aplikacím, jenž potřebují, ať jsou přihlášeni na jakémkoliv počítači. Tyto aplikace mohou být centrálně aktualizovány, spravovány nebo odebírány. Tuto funkcionalitu poskytuje jedno z **CSE** rozšíření, rozšíření instalací softwaru (*Software Instalation Extension*).

GPSI využívá **Instalační službu systému Windows** (*Windows Installer service*) pro instalaci, aktualizaci a odstraňování softwaru. Tato služba pracuje s instalačními balíky Windows (*Windows Installer package*), což jsou soubory s příponou *.msi*, které zachycují stav nainstalované aplikace. Tento balík

obsahuje informace potřebné pro instalaci a odebrání dané aplikace. Instalační balíky Windows lze také upravovat jedním z následujících způsobů:

- **Transformační soubory** (*Transform files*). Soubory s příponou *.mst*, které umožňují upravovat proces instalace dané aplikace. Tyto soubory se používají hlavně pro konfiguraci instalátoru aplikace tak, aby mohla být provedena bez zásahu uživatele.
- **Záplatové soubory** (*Patch files*). Soubory s příponou *.msp*, které umožňují aktualizovat existující *.msi* soubory. Tyto soubory se používají hlavně pro aplikaci aktualizací a oprav. Obsahují informace potřebné pro aplikaci aktualizovaných souborů a klíčů registrů.

GPSI poskytuje několik možností, jak provést instalaci aplikace. Buď lze aplikaci přiřadit uživateli či počítači, nebo publikovat uživateli:

- **Přiřazení aplikace** (*assigning*). Při přiřazení aplikace uživateli jsou na počítači, kde je uživatel přihlášen, zapsána nastavení této aplikace do lokálního registru (včetně přípon souborů dané aplikace) a přidáni zástupci na plochu nebo do nabídky Start. Aplikace je nainstalována teprve tehdy, když ji uživatel spustí nebo otevře soubor, s jehož příponou je aplikace asociována. Pokud je aplikace přiřazena počítači, je nainstalována při startu daného počítače.
- **Publikování aplikace** (*publishing*). Při publikování aplikace uživateli je aplikace pouze k dispozici pro instalaci v Přidat nebo odebrat programy (*Add Or Remove Programs*) ve starších systémech jako Windows XP nebo v Programy a funkce (*Programs And Features*) na novějších systémech jako Windows Vista, Windows 7 nebo Windows Server 2008 (R2). Instalace je také spuštěna, pokud uživatel otevře soubor, jenž je asociován s danou aplikací.

CSE rozšíření mohou automaticky ověřovat rychlost linky, kterou jsou spojeny s řadičem domény. Rozšíření instalací softwaru, které využívá **GPSI**, je jedním z nich. Za pomalou linku (*slow link*) se bere ve výchozím nastavení linka s rychlostí nižší než 500 kbps. **GPSI** standardně neprovádí instalace softwaru přes pomalou linku. Toto Chování lze změnit v zásadách skupiny, stejně jako práh pro rozhodování, zda je daná linka pokládána za pomalou.

Úkoly vedené lektorem

- Před spuštěním jednotlivých virtuálních strojů zkontrolujte správné nastavení jejich síťových adaptérů !!! U všech stanic (**win2008r2-dc**, **win7-domain** a **win2008r2-mbr**) musí být povoleny adaptéry *Internal* a *Private1*. A vždy v tomto pořadí !!!
- Na všech stanicích zakažte *Internal* síťové rozhraní (**LAN1**) a povolte ho pouze v případech, že je potřeba přistupovat na externí síť !!!
- Pro přístup na server **yetti** přes *Internal* síťové rozhraní je nutné použít jeho plně kvalifikované doménové jméno **yetti.nepal.aps**

Lab L01 – GPME (Group Policy Management Editor) [Na cvičeních]

Lab L02 – Zpracování GPO objektů [Provést]

Cíl cvičení

Naučit se pracovat s GPO objekty, prakticky si vyzkoušet postup uplatňování nastavení zásad obsažených v GPO objektech, seznámit se s výjimkami ovlivňujícími priority a pořadí aplikace GPO objektů

Potřebné virtuální stroje

Windows 7 AD, Enterprise 32bit (**win7-domain**)
Windows 2008R2 AD, Enterprise 64bit (**win2008r2-dc**)

Další prerekvizity

Účet uživatele **homer** v organizační jednotce **brno** v doméně **testing.local**

1. Otevřete **GPME** (*Group Policy Management Editor*)
   a. Start → (All Programs) → Administrative Tools → **Group Policy Management**
2. Vytvořte nový GPO objekt **Site GPO**
   a. Klikněte pravým na kontejner Group Policy Objects a zvolte New
   b. Jako název (Name) zvolte **Site GPO** a u Source Starter GPO ponechte **(none)**
   c. Potvrďte OK
3. Zakažte v GPO objektu **Site GPO** zobrazování některých položek v ovládacích panelech
   a. Klikněte pravým na GPO objekt **Site GPO** a zvolte Edit…
   b. Vyberte uzel User Configuration \ Policies \ Administrative Templates \ Control Panel
   c. Klikněte pravým zásadu na Hide specified Control Panel items a zvolte Edit
   d. Přepněte nastavení na Enabled a pod Options zvolte Show… u List of disallowed Control Panel items
   e. Do řádků sloupce Value postupně zadejte **Microsoft.Fonts**, **Microsoft.DeviceManager**, **Microsoft.BackupAndRestore** a **Microsoft.AdministrativeTools** a potvrďte OK
   f. Potvrďte nastavení zásady pomocí OK
4. Připojte GPO objekt **Site GPO** k místu **Default-First-Site-Name**
   - Pokud se pod kontejnerem Sites nenachází místo **Default-First-Site-Name**, pak klikněte pravým na kontejner Sites a zvolte Show Sites…, zaškrtněte **Default-First-Site-Name** a potvrďte OK
   a. Klikněte pravým na místo **Default-First-Site-Name** a zvolte Link an Existing GPO…
   b. Pod Group Policy objects vyberte **Site GPO** a potvrďte OK
5. Přihlaste se na **win7-domain** jako uživatel **homer** a ověřte, že nastavení byla aplikována

   a. Ověřte, že v Control Panel chybí možnosti Fonts, Device Manager, Backup and Restore, Administrative Tools

6. Vytvořte nový GPO objekt **Domain GPO** a rovnou ho připojte k doméně **testing.local**
   a. Klikněte pravým na doménu **testing.local** a zvolte Create a GPO in this domain, and Link it here…
   b. Jako název (Name) zvolte **Domain GPO** a u Source Starter GPO ponechte **(none)**
   c. Potvrďte OK
7. Zakažte v GPO objektu **Domain GPO** zobrazování několika položek, nyní jen **Microsoft.Fonts**, **Microsoft.DeviceManager**, **Microsoft.BackupAndRestore**, podle postupu z **bodu 3**
8. Na **win7-domain** ověřte, že byla aplikována nastavení zásad z GPO objektu **Domain GPO**
   a. Spusťte příkaz **gpupdate /force**
   b. Ověřte, že Administrative Tools jsou nyní přítomny v Control Panel

   ➢ Standardní GPO objekty připojené k doméně mají vždy vyšší prioritu než standardní GPO objekty připojené k místu, **Domain GPO** objekt bude aplikován až po **Site GPO** objektu a přepíše tedy konfliktní nastavení
9. Vytvořte nový GPO objekt **Brno GPO** a připojte ho k organizační jednotce **brno** podle postupu z **bodu 6**
10. Zakažte v GPO objektu **Brno GPO** zobrazování několika položek, tentokrát **Microsoft.Fonts** a **Microsoft.DeviceManager**, podle postupu z **bodu 3**
11. Na **win7-domain** ověřte, že byla aplikována nastavení zásad z GPO objektu **Brno GPO**
    a. Spusťte příkaz **gpupdate /force**
    b. Ověřte, že Administrative Tools i Backup and Restore jsou přítomny v Control Panel

    ➢ Standardní GPO objekty připojené k nějaké organizační jednotce mají vždy vyšší prioritu než standardní GPO objekty připojené k místu či doméně, **Brno GPO** objekt bude tedy aplikován až po **Domain GPO** a **Site GPO** objektech a přepíše tedy konfliktní nastavení
12. Vytvořte nový GPO objekt **Brno Priority GPO** a připojte ho k organizační jednotce **brno** podle postupu z **bodu 6**
13. Zakažte v GPO objektu **Brno Priority GPO** zobrazování jediné položky **Microsoft.Fonts** podle postupu z **bodu 3**
14. Nastavte u GPO objektu **Brno Priority GPO** vyšší prioritu, než má GPO objekt **Brno GPO**
    a. Vyberte organizační jednotku **brno**
    b. Na záložce Linked Group Objects Objects posuňte pomocí šipek vlevo **Brno Priority GPO** nad **Brno GPO**, aby **Brno Priority GPO** mělo nižší *link order* než **Brno GPO**
15. Na **win7-domain** ověřte, že byla aplikována nastavení zásad z GPO objektu **Brno Priority GPO**
    a. Spusťte příkaz **gpupdate /force**
    b. Ověřte, že Device Manager je nyní přítomen v Control Panel

    ➢ V případě, že mají dva GPO objekty stejnou prioritu (jsou oba připojeny k doméně, místu nebo dané organizační jednotce), rozhoduje o pořadí jejich aplikace tzv. pořadí připojení (*link order*), **Brno Priority GPO** má nižší *link order* než **Brno GPO**, bude tedy aplikován až po aplikaci **Brno GPO** a přepíše konfliktní nastavení
16. Odeberte v GPO objektu **Domain GPO** odkaz na adresář s hrami z nabídky Start
    a. Klikněte pravým na GPO objekt **Domain GPO** a zvolte Edit…
    b. Vyberte uzel User Configuration \ Policies \ Administrative Templates \ Start Menu and Taskbar
    c. Klikněte pravým zásadu na Remove Games link from Start Menu a zvolte Edit
    d. Přepněte nastavení na Enabled a potvrďte OK

17. Na **win7-domain** ověřte, že došlo k aplikaci nastavení zásad z GPO objektů **Brno Priority GPO** a **Domain GPO**
    a. Spusťte příkaz **gpupdate /force**
    b. Ověřte, že v Control Panel chybí pouze Fonts a v nabídce Start zase chybí Games
    ➢ Jelikož nastavení zásady, které odebírá odkaz na adresář s hrami, není definováno v GPO objektech připojených k organizační jednotce **brno**, dojde ke zdědění této zásady z GPO objektů výše (GPO objektů aplikovaných dříve), v tomto případě z **Domain GPO**
18. Zakažte dědičnost na organizační jednotce **brno**
    a. Klikněte pravým na organizační jednotku **brno** a zvolte Block Inheritance
19. Na **win7-domain** ověřte, že nedošlo k aplikaci nastavení zásad z GPO objektu **Domain GPO**
    a. Spusťte příkaz **gpupdate /force**
    b. Ověřte, že nabídka Start nyní obsahuje Games
20. Vynuťte aplikaci GPO objektu **Domain GPO** na doménu **testing.local**
    a. Klikněte pravým na GPO odkaz **Domain GPO** připojený k doméně **testing.local** a vyberte Enforced
21. Na **win7-domain** ověřte, že došlo k aplikaci nastavení zásad z GPO objektu **Domain GPO** a ty navíc přepsaly konfliktní nastavení z GPO objektů **Brno GPO** i **Brno Priority GPO**
    a. Spusťte příkaz **gpupdate /force**
    b. Ověřte, že pouze Administrative Tools jsou přítomny v Control Panel a že v nabídce Start chybí Games
    ➢ Vynucené (*enforced*) GPO objekty jsou aplikovány i v případě blokováni dědičnosti, navíc má tento typ objektů vyšší prioritu, jsou aplikovány vždy až po aplikaci všech standardních GPO objektů, zde tedy nastavení zásad z GPO objektu **Domain GPO** přepíšou konfliktní nastavení zásad z GPO objektů **Brno GPO** a **Brno Priority GPO**
22. Vynuťte aplikaci GPO objektu **Site GPO** na místo **Default-First-Site-Name**
    a. Klikněte pravým na GPO odkaz **Site GPO** připojený k místu **Default-First-Site-Name** a pak zvolte Enforced
23. Na **win7-domain** ověřte, že nastavení zásad z GPO objektu **Site GPO** přepsalo konfliktní nastavení zásad z GPO objektu **Domain GPO**
    a. Spusťte příkaz **gpupdate /force**
    b. Oěřte, že v Control Panel chybí možnosti Fonts, Device Manager, Backup and Restore, Administrative Tools a v nabídce Start chybí Games
    ➢ Vynucené (*enforced*) GPO objekty mají opačnou prioritu aplikace, nejprve vynucené objekty připojené k organizačním jednotkám, pak k doménám a až nakonec k místům

Lab L03 – Výsledné sady zásad

[Na cvičeních]

Studentské úkoly

- Na všech stanicích zakažte *Internal* síťové rozhraní (**LAN1**)

Lab S01 – Loopback zpracování GPO objektů [Povinné]

Cíl cvičení

Nastavit *Loopback* zpracování GPO objektů a ověřit jeho funkčnost

Potřebné virtuální stroje

Windows 7 AD, Enterprise 32bit (**win7-domain**)
Windows 2008R2 AD, Enterprise 64bit (**win2008r2-dc**)

Další prerekvizity

Účet počítače **win7-domain** v organizační jednotce **brnopcs** v doméně **testing.local,** účet uživatele **homer** v organizační jednotce **brno** v doméně **testing.local**, GPO objekt **Brno GPO** připojený k organizační jednotce **brno** v doméně **testing.local**

1. Otevřete **GPME** (*Group Policy Management Editor*)
   a. Start → (All Programs) → Administrative Tools → **Group Policy Management**
2. Odeberte v GPO objektu **Brno GPO** odkazy na adresáře s obrázky a hudbou z nabídky Start
   a. Klikněte pravým na GPO objekt **Brno GPO** a zvolte Edit…
   b. Vyberte uzel User Configuration \ Policies \ Administrative Templates \ Start Menu and Taskbar
   c. Klikněte pravým zásadu na Remove Pictures icon from Start Menu a zvolte Edit
   d. Přepněte nastavení na Enabled a potvrďte OK
   e. Klikněte pravým zásadu na Remove Music icon from Start Menu a zvolte Edit
   f. Přepněte nastavení na Enabled a potvrďte OK
3. Vytvořte nový GPO objekt **BrnoPCs GPO** a rovnou ho připojte k organizační jednotce **brnopcs**
   a. Klikněte pravým na organizační jednotku **brnopcs** a vyberte Create a GPO in this domain, and Link it here…
   b. Jako název (Name) zvolte **BrnoPCs GPO** a u Source Starter GPO ponechte **(none)**
   c. Potvrďte OK
4. V GPO objektu **BrnoPCs GPO** odeberte odkaz na adresář s dokumenty z nabídky Start a zároveň vynuťte zobrazení odkazu na adresář s obrázky v nabídce Start
   a. Klikněte pravým na GPO objekt **BrnoPCs GPO** a zvolte Edit…
   b. Vyberte uzel User Configuration \ Policies \ Administrative Templates \ Start Menu and Taskbar
   c. Klikněte pravým zásadu na Remove Documents icon from Start Menu a zvolte Edit
   d. Přepněte nastavení na Enabled a potvrďte OK
   e. Klikněte pravým zásadu na Remove Pictures icon from Start Menu a zvolte Edit
   f. Přepněte nastavení na Disabled a potvrďte OK
5. Přihlaste se na **win7-domain** jako uživatel **homer** a ověřte, že v nabídce Start chybí odkazy na adresáře s obrázky (Pictures) a hudbou (Music)
   - Na uživatele jsou aplikována pouze nastavení z těch GPO objektů, v jejichž rozsahu daný uživatel leží, tedy nastavení z **BrnoPCs GPO** nejsou aplikována
6. Povolte *Loopback* zpracování GPO objektů v režimu nahrazení
   a. Klikněte pravým na GPO objekt **BrnoPCs GPO** a zvolte Edit…

b. Vyberte uzel Computer Configuration \ Policies \ Administrative Templates \ System \ Group Policy
c. Klikněte pravým zásadu na User Group Policy loopback processing mode a zvolte Edit
d. Přepněte nastavení na Enabled a režim (Options / Mode) ponechte **Replace**
e. Potvrďte OK

7. Na **win7-domain** ověřte, že došlo k aplikaci pouze nastavení zásad z **BrnoPCs GPO** objektu
   a. Spusťte příkaz **gpupdate /target:computer /force**
   b. Spusťte příkaz **gpupdate /force**
   c. Ověřte, že v nabídce Start chybí Documents, ale Pictures i Music jsou přítomny

   ➢ V režimu nahrazení (*replace*) jsou aplikována uživatelská nastavení pouze z GPO objektů, které mají ve svém rozsahu počítač, kde je daný uživatel přihlášen

8. Změňte režim *Loopback* zpracování GPO objektů na režim slučování
   a. Klikněte pravým na GPO objekt **BrnoPCs GPO** a zvolte Edit…
   b. Vyberte uzel Computer Configuration \ Policies \ Administrative Templates \ System \ Group Policy
   c. Klikněte pravým zásadu na User Group Policy loopback processing mode a zvolte Edit
   d. U Mode pod Options vyberte **Merge** a potvrďte OK

9. Na **win7-domain** ověřte, že došlo k aplikaci jak nastavení zásad z GPO objektu **Brno GPO**, tak také z GPO objektu **BrnoPCs GPO**
   a. Spusťte příkaz **gpupdate /target:computer /force**
   b. Spusťte příkaz **gpupdate /force**
   c. Ověřte, že v nabídce Start chybí Documents i Music, ale Pictures jsou přítomny

   ➢ V režimu sloučení (*merge*) jsou nejprve aplikována uživatelská nastavení z GPO objektů, které mají ve svém rozsahu daného uživatele, a poté dále nastavení z GPO objektů, jenž mají ve svém rozsahu počítač, kde je daný uživatel přihlášen

Lab S02 – Bezpečnostní filtry

[Povinné]

Cíl cvičení

Definovat rozsah GPO objektu na základě příslušnosti uživatelů do skupin

Potřebné virtuální stroje

Windows 7 AD, Enterprise 32bit (**win7-domain**)
Windows 2008R2 AD, Enterprise 64bit (**win2008r2-dc**)

Další prerekvizity

Účet uživatele **student** v kontejneru Users v doméně **testing.local**, který nepatří do skupiny **Simpsons**, účet uživatele **homer** v kontejneru Users v doméně **testing.local**, jenž náleží do skupiny **Simpsons**

1. Otevřete **GPME** (*Group Policy Management Editor*)
   a. Start → (All Programs) → Administrative Tools → **Group Policy Management**
2. Vytvořte nový GPO objekt **Simpsons GPO** a rovnou ho připojte k doméně **testing.local**
   a. Klikněte pravým na doménu **testing.local** a zvolte Create a GPO in this domain, and Link it here…
   b. Jako název (Name) zvolte **Simpsons GPO** a u Source Starter GPO ponechte **(none)**
   c. Potvrďte OK
3. Odeberte v GPO objektu **Simpsons GPO** odkaz na výchozí programy z nabídky Start
   a. Klikněte pravým na GPO objekt **Simpsons GPO** a zvolte Edit…

   b. Vyberte uzel User Configuration \ Policies \ Administrative Templates \ Start Menu and Taskbar
   c. Klikněte pravým zásadu na Remove Default Programs link from the Start Menu. a zvolte Edit
   d. Přepněte nastavení na Enabled a potvrďte OK

4. Nastavte rozsah GPO objektu **Simpsons GPO** pouze na uživatele skupiny **Simpsons**
   a. Vyberte GPO objekt **Simpsons GPO**
   b. Na záložce Scope v části Security Filtering zvolte Add…
   c. Do Enter the object name to select zadejte **Simpsons** a ověřte pomocí Check Names
   d. Potvrďte OK
   e. Vyberte skupinu Authenticated Users, zvolte Remove a potvrďte OK
5. Vytvořte nový GPO objekt **NonSimpsons GPO** podle postupu z **bodu 2**
6. Odeberte v GPO objektu **NonSimpsons GPO** nápovědu z nabídky Start
   a. Klikněte pravým na GPO objekt **NonSimpsons GPO** a zvolte Edit…
   b. Vyberte uzel User Configuration \ Policies \ Administrative Templates \ Start Menu and Taskbar
   c. Klikněte pravým zásadu na Remove Help menu from Start Menu a zvolte Edit
   d. Přepněte nastavení na Enabled a potvrďte OK
7. Nastavte rozsah GPO objektu **NonSimpsons GPO** na všechny uživatele, jenž nejsou členy skupiny **Simpsons**
   a. Vyberte GPO objekt **NonSimpsons GPO**
   b. Na záložce Delegation zvolte Advanced…
   c. Na záložce Security pod Group or user names zvolte Add…
   d. Do Enter the object name to select zadejte **Simpsons** a ověřte pomocí Check Names
   e. Potvrďte OK
   f. Odškrtněte Allow u Read a zaškrtněte Deny u Apply group policy
   g. Potvrďte OK a následně zvolte Yes
8. Přihlaste se na **win7-domain** jako uživatel **homer** a ověřte, že v nabídce Start chybí Default Programs
9. Přihlaste se na **win7-domain** jako uživatel **student** a ověřte, že v nabídce Start chybí Help and Support

Lab S03 – Publikace aplikací pomocí GPO objektů

[Volitelné]

Cíl cvičení

Zpřístupnit aplikaci uživatelům v podnikové síti pro případnou instalaci

Potřebné virtuální stroje

Windows 7 AD, Enterprise 32bit (**win7-domain**)
Windows 2008R2 AD, Enterprise 64bit (**win2008r2-dc**)

Další prerekvizity

Účet uživatele **homer** v organizační jednotce **brno** v doméně **testing.local**, GPO objekt **Brno GPO** připojený k organizační jednotce **brno** v doméně **testing.local**, sdílený adresář **share** na **win2008r2-dc** obsahující soubor **7z465.msi** (**7z465.msi** je k dispozici lokálně na serveru **yetti** v adresáři **\\yetti.nepal.aps\data\kurzy pro FIT a FEKT\IW2\cv4**)

1. Otevřete **GPME** (*Group Policy Management Editor*)
   a. Start → (All Programs) → Administrative Tools → **Group Policy Management**
2. V GPO objektu **Brno GPO** publikujte (*publish*) aplikaci uživatelům

a. Klikněte pravým na GPO objekt **Brno GPO** a zvolte Edit…
b. Vyberte uzel User Configuration \ Policies \ Software Settings
c. Klikněte pravým na Software Instalation a zvolte New → Package…
d. Vyberte instalační soubor **\\win2008r2-dc\share\7z465.msi**
   - Zadaná cesta musí být síťovou cestou k instalačnímu souboru aplikace, jinak nebude pro klienta možné lokalizovat na síti tento instalační soubor a instalace selže
e. U Select deployment method zvolte **Advanced**
f. Na záložce Deployment zvolte u Deployment type typ **Published** a níže pod Deployment options zaškrtněte nastavení **Uninstall this application when it falls out of the scope of management**
g. Potvrďte OK

3. Na **win7-domain** se přihlaste jako uživatel **homer** a nainstalujte aplikaci
   a. Otevřete Programs and Features
      1. Start → Control Panel → Programs and Features
   b. V panelu vlevo zvolte Install a program from the network
   c. V seznamu vyberte **7-Zip 4.65** a zvolte Install
   d. Ponechte výchozí nastavení, přijměte licenční podmínky a nainstalujte aplikaci
   e. Spusťte **7-Zip File Manager** a ověřte, že aplikace byla opravdu nainstalována
4. Přesuňte uživatele **homer** do kontejneru Users
5. Znova se přihlaste na **win7-domain** jako uživatel **homer** a ověřte, že aplikace byla odstraněna
   - V případě, že se změny neprojeví, spusťte **gpupdate /force**, bude vyžadováno odhlášení uživatele, které potvrďte pomocí **Y** a přihlaste se zpět

Lab S04 – Instalace aplikací pomocí GPO objektů a WMI filtrů [Volitelné]

Cíl cvičení

Centrálně nasadit 32-bit a 64-bit verze aplikace pomocí GPO objektů a WMI filtrů

Potřebné virtuální stroje

Windows 7 AD, Enterprise 32bit (**win7-domain**)
Windows 2008R2 AD, Enterprise 64bit (**win2008r2-dc**)
Windows 2008R2 AD Member, Enterprise 64bit (**win2008r2-mbr**)

Další prerekvizity

Účet uživatele **homer** v doméně **testing.local**, sdílený adresář **share** na **win2008r2-dc** obsahující soubory **7z465.msi** a **7z465-x64.msi** (**7z465.msi** i **7z465-x64.msi** jsou k dispozici lokálně na serveru **yetti** v adresáři **\\yetti.nepal.aps\data\kurzy pro FIT a FEKT\IW2\cv4**)

1. Otevřete **GPME** (*Group Policy Management Editor*)
   a. Start → (All Programs) → Administrative Tools → **Group Policy Management**
2. Vytvořte nový GPO objekt **32bit Apps GPO** a rovnou ho připojte k doméně **testing.local**
   a. Klikněte pravým na doménu **testing.local** a zvolte Create a GPO in this domain, and Link it here…
   b. Jako název (Name) zvolte **32bit Apps GPO** a u Source Starter GPO ponechte **(none)**
   c. Potvrďte OK
3. V GPO objektu **32bit Apps GPO** přiřaďte (*assign*) aplikaci počítačům
   a. Klikněte pravým na GPO objekt **32bit Apps GPO** a zvolte Edit…
   b. Vyberte uzel Computer Configuration \ Policies \ Software Settings
   c. Klikněte pravým na Software Instalation a zvolte New → Package…

d. Vyberte instalační soubor **\\win2008r2-dc\share\7z465.msi**

   ➢ Zadaná cesta musí být síťovou cestou k instalačnímu souboru aplikace, jinak nebude pro klienta možné lokalizovat na síti tento instalační soubor a instalace selže

e. U Select deployment method zvolte **Advanced**
f. Na záložce Deployment ponechte u Deployment type typ **Assigned** a pod Deployment options zaškrtněte nastavení **Uninstall this application when it falls out of the scope of management**
g. Potvrďte OK

4. Vytvořte nový WMI filtr **32bit OS**, jenž vybere pouze počítače s 32-bit operačním systémem
   a. Klikněte pravým na kontejner WMI Filters a zvolte New…
   b. Jako název (Name) zvolte **32bit OS** a u Queries zvolte Add
   c. Jmenný prostor (Namespace) ponechte **root\CIMv2** a do Query zadejte **SELECT * FROM Win32_OperatingSystem WHERE OSArchitecture="32-bit"**
   d. Vložte dotaz pomocí OK
   e. Potvrďte vytvoření filtru pomocí Save
5. Omezte rozsah GPO objektu **32bit Apps GPO** pouze na 32-bit operační systémy
   a. Vyberte GPO objekt **32bit Apps GPO**
   b. Na záložce Scope v části WMI filtering u This GPO is linked to the following WMI filter vyberte v seznamu **32bit OS** a potvrďte Yes
6. Opakujte **body 2 - 5** pro GPO objekt **64bit Apps GPO**, instalační soubor **7z465-x64.msi** a WMI filtr **SELECT * FROM Win32_OperatingSystem WHERE OSArchitecture="64-bit"**
7. Restartujte počítače **win7-domain** a **win2008r2-mbr**
   ➢ Nastavení počítače se aktualizují při startu počítače, nestačí se pouze odhlásit
8. Přihlaste se na **win7-domain**, resp. **win2008r2-mbr**, jako uživatel **homer** a ověřte, že byly nainstalovány aplikace **7-Zip 4.65**, resp. **7-Zip 4.65 (x64 edition)**
   a. Otevřete Programs and Features
      1. Start → Control Panel → Programs and Features
   b. Zkontrolujte, že je v seznamu přítomen **7-Zip 4.65** resp. **7-Zip 4.65 (x64 edition)**
   ➢ V případě, že se změny neprojeví, spusťte **gpupdate /force**, bude vyžadován restart počítače, který potvrďte pomocí **Y** a po naběhnutí počítače se opět přihlaste