Zásady skupiny – část 1

[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, která 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 připojen 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, jež 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 moduly, 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, jež 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 ně-jaký 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*). Ty jsou uloženy přímo na cílovém počítači. Druhým typem jsou doménové **GPO** objekty (*Domain-Based GPOs*) nacházející se 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 novějších systémů, počínaje Windows Vista a Windows Server 2008, 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**. Sem patří **GPO** objekty pro skupinu administrátorů (*Administrators*) a pro všechny ostatní uživatele (*Non-Administrators*). V těchto **GPO** objektech lze definovat pouze uživatelská nastavení aplikovatelná jen na uživatele patřící resp. nepatřící 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 aplikovaná 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** aplikovaných později, přepíší 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 a Windows Server 2008 mají možnost definovat více lokálních **GPO** objektů (tzv. *multiple local GPOs*).
   b. **GPO objekty připojené k místu** (*Site GPOs*). Všechny **GPO** objekty připojené 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 z dříve aplikovaných **GPO** objektů.
   c. **GPO objekty připojené k doméně** (*domain GPOs*). Stejně jako u *site* **GPO** objektů, i zde jsou přidány jednotlivé **GPO** objekty, jež 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, používaných málokdy) a vynutí tedy svá 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*) kontejneru, 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, jež 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 aplikovaná 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 zahrnující jej 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 zahrnujících 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 ovlivňujících 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.

Studentské úkoly

- Pro přístup na server **file** (a jiné) přes síťové rozhraní *Default switch* je nutné použít jeho plně kvalifikované doménové jméno **file.nepal.local**
- Přístupové údaje na server **file**: **nepal\hstudent** heslo: **aaa**
- Rozsah IP adres přidělených z *Default switch* se může od níže uvedeného rozsahu lišit.

Lab S00 – konfigurace virtuálních stanic

[Provést]

Připojte sítové adaptéry stanic k následujícím virtuálním přepínačům:

Adaptér (MAC suffix)	LAN1 (-01)	LAN2 (-02)	LAN3 (-03)	LAN4 (-04)
w10-domain	Nepřipojeno	Private1	Nepřipojeno	Nepřipojeno
w2016-dc	Nepřipojeno	Private1	Nepřipojeno	Nepřipojeno

- v případech, kdy je potřeba přistupovat na externí síť, připojte adaptér **LAN1** k přepínači *Default switch*.

Lab X01 – GPME (Group Policy Management Editor)

[Projít]

Cíl cvičení

Seznámení s GPME konzolí

Potřebné virtuální stroje

w2016-dc

Otevřete **GPME** (*Group Policy Management Editor*, Start → Windows Administrative Tools → **Group Policy Management**) konzoli a projděte ji.

Všimněte si samostatných uzlů pro místa (*site*) a domény. V případě více míst nebo domén se může stát, že zde nebudou zobrazeny všechny – potřebné místo/doménu pak lze zobrazit pomocí kontextové nabídky nad uzlem Domain \ Show Domains… resp. nad uzem Sites \ Show Sites….

U záložky Linked Group Policy Objects si všimněte hodnoty *link order* určující prioritu nalinkovaných a že nižší číslo znamená vyšší prioritu.

Na záložce Group Policy Inheritance naleznete informace o dědičnosti. Pozor, **GPO** objekty připojené k místu (*site*) na této záložce u domény/OU neuvidíte.

Zopakujte si rozdíl mezi **GPO** objekty a odkazy.

Projděte jednotlivé záložky u **GPO** objektu a odkazů.

Lab X02 – 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

w2016-dc
w10-domain

Další prerekvizity

Účet počítače **w10-domain** v organizační jednotce **brnopcs** v doméně **testing.local**, účet uživatele **homer** v organizační jednotce **brno** v doméně **testing.local**

1. Otevřete **GPME** (*Group Policy Management Editor*)
   a. Start → Windows 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 na zásadu 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**
   a. Pokud se pod kontejnerem Sites nenachází místo **Default-First-Site-Name**
      - klikněte pravým na kontejner Sites a zvolte Show Sites…, zaškrtněte **Default-First-Site-Name** a potvrďte OK
   b. Klikněte pravým tlačítkem myši na místo **Default-First-Site-Name** a zvolte Link an Existing GPO…
   c. Pod Group Policy objects vyberte **Site GPO** a potvrďte OK
5. Přihlaste se na **w10-domain** jako uživatel **homer** a ověřte, že nastavení byla aplikována
   a. Ověřte, že v Control Panel chybí možnosti Fonts, Device Manager, Backup and Restore a Administrative Tools
      - Tip: přepněte zobrazení na velké ikony (View by: Large icons)
      - Pokud jsou zobrazené, spusťte **gpupdate /force**, zavřete a znova otevřete Control Panel

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** a **Microsoft.BackupAndRestore**, podle postupu z **bodu 3**
8. Na **w10-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 **w10-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 **w10-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. V GPO objektu **Domain GPO** odeberte uživatelům hodiny z hlavního panelu (taskbaru)
    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 na zásadu Remove Clock from system notification area a zvolte Edit
    d. Přepněte nastavení na Enabled a potvrďte OK

17. Na **w10-domain** ověřte, že došlo k aplikaci nastavení zásad z GPO objektů **Brno Priority GPO** a **Domain GPO**
    a. Spusťte příkaz **gpupdate /force**
    b. Odhlaste a znova přihlaste uživatele **homer** (aby se projevily změny v taskbaru)
    c. Ověřte, že v Control Panel chybí pouze Fonts a na hlavním panelu chybí hodiny
        - Jelikož nastavení zásady, jenž odebírá hodiny, není definováno v GPO objektech připojených k organizační jednotce **brno**, dojde ke zdědění nastavení této zásady z GPO objektů výše (GPO objektů aplikovaných dříve), v tomto případě z GPO objektu **Domain GPO**
18. Zakažte dědičnost na organizační jednotce **brno**
    a. Klikněte pravým na organizační jednotku **brno** a zvolte Block Inheritance
19. Na **w10-domain** ověřte, že nedošlo k aplikaci nastavení zásad z GPO objektu **Domain GPO**
    a. Spusťte příkaz **gpupdate /force**
    b. Odhlaste a znova přihlaste uživatele **homer** (aby se projevily změny v taskbaru)
    c. Ověřte, že jsou hodiny opět na svém místě
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 **w10-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. Odhlaste a znova přihlaste uživatele **homer** (aby se projevily změny v taskbaru)
    c. Ověřte, že pouze Administrative Tools jsou přítomny v Control Panel a na hlavním panelu chybí hodiny
        - Vynucené (*enforced*) GPO objekty jsou aplikovány vždy, i v případě blokování dědičnosti, navíc má tento typ GPO objektů vyšší prioritu než standardní GPO objekty, tyto objekty jsou tedy aplikovány až po aplikaci všech standardních GPO objektů, zde tedy nastavení zásad z GPO objektu **Domain GPO** přepíší 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 **w10-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. Odhlaste a znova přihlaste uživatele **homer** (aby se projevily změny v taskbaru)
    c. Ověřte, že v Control Panel chybí možnosti Fonts, Device Manager, Backup and Restore, Administrative Tools a na hlavním panelu chybí hodiny
        - Vynucené (*enforced*) GPO objekty mají opačnou prioritu aplikace, nejprve vynucené objekty připojené k organizačním jednotkám, pak k doménám a až nakonec k místům

Lab X03 – Výsledné sady zásad

[Projít]

Cíl cvičení

Seznámení s nástroji Group Policy Modeling a Group Policy Results.

Potřebné virtuální stroje

w2016-dc
w10-domain

Prozkoumejte nástroje Group Policy Modeling a Group Policy Results v **GPME**.
V čem spočívá jejich rozdíl?
Pomocí Group Policy Modeling nasimulujte přesun uživatele **homer** do kontejneru Users a ukažte, že na něj po přesunu už nebudou aplikovány GPO objekty **Brno GPO** a **Brno Priority GPO**.
Na klientské stanici spusťte nástroj **gpresult** (obdoba Group Policy Results pro příkazový řádek) **gpresult /user homer /h homer.html** a prozkoumejte vygenerovaný report.

Lab S01 – Loopback zpracování GPO objektů

[Povinné]

Cíl cvičení

Nastavit *Loopback* zpracování GPO objektů a ověřit jeho funkčnost

Potřebné virtuální stroje

w2016-dc
w10-domain

Další prerekvizity

Účet počítače **w10-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 → Administrative Tools → **Group Policy Management**
2. Pomocí GPO objektu **Brno GPO** zakažte změnu tapety a barevného schématu
   a. Klikněte pravým na GPO objekt **Brno GPO** a zvolte Edit…
   b. Vyberte uzel User Configuration \ Policies \ Administrative Templates \ Control Panel \ Personalization
   c. Klikněte pravým na zásadu Prevent changing desktop background a zvolte Edit
   d. Přepněte nastavení na Enabled a potvrďte OK
   e. Klikněte pravým na zásadu Prevent changing color and appearance 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** zakažte změnu zvuků a zároveň vynuťte povolení změny barevného schématu
   a. Klikněte pravým na GPO objekt **BrnoPCs GPO** a zvolte Edit…
   b. Vyberte uzel User Configuration \ Policies \ Administrative Templates \ Control Panel \ Personalization

   c. Klikněte pravým na zásadu Prevent changing sounds a zvolte Edit
   d. Přepněte nastavení na Enabled a potvrďte OK
   e. Klikněte pravým na zásadu Prevent changing color and appearance a zvolte Edit
   f. Přepněte nastavení na Disabled a potvrďte OK
5. Přihlaste se na **w10-domain** jako uživatel **homer** a ověřte, že nelze změnit tapetu (Settings – Personalization – Background) ani barevné schéma (Settings – Personalization – Colors)
   - 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 na zásadu Configure 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 **w10-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 nelze změnit zvuky (Settings – Personalization – Themes – Sounds), ale změnit tapetu (Settings – Personalization – Background) i barevné schéma (Settings – Personalization – Colors) lze.
      - 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 na zásadu User Group Policy loopback processing mode a zvolte Edit
   d. U Mode pod Options vyberte **Merge** a potvrďte OK
9. Na **w10-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 nelze změnit zvuky (Settings – Personalization – Themes – Sounds) ani tapetu (Settings – Personalization – Background), ale změnit barevné schéma (Settings – Personalization – Colors) lze.
      - 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, které mají ve svém rozsahu počítač, kde je daný uživatel přihlášen