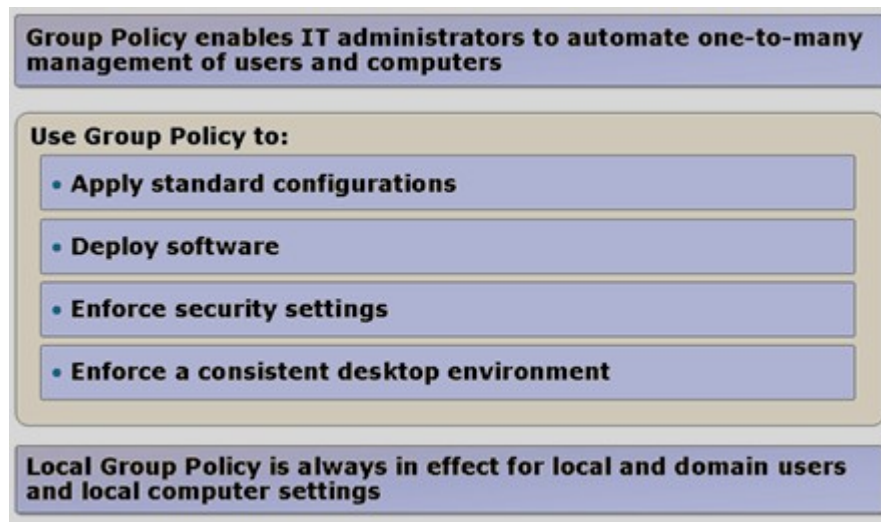


Skupinová politika / Zásady skupiny (Group Policy)

Skupiny zásad (Group Policy) je nástroj pro hromadnou správu oprávnění a nastavení aplikovaných jak na celý počítač, tak na přihlášeného uživatele. Ve skupinách zásad je možné vytvářet kolekce nastavení, kterým říkáme Group Policy Object GPO, které dokáží měnit konkrétní parametry chování počítače nebo uživatele. Samotné nastavení GPO se pak „linkuje“ na jednotlivé organizační jednotku OU v AD, čímž zajistíte aplikování nastavení jen na vybrané počítače nebo uživatele. Tímto způsobem tedy můžeme spravovat potenciálně tisíce počítačů nebo uživatelů změnou jednoho GPO.



Obr. – souhrn vlastností skupinových politik

Group Policy

nástroj pro hromadnou správu oprávnění a nastavení aplikovaných jak na celý počítač, tak na přihlášeného uživatele.

Používá se pro:

- aplikování firemních standardů (skrytí ovládacích panelů, síťové tiskárny, spuštění skriptů)
- aplikování zabezpečení (změna oprávnění na určitých složkách, složitost hesla, skupiny s možností se lokálně přihlásit)
- skripty – určí se, které skripty se spustí při přihlášení, odhlášení, zapnutí, vypnutí počítače
- přesměrování složky – umožňuje umístit složky jako dokumenty či profil na server popř. složky jednotlivých aplikací
- hromadná instalace aplikací (Java, Adobe Reader, Flash atd.)

Group Policy Object „GPO“ neboli Objekt zásad skupiny

Množina nastavení zásad se nazývá objekt GPO:

- může obsahovat několika zásad (nastavení) najednou
- je komponentou globální politiky

- dělí se na nastavení pro počítač tak na nastavení pro uživatele
- linkuje se na organizační jednotky OU v AD
- jeden GPO může být linkován hned na několik OU

Policy „Politika“

Politiky dělíme na Lokální a Doménové.

Lokální:

každý počítač od Windows 2000 má lokální politiky (local Group Policy), které ovlivňují lokální počítač a přihlášené uživatele. Pokud počítač není připojen do domény, tak právě lokální politiky jsou jako jediné použity.

Př. Pokud vytvoříte uživatele a nastavíte mu omezené oprávnění, chování tohoto uživatele vymezuje právě lokální politika.

Lokální politiky jsou uloženy ve skrytém adresáři **%systemroot%\system32\GroupPolicy**

Doménové:

doménové politiky lze použít výhradně u počítačů a uživatelů, jenž jsou členy nějaké domény. Existují dvě základní doménové politiky, které jsou vytvořeny již při instalaci AD

Politiky	Popis
Default Domain Policy	Tato politika je spojena s kontejnerem domény a ovlivňuje všechny objekty v doméně.
Default Domain Controller Policy	Tato politika je spojena s kontejnerem doménového kontroléru DC a ovlivňuje všechny DC v doméně.

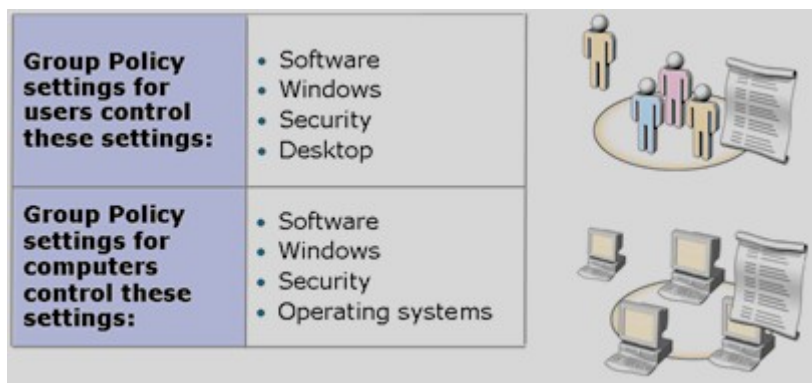
Pořadí implementace

Zásady skupiny jsou zpracovány napříč doménami v následujícím pořadí:

- Místní objekt GPO.
- Objekty GPO propojené s lokalitou, v pořadí určeném správcem. Viz. složka Propojené objekty zásad skupiny (Linked Group Policy Objects v konzole Správa zásad skupiny (GPMC – Group Policy Management Console) Objekt GPO s nejnižším pořadím propojení se zpracuje nakonec, a proto má nejvyšší prioritu.
- Objekty GPO domény v pořadí určené správcem. Objekt GPO s nejnižším pořadím propojení se zpracuje nakonec, a proto má nejvyšší prioritu.
- Objekty GPO organizační jednotky (OU) v pořadí od největší po nejmenší OU. Objekt GPO s nejnižším pořadím propojení se zpracuje nakonec, a proto má nejvyšší prioritu.

V tomto pořadí vyhrává poslední zapsané nastavení. Pokud se více GPO pokusí o protichůdná nastavení, vyhraje objekt s největší prioritou.

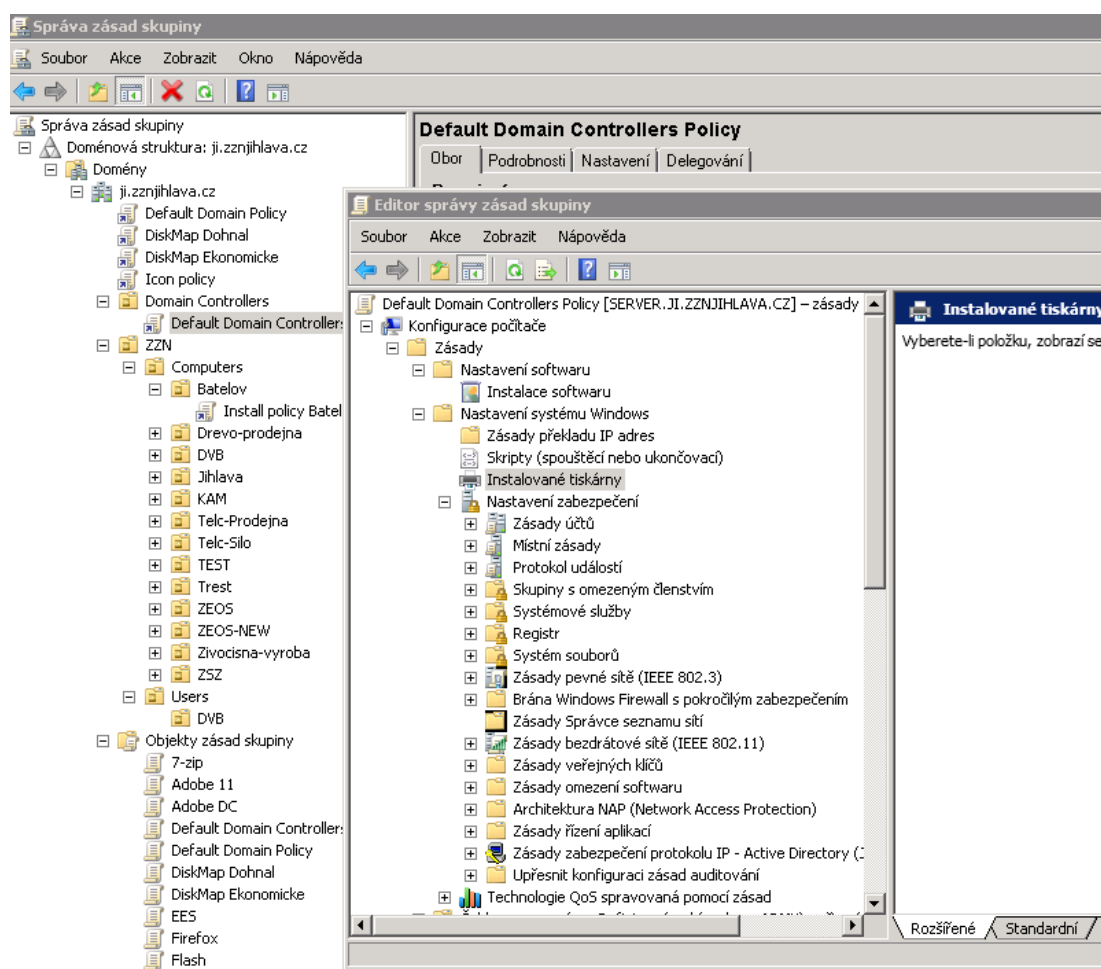
Struktura GPO



Obr. – struktura GPO

Group Policy obsahuje tisíce různých nastavení ovlivňující chování jak počítače, tak přihlášeného uživatele. Není bohužel možné použít všechny nastavení na všechny operační systémy najednou (2000, XP, Vista, 7, 8, 10), jelikož s každým novým operačním systémem přichází stovky nových nastavení, které lze však použít pouze pro daný systém. Pokud byste tedy použili nastavení určené pro Windows 7 na Windows 10, bude je jednoduše ignorovat.

Doporučujeme číst popisy všech nastavení, kde se uvádí, pro jaký systém bude nastavení aplikováno.



Obr. – možnosti GPO editoru

Rozdělení GPO

globální politiky se dělí na dvě části, a to konfigurace počítače (**Computer configuration**) a konfigurace uživatele (**User configuration**)

Group Policy area	Co to dělá?
Computer configuration	mění registry v: HKEY_Local_Machine
User configuration	mění registry v: HKEY_Current_User

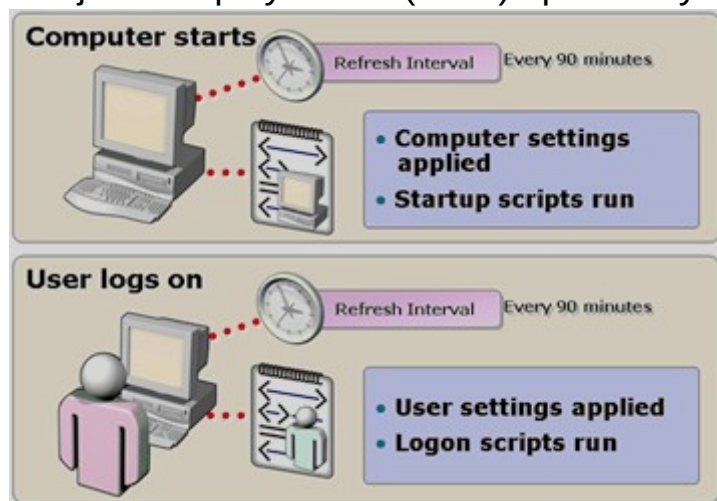
Při vytváření GPO máte možnost jednu z částí (Users/Computers) vypnout a tak snížit celkovou velikost vytvořené GPO

každá z těchto částí se dělí na další tři sekce:

- nastavení softwaru (**Software settings**)
- nastavení systému Windows (**Windows settings**)
- šablony pro správu (**Administrative templates**)

Section	Description
Software settings	Instalace softwaru. Pokud je definován v části konfigurace počítače, bude nainstalován ještě před přihlášením, pokud je definován v části konfigurace uživatele, bude nainstalován až po přihlášení konkrétního uživatele
Windows settings	Obsahují skripty (při přihlášení, při odhlášení) a nastavení zabezpečení pro uživatele i počítače a Internet Explorer ®
Administrative templates	Obsahují stovky nastavení registru pro ovládání různých aspektů uživatele nebo počítačového prostředí.

Jak jsou skupiny zásad (GPO) aplikovány



Obr. - Aplikace politik

Aplikování Skupin zásad je na dvou úrovních a to zvlášť pro konfigurace počítače a zvlášť pro konfigurace uživatele. Oboje zajišťuje služba **Group Policy Client**.

Aplikování konfigurace počítače

- při startu počítače a jinak každých 90 minut
- aplikují se Startup scripty

aplikování konfigurace počítače každých 90min. je až od Windows Vista. Windows XP se aplikovaly pouze při spuštění počítače.

Aplikování konfigurace uživatele

- při zalogování uživatele a jinak každých 90 minut
- aplikují se Logon scripty

Pomocí příkazu **gpupdate /force** lze znovu aplikovat všechny politiky.

Jak se GPO zpracovává při spuštění počítače:

1. Počítač najde DC a přihlásí se k němu, stejně jako uživatel. Pro úspěšné přihlášení musí být povolené následující porty: UDP 53 (DNS), UDP a TCP 389 (LDAP), TCP 135 (RPC Portmapper), UDP 88 (Kerberos)
2. Počítač pomocí ICMP paketů zjistí, zda je na pomalé lince (Slow Link Detection)
3. Pomocí LDAPu zjistí, jaké GPO jsou navázány OU, doménu, síť. Z těchto odpovědí si vytvoří seznam všech GPO, které jsou na něj aplikovány.
4. Pomocí LDAPu pošle počítač otázku na seznam filtrů na všechny GPO, které našel + si požádá o atributy jako je cesta ke GPT (Group Policy Templates), číslo verze GPC (Group Policy Configuration), gpCMachineExtensionNames a gpCUserExtensionnames atribut.
5. Počítač pomocí SMB (port TCP 445) se připojí k SYSVOLu a přečte si GPT.INI pro každé GPO, které se na něj aplikuje.
6. Group Policy process začne porovnávat verzi GPO s verzí GPO, kterou má lokálně uloženou v (HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\History)
7. Pokud se verze GPO nezměnila, je přeskočena. V GPO se dá nastavit, aby se toto nedělo a politiky se aplikovaly pokaždé, i když nenastala změna. Toto se dá vynutit i přes CMD pomocí příkazu *gpupdate /force*
8. CSE (Client Side Extension) zjistí, zda má dostatečná práva na všechny GPO, které se mají aplikovat. Pokud ne, dané GPO je vyhozeno ze seznamu. Pokud je na GPO nastaveno Enforced (vynucené) je v tomto kroku přeneseno na konec seznamu. To znamená, že nastavení z tohoto GPO vždycky vyhrají, pokud nastane nějaký konflikt.
9. CSE začne zpracovávat jednotlivá GPO.
10. Po každém zpracování GPO CSE zaloguje RSoP (Result of Policy) přes WMI do CIMOM (Common information Management Object Model) databáze na počítači, kde se zpracují politiky.
11. Po přihlášení se celý proces opakuje s nastavením aplikovaných na uživatele.

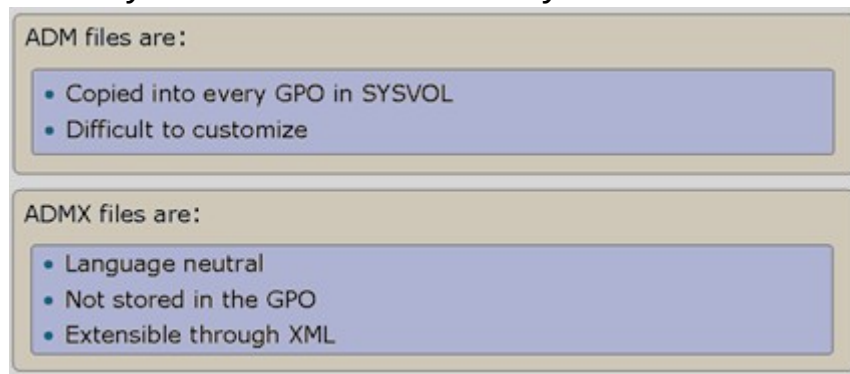
Výjimky aplikování politik

Slow links	<ul style="list-style-type: none"> • 500 kilobits per second (kbps) by default • Certain client side extensions are not processed • Prior to Windows Vista, ICMP is used to detect a slow link • Windows Vista uses Network Location Awareness
Cached credentials	<ul style="list-style-type: none"> • Windows XP and Windows Vista use cached credential for faster logons • Many GPO settings take two logons to take effect
Additional exceptions:	
<ul style="list-style-type: none"> • Remote access connections • Moving a user or computer object in AD DS 	

Globální politiky dokáží detekovat rychlost linky a v případě pomalé linky (méně než 500 kb/s) a několika dalších faktorů, nemusí být některé z politik aplikovány.

Procesy	Aplikování při zjištění pomalé linky	Může se dát změnit?
Zpracování zásad registru	Ano	Ne
Nastavení Internet Explorer	Ne	Ano
Politiky instalování SW	Ne	Ano
Politiky přesměrování adresy	Ne	Ano
Scripty	Ne	Ano
Politiky zabezpečení	Ano	Ne
Internet Protocol Security (IPSec)	Ne	Ano
Politiky bezdrátových sítí	Ne	Ano
EFS Recovery	Ano	Ano
Politiky diskových kvót	Ne	Ano

Šablony a ADM a ADMX soubory



Z důvodů rozsáhlosti nastavení a možnosti grafického zobrazení v GPM Skupinových zásad vznikly šablony, které v sobě zahrnují již přednastavené vlastnosti GPO dle použití, nebo slouží k tváření nových GPO. Od Windows Vista a Serveru 2008 zde máme již 2 formáty. Staré ADM a nové ADMX.

ADM

Ve výchozím nastavení při vytváření nových GPO jsou použity vždy dva ADM soubory, a to: Inetres.adm (nastavení aplikace Internet Explorer), a System.adm (nastavení operačního systému Windows). Při vytvoření politiky jsou pak tyto soubory překopírovány z umístění **%SystemRoot%\Inf**, do příslušné složky GPO v SYSVOL. Každý nový objekt GPO spotřebuje asi 3,5 MB (MB) volného místa ve složce SYSVOL. Ve velkých organizacích s mnoha GPO může toto vést k významnému zatížení replikace složky SYSVOL.

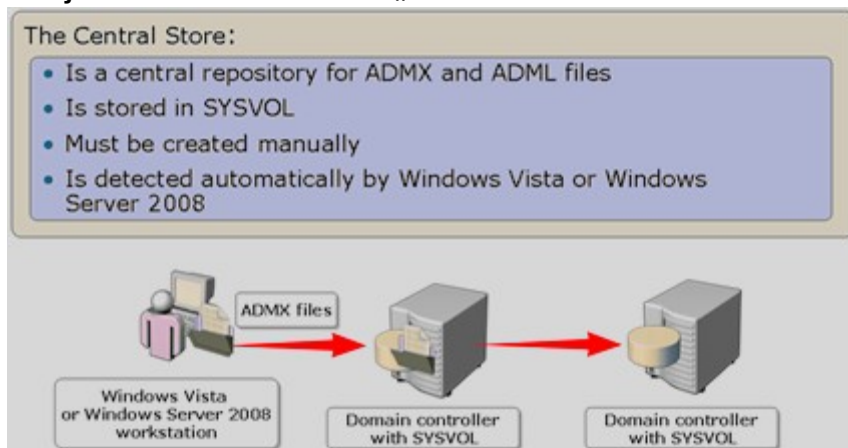
ADMX

Windows Vista a Windows Server 2008 zavádí nový formát pro zobrazení zásad. Zásady jsou definovány pomocí standardů XML formát známý jako soubory ADMX. Tyto nové soubory nahrazují soubory ADM. Windows Vista a Server 2008 nadále rozeznávají i ADM soubory. ADMX soubory jsou uloženy v složce **%systemroot%\PolicyDefinitions** a při vytváření nové politiky se nekopírují do SYSVOL

výhody ADMX:

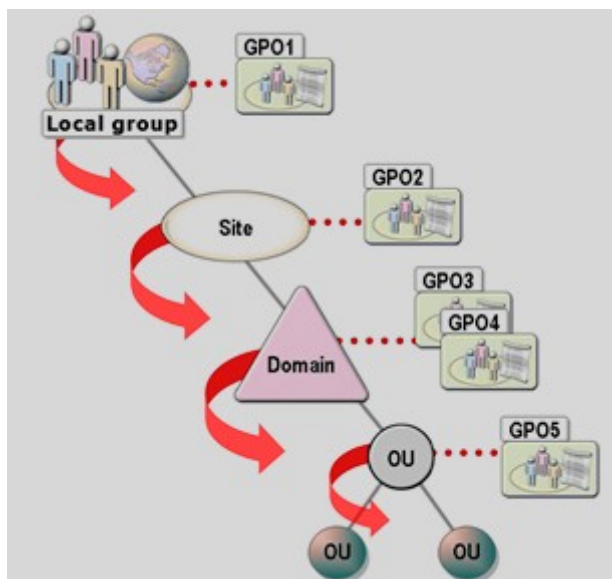
- jazykově neutrální
- neukládají se do SYSVOL
- ADMX formát je díky XML standardu kdykoliv rozšiřitelný

Co je centrální úložiště „Central Store“



Centrální úložiště „**Central Store**“ je nutné vytvořit manuálně v adresáři SYSVOL, aby byla zajištěna replikace tohoto adresáře na všechny DC. Úložiště slouží k uložení ADMX a ADML souborů. Díky centrálnímu úložišti budou jakékoliv změny v šablonách ADMX automaticky replikovány na všechny DC.

Aplikování skupin zásad „Group Policy Processing“

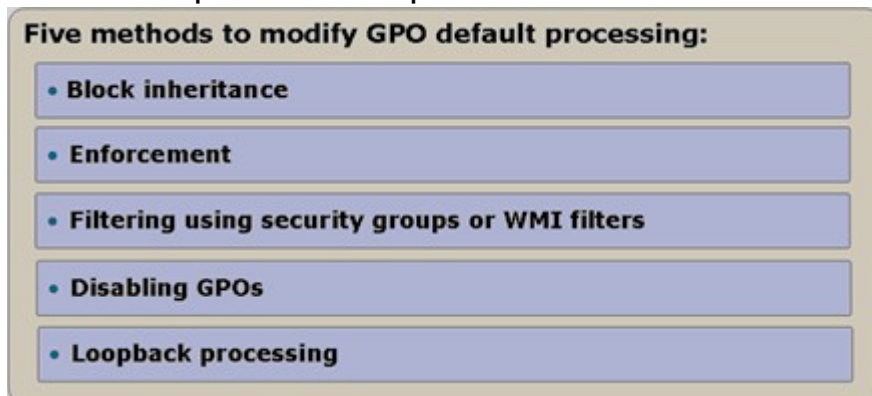


Politiky dělíme na lokální a doménové. Pokud bychom toto rozdělení měli ještě více specifikovat, členění by bylo:

1. Lokální politiky „Local Group Policy“
2. Politiky na úrovni oblastí „Site Level GPOs“
3. Politiky na úrovni domény „Domain level GPOs“
4. Politiky na úrovni organizačních jednotek „Organizational Unit GPOs“
5. Politiky na úrovni podskupin organizačních jednotek „Any child Organizational Unit GPOs“

Aplikování politik je pak z úrovně 1 na úroveň 5, tedy pokud na úrovni jedna máme nastaveno např. PROXY Enable a na úrovni 4 je PROXY Disable, vyhraje úroveň 4 a proxy v počítači zůstává ve stavu Disable.

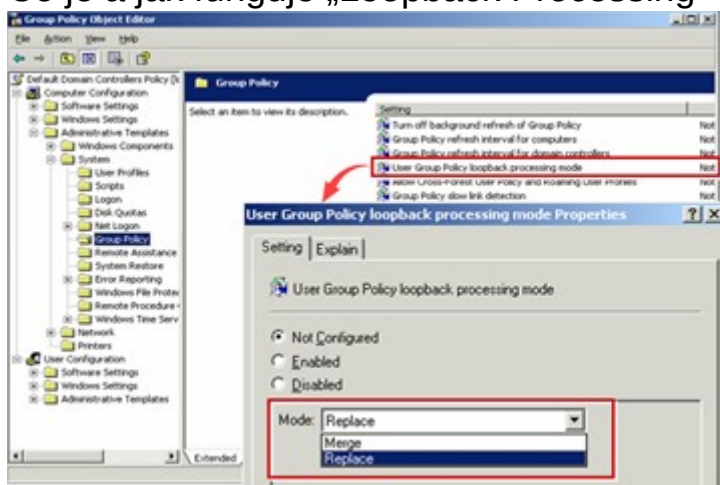
Ovlivnění aplikování skupin zásad



Samotné aplikování skupin zásad je možné ovlivňovat, a to přímo na úrovni každé z politik (GPO). Na každé politice tedy může být nastaveno:

Method	Description
Blocking inheritance	Blokování dědění doménových politik nebo politik z nadřazených OU
Enforcement of GPO links	Vynucení politiky. Využívá se, pokud chcete zajistit, že politika nebude přepsána.
Filtering using security groups	Na Každé GPO je možné nastavit oprávnění, tím můžete definovat, na jaké uživatele či skupiny bude politika aplikována
Filtering using WMI filters	Pomocí WMI filtrů je možné aplikování politik, třeba jen na PC s WIN XP, nebo na počítače s větší RAM od 3GB atd.
Disabling GPOs	Můžete zcela zablokovat použití GPO pro danou síť, doménu nebo organizační jednotku. Můžete také zcela vypnout část GPO Uživatelé nebo Počítače, aby výsledná politika měla menší velikost

Co je a jak funguje „Loopback Processing“



















Loopback Processing je jedna z možností nastavení GPO na úrovni Computers. Při jeho zapnutí se aplikuje i veškeré nastavení na úrovni Users, i když je politika linkována do

kontejneru Computers. Toto se využívá třeba u terminálových serverů, kde je zapotřebí aplikovat zabezpečení uživatele už na úrovni počítače.

Toto nastavení má dva módy:

- Merge mode
- Replace mode

Delegování oprávnění pro administraci Skupiny zásad

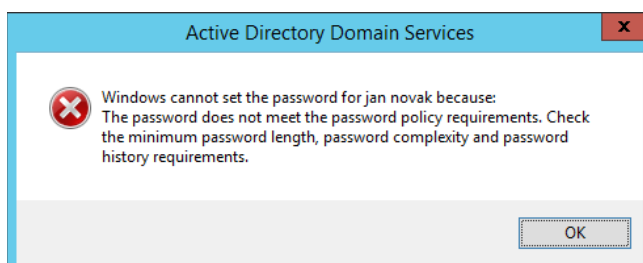
Methods to delegate control of GPOs	Create GPOs in the domain	Edit or delete GPOs	Link GPOs to containers	Use reporting tools
Membership in Group Policy Creator Owners group or explicit permission to create GPOs				
Assign Edit rights to individual policies				
Delegate the right to link GPOs to containers				
Delegate the right to use Group Policy reporting tools				

Password Policies

V každé síti je nutné řídit bezpečnost. Mezi hlavní útoky na firemní síť patří prolomení hesla uživatele, a proto musíme mít definovanou politiku, která se tomuto pokusí bezpečně předejít. Pokud máme v plánu spravovat hesla v doméně, nejlepším prostředkem je využít Group Policy, kde si můžeme jednoduše nadefinovat parametry hesel. V politice hesla (Password policy) lze definovat:

- Heslo musí splňovat požadavky na složitost
- Maximální stáří hesla
- Minimální délka hesla
- Minimální stáří hesla – uživatel si po změně hesla nemůže hned heslo dále měnit
- Ukládat hesla pomocí reverzibilního šifrování
- Vynutit použití historie hesel

Při zakládání nového uživatele v Active Directory se může objevit hláška, že heslo, které jsme zadali, nesplňuje požadavky zásad hesla.

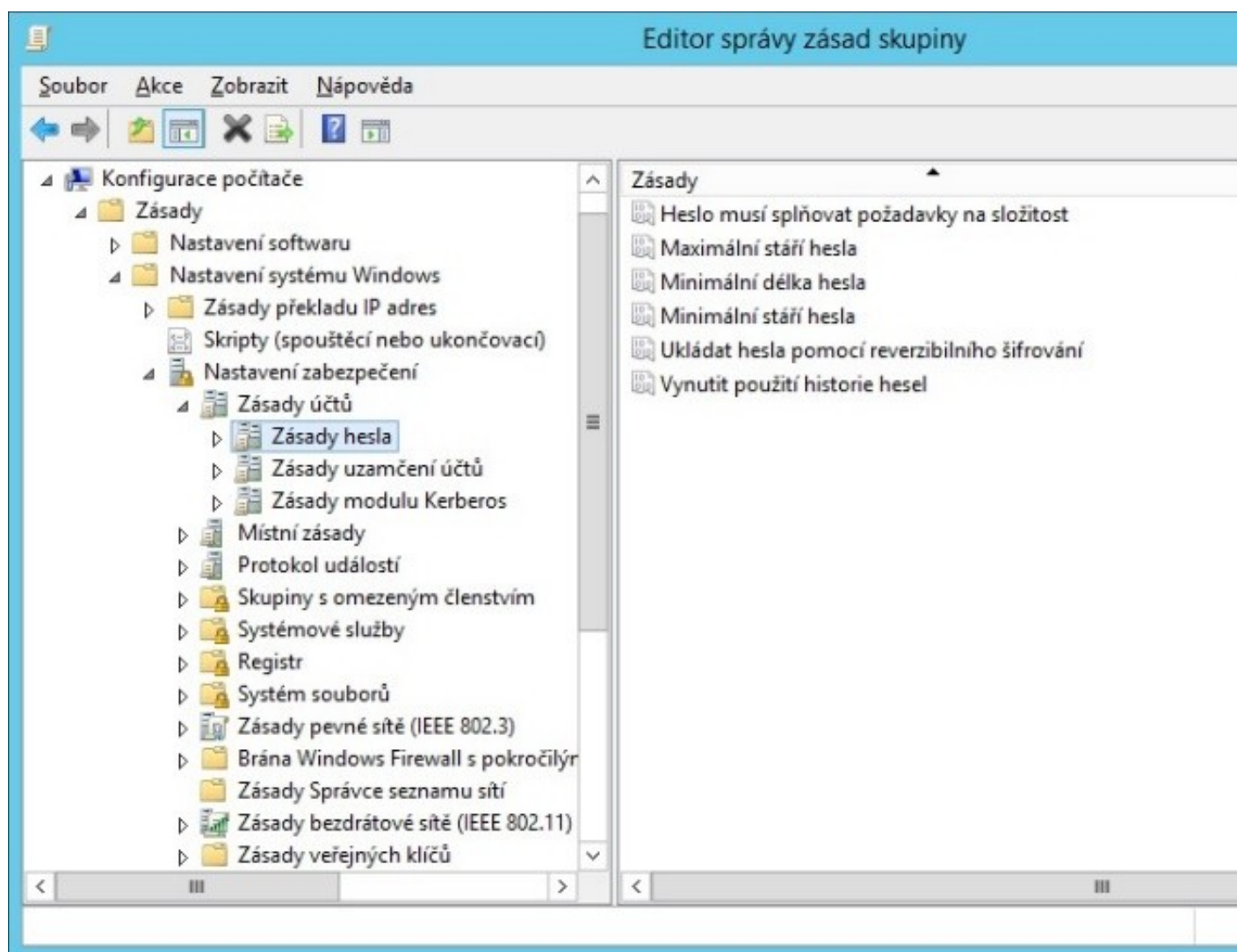


Obr. – hlášení, že heslo nesplňuje politiku

Možné řešení:

- Spustíte Správu zásad skupiny – gpmc.msc
- Domény > Vaše doména > Default domain policy > edit
- Přejděte do Konfigurace počítače > Zásady > Nastavení systému Windows > Nastavení zabezpečení > Zásady účtů > Zásady hesla a změňte zásady dle vašich požadavků.

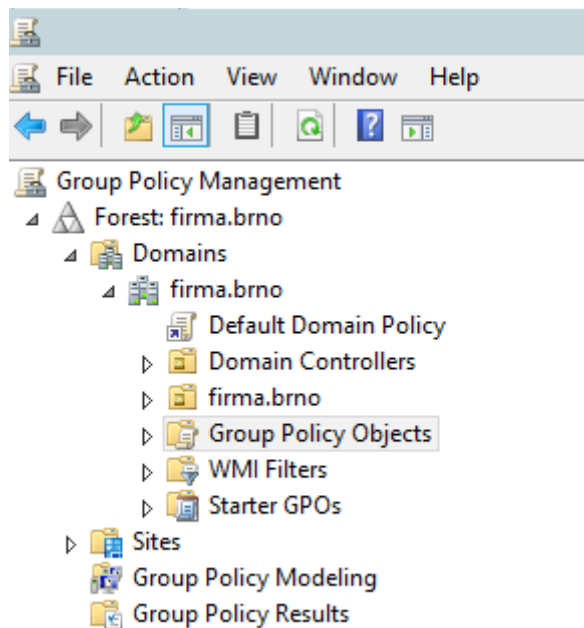
Na serveru spustíte `gpupdate /force` a poté zkuste znovu vytvořit uživatele.



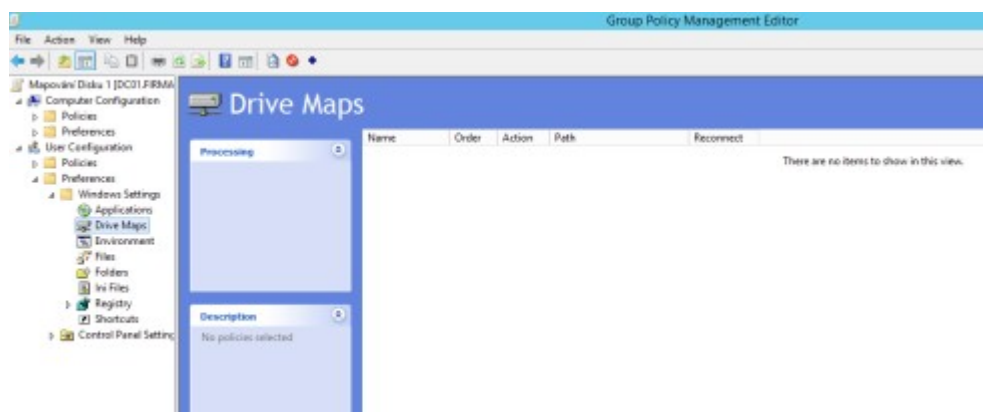
Obr. Editor správy zásad skupiny

Mapování síťových disků

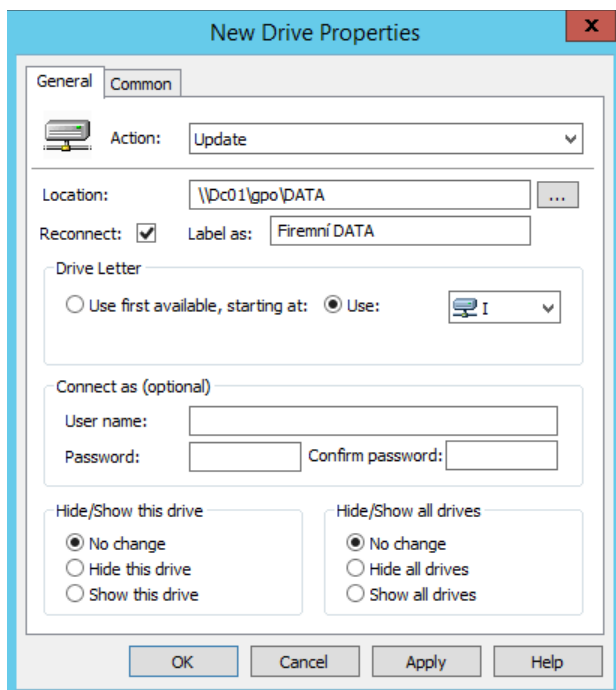
Mapování síťového disku pomocí Group Policy je velice jednoduché a účinné řešení.



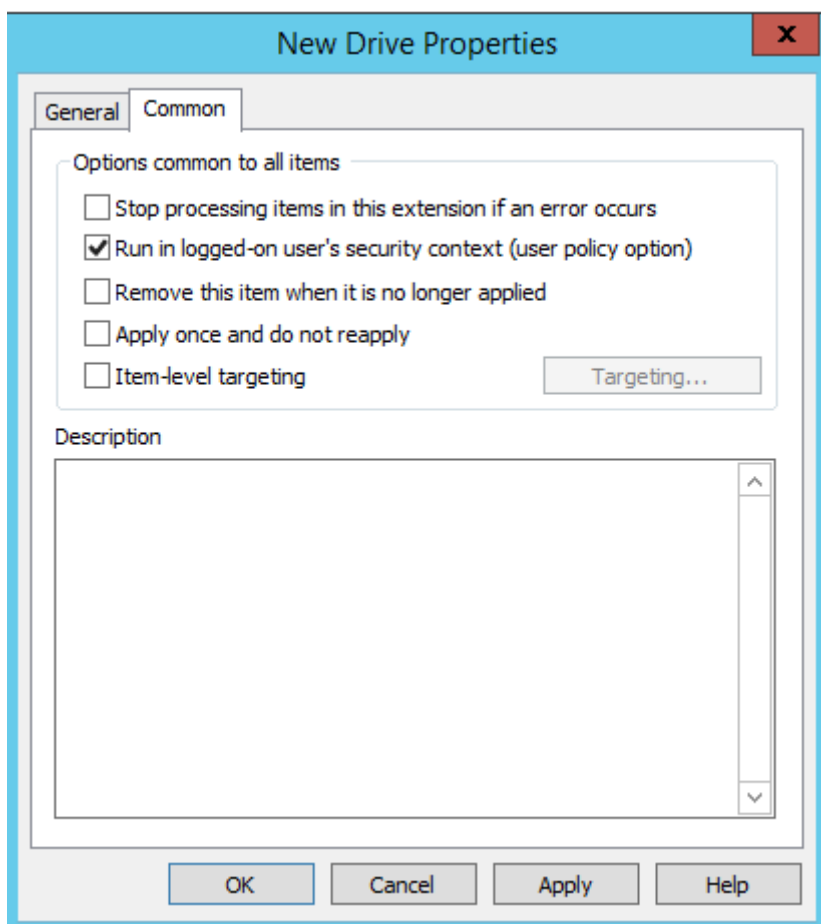
Nejdříve spustíme konzoli pro management group policy tedy **gpmc.msc**, ve které následně vyhledáme kontajner Group Policy Objects, zde vytvoříme nový GPO pod názvem Mapování disku 1.



Následně je jej potřeba editovat a na to právě slouží konzole group policy management editor, kde pod User Configurations > Preferences > Windows Settings > Drive maps vytvořím nové mapování.

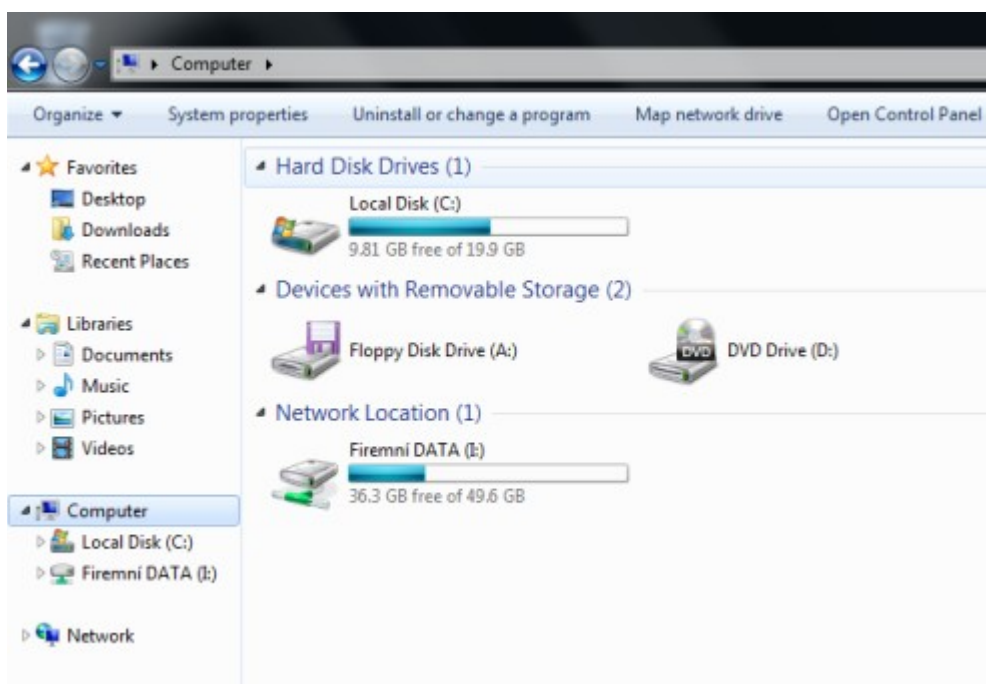


Lokaci je vždy nutné uvádět ve tvaru \\hostname\\sdilenaslozka, zaškrtnout Reconnect a Label as (tak ji uvidím v průzkumníku), tedy Firemní DATA, jako Drive Letter nastavit napevno „I“, je zde možnost i použít první dostupné písmeno, ale to by poté znamenalo, že na každé stanici bude mít mapování jiné písmeno, což by mohlo působit problémy a zmatky.

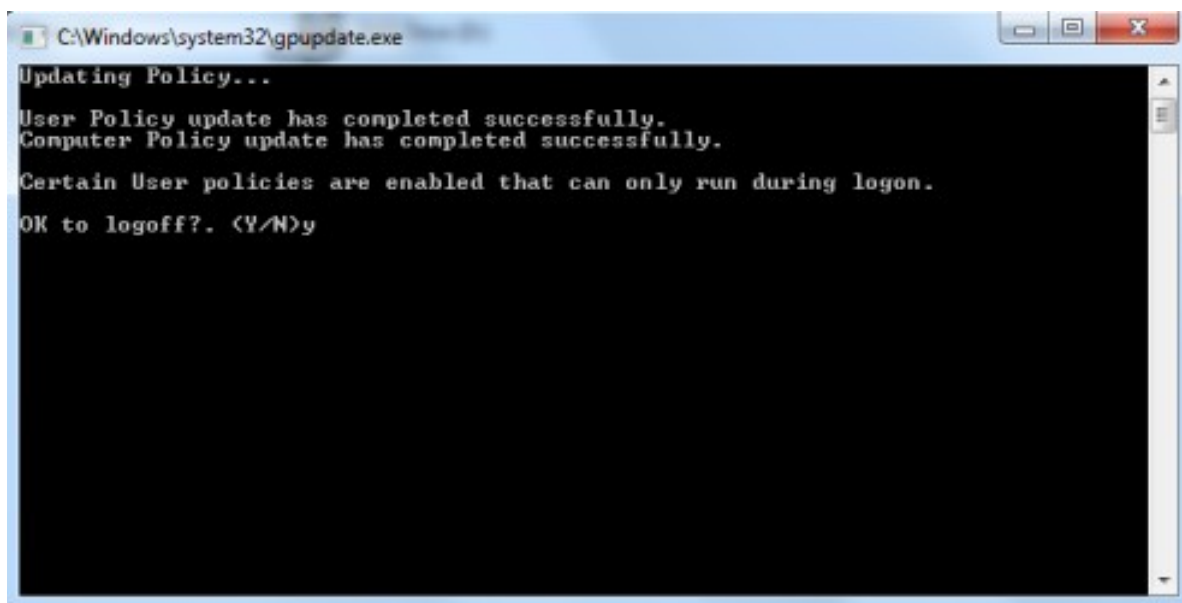


Na kartě Common, zaškrtnout možnost „Run in logged-on users security context“ což znamená, že se uživatel ke složce bude přihlašovat se svými právy, lze to obejít například tak, že na kartě General nastavíte v Connect as – třeba nějaký vyšší účet.

Nyní je potřeba GPO linknout na daný kontejner, v tomto případě to bude firma.brno a následně na stanici provést log off a log in, poté by mělo být vše funkční.



Vynutit načtení politiky na stanici lze příkazem: *gpupdate /force*



Zdroje:

<http://www.ondrej-soukup.cz/2009/09/co-jsou-skupiny-zasad-group-policy/>

<http://tomaskalabis.com/wordpress/windows-server-2012-r2-heslo-nesplnuje-pozadavky-zasad-hesla/>

Administrace MS Windows server 2008 – Velký průvodce administrátora