

# Serverové systémy Microsoft Windows

IW2/XMW2 2013/2014

**Jan Fiedor**

ifiedor@fit.vutbr.cz

Fakulta Informačních Technologií

Vysoké Učení Technické v Brně

Božetěchova 2, 612 66 Brno

Revize 19. 3. 2014

# Active Directory

## Zásady skupiny (objekty, zpracování)

# Zásady skupiny (Group Policies)

- Umožňují centrální správu a konfiguraci systémů Windows, aplikací a uživatelů v Active Directory
  - Určují co (ne)může dělat uživatel na daném počítači
- Sada nastavení popisujících konfiguraci počítačů a/nebo uživatelů v prostředí Active Directory
  - Nastavení definována a uložena na řadičích domény
- Správa pomocí konzole **Správa zásad skupiny** (GPMC, *Group Policy Management Console*)
  - K dispozici po přidání funkce **Správa zásad skupiny**

# Správa zásad skupiny

Správa zásad skupiny

Soubor Akce Zobrazit Okno Nápověda

Správa zásad skupiny

- Doménová struktura: testing.local
  - Domény
    - testing.local
      - Default Domain Policy
      - Password Policy
      - Domain Controllers
        - Default Domain Controllers Policy
      - Objekty zásad skupiny
        - Default Domain Controllers Policy
        - Default Domain Policy
        - Password Policy
      - Filtiry rozhraní WMI
      - Objekty GPO Starter
    - Lokality
      - Default-First-Site-Name
    - Modelování zásad skupiny
    - Výsledky zásad skupiny

**Default Domain Policy**

Obor Podrobnosti **Nastavení** Delegování Stav

**Default Domain Policy**  
Datum shromáždění dat: 17. 3. 2014 23:37:08 [zobrazit vše](#)

<b>Konfigurace počítače (povolena)</b>	<a href="#">skrýt</a>
<b>Zásady</b>	<a href="#">skrýt</a>
<b>Nastavení systému Windows</b>	<a href="#">skrýt</a>
<b>Nastavení zabezpečení</b>	<a href="#">zobrazit</a>
<b>Konfigurace uživatele (povolena)</b>	<a href="#">skrýt</a>

Nejsou definována žádná nastavení.

# Nastavení zásady (policy setting)

- Zásada (*policy*)
  - Specifické nastavení systému Windows (registru, ...)
  - Windows 8 a Server 2012 obsahuje přes 3500 zásad
- Definuje změnu v konfiguraci systému Windows
  - Většina nastavení se týká jen povolení resp. zakázání nějaké služby, vlastnosti nebo funkcionality systému
  - Některá nastavení vyžadují dodatečné informace
- Zásady mohou být nedefinovány (*not defined*)
  - Uplatní se dříve aplikované nebo výchozí nastavení

# Aplikace nastavení zásad

- Nastavení aplikovaná na celý počítač
  - Obsažena pod uzlem konfigurace počítače (*computer configuration settings*)
  - Má přednost v případě, že je stejná zásada nastavena i v sekci aplikující nastavení na přihlášené uživatele
  - Nastavení zabezpečení (hesla, práva, ...), systému, ...
- Nastavení aplikovaná na přihlášeného uživatele
  - Obsažena pod uzlem konfigurace uživatele (*user configuration settings*)
  - Nastavení plochy, nabídky Start, součástí systému, ...

# Konfigurace počítače a uživatele

Název	Popis
Zásady účtů	Heslo a zásady zamknutí účtu
Místní zásady	Zásady auditování, uživatelských práv a zabezpečení
Protokol událostí	Protokol událostí
Skupiny s omezeným členstvím	Skupiny s omezeným členstvím
Systémové služby	Nastavení systémové služby
Registr	Nastavení zabezpečení registru
Systém souborů	Nastavení zabezpečení systému souborů
Zásady pevné sítě (IEEE 802.3)	Správa zásad kabelové sítě. Umožňuje správu
Brána Windows Firewall s pokročilým zabezpečením	Brána Windows Firewall s pokročilým zabezpečením
Zásady Správce seznamu sítí	Zásady skupiny pro název sítě, ikonu a umístění
Zásady bezdrátové sítě (IEEE 802.11)	Správa zásad bezdrátové sítě. Umožňuje správu
Zásady veřejných klíčů	
Zásady omezení softwaru	
Architektura NAP (Network Access Protection)	Architektura NAP (Network Access Protection)
Zásady řízení aplikací	Zásady řízení aplikací
Zásady zabezpečení protokolu IP - Active Directory	Správa protokolu IPsec (Internet Protocol Security)

# Objekty zásad skupiny (GPO objekty)

- Objekty Active Directory, jenž obsahují jednotlivá nastavení zásad
  - Fyzická reprezentace zásad skupiny v Active Directory
- Aplikace nastavení na základě rozsahu (*scope*)
  - Určuje uživatele a počítače, na které se mají aplikovat nastavení obsažená v daném GPO objektu
  - Lze definovat pomocí
    - GPO odkazu (*GPO link*)
    - WMI filtru (*Windows Management Instrumentation filter*)
    - Bezpečnostního filtru (*Security filter*)



# GPO odkazy (GPO links)

- Propojují GPO objekty s doménami, místy (*sites*) a organizačními jednotkami (OUs)
  - Každý GPO objekt může být propojen s jedním i více kontejnery (doménami, místy, OU jednotkami)
  - Nastavení aplikováno na uživatele a počítače v těchto kontejnerech (a ostatních obsažených kontejnerech)
- Určují maximální rozsah GPO objektu
  - Filtry mohou z tohoto rozsahu vyřadit uživatele nebo počítače, ale nemohou žádné další přidat

# Filtry

- WMI filtry
  - Omezují rozsah GPO objektů na uživatele a počítače, kteří splňují zadaný WMI dotaz (*query*)
  - Např. omezení aplikace na konkrétní operační systém

```
Select * from Win32_OperatingSystem  
where Caption = "Microsoft Windows 7 Professional"
```

- Bezpečnostní filtry
  - Omezují rozsah GPO objektů na uživatele a počítače, jenž (ne)náleží do zadané (bezpečnostní) skupiny
  - Nastavují oprávnění pro čtení a použití zásad skupiny

# Nastavení rozsahu GPO objektu

The screenshot shows the Group Policy Management console window titled "Správa zásad skupiny". The left pane displays a tree view of the Group Policy Objects (GPOs) for the "testing.local" domain. The "Default Domain Policy" is selected and highlighted in blue.

The right pane shows the configuration for the "Default Domain Policy". The "Propojení" (Linking) tab is active. The "Zobrazit propojení v tomto umístění:" (Show link in this location) dropdown is set to "testing.local". Below this, a table lists the linked locations:

Umístění	Vynucené	Propojení povoleno	Cesta
testing.local	Ne	Ano	testing.local

The "Filtrování zabezpečení" (Security filtering) section shows that the policy is applied to "Authenticated Users". The "Filtrování rozhraní WMI" (WMI interface filtering) section shows that the policy is linked to the "<Žádný>" (None) filter.

# Nastavení stavu GPO objektu

The screenshot shows the Group Policy Management console window titled "Správa zásad skupiny". The left pane displays a tree view of the domain structure for "testing.local", with "Default Domain Policy" selected under "Objekty zásad skupiny". The right pane shows the configuration details for this policy.

Obor	Podrobnosti	Nastavení	Delegování	Stav
Doména:		testing.local		
Vlastník:		Domain Admins (TESTING\Domain Admins)		
Vytvořeno:		24. 2. 2013 21:35:51		
Změněno:		24. 2. 2013 21:43:30		
Verze uživatele:		0 (AD), 0 (SYSVOL)		
Verze počítače:		3 (AD), 3 (SYSVOL)		
Jedinečné ID:		{31B2F340-016D-11D2-945F-00C04FB984F9}		
Stav objektu GPO:				Povoleno
Komentář:				Nastavení konfigurace počítače zakázáno Nastavení konfigurace uživatele zakázáno Povoleno Všechna nastavení zakázána

# Typy GPO objektů

- Lokální GPO objekty (*Local GPOs*)
  - Ovlivňují pouze počítač, na kterém jsou definovány
  - Uloženy v adresáři **<system>\System32\GroupPolicy**
  - Od Windows Vista a Server 2008 možnost vytváření více než jednoho GPO objektu (*multiple local GPOs*)
- Doménové GPO objekty (*Domain GPOs*)
  - Aplikovány na různé počítače a uživatele v doméně
  - Uloženy v Active Directory (na řadičích domény)

# Lokální (multiple local) GPO objekty

- GPO místního počítače (*Local Computer GPO*)
  - Jediný lokální GPO objekt, kde lze definovat nastavení aplikované na počítač (konfigurace počítače)
  - Uživatelská nastavení aplikována na všechny uživatele
- GPO speciálních skupin
  - Obsahuje uživatelská nastavení aplikované na správce nebo ostatní uživatele (nelze použít jiné skupiny)
- GPO místních uživatelů (*User-Specific Local GPO*)
  - Zahrnuje uživatelská nastavení pro jednoho uživatele

# Pořadí aplikace lokálních GPO objektů

- Podle specifičnosti (menší rozsah, vyšší priorita)
- Konfigurace počítače
  - 1) GPO místního počítače
- Konfigurace uživatele
  - 1) GPO místního počítače
  - 2) GPO správců / ostatních uživatelů
  - 3) GPO přihlášeného uživatele

# Doménové GPO objekty (odkazy)

- GPO objekty připojené k místu (*Site GPOs*)
  - Aplikovány na všechny počítače v konkrétním místě a na uživatele přihlášené na těchto počítačích
- GPO objekty připojené k doméně (*Domain GPOs*)
  - Aplikovány na všechny počítače a uživatele v doméně
- GPO objekty připojené k organizační jednotce (*OU GPOs*)
  - Aplikovány na všechny počítače a uživatele obsažené v organizační jednotce a vnořených org. jednotkách



# Základní doménové GPO objekty

- Výchozí zásady domény (*Default Domain Policy*)
  - Připojen k doméně
    - Aplikace na veškeré uživatele a počítače v dané doméně
  - Definuje nastavení týkající se hesel, uzamykání účtů a služby Kerberos
- Výchozí zásady řadičů domény (*Default Domain Controllers Policy*)
  - Připojen k organizační jednotce Řadiče domény
    - Aplikace na všechny (obsažené) řadiče domény
  - Definuje nastavení ohledně zásad auditu a práv

# Vynucené (enforced) GPO objekty

- Mají vyšší prioritu než standardní GPO objekty
  - Aplikovány jako poslední (přepisují dřívější nastavení)
- Vytvářejí se vynucením konkrétního GPO odkazu
  - Stejný GPO objekt může být zároveň standardní GPO objekt i vynucený GPO objekt (záleží jak je připojen)
- Ignorují (neplatí pro ně) blokování dědičnosti
  - Vždy aplikovány na uživatele a počítače ve vnořených kontejnerech (organizačních jednotkách)

# Vynucení aplikace GPO objektu

The screenshot shows the Group Policy Management console window titled "Správa zásad skupiny". The left pane displays a tree view of the domain structure for "testing.local", with "Default Domain Policy" selected. A context menu is open over this policy, showing options like "Upravit...", "Vynucené" (checked), "Propojení povoleno" (checked), "Uložit sestavu...", "Otevřít v novém okně", "Odstranit", "Přejmenovat", "Aktualizovat", and "Nápověda".

The right pane is titled "Domain Controllers" and shows a list of GPO objects. A message at the top states: "Tento seznam neobsahuje žádné objekty GPO propojené s lokalitami. Další informace najc". Below this is a table with the following data:

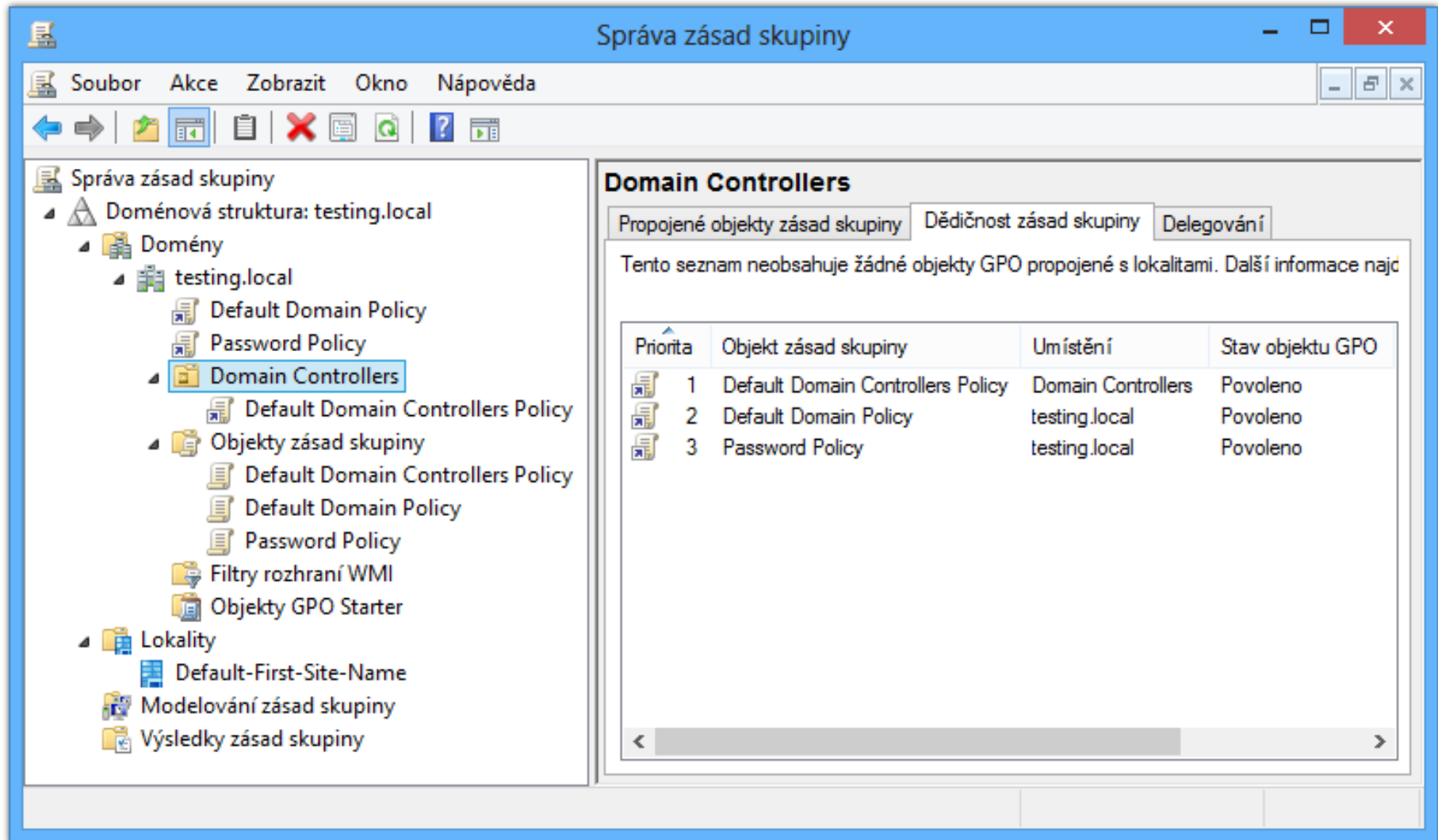
Priorita	Objekt zásad skupiny	Umístění
1 (Vynuceno)	Default Domain Policy	testing.local
2	Default Domain Controllers Policy	Domain Controllers
3	Password Policy	testing.local

At the bottom of the console, a status bar displays the message: "Zapnout atribut Vynuceno pro toto propojení".

# Pořadí aplikace GPO objektů

- 1) Lokální GPO objekty
- 2) Doménové GPO objekty
  - a) Připojené k místu
  - b) Připojené k doméně
  - c) Připojené k organizačním jednotkám
- 3) Vynucené doménové GPO objekty
  - a) Připojené k organizačním jednotkám
  - b) Připojené k doméně
  - c) Připojené k místu

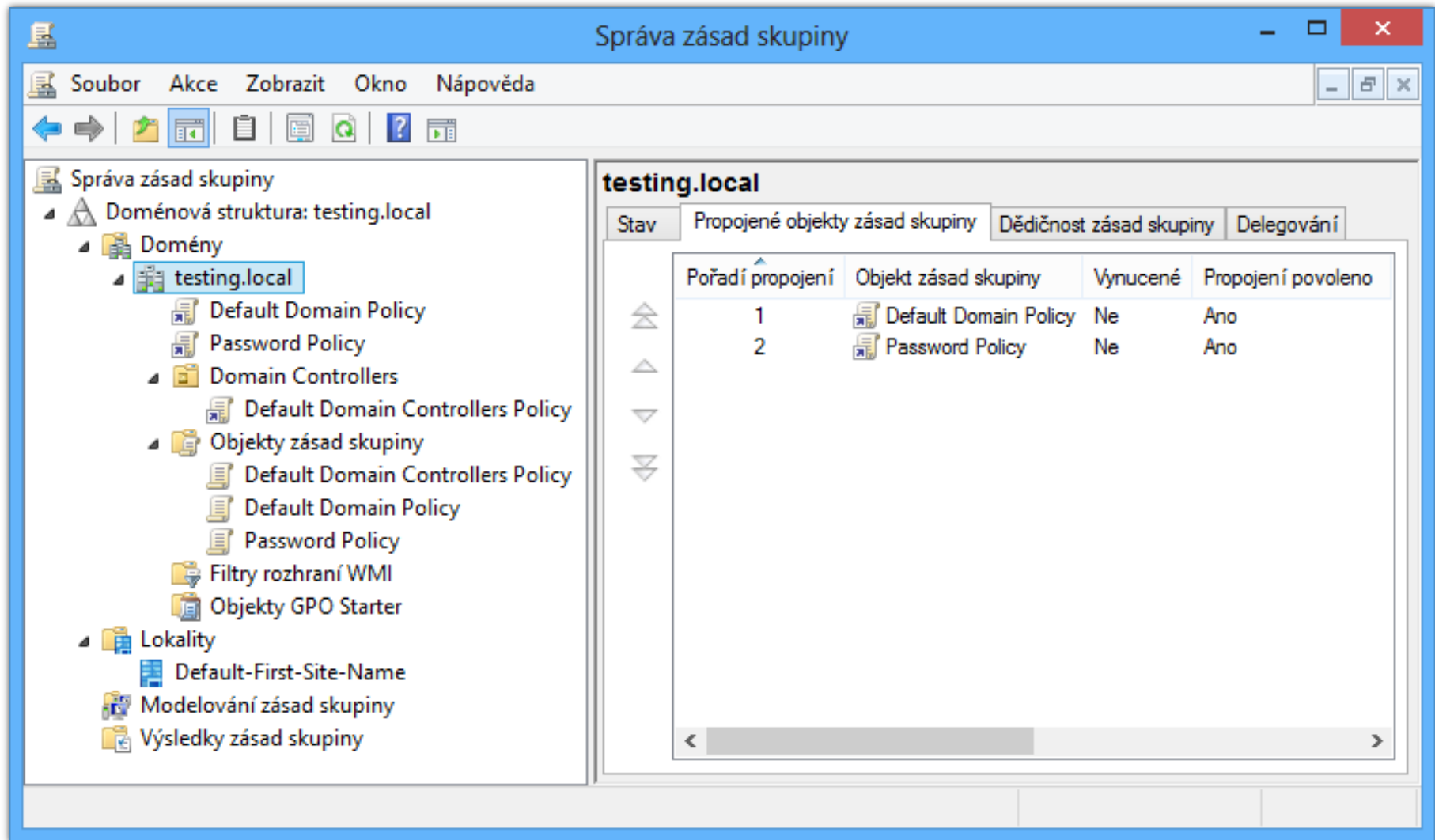
# Zjištění pořadí aplikace GPO objektů



The screenshot shows the Group Policy Management console for the 'testing.local' domain. The left pane displays the hierarchy: Správa zásad skupiny > Doménová struktura: testing.local > Domény > testing.local > Domain Controllers. The right pane, titled 'Domain Controllers', shows the 'Propojené objekty zásad skupiny' tab. A message states: 'Tento seznam neobsahuje žádné objekty GPO propojené s lokalitami. Další informace najd' (This list does not contain any GPO objects linked to sites. Further information can be found...). Below the message is a table listing the GPOs applied to the Domain Controllers.

Priorita	Objekt zásad skupiny	Umístění	Stav objektu GPO
1	Default Domain Controllers Policy	Domain Controllers	Povoleno
2	Default Domain Policy	testing.local	Povoleno
3	Password Policy	testing.local	Povoleno

# Pořadí aplikace v rámci kontejneru



The screenshot shows the Group Policy Management console for the domain **testing.local**. The left pane displays the domain structure, including the **testing.local** domain and its various policy objects. The right pane shows the **Propojené objekty zásad skupiny** (Linked Group Policy Objects) tab, which lists the linked GPOs and their order.

Stav	Propojené objekty zásad skupiny	Dědičnost zásad skupiny	Delegování
Pořadí propojení	Objekt zásad skupiny	Vynucené	Propojení povoleno
1	Default Domain Policy	Ne	Ano
2	Password Policy	Ne	Ano

# Blokování dědičnosti (GPO objektů)

- Zabraňuje aplikaci nadřazených GPO objektů na uživatele a počítače v konkrétním kontejneru
  - Blokuje dědění GPO objektů z otcovských kontejnerů
  - Nelze použít pro blokování vynucených GPO objektů
- Nastavuje se na organizačních jednotkách nebo na celé doméně

# Zablokování dědičnosti (GPO objektů)

The screenshot shows the 'Správa zásad skupiny' (Group Policy Management) console. The left pane displays the domain structure for 'testing.local', with 'Domain Controllers' selected. A context menu is open over 'Domain Controllers', and the option 'Zablokovat dědičnost' (Block inheritance) is checked. The right pane shows the 'Domain Controllers' GPO details, including a table of linked GPOs.

**Správa zásad skupiny**

Soubor Akce Zobrazit Okno Nápověda

Správa zásad skupiny

- Doménová struktura: testing.local
  - Domény
    - testing.local
      - Default Domain Policy
      - Password Policy
      - Domain Controllers**

**Domain Controllers**

Propojené objekty zásad skupiny Dědičnost zásad skupiny Delegování

Tento seznam neobsahuje žádné objekty GPO propojené s lokalitami. Další info

Priorita	Objekt zásad skupiny	Umístění
1 (Vynuceno)	Default Domain Policy	testing.local
2	Default Domain Controllers Policy	Domain Controllers

Zapnout dědičnost bloku



# Klient zásad skupiny

- Služba zajišťující aplikaci nastavení zásad na daný počítač nebo uživatele
  - Využívá *pull* metodu (klient sám stahuje GPO objekty z řadiče domény, řadič domény jen ověřuje přístup)
- Změny provádějí tzv. klientská (CSE) rozšíření
  - Zajišťují zpracování konkrétní kategorie zásad skupiny
- Rozdílové zpracování GPO objektů
  - Aplikace jen těch nastavení zásad, jenž byly změněny (jsou odlišné od nastavení aplikovaných předtím)
  - Lze vypnout (vynutit aplikaci všech nastavení zásad)

# Postup zpracování zásad skupiny

- 1) Stažení seznamu GPO objektů
- 2) Zpracování obsažených GPO objektů
  - a) Kontrola stavu GPO objektu (povolen / nepovolen)
  - b) Kontrola oprávnění (číst a používat zásady skupiny)
  - c) Vykonání a vyhodnocení WMI dotazu ve WMI filtru
- 3) Aplikace nastavení obsažených v GPO objektech
  - a) Zpracování nastavení (definováno / nedefinováno)
  - b) Zavolání odpovídajícího CSE rozšíření
- 4) Zopakování bodů 1) až 3) za 90 – 120 minut

# Loopback zpracování zásad skupiny

- Umožňuje aplikovat nastavení zásad na uživatele na základě počítače, na který je přihlášen
  - Povoluje aplikaci uživatelských nastavení obsažených v GPO objektech, jenž mají ve svém rozsahu počítač, na který je uživatel přihlášen, a ne daného uživatele
- Povoluje se v zásadách skupiny
  - Projeví se teprve při druhé aplikaci zásad skupiny
    - Při první aplikaci dochází k přepnutí klienta zásad skupiny do loopback režimu zpracování
  - Nastavení počítače (nelze povolit pro určité uživatele)

# Povolení loopback zpracování

The screenshot displays the Group Policy Editor interface. The left pane shows the tree structure with 'Zásady skupiny' selected. The right pane shows a list of policies under 'Nastavení'. The policy 'Konfigurovat režim zpracování zásad skupiny uživatele ve zpětné smyčce' is highlighted and set to 'Povoleno'.

Nastavení	Stav
Protokolování a trasování	
Konfigurovat připojení Direct Access jako rychlá síťová připojení	Není na...
<b>Konfigurovat režim zpracování zásad skupiny uživatele ve zpětné smyčce</b>	<b>Povoleno</b>
Konfigurovat rozpoznání pomalého připojení zásad skupiny	Není na...
Konfigurovat zpracování zásad bezdrátové sítě	Není na...
Konfigurovat zpracování zásad diskových kvót	Není na...
Konfigurovat zpracování zásad drátové sítě	Není na...

# Režimy loopback zpracování

- Nahradit (*replace*)
  - Použije uživatelská nastavení z GPO objektů počítače, na kterém je daný uživatel přihlášen
  - Nastavení z GPO objektů uživatele jsou ignorovány
- Sloučit (*merge*)
  - Použije uživatelská nastavení z GPO objektů uživatele i počítače, na kterém je daný uživatel přihlášen
  - Nastavení z GPO objektů počítače aplikovány později (přepisují nastavení z GPO objektů uživatele)
    - Dodatečná úprava uživatelských nastavení pro daný počítač

# Režim pomalého připojení (slow-link)

- Zabraňuje aplikaci nastavení některých zásad při detekci pomalého spojení s řadičem domény
  - Týká se hlavně nastavení zásad, jejichž aplikace vede k objemnějším přenosům dat (např. instalace SW)
- Aktivován pokud přenosová rychlost klesne pod definovaných práh (*threshold*)
  - Ve výchozím nastavení je práh 500 Kbit/s
  - Lze změnit v zásadách skupiny

# Nastavení prahu pro pomalé připojení

The image shows two overlapping windows of the Group Policy Editor. The background window is titled 'Editor správy zásad skupiny' and shows the 'Zásady skupiny' (Group Policies) folder expanded in the left-hand tree. The foreground window is also titled 'Editor správy zásad skupiny' and displays a list of policies under the 'Zásady skupiny' folder. The policy 'Konfigurovat rozpoznání pomalého připojení zásad skupiny' (Configure slow link connection detection) is selected and highlighted in blue, with its status set to 'Povoleno' (Enabled).

Nastavení	Stav
Protokolování a trasování	
Konfigurovat připojení Direct Access jako rychlá síťová připojení	Není na...
Konfigurovat režim zpracování zásad skupiny uživatele ve zpětné smyčce	Není na...
<b>Konfigurovat rozpoznání pomalého připojení zásad skupiny</b>	<b>Povoleno</b>
Konfigurovat zpracování zásad bezdrátové sítě	Není na...
Konfigurovat zpracování zásad diskových kvót	Není na...
Konfigurovat zpracování zásad drátové sítě	Není na...

# Výsledné sady zásad (RSOP)

- Vyhodnocují výslednou sadu nastavení zásad pro konkrétního uživatele nebo počítač
- Výsledky zásad skupiny (*results*)
  - Zjišťuje aktuální nastavení zásad
  - Možnost vyhodnocení pomocí nástroje **gpresult**
- Modelování zásad skupiny (*modeling*)
  - Simuluje výsledné nastavení zásad (např. po přesunu uživatele nebo počítače)
  - Realizují řadiče domény (musí být k dispozici)



# Informace o použitých GPO objektech

**Správa zásad skupiny**

Soubor Akce Zobrazit Okno Nápověda

**Správa zásad skupiny**

- Doménová struktura: testing.local
  - Domény
    - testing.local
      - Default Domain Policy
      - Password Policy
      - Domain Controllers
        - Default Domain Controllers Policy
      - Objekty zásad skupiny
        - Default Domain Controllers Policy
        - Default Domain Policy
        - Password Policy
        - Filtry rozhraní WMI
        - Objekty GPO Starter
    - Lokality
      - Default-First-Site-Name
    - Modelování zásad skupiny
    - Výsledky zásad skupiny
      - Administrator na WSRV2012**

**Administrator na WSRV2012**

Souhm Podrobnosti Události zásad

**Výsledky zásad skupiny**

**TESTING\Administrator (TESTINGWSRV2012)**  
Datum shromáždění dat: 18. 3. 2014 0:49:41 [zobrazit vše](#)

[Podrobnosti o počítači](#) [sknýt](#)

**Obecné** [zobrazit](#)

**Stav součásti** [zobrazit](#)

**Nastavení** [zobrazit](#)

**Objekty zásad skupiny** [sknýt](#)

**Použité objekty zásad skupiny** [sknýt](#)

Default Domain Controllers Policy	<a href="#">zobrazit</a>
Default Domain Policy	<a href="#">zobrazit</a>
Místní zásady skupiny	<a href="#">zobrazit</a>
Password Policy	<a href="#">zobrazit</a>

**Odmítnuté objekty zásad skupiny** [sknýt](#)

**Filtry rozhraní WMI** [zobrazit](#)

[Podrobnosti o uživateli](#) [sknýt](#)

# Výsledná nastavení

The screenshot shows the 'Správa zásad skupiny' (Group Policy Management) console. The left pane shows the hierarchy: Doménová struktura: testing.local > Domény > testing.local > Objekty zásad skupiny > Administrator na WSRV2012. The right pane shows the details for this GPO, with the 'Podrobnosti o počítači' section expanded to show the 'Zásady účtu/Zásada hesel' (Account Policies) section.

Zásady	Nastavení	Vítězný objekt zásad skupiny
Heslo musí splňovat požadavky na složitost	Zakázáno	Password Policy
Maximální stáří hesla	0 dní	Password Policy
Minimální délka hesla	1 znaků	Password Policy
Minimální stáří hesla	0 dní	Password Policy
Ukládat hesla pomocí reverzibilního šifrování	Zakázáno	Default Domain Policy
Vynutit použití historie hesel	0 hesel zapamatováno	Password Policy