Lokální a globální politiky ve Windows Server 2019

cvičení 6

Fakulta Informatiky a Managementu

Univerzita Hradec Králové

Ing. David Šec (david.sec@uhk.cz),

Ing. Tomáš Svoboda, Ph.D. (tomas.svoboda@uhk.cz)

leden 2021

1 Seznam úkolů

1. Otevřete správu zásad skupin a zjistěte, jaké výchozí objekty zásad skupin existují.

2. Zjistěte, jaké jsou rozdíle mezi lokálními a globálními zásadami skupin. Zjistěte, jaké jsou nadřazené.

3. Pro skupinu Marketing definujte pravidlo, které zakáže uživatelům této skupiny přístup k ovládacím panelům.

4. Vyzkoušejte se přihlásit pod účtem ze skupiny Marketing a zjistěte, jestli toto pravidlo reálně funguje, pokud ne, tak zjistěte, proč a opravte to.

5. Zjistěte, kdy se která pravidla aplikují a jak lze aplikaci globálních pravidel vynutit.

6. V objektu group policy Marketing nadefinujte tyto pravidla pro uživatele:
   - Nastavte obrázek plochy na vámi preferovaný (např. Jellyfish)
   - Zakažte upravování obrázku plochy
   - Odeberte možnost zobrazení síťových připojení v nabídce Start
   - Odeberte správce úloh

7. V objektu group policy Marketing definujte tyto nastavení pro počítače:
   - Nastavte automatické spuštění programu notepad po přihlášení k počítači
   - Nastavte systémový čas počítače, aby využíval NTP server tik.cesnet.cz

8. Zjistěte, kdy se která pravidla aplikují a jak lze aplikaci globálních pravidel vynutit a nastavte vynucení pravidla Povolit ovládací panely

9. Zablokujte dědičnost na OU Marketing.

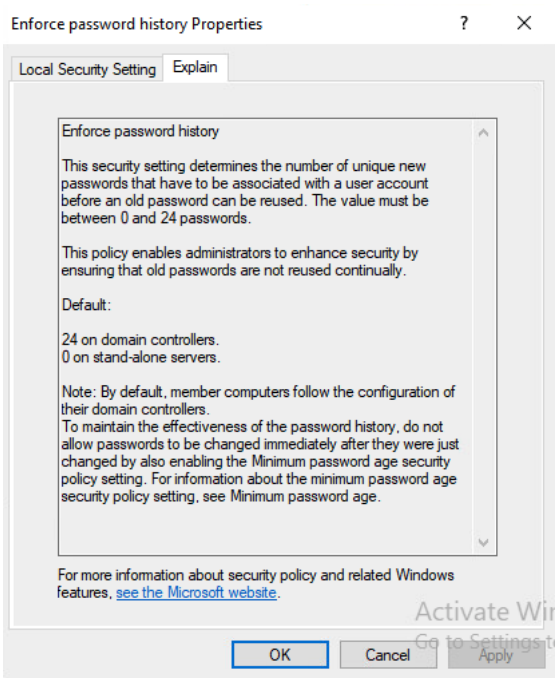
2 Postup řešení

2.1 Lokální zásady (Local Policies)

Zkontrolujte si, zda máte přidanou, případně přidejte serverovou roli Group Policy Management.

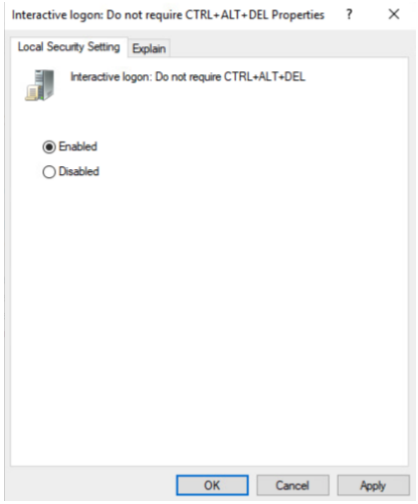
- Otevřete si Local Security Policy v nabídce Tools a prozkoumejte položky Account Policies a Local Policies.

Zjistěte, jaké jsou politiky pro zadávání hesla, jaké jsou požadavky na minimální délku hesla, a kolik předchozích hesel se vy systému uchovává pro zajištění jedinečnosti zadaného hesla, jaká je maximální doba platnosti hesla apod. Prozkoumejte kartu *Explain* ve vlastnostech dané politiky (Obrázek 1).



Obrázek 1: Historie hesel – Detailní popis

V následujícím kroku zkuste vypnout zadávání kombinace CTRL+ALT +Del před přihlášením uživatele do systému. Aktivováním položky *Interactive Logon: Do not require CTRL+ALT + Del* v Local Policies → Security Options. Volbou enabled dané pravidlo aktivujete (viz Obrázek 2).



Obrázek 2: Deaktivace Interactive logon screen

2.2 Globální zásady skupiny (Global Policy)

2.2.1 Zjistěte,jaké jsou rozdíly mezi lokálními a globálními zásadami skupin?

Každý počítač již od Windows 2000 má lokální politiky (Local Group Policy), které ovlivňují lokální počítač a přihlášené uživatele na něj. Pokud není počítač připojen do domény, tak právě tyto lokální politiky jsou použity jako jediné. Pokud například vytvořím uživatele na počítači a nastavím mu nějaké omezené oprávnění, chování právě tohoto uživatele vymezuje lokální politika. Tyto lokální politiky jsou uloženy ve skrytém adresáři %systemroot%\system32\ GroupPolicy.

Zdroj: STANEK, William R. Group Policy: zásady skupiny ve Windows: kapesní rádce administrátora. Vyd. 1. Brno: Computer Press, 2010, 351 s. ISBN 978-80-251-2920-3.

2.2.2 Jaké politiky jsou nadřaznené?

Na počítač jsou aplikovány nejprve lokální politiky, přes které jsou v následujícím pořadí aplikovány další politiky:

1. Objekty Lokální politiky (LGPO – Local Group Policy Objects)
2. Globální politiky pro lokalitu (GPO – Global Policy Objects)
3. GPO pro doménu

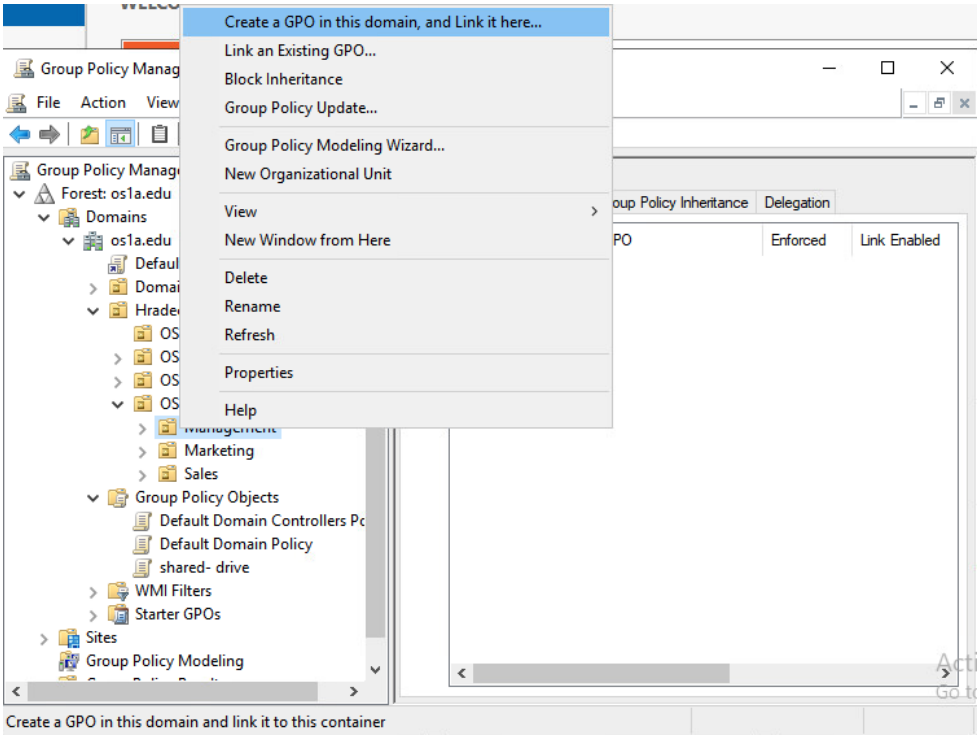
4. GPO pro Organizační jednotku
5. GPO pro podřízenou Organizační jednotku

V praxi to znamená že lokální politiky jsou přepisovány těmi globálními, které lze následně dále specifikovat na úrovni lokalit, domén, OU. Vezmeme-li v úvahu strukturu z minulého cvičení, tak politiky vytvořené pro organizační jednotku OS1a Users jsou aplikovány na všechny členy skupiny, zároveň však můžeme aplikovat stejné pravidlo na podřízenou OU Management s rozdílnou hodnotou a tím předchozí pravidlo „přebít“. V případě že potřebujeme dané pravidlo aplikovat bez ohledu na další zanožení, lze jej vynutit (GPO Enforcement), čímž zamezíme přepsání pravidla podřízenými OU.

2.3 Vytváření GPO

Nyní definujeme pravidlo pro skupinu Marketing, které zakáže uživatelům této skupiny přístup k ovládacím panelům.

V Goup Policy Management si v doméně os1a.edu vyhledáme organizační jednotku management. V ní s následně vytvoříme nový GPO kliknutím pravým tlačítkem na danou OU a volbou *Create GPO in this domain and link it here…* (viz Obrázek 3).



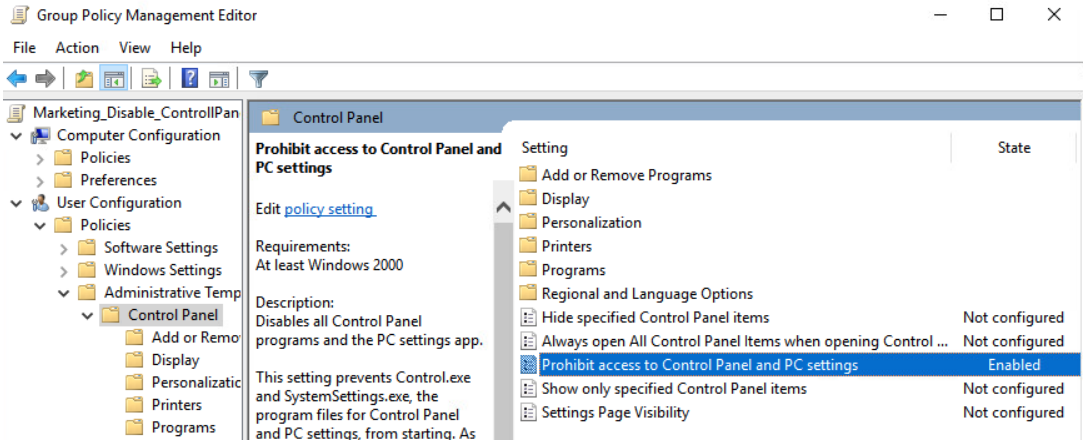
Obrázek 3: Vytvoření nové GPO v OU Marketing

Tu si následně pojmenujeme, tak abychom ji později dokázali identifikovat například:

Název GPO: *Marketing_disable_ControllPanel*

Následně volbou Edit přidáme GPO.

V *User Configuration* → *Policies* → *Administrative templates* → *Controll Panel* vyhledáme volbu *Prohibit access to Controll Panel and PC Settings* a změnou stavu na enabled toto pravidlo aplikujeme (Obrázek 4).



Obrázek 4: Zakázání ovládacího panelu

Zkontrolujte funkčnost pravidla tak, že se přihlásíme jako uživatel user001, který je členem skupiny Marketing. Pokud se nastavení neprojeví, vynutíme jej volbou *Enforce*.

V GPO Marketing nadefinujte tato pravidla pro uživatele:

Nastavte obrázek plochy na vámi preferovaný (např. Jellyfish):

User Configuration → Policies → Administrative Temaplates → Desktop → Desktop → Desktop Walpaper.

(Adresář s obrázky se nachází v C:\Windows\Web\Wallpaper)

Odeberte možnost zobrazení síťových připojení v nabídce Start

User Configuration → Policies → Administrative Temaplates Network → ProhibitTCP/IP advanced configuration

Odeberte správce úloh

System Ctrl + Alt + Del Options → Remove Task Manager

Nastavte automatické spuštění programu notepad po přihlášení k počítači

Computer Configuration → Policies → Administrative Templates → System → Logon → Run these programs at user logon
a do seznamu spouštěných programů přidejte notepad.exe.

Nastavte systémový čas počítače, aby využíval NTP server tik.cesnet.cz

Systém → Windows Time Service → Time Providers → Configure Windows NTP Client
a nastavte zadané NTP.

Zablokujte dědičnost na OU Marketing.

Označte OU Marketing a volbou Block Inheritance zablokujete dědičnost této OU.