Strategický rozvoj Univerzity Hradec Králové
CZ.02.2.69/0.0/0.0/16_015/0002427

Konfigurace GPO

Mgr. Josef Horálek, Ph.D.

Konfigurace GPO

Zadáním této úlohy je vytvoření a propojení objektů zásad skupin (GPO) ke vhodným OU.

V první části bude vytvořena zásada pro mapování sdíleného prostoru. Tento sdílený prostor bude představovat adresář Sdílené dokumenty vytvořený ve třetí úloze. Vytvořený objekt bude použit pro všechny uživatele domény kromě administrátorských účtů.

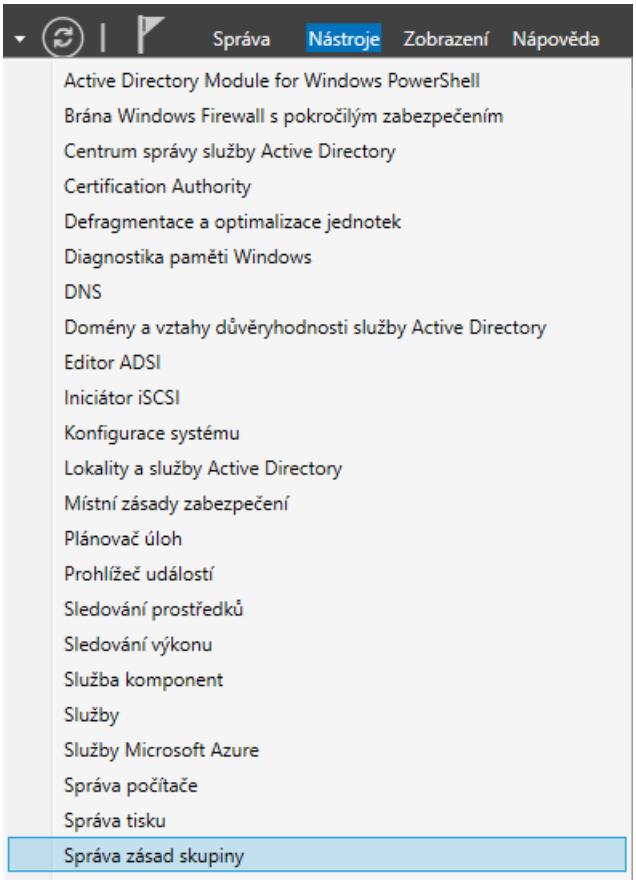
Ve druhé části budou nastaveny zásady skupin tak, aby existovaly v doméně tři typy uživatelských prostředí. Prvním z nich bude prostředí pro administrátory. Druhým bude prostředí pro školitele, kteří vystupují jako pokročilí uživatelé a mají běžná uživatelská oprávnění. Budou tak moci přistupovat např. k Ovládacím panelům a ke Správci úloh. Třetí typ bude představovat prostředí pro obchodní zástupce, kteří budou mít omezený přístup k ovládacím prvkům OS, jako je např. Správce úloh a Ovládací panely.

U objektů zásad skupiny je možné nadefinovat konfiguraci pro počítače, uživatele anebo kombinaci obou možností. Rozhodnutí, kterou z konfigurací použít, záleží na určení podmínek, za jakých budou dané GPO použity. V naší úloze budou vždy použity jen zásady pro uživatele. Každý GPO, který bude aktivně využíván, je potřeba propojit s objektem domény. V prostředí této domény budou zásady svázány s organizačními jednotkami.

Mapování síťových disků

V této části úlohy bude vytvořen GPO objekt, který bude zajišťovat mapování síťového disku se sdílenými dokumenty. Vytvořená jednotka bude označena písmenem „S“ a bude na ni použita akce aktualizace. Tzn. v případě, že síťová jednotka není u klienta připojena, automaticky se připojí, a v případě, že jednotka s označením „S“ existuje, bude přepsána těmito sdílenými dokumenty.

Vytvoření nového GPO objektu je možné za pomoci Správce serveru, kde se v **Nástrojích** nachází modul pro **Správu zásad skupiny**.

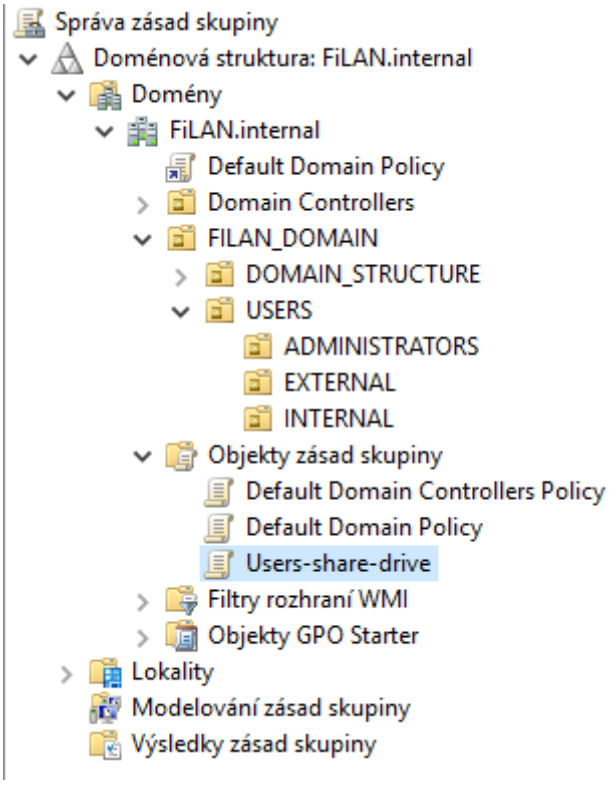


Obr. 1 Správa zásad skupiny ve Správci serveru

V tomto modulu je zobrazena hierarchie domény a adresář Objekty zásad skupiny. Do tohoto adresáře jsou automaticky přidány všechny existující GPO. Ve výchozím stavu jsou obsahem pouze Default Domain Policy a Default Domain Controller Policy.

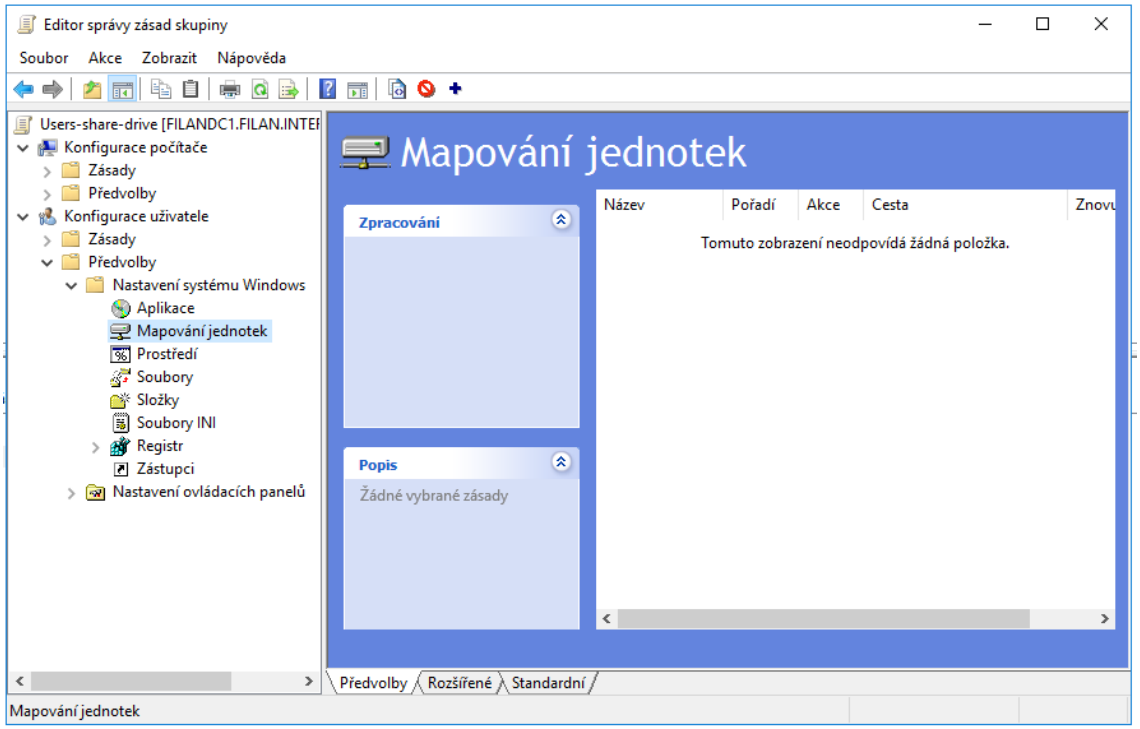
Každý nový objekt by měl být pojmenován vhodným názvem, který ho bude jasně identifikovat, a měl by obsahovat pouze potřebná nastavení. Objekt **Default Domain Policy** by měl obsahovat pouze nastavení účtů, hesel, uzamykání a zásady protokolu Kerberos. Tyto zásady jsou použity na úrovni celé domény a jsou tak aplikovány na všechny uživatele a počítače. Objekt **Default Domain Controller Policy** je používán pro konfiguraci uživatelských oprávnění a politik auditování. (10)

V naší úloze bude vytvořena zásada s názvem **Users-share-drive**, která bude umístěna v adresáři pro Objekty zásad skupiny. Vytvoření je možné za pomoci PTM.



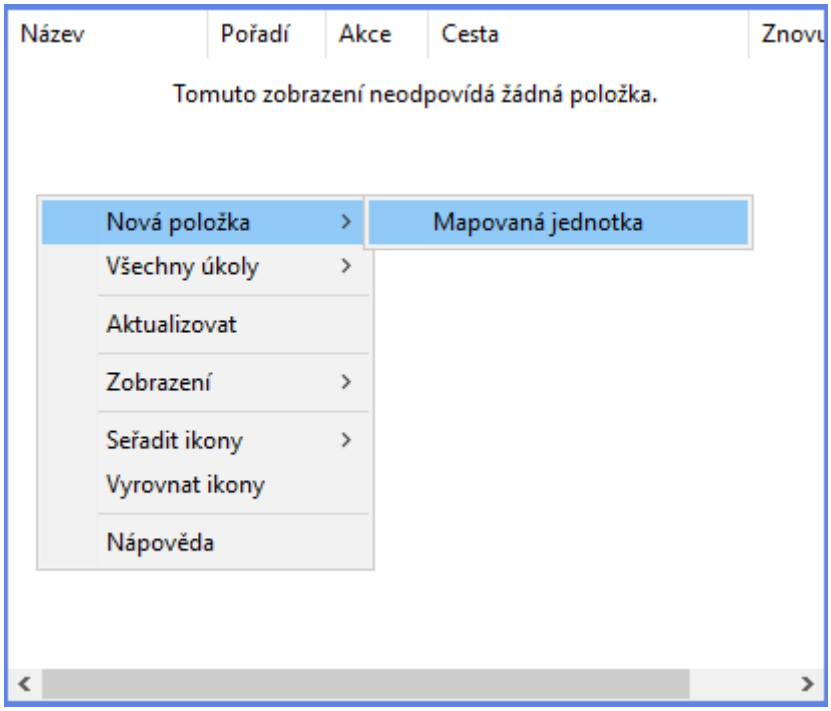
Obr. 2 Vytvoření GPO

Každé vytvořené zásadě je potřeba určit, jaké činnosti bude vykonávat. Určení lze provést znovu za pomoci použití PTM. Po tomto kroku je zobrazen Editor správy zásad skupiny, ve kterém bude vybrána vhodná zásada nebo předvolba. V našem případě se jedná o předvolbu nastavení systému Windows, kde bude zvoleno mapování jednotek.



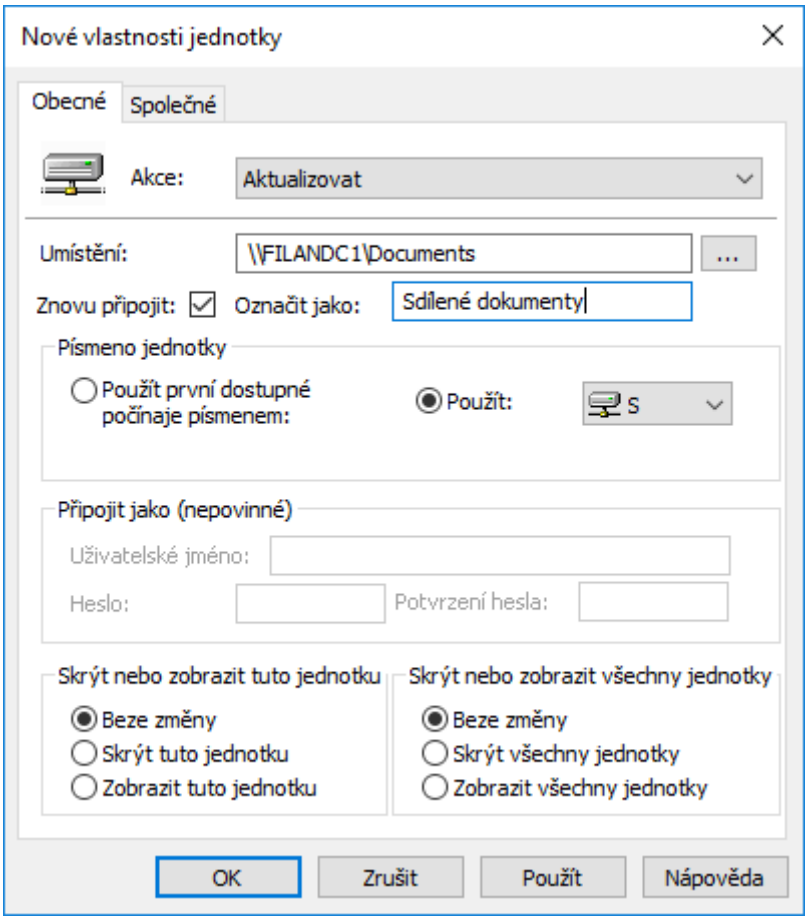
Obr. 3 Editace GPO

Nová jednotka bude vložena také za pomoci PTM.



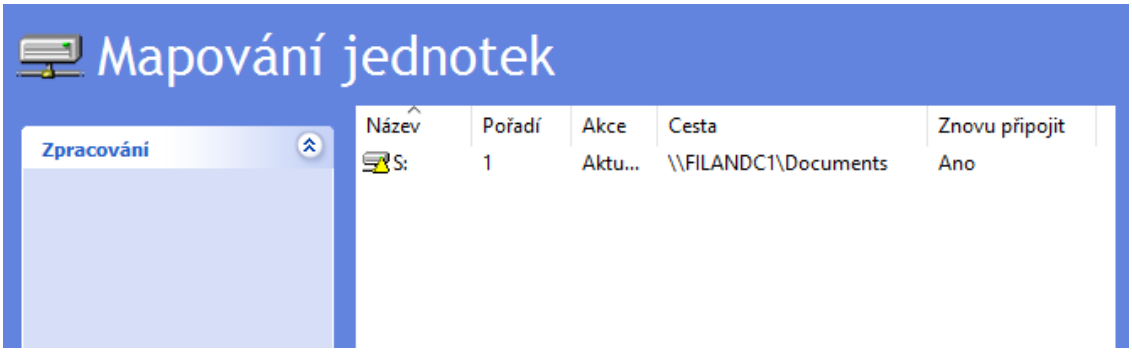
Obr. 4 Nastavení mapování jednotky pomocí GPO

Ve vlastnostech jednotky budou určeny parametry sdíleného disku. V naší úloze se jedná o cestu umístění \\FILANDC1\Documents. Tento sdílený adresář ponese název **Sdílené dokumenty** a bude označen ke znovu připojení v případě odpojení. Označením této jednotky je písmeno „S“. Akce, která bude vykonána při použití tohoto pravidla, bude **Aktualizace**, dle zadání úlohy.



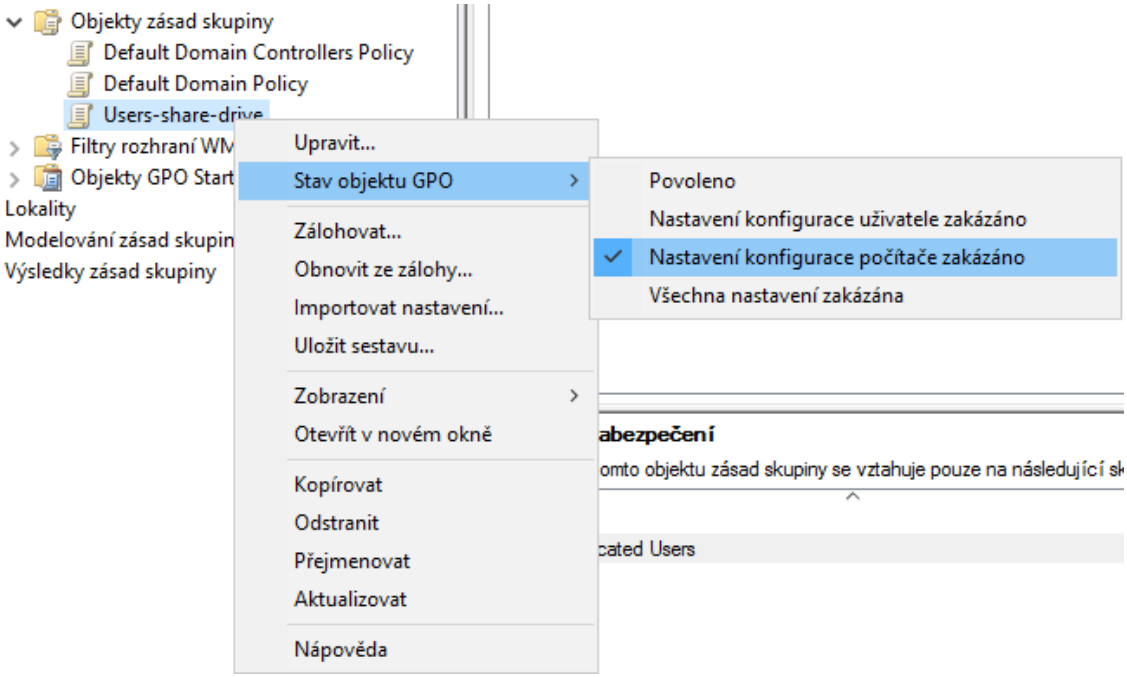
Obr. 5 Vlastnosti mapované jednotky

Po vytvoření této jednotky je zobrazen stav, jako na Obr. 54. Stejným způsobem je možné přidat libovolné množství jednotek.



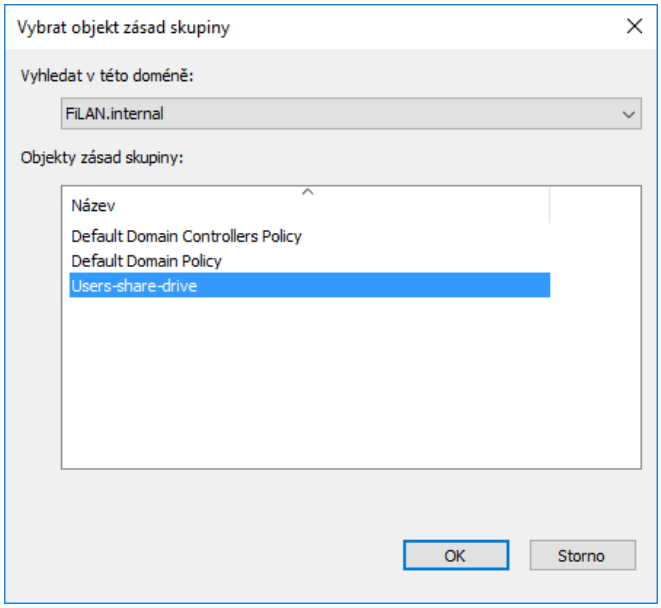
Obr. 6 Mapovaná jednotka S:

V případě, že je u GPO objektu použita konfigurace jen pro uživatele, je vhodné zakázat konfiguraci pro počítače. To samé platí i v opačném případě. Důvodem je rychlejší zpracování GPO.

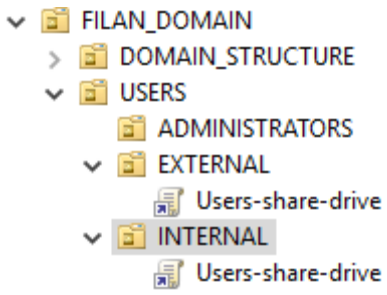


Obr. 7 Konfigurace stavu objektu GPO

Objekt zásad skupiny je vytvořen a zbývá ho propojit ke vhodné OU. Propojení je možné kliknutím PTM na požadovanou OU. V našem případě budou použity OU EXTERNAL a INTERNAL.

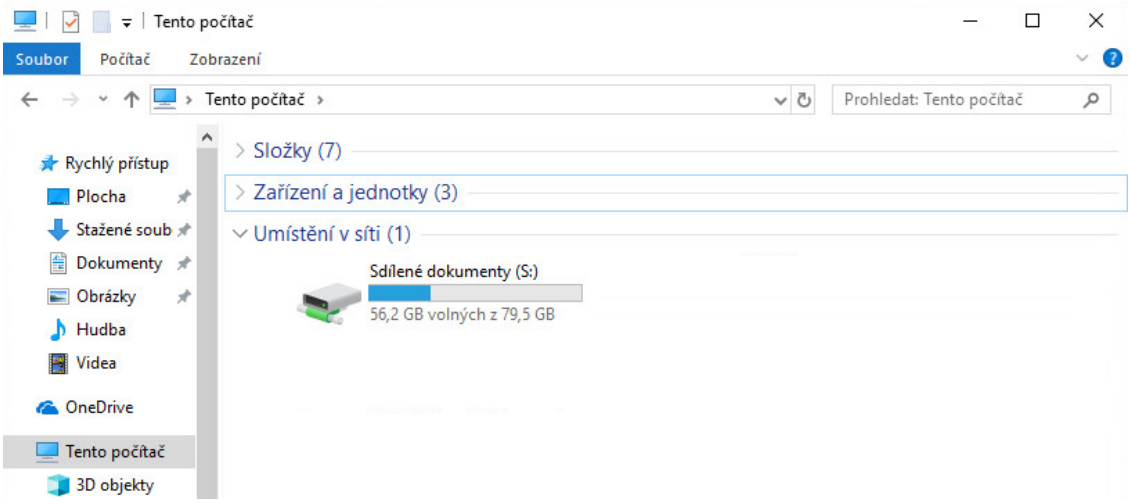


Obr. 8 Propojení GPO s OU



Obr. 9 Výsledek správného propojení GPO s OU

Obě OU by měly být uvedeny jako použitý obor u objektu Users-share-drive. V tuto chvíli je objekt správně nastaven a každému uživateli, kromě administrátorů, se po přihlášení ke svému doménovému účtu, automaticky připojí síťová jednotka.

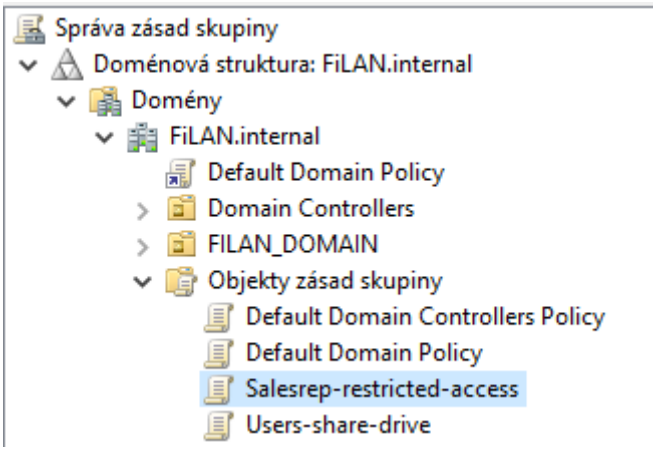


Obr. 10 Automaticky připojený sdílený adresář u klienta

Nastavení uživatelského prostředí

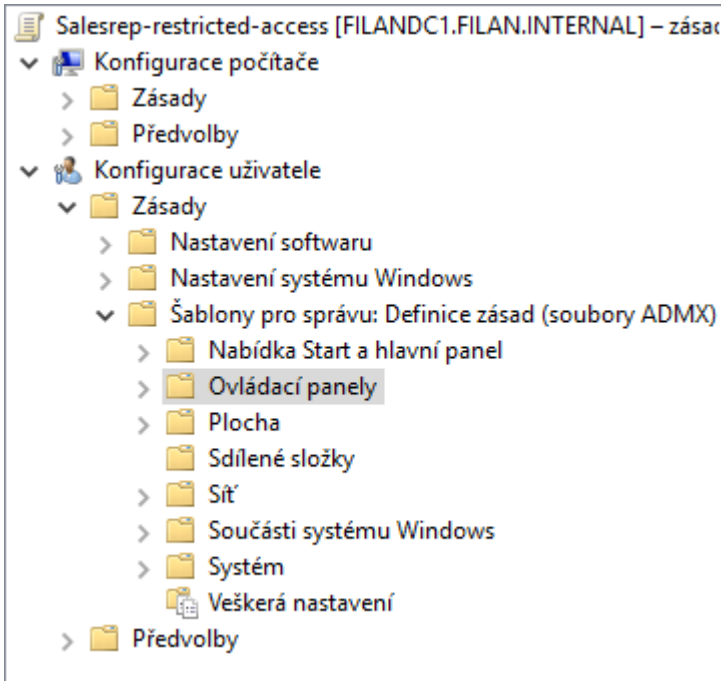
Tato část úlohy je věnována konfiguraci uživatelského prostředí. Zadáním úlohy je vytvořit prostředí pro účty obchodních zástupců, kteří využívají počítače pouze pro vyřizování obchodních aktivit a k absolvování školení. Z těchto důvodů není potřeba, aby měli tito uživatelé přístup k ovládacím prvkům OS Windows. Požadované omezení lze zajistit za pomoci GPO.

Prvním krokem bude, jako v úloze 4.4.1, vytvoření nového objektu GPO. Objekt bude nést název **Salesrep-restricted-access**.



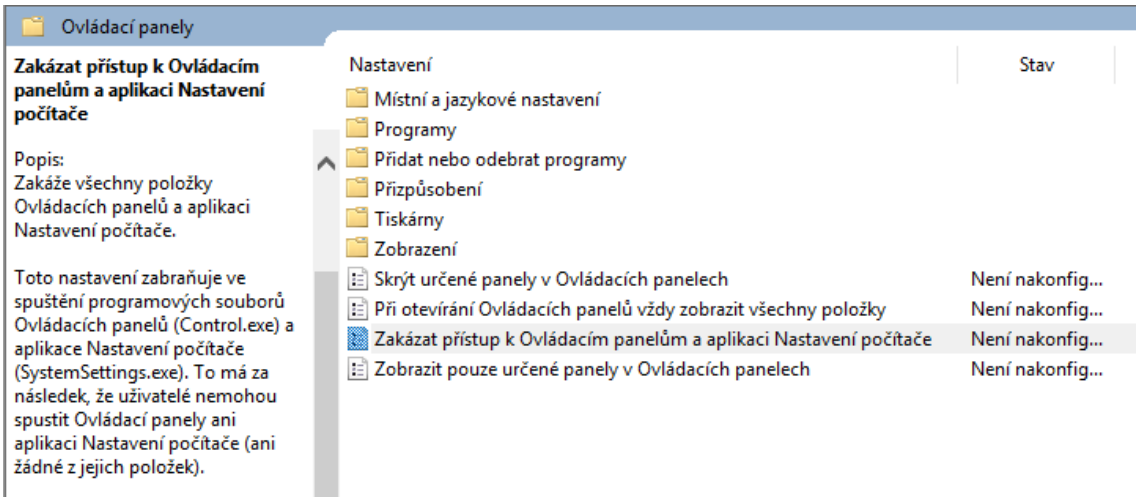
Obr. 11 Vytvoření GPO Salesrep-restricted-access

V editoru správy zásad skupiny bude znovu použita konfigurace uživatele, kde dojde nejprve k editaci **zásad pro Ovládací panely**. Tuto volbu je možné nalézt v sekci Šablon pro správu.



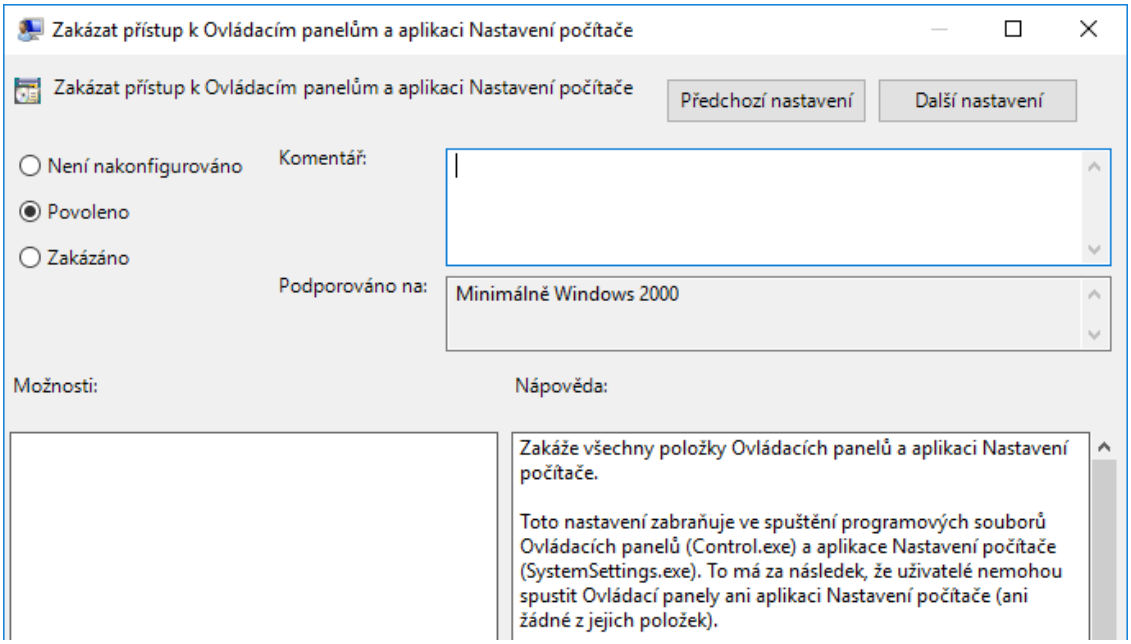
Obr. 12 Konfigurace uživatelských zásad

Dále bude vybrána možnost **Zakázat přístup k Ovládacím panelům a aplikaci Nastavení počítače**. Jak už název napovídá, dojde k zákazu Ovládacích panelů a Nastavení. Pokud by chtěl uživatel k těmto položkám přistoupit, zobrazí se mu oznámení o odepřeném přístupu.



Obr. 13 Nastavení omezení přístupu k Ovládacím panelům

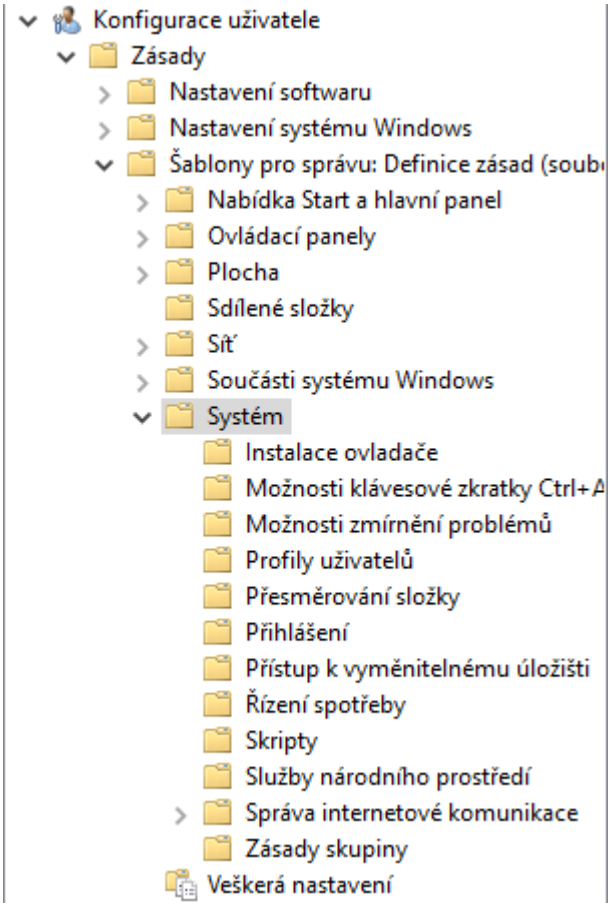
Ve výchozím stavu není zásada nakonfigurována a je potřeba ji povolit. Povolení je možné nastavit v její editaci.



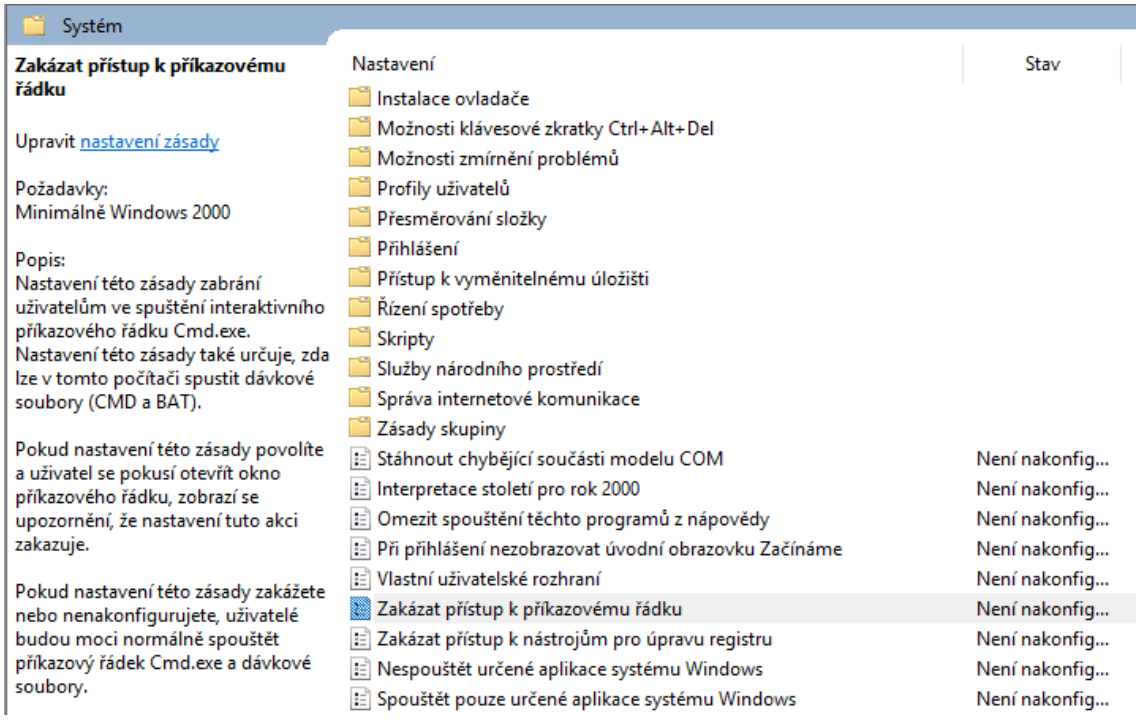
Obr. 14 Povolení zásady

Jakmile bude nastavena konfigurace pro Ovládací panely, přichází na řadu **Zakázání přístupu k příkazovému řádku**. Stále se jedná o objekt Salesrep-restricted-access.

V Šablonách pro správu se nachází větev Systém, ve které je umístěna zásada pro zakázání přístupu k příkazovému řádku.

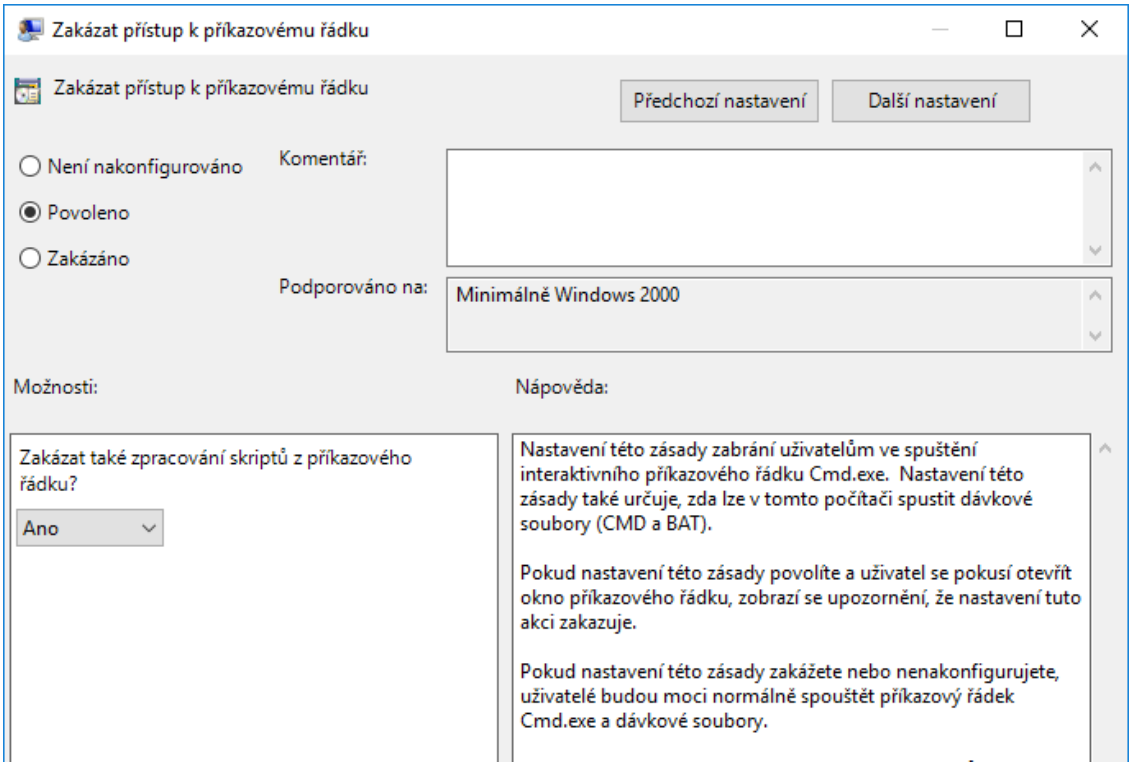


Obr. 15 Umístění zásady zakázání příkazového řádku



Obr. 16 Zakázání přístupu k příkazovému řádku

V editoru této zásady je potřeba znovu provést povolení a dodatečně zakázat zpracování skriptů z příkazového řádku, kvůli vyšší úrovni zabezpečení.

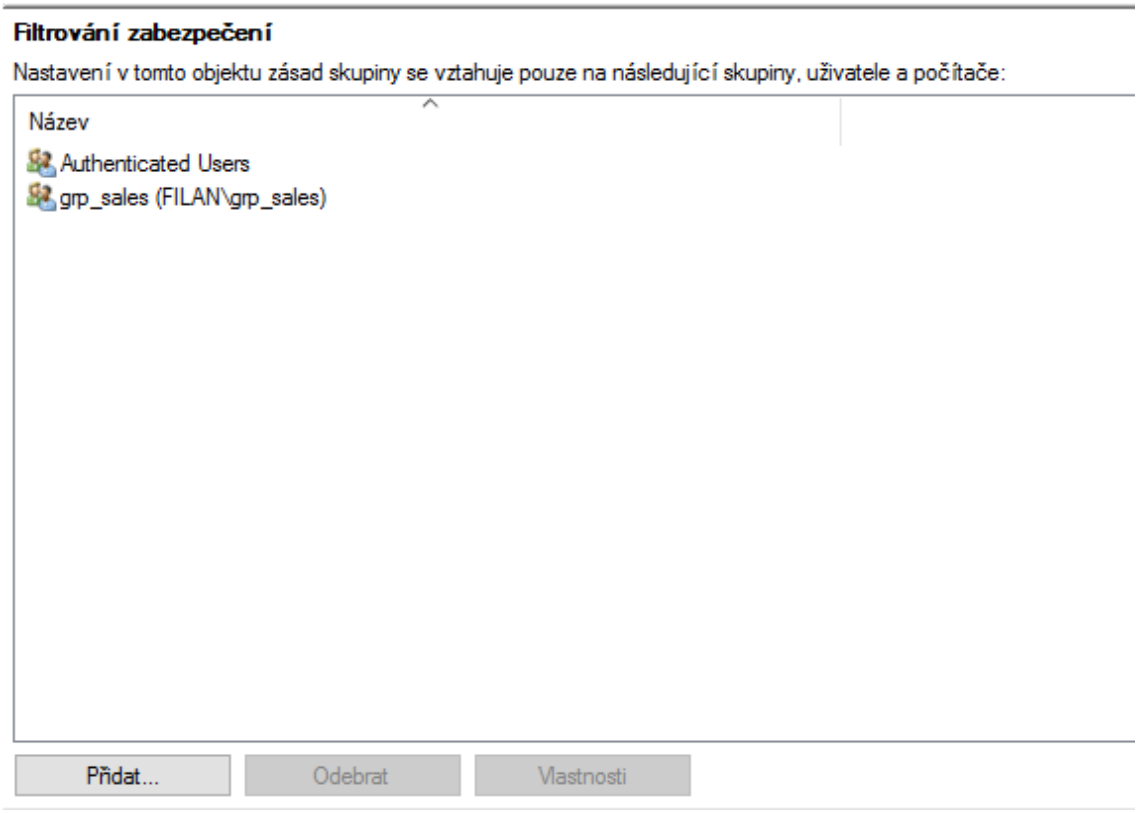


Obr. 17 Povolení zásady

GPO objekt je v tuto chvíli nakonfigurovaný. Nastává fáze vytvoření propojení s vhodnou OU.

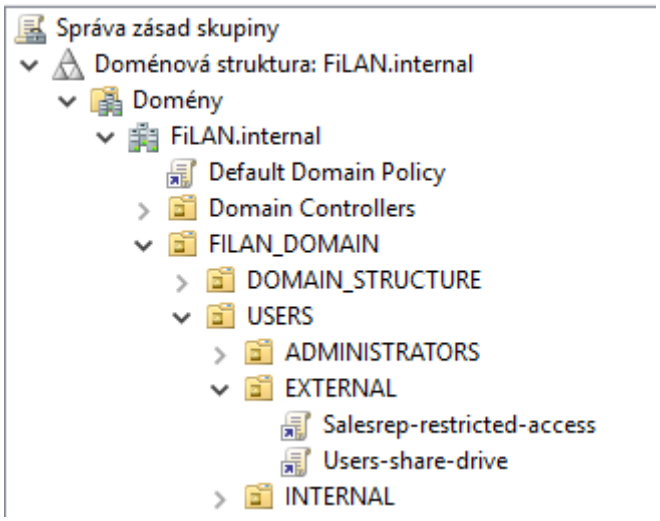
Tento objekt by měl být propojený s OU EXTERNAL, jelikož se v ní nachází účty obchodních zástupců. Propojení s OU SALES by nemělo smysl, protože se v ní nachází pouze skupina pro obchodní zástupce – grp_sales – a ne uživatelské účty.

Aby nedošlo k omezení přístupu k ovládacím prvkům pro všechny uživatele v OU EXTERNAL, je potřeba nastavit filtrování zabezpečení. Do filtru bude přidána skupina grp_sales a nastavená pravidla se budou vztahovat jen na uživatele, kteří jsou členy této skupiny.



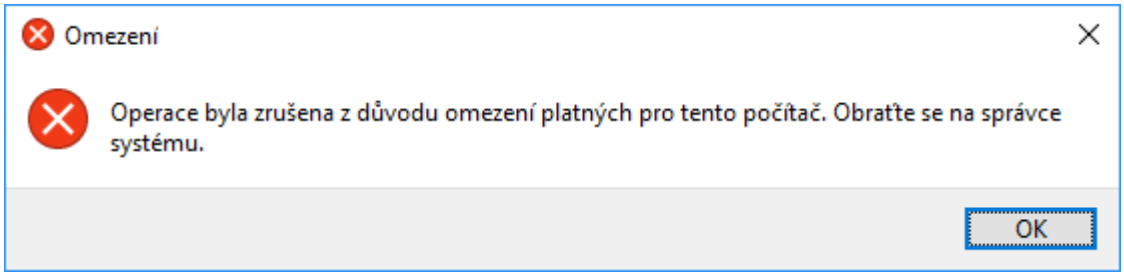
Obr. 18 Filtrování zabezpečení GPO

Po nastavení filtru zbývá jen provést propojení s OU EXTERNAL stejným způsobem jako u objektu Users-share-drive.

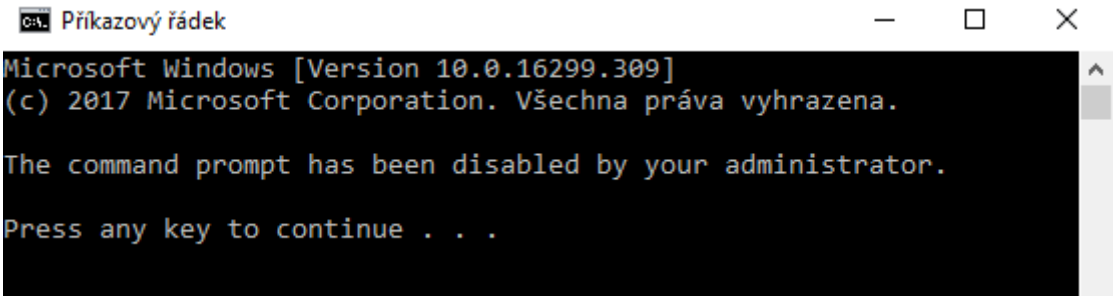


Obr. 19 Aplikace GPO Salesrep-resticted-access

V případě, že uživatel spustí Ovládací panely anebo Příkazový řádek, bude mu odepřen přístup a zobrazeny výstražné hlášky.



Obr. 20 Omezení přístupu k Ovládacím panelům u klienta



Obr. 21 Omezení přístupu k příkazovému řádku u klienta