Univerzita Hradec Králové

Fakulta informatiky a managementu

Katedra informatiky a kvantitativních metod

Efektivní návrh služby Active Directory pro potřeby středně velké firmy

Bakalářská práce

Autor: Filip, Antoš
Studijní obor: Aplikovaná informatika, kombinovaná forma

Vedoucí práce: Mgr. Josef Horálek, Ph.D.

Hradec Králové listopad 2018

Prohlášení:

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně a s použitím uvedené literatury.

V Hradci Králové dne 12.11.2018 Filip Antoš

Poděkování:

Děkuji vedoucímu bakalářské práce panu Mgr. Josefu Janu Horálkovi, Ph.D. za ochotu, metodické vedení práce a připomínky při jejím zpracování.

Anotace

Cílem bakalářské práce je představení logické struktury služby Active Directory (AD) spolu se službou DNS pro potřeby středně velké firmy.

V teoretické části bude uvedena samotná technologie a její hlavní komponenty, které představí princip fungování AD. Dále budou uvedeny vlastnosti služby DNS a její vztah s Active Directory. Na závěr teoretické části budou prezentovány konkurenční systémy a jejich základní vlastnosti.

Praktická část se bude zaměřovat na aplikaci získaných poznatků na praktických úlohách, ke kterým bude použito prostředí Windows Server 2016. Doména AD bude implementována na virtuálních serverech. Výstupem praktické části bude step-by-step postup konfigurace AD, který bude využitelný pro studenty předmětu OS1.

Klíčová slova:

Active Directory, instalace domény Windows, Group Policy Objects, DNS

Annotation

Title: The effective implementation of Active Directory services in environment of medium-sized business

The aim of the Bachelor Thesis is to present the logical structure of AD service together with DNS service for needs of medium-sized companies.

In the first part of the thesis there will be present the main idea of the AD technology and its components for demonstration of its functionality. At the same level there will be part about DNS which is necessary for domain functionality.

Practical part is about implementation in real environment of Windows Server 2016. Final output of practical part will be step-by-step instructions that can be used by students of OS1 subject.

Keywords:

Active Directory, Windows domain installation, Group Policy Objects, DNS

Obsah

Seznam obrázků

1 Úvod

Cílem práce je návrh logické struktury Active Directory pro potřeby středně velké firmy. V návrhu je zahrnuto i nastavení služby DNS a aplikace pravidel zásad zabezpečení. Práce je určena jako step-by-step návod k využití při laboratorních úlohách předmětu OS1. Návrh struktury Active Directory je určen pouze pro prostředí Windows domény.

K úspěšnému splnění cíle práce je potřeba mít určité předpoklady, mezi které patří alespoň základní znalost služby Active Directory a DNS. Obě tyto služby budou pro jejich správné pochopení představeny v teoretické části bakalářské práce.

V kapitole o Active Directory je nejprve vysvětlen základní princip fungování této služby a možnosti jejího uplatnění při nasazování v reálném prostředí. Dále je potřeba porozumět, ze kterých komponent se AD skládá, a jaké je jejich využití. Tyto informace budou představeny v jednotlivých podkapitolách stejně jako Group Policy Objects (GPO), které jsou využívány k řízení objektů. Pro lepší orientaci budoucích administrátorů v produktech nabízejících adresářové služby, bude uvedeno pár konkurenčních systémů.

V teoretické části se zabýváme také službou DNS, která je nezbytnou součástí AD. Bez této služby nemůže AD fungovat. Stejně jako v případě služby AD, budou představeny její základní vlastnosti a principy fungování.

Praktické úlohy se skládají ze zadání nastiňující problematiku, která bude v každé z nich řešena. Dělení je do 6 základních úloh, které mají své další podúlohy. Zadání zahrnuje vytvoření a instalaci domény, tvorbu hierarchie domény, sdílení souborů a řízení přístupů k nim, konfiguraci GPO, konfiguraci DNS a nastavení základního auditování. Po uvedení do dané situace bude popsán postup k realizaci řešení včetně ilustračních obrázků. Úlohy jsou prováděny v prostředí MS Windows Server 2016 Essentials a MS Windows 10 Professional.

Bakalářská práce obsahuje spoustu odborných termínů v českém i anglickém jazyce. Pro zdůraznění některých z nich je použito tučné písmo.

Veškerá ilustrace je dílem autora bakalářské práce.

2 Úvod do Active Directory

2.1 Co je to AD a k čemu slouží

Active Directory je adresářová služba. Pod pojmem adresářová služba si můžeme představit skupinu aplikací, které organizují informace o počítačích, uživatelích, skupinách a dalších zdrojích v počítačové síti. Tyto získané informace jsou zprostředkovávány správcům AD, uživatelům, aplikacím apod. a jsou uloženy v *„centrální organizované databázi (databáze informací o objektech a jejich vzájemných vztazích)“* (1). AD je založena na principu fungování síťového protokolu LDAP[1], kde je jeho funkčnost jednou z nezbytných součástí.

„AD je adresářová služba od společnosti Microsoft založená na LDAP. V současné době je nejpoužívanější adresářovou službou. Hlavní cíl AD je ověřovat uživatele a počítače vůči doméně a spravovat politiky členských počítačů, …“ (1)

V roce 1999 byla služba Active Directory, od společnosti Microsoft, poprvé představena a její první implementace byla uvedena v operačním sytému Windows 2000 Server. V následujících verzích Windows serverů byla postupně vylepšována funkčnost a správa služby Active Directory.

Od verze Microsoft Windows Server 2008 je pro Active Directory používán název Active Directory Domain Services (ADDS). Od této verze systému je oproti předchozím verzím poskytována minimalistická instalace serveru tzv. Server Core, která představuje minimální nutnou konfiguraci pro samotný běh OS. Windows Server umožňuje doinstalování rolí, ve kterých bude server vystupovat pro okolní svět. Když se řekne Active Directory, je obecně myšlena role Microsoft Windows Server – Active Direcory Domain Services (ADDS). Každá taková role serveru

[1] LDAP (Lightweight Directory Access Protocol) je definovaný protokol pro ukládání a přístup k datům na adresářovém serveru. Podle tohoto protokolu jsou jednotlivé položky na serveru ukládány formou záznamů a uspořádány do stromové struktury (jako ve skutečné adresářové architektuře).

se skládá ze služeb, které obsahují funkce. Je potřeba zmínit, že pod název AD patří i další služby, kterými jsou:

- ADDS – Služby domén Active Directory (Active Directory Domain Services)
- ADCS – Služby certifikátů Active Directory (Active Directory Certificate Services)
- ADFS – Služby federace Active Directory (Active Directory Federation Services)
- ADLDS – Active Directory Lightweight Directory Services
- ADRMS – Active Directory Rights Management Services

Hlavním úkolem AD je ověřování uživatelů a počítačů v doméně a správa politik na ně aplikovaných. AD je tvořena objekty, které představují počítače, uživatelské účty, skupiny apod. V současné době patří AD mezi nejpoužívanější adresářovou službu. (1)

2.2 Možnosti využití AD

AD můžeme využít v každém prostředí, ve kterém je zajištěn správný síťový provoz a je vyžadován přístup 24/7[2]. Taková prostředí mohou představovat firemní organizace, nemocnice, správní instituce apod., ve kterých často dochází ke změnám uživatelů a používaných zařízení. AD dokáže zajistit jejich efektivní správu při vysoké úrovni zabezpečení. Další z hlavních výhod je, že nemá žádné omezení na velikost lokality, kterou má pokrýt.

2.3 Komponenty AD

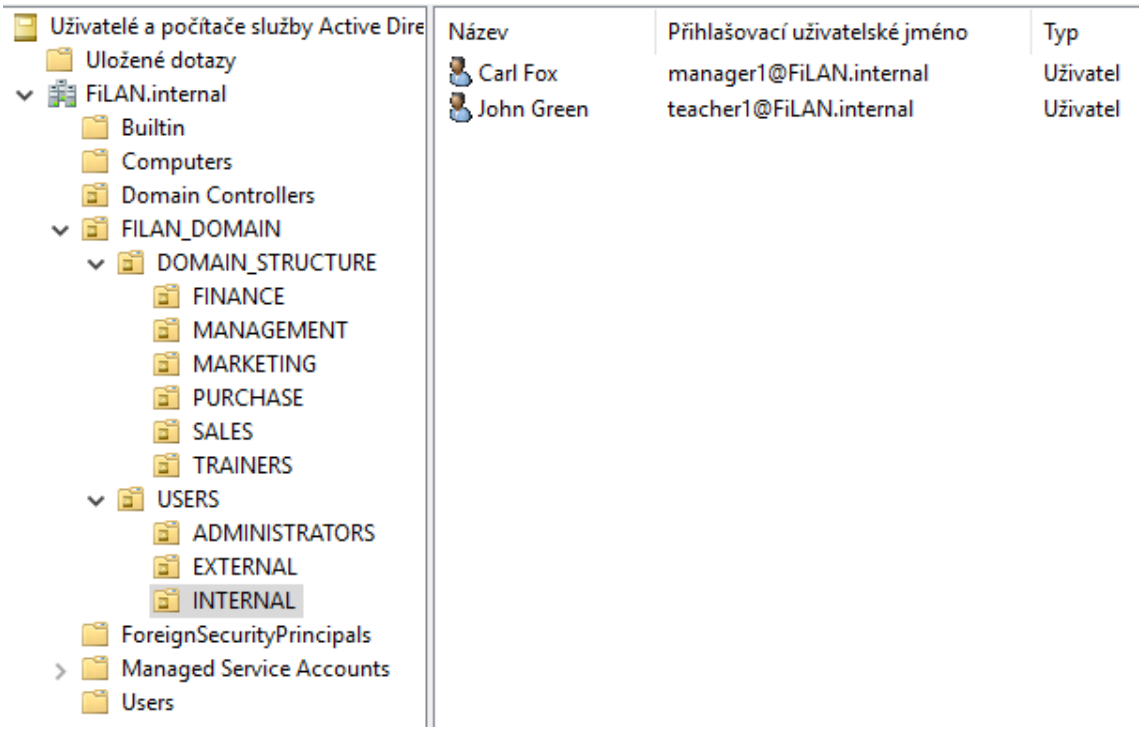
Active Directory je dělena dle dvou základních kritérií – logická struktura a fyzická struktura.

Logická struktura je používána, aby byla správně chápána organizace domény a doménových zdrojů. Na logické úrovni je vytvořeno hierarchické uskupení.

[2] 24/7 = provoz 24hodin, 7 dní v týdnu

Správně vytvořená logická struktura by měla odrážet skutečnou situaci prostředí, ve kterém je aplikována. Její nejmenší jednotkou je objektový list (Leaf Object), což je objekt, který nemá žádné další „potomky“. Jako Leaf Object je možné si představit např. konkrétního uživatele, počítač nebo tiskárnu.

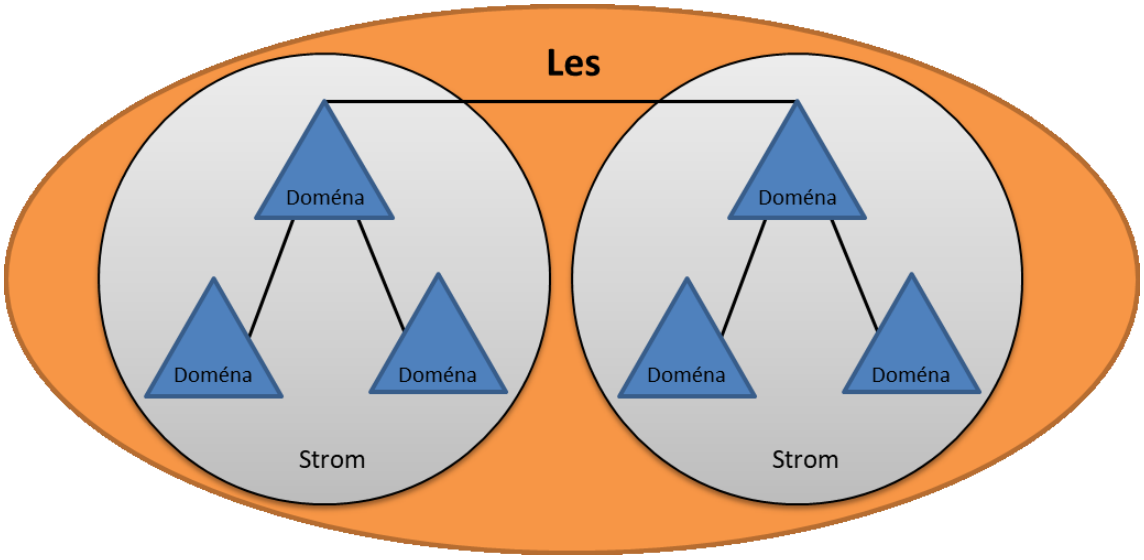
Fyzickou strukturu představují fyzická zařízení, kterými jsou např. doménové kontroléry (DC), sítě a podsítě (site) (2)



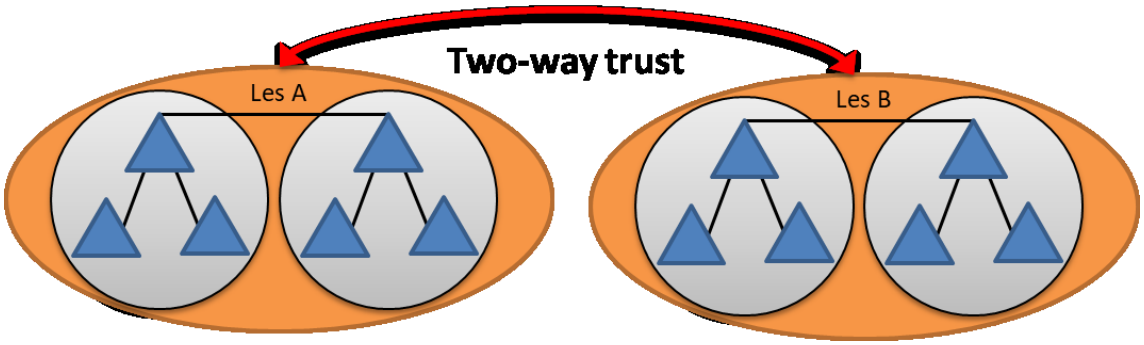
Obr. 1 Ukázková reprezentace logické struktury

2.3.1 Les

Les je objektový kontejner na nejvyšší úrovni v logické struktuře. Les představuje společný prostor pro jeho podřazené prvky. Pro existenci lesa je potřeba alespoň jednoho stromu. Zahrnuje v sobě domény, schémata, konfigurace a další informace. V lese je nejdůležitějším prvkem tzv. **Root Domain**, která představuje nejvyšší úroveň jmenného prostoru (**Namespace**) v rámci jednoho celého lesa. Každá doména v lese pracuje nezávisle, ale díky lesu je umožněna jejich vzájemná komunikace. V případě požadavků na vytvoření větší sítě je možné propojit více lesů vzájemně pomocí implicitního dvoucestného vztahu důvěry (**Forest Trust**). (3)



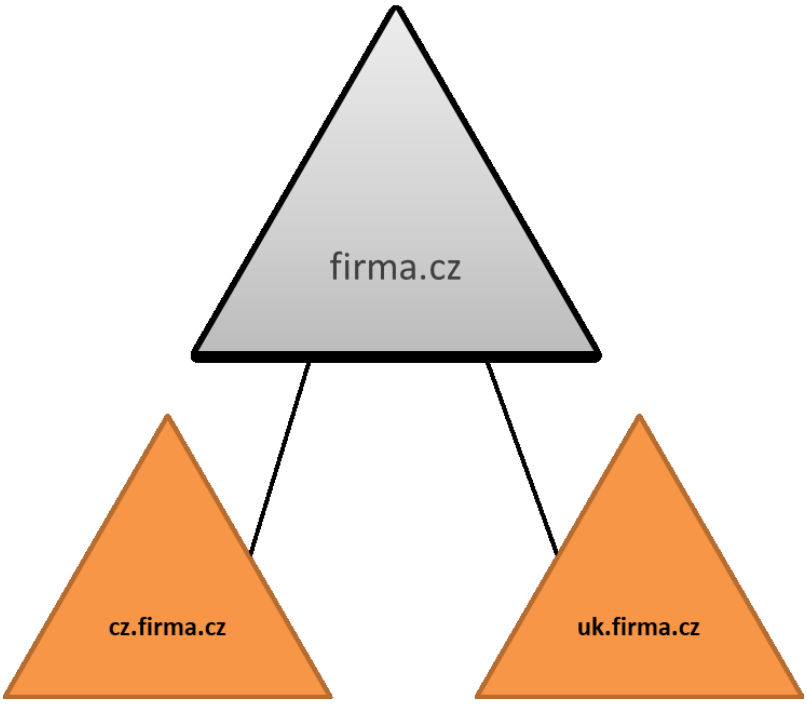
Obr. 2 Les



Obr. 3 Forest trust – propojení více lesů

2.3.2 Strom

Strom je objektový kontejner podřízený objektovému kontejneru les a nadřazený doméně. Každý strom patří do nějakého lesa. Strom může obsahovat libovolný počet domén nižšího řádu. Obrázek č. 4 vyobrazuje propojení rodičovské domény (Parent Domain) **firma.cz** s podřízenými doménami (Child Domain) **cz.firma.cz** a **uk.firma.cz**. Doména **firma.cz** je považována za kořenovou doménu (Root Domain). Domény v jednom stromě sdílí vlastní jmenný prostor. (3)

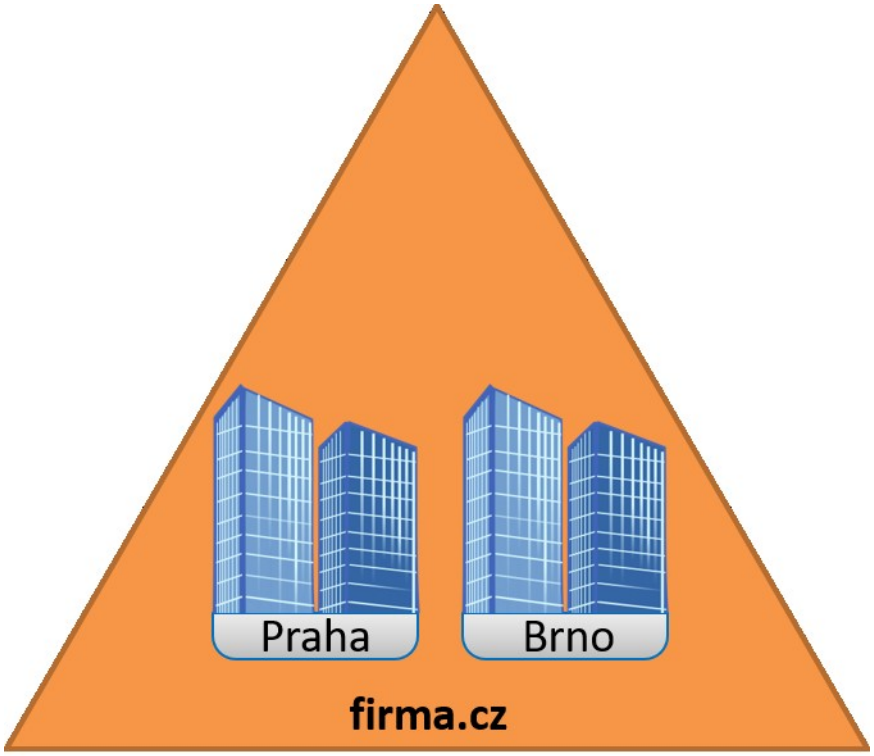


Obr. 4 Stromy domény

2.3.3 Doména

Doména je základní komponentou logické struktury AD. Je považována za administrativní a bezpečnostní hranici. V doméně jsou přímo uloženy objekty (může se jednat o milióny), které do ní patří. Každá doména má svou skupinu správců a ti mají plná práva nad každým jejím objektem. Oprávnění těchto správců se nevztahují na objekty mimo doménu. AD může být tvořena jednou nebo více doménami. V praxi se nejčastěji setkáváme s použitím pouze jedné domény. Doména není omezena na fyzickou lokaci a může tedy být geologicky nezávisle velká. Přístup k doménovým objektům je řízen pomocí ACL (Access Control List), které upravuje oprávnění přístupu k objektům. (3)

Demonstrace na Obr. 5 představuje doménu **firma.cz**, která má pobočky v Praze a v Brně. I přes to, že jsou tyto budovy od sebe velmi vzdálené, je možné, aby takovouto doménu spravovala jedna skupina administrátorů s kanceláří např. v Praze. Podobný příklad platí i pro uživatele z Brna, kteří mohou komunikovat s uživateli v Praze, protože jsou všichni členy jedné domény.



Obr. 5 Doména

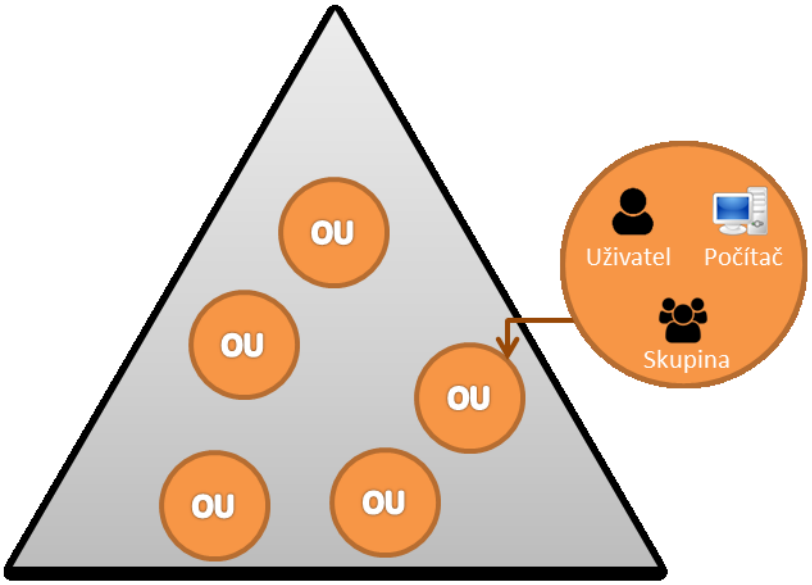
2.3.4 Organizační jednotka (OU)

Organizační jednotka je kontejner, který se uvnitř domény používá k seskupování/organizování objektů do logických administračních skupin. Důvodem k tomuto seskupování může být aplikace rozdílných politik přístupu, jelikož OU je nejmenší jednotka, na kterou můžeme delegovat administrační oprávnění. OU nemusí být vždy jen skupina objektů, ale i pouze jeden objekt (uživatel). (2)

„OU můžeme zanořovat do sebe a vytvářet libovolnou hierarchickou strukturu. Hierarchie OU je lokální uvnitř domény a neovlivňuje jiné domény.“ (3)

V praxi může organizační jednotka představovat jednotlivá oddělení v rámci dané společnosti. Pokud bychom jako příklad uvedli obchodní firmu, tak by sem určitě patřily OU pro vedení společnosti, oddělení financí, oddělení marketingu, nákupu, prodeje apod. Do těchto skupin by byli zahrnuti jednotliví zaměstnanci. V případě, že by některý ze zaměstnanců měl více funkcí, spadal by do více OU.

Příklad: Oblastní vedoucí, který vede skupinu obchodních zástupců, by byl v OU vedení společnosti a v OU svěřené skupiny obchodních zástupců.

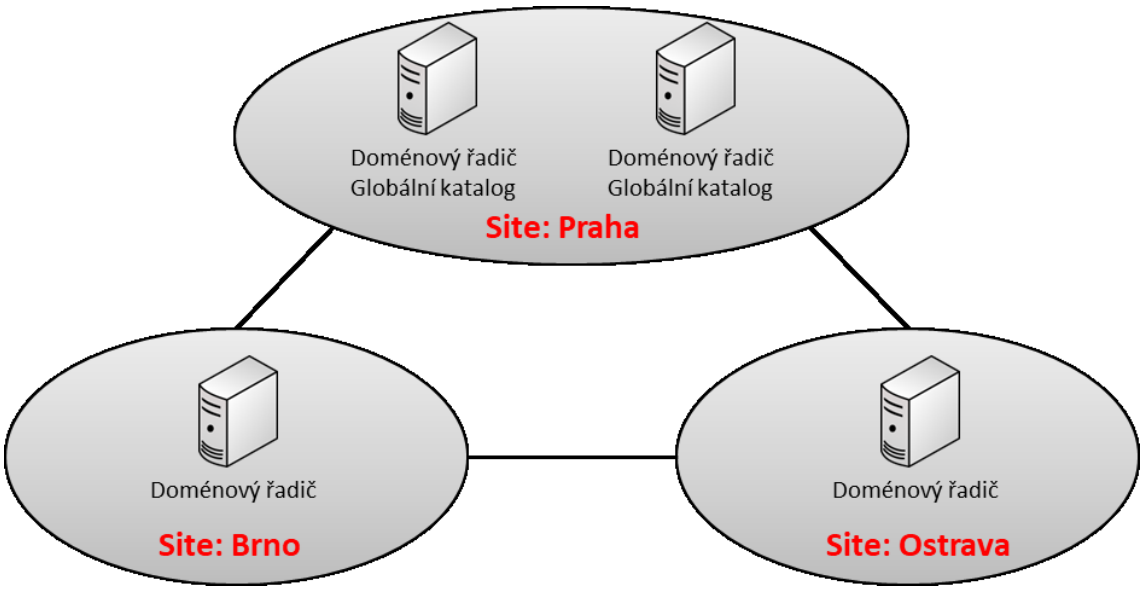


Obr. 6 Organizační jednotka

2.3.5 Site

Site = pobočka/lokalita. Sites představují fyzickou síťovou topologii, do které patří alespoň jedna podsíť (Subnet). Nová site je použita vždy, když zavádíme do domény novou lokalitu. V podstatě je vytvořena nová podsíť. Site zajišťuje replikaci dat mezi jednotlivými doménovými kontroléry/řadiči (Domain Controller). Replikace dat musí probíhat jak v rámci jedné site, tak i mezi ostatními, aby byl zajištěn konzistentní stav doménových řadičů.

„Site je kombinace jednoho nebo více IP subnetů, které jsou spojeny spolehlivými a rychlými linkami. Pokud máme více lokálních sítí (lokalit, poboček) spojených pomocí WAN sítě, tak se většinou vytváří site pro každou LAN.“ (3)



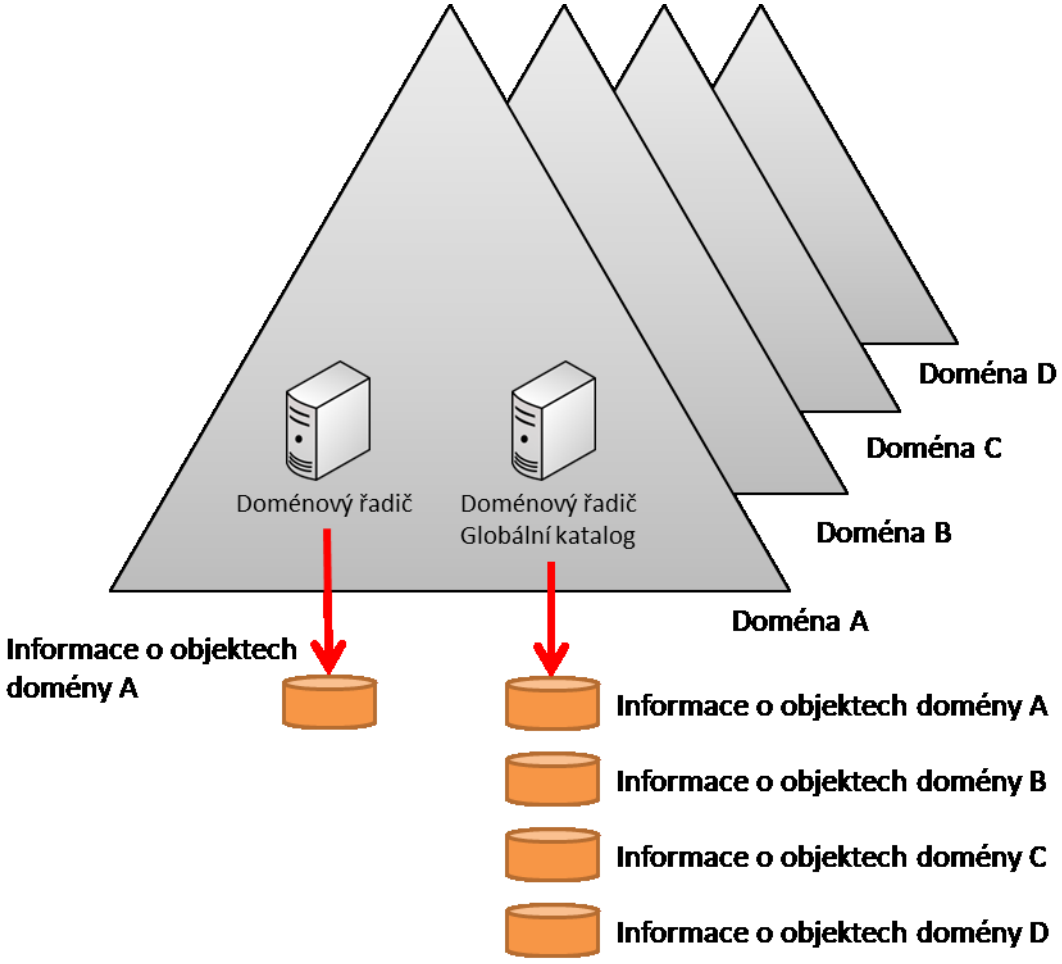
Obr. 7 Site – propojení více site/poboček

2.3.6 Globální katalog (GC)

Globální katalog je komponenta AD, která není součástí fyzické ani logické struktury. Hlavní funkcí GC je vlastnit základní informace o všech objektech v rámci celého lesa. (4)

Základními informacemi je myšleno uživatelské jméno (má tvar e-mailové adresy), lokace, telefon, e-mail, členství v univerzálních skupinách apod. V každé doméně musí být minimální jeden GC server, který je zároveň i doménovým řadičem. Jako GC server je automaticky vybrán prvně instalovaný DC v lese.

Představme si situaci, kdy máme les dvou a více domén, a chceme přistoupit k objektu z jiné domény. Všechny DC v doméně, ze které je přistupováno, mají informace pouze o objektech naší domény, uložené ve svém GC. Aby získaly informace o objektech z jiné domény, dotazují se právě globálního katalogu nadřazené domény nebo přímo lesa, který jim poskytne požadované základní informace.



Obr. 8 Globální katalog – schéma

2.4 Group Policy Objects (GPO)

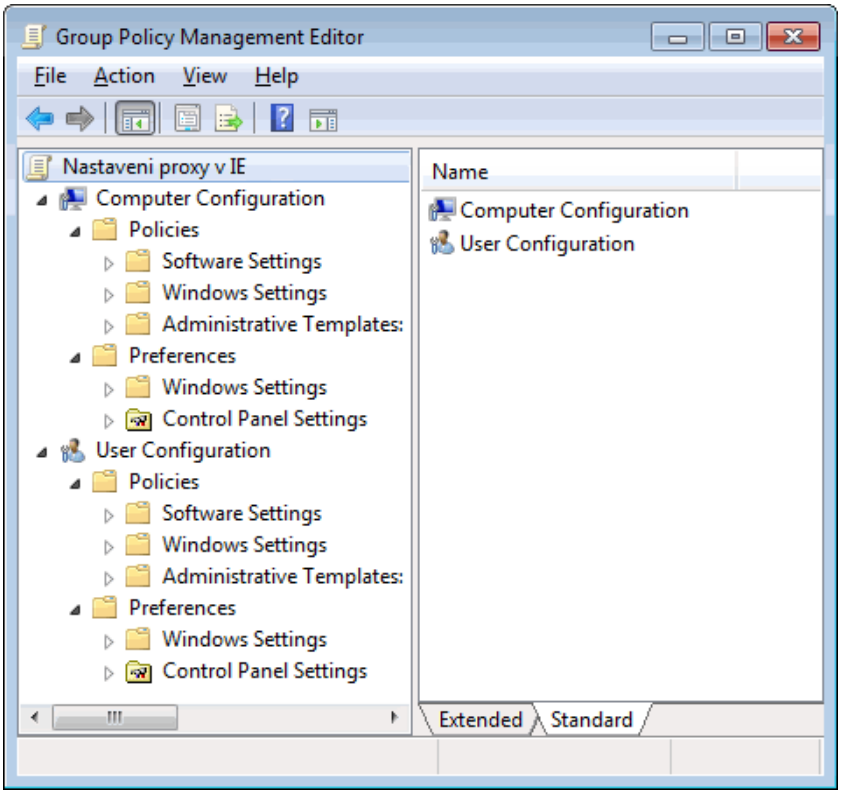
Se službou Active Directory souvisí také Group Policy Object. Jak píše autor webu SAMURAJ-cz.com Petr Bouška, definice GPO je: *„Group Policy (skupinové politiky) slouží k centrální správě počítačů s pomocí Active Directory. Hlavně se tedy využijí pro počítače zařazené do domény.“* (5) Jedná se o nástroj, kterým je řízeno chování objektů v doméně (počítače, skupiny, uživatelé apod.).

Oproti GPO je možné využít i lokální politiky (Local Group Policy), ale od těchto bude tato práce oproštěna.

Za pomoci editoru globálních politik (Group Policy Management Console) je administrátor domény schopen určovat širokou škálu nastavení objektů jako jsou např.:

- Politiky zabezpečení – pravidla hesel, uzamykání účtů apod.
- Politiky chování systémů – úprava plochy, zpřístupnění SW, nastavení zvuku
- Instalace SW
- Mapování síťových disků

GPO mají dvě hlavní části – konfigurace politik uživatelů a konfigurace politik počítače. Obě tyto části zapisují změny do registrů. Rozdíl je pouze ve větvi, kterou používají, a to buď HKEY_LOCAL_MACHINE (HKLM) anebo HKEY_CURRENT_USER (HKCU). Při použití konfigurace pro objekt počítače, jsou politiky aplikovány při jeho startu. Při aplikaci konfigurace pro uživatele jsou až při přihlášení uživatele. (5)



Obr. 9 Editor správy Group Policy

Aplikace GPO je provedena propojením (Link to) na některý z doménových kontejnerů (les, strom, doména…). Při použití politik platí pravidla dědění – podřízený kontejner dědí ze všech nadřazených – aplikována dle hierarchie v AD.

2.5 Jak funguje AD

Hlavním cílem AD je autentizace a autorizace objektů v doméně. Tuto činnost zajišťují tzv. doménové kontroléry (DC). Jsou to servery běžící na OS Windows Server. Každý DC může patřit vždy jen do jedné domény.

Doménové kontroléry bývají zpravidla minimálně dva v každé doméně. Důvodem je replikace doménového adresáře. Díky replikaci je zajištěna záloha domény v případě, že by některý ze serverů přestal fungovat.

AD je velmi úzce spjata se službou DNS a GPO. Služba DNS zajišťuje její funkčnost a GPO slouží k řízení přístupů.

„Aby AD správně fungovaly, je nutné mít funkční DNS server, pomocí kterého si pracovní *stanice a servery zjišťují umístění nezbytných služeb v síti (řadič domény, LDAP, KERBEROS, …)“* (1)

„K doméně AD se mohou připojit klientské systémy Windows pouze ve vyšších edicích (Enterprise, Professional, …)“ (1)

2.6 Konkurenční systémy

Na trhu můžeme nalézt i jiné systémy poskytující adresářové služby. Miroslav Pokorný uvádí na svém webu některé z nich. Můžou to být: eDirectory od firmy Novell, Open Directory od firmy Apple, Samba (emulace AD na operačním systému Linux) (1).

Rozdíly jsou především v tom, v jakém prostředí jsou implementovány. Dále pak pořizovací náklady a nároky na HW vybavení.

Jelikož Active Directory je proprietární software společnosti Microsoft, tak je její funkčnost nejlépe zajištěna ve spolupráci s dalšími produkty této firmy. Může se jednat jak o serverové, tak klientské systémy.

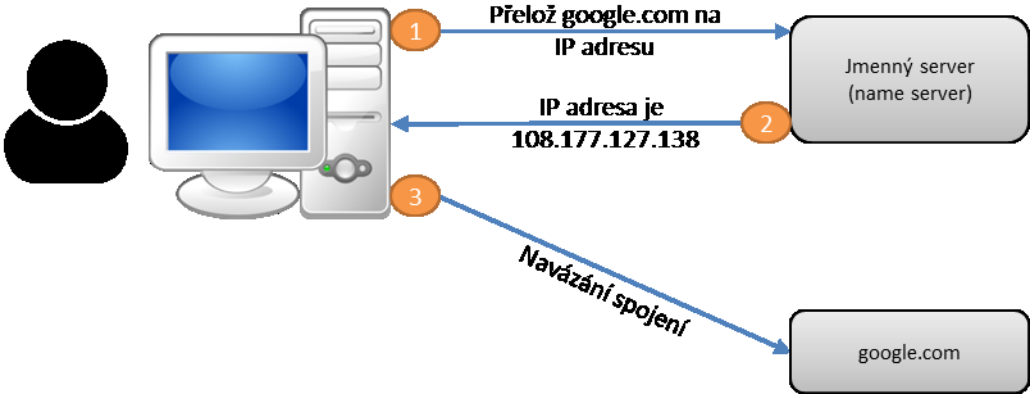
Naproti tomu jiné adresářové služby, jako např. Samba, můžou spolupracovat jak s produkty firmy Microsoft, tak se svobodnými OS typu Linux. Hlavní úskalí spočívá v náročnosti konfigurace a zajištění správné komunikace mezi jednotlivými systémy.

3 Domain Name System (DNS)

3.1 Co je DNS a k čemu slouží

Veškeré aplikace v síti Internet, zajišťující komunikaci mezi počítači, používají k identifikaci konkrétního síťového uzlu IP adresu. Pro člověka je IP adresa těžko zapamatovatelná a mnohem snadněji si dokáže zapamatovat nějaký název. Z tohoto důvodu je téměř každé IP adrese přiřazeno tzv. **doménové jméno**.

(6 str. 255) Další z výhod doménového jména je, že jedno doménové jméno může zastupovat více IP adres. Podmínkou pro adresaci pomocí doménových jmen je mít dostupný **jmenný server**. Jmenný server je síťový počítač, na kterém je aplikován Domain Name System (DNS). Jeho hlavní funkcionalitou je překlad doménových jmen na IP adresy a obráceně.



Obr. 10 Schéma překladu doménových jmen

Postupným vývojem se systém DNS, kromě pouhého překladu adres, začal používat také k doručování elektronické pošty nebo k IP telefonii.

„DNS (zkratka z anglického Domain Name System) je název pro protokol umožňující hierarchický systém doménových jmen. Součástí systému jsou také tzv. DNS servery, které uchovávají informace o spravovaných doménách a k nim příslušející záznamy.“ (7)

3.2 Jak funguje DNS?

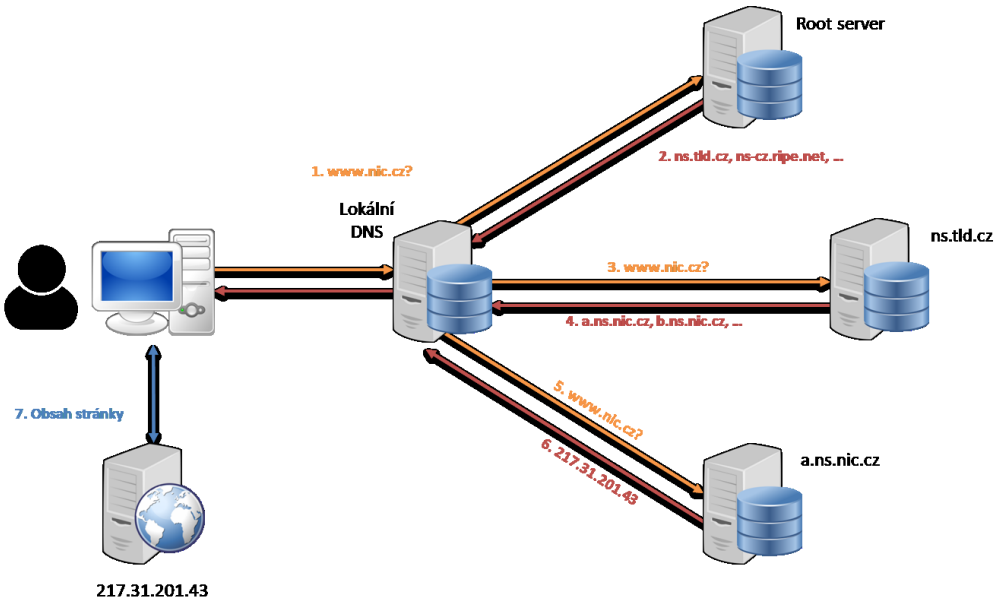
Systém DNS funguje obdobným způsobem jako telefonní seznam. Do telefonního seznamu jsou zapisována telefonní čísla a jména osob, které můžeme daným číslem kontaktovat. Stejně tak DNS přiřazuje k číselné IP adrese doménové jméno, které je uživatelsky lépe zapamatovatelné.

Pokud by existoval pouze jeden takový „telefonní seznam“, nastaly by problémy v případě stejných názvů, např. pro webové servery, e-mailové servery apod. Z tohoto důvodu byla do systému DNS zavedena určitá hierarchie.

Maximální délka celého doménového názvu je 255 znaků a každý jeden řetězec, který je oddělován vždy tečkou, má délku maximálně 63 znaků. Název může obsahovat pouze písmena, číslice a pomlčky. (6 str. 258)

Dle webu nic.cz funguje použití DNS v praxi následovně:

„Každý počítač má nastaven jmenný server, který používá pro překlad jmen. Když uživatel počítače použije jméno domény tím, že je napíše do řádku adresy ve webovém prohlížeči, počítač pošle dotaz, jaká IP adresa odpovídá tomuto jménu domény, jmennému serveru. Ten buď dotaz zodpoví přímo, pokud dotazované jméno domény zná, anebo dotaz předá dál, dalším jmenným serverům v doménovém stromu, viz následující příklad.



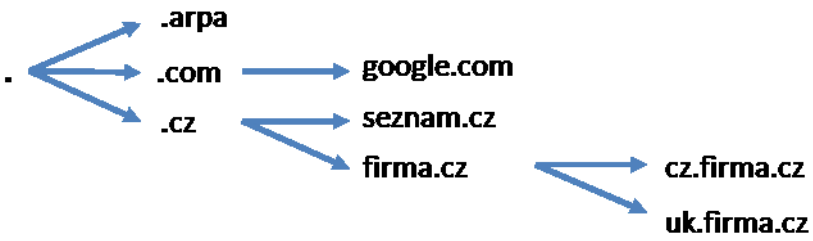
Obr. 11 DNS schéma

1. *Lokální DNS server se zeptá na jméno www.nic.cz některého z kořenových serverů*
2. *Ten odpověď nezná, ale jelikož zná alespoň kam je delegována doména .cz, pošle seznam jmenných serverů pro doménu .cz*
3. *Lokální DNS použije informaci od kořenového serveru a zeptá se jednoho z těchto serverů na jméno www.nic.cz*
4. *Server opět odpověď nezná, ale jelikož obsahuje informaci o všech subdoménách .cz, pošle nazpět informaci o tom, který další server obsahuje doménu nic.cz*
5. *Lokální server postupuje dále a zeptá se jednoho ze serverů, které poskytují doménu nic.cz, na jméno www.nic.cz*
6. *Dotázaný server obsahuje informaci o všech subdoménách nic.cz, takže www.nic.cz zná a pošle zpět odpověď, že jménu www.nic.cz odpovídá IP adresa 217.31.201.43*

Tuto adresu poskytne lokální DNS server zpět počítači uživatele. Ten se poté spojí s www serverem na příslušné adrese, stáhne obsah stránky a zobrazí jej uživateli na obrazovce.“ (8)

3.3 Úrovně DNS

Doménová jména se začala oddělovat pomocí tečkové notace, kterou jsou odlišovány jednotlivé úrovně hierarchie. Každá z těchto úrovní zná své potomky a svého rodiče.



Obr. 12 DNS úrovně

3.3.1 Root Domain

Doménové úrovně jsou číslovány od konce. Nejvyšší úroveň je samostatná tečka, která označuje tzv. kořenovou doménu (**Root Domain**). Znak tečky, používaný k označení této úrovně domény, se většinou v doménových názvech neuvádí.

3.3.2 Top Level Domain (TLD)

Další v pořadí následuje úroveň názvu nejvyšší úrovně tzv. **Top Level Domain**. Tato úroveň je dělena logicky do dvou skupin:

- „***Generické TLD (gTDL)**, které mají tři a více znaků: aero, asia, biz, cat, com, coop, info, jobs, mobi, museum, name, net, org, pro, tel, travel, gov, edu, mil, int a arpa.*
- ***Národní TLD**, které jsou dvouznakové. Tyto dva znaky jsou totožné s identifikací země podle normy ISO-3166. Anglicky se označují ccTLD (cc = Country Code). Pro Českou republiku tak máme doménu .cz, pro Evropskou unii máme doménu .eu atd*.“ (6 str. 257)

3.3.3 Second Level Domain (SLD)

Second Level Domain (úrovně druhého řádu) představují libovolný název domény. Těmito názvy mohou být např. google.com, seznam.cz, idnes.cz apod.

3.3.4 Úrovně třetího řádu a nižší

Na úrovni třetího a nižšího řádu se nejčastěji nachází různé aplikační a webové servery domén SLD. Např. mail.uhk.cz, oliva.uhk.cz, stag.uhk.cz apod.

4 Praktické úlohy

V počáteční fázi, kdy je rozhodováno o vytvoření domény v AD, je potřeba provést přípravu prostředí, ve kterém budeme Active Directory používat.

Prvním krokem je správná funkčnost počítačové sítě a příprava HW, na kterém bude služba AD implementována. V této bakalářské práci nebude popsáno, co vše je potřeba nastavovat na této úrovni, jelikož to není jejím cílem. Úlohy týkající se této práce budou realizovány v prostředí Windows Server 2016 Essentials a klientského OS Windows 10 Professional.

4.1 Úloha 1 – Vytvoření domény a instalace rolí AD a DNS

V první úloze nastává fáze vytvoření domény. K tomuto kroku je nutné mít nainstalované a správně nastavené role Active Directory Domain Services a DNS na doménových řadičích.

Zadáním této úlohy je instalace těchto rolí a vytvoření domény s názvem **FiLAN.internal**. V doméně budou použity minimálně dva doménové řadiče, kvůli zajištění správné replikace dat.

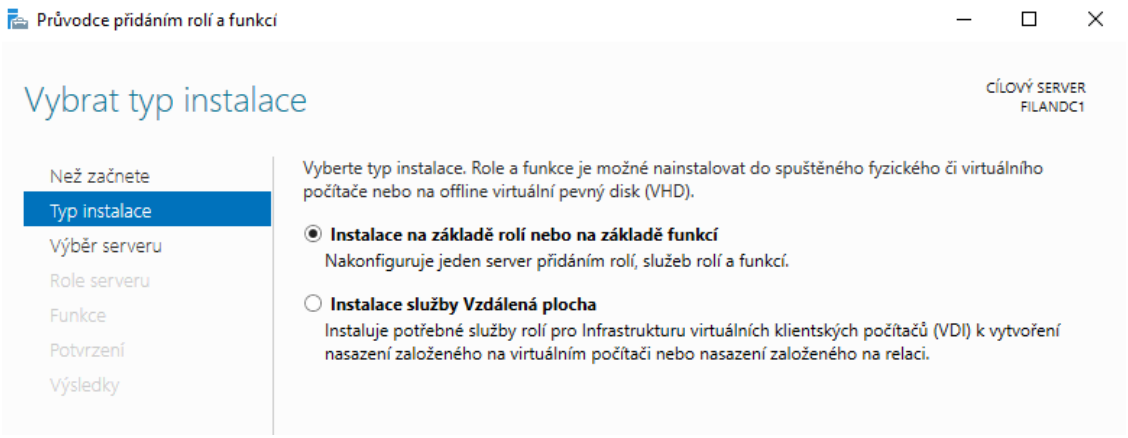
Předpokladem k instalaci doménových serverů je, dle dobrých zvyků, nastavit jim doménový název a síťovým adaptérům, připojeným do sítě LAN, statické IP adresy. Pro potřeby praktických úloh je použita síť 192.168.116.0/24, ve které se budou nacházet všechna síťová zařízení.

IP adresa **192.168.116.2** bude přiřazena serveru s názvem **FILANDC1**, který představuje první řadič v doméně a IP adresa **192.168.116.3** pro druhý řadič s názvem **FILANDC2**.

4.1.1 Instalace rolí AD a DNS

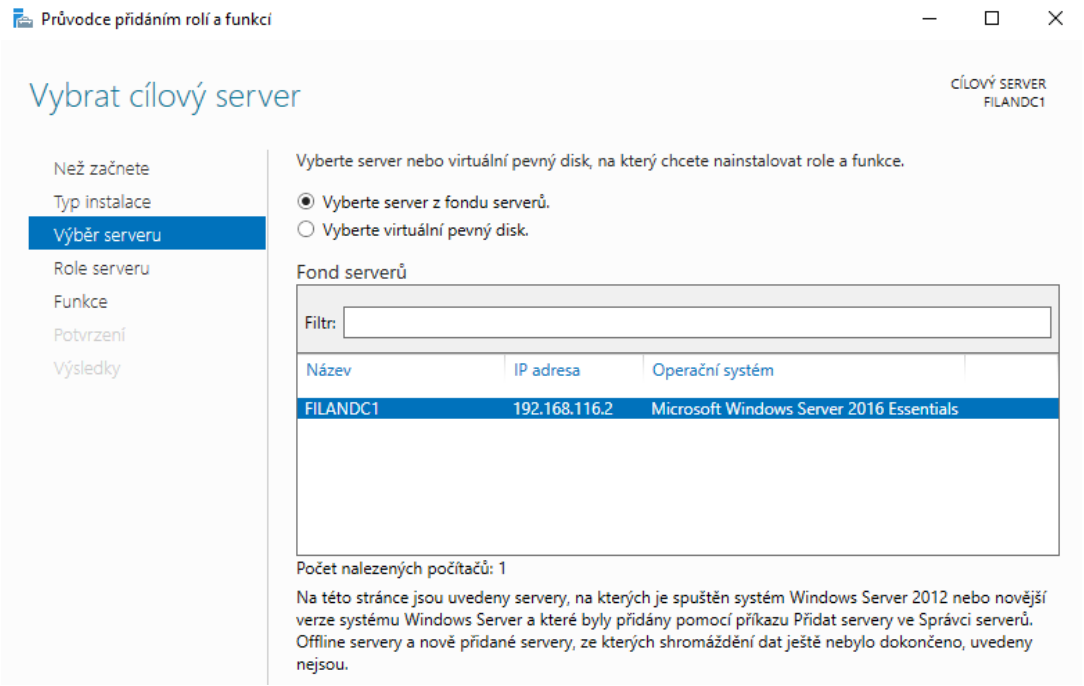
Instalace jakýchkoliv rolí v OS Windows Server 2016 je prováděna pomocí Průvodce přidáním rolí a funkcí. Tohoto průvodce je možné nalézt v řídícím panelu Správce serveru pod volbou „Přidat role a funkce“.

Na začátku průvodce vyžaduje výběr typu instalace. V našem případě bude vybrána možnost Instalace na základě rolí nebo funkcí, protože budou instalovány role serveru.



Obr. 13 Instalace rolí serveru FILANDC1

V dalším kroku průvodce nabízí výběr serveru případně skupiny serverů, na které budou role instalovány. V naší úloze bude zvolen server s názvem FILANDC1.

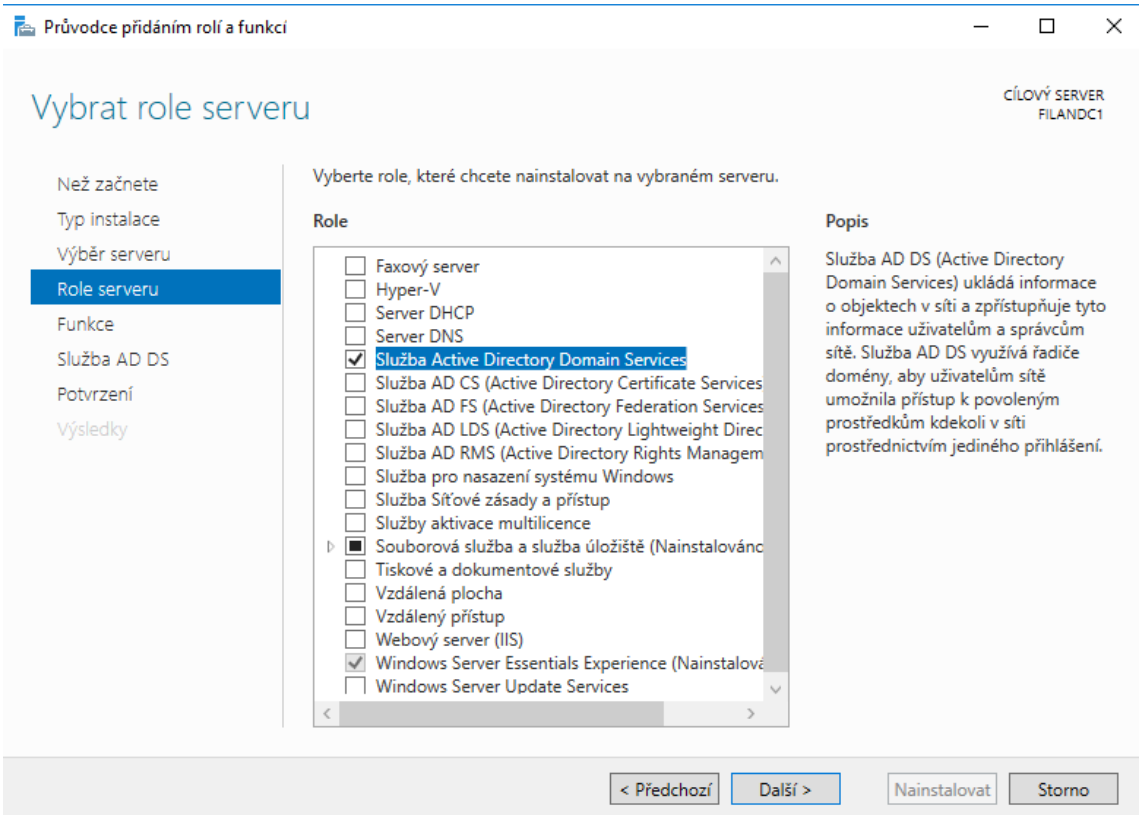


Obr. 14 Výběr cílového serveru

Přichází na řadu výběr rolí serveru, které budou instalovány. Na výběr je mnoho rolí, ve kterých server může vystupovat, ale zadání úlohy udává instalaci rolí ADDS a DNS.

V průvodci stačí vybrat pouze roli ADDS. Role DNS bude automaticky také naistalována, jelikož DNS server je pro Active Directory nutnou součástí.

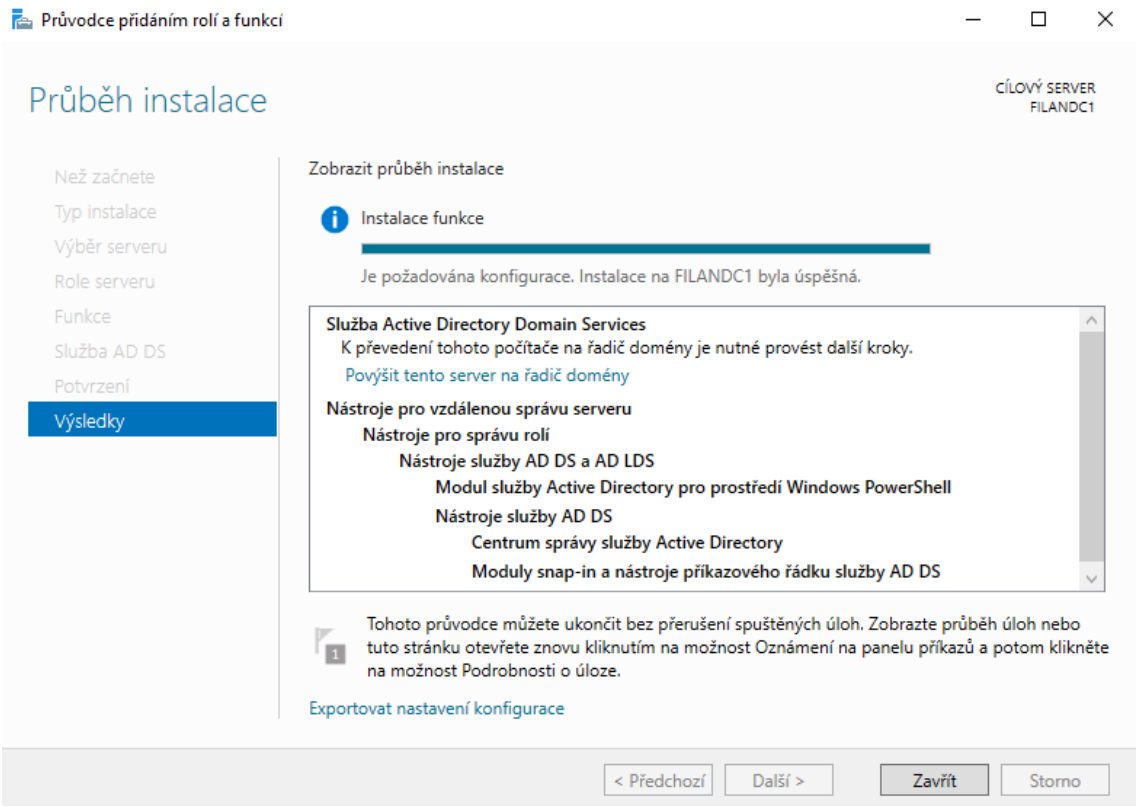
Pokud se v síti nenachází žádný DHCP server[3], který by se staral o přidělování IP adres v síti, je možné provést jeho instalaci v tomto kroku.



Obr. 15 Výběr rolí k instalaci

Po výběru potřebných rolí zbývá projít pomocí průvodce až k samotné instalaci. V případě potřeby instalace dalších funkcí serveru zvolíme požadované v následujících krocích.

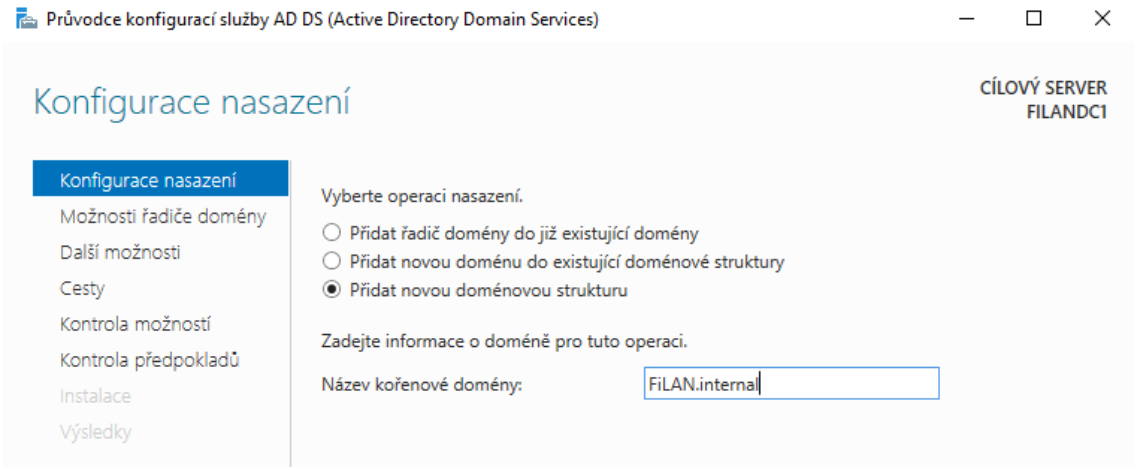
[3] DHCP (Dynamic Host Configuration Protocol) přiděluje počítačům pomocí DHCP protokolu IP adresu, masku sítě, adresu výchozí brány a adresu DNS serveru



Obr. 16 Povýšení serveru na řadič domény

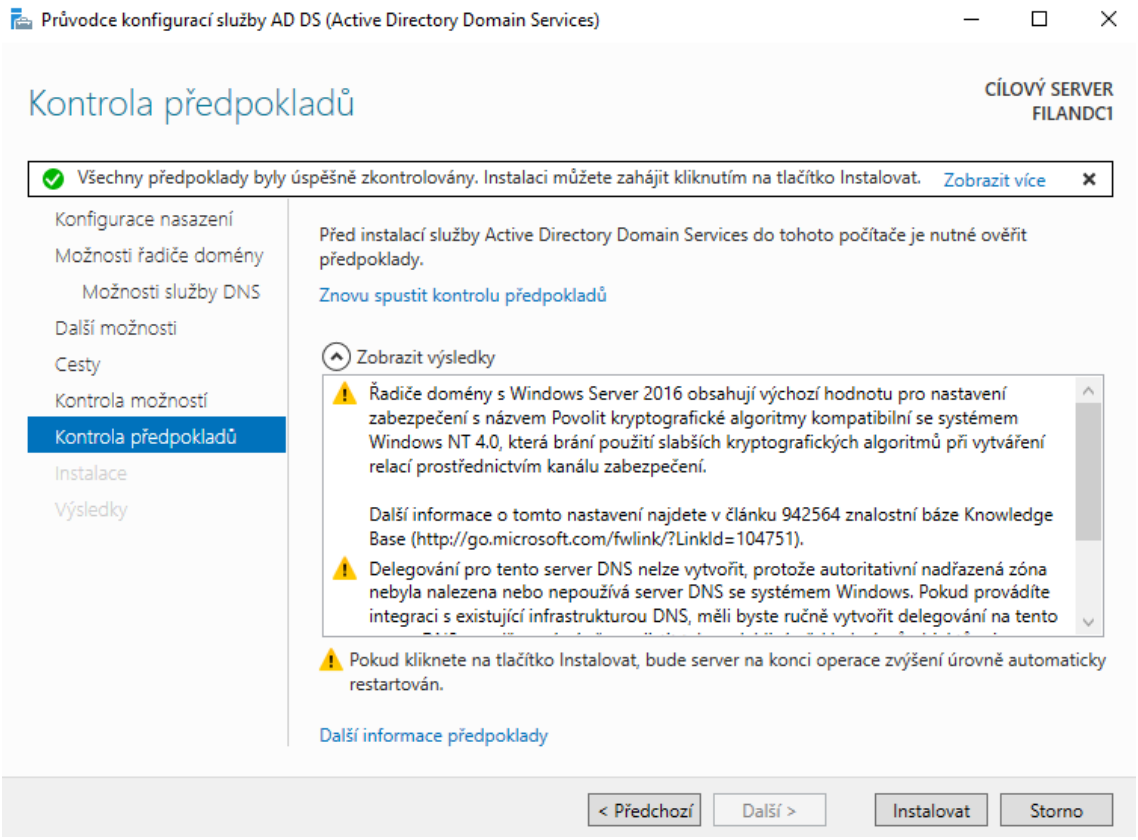
4.1.2 Konfigurace ADDS

Po úspěšné instalaci všech potřebných rolí a funkcí je server FILANDC1 připraven k povýšení na řadič domény. S tímto krokem je spojeno vytvoření nového **lesa** s názvem **FiLAN.internal**. V tomto lese se bude nacházet **pouze jeden strom**. Vznikne tím tzv. Single-Domain Forest. Vytvoření více stromů – sub-domén – není, podobně jako v běžné praxi, pro potřebu této úlohy nutné.



Obr. 17 Konfigurace nasazení ADDS

Další kroky nastavení, jako jsou např. NetBIOS název a určení Cest, budou ponechány ve výchozích hodnotách.



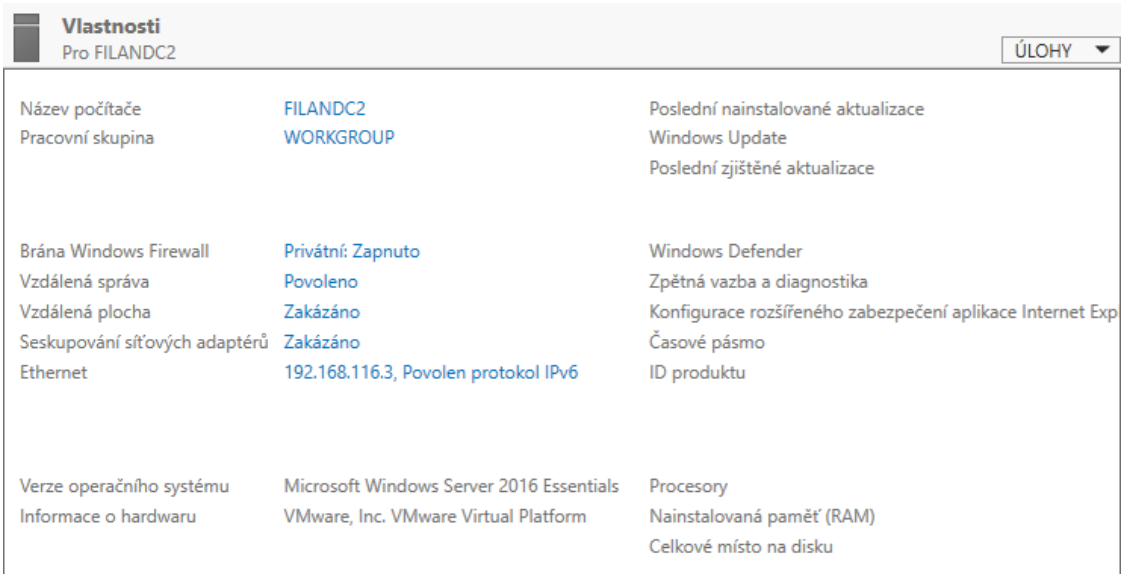
Obr. 18 Instalace služby ADDS

Konfigurace je dokončena úspěšnou instalací.

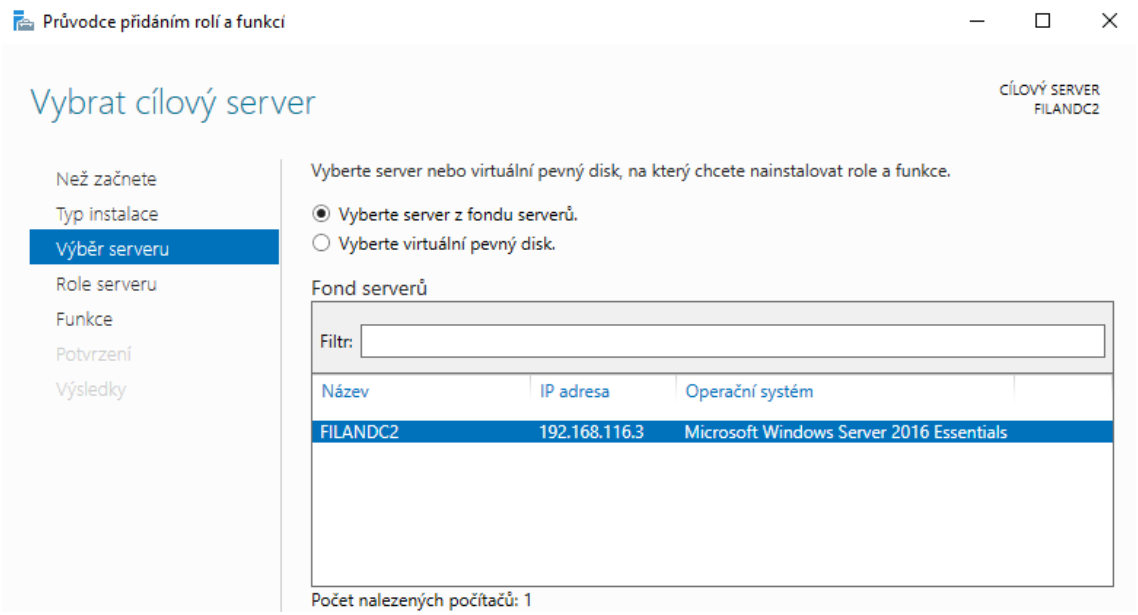
4.1.3 Přidání dalších radičů do domény

Při nasazování Active Directory je, dle obecně získaných zkušeností z různých prostředí užití, dobré použít alespoň dva doménové řadiče. Použitím dalších řadičů dochází k replikaci dat domény a je tím zajištěna záloha např. v případě výpadku HW. Z důvodů vyšší úrovně zálohy je také doporučeno HW fyzicky oddělit např. do jiné budovy nebo lokality.

Každý další doménový kontrolér se instaluje stejným způsobem jako první. Je znovu nastaven název serveru, IP adresa a nainstalovány role ADDS a DNS. V našem případě bude název serveru **FILANDC2** a jeho IP adresa **192.168.116.3**.



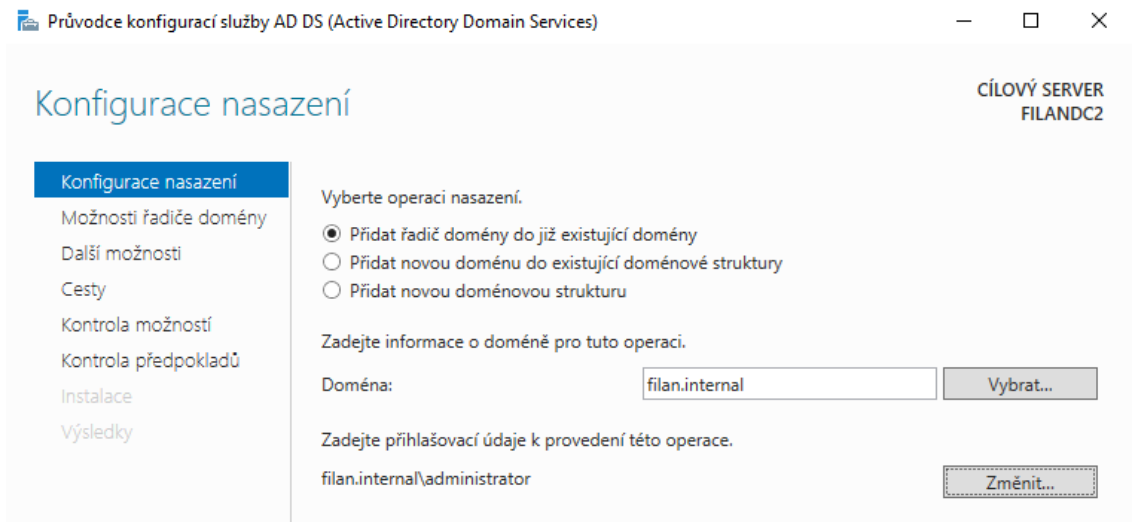
Obr. 19 Vlastnosti serveru FILANDC2 před přidáním do domény



Obr. 20 Volba dalšího DC k instalaci

Po těchto krocích nastává moment povýšení serveru na doménový řadič pomocí Průvodce konfigurací služby ADDS.

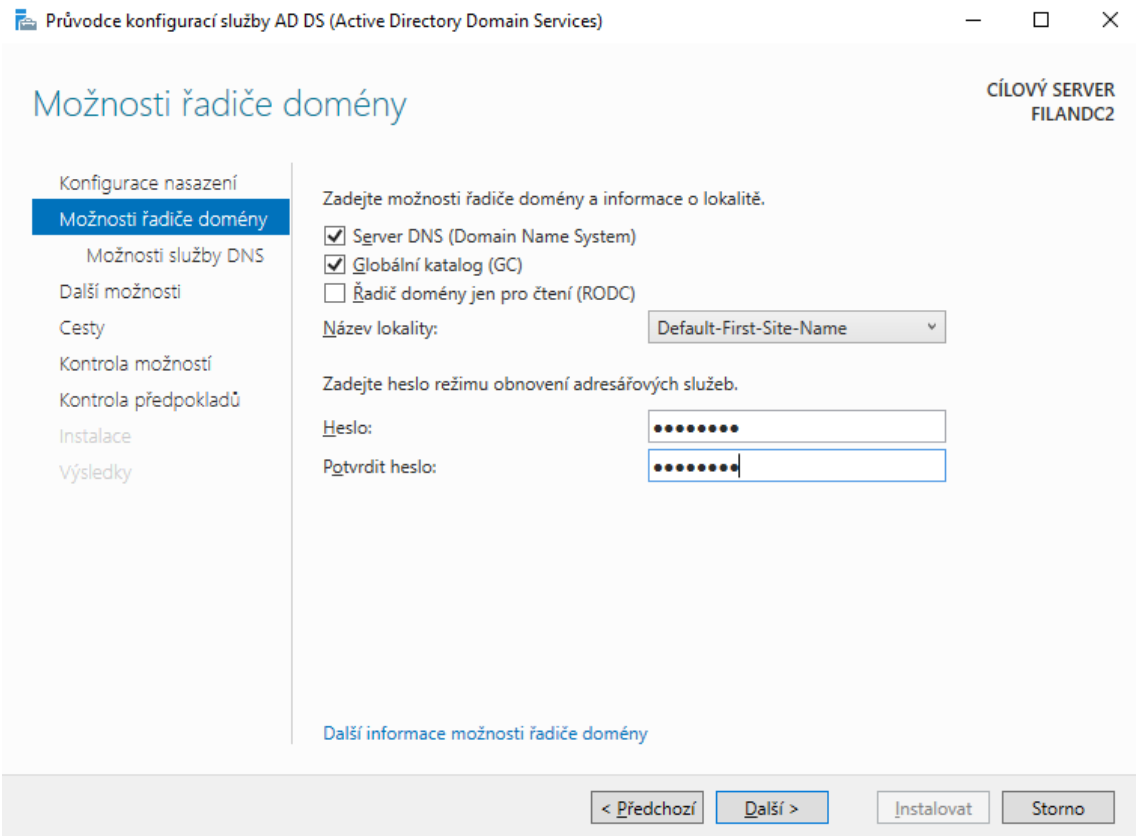
Při zařazení dalších řadičů do domény je hlavní rozdíl v prvním kroku průvodce, kde na rozdíl od řadiče FILANDC1, který byl přidáván do nové doménové struktury, je vybrána možnost přidání řadiče do **již existující domény**.



Obr. 21 Přidání řadiče do existující domény

V dalším kroku možností řadiče domény je znovu nabízena volba, kde je možné vybrat, zda se server FILANDC2 bude také chovat jako server DNS, a zda bude poskytovat globální katalog. V jedno-doménových lesích je, dle společnosti

Microsoft, doporučeno, aby poskytoval GC a DNS server každý doménový řadič z důvodu vysoké dostupnosti. Výkonnost serveru se nijak nezmění, jelikož při používání GC není vyžadován navíc žádný diskový prostor ani výkon CPU. (9)

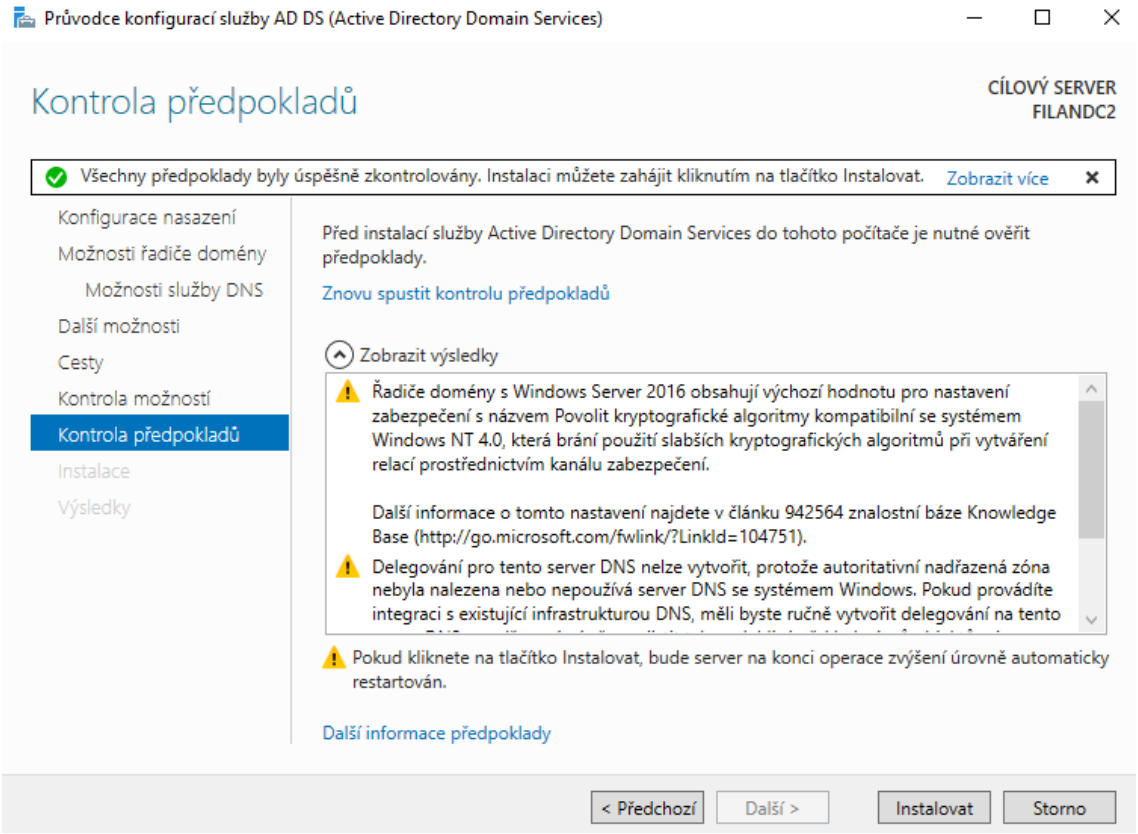


Obr. 22 Možnosti řadiče FILANDC2

Na nabídce Další možnosti přichází na řadu výběr serveru, který bude FILANDC2 **replikovat**. V našem prostředí je pouze jeden další DC a tím je server s názvem **FILANDC1**.

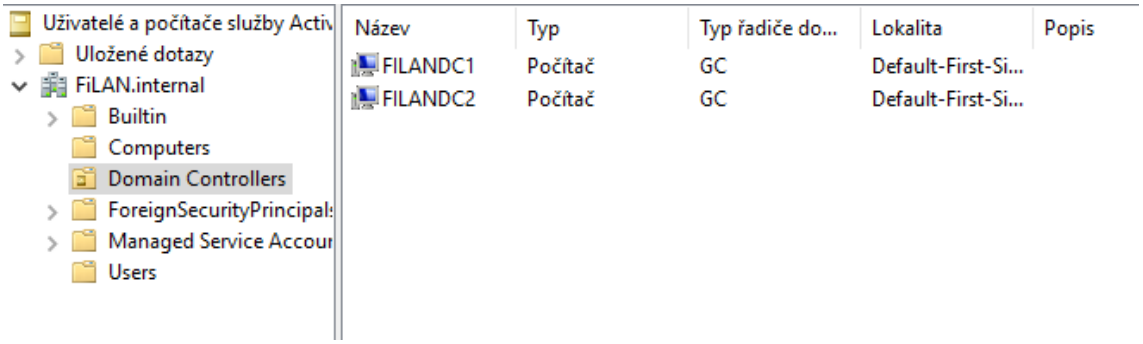
Obr. 23 Výběr zdroje replikace

Po výběru zdroje replikace přichází už jen kontrola předpokladů k instalaci. Pokud jsou všechny předpoklady splněny, je možné provést instalaci.



Obr. 24 Kontrola předpokladů instalace serveru

Úspěšnost povýšení serveru na řadič domény, je možné si zkontrolovat ve Správci uživatelů a počítačů služby AD, kde jsou zobrazeny všechny dostupné doménové řadiče.



Obr. 25 Úspěšně zařazené DC v doméně

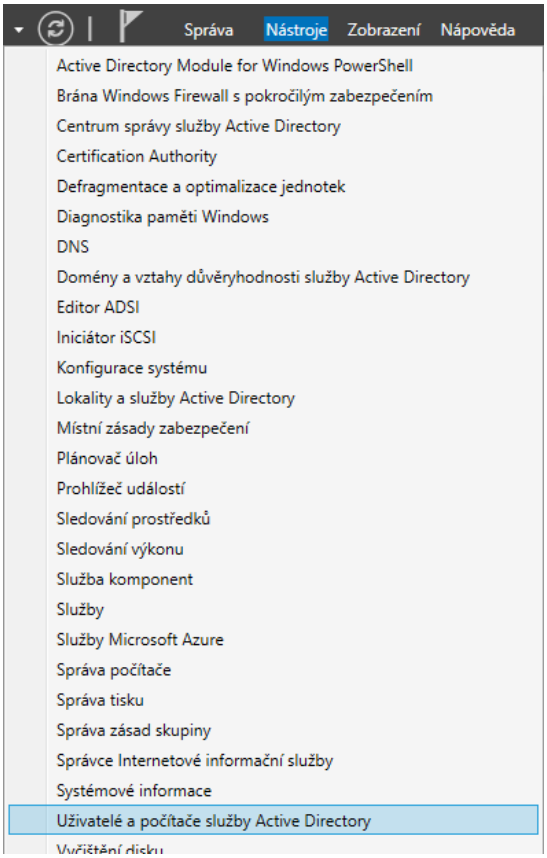
4.2 Úloha 2 – Tvorba hierarchie domény

V první části této úlohy je hlavním úkolem vytvoření doménové hierarchie. Logický návrh bude odpovídat reálnému stavu struktury společnosti. Realizace bude provedena za pomoci využití komponent AD, jako jsou organizační jednotky, skupiny, uživatelé apod. Organizační jednotky budou představovat jednotlivá oddělení, ve kterých budou umístěny skupiny uživatelů. Do těchto skupin budou zařazeni všichni uživatelé/zaměstnanci.

Druhá část úlohy bude uvažovat o personálních organizačních změnách ve společnosti a jejím dopadům na změny v hierarchii domény. Dojde ke změně pracovní pozice obchodního zástupce, který se po dosažení plánovaných cílů stane členem top managementu.

4.2.1 Vytvoření hierarchie domény

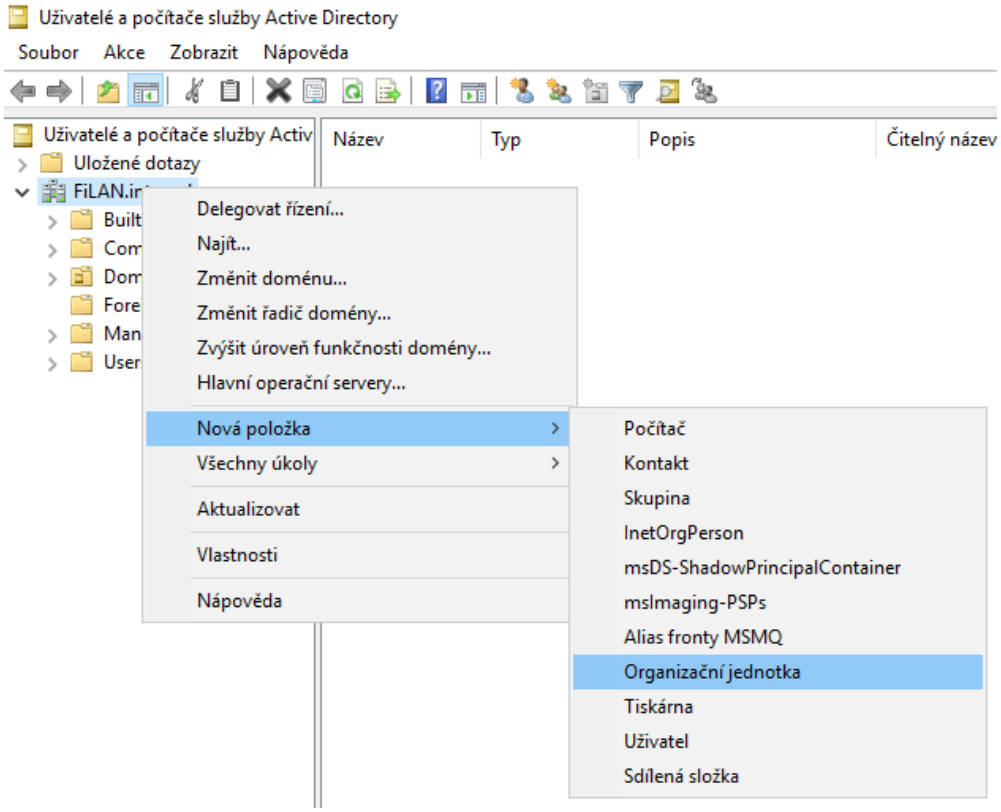
Tvorba hierarchie domény je prováděna za pomoci modulu Uživatelé a počítače služby Active Directory, kterou nalezneme ve Správci serveru.



Obr. 26 Nástroje Správce serveru

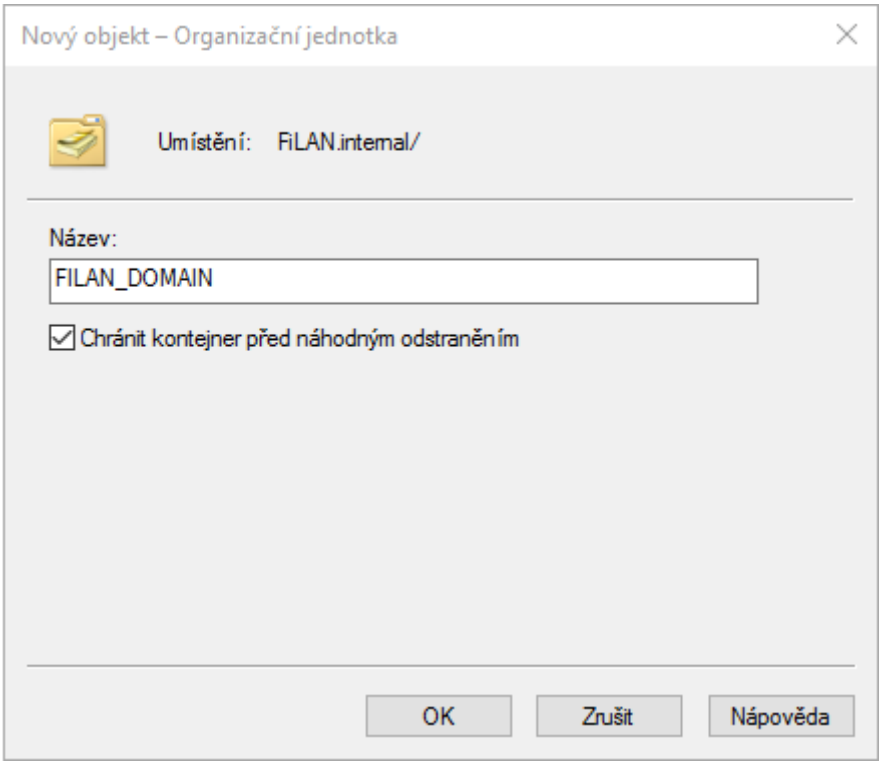
V tomto kroku je zobrazena výchozí struktura domény, ve které se nachází adresáře s výchozími uživatelskými účty, skupinami, se všemi aktuálně připojenými počítači a s doménovými řadiči. Obecně je možné zachovat tuto strukturu, ale v této úloze budou vytvořeny vlastní organizační jednotky.

Nejprve bude založena nová organizační jednotka s názvem **FILAN_DOMAIN**, pod kterou budou dále vnořovány další OU. Na tento model návrhu budou později lépe aplikovány zásady skupin (GPO). Vytvoření každé nové komponenty lze provést pomocí PTM a kontextové nabídky.



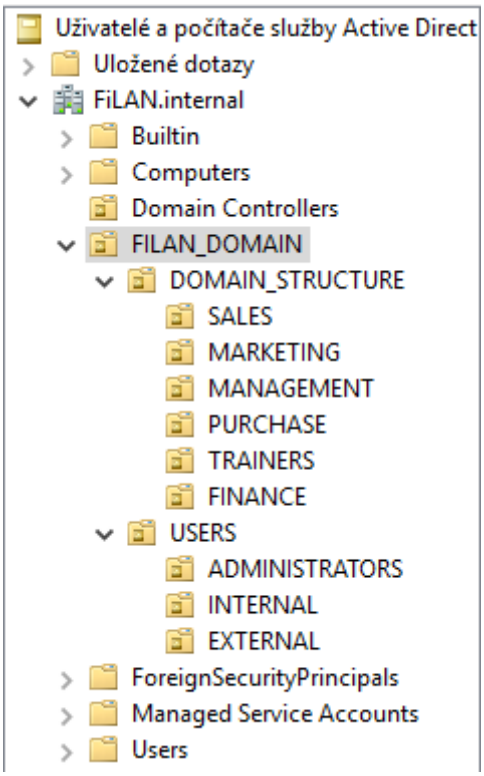
Obr. 27 Vytvoření nové OU

Každý objekt má možnost povolení prevence před jeho náhodným odstraněním, kterou je vhodné zvolit.



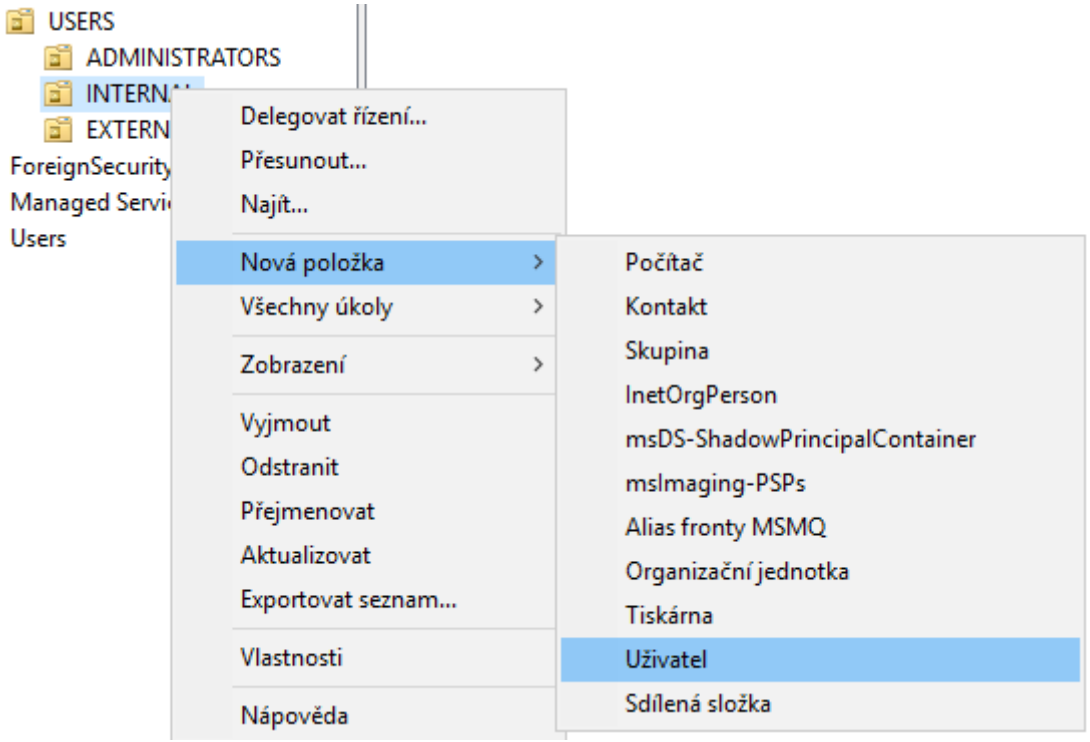
Obr. 28 Pojmenování nové OU

Postupným přidáváním organizačních jednotek, je možné vytvořit libovolnou hierarchii. V našem případě došlo k rozdělení OU **FILAN_DOMAIN** na dvě části. **DOMAIN_STRUCTURE** představuje OU pro jednotlivá oddělení společnosti a **USERS** bude použita k zařazení uživatelů do skupin ADMINISTRATORS, INTERNAL a EXTERNAL. V OU EXTERNAL jsou uživatelé pracující v terénu a v INTERNAL uživatelé pracující v administrativě.



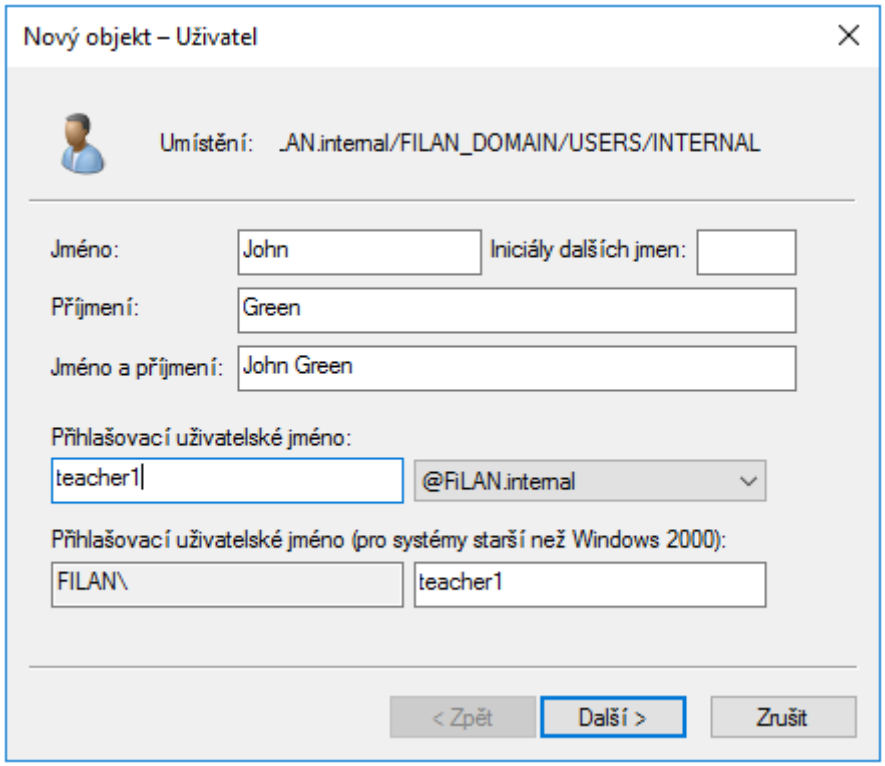
Obr. 29 Hierarchie organizačních jednotek v doméně

Nové uživatele můžeme vytvořit stejným způsobem, jako OU, pomocí pravého tlačítka myši.



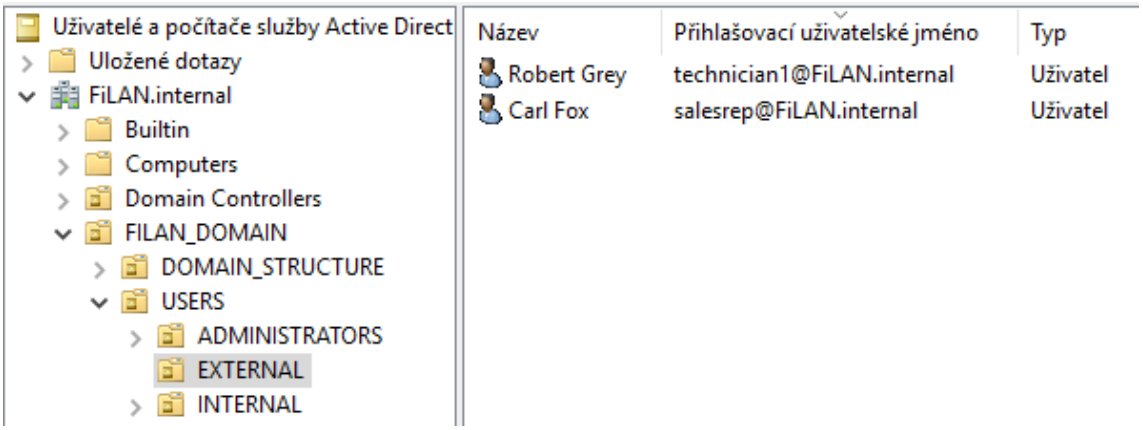
Obr. 30 Vytvoření uživatele domény

Při vytváření nového uživatele existuje, oproti vytváření nové OU, více parametrů, které je možné nadefinovat. Jméno a příjmení je dané, ale uživatelské jméno může být zvoleno dle vlastních preferencí. Je doporučeno používat konvenci přihlašovacích jmen takovou, aby byla snadno zapamatovatelná.



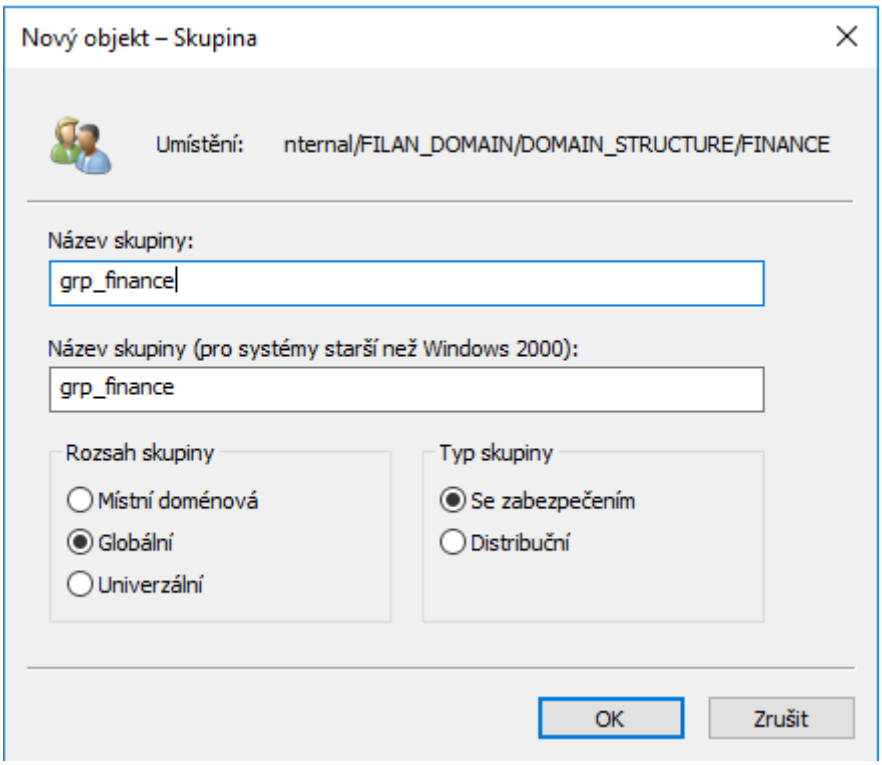
Obr. 31 Nastavení uživatele

Na Obr. 32 jsou v OU EXTERNAL vytvořeny dva uživatelské účty. Uživatel Robert Grey představuje zaměstnance pracujícího jako technik pohybující se v terénu a Carl Fox je obchodní zástupce. Stejným postupem jsou vytvořeny všechny doménové účty pro uživatele AD.



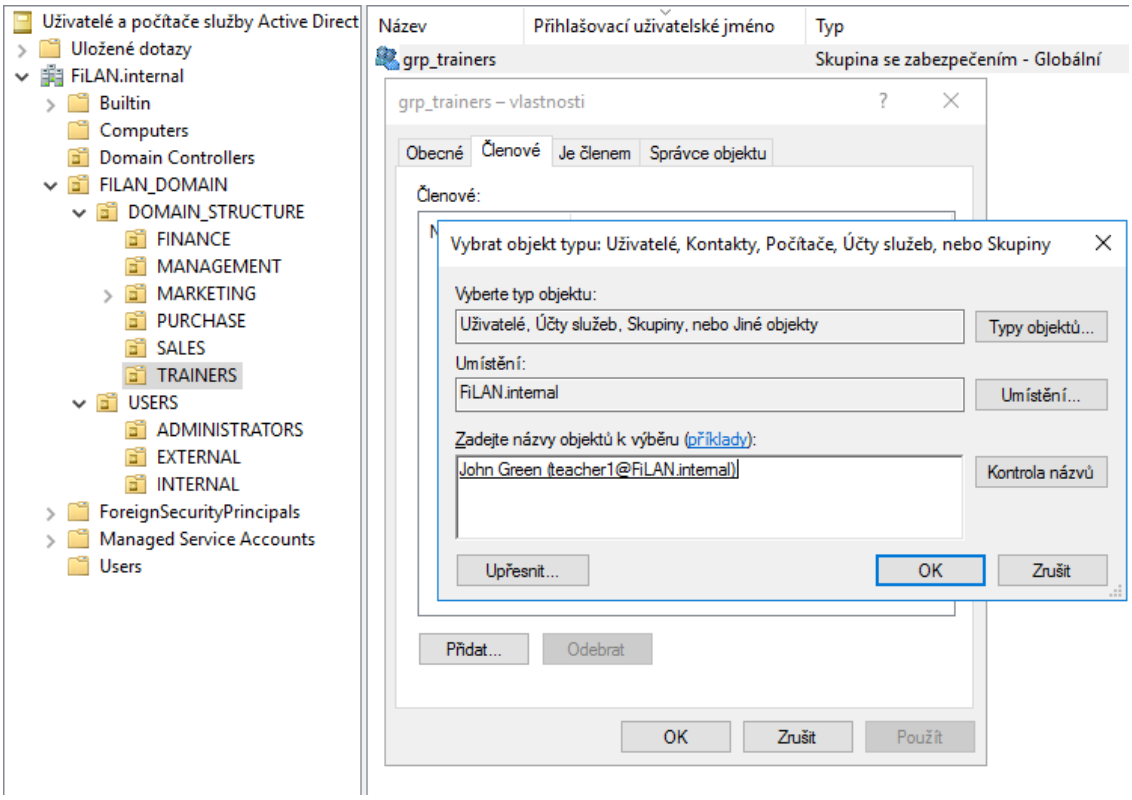
Obr. 32 Uživatelé v organizační jednotce

Skupina uživatelů bude vytvářena vždy, když budou kladeny požadavky na seskupení části uživatelů, na které mohou být později aplikovány zejména pravidla přístupů a jiné další politiky např. GPO.



Obr. 33 Vytvoření skupiny uživatelů

Při vytváření nové skupiny je potřeba pouze určit její název a zvolit uživatele, kteří do ní budou zahrnuti. V naší úloze bude přidán uživatel John Green, na pozici produktového školitele, do skupiny **grp_trainers.**



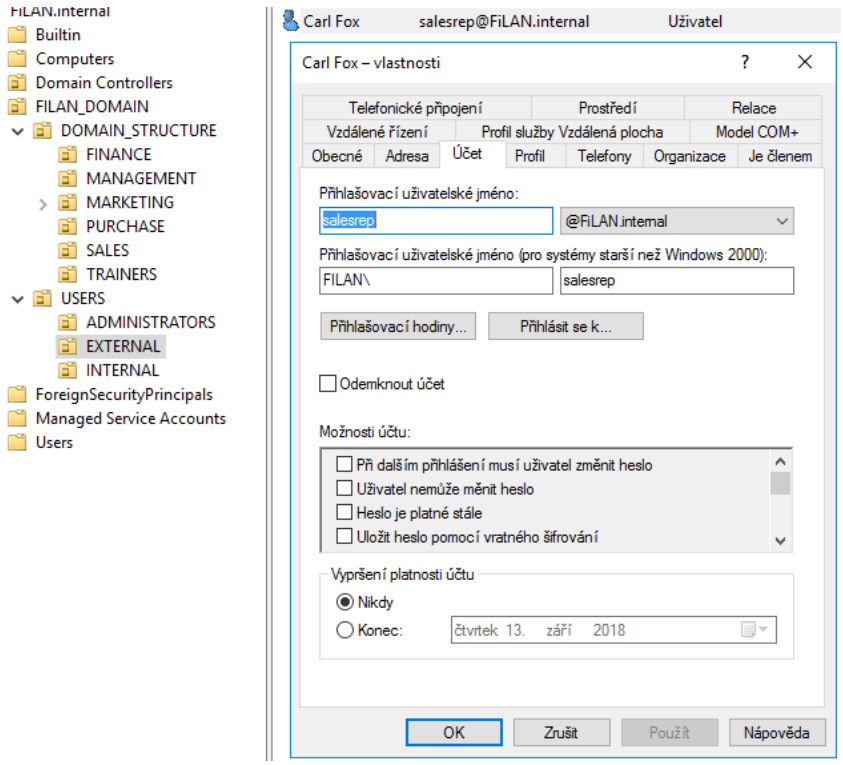
Obr. 34 Přidání uživatele do skupiny

4.2.2 Hierarchie domény po změně organizační struktury

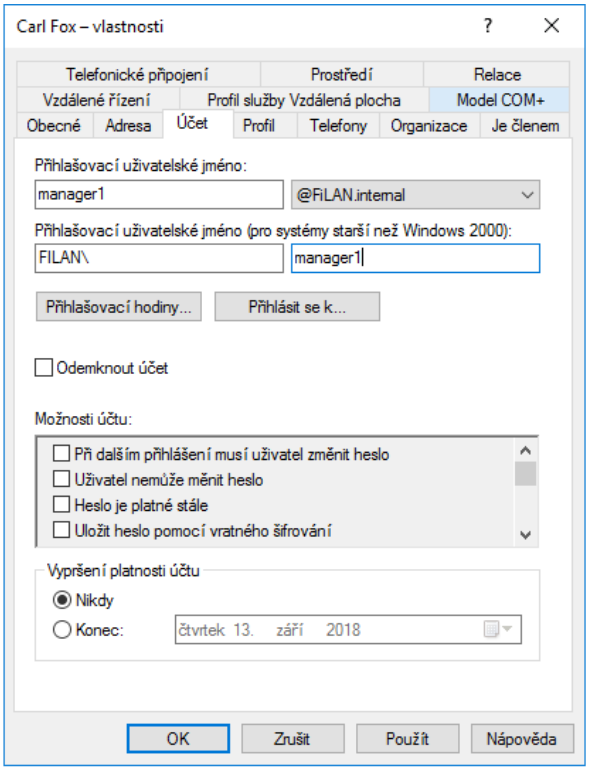
Při vytváření domény v prostředí Active Directory, kdy byla navržena kompletní korektní hierarchie uživatelů, skupin a organizačních jednotek, je možné čelit nástrahám, jako jsou personální změny ve společnosti. V takovýchto momentech často přichází na řadu provádění změn ve struktuře. Můžou nastat situace, kdy je zaměstnanec povýšen, přestoupí na jiné oddělení apod.

V této úloze předpokládejme změnu pracovní pozice obchodního zástupce Carla Foxe, který se díky výborným pracovním výsledkům stane členem top managementu.

V našem prostředí je přihlašovací jméno nastaveno dle pracovní pozice. Z důvodu povýšení zaměstnance bude u uživatele provedena nejprve změna přihlašovacího jména ze **salesrep** na **manager1**.

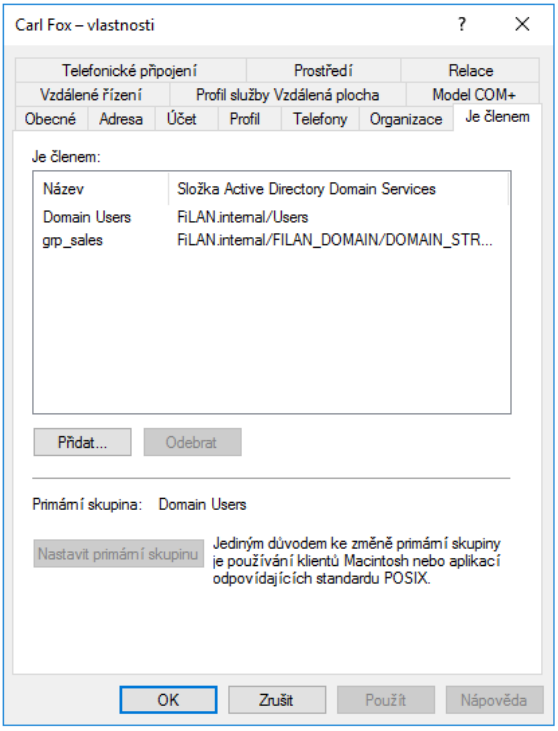


Obr. 35 Vlastnosti uživatelského účtu

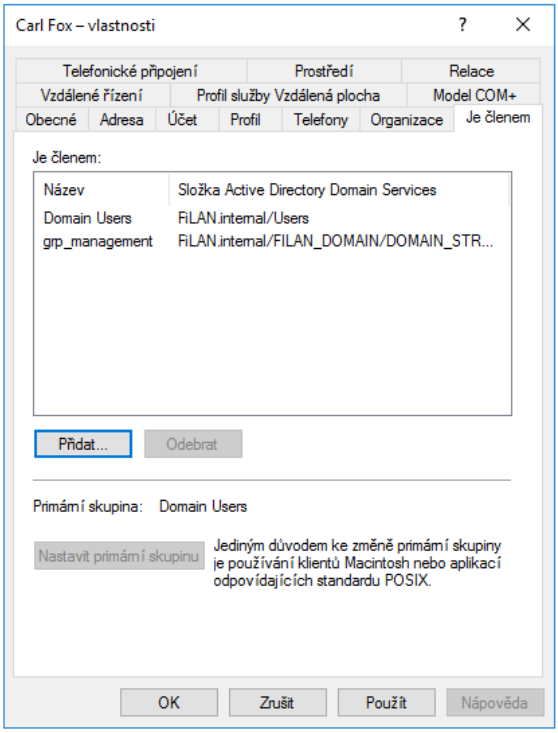


Obr. 36 Změna přihlašovacího jména uživatele

Dále nastává okamžik změny zařazení do skupiny. Existují dvě možnosti, jakými lze změnu zařazení provést. První možností je editace na kartě **Je členem**. Zde jsou vypsány všechny skupiny, ve kterých se uživatel nachází. Uživatel Carl Fox je ve skupině **gpr_sales** a nově bude členem skupiny **grp_management**.

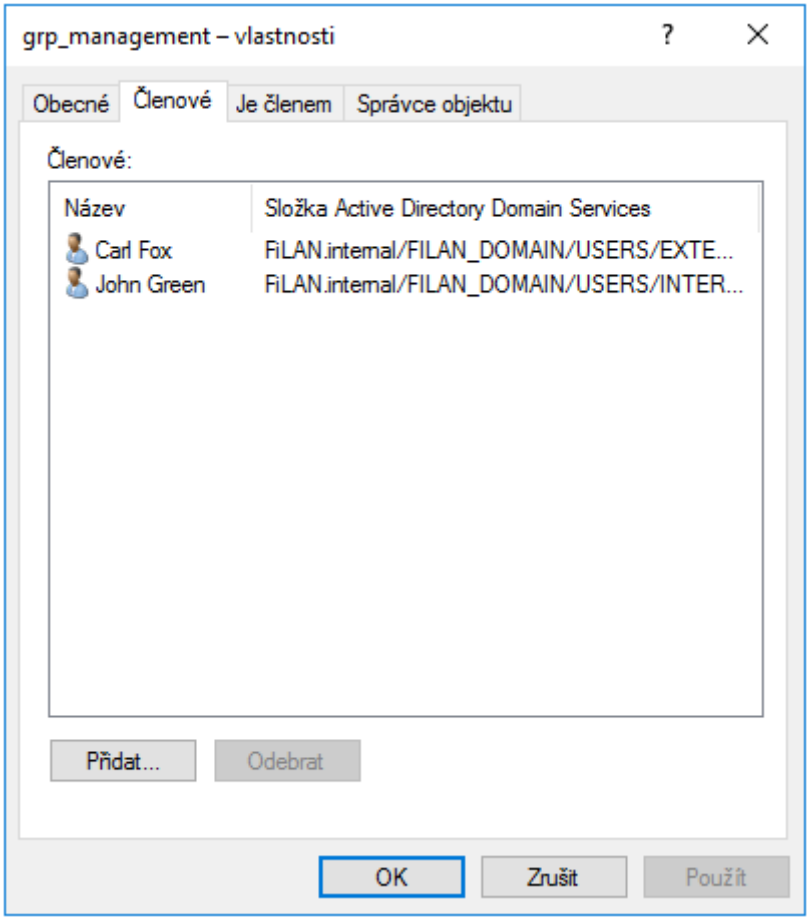


Obr. 37 Uživatel ve skupině gpr_sales



Obr. 38 Uživatel ve skupině gpr_management

Druhým způsobem, jakým lze provést přiřazení/odebrání člena do skupiny, je přes vlastnosti objektu skupiny, kde na kartě **Členové** jsou, podobně jako u uživatele, zobrazeni všichni členové skupiny.



Obr. 39 Členové skupiny grp_management

Pokud byla v první úloze nastavena správná replikace doménových řadičů, tak by mělo dojít k přenesení vytvořené hierarchie z celé této úlohy na server FILANDC2.

4.3 Úloha 3 – Sdílení souborů a řízení přístupů

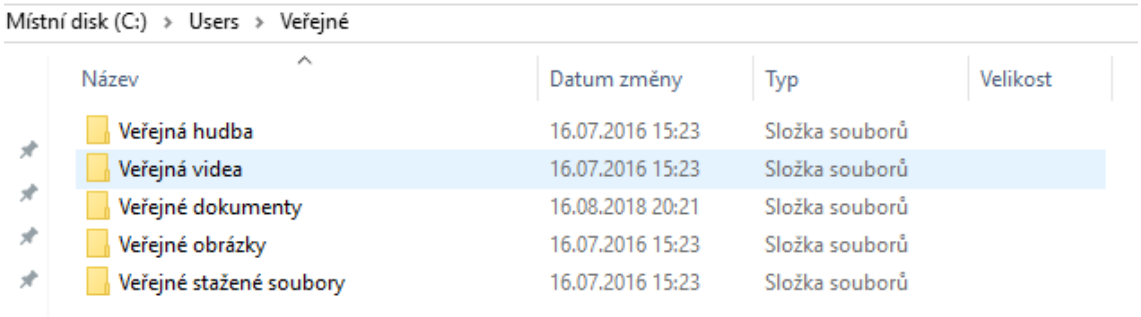
Zadáním této úlohy je vytvoření sdílených souborů a adresářů a nastavení odpovídajících oprávnění přístupů.

Úkolem je vytvořit **centrální sdílený adresář**, ke kterému budou mít přístup **všichni členové** skupiny **gpr_filandomain**. Obsahem tohoto sdíleného prostoru budou podadresáře pojmenované dle názvů oddělení. K těmto podadresářům budou moci přistupovat pouze členové daného oddělení.

Dále bude vytvořen jeden speciální adresář, na kterém bude předvedena funkce **vypnutí dědičnosti**. Tento adresář bude pojmenován **Wages** (mzdy). Obsahem tohoto adresáře budou např. podklady pro zpracování mezd, výplatní pásky apod. K tomuto adresáři budou smět přistupovat pouze členové skupiny **grp_finace**. Pro všechny ostatní skupiny a uživatele bude tento adresář „neviditelný“.

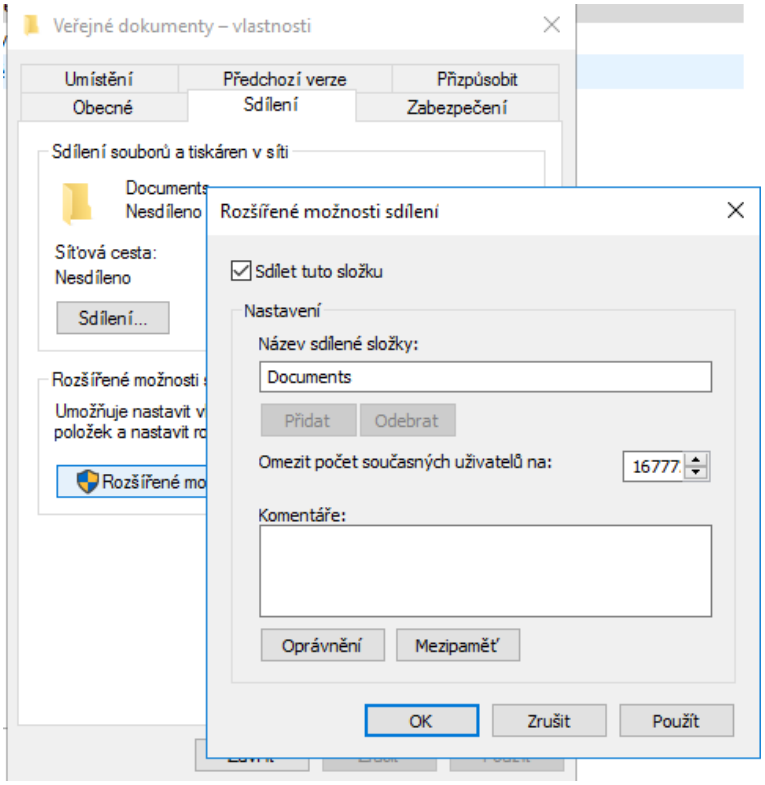
4.3.1 Vytvoření sdíleného adresáře

Hlavním sdíleným adresářem bude adresář **Veřejné dokumenty** sdílený ze serveru **FILANDC1**. Tento adresář je výchozím adresářem operačních systémů Windows a nachází se v umístění „C:\Users\Veřejné“ spolu s dalšími veřejnými adresáři. Ke sdílení souborů je možné si vytvořit i vlastní adresář v libovolném umístění.



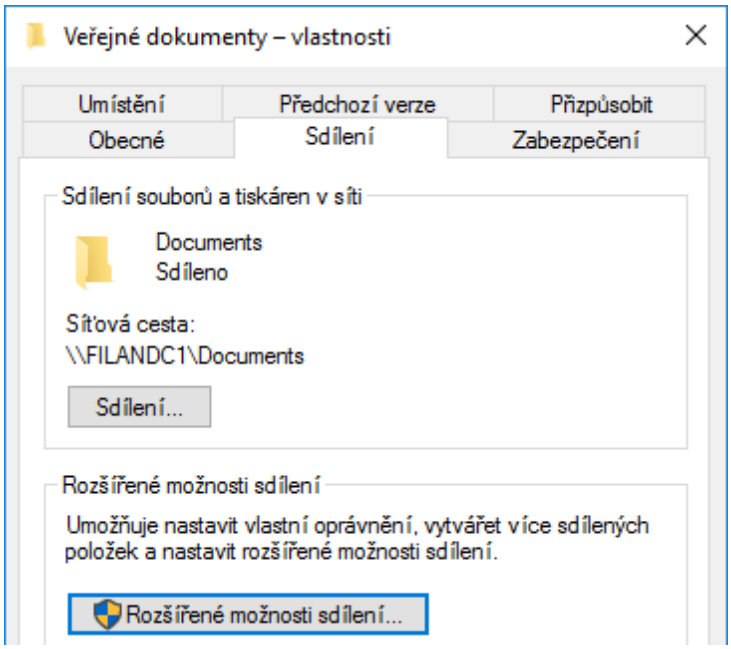
Obr. 40 Vytvoření sdílené složky

K povolení sdílení adresáře Veřejné dokumenty je možné se dostat přes PTM, kde na kartě Sdílení je potřeba vybrat volbu **Sdílet tuto složku**. V tomto bodě je také možné změnit název sdílené složky.



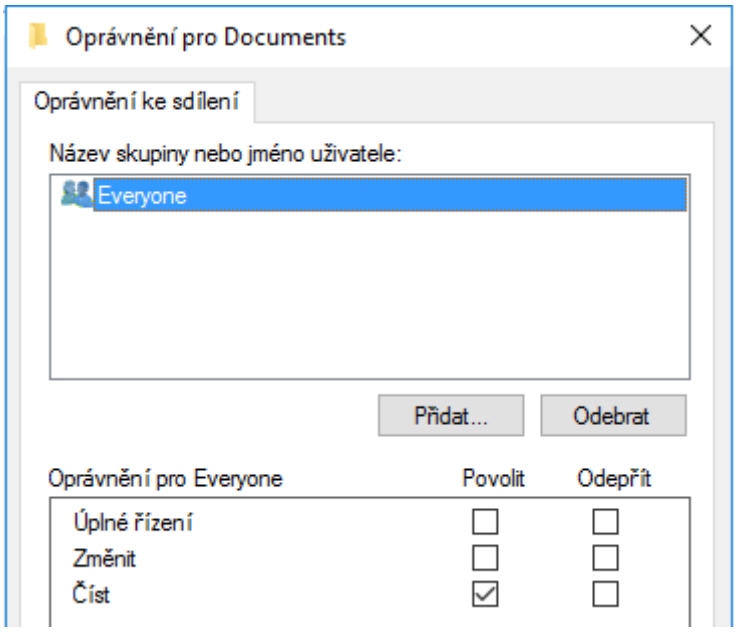
Obr. 41 Možnosti sdílené složky

Pokud nastavení sdílení proběhne v pořádku, bude zobrazen stav **Sdíleno**.



Obr. 42 Vlastnosti sdílené složky

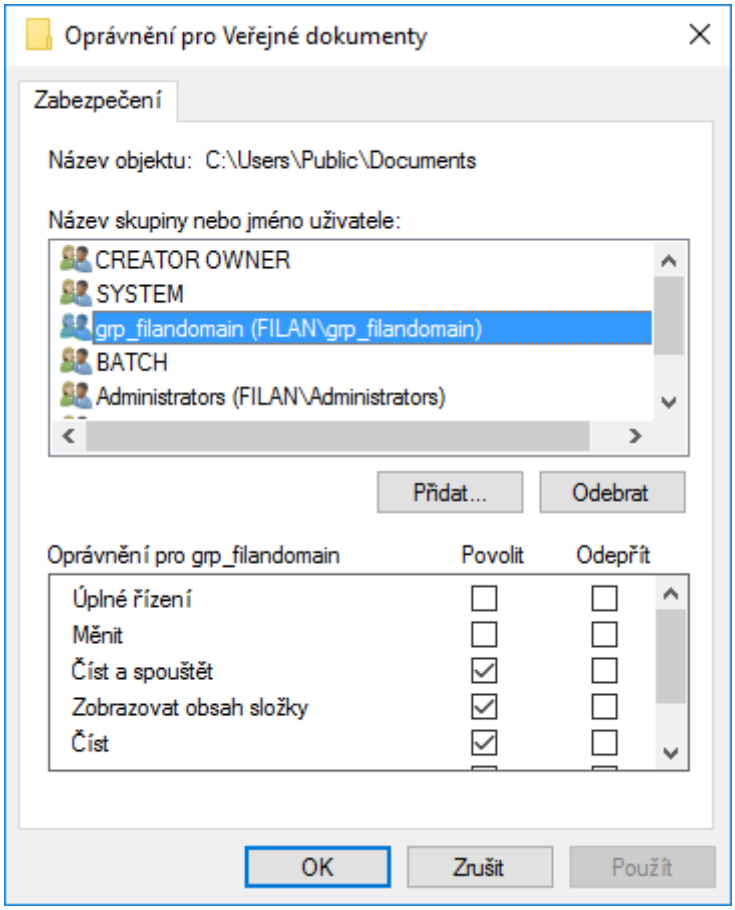
Pomocí rozšířených možností sdílení je možné definovat oprávnění pro sdílení. V našem případě jsou ponechány výchozí hodnoty. Skupina Everyone bude mít na úrovni sdílení přístup jen pro čtení.



Obr. 43 Nastavení oprávnění ke sdílení

V nastavení zabezpečení adresáře Veřejné dokumenty je možné určit, kdo k němu bude mít, na úrovni NTFS, přístup. V tento okamžik nastává důležité rozhodnutí, komu a jaké NTFS oprávnění přidělit. Výchozími hodnotami bývají skupiny jako CREATOR OWNER pro vlastníky adresáře, SYSTEM pro samotný OS a jeho služby, Administrators pro doménové administrátory a další. Nastavené oprávnění dané skupiny je zobrazeno ve spodní části okna.

Úrovní oprávnění existuje několik a liší se dle možností přístupů na úplné řízení, provádění změn, čtení a spouštění, pouze čtení, zobrazení obsahu složek, zapisování a oprávnění ke zvláštnímu přístupu. Oprávnění je možné buď **povolit** anebo **odepřít**. Je důležité poznamenat, že odepřená oprávnění mají přednost před povolenými. Na tomto adresáři bude nastaveno oprávnění číst a spouštět skupině **grp_filandomain**, do které patří všichni uživatelé domény.



Obr. 44 Nastavení oprávnění NTFS

Dále budou vytvořeny adresáře pro jednotlivá oddělení a adresář Wages pro mzdy. Každému adresáři budou nastaveny oprávnění přístupu obdobným způsobem jako u nadřazeného adresáře.

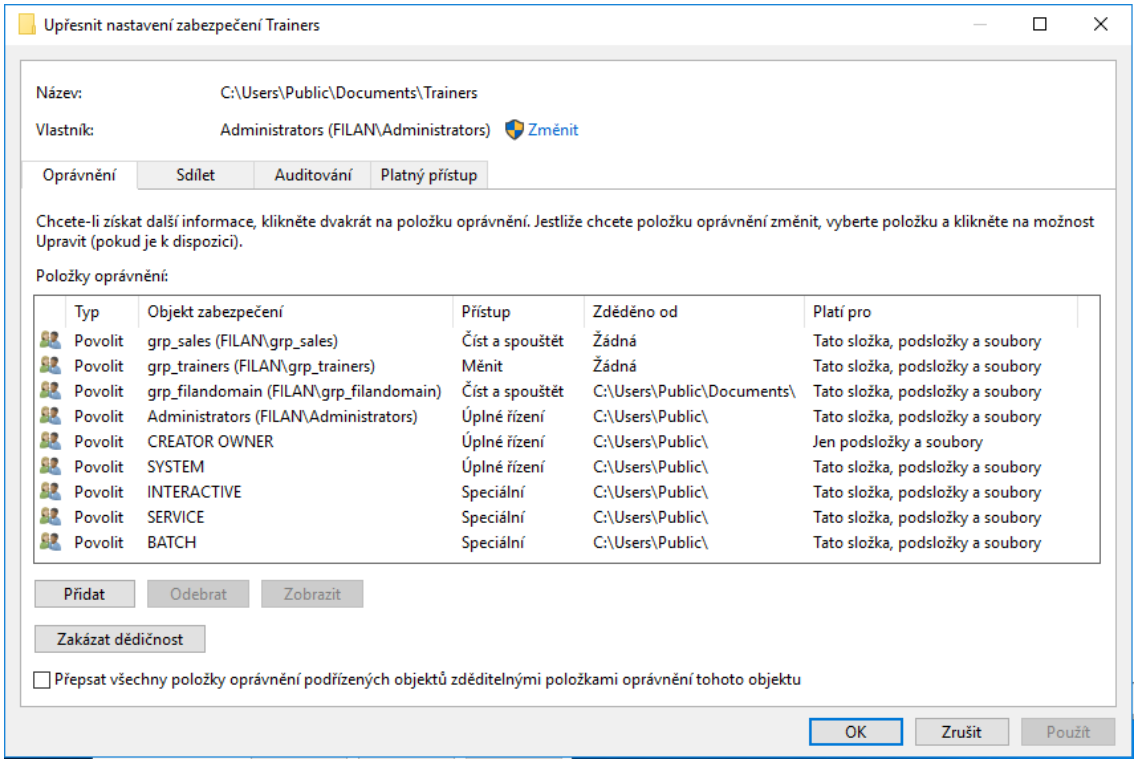
Název	Datum změny	Typ	Velikost
Finance	16.08.2018 21:35	Složka souborů	
Management	16.08.2018 21:35	Složka souborů	
Marketing	16.08.2018 21:36	Složka souborů	
Purchase	16.08.2018 21:35	Složka souborů	
Sales	16.08.2018 21:35	Složka souborů	
Trainers	16.08.2018 21:35	Složka souborů	
Wages	16.08.2018 21:46	Složka souborů	

Obr. 45 Vytvořené podadresáře ve sdíleném adresáři

V upřesňujících nastaveních zabezpečení je možné vidět detailnější pohled konfigurace oprávnění. Každý z vytvořených podadresářů, adresáře Veřejné dokumenty, by měl mít nastaveno oprávnění pro **čtení a spouštění** uživatelům

ve skupině **grp_filandomain**. Skupina daného oddělení bude mít nastavena oprávnění k provádění změn.

V případě adresáře **Trainers** jsou nastavena oprávnění ke změnám pro skupinu školitelů **grp_trainers** a obchodní zástupci společnosti (**grp_sales**) mají oprávnění pouze číst a spouštět. Obsahem tohoto adresáře mohou být např. školící materiály.



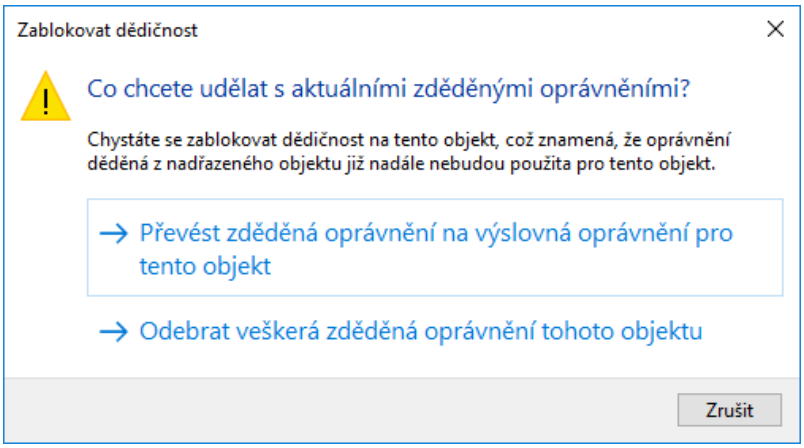
Obr. 46 Nastavení oprávnění v adresáři Trainers

Jelikož je na všech nově vytvořených podadresářích nastavena výchozí hodnota **dědičnosti** na stav **zapnuto**, je zděděno oprávnění z nadřazeného adresáře. Z tohoto důvodu je automaticky doplněna i skupina grp_filandomain.

4.3.2 Vypnutí dědičnosti

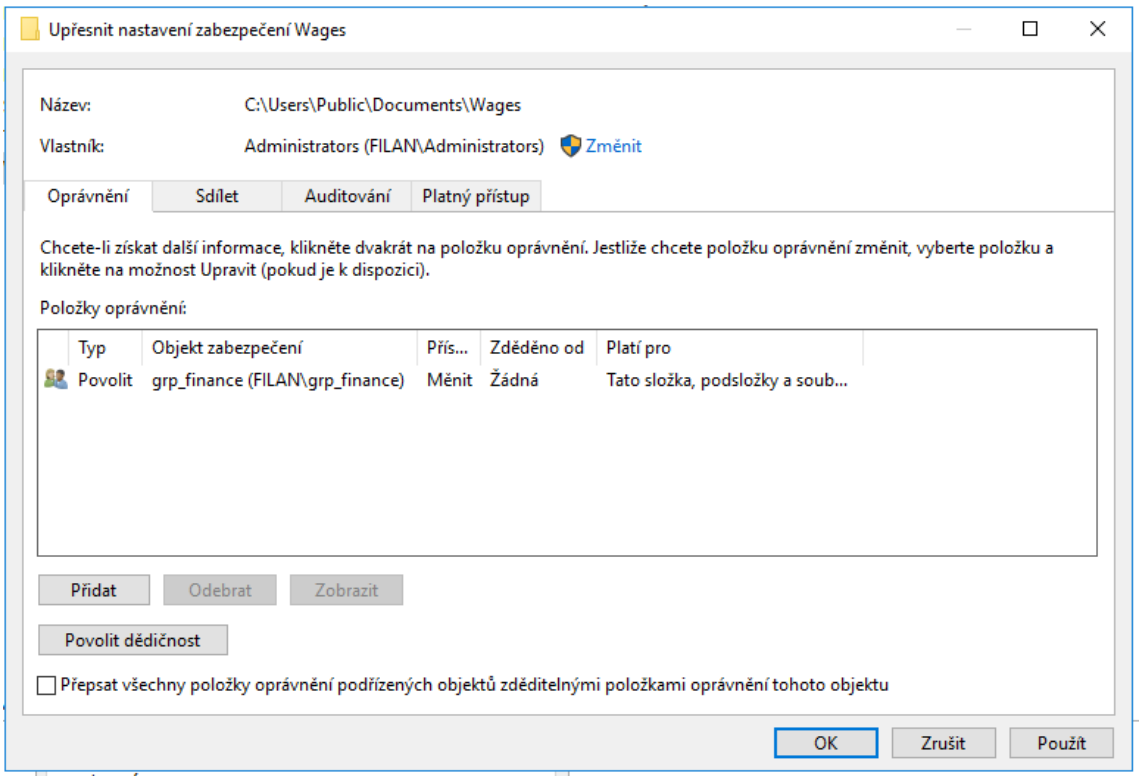
Dle zadání úlohy je požadováno, aby k adresáři **Wages** měla přístup pouze skupina zastupující finanční oddělení grp_finance. Tohoto speciálního případu je možné dosáhnout tak, že bude zakázána dědičnost. Změnu nastavení této funkce můžeme provést v upřesňujících nastaveních zabezpečení pomocí tlačítka **Zakázat dědičnost**. Operační systém zobrazí hlášku, kde je možné se rozhodnout, zda budou stávající oprávnění zkopírována pro další úpravy anebo zda budou

úplně odebrána. V případě adresáře Wages bude zvolena volba pro odebrání veškerých oprávnění k tomuto objektu.



Obr. 47 Vypnutí dědičnosti

Po tomto kroku má k adresáři přístup pouze vlastník a tím je skupina Administrators. Aby byly splněny požadavky zadání úlohy, je potřeba přidat skupinu **grp_finance** a nastavit jí potřebná oprávnění.



Obr. 48 Nastavení oprávnění v adresáři Wages

Těmito kroky je splněno zadání úlohy, kdy k adresáři Wages mají přístup pouze členové skupiny grp_finance.

4.4 Úloha 4 – 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.

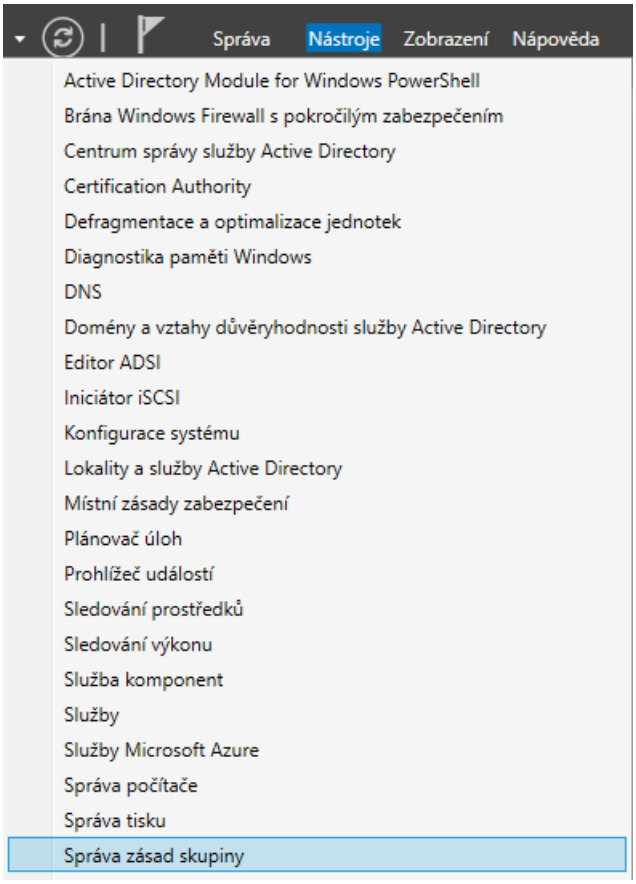
Ve druhé části budou nastaveny zásady skupin tak, aby existovaly v doméně tři typy uživatelských prostředí. Prvním z nich bude prostředí pro administrátory. Druhým bude prostředí pro školitele, kteří vystupují jako pokročilí uživatelé a mají běžná uživatelská oprávnění. Budou tak moci přistupovat např. 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.

4.4.1 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**.

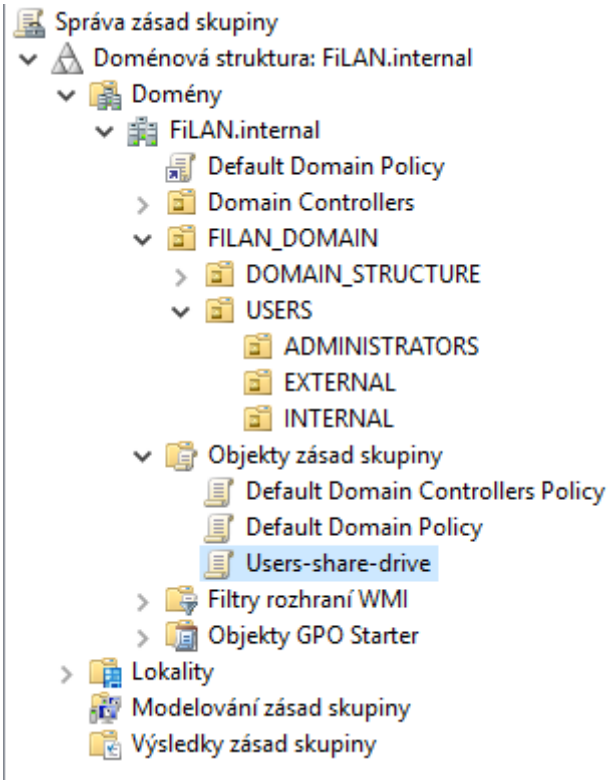


Obr. 49 Správa zásad skupiny ve Správci serveru

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.

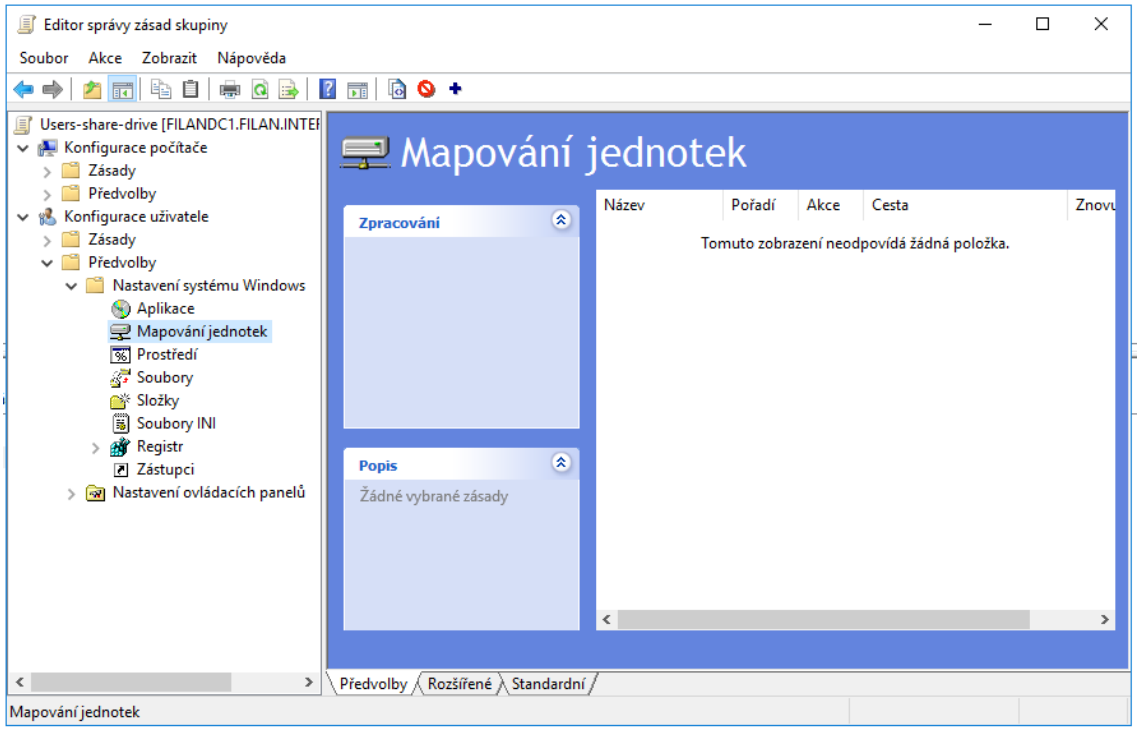
Každý nový objekt by měl být pojmenován vhodným názvem, který ho bude jasně identifikovat, a měl by obsahovat pouze potřebná nastavení. Objekt **Default Domain Policy** by měl obsahovat pouze nastavení účtů, hesel, uzamykání a zásady protokolu Kerberos. Tyto zásady jsou použity na úrovni celé domény 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.



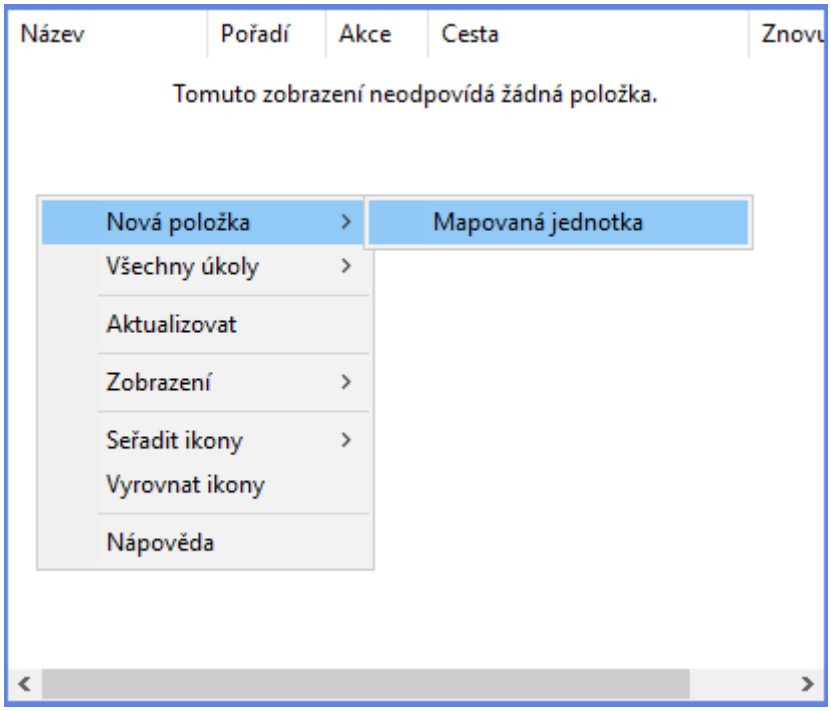
Obr. 50 Vytvoření GPO

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. 51 Editace GPO

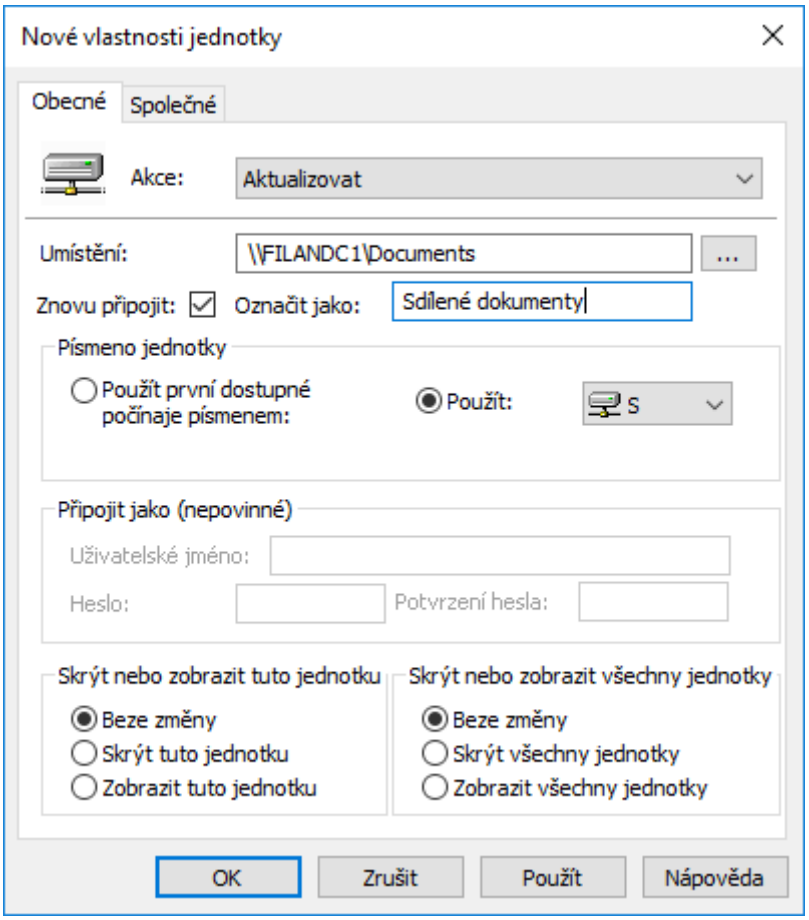
Nová jednotka bude vložena také za pomoci PTM.



Obr. 52 Nastavení mapování jednotky pomocí GPO

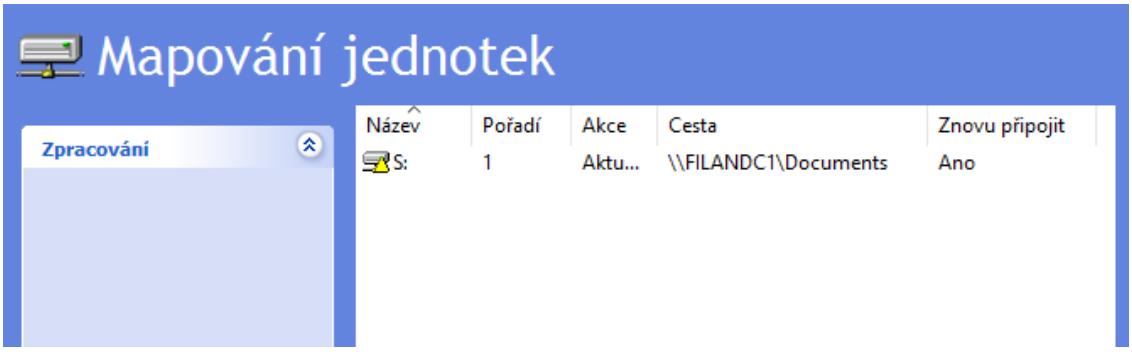
Ve vlastnostech jednotky budou určeny parametry sdíleného disku. V naší úloze se jedná o cestu umístění \\FILANDC1\Documents. Tento sdílený adresář ponese

název **Sdílené dokumenty** a bude označen ke znovupřipojení v případě odpojení. Označením této jednotky je písmeno „S“. Akce, která bude vykonána při použití tohoto pravidla, bude **Aktualizace**, dle zadání úlohy.



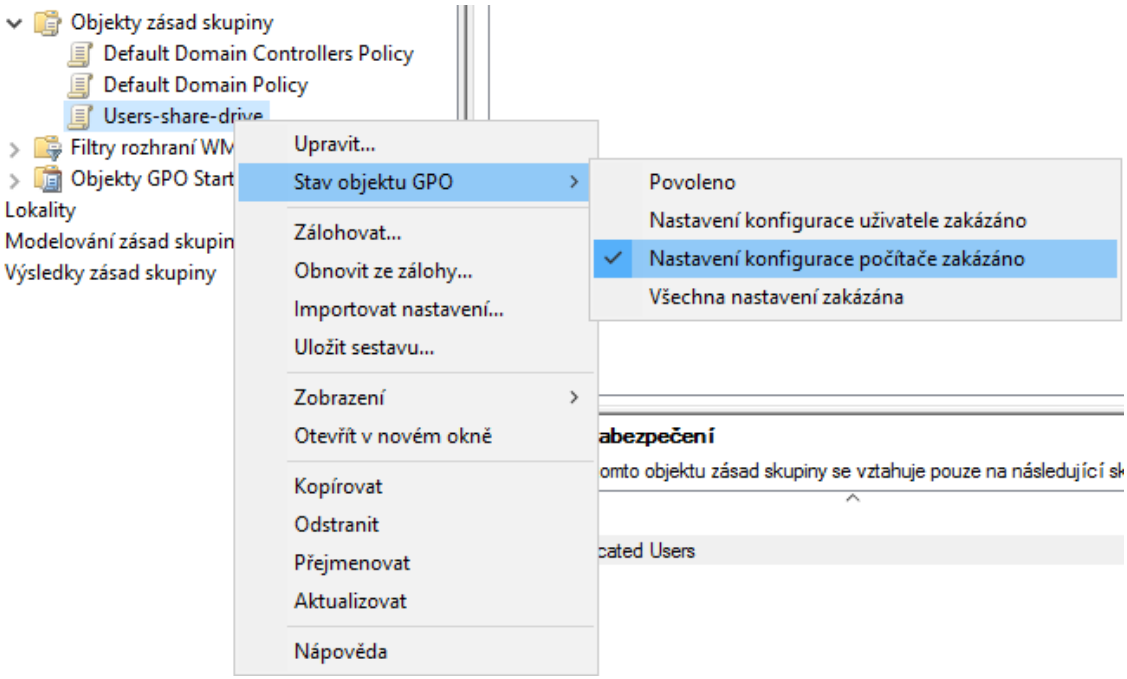
Obr. 53 Vlastnosti mapované jednotky

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



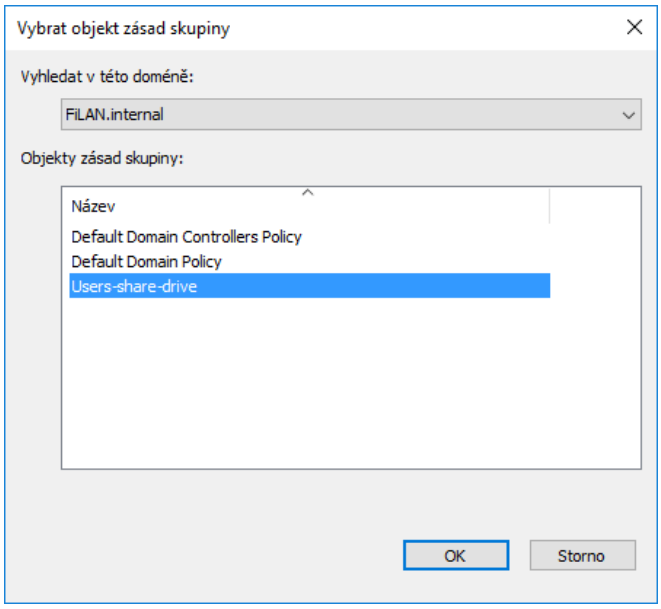
Obr. 54 Mapovaná jednotka S:

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.

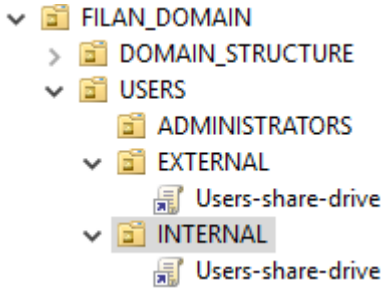


Obr. 55 Konfigurace stavu objektu GPO

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.

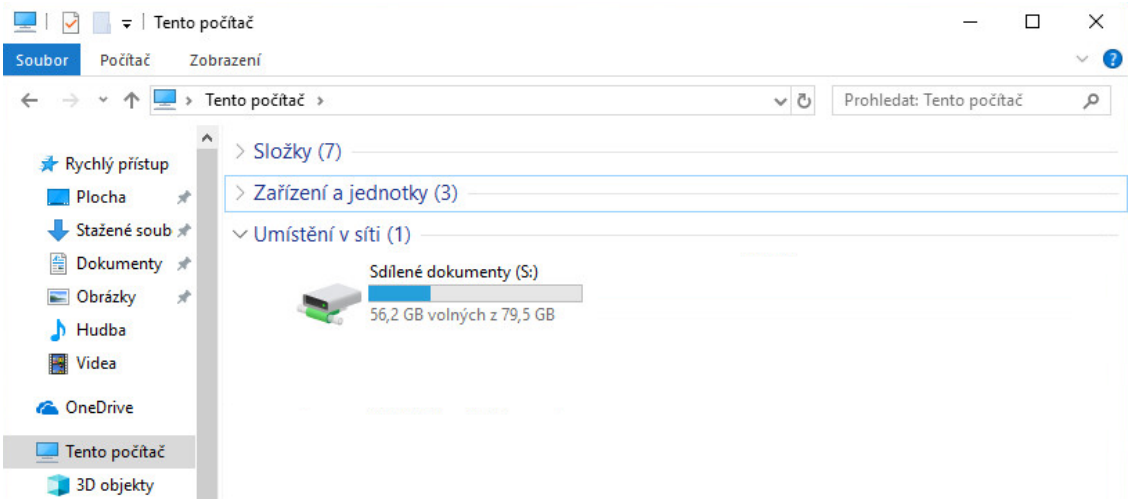


Obr. 56 Propojení GPO s OU



Obr. 57 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.

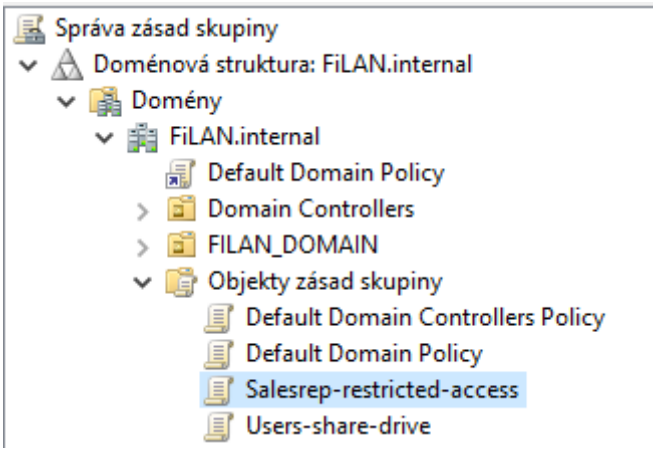


Obr. 58 Automaticky připojený sdílený adresář u klienta

4.4.2 Nastavení uživatelského prostředí

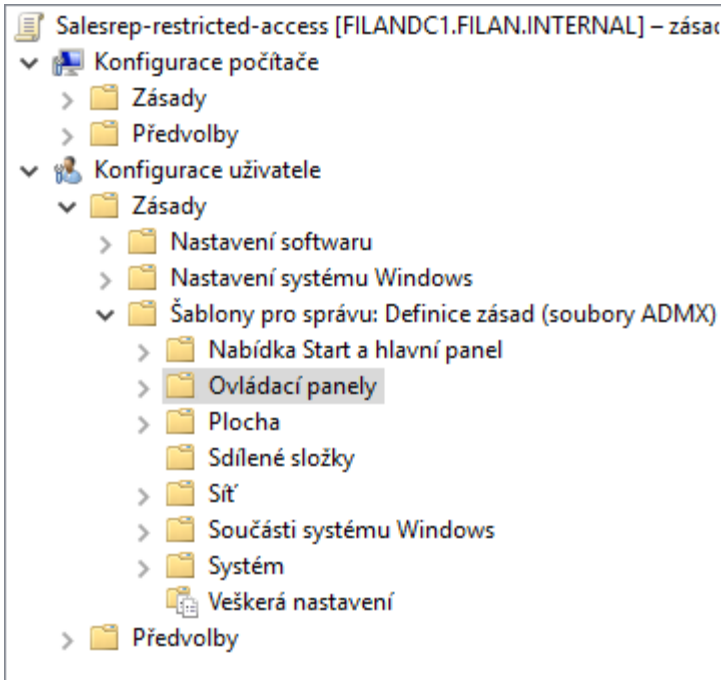
Tato část úlohy je věnována konfiguraci uživatelského prostředí. Zadáním úlohy je vytvořit prostředí pro účty obchodních zástupců, kteří využívají počítače pouze pro vyřizování obchodních aktivit a k absolvování školení. Z těchto důvodů není potřeba, aby měli tito uživatelé přístup k ovládacím prvkům 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**.



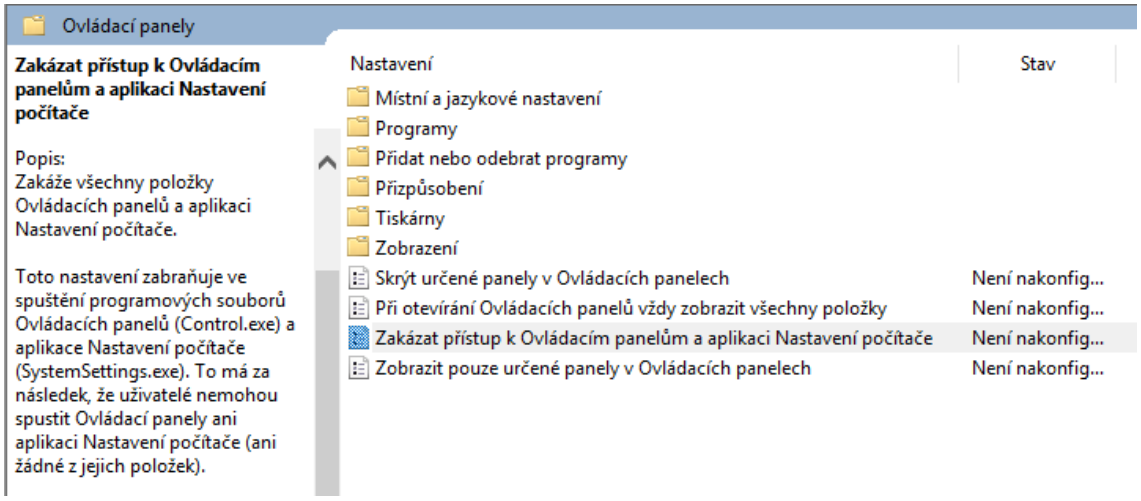
Obr. 59 Vytvoření GPO Salesrep-restricted-access

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.



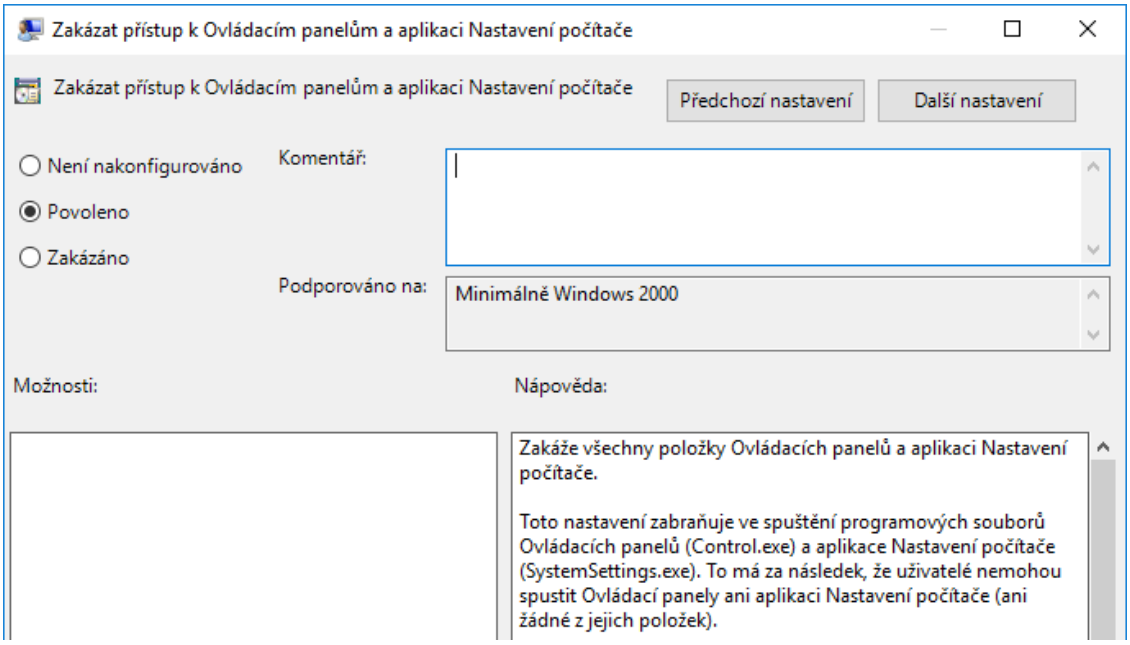
Obr. 60 Konfigurace uživatelských zásad

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. 61 Nastavení omezení přístupu k Ovládacím panelům

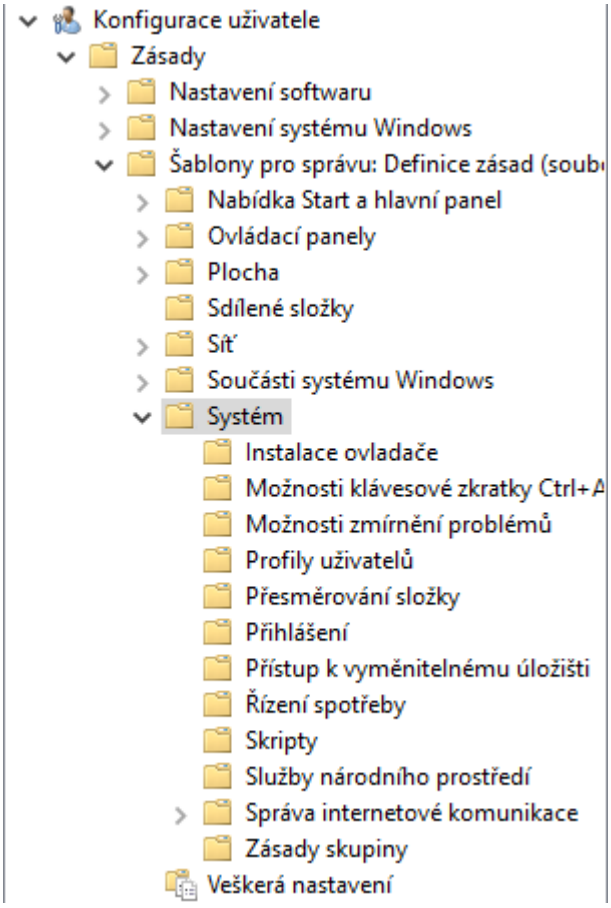
Ve výchozím stavu není zásada nakonfigurována a je potřeba ji povolit. Povolení je možné nastavit v její editaci.



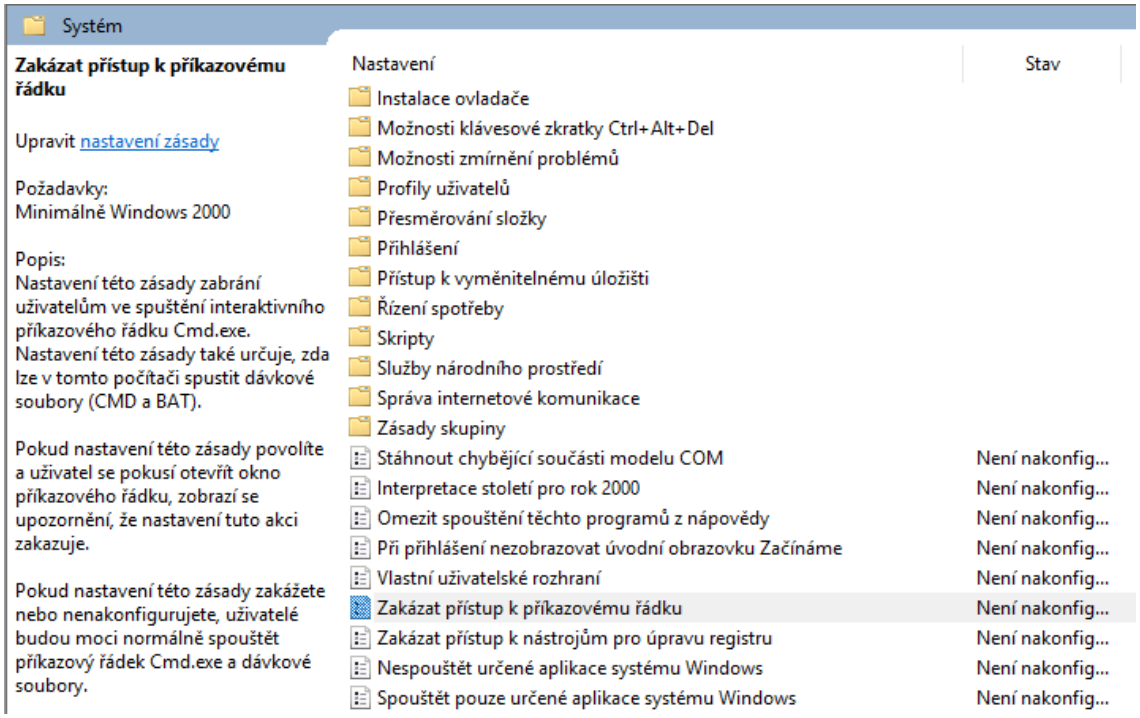
Obr. 62 Povolení zásady

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.

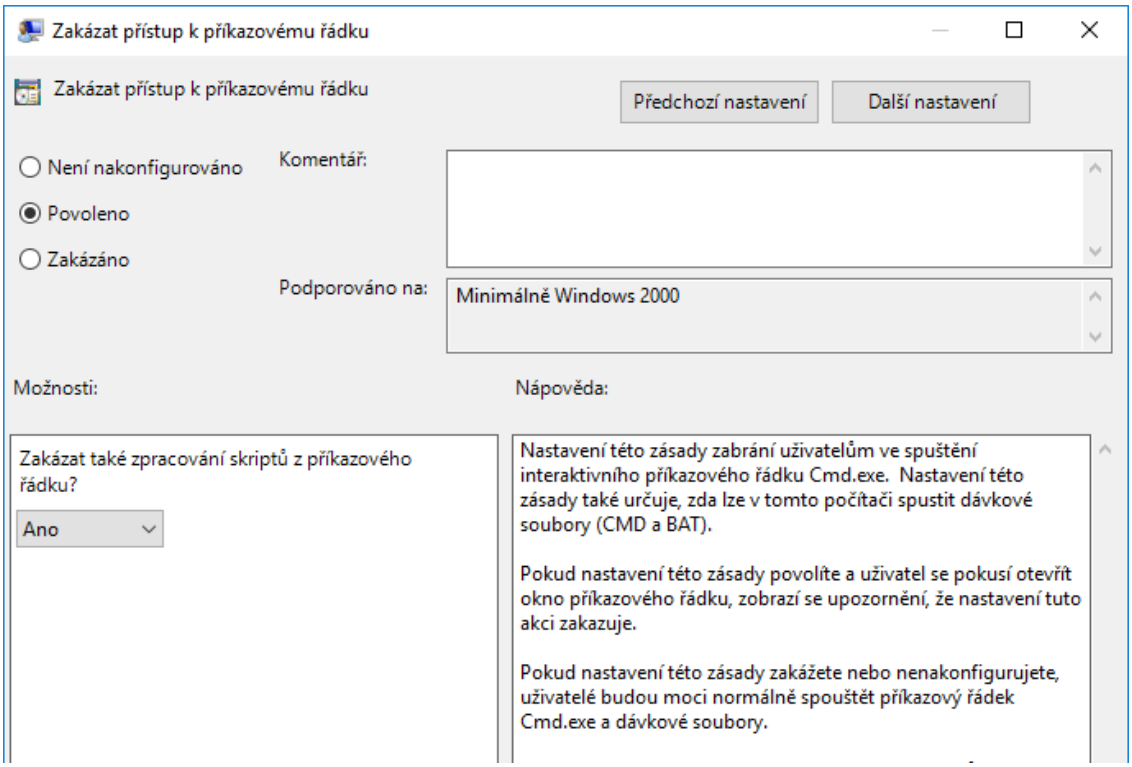


Obr. 63 Umístění zásady zakázání příkazového řádku



Obr. 64 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.

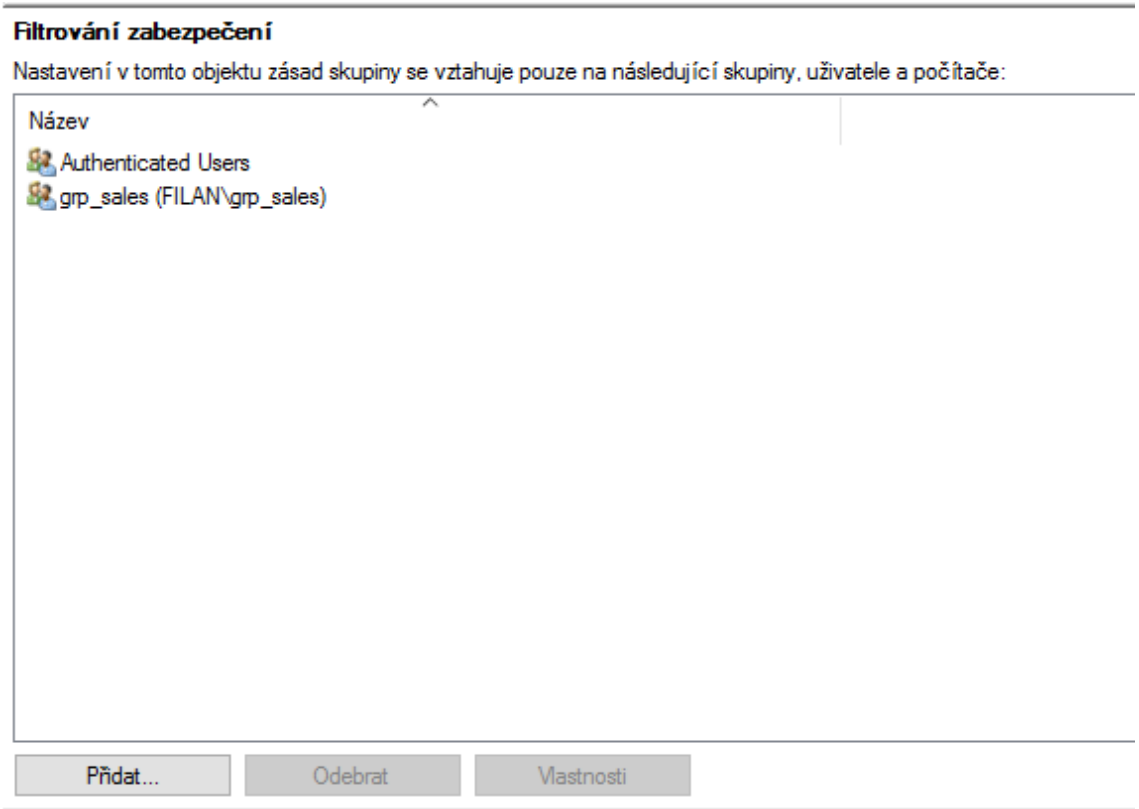


Obr. 65 Povolení zásady

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

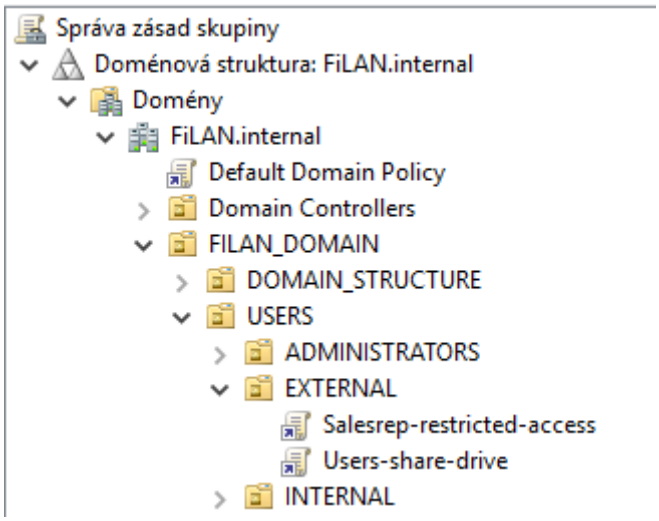
Tento objekt by měl být propojený s OU EXTERNAL, jelikož se v ní nachází účty obchodních zástupců. Propojení s OU SALES by nemělo smysl, protože se v ní nachází pouze skupina pro obchodní zástupce – grp_sales – a ne uživatelské účty.

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.



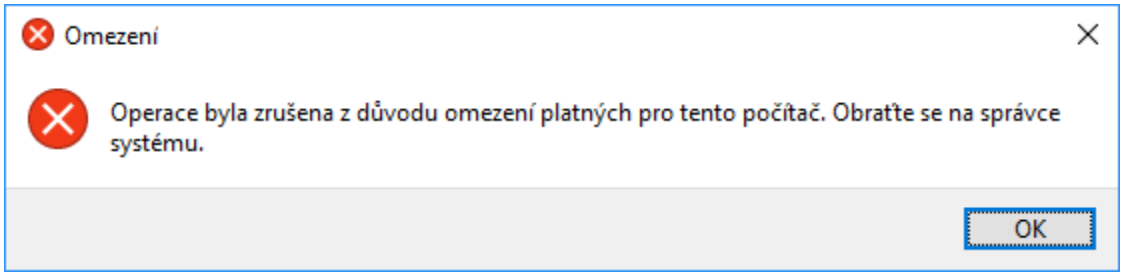
Obr. 66 Filtrování zabezpečení GPO

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

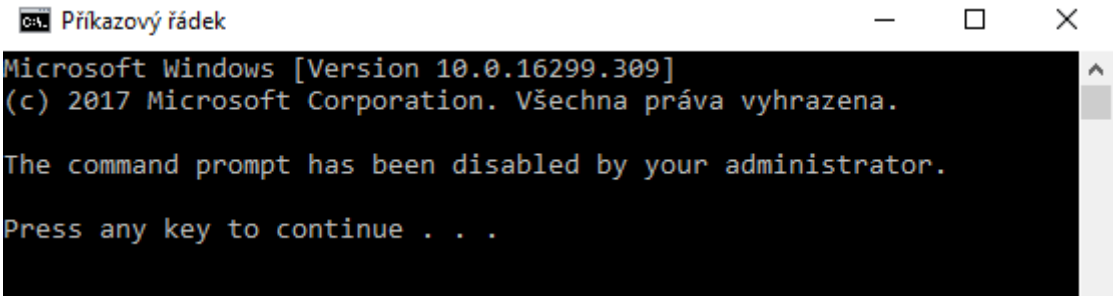


Obr. 67 Aplikace GPO Salesrep-resticted-access

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



Obr. 68 Omezení přístupu k Ovládacím panelům u klienta



Obr. 69 Omezení přístupu k příkazovému řádku u klienta

4.5 Úloha 5 – Konfigurace DNS

DNS server nainstalovaný na serveru FILANDC1 zajišťuje v doméně FiLAN.internal správný překlad doménových jmen na IP adresy a IP adresy na doménová jména. V této úloze je hlavním úkolem vytvoření alespoň jedno záznamu typu **A**, **CNAME** a **MX** v **zóně dopředného vyhledávání** (Forward Lookup Zone) FiLAN.internal.

Na serveru DNS existuje několik typů záznamů a každý z nich plní jiný úkol. Prvním představeným typem je záznam **A**, který je určen k nastavení konkrétní IPv4 adresy jakémukoliv doménovému názvu. Příkladem může být počítač s doménovým názvem FILANPC, který je dosažitelný na adrese 192.168.116.55. Pro IPv6 adresy existuje záznam typu **AAAA**, ale ten nebude v naší úloze použit. Jeho přínos je stejný, jako v případě záznamu typu A.

Dalším typem záznamu je CNAME. **CNAME** (Canonical Name Record) je záznam, který je používán, jako alias k jinému doménovému názvu. Hodnotou tohoto záznamu je pouze textová hodnota. Takový typ záznamu je možné použít např., pokud by měl být server FILANDC1 dosažitelný také pod doménovým názvem

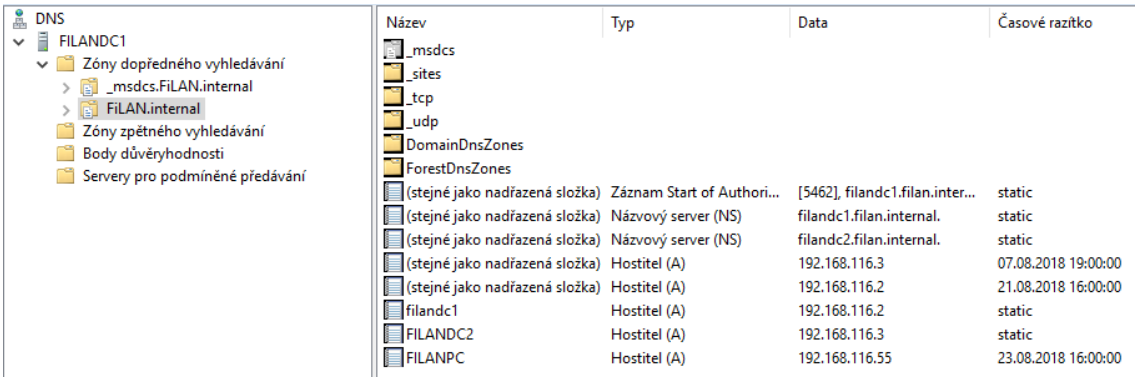
SERVER1. Výhodou tohoto záznamu je, že bude funkční i v případě, že by se změnila IP adresa serveru FILANDC1.

Záznam typu **MX** (Mail Exchange Record) slouží k nastavení názvu poštovního serveru, na který je doručována elektronická pošta. U tohoto typu záznamu je kromě názvu určena také priorita. Platí, že nejvyšší prioritu má poštovní server s nejnižším číslem v záznamu. Pokud je zaslán dotaz na tento typ záznamu a klient nedostane odpověď, automaticky je dotaz předán na další MX záznam v pořadí. Jestliže existují i další záznamy, pak tyto adresy představují záložní mailservery.

4.5.1 Vytváření nových záznamů

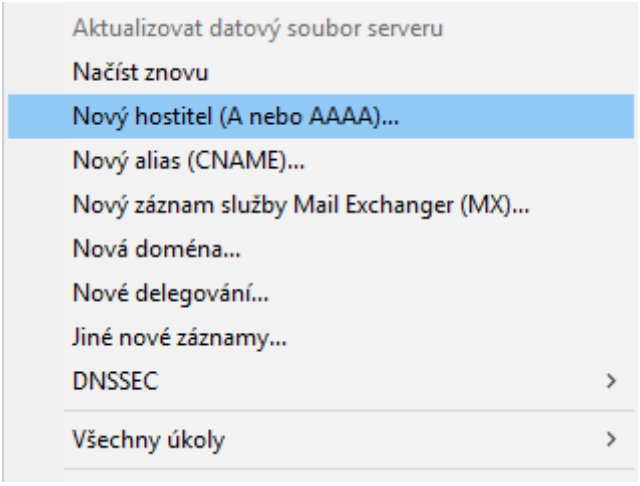
Spravovat DNS server je možné pomocí Správce DNS, který se nachází v Nástrojích Správce serveru.

Po vytvoření domény jsou ve výchozím stavu, v zóně dopředného vyhledávání FiLAN.internal, automaticky vloženy všechny záznamy počítačů, které kontaktovaly DNS server. Vždy se bude jednat alespoň o počítače přidané do domény, protože při ověřování předávají svůj doménový název. Všechny tyto záznamy jsou typu A, tedy pouze doménový název a IPv4 adresa.



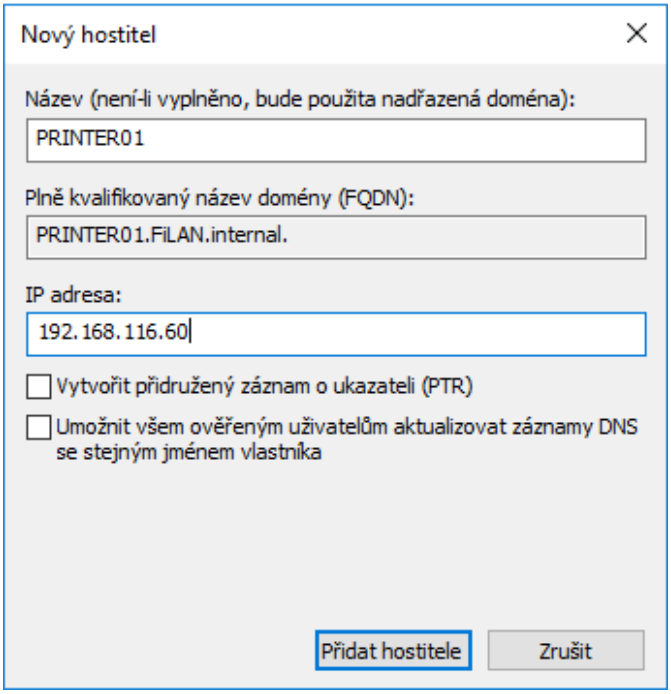
Obr. 70 Výchozí záznamy na DNS serveru

Nový záznam je možné vložit pomocí PTM, kde jsou v kontextové nabídce dostupné různé typy záznamů. Prvním typem je zadání nového hostitele (A nebo AAAA).



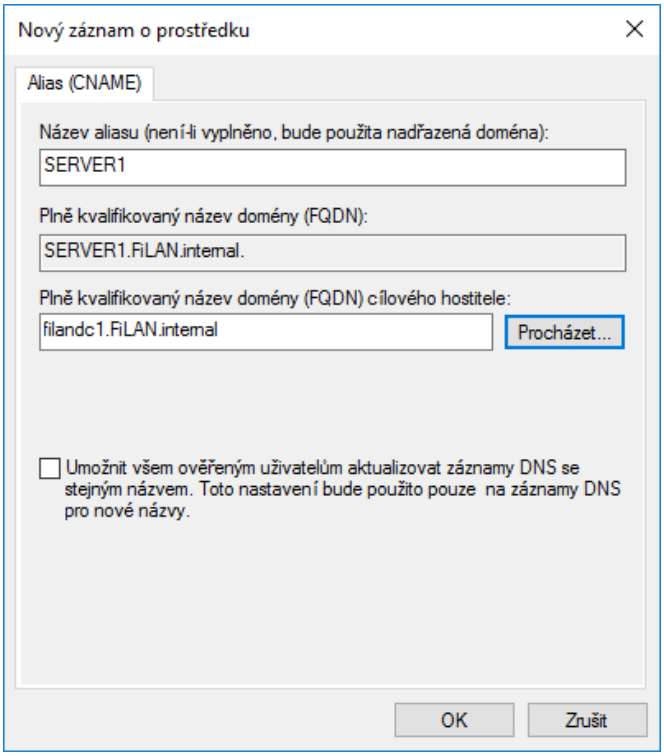
Obr. 71 Vytvoření záznamu typu A

Pro ukázku je použit název záznamu **PRINTER01**, který představuje název síťové tiskárny s IPv4 adresou 192.168.116.60. Tato tiskárna nebyla k síti doposud připojena, proto se automaticky mezi ostatními záznamy nenacházela.



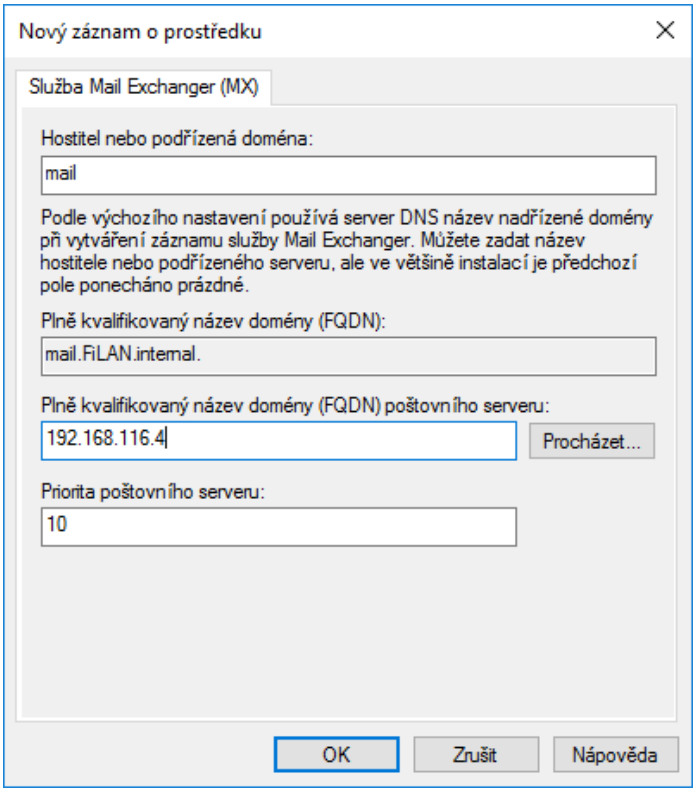
Obr. 72 Nastavení záznamu typu A

Další bude přidán nový alias (CNAME). Tento záznam je pojmenován SERVER1 a je použit jako alias k doménovému řadiči FILANDC1. Po jeho přidání bude možné kontaktovat řadič domény pod názvy FILANDC1 i SERVER1.



Obr. 73 Vytvoření záznamu typu CNAME

Třetím, manuálně vloženým záznamem, bude záznam služby Mail Exchanger (MX). U tohoto záznamu bude zvolen název **mail**. Plně kvalifikovaný název domény představuje IP adresa 192.168.116.4, jelikož v této doméně není zatím žádný funkční poštovní server. Až tento server bude implementován, tak bude dostupný pod názvem **mail.filan.internal**. V našem prostředí bude pouze jeden mailserver a proto stačí použít jeden MX záznam.



Obr. 74 Vytvoření záznamu typu MX

Po úspěšném vytvoření všech předchozích kroků by měl být výpis záznamů stejný jako na Obr. č. 75.

Název	Typ	Data	Časové razítko
_msdcs			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(stejné jako nadřazená složka)	Záznam Start of Authority (S...	[5462], filandc1.filan.inter...	static
(stejné jako nadřazená složka)	Názvový server (NS)	filandc1.filan.internal.	static
(stejné jako nadřazená složka)	Názvový server (NS)	filandc2.filan.internal.	static
(stejné jako nadřazená složka)	Hostitel (A)	192.168.116.3	07.08.2018 19:00:00
(stejné jako nadřazená složka)	Hostitel (A)	192.168.116.2	21.08.2018 16:00:00
filandc1	Hostitel (A)	192.168.116.2	static
FILANDC2	Hostitel (A)	192.168.116.3	static
FILANPC	Hostitel (A)	192.168.116.55	23.08.2018 16:00:00
PRINTER01	Hostitel (A)	192.168.116.60	
SERVER1	Alias (CNAME)	filandc1.FiLAN.internal	
mail	Služba Mail Exchanger (MX)	[10] 192.168.116.4	

Obr. 75 Přehled záznamů po vlastním vložení nových záznamů

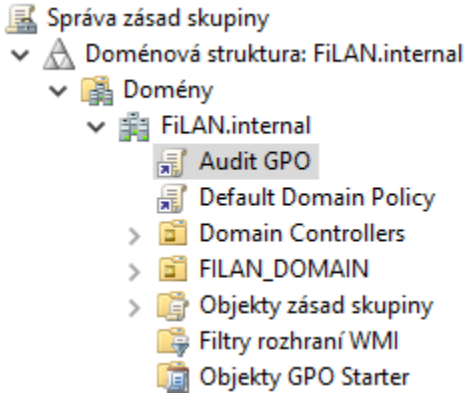
4.6 Úloha 6 – Auditování událostí v doméně

Zadáním úlohy 6 je konfigurace auditování bezpečnostních událostí v doméně, kde bude nastaveno základní logování chování objektů. Do této konfigurace budou spadat běžné události, jako je uzamčení uživatelských účtů a události s žádostí o vyšší oprávnění přístupu.

4.6.1 Vytvoření Audit Policy

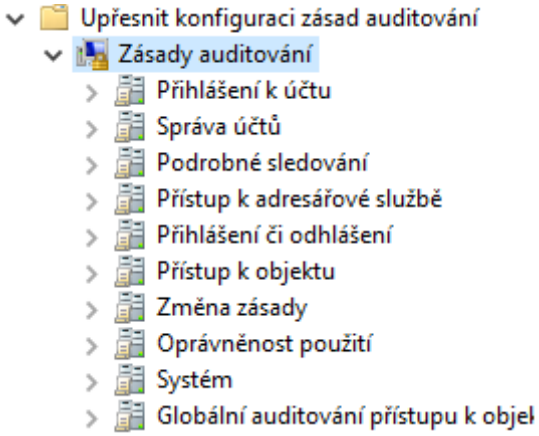
K reportování probíhajících událostí v doméně Active Directory je potřeba nejprve určit jaké události a za jakých podmínek mají být sledovány. Tohoto nastavení lze dosáhnout vytvořením GPO, propojeným s požadovanou skupinou objektů, u kterého bude zvoleno, jaké chování bude monitorováno.

V této úloze bude vytvořen objekt zásad skupiny pojmenovaný „**Audit GPO**“ a bude aplikován na všechny objekty v doméně FiLAN.internal, stejně jako Default Domain Policy.



Obr. 76 Vytvoření Audit GPO

Dalším krokem je konfigurace vytvořeného GPO, ve kterém bude určeno, jaké události mají být administrátorem domény sledovány. Pro potřeby tohoto prostředí jsou zvoleny zásady auditování **Správy účtů** a **Oprávněnosti použití**. Pomocí těchto zásad budou sledovány události při změnách účtů v počítačích, dále při vytvoření, změně, odstranění a uzamčení účtu uživatele a události s žádostí o povolení vyšší úrovně oprávnění. Cesta k nalezení těchto zásad v editoru je: Konfigurace počítače\ Zásady\ Nastavení systému Windows\ Nastavení zabezpečení\ Upřesnit konfiguraci zásad auditování\ Zásady auditování.



Obr. 77 Cesta k zásadám auditování

V podkategorii **Správa účtů** jsou nastaveny audity pro správu účtů počítače a pro správu účtů uživatelů. U obou těchto možností budou sledovány pouze úspěšné kontroly auditu.

Podkategorie	Události auditování
Auditovat správu skupin aplikací	Není nakonfigurováno
Auditovat správu účtů počítače	Úspěch
Auditovat správu skupin distribuce	Není nakonfigurováno
Auditovat jiné události správy účtu	Není nakonfigurováno
Auditovat správu skupiny zabezpečení	Není nakonfigurováno
Auditovat správu účtů uživatelů	Úspěch

Obr. 78 Auditování účtů počítačů a uživatelů

V podkategorii **Oprávněnost použití** bude zvoleno monitorování úspěšných i neúspěšných událostí v případě použití citlivých oprávnění. Po nakonfigurování této možnosti bude docházet k informování administrátora o každé události s žádostí o oprávnění správce. Taková volba je vhodná k upozornění administrátora před možnými útoky a nastavení potřebné úrovně zabezpečení.

Podkategorie	Události auditování
Auditovat použití oprávnění, která nejsou citlivá	Není nakonfigurováno
Auditovat události použití jiných oprávnění	Není nakonfigurováno
Auditovat použití citlivých oprávnění	Úspěchy a chyby

Obr. 79 Auditování použití citlivých oprávnění

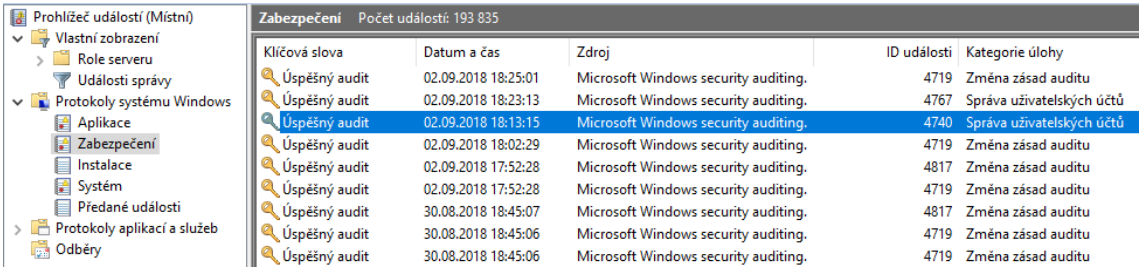
Výsledkem použitých zásad auditování by měl být stejný stav, jako na Obr. 80.

Souhrn

Kategorie	Konfigurace
Přihlášení k účtu	Není nakonfigurováno
Správa účtů	Nakonfigurováno
Podrobné sledování	Není nakonfigurováno
Přístup k adresářové službě	Není nakonfigurováno
Přihlášení či odhlášení	Není nakonfigurováno
Přístup k objektu	Není nakonfigurováno
Změna zásady	Není nakonfigurováno
Oprávněnost použití	Nakonfigurováno
Systém	Není nakonfigurováno
Globální auditování přístupu k objektům	Není nakonfigurováno

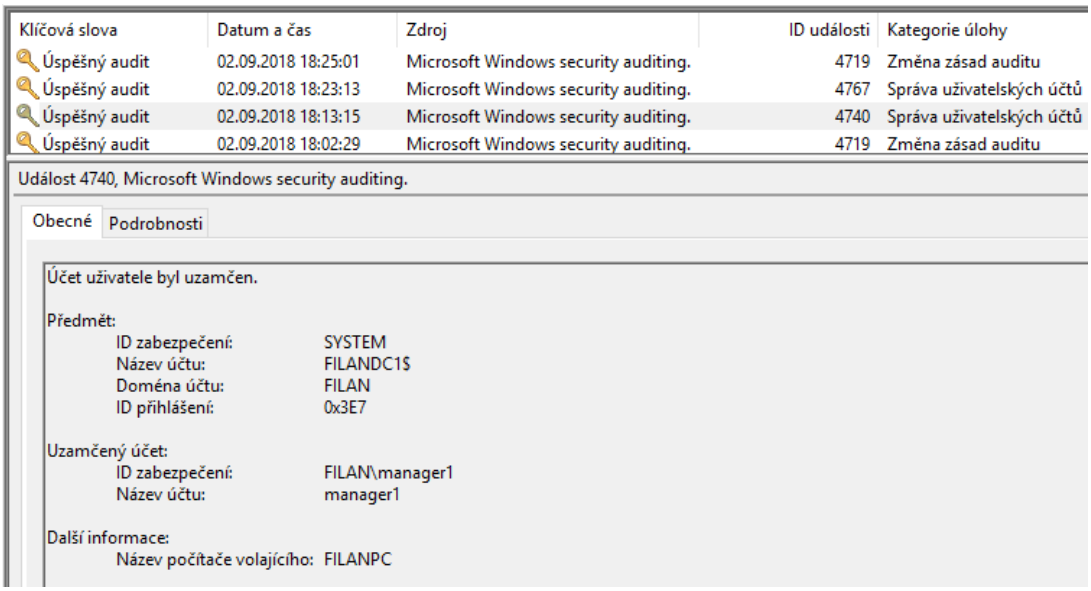
Obr. 80 Přehled nastavených zásad auditování

Zaznamenané události je poté možné sledovat v Prohlížeči událostí na doménových řadičích mezi protokoly zabezpečení.



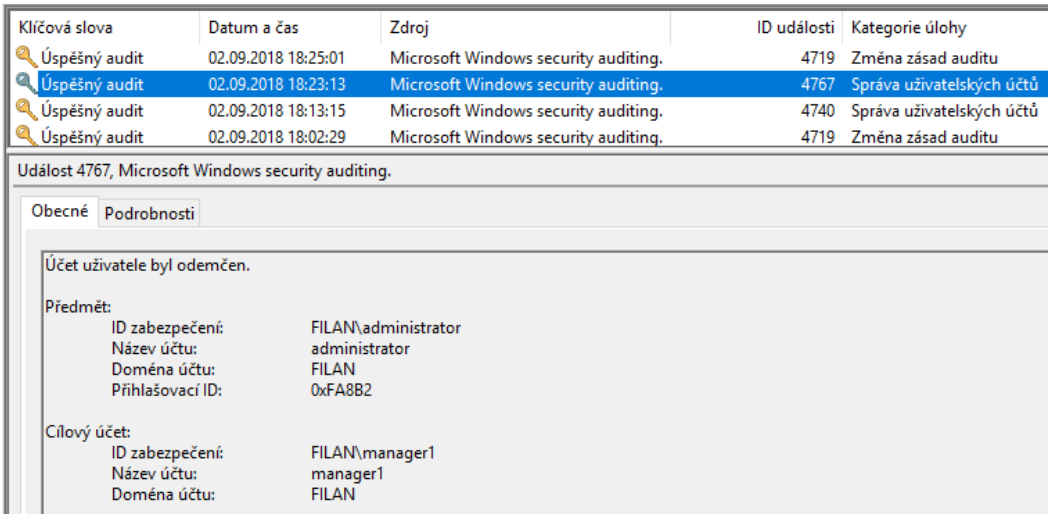
Obr. 81 Prohlížeč událostí na DC

Prvním příkladem ověření funkčnosti nastaveného auditu může být událost s ID 4740, která oznamuje, že došlo k **uzamčení** uživatelského účtu **manager1** na počítači **FILANPC**.



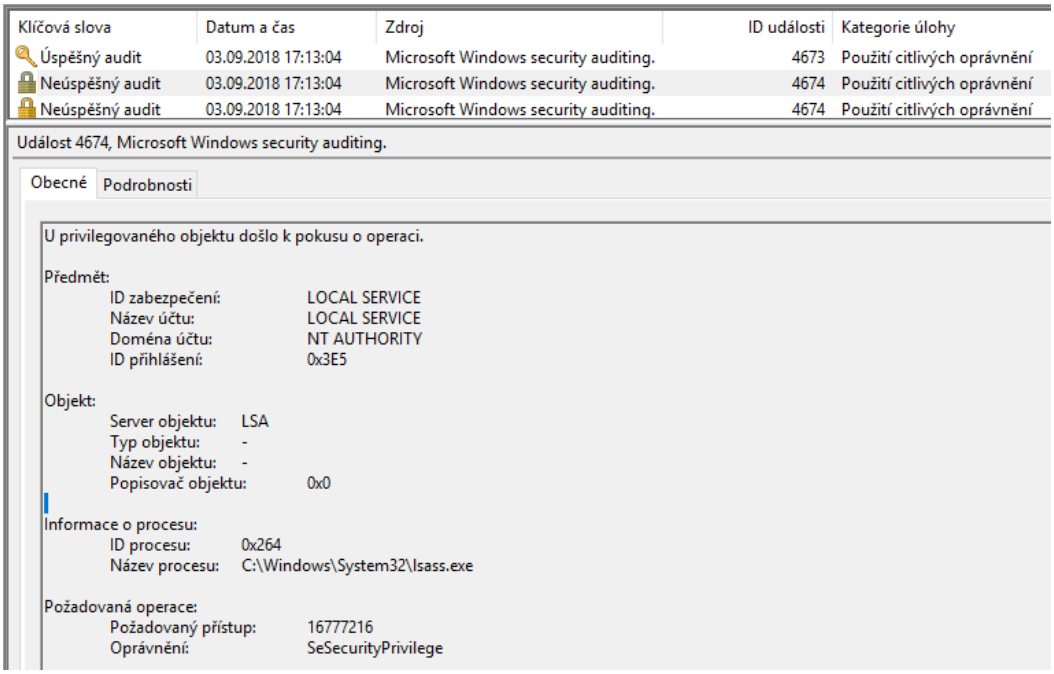
Obr. 82 Úspěšný audit uzamčeného uživatelského účtu

Přibližně 10 minut po této události došlo k manuálnímu odemčení uživatelského účtu **manager1** účtem **Administrator**, při kterém vznikla událost auditu s ID 4767.



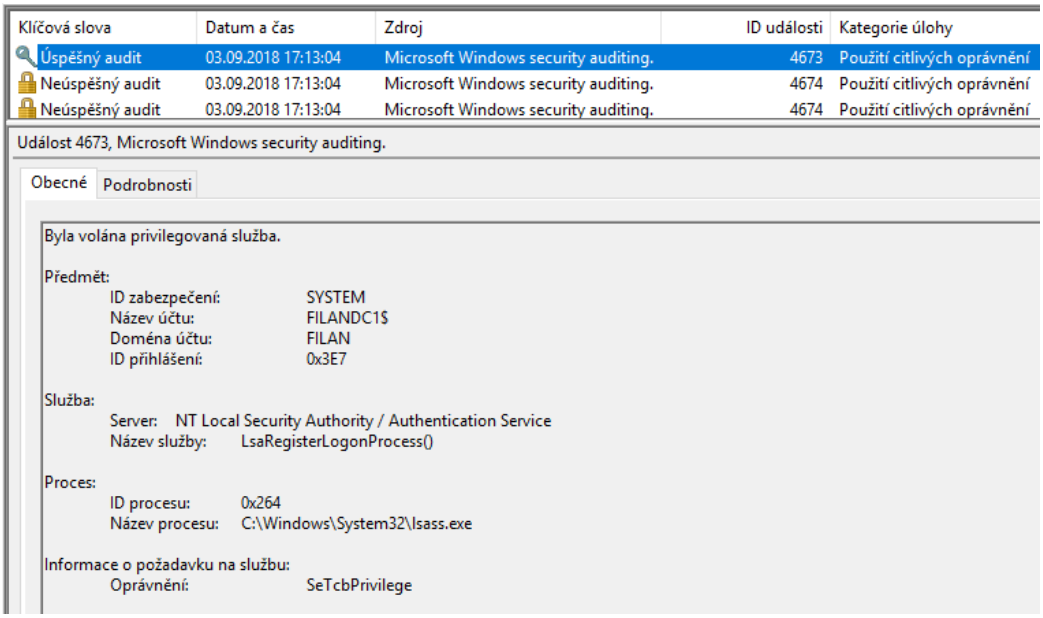
Obr. 83 Úspěšný audit administrátorem odemčeného účtu

Dalším příkladem můžou být události zaznamenávající použití **citlivých/privilegovaných** oprávnění. U GPO Audit Policy bylo nastaveno sledování takovýchto událostí v případě úspěchu i neúspěchu. Na Obr. 84 je zobrazen neúspěšný audit události s ID 4674, kdy došlo k zadání špatného hesla pro účet Administrator.



Obr. 84 Neúspěšný audit privilegovaného přístupu

Ve chvíli, kdy došlo k zadání správného hesla pro požadovaný privilegovaný přístup, vznikla událost s ID 4673, kde proběhl úspěšný audit této události.



Obr. 85 Úspěšný audit privilegovaného přístupu

Zajímavým faktem je, že v prohlížeči událostí je možné zaznamenat vytvoření více záznamů ve výpisu, po vykonání pouze jedné události. V prostředí Microsoft Windows domény existuje spousta dalších možností, jaké události a na jaké úrovni je možné sledovat. Jejich vytvoření závisí pouze na zadaných požadavcích.

5 Závěry a doporučení

Cílem práce bylo vytvořit návrh logické struktury Active Directory pro potřeby středně velké firmy ve formě step-by-step návodu určenému všem, kteří se rozhodnou pro implementaci doménového prostředí Windows.

Teoretická část bakalářské práce měla za úkol čtenáře seznámit s fungováním služeb Active Directory a DNS a důležitými pojmy používanými v těchto okruzích.

V praktických úlohách byl předveden způsob, jakým je možné tyto služby použít v reálném prostředí.

Pro vytvoření domény v AD bylo důležitým krokem určení vhodného názvu. V takto vytvořené doméně byly dále prováděny další úlohy.

Následujícím krokem bylo navržení organizační struktury, na kterou bylo poté možné použít odpovídající oprávnění přístupů ke sdíleným souborům. Mimo sdílení souborů bylo možné hierarchii použít také ke konfiguraci a aplikaci GPO.

Zbylé praktické úlohy byly o nastavení služby DNS a vytvoření auditování vzniklých událostí v doméně.

Oblast Windows domén je velice rozsáhlá a nebylo možné zahrnout veškeré možnosti, které mohou v reálném prostředí nastat. V prostředí Active Directory je možné aplikovat spoustu dalších funkcionalit, které jsou velice užitečné. Takovými funkcemi může být vytvoření souborového serveru, DHCP serveru nebo WSUS (Windows Server Update Services). Tyto další možnosti by mohly být vhodným obsahem obdobné práce.

6 Seznam použité literatury

1. **Miroslav, Pokorný.** TNPW1. *O Active Directory.* [Online] [Citace: 7. 7 2018.] http://lide.uhk.cz/fim/student/pokormi2/tnpw1/.

2. **Corporation, Microsoft.** What are domains and forests? [Online] 22. 7 2018. https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc759073(v=ws.10).

3. **Bouška, Petr.** SAMURAJ-cz.com. [Online] [Citace: 12. 7 2018.] https://www.samuraj-cz.com/clanek/active-directory-komponenty-domain-tree-forest-site/.

4. **Corporation, Microsoft.** Active Directory Domain Services. [Online] 21. 7 2018. https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/active-directory-domain-services.

5. **Bouška, Petr.** Group Policy - řízení aplikace a politik. *SAMURAJ-cz.com.* [Online] 12. 12 2010. [Citace: 25. 7 2018.] https://www.samuraj-cz.com/clanek/group-policy-rizeni-aplikace-politik/.

6. **Alena Kabelová, Libor Dostálek.** *Velký průvodce protokoly TCP/IP a systémem DNS 5. aktualizované vydání.* Brno : Computer Press, 2012. ISBN 978-80-251-2236-5.

7. **Adaptic, s. r. o. – tvorba webu, webdesign.** Co je DNS. *adaptic.cz.* [Online] [Citace: 19. 7 2018.] http://www.adaptic.cz/znalosti/slovnicek/dns/.

8. **CZ.NIC.** O doménách a DNS. [Online] [Citace: 19. 7 2018.] https://www.nic.cz/page/312/o-domenach-a-dns/.

9. **Corporation, Microsoft.** Planning Global Catalog Server Placement. *Microsoft Docs.* [Online] 31. 5 2017. [Citace: 12. 08 2018.] https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/planning-global-catalog-server-placement.

10. **Allen, Robert.** Group Policy Best Practices. *activedirectorypro.com.* [Online] 24. 12 2016. [Citace: 22. 8 2018.] https://activedirectorypro.com/group-policy-best-practices/.

Univerzita Hradec Králové
Fakulta informatiky a managementu
Akademický rok: 2018/2019

Studijní program: Aplikovaná informatika
Forma: Kombinovaná
Obor/komb.: Aplikovaná informatika (ai3-k)

Podklad pro zadání BAKALÁŘSKÉ práce studenta

PŘEDKLÁDÁ:	ADRESA	OSOBNÍ ČÍSLO
Antoš Filip	Březno 156, Březno	I14480

TÉMA ČESKY:

Efektivní návrh služby Active Directory pro potřeby středně velké firmy

TÉMA ANGLICKY:

VEDOUCÍ PRÁCE:

Mgr. Josef Horálek, Ph.D. - KIT

ZÁSADY PRO VYPRACOVÁNÍ:

Cílem bakalářské práce je návrh logické struktury Active Directory v prostředí středně velké firmy. Autor v teoretické části práce představí technologii Active Directory, její komponenty, role serverů Active Directory, problematiku domén a vztah AD se službou DNS. V praktické části budou získané poznatky aplikovány v podobě praktických úloh konfigurací Windows Server 2016 a využití jednotlivých funkcionalit AD ve formě deseti paktickckých úloh. Ulohy budou zpracovány ve formě step-by-step postupů využitelných jako pokročilé laboratorní úlohy pro předmět OS1.

SEZNAM DOPORUČENÉ LITERATURY:

PANEK, William. MCSA Windows Server 2016 Study Guide: Exam 70-741. 1. New York, United States: John Wiley, 2017. ISBN 9781119359333.

STANEK, William. Active Directory Infrastructure Self-Study Training Kit : Stanek & Associates Training Solutions. 1. United States: Createspace, 2015. ISBN 9781514780619.

Podpis studenta: ..... **Datum:** .....

Podpis vedoucího práce: ..... **Datum:** .....