

UNIVERZITA PALACKÉHO V OLOMOUCI
PEDAGOGICKÁ FAKULTA



Katedra technické a informační výchovy

Michal Chmel

SPRÁVA POČÍTAČOVÉ UČEBNY POMOCÍ ACTIVE
DIRECTORY DOMAIN SERVICES

Bakalářská práce

Vedoucí práce: doc. PhDr. Milan Klement, Ph.D.

Olomouc 2017

Prohlašuji, že jsem bakalářskou práci s názvem „Správa počítačové učebny pomocí Active Directory Domain Services“ vypracoval samostatně a s použitím uvedených pramenů.

V Olomouci dne 21.4.2017

.....
Michal Chmel

Poděkování

Touto cestou bych velmi rád poděkoval vedoucímu práce doc. PhDr. Milanu Klementovi, Ph.D. za cenné rady, připomínky a odborné vedení při zpracování této kvalifikační práce.

Obsah

ÚVOD	6
1 CENTRALIZACE	8
1.1 CENTRALIZACE A DECENTRALIZACE	8
2 MICROSOFT WINDOWS SERVER	9
2.1 LICENCE WINDOWS SERVER 2012 R2	9
2.2 HARDWAROVÉ POŽADAVKY	10
2.3 ROLE, SLUŽBY ROLÍ A FUNKCE.....	11
3 ACTIVE DIRECTORY DOMAIN SERVICES	13
3.1 DOMÉNA A DOMÉNOVÝ LES	13
3.2 DOMAIN CONTROLLER	14
3.3 ORGANIZAČNÍ JEDNOTKY.....	14
3.4 GROUP POLICY.....	15
4 SLUŽBA DNS	16
4.1 DŮLEŽITÉ POJMY SLUŽBY DNS	16
4.2 ZÓNY DNS	17
4.3 ACTIVE DIRECTORY DNS.....	17
5 FILE AND STORAGE SERVICES	18
5.1 SDÍLENÍ SLOŽEK	19
5.2 NTFS	19
6 WINDOWS SERVER BACKUP	20
6.1 TYPY ZÁLOH.....	21
7 SLUŽBA DHCP	22
7.1 DORA PROCES.....	23
7.2 DHCP SCOPE	23
7.3 EXKLUZE A REZERVACE.....	24
8 PLÁNOVÁNÍ POČÍTAČOVÉ UČEBNY	24
8.1 FYZICKÝ NÁVRH UČEBNY.....	25
8.2 DOMÉNOVÁ STRUKTURA.....	26
9 INSTALACE SERVERU A POTŘEBNÝCH SLUŽEB	27
9.1 SERVER MANAGER.....	28

9.2	INSTALACE A KONFIGURACE OPERAČNÍHO SYSTÉMU	29
9.3	INSTALACE A KONFIGURACE ROLE ACTIVE DIRECTORY	30
9.4	INSTALACE A KONFIGURACE SLUŽBY DHCP	31
9.5	INSTALACE A KONFIGURACE FUNKCE WINDOWS SERVER BACKUP	33
10	TVORBA A SPRÁVA DOMÉNOVÝCH OBJEKTŮ	35
10.1	TVORBA OBJEKTŮ	35
10.2	TVORBA DOMÉNOVÝCH PRÁV	39
11	TVORBA SDÍLENÉHO ÚLOŽIŠTĚ	42
11.1	OSOBNÍ SOUBORY	42
11.2	SDÍLENÉ SOUBORY	44
	ZÁVĚR	46
	SEZNAM ILUSTRACÍ A TABULEK	48
	SEZNAM POUŽITÉ LITERATURY	49
	ANOTACE	53

Úvod

Není žádnou novinkou, že se na každé škole dnes setkáme s počítači¹. Počítače se staly nedílnou součástí našich životů, a tak je přirozené, že se tyto technologie využívají i ve školním prostředí. Notebooky jsou již nezbytnou součástí univerzitního studia, avšak na středních a základních školách tomu tak ještě často není. Na těchto institucích jsou hlavním nástrojem k poznávání světa informačních technologií počítačové učebny. Stále více studentů má zájem se naučit efektivně využívat informační technologie, a školy se snaží této skutečnosti přizpůsobit. Čeká nás budoucnost, ve které bude počítač nezbytnou součástí výbavy každého žáka.

Je tedy potřeba se zamyslet, jak tyto technologie co nejefektivněji spravovat. Počítačové učebny dnes musí být schopny uspokojit nejrůznější nároky studentů. Už se nejedná pouze o klasickou výuku informační výchovy. Počítače můžeme využít také při výuce angličtiny, matematiky, výtvarné výchovy, hudební výchovy, ale také moderních předmětů jako je design a animace. Každý student těchto předmětů má samozřejmě úplně jiné nároky na to, co by měla jeho pracovní stanice obsahovat. Studenti by měli mít možnost si prostředí své pracovní stanice upravit tak, aby vyhovovalo jejich osobním potřebám a nemuseli brát ohled na ostatní studenty.

Klasické propojení počítačů pomocí domácí nebo pracovní skupiny sice umožňuje určit jednoduchá pravidla sdílení složek a souborů, ale nikdy nedosáhne komplexnosti domény. Tedy situace, kdy je organizace učebny řízena z jednoho místa pomocí serveru, kterému jsou pracovní stanice hierarchicky podřízené. Tato hierarchická struktura, neboli doména, nám tedy umožňuje převzít úplnou kontrolu nad organizací uživatelů a stanic učebny.

Tato práce si klade za cíl ukázat některé výhody využití platformy Microsoft Windows Server zejména jeho služeb Active Directory pro správu počítačové učebny. Hlavním cílem je zefektivnit organizaci počítačové učebny tak, aby se nejen zjednodušila samotná správa, ale aby měli studenti k dispozici vždy takové pracovní prostředí, které bude přesně odpovídat jejich individuálním potřebám.

¹ Pod tímto pojmem pro zjednodušení, shrnujeme různé typy zařízení jako jsou osobní počítače, notebooky, netbooky a některé typy dotykových zařízení.

V prvních sedmi kapitolách se zaměřujeme na teoretické základy a popis jednotlivých funkcí, které jsou potřebné pro pochopení podstaty a výhod, které Windows Server nabízí. První kapitola vymezuje pojem centralizace a představí výhody tohoto typu organizace. Další kapitola se zaměřuje na samotný Microsoft Windows Server a jeho součásti. Třetí kapitola popisuje službu Active Directory Domain Services a její součásti potřebné v rozsahu této práce. Čtvrtá kapitola popisuje fungování služby DNS. Další kapitola objasňuje pojem File Server a roli File and Storage Services, která je nezbytnou součástí pro tvorbu centralizovaného úložiště. Šestá kapitola teoretické části se zabývá problematikou zálohování a možností zálohování operačního systému Microsoft Windows Server. Kapitola sedmá se věnuje službě DHCP, která velmi usnadňuje správu a troubleshooting, ačkoliv není nezbytnou součástí domény a AD DS.

Kapitoly osm až jedenáct se věnují uvedením těchto poznatků do praxe. Na názorném příkladu popisujeme samotnou implementaci potřebných funkcí a služeb v souladu s potřebami konkrétní učebny a jejich uživatelů. Vzhledem k obsáhlosti tématu a náročnosti procesu je tato část pouze nastíněním toho, jak by jednotlivé funkce měly fungovat. Kapitola osmá se zabývá fyzickým plánem učebny, tedy návrhem, jak by měla učebna vypadat, a také jak bude uživatelsky rozdělena. Devátá kapitola objasňuje proces instalace a základní konfigurace serveru a potřebných služeb a funkcí. Kapitola desátá popisuje proces tvorby doménových objektů a aplikaci doménových práv. Poslední kapitola vysvětluje proces tvorby sdíleného úložiště.

1 Centralizace

Tato kapitola se bude věnovat objasnění pojmu centralizace a jejím typům. Jelikož je cílem této práce přetvořit necentralizovanou počítačovou učebnu na centralizovanou, je vymezení pojmu centralizace zásadní. Než se tedy budeme zabývat jednotlivými součástmi Microsoft Windows serveru, je potřeba objasnit na jakém principu vlastně centrálně organizovaná správa funguje a jaké jsou její výhody.

Co je to Centralizace?

Pojem centralizace označuje způsob řízení tzv. „shora dolů“, kdy největší odpovědnost leží na objektu, který stojí na vrcholu. Dále také tento pojem označuje rozložení objektů určitého systému tak, že nejdůležitější a řídicí součásti jsou soustředěny na jednom místě (1).

1.1 Centralizace a Decentralizace

Na samotných počátcích komunikačních technologií, byly všechny komunikační sítě centralizované. V roce 1964 představil Paul Baran pojem decentralizace, který měl zásadně vylepšit fungování telefonní komunikace. Hlavní nevýhodou centralizace je totiž fakt, že jakmile dojde k přerušení spojení s centrem, všechny závislé systémy přestanou být použitelné. Decentralizace tento problém řeší rozmístěním těchto důležitých, centrálních součástí do několika center. Pokud tak jedno z těchto center vypadne, ostatní centra můžou bez problému fungovat dál, viz. obrázek 1 (2).

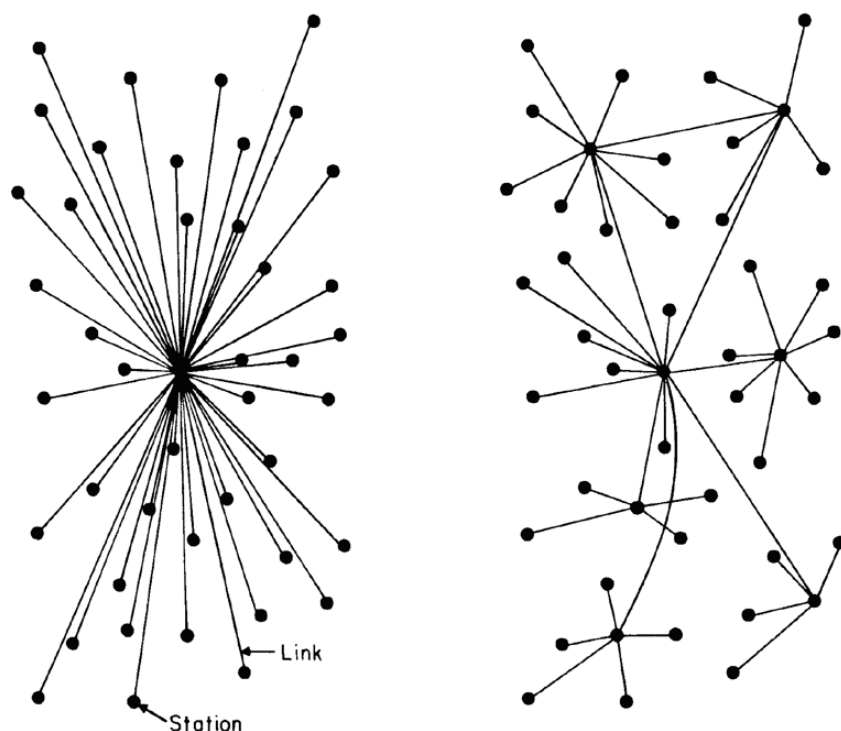
Každý z těchto typů organizace má své nesporné výhody. V případě decentralizované správy jsou to převážně (3):

- vzájemná nezávislost jednotlivých uzlů,
- redundance kritických součástí.

Centralizovaná organizace zase nabízí:

- nižší stavební náklady,
- lepší kontrolu nad informacemi,
- jednodušší správu.

Vzhledem k tomu, že počítačová učebna je velmi malá organizační struktura a nejsou na ní závislé další součásti, bude se tato práce řídit modelem centralizovaným.



Obrázek 1: grafické zobrazení Centralizované a Decentralizované sítě (4, s.2)

V této kapitole jsme si tedy stručně vysvětlili pojem centralizace a princip jejího fungování. Nyní by tedy bylo vhodné podívat se na nástroj, který nám tento způsob organizace počítačové sítě umožní uskutečnit.

2 Microsoft Windows Server

Windows Server je operační systém vytvořený společností Microsoft. Umožňuje centralizovanou správu dat, aplikací a komunikace (5). Cílem této kapitoly je poskytnout základní informace o tomto operačním systému počínaje licenční problematikou, přes hardwarové požadavky až k hlavním funkcím tohoto systému.

2.1 Licence Windows Server 2012 R2

Windows Server 2012 R2 může fungovat jako operační systém jak ve fyzickém prostředí, tak v prostředí virtuálním. Microsoft proto navrhl nový licenční model založený na počtu procesorů, uživatelů a počtu virtuálních instancí. Vznikly tak čtyři hlavní edice tohoto produktu.

- **Windows Server 2012 R2 Foundation.** Má velmi omezené funkce určené pro malé firmy, které potřebují jen základní služby, jako file and print služby a podporu aplikací. Podporuje maximálně jeden fyzický procesor, 15 uživatelů a neobsahuje možnosti virtualizace.
- **Windows Server 2012 R2 Essentials.** Tato edice má skoro všechny funkce jako Standart, ale neobsahuje Server Core, Hyper-V a Active Directory Federation Services.
- **Windows Server 2012 R2 Standart.** Má všechny klíčové funkce. Nabízí podporu až pro 64 fyzických procesorů. Tato licence zahrnuje 2 fyzické procesory a 2 virtuální instance.
- **Windows Server 2012 R2 Datacenter.** Obsahuje rovněž všechny podstatné funkce. Je určena pro velmi výkonné stroje. Podporuje až 64 fyzických procesorů, jedno fyzické prostředí a neomezený počet virtuálních instancí. Oproti verzi Standart není tato edice nijak licenčně omezena počtem virtuálních instancí. Rozhodující tak je pouze počet fyzických procesorů (6, s.17-18).

Ceny jednotlivých licencí se odvíjí od toho, co nabízí. K efektivnímu využití financí je tedy potřeba důkladně naplánovat a zvážit, která licence nejlépe vyhovuje potřebným požadavkům.

2.2 Hardwarové požadavky

Jako každý software i operační systém potřebuje minimální hardwarový výkon, na kterém je schopen optimálně fungovat. Pro Windows Server 2012 platí tyto požadavky:

- 1.4-GHz 64-bit procesor,
- 512 RAM,
- 32 GB volného místa na disku,
- DVD mechanika,
- super VGA (800 x 600) nebo monitor s větším rozlišením,
- klávesnice a myš,
- přístup k internetu.

Tyto požadavky by měly být považovány jako absolutní minimum potřebné k instalaci operačního systému. 32 GB disk ovšem nebude stačit, bude-li systém instalován ze vzdálené lokace, nebo bude-li využívat více než 16 GB RAM (7, s.21).

2.3 Role, služby rolí a funkce

Oproti klasickému klientskému operačnímu systému Windows, kde je hlavním zdrojem funkcionality samotný operační systém, nabízí Windows Server selektivní funkcionality. Máme možnost si tak pomocí instalace rolí, služeb rolí a funkcí zvolit, k jakému účelu bude konkrétní server sloužit. Jedná se tedy o vysoce multifunkční nástroj.

Role

Serverové role jsou součástí softwaru umožňující serveru vykonávat určitou funkci, která může sloužit uživatelům a ostatním počítačům v síti. Server může být vyhrazen pouze na jednu roli, jako například webový server, nebo může poskytovat roli několik (9).

Služby rolí

Služby rolí jsou softwarové komponenty, které poskytují funkcionality serverových rolí. Každá serverová role má jednu nebo více příbuzných služeb rolí. Některé serverové role jako například Domain Name System (DNS), mají pouze jednu funkcionality a nainstalováním této role nainstalujeme i tuto funkci. Ovšem jiné role, jako například Network Policy a Active Directory Certificate Services, mají několik služeb rolí, které můžeme nainstalovat. Instalací služeb rolí, tak specifikujeme, kterou funkcionality dané serverové role budeme využívat (8). Mezi nejpoužívanější role a služby rolí patří (6, s.413-418):

- Active Directory Domain Services (ADDS),
- Application Server,
- DHCP Server,
- DNS Server,
- File And Storage Server,
- Hyper-V,

- Print And Document Services,
- Remote Desktop Services,
- Web Server (ISS),
- Windows Server Update Services (WSUS).

Funkce

Funkce jsou součástí softwaru, které poskytují další funkcionalitu. Tyto funkce se instalují odděleně od rolí a služeb rolí. Jejich hlavní účelem je podporovat role, které jsou již nainstalované, nebo vylepšovat funkcionalitu serveru (9). Například funkce Failover Clustering, která umožňuje zapojit server do clusteru² a zajišťuje tak ochranu proti výpadku a zvýšený výkon, rozšiřuje funkcionalitu rolí. Mezi nejpoužívanější funkce patří (6, s.418-427):

- Bitlocker Drive Encryption,
- BranchCache,
- Failover Clustering,
- Group Policy Management,
- Remote Server Administration Tools (RSAT),
- Simple Mail Transfer Protocol Server (SMTP),
- Windows PowerShell,
- Windows Server Backup,
- WINS Server.

Při instalaci nového serveru je potřeba dbát na důkladné naplánování toho, jaké role a funkce na konkrétní server budeme instalovat. V závislosti na síťovém provozu, nebo vytíženosti konkrétní aplikace, mohou být totiž některé role velmi hardwarově náročné a jejich kombinace by mohla způsobit velmi nízkou výkonost. V případě počítačové učebny lze předpokládat, že vytíženost serveru bude velmi malá a proto budeme moci využít na jednom serveru rolí hned několik. Hlavní rolí, kterou budeme při budování počítačové učebny a následné tvorbě domény potřebovat je Active Directory Domain Services.

² Propojení více počítačů tak, že pracují jako jeden.

3 Active Directory Domain Services

Tato kapitola poskytuje základní informace o serverové roli Active Directory Domain Services (AD DS) a všech jejích součástí, které budou potřeba při správě počítačové učebny.

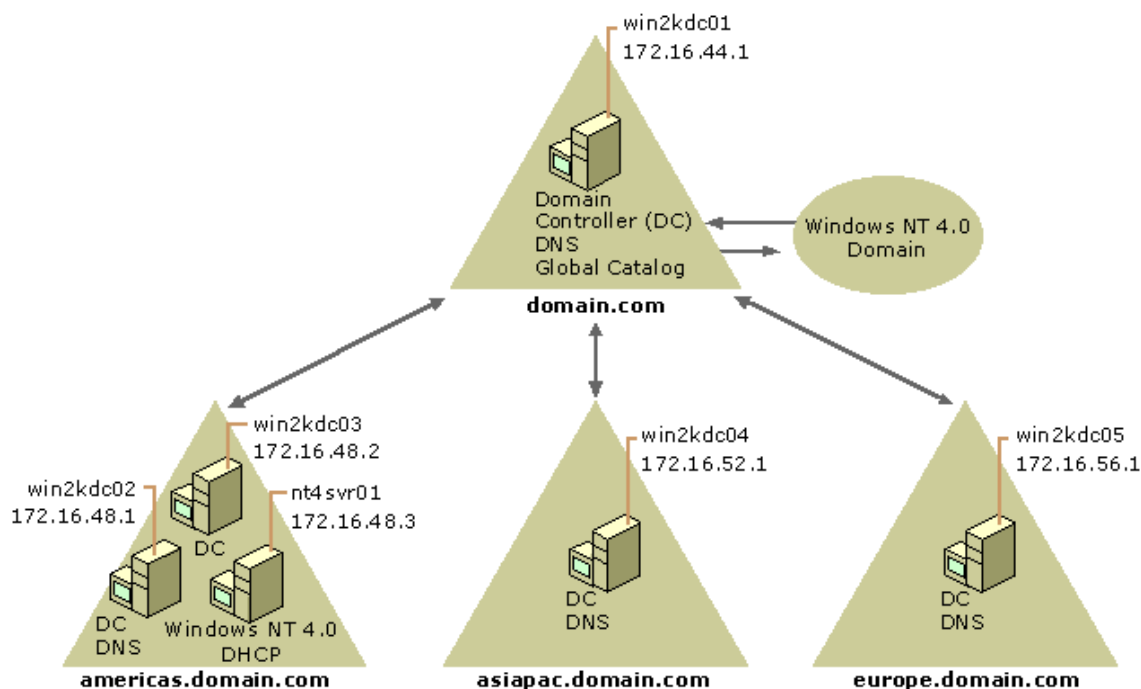
Active Directory Domain Services je jednou z mnoha rolí operačního systému Microsoft Windows Server. Jedná se o nástroj, pomocí kterého lze vytvořit doménu a spravovat všechny objekty, které jsou její součástí. Kromě tvorby samotné domény můžeme také tvořit, upravovat a omezovat uživatele a počítače, vytvářet pravidla, která řídí doménový provoz, nebo propojovat jednotlivé domény mezi sebou a vytvořit tak doménový les. Máme tedy možnost vytvořit logicky a hierarchicky modelovanou strukturu, která spravuje veškeré objekty v naší síti (10).

3.1 Doména a Doménový les

Logická struktura Active Directory je postavena na základně konceptu domén. Domény byly představeny již ve verzi Windows NT 3.x a 4.0. Od té doby se však tato zprvu neobsáhlá a neflexibilní struktura významně vylepšila. Doména Active Directory se skládá z následujících součástí (11, s.44-45):

- hierarchická struktura objektů a složek postavena na standardu X.500,
- unikátní identifikátor DNS,
- bezpečnostní služba, která ověřuje a opravňuje veškerý přístup do domény službám a uživatelům,
- pravidla, které omezují práva jednotlivých uživatelů a počítačů.

Pro lepší představu toho co je to doména si můžeme představit strom. Kmen stromu je doménový řadič, který obsahuje veškeré informace o doméně a je hlavním koordinátorem doménového provozu. Jednotlivé větve stromu pak představují různá firemní oddělení, listy jsou pracovní stanice a samotní uživatelé. Doménový les je pak spojení několika domén dohromady.



Obrázek 2: hlavní doména rozdělená do pod-domén, doménový strom (12)

3.2 Domain Controller

Domain Controller, neboli doménový řadič, je server, který má na starosti celou doménu. Autorizuje uživatele a umožňuje samotný přístup do domény. Jeden doménový řadič může spravovat pouze jednu doménu.

Důležitou součástí Active Directory a doménového řadiče je Globální Katalog. Ten obsahuje informace o veškerých objektech uložených v databázi Active Directory a využívá se tak pro doménové hledání (13).

3.3 Organizační jednotky

Pokud si představíme doménu Active Directory, zjistíme, že se jedná o hierarchickou strukturu složenou z objektů. Některé objekty mohou sloužit jako složky. Nejčastějším typem složky, který se používá pro ukládání objektů, je organizační jednotka (organizational unit). Dalším typem složky, do které lze ukládat jiné objekty, je container. Důvod proč se častěji používá organizační jednotka je ten, že na container není možné aplikovat Group Policy (11, s.54). Organizační jednotka může obsahovat například tyto objekty:

- uživatelé,

- skupiny,
- počítače,
- tiskárny,
- jiné organizační jednotky.

Pomocí organizačních jednotek si tak můžeme navrhnout smysluplné a logické rozvržení všech objektů, které v Active Directory ukládáme. Výhodou je, že veškeré nastavení a restriktce, které na konkrétní jednotku přiřadíme, se dědí na všechny podřazené objekty.

3.4 Group Policy

Doménová práva Group Policy jsou nejjednodušším způsobem jak vytvořit souhrn pravidel pro počítače a uživatele v síti fungující pod správou Active Directory (14). Hlavní funkce a možnosti práv Group Policy by se daly shrnout do těchto bodů (11, s.684):

- mohou se vztahovat na počítače, uživatele, domény a organizační jednotky,
- umí automaticky měnit hodnoty při definovaných podmínkách,
- automaticky spouští skripty při přihlášení a odhlášení uživatele nebo zapnutí a vypnutí počítače,
- nabízí znatelně větší funkcionalitu než lokální local group policy editor.

Při tvorbě nebo úpravě práv Group Policy se setkáme se třemi typy nastavení (14):

- Enabled – nastavení bylo konfigurováno. Někdy je potřeba specifikovat hodnoty,
- Disabled – nastavení je vypnuto. V tomto případě je cílem administrátor zabránit určité funkcionalitě,
- Not Configured – toto nastavení není ani zapnuto nebo vypnuto. Tato volba je výchozí hodnota pro většinu nastavení.

Stejně jako nastavení organizačních jednotek i Group Policy podléhá dědičnosti. Pokud tedy vytvoříme Policy na doménové úrovni pak všechny objekty, které jsou pod touto doménou, budou této Policy podléhat. Dědičnost práv Group Policy je kumulativní.

Jestliže tedy na jeden objekt směřuje více nastavení práv, tyto nastavení se propojují. Může se ale stát, že dvě různá nastavení upravují jednu hodnotu a to tak, že každé jiným způsobem. V tomto případě vyhrává to nastavení, které je poslední, tedy to, které je v hierarchickém pořadí nejbližší objektu, který nastavení ovlivňuje. Pokud potřebujeme dědičnost práv upravit manuálně, můžeme použít volby Block nebo Force Policy Inheritance. Můžeme tak dědičnosti zabránit nebo ji naopak vynutit (15).

Vzhledem k tomu, že služba Active Directory Domain Services je velice obsáhlá a má širokou škálu funkcionalit, potřebuje využít sílu jiných rolí. Jednou z těchto nezbytných rolí, která je potřeba pro fungování AD DS je role Domain Name System neboli DNS.

4 Služba DNS

Tato kapitola se zaměřuje na objasnění pojmu Domain Name System, jež je nedílnou součástí Active Directory. Stejně jako většina technologií i operační systémy Windows podporují a využívají ke komunikaci protokol TCP/IP. Veškerý hardware fungující na tomto protokolu má v internetové síti přiřazenou unikátní adresu IP (Internet Protocol). IP adresa se skládá ze 4 čísel nabývajících hodnot od 0 do 255 oddělených tečkami. Validní IP adresa tedy může vypadat například takto: 192.168.2.35. Ačkoliv počítače s touto hodnotou nemají žádný problém, pro člověka je nepředstavitelné pamatovat si desítky takovýchto adres. Mnohem jednoduší je nahrazení těchto číselných hodnot jmény (16). Lidský mozek si určitě lépe zapamatuje seznam.cz než 77.75.77.53.

K tomuto účelu se využívá služba DNS (Domain Name System), která za nás překládá síťová jména na IP adresy protokolu TCP/IP. Službu DNS si můžeme představit jako telefonního operátora, který zná všechna telefonní čísla. Stačí tedy sdělit komu chceme volat a nemusíme znát telefonní číslo.

4.1 Důležité pojmy služby DNS

Pro pochopení podstaty fungování DNS Serveru a jednotlivých procesů je nutné si definovat základní pojmy, které tuto službu tvoří (17, s.127-128).:

- **DNS Server** – jakýkoliv počítač poskytující Domain Name Service je DNS Server,

- **DNS Klient** – je jakýkoliv počítač posílající dotazy DNS Serveru. Tyto dotazy se posílají pomocí tzv. Resolveru,
- **Resolver** – je softwarový proces, který provádí samotné vyhledávání odpovědí na DNS dotazy. Resolver bývá zabudovaný do větších programů, a proto není potřeba využívat žádné externí knihovny pro jeho zavolání. Příkladem takového softwaru je například Internet Explorer,
- **Dotaz** – je požadavek na informaci zaslaný DNS serveru. Existují tři typy: rekurzivní, inverzní a iterativní.

4.2 Zóny DNS

Zóna je hlavním zdrojem informací každé DNS domény, která je v zóně obsažena. Obsahuje záznamy o všech objektech v doméně. Pro účel této práce budeme využívat primární zónu integrovanou s Active Directory (18).

4.3 Active Directory DNS

S příchodem Windows Server 2003 přibyla při tvorbě nové DNS zóny možnost integrovat primární zónu s Active Directory. Tato integrace přináší své výhody i nevýhody (17, s.144-145):

- **nevýhody** – hlavní nevýhodou tohoto typu zóny je, že musí být přítomna na doménovém řadiči, protože DNS databáze je uložena v Active Directory. Nemůžeme tak tuto zónu využít na členských serverech. Malá firma tak může mít potíže s nedostatkem prostředků pro vytvoření samostatného doménového řadiče,
- **výhody** – jelikož je DNS databáze uložena přímo v Active Directory, všechny ostatní Active Directory DNS servery mají k této databázi přístup. Pokud bychom tedy přišli o přístup k jednomu serveru, můžeme data získat ze serveru jiného. Active Directory DNS také šetří síťový provoz. Veškeré DNS záznamy se replikují společně s běžnou replikací Active Directory, nevzniká tedy nadbytečný síťový provoz.

V této chvíli máme tedy možnost vytvářet a spravovat objekty v doméně. Uživatelé ale budou potřebovat pracovat s daty. Data je potřeba ukládat, kontrolovat a zabezpečit. K těmto účelům je skvělým pomocníkem File Server.

5 File And Storage Services

Tato kapitola vysvětluje pojem File and Storage Services a popisuje jeho nejdůležitější součásti potřebné k pochopení funkce této role.

Na rozdíl od volitelných součástí Serveru jako AD DS, DNS apod., je role File And Storage Services defaultní rolí, která se nainstaluje společně s operačním systémem. Defaultně však obsahuje jen základní funkcionalitu a pro získání rozšířených funkcí je potřeba přidat požadované služby rolí.

Role File and Storage Services umožňuje spravovat jeden nebo více file serverů, což jsou servery, které slouží jako centrální úložiště v síti. Pomocí File Serveru můžeme sdílet a ukládat data v celé síti (19). Mezi základní aplikace File Serveru, které můžeme pomocí role File and Storage Services využít patří (20):

- **Prostory úložiště** – umožňují virtualizovat úložiště seskupením standardních disků do fondů úložišť a pak z dostupné kapacity fondů úložišť vytvořit virtuální disky nazývané prostory úložiště (21),
- **Přesměrování složek, Offline soubory a Cestovních profilů uživatelů** – pro přesměrování lokálních složek do vzdáleného úložiště, ukládání vzdálených souborů lokálně a tvorbu profilů, které mají své data uloženy na sdíleném disku (22),
- **Pracovní složky** – poskytují konzistentní způsob, jak uživatelům umožnit přístup k jejich pracovním souborům ze svých počítačů a zařízení (23),
- **Odstranění duplicitních dat** – umožňuje snížit rozsah využitého prostoru, což šetří místo na disku,
- **iSCSI Target Server** – používá se k vytvoření centralizovaných, hardwarově nezávislých úložišť. Vhodné zejména při tvorbě virtuálních prostředí,
- **Server Manager** – umožňuje vzdálenou správu několika file serverů z jednoho místa,
- **Windows PowerShell** – vhodný pro tvorbu automatizačních skriptů při správě file serverů.

5.1 Sdílení složek

File server slouží k sdílení a ukládání dat. Abychom mohli tuto funkci využívat, je potřeba vědět jak na serveru vytvořit sdílenou složku. Sdílená složka je složka sdílená mezi klienty v síti, tak aby klienti byli schopni tuto složku využívat k příjmu a ukládání dat. Administrátor má možnost určovat, kteří uživatelé nebo uživatelské skupiny budou mít do této složky přístup a také to, jaké operace budou moci v dané složce vykonávat (6, s.1437).

Přístupová práva

Sdílené složky můžeme zabezpečit přístupovými právy. K nastavení přístupových práv můžeme využít dva nástroje. Buď využijeme jednodušší nástroj sdílení nebo NTFS.

5.2 NTFS

NTFS je jeden z formátů, který můžeme zvolit při formátování disku. Operační systém Windows nabízí výběr ze tří formátů (17, s.1113):

- File Allocation Table (FAT), který je podporován pouze na starších operačních systémech (Server 2003, Server 200, Windows XP a tak dále),
- FAT32, který podporuje Windows Server 2012,
- NTFS, který také podporuje Windows Server 2012.

Oproti FAT a FAT32 nabízí formát NTFS mnoho výhod. Mezi tyto výhody patří (24):

- **komprese** – umí zmenšovat soubory a složky, což umožňuje šetřit místo na disku. Ze souboru, který má 20 MB jsme schopni kompresí vytvořit soubor, který na disku zabírá pouze 13 MB,
- **kvóty** – umožňují nastavovat maximální hodnotu místa, kterou může daný uživatel na serverovém disku zabrat,
- **šifrování** – Encryption File System (EFS), umožňuje uživateli nebo administrátorovi zabezpečit soubory a složky pomocí šifrování. Soubor se tak pomocí unikátního bezpečnostního identifikačního čísla (SID) zašifruje a je přístupný pouze konkrétnímu uživateli,

- **bezpečnost** – je jednou z nejdůležitějších složek IT. Výhodou formátu NTFS je, že bezpečnostní práva můžeme aplikovat na jednotlivé soubory a složky. Můžeme tak určit, který uživatel nebo skupina budou mít k daným souborům přístup (Read), budou moci ukládat změny (Write), mazat soubory (Modify) a celkovou kontrolu (Full Control).

File Server nám tedy umožňuje spravovat uživatelská data a sdílet je. Jsme tak schopni vytvořit bezpečné úložiště, které má svá pravidla a logickou strukturu. Toto centralizované úložiště nám taky pomůže efektivně zálohovat důležitá data.

6 Windows Server Backup

Tato kapitola se věnuje problematice zálohování pomocí funkce Windows Server Backup, která je volitelnou součástí operačního systému Microsoft Windows Server. Cílem je objasnit pojem zálohování a popsat možnosti, které funkce Windows Server Backup nabízí.

Zálohování a obnova jsou pojmy popisující proces ochrany dat. Hlavním účelem zálohování je vytvořit kopie souborů, aby je bylo možné v případě potřeby obnovit. Pokud se tedy stane, že je soubor smazán či nenávratně poškozen, máme k dispozici identickou kopii a jsme tak schopni minimalizovat škody. Abychom zaručili, že zálohovaná data budou vždy aktuální, je potřeba dbát na pravidelné zálohování. K těmto účelům je v operačním systému Windows Server k dispozici funkce Windows Server Backup

Funkce Windows Server Backup nám umožňuje chránit naše data. Ať už se jedná o samotný operační systém, data aplikací, soubory nebo celé disky. Získané zálohy pak můžeme ukládat na jeden nebo více disků, na jeden nebo více svazků, DVD nebo do vzdálených sdílených složek. Zálohování můžeme spouštět manuálně nebo automaticky podle nastaveného rozvrhu (25).

Při konfiguraci nové zálohy je potřeba se zamyslet, co vlastně potřebujeme zálohovat. Ne vždy je totiž výhodné zálohovat kompletní obsah počítače. Windows Server Backup umožňuje zvolit si rozsah zálohy, který odpovídá konkrétním potřebám. To, co se rozhodneme zálohovat, ovlivní možnosti obnovení. Zálohovat můžeme (25):

- celý server – umožňuje obnovit kompletně celý obsah serveru a všechny svazky, které server obsahuje,
- „Bare metal“ – pokud chceme obnovit pouze operační systém (pouze kritické svazky). Tento typ zálohy je vhodný pro případy, kdy není možné použít system state nebo jinou zálohu. K obnovení potřebujeme originální instalační soubory operačního systému, například instalační DVD,
- system state – zálohuje veškeré soubory potřebné k obnovení stavu systému, ve kterém byl při provedení zálohy,
- jednotlivé svazky – pokud potřebujeme zálohovat pouze specifické soubory, aplikace nebo jiná data, která jsou na těchto svazcích uložena,
- soubory a složky – záloha pouze konkrétních složek a souborů, které budeme chtít obnovit.

Windows Server Backup je schopen proces zálohování také optimalizovat. Záloha se chová jako inkrementální záloha viz kapitola 6.1, což umožňuje šetřit místo na disku a zkracuje dobu samotného zálohování. Pokud použijeme pevný disk nebo svazek k uložení zálohy, Windows Server Backup automaticky smaže staré zálohy v případě, že na disku již není dostatek volného místa (25).

6.1 Typy záloh

Jak již bylo zmíněno, Windows Server Backup funguje jako inkrementální záloha. Ovšem toto není jediný typ zálohy a je tedy na místě vysvětlit podrobněji nejen tento typ, ale také typy ostatní. V zásadě existují tři typy záloh (26):

- **úplná záloha** – nejzákladnějším a nejkompexnějším typem zálohy je úplná záloha. Tento typ zálohuje veškerá data, která jsou k dispozici. Hlavní výhodou je, že máme k dispozici veškerá data na jednom místě. Díky tomu je proces obnovy dat bezkonkurenčně nejrychlejší oproti ostatním typům. Nevýhodou však je dlouhá doba samotného zálohování a také velikost, kterou výsledná záloha má. Z těchto důvodů se tak většinou využívá úplná záloha v kombinaci s jiným typem zálohy,
- **inkrementální záloha** – ukládá pouze ta data, která se změnila od poslední zálohy. Využívá se časová známka souborů, která se porovnává s časovou známkou souborů starší zálohy. Vzhledem k tomu, že tento typ zálohy zálohuje

pouze malou část dat, lze jej spouštět kdykoliv. Oproti úplné záloze má totiž velmi malý vliv na výkon serveru. Princip fungování spočívá ve vytvoření úplné zálohy a poté ukládání inkrementálních záloh, které na sebe navazují a obsahují pouze data, která se změnila od zálohy předchozí,

- **rozdílová záloha** – stejně jako inkrementální i rozdílová záloha spoléhá na předchozí úplnou zálohu. Tento typ zálohy však vždy ukládá všechna data, která se liší od původní úplné zálohy. Spotřebuje se tak více úložného prostoru než při inkrementální záloze, ovšem mnohem méně než při záloze úplné. Stejně je to s časem potřebným k dokončení zálohy.

	Úplná	Inkrementální	Rozdílová
Záloha 1	Všechna data	Všechna data	Všechna data
Záloha 2	Všechna data	Změny zálohy 1	Změny zálohy 1
Záloha 3	Všechna data	Změny zálohy 2	Změny zálohy 1
Záloha 4	Všechna data	Změny zálohy 3	Změny zálohy 1

Tabulka 1: porovnání jednotlivých typů záloh (27)

Windows Server Backup nám tedy v kombinaci s file serverem umožňuje zálohovat veškerá důležitá data učebny. Máme tak k dispozici nejen obnovitelná data žáků, která jsou uložena na serveru, ale také zálohu celé domény.

7 Služba DHCP

Ačkoliv tato role není nezbytnou součástí potřebnou pro správu počítačové učebny, můžeme s její pomocí zvýšit efektivitu administrace a bezpečnosti učebny. Tato kapitola popisuje roli DHCP a její součásti potřebné k pochopení podstaty její funkce.

Jak již bylo zmíněno v kapitole 4, počítače využívají ke komunikaci převážně protokol TCP/IP. Každý počítač v síti tak potřebuje získat správnou konfiguraci TCP/IP protokolu, včetně unikátní IP adresy. TCP/IP protokol lze konfigurovat dvěma způsoby: manuálně nebo automaticky.

Manuální konfigurace TCP/IP protokolu je velmi jednoduchá. Vyžaduje fyzický přístup ke konkrétnímu počítači a administrátorská práva. Problém této metody ovšem nastává v situaci, kdy má administrátor takto nakonfigurovat několik stovek počítačů najednou. Je těžko představitelné, že by měl administrátor tyto počítače konfigurovat jeden po druhém.

Tento problém řeší konfigurace automatická. Pomocí služby DHCP lze nastavit automatickou konfiguraci TCP/IP protokolu všech počítačů v síti. Každému klientovi, který se připojí do domény je pak automaticky přiřazená správná konfigurace TCP/IP protokolu, včetně unikátní IP adresy.

7.1 DORA proces

Pro pochopení principu fungování DHCP je potřeba si představit tzv. DORA proces neboli Discover, Offer, Request and Acknowledge. Ten probíhá následovně (7, s.457-458):

- Discover: Jakmile se klient připojí do sítě pošle speciální správu zvanou DHCPDISCOVER,
- Offer: Jakýkoliv DHCP server, který obdrží discover požadavek, ověří svou databázi a odpoví zprávou DHCPOFFER, která obsahuje dostupnou IP adresu,
- Request: Klient obdrží jednu nebo více DHCPOFFER zpráv a jednu si vybere. Jako odpověď odešle DHCPREQUEST, čímž přijme přidělenou IP konfiguraci. Ostatním DHCP serverům tato zpráva sděluje, že klient jejich nabídku nepřijmul,
- Acknowledge: Jakmile DHCP server obdrží DHCPREQUEST, označí příslušnou IP adresu jako využívanou. Poté pošle klientovi zprávu DHCPACK,
- jestliže není schopen přijmout DHCPREQUEST, odešle klientovi zprávu DHCPNAK, čímž zahájí celý konfigurační proces znovu.

7.2 DHCP Scope

DHCP scope je rozmezí IP adres, které má DHCP server na starosti. Zpravidla se používá jeden scope na jednu fyzickou podsíť, který může pokrývat adresy třídy A, B, C nebo adresy protokolu TCP/IPv6.

Každý scope obsahuje parametry a nastavení, která lze upravovat. Tato nastavení upravují informace doručené klientům při dorozumívání s určitým serverem. Můžeme tak nastavit například: výchozí DNS server, výchozí bránu a tak dále (17, s.797-798).

7.3 Exkluze a rezervace

Je důležité si uvědomit, že jakmile vytvoříme určitý DHCP scope, všechny IP adresy mohou být volně používány klienty v síti. Proto je dobré se zamyslet, zda by nebylo vhodné některé z těchto IP adres z rozsahu vyřadit, nebo rezervovat pro konkrétního klienta.

V případě, že vytvoříme scope obsahující IP adresu, která už je v síti využívána jiným zařízením, je potřeba tuto adresu ze seznamu vyloučit tzv. exkluzí. Zamezíme tak duplikování IP adres v síti. Naopak pokud vytvoříme scope a víme, že určitý klient bude potřebovat statickou IP adresu, je vhodné tuto adresu rezervovat. Potřebnému klientovi tak přiřadíme adresu a nestane se tak, že by tento klient při obnovovacím DORA procesu získal adresu jinou (28).

V počítačové učebně tak využitím služby DHCP vytvoříme přehledné síťové prostředí, ve kterém bude mít každý počítač přiřazenou pevnou IP adresu. Toto nastavení nám umožní rychleji identifikovat síťové problémy nebo odhalit případné bezpečnostní riziko.

8 Plánování počítačové učebny

Cílem této kapitoly je nastínit reálný model centralizované učebny spravované pomocí platformy Microsoft Windows Server, zejména pomocí role Active Directory Domain Services a dalších rolí a funkcí, které jsou potřeba k efektivnímu provozu.

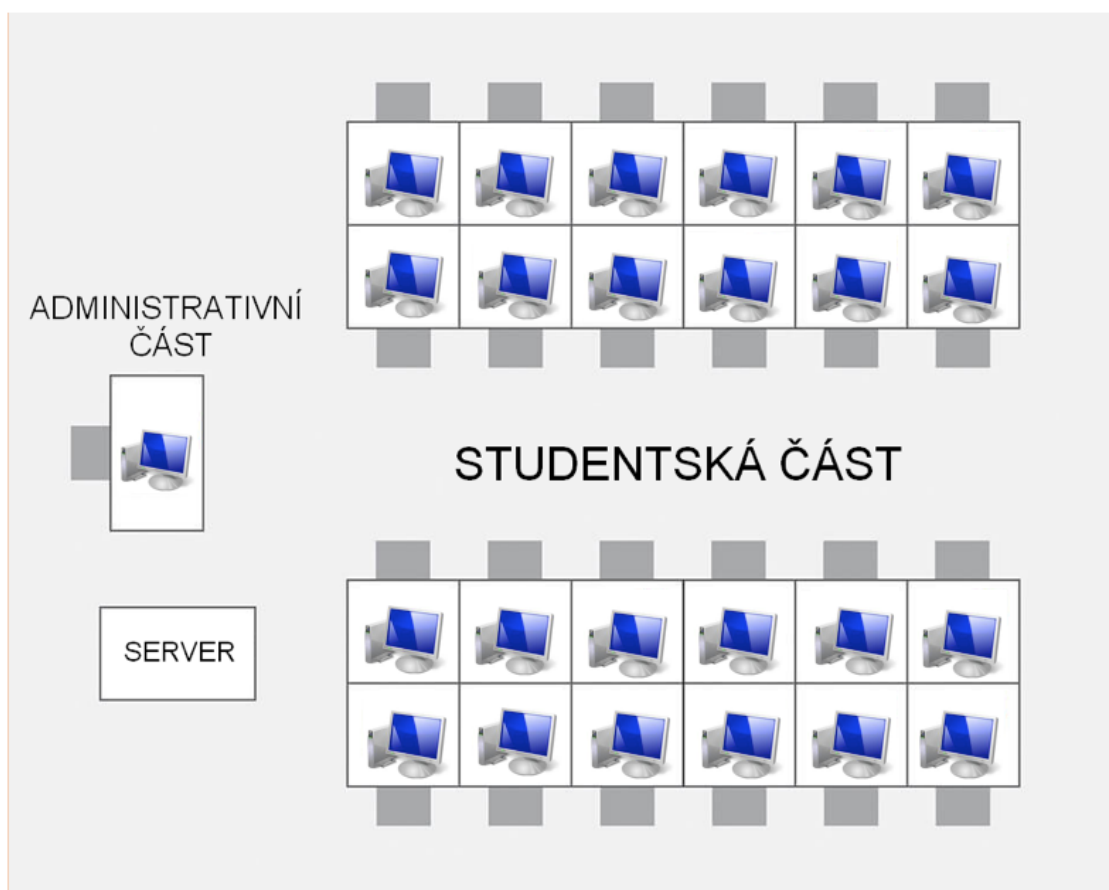
Hlavní částí této kapitoly bude návrh struktury domény a definice objektů, které v naší doméně budou figurovat. Mezi tyto objekty patří: uživatelé, uživatelské skupiny, organizační jednotky a pracovní stanice. Tyto objekty budou mít jasně definovaná pravidla, která budou určovat jejich vyhrazený prostor v doméně.

Dalším bodem je návrh fyzického modelu, tedy toho, jak by mohla taková počítačová učebna vypadat. Vzhledem k tomu, že hardwarové řešení není součástí této práce, bude

tato část sloužit výhradně pro lepší představu reálné situace. Tato část tak nebude obsahovat popis síťových prvků ani ostatních hardwarových zařízení jako tiskárny, projektory apod.

8.1 Fyzický návrh učebny

Než se budeme věnovat struktuře samotné domény je potřeba vytvořit si představu o tom, jak bude ilustrativní učebna vypadat. V této učebně budou mít žáci k dispozici 24 pracovních stanic. V čele učebny bude jedna pracovní stanice určena výhradně vyučujícím a vzdálené správě serveru. Celá učebna bude mít tedy dvě hlavní části, studentskou a učitelskou/administrativní, viz obrázek 3. Studentská část bude sloužit studentům jako pracovní prostor a administrativní část bude sloužit vyučujícím a administrátorům, celkem tedy třem skupinám uživatelů.



Obrázek 3: grafické znázornění počítačové učebny

Ve fyzickém modelu jsme si tedy definovali tyto stěžejní body:

- studentská část

- 24 pracovních stanic,
- slouží studentům.
- administrativní část
 - pracovní stanice vyučujícího,
 - slouží vyučujícím a administrátorům.

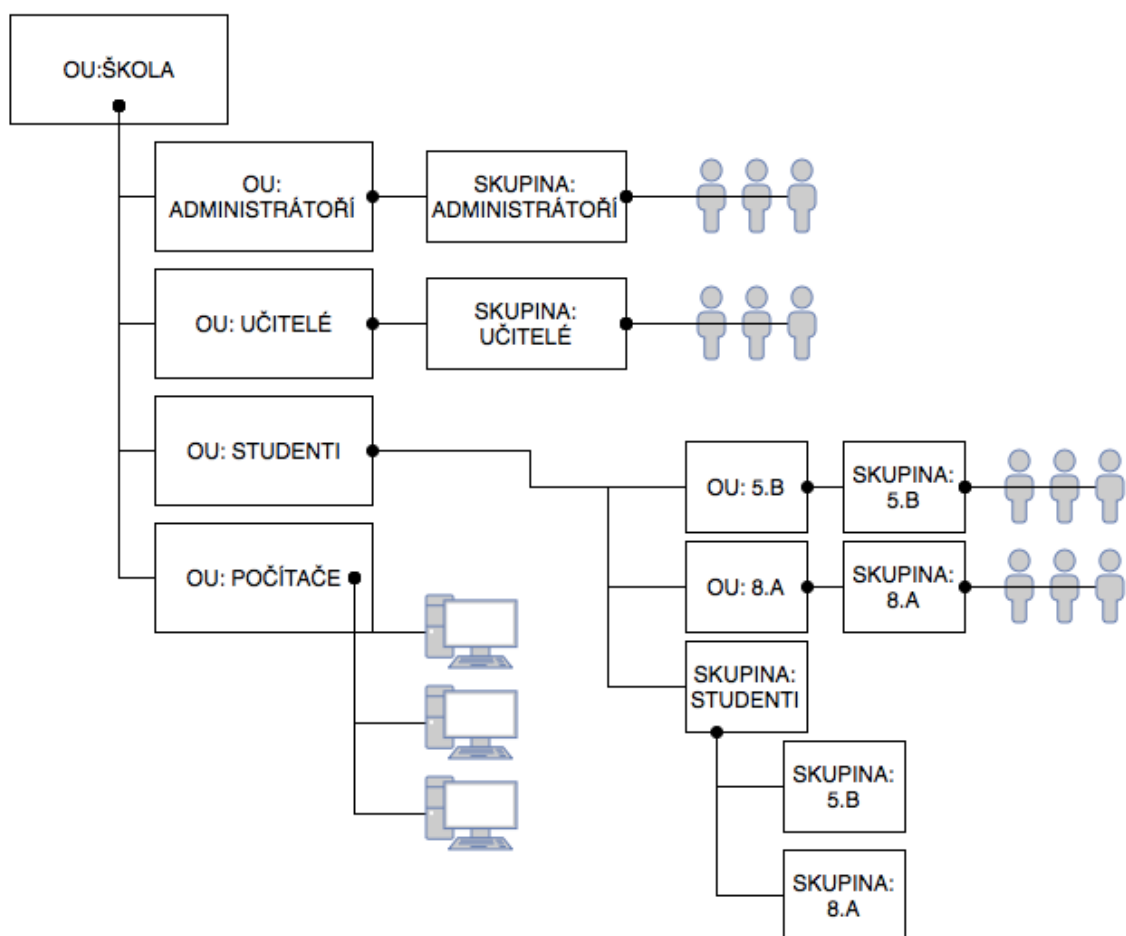
Máme tedy základní představu o tom, jak počítačová učebna vypadá a komu budou sloužit její jednotlivé části. Při tvorbě domény se tedy zaměříme na převedení tohoto fyzického modelu do doménové struktury.

8.2 Doménová struktura

Před samotnou tvorbou domény je potřeba naplánovat, jak budou jednotlivé objekty domény rozděleny a jaká budou jejich doménová práva. Při návrhu struktury použijeme již vytvořený fyzický návrh. Z tohoto návrhu vyplývá, že budeme potřebovat tři nezávislé skupiny uživatelů. Tyto tři skupiny budou mít také odlišný stupeň práv.

Nejjednodušším způsobem jak přehledně rozdělit objekty v doméně, je využití organizačních jednotek. Do těchto organizačních jednotek pak můžeme ukládat jednotlivé uživatele a jejich skupiny. Výhodou tohoto rozdělení je také to, že práva Group Policy lze aplikovat přímo na organizační jednotky. Jelikož se doménová práva aplikují i na počítače v síti, nesmíme zapomenout vytvořit organizační jednotku určenou pro počítače.

Musíme tedy pečlivě naplánovat, jak budou jednotlivé objekty rozděleny. Cílem je zajistit co nejjednodušší administraci. Výsledná struktura by mohla vypadat například takto viz. obrázek 4. Jedná se o zjednodušený návrh toho, jak by mohla výsledná doména vypadat.



Obrázek 4: návrh doménové struktury

Všimněte si, že každá třída studentů má jak vlastní organizační jednotku, tak vlastní skupinu. Toto rozdělení nám umožňuje specifikovat doménová práva pro jednotlivé třídy zvlášť a také zjednodušuje následnou administraci.

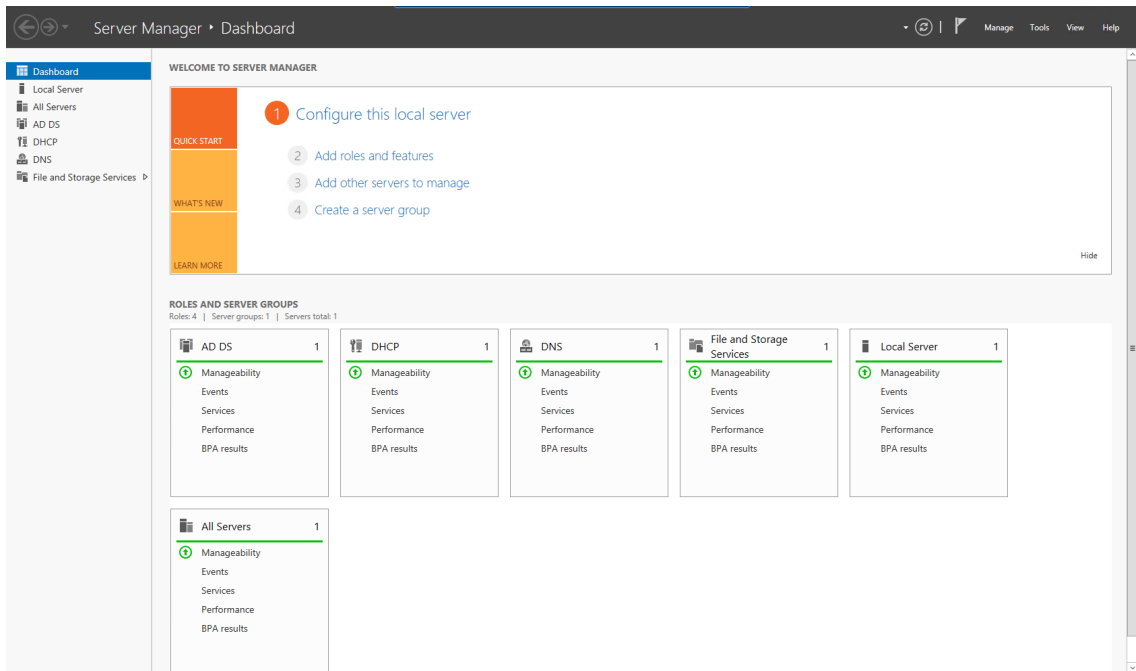
Nyní máme základní představu o tom, jak vypadá učebna fyzicky a jak bude vypadat struktura budoucí domény. Dalším bodem tedy bude seznámit se s tím, jak tyto návrhy uskutečnit.

9 Instalace Serveru a potřebných služeb

S teoretickým popisem Operačního systému Windows Server a jeho součástí jsme se seznámili v teoretické části této práce, nyní se zaměříme na to, jak tyto prvky zprovoznit a nastavit.

9.1 Server Manager

Server Manager je konzole, která je součástí operačního systému Windows Server. Jedná se o nástroj, který velmi usnadňuje práci administrátora. Jde o rozcestník všech operací a nástrojů, které můžeme potřebovat.



Obrázek 5: hlavní menu nástroje Server Manager

Pomocí tohoto nástroje můžeme z jednoho místa vykonávat tyto administrativní úkony (29):

- sledovat a provádět změny v serverových rolích a funkcích instalovaných na serveru,
- provádět správní úkony jako například spouštění a zastavování služeb nebo správa lokálních uživatelských účtů,
- sledovat stav serveru, identifikovat kritické události a řešit konfigurační problémy nebo selhání.

Velkou výhodou Server Manageru je také možnost spravovat nejen lokální server, ale také ostatní server v síti, které lze přímo do Server Manageru přidat. Máme tak nejen přehled o reálném stavu těchto serverů, ale můžeme je také vzdáleně spravovat.

9.2 Instalace a konfigurace operačního systému

Při instalaci serverového operačního systému nenajdeme oproti klasickému klientskému operačnímu systému mnoho rozdílů. Jedná se o klasický instalační proces, který počíná vložením instalačních dat (DVD, flash disk) a končí vítací obrazovkou nového operačního systému. Přesto je však potřeba si při instalaci dát na několik bodů pozor.

Při výběru licence máme na výběr instalovat server s grafickým rozhraním nebo v režimu server core. Server core neobsahuje grafické rozhraní a lze jej lokálně spravovat jen pomocí příkazové řádky. Tato volba je vhodná zejména když potřebujeme co nejvíce snížit hardwarové využití serveru a nebude-li server vyžadovat častou administraci. V rozsahu počítačové učebny je volba grafického rozhraní nejvhodnějším řešením.

Dalším důležitým bodem instalace je tvorba hesla pro lokální účet administrátora. Defaultní nastavení lokální politiky hesel nevyžaduje, aby heslo splňovalo podmínky komplexního hesla. Při tvorbě nové domény se však dostaneme do situace, kdy se lokální administrátor stává administrátorem doménovým a pro tento účet už požadavek komplexního hesla platí. Pokud tak při instalaci serveru nevytvoříme komplexní heslo, budeme jej muset při tvorbě nové domény měnit. Je tedy vhodné se tomuto kroku vyhnout a nastavit komplexní heslo již při instalaci serveru. Heslo by tedy mělo obsahovat: velká i malá písmena, číslo a speciální znak.

Po dokončení instalace operačního systému je také vhodné změnit defaultně vytvořený název počítače tak, aby vyhovoval našim požadavkům a abychom jej byli schopni identifikovat v síti. Tento krok vyžaduje restart.

Dále nesmíme zapomenout, že server je na rozdíl od klientských pracovních stanic řídicí jednotkou v síti. Abychom zajistili, že všechny objekty v síti budou schopny tuto řídicí jednotku vždy najít, musíme serveru přiřadit statickou IP adresu. Do pole DNS serveru vyplníme IP adresu serveru nebo adresu localhost 127.0.0.1³, jelikož bude server po instalaci role AD DS sloužit jako DNS server.

³ Univerzální IP adresa, která vždy odkazuje zpět na hosta.

9.3 Instalace a konfigurace role Active Directory

Pro instalaci rolí, služeb rolí a funkcí využijeme Server Manager, kde zvolíme tlačítko „přidat role a funkce“. Dostaneme se tak do instalačního průvodce, ve kterém máme možnost zvolit konkrétní roli nebo funkci.

Proces instalace role či funkce je srovnatelný s instalací běžného softwaru, musíme však většinou specifikovat více nastavení, což závisí na obsáhlosti funkcí role, kterou instalujeme. Jelikož je role AD DS poměrně rozsáhlou rolí, je proces instalace náročnější než například instalace funkce Windows Server Backup.

Tvorba domény probíhá již během instalace a neobejde se bez nutné konfigurace. Ta se v případě, že vytváříme nový doménový les a nepřipojujeme server do již existující domény, skládá z několika bodů.

Výběr jména kořenové domény (root domain name) – Ve chvíli, kdy vytváříme nový doménový les, si musíme vybrat, jak se bude jmenovat kořenová doména. Pro výběr správného jména existuje spousta pravidel. Pokud bychom chtěli doménu zpřístupnit i uživatelům mimo počítačovou učebnu, tedy uživatelům internetu mimo interní síť, musíme brát v potaz fakt, že každá doména musí mít unikátní název. V našem případě interní počítačové učebny však tento problém řešit nemusíme, protože doména bude přístupná jen uživatelům školní sítě. Jméno domény si tedy můžeme zvolit dle libosti. Klasickými příklady jsou například: *název.local*, *název.com*, *název.cz* apod.

Tvorba DSRM hesla – V dalším kroku instalace je hlavním bodem tvorba hesla pro obnovu, neboli Domain Services Restore Mode password. Mód DSRM slouží jako zadní vrátka do databáze v případě selhání Active Directory, nebo v případě obnovy (30). Heslo musí splňovat pravidla komplexnosti.

NetBIOS domain name – Doménové jméno NetBIOS umožňuje starším verzím softwaru, jako například Windows NT 4.0 které se neidentifikují v síti pomocí DNS, nalézt primární doménový radič. Při tvorbě nové domény je automaticky vytvořeno NetBIOS jméno, a to z názvu domény zleva (31). Toto jméno je možné během procesu tvorby změnit, ale později už změna možná není.

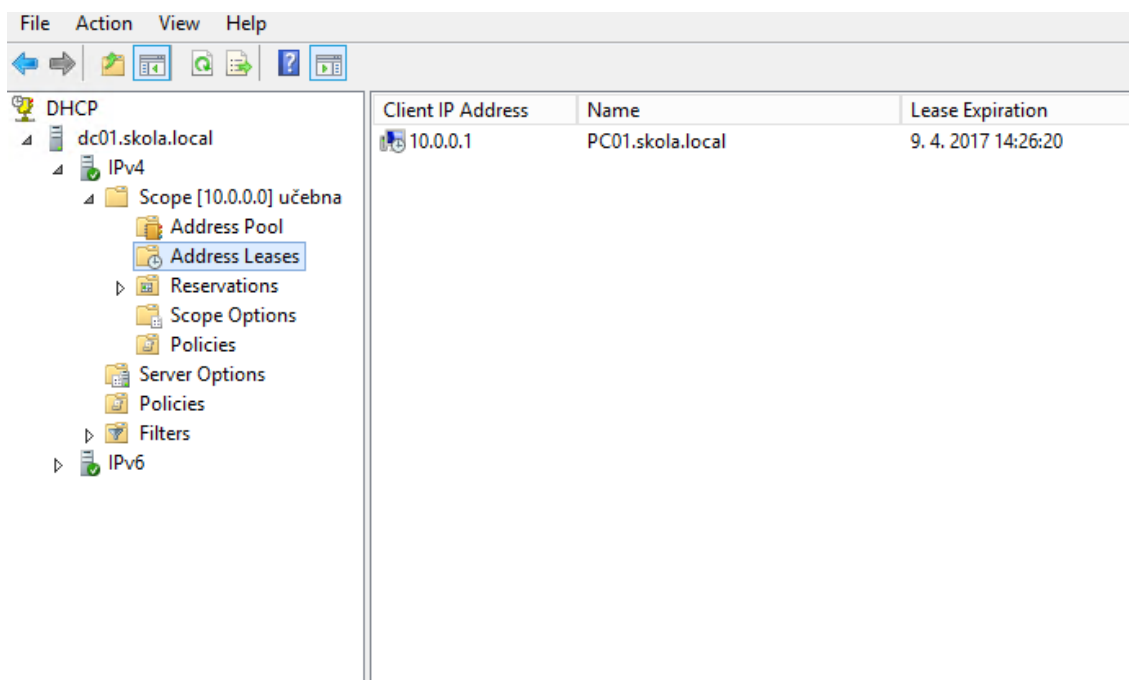
Umístění databáze AD DS, logů a SYSVOL složek – Tyto složky obsahují nezbytné informace pro fungování Active Directory. Defaultně se tyto složky ukládají na systémový disk do složky Windows tedy například: C:\Windows\SYSVOL. Toto umístění je možné během konfigurace změnit, ale obecně se tento postup nedoporučuje. Nejvhodnějším řešením je tedy nechat složky na výchozím umístění.

Prerequisites Check (kontrola předpokladů) – Finální část instalace, kdy se kontroluje, zda je vše nastaveno správně a zda jsou splněny všechny podmínky pro dokončení instalace AD DS. V tomto bodě také dochází ke kontrole hesla administrátorského účtu, který se povyšuje na doménového administrátora.

Pokud jsme v těchto konfiguračních krocích instalace postupovali správně, instalace bude ukončena a proběhne restart systému. Po znovunačtení nás již přivítá přihlašovací obrazovka. V tomto případě se již nebudeme přihlašovat účtem lokálním, ale účtem doménovým.

9.4 Instalace a konfigurace služby DHCP

Proces instalace služby DHCP je velmi přímočarý proces bez nutnosti složité konfigurace. Opět pomocí konzole Server Manager zvolíme ze seznamu služeb DHCP a potvrdíme instalaci. Jedinou výzvou, kterou během instalace dostaneme, je výběr účtu, který bude autorizován pro správu služby DHCP. Dokončení instalace nevyžaduje restart a nová služba je tak okamžitě připravena.



Obrázek 6: okno nástroje pro správu DHCP

Nástroj pro správu služby DHCP najdeme pod tlačítkem „Tools“ v horním rohu konzole Server Manager. Po rozkliknutí domény vybereme příslušnou verzi TCP protokolu, v tomto případě IPv4, a pravým kliknutím otevřeme kontextové menu, kde zvolíme možnost „New Scope“. Vytvořením nového oboru (New Scope) nás provede konfigurační průvodce. Pro správnou konfiguraci nového oboru musíme znát a předem si naplánovat několik bodů.

Rozsah IP adres – Volíme IP adresy, které budeme chtít distribuovat mezi klienty. Zadává se ve tvaru od – do, například: 192.168.2.1 – 192.168.2.150.

Exkluze – Ty IP adresy, které chceme ze zvoleného rozsahu vyloučit. V případě, že již máme v síti zařízení, která používají IP adresu obsaženou v našem rozsahu a vznikl by tak síťový konflikt. Opět zadáváme v rozsahu od – do.

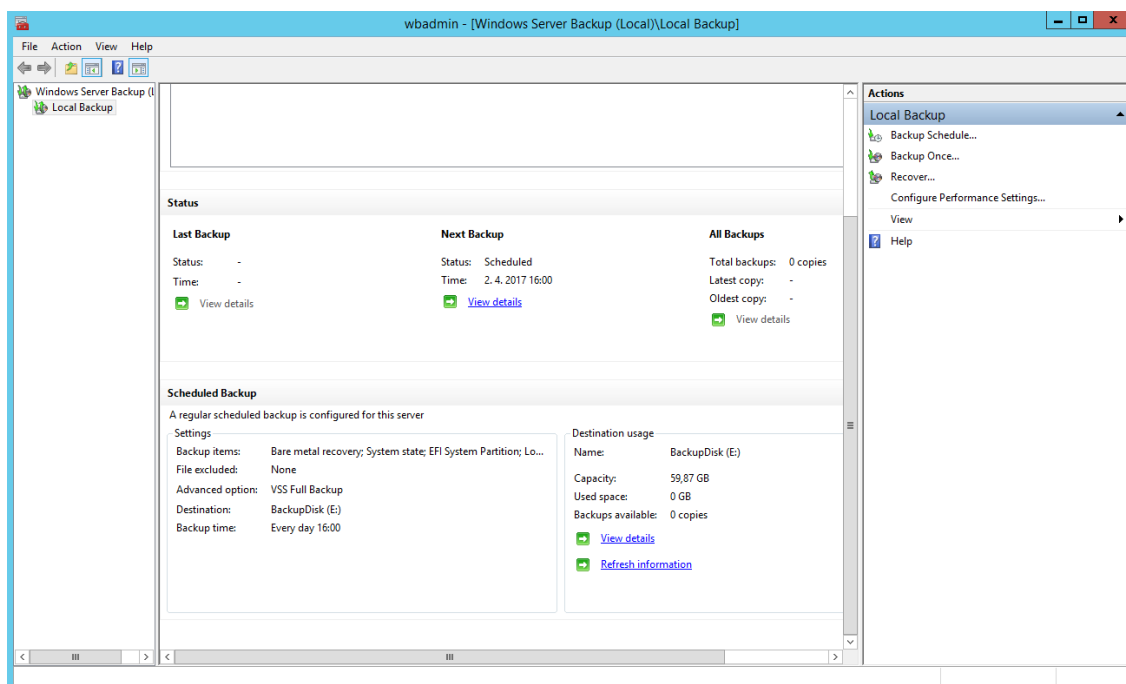
Doba výpůjčky – Tedy doba, po kterou bude přiřazená IP adresa náležet klientovi. Po uplynutí této doby si klient vyžádá novou IP adresu nebo se prodlouží výpůjčka staré. Kratší doba se doporučuje pro síť s velkým počtem mobilních zařízení. Delší doba naopak pro síť s pevnými zařízeními, jako například počítačová učebna.

Výchozí brána – Zadáváme IP adresu výchozí brány, kterou využíváme v síti. Například IP adresu Wi-Fi routeru. Není potřeba vyplňovat, máme-li zcela uzavřenou síť a výchozí bránu tak nepotřebujeme.

Dokončením konfigurace dojde k okamžitému vytvoření nového oboru v okně nástroje DHCP. Najdeme zde: zvolený rozsah, seznam přidělených IP adres, seznam rezervací atd. V tomto okamžiku již každé nové zařízení, které se do sítě připojí, obdrží jednu z IP adres nastaveného rozsahu a bude viditelné v seznamu výpůjček.

9.5 Instalace a konfigurace funkce Windows Server Backup

Na rozdíl od služby AD DS nebo DHCP, je Windows Server backup pouze funkcí. Instalační proces je tedy velmi jednoduchý a nevyžaduje žádné plánování. Funkci jednoduše nainstalujeme pomocí konzole Server Manager a můžeme okamžitě zálohovat.



Obrázek 7: okno nástroje pro správu funkce Windows Server Backup

Po dokončení instalace si pomocí tlačítka „Tools“ otevřeme nástroj pro správu funkce Windows Server Backup. Pomocí tohoto nástroje můžeme vytvořit okamžitou jednorázovou zálohu systému, naplánovat každodenní automatickou zálohu ve zvoleném čase nebo spustit proces obnovy.

Při tvorbě plánované zálohy nás konfigurační průvodce provede několika body. Pomocí tohoto průvodce specifikujeme, jak bude záloha probíhat. Nastavení je velmi jednoduché a skládá se ze tří kroků.

Výběr typu zálohy – Volíme mezi kompletní zálohou celého systému a všech svazků a disků (Full Backup) nebo vlastní zálohou (Custom Backup), kde můžeme přímo zvolit, které objekty se budou zálohovat.

Čas zálohování – To je čas, ve kterém bude záloha zahájena. Lze nastavit jednodenní zálohu, například každý den v 20:00 nebo můžeme zálohovat i několikrát denně. Vhodný čas pro zahájení zálohování je ve chvíli, kdy neočekáváme vysokou vytíženost serveru. Zálohovací proces totiž může způsobit výrazné snížení rychlosti systému.

Umístění zálohy – Zde volíme, kam se bude záloha ukládat. Na výběr máme ze tří možností:

- záloha na pevný disk: v tomto případě dojde k naformátování a disk bude vyhrazen pouze pro ukládání záloh.
- záloha na svazek: tato možnost je vhodná, pokud nemůžeme vyhradit celý pevný disk pouze zálohám. Nevýhodou je velké vytížení disku během zálohování.
- záloha do sdílené síťové složky: pokud nechceme ukládat zálohy lokálně, můžeme je ukládat do síťové lokace. V tomto případě se ovšem ukládá pouze jedna záloha a nová záloha okamžitě přepisuje tu starou. Pro obnovu máme tedy k dispozici vždy jen nejaktuálnější zálohu.

Jakmile veškeré předvolby plánovaného zálohování potvrdíme, dojde k automatickému vytvoření zálohovacího plánu. Defaultně dojde k první záloze druhý den od tvorby plánu. Historii záloh včetně záznamu o jejich průběhu můžeme sledovat přímo v okně nástroje Windows Server Backup.

Pokud bychom potřebovali vytvořit zálohu okamžitě, můžeme využít funkce „Zálohovat jednou“ (Backup Once), kdy dojde k vytvoření zálohy okamžitě. Pokud již máme předem vytvořený zálohovací plán, není nutné jednorázovou zálohu nastavovat. Stačí vybrat možnost zálohovat podle pravidel plánu a záloha se okamžitě provede přesně tak, jako by se provedla v čase, který je pro zálohování vyhrazen.

V tomto okamžiku máme tedy k dispozici automatické zálohování celého serveru včetně přiřazených disků. Máme tedy jistotu, že pokud dojde k poruše či korupci dat, budeme schopni tyto data pomocí funkce Windows Server Backup obnovit.

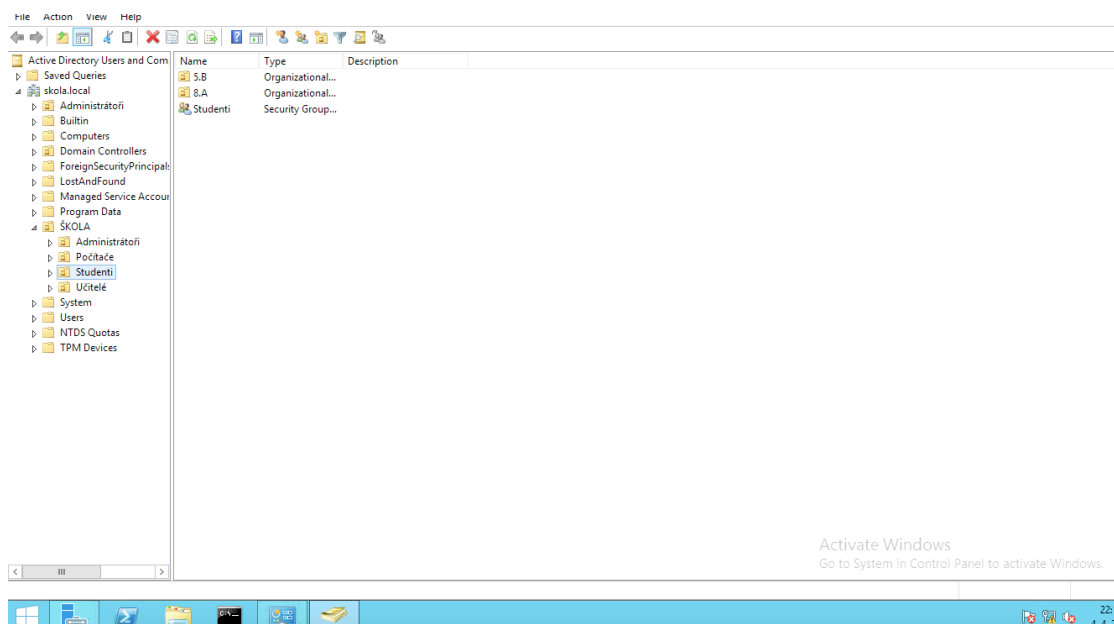
V této kapitole jsme si tedy stručně vysvětlili proces instalace potřebných součástí serveru včetně základní konfigurace potřebné ke správnému fungování těchto služeb a funkcí. Máme tedy server, který je připraven plnit svou funkci jako koordinátor učebny. Potřebujeme tedy přidat doménové objekty, tedy uživatele, kteří budou funkce server používat.

10 Tvorba a správa doménových objektů

Tato kapitola se zabývá popisem procesu tvorby a organizace doménových objektů a toho, jak můžeme tyto objekty spravovat. V první části si tedy popíšeme proces tvorby organizačních jednotek, uživatelských skupin a uživatelských účtů. Druhá část této kapitoly se bude věnovat popisu využití nástroje pro úpravu doménových práv Group Policy. Princip tvorby a fungování doménových práv si ukážeme na názorném příkladu přesměrování uživatelských složek do společné lokace.

10.1 Tvorba objektů

Pro tvorbu objektů domény využijeme nástroj Active Directory Users and Computers, který jsme získali instalací služby AD DS. Tento nástroj nám umožňuje vytvářet, upravovat a mazat doménové objekty.



Obrázek 8: okno nástroje pro správu AD DS Users and Computers

Samotná tvorba objektů je velmi podobná jako tvorba nových složek či dokumentů v klasickém operačním systému Windows. Pomocí pravého tlačítka do příslušné lokace, kde chceme vytvářet nový objekt, vyvoláme kontextové menu. Po zvolení možnosti „New“ si vybereme námi požadovaný objekt. Objekt se okamžitě vytvoří a máme možnost specifikovat jeho podrobnosti v nově zobrazeném okně. Pro potřeby počítačové domény budeme potřebovat vytvořit čtyři základní objekty: organizační jednotku, skupinu uživatelů, uživatelský účet a účet počítače. Tvorba objektů je velmi jednoduchá, liší se zejména specifikací podrobností, o které je potřeba objekty doplnit.

Organizační jednotka

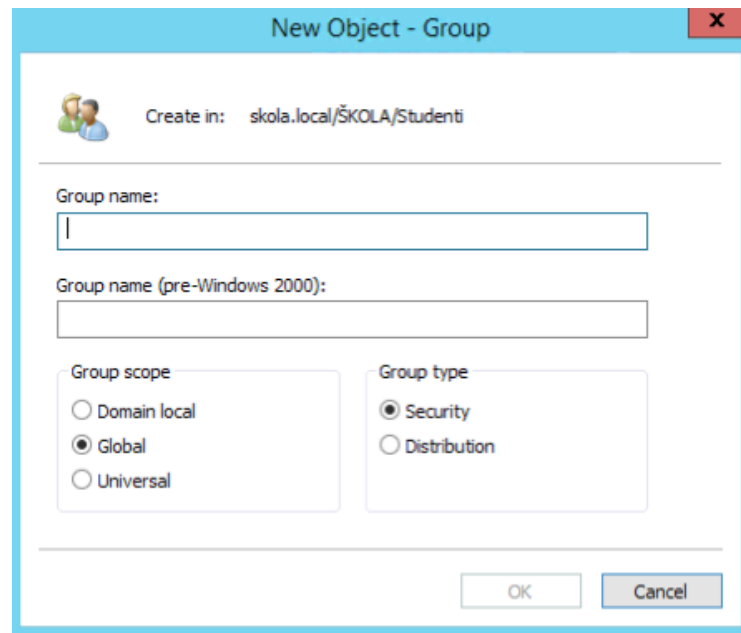
Při tvorbě organizační jednotky specifikujeme pouze jméno a ochranu proti náhodnému smazání. Ochrana proti náhodnému smazání neumožňuje soubor smazat klasickým způsobem, ale je potřeba nejdříve tuto ochranu zrušit a až poté je možné objekt smazat.

Uživatelská skupina

Tvorba nové skupiny uživatelů je velmi jednoduchá. Specifikujeme pouze jméno skupiny, rozsah skupiny a typ skupiny. viz. obrázek 9. Jméno by mělo vystihovat uživatele, které obsahuje. Rozsah skupiny ovlivňuje to, kde budou moci členové této skupiny působit. Lokální skupina může působit pouze v doméně na které sídlí. Globální skupina může působit na kterékoliv doméně doménového lesa. Universální skupina pak

může působit v rámci několika doménových lesů. Co se typu skupiny týče pak na Bezpečnostní skupinu lze aplikovat bezpečnostní práva NTFS, zatímco na Distribuční skupinu nikoliv. Distribuční typ je vhodný zejména pokud potřebujeme šetřit vytiženost serveru způsobenou neustálým ověřováním bezpečnostních práv (32).

Uživatele či jiné skupiny přidáváme do skupiny v nastavení vlastností po vytvoření v kolonce „Members“.



Obrázek 9: specifikace podrobností nové skupiny

Uživatelský účet

V tomto případě specifikujeme základní osobní údaje uživatele, přihlašovací jméno a heslo. Je potřeba si promyslet, jaký tvar přihlašovacího jména použijeme. Běžně se používá například tvar 5+3, tedy pět prvních písmem příjmení + tři první písmena křestního jména.

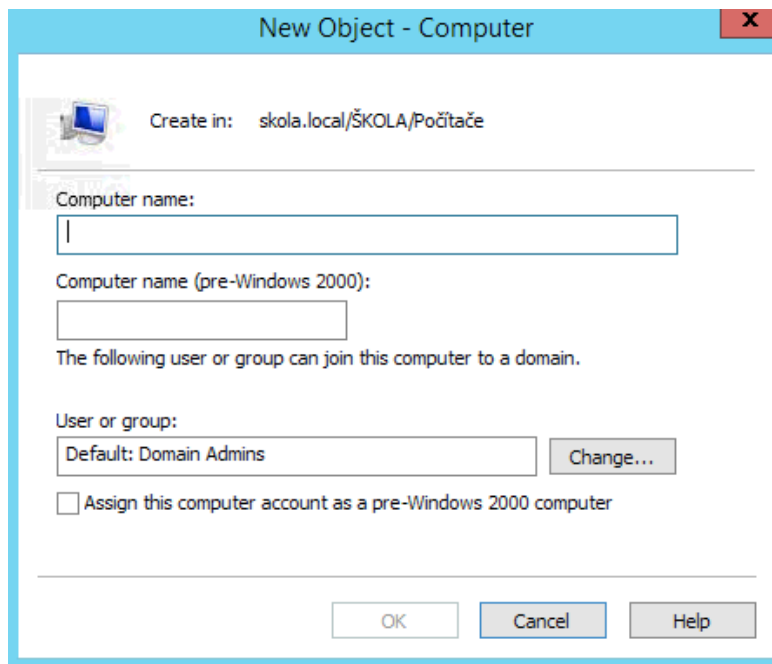
The image shows a Windows dialog box titled "New Object - User". At the top, it says "Create in: skola.local/ŠKOLA/Studenti/5.B". Below this, there are several input fields: "First name:" with an empty text box and "Initials:" with a smaller empty text box; "Last name:" with an empty text box; "Full name:" with an empty text box; "User logon name:" with an empty text box and a dropdown menu showing "@skola.local"; and "User logon name (pre-Windows 2000):" with "SKOLA\'" entered in the text box. At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel".

Obrázek 10: specifikace podrobností nového uživatelského účtu

Po vytvoření objektu musíme také nového uživatele přidat do příslušné skupiny. To můžeme udělat buď pomocí upravením vlastností uživatele, nebo uživatelské skupiny, do které jej chceme přidělit. V případě uživatele se jedná o kolonku „Member of“.

Účet počítače

Opět velmi jednoduchý proces. Specifikujeme jméno, které by mělo odpovídat tomu, jak jsme počítač pojmenovali v operačním systému a vybereme uživatele nebo skupinu, která je oprávněna tento počítač připojit do domény. Nově přidaný počítač se pak automaticky připojí k tomuto účtu.

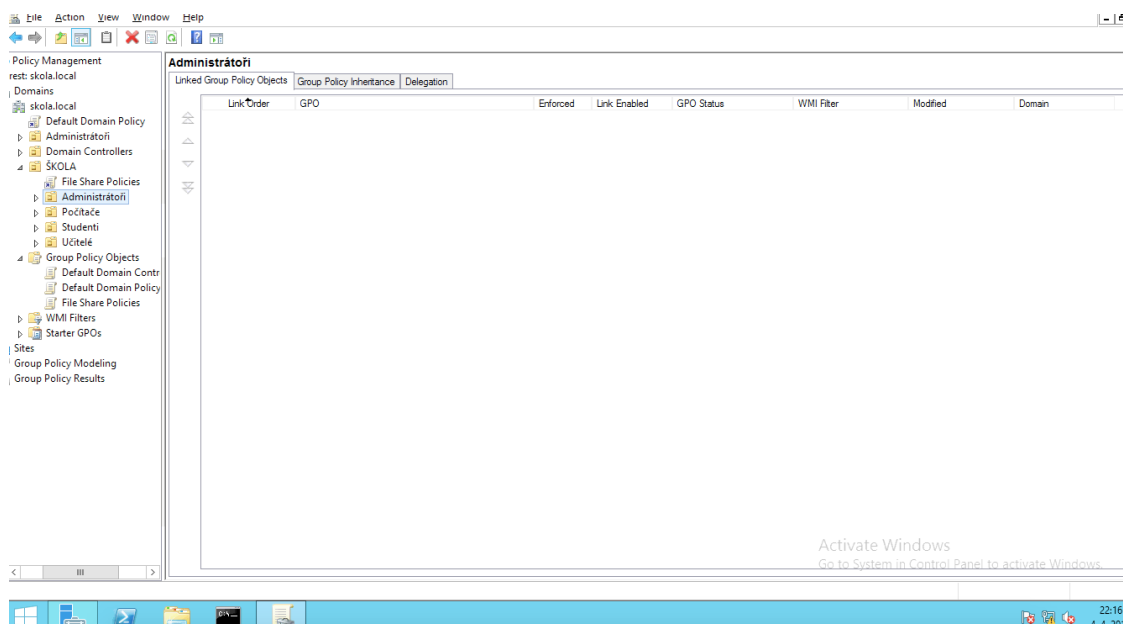


Obrázek 11: specifikace podrobností nového účtu počítače

V této chvíli máme tedy vytvořené veškeré objekty, které budou v počítačové učebně figurovat. Nyní si popíšeme jak vytvořit a upravit doménová práva, která budou tyto objekty omezovat. Vzhledem k tomu, že problematika doménových práv je velmi obsáhle téma, které by vystačilo na několik knih, jedná se spíše o nastínění základního procesu tvorby a úpravy.

10.2 Tvorba doménových práv

K tvorbě a úpravě doménových práv využijeme nástroj pro správu Group Policy. Pomocí tohoto nástroje můžeme vytvářet a upravovat doménová práva. Při tvorbě domény se automaticky vytvoří defaultní doménová práva, která upravují všechny objekty v doméně. Vhodným postupem je tyto výchozí práva neupravovat a pro potřebu vlastních změn vytvářet práva nová.



Obrázek 12: okno nástroje pro úpravu doménových práv

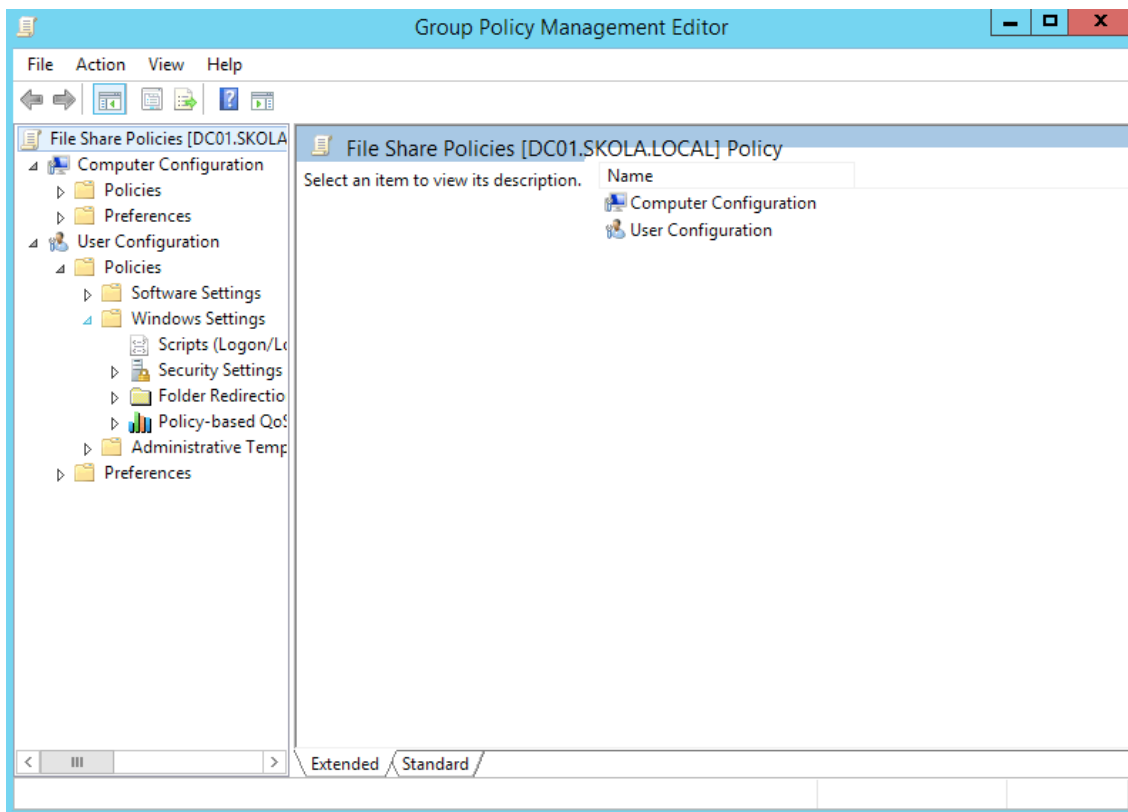
Nově vytvořená práva se automaticky ukládají do složky Group Policy Objects. Z této složky pak můžeme tyto práva odkazovat na příslušné objekty. Práva lze odkazovat na úroveň domény nebo na vybrané organizační jednotky. Pokud vybereme úroveň domény, práva budou platit pro všechny objekty domény. Pokud odkážeme na konkrétní organizační jednotku, práva budou platit na všechny objekty, které tato jednotka obsahuje.

Přesměrování složek

Pro představu, jak probíhá tvorba doménových práv, si ukážeme názorný příklad, kdy osobní složky: *dokumenty* a *plocha* přesuneme na serverové úložiště, abychom zajistili, že data v těchto složkách budou zálohovány. Po nastavení tak automaticky dojde k vytvoření osobní složky uživatele ve specifikované sdílené lokaci, která bude obsahovat osobní složky *dokumenty* a *plocha*. Velkou výhodou je, že uživatel nepozná, že byly jeho složky přesměrovány.

Začneme tedy v okně nástroje pro úpravu doménových práv, kde vytvoříme nová práva s názvem například „Práva úložiště“. Práva můžeme ihned odkázat na nejvýše postavenou organizační jednotku. Chceme, aby se tato změna týkala všech objektů, které jsme v doméně vytvořili. Poté na nově vytvořená práva klikneme pravým

tlačítkem a vybereme možnost „Edit“. Zobrazí se nám okno editoru pro specifikaci konkrétních nastavení.



Obrázek 13: okno editoru doménových práv

V tomto editoru můžeme konfigurovat jak nastavení pro počítače, tak nastavení pro uživatele. V našem případě budeme využívat přesměrování složek uživatelů. Budeme tedy postupovat přes složky User Configuration, Policies, Windows Settings a Folder Redirection kde si vybere složky, které budeme chtít přesměrovat. V našem případě složky Documents a Desktop. Pravým klikem otevřeme okno vlastností, kde provedeme potřebná nastavení.

Zde volíme možnost uložení všech souborů do společné lokace a specifikujeme, že chceme pro každého uživatele vytvořit samostatnou složku. Posledním krokem je výběr síťové lokace, do které budeme tyto složky ukládat. Je důležité, aby do této složky měl přístup každý uživatel a to jak Read, tak Write.

Po ukončení editoru se naše nastavení uloží a stane se platným. Některé změny práv vyžadují, aby se uživatel odhlásil a znovu přihlásil. Některá nová práva se totiž aplikují ve chvíli, kdy se uživatel přihlašuje.

V této kapitole jsme si popsali proces tvorby základních objektů domény, které budeme využívat. Dále jsme si na názorném příkladu stručně vysvětlili proces tvorby nových doménových práv. Pro potřeby učebny bude potřeba specifikovat takovýchto nastavení doménových práv daleko více. Tento příklad byl opravdu spíše ilustrativním popisem toho, jak tento proces probíhá. Jelikož jsme v tomto příkladu specifikovali síťovou lokaci, do které se budou ukládat uživatelské soubory, bylo by vhodné se nyní podívat na to, jak takové síťové úložiště vytvořit.

11 Tvorba sdíleného úložiště

Tato kapitola se zaměřuje na vysvětlení procesu tvorby sdílených složek a úpravu přístupových práv. Cílem je vytvořit sdílené úložiště, které bude sloužit uživatelům školní učebny k ukládání a sdílení potřebných souborů. Názorně si také ukážeme, jak funguje jednoduchý nástroj sdílení a jak nastavujeme bezpečnostní práva NTFS.

V našem úložišti využijeme dvě hlavní, tzv. kořenové složky. Jedna bude sloužit pro uložení osobních složek uživatelů, které jsme přesměrovali v kapitole 10, a druhá bude sloužit pro sdílení souborů.

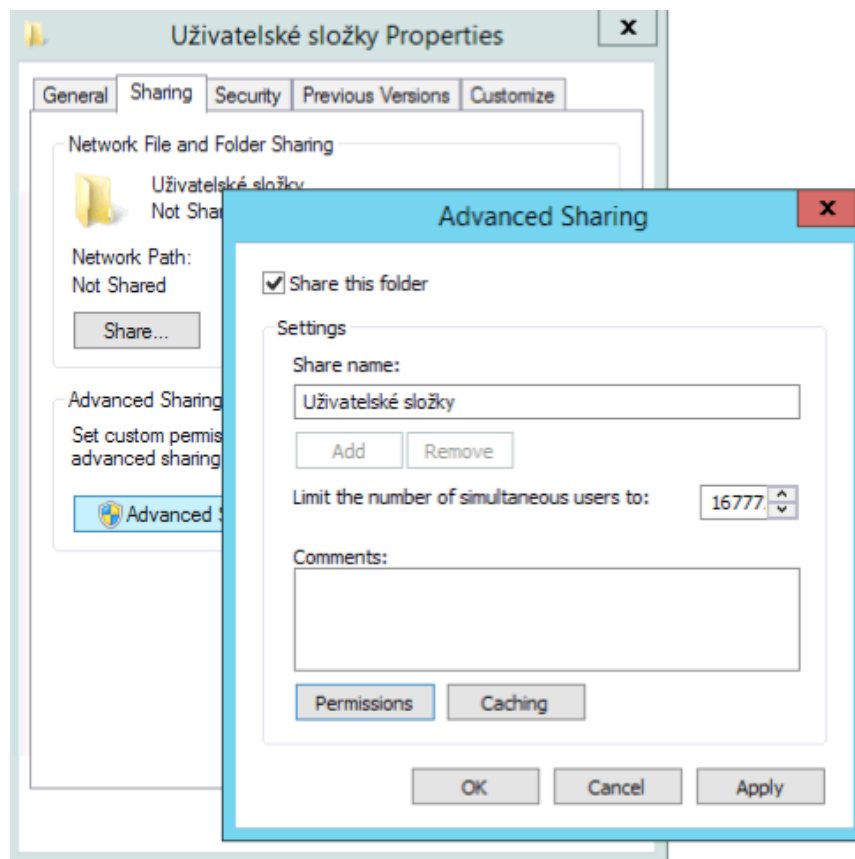
11.1 Osobní soubory

Velmi jednoduchým procesem bude vytvoření kořenové složky pro ukládání osobních souborů uživatelů. Na požadovaném disku vytvoříme novou složku⁴. Ve vlastnostech této složky vybereme kolonku „Sharing“ a poté možnost „Advanced Sharing“. V okně pokročilých nastavení můžeme specifikovat jméno sdílené složky, které je vhodné zvolit totožné se jménem složky a také přístupová práva. Dále můžeme specifikovat přístupová práva této složky, kde určíme, kteří uživatelé či uživatelské skupiny budou moci k této složce přistupovat a zda budou moci provádět změny.

Jelikož potřebujeme, aby se v této lokaci mohla vytvořit osobní složka pro každého uživatele, musíme tuto složku zpřístupnit všem uživatelům. Výchozí skupinou, které má přístupová práva k nově sdílené složce je skupina „Everyone“, tedy všichni. Jedná se o jednu z výchozích uživatelských skupin operačního systému. Tato skupina tedy umožňuje přístup do sdílené složky komukoliv na síti. To ovšem představuje

⁴ Nesmíme zapomenout upravit cestu k této složce v editoru doménových práv, kde jsme přesměrovali osobní složky.

potencionální bezpečnostní riziko, protože našim cílem je, aby k doménovým souborům měli přístup pouze ti uživatelé, kteří mají platný doménový účet. K těmto účelům se využívá další výchozí skupina s názvem „Authenticated Users“ neboli ověření uživatelé. Nesmíme této skupině zapomenout přidělit přístupová práva pro čtení a zápis.



Obrázek 14: okno nastavení pokročilých možností sdílení

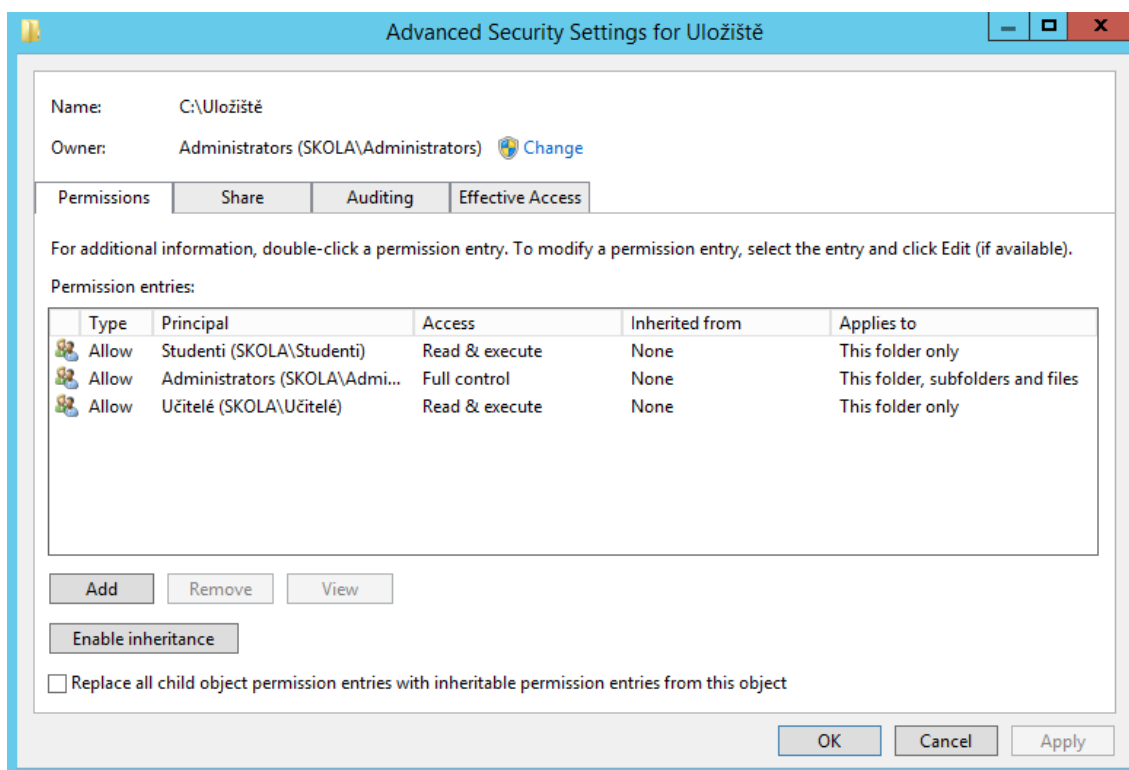
Jakmile dokončíme nastavení sdílení složky, do které jsme přesměrovali uživatelské osobní složky, začnou se v této lokaci automaticky vytvářet složky s přihlašovacím jménem uživatelů, kteří se přihlásili do domény. Výhodou je, že ačkoliv jsme umožnili do centrální složky přístup všem uživatelům, na jednotlivé osobní složky se aplikují doménová práva, která povolí přístup pouze majitelům těchto složek. Třetí osoba tak nemůže nahlížet do osobních souborů a my nemusíme konfigurovat bezpečnostní práva NTFS. Nejdůležitější soubory uživatelů tedy ty, které si uloží do složky dokumenty nebo ponechají na ploše, jsou nyní uloženy také na serveru a řádně zálohovány.

11.2 Sdílené soubory

V této chvíli máme tedy vytvořenou centrální složku, do které se ukládají osobní soubory uživatelů, ke kterým mají přístup pouze majitelé těchto složek. Ve školním prostředí je ale také potřeba sdílet soubory mezi jednotlivými uživateli, ať už se jedná o odevzdávání prací nebo elektronické zadání úkolu. Musíme tedy vytvořit takové úložiště, které bude veřejné, ale bude nabízet rozdílná přístupová práva. Jedna část tohoto úložiště by tak měla sloužit učitelům, pro ukládání a zadávání prací pro studenty a druhá část by měla sloužit studentům pro sdílení a případné odevzdávání úkolů.

Vytvoříme si tedy novou sdílenou kořenovou složku tak jako v případě složky pro ukládání přesměrovaných souborů. Tentokrát v této složce vytvoříme dvě podsložky: učitelé a studenti. Musíme ovšem uživatelům zamezit tvorbu a mazání souborů a složek v kořenové složce, tak aby nenarušovali strukturu úložiště. Následně musíme nastavit různá přístupová práva do složek studenti a učitelé. Jelikož v tomto případě neaplikujeme žádná speciální doménová práva, která by zajistila práva přístupová, musíme využít nástroje pro správu bezpečnostních práv NTFS a definovat přístupová práva ručně.

Kořenovou složku zpřístupníme ostatním uživatelům pomocí okna „Advanced Sharing“, kde specifikujeme skupinu „Authenticated Users“ a udělíme jí práva „Full Control“ tedy úplná práva. V tuto chvíli jsme umožnili přístup ověřeným uživatelům v doméně bez omezení práv. Nyní musíme uživatele omezit úpravou bezpečnostních práv.



Obrázek 15: okno pokročilých nastavení práv NTFS

Pomocí nastavení práv NTFS upravíme práva požadovaných uživatelských skupin, aby mohli z kořenové složky číst, ale nemohli soubory vytvářet a upravovat. Jelikož se práva sdílení dědí i na podsložky musíme u toho nastavení tuto dědičnost vypnout. Pokud bychom tento krok neučinili, uživatelé by nemohli zapisovat ani do podsložek, ve kterých to požadujeme. Tímto způsobem zachováme tvar kořenové složky tak, že bude obsahovat pouze složky studenti a učitelé a tuto strukturu nebudou uživatelé moci narušit.

Posledním krokem je upravit bezpečnostní práva NTFS podsložek studenti a učitelé. Studentské skupině uživatelů musíme zakázat možnost zápisu a úprav ve složce učitelé a stejné omezení můžeme natakavit pro učitelkou skupinu ve složce studenti. V tomto případě jde o to, jaké požadavky na úložíště máme.

Posledním krokem by mohla být úprava doménových práv tak, že se sdílená složka každému uživateli uloží jako síťový disk a bude tak vždy jednoduše dostupná.

Cílem této kapitoly bylo stručně nastínit popis tvorby sdíleného úložíště, které může sloužit k záloze důležitých souborů uživatelů a také sdílení souborů mezi uživateli. Na tomto základě lze dle individuálních potřeb úložíště dále rozvíjet a upravovat.

Závěr

Cílem této práce bylo ukázat některé výhody, které přináší využití operačního systému Microsoft Windows Server a to zejména služby Active Directory Domain Services, pro správu počítačové učebny.

Aby bylo možné si tyto výhody představit, vytvořili jsme model reálné počítačové učebny. Na tento model jsme aplikovali jednotlivé služby a funkce a názorně jsme si předvedli jakým způsobem je instalovat, konfigurovat a spravovat. Výhody, které tato aplikace přináší, jsme si tak nejen ukázali, ale jsme je schopni i realizovat.

První kapitola nás seznámila s pojmem centralizace a jejími typy. Na tomto základě jsme pak v kapitole osm vytvářeli fyzický model názorné učebny a celkovou strukturu nové domény. Díky centralizaci správy tak lze zefektivnit administraci a bezpečnost učebny.

Druhá kapitola se zabývala popisem operačního systému Microsoft Windows Server. Operační systém byl také první instalovanou součástí, kterou se zabývala kapitola devět.

Dále jsme si představili službu Active Directory. Důležitými body této kapitoly byly pojmy doména a doménová práva Group Policy. Službu AD DS jsme v kapitole devět naistalovali a poté jsme si v kapitole deset nastínili proces její správy od tvorby uživatelů až po definici doménových práv. Active Directory se také týkala kapitola čtyři, ve které je popsána služba DNS.

V páté kapitole je vysvětlen pojem file server a také problematika možnosti sdílení souborů a nastavení přístupových práv. Tyto znalosti pak aplikujeme v kapitole jedenáct při tvorbě společného úložiště. Uživatelé učebny tak mohou sdílet a ukládat svá data.

Kapitola šestá popisuje problematiku zálohování pomocí funkce Windows Server Backup. Celkový proces instalace a konfigurace je pak názorně popsán v kapitole devět. Záloha tak chrání data uživatelů a nabízí ochranu proti nečekanému selhání techniky.

Posledním prvkem, který jsme v deváté kapitole instalovali a konfigurovali, pak byla služba DHCP, jež je popsána v kapitole sedm. Tato služba poskytuje přehled nad počítači v síti, což přispívá k celkové bezpečnosti a jednodušší administraci.

Využitím služby Active Directory Domain Services a dalších služeb a funkcí, které operační systém Windows Server nabízí, se nám podařilo vytvořit multifunkční prostředí, které umožňuje zefektivnit administraci, zvýšit bezpečnost uživatelů a jejich dat, a hlavně nabízí uživatelům vlastní pracovní prostředí, jak bylo stanoveno v úvodu této práce.

V budoucnu by bylo možné například celou učebnu virtualizovat, což by mohlo pomoci snížit náklady na hardwarové vybavení učebny. Dalšími možnostmi by bylo rozšířit již fungující doménovou strukturu na úroveň celé školní sítě nebo vylepšit funkcionalitu serveru migrací na novou verzi operačního systému.

Seznam ilustrací a tabulek

Obrázek 1: grafické zobrazení Centralizované a Decentralizované sítě

Obrázek 2: hlavní doména rozdělená do pod-domén, doménový strom

Obrázek 3: grafické znázornění počítačové učebny

Obrázek 4: návrh doménové struktury

Obrázek 5: hlavní menu nástroje Server Manager

Obrázek 6: okno nástroje pro správu DHCP

Obrázek 7: okno nástroje pro správu funkce Windows Server Backup

Obrázek 8: okno nástroje pro správu AD DS Users and Computers

Obrázek 9: specifikace podrobností objektu nové skupiny

Obrázek 10: specifikace podrobností nového uživatele

Obrázek 11: specifikace podrobností nové účtu počítače

Obrázek 12: okno nástroje pro správu doménových práv

Obrázek 13: okno editoru doménových práv

Obrázek 14: okno nastavení pokročilých možností sdílení

Obrázek 15: okno pokročilých nastavení práv NTFS

Tabulka 1: porovnání jednotlivých typů záloh

Seznam použité literatury

1. Centralization. *BusinessDictionary*[online]. WebFinance, c2017 [cit. 2017-04-08]. Dostupné z:
<http://www.businessdictionary.com/definition/centralization.html>
2. Your IT Organizational Structure: Should You Centralize or Decentralize? *Software Advice*[online]. Software Advice™, c2006-2017 [cit. 2017-04-08]. Dostupné z: <http://www.softwareadvice.com/resources/it-org-structure-centralize-vs-decentralize/>
3. Network Planning: Centralized Vs. Decentralized Data Processing | Computer Networking. *YourArticleLibrary* [online]. YourArticleLibrary.com, c2016 [cit. 2017-04-12]. Dostupné z: <http://www.yourarticlelibrary.com/networks/network-planning-centralized-vs-decentralized-data-processing-computer-networking/10447/>
4. BARAN, Paul. *On distributed communications: Introduction to distributed communications networks*. California: The Rand Corporation, 1964.
5. Windows Server. *Msdn*[online]. Microsoft, c2017 [cit. 2017-04-08]. Dostupné z: [https://msdn.microsoft.com/en-us/library/dn636873\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/dn636873(v=vs.85).aspx)
6. STANEK, William R. *Microsoft Windows server 2012 inside out*. Redmond, Wash.: Microsoft Press, c2013. ISBN 0735666318.
7. ZACKER, Craig. *Exam ref 70-410: installing and configuring Windows Server 2012 R2*. Sixth printing. Redmond, Washington: Microsoft Press, 2015. ISBN 978-0735684249.
8. Roles, Role Services, and Features. *Technet*[online]. Microsoft, c2017 [cit. 2017-03-29]. Dostupné z: [https://technet.microsoft.com/en-us/library/cc754923\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/cc754923(v=ws.11).aspx)

9. Chapter 7: Configuring Roles, Role Services, and Features. *Msdn*[online]. Microsoft, c2017 [cit. 2017-04-12]. Dostupné z: <https://msdn.microsoft.com/en-us/library/dd184080.aspx>
10. Active Directory Domain Services. *Msdn*[online]. Microsoft, c2107 [cit. 2017-03-29]. Dostupné z: [https://msdn.microsoft.com/en-us/library/aa362244\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/aa362244(v=vs.85).aspx)
11. DESMOND, Brian, Joe RICBARDS, Robbie ALLEN a Alistair G. LOWE-NORRIS. *Active Directory*. 5th edition. Sebastopol: O'Reilly Media, 2013. ISBN 1449320023.
12. Documenting the Lab Configuration. *Technet* [online]. Microsoft, c2017 [cit. 2017-04-09]. Dostupné z: <https://technet.microsoft.com/en-us/library/cc961191.aspx>
13. Domain Controller Roles. *Technet* [online]. Microsoft, c2017 [cit. 2017-04-08]. Dostupné z: [https://technet.microsoft.com/en-us/library/cc786438\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc786438(v=ws.10).aspx)
14. Step-by-Step Guide to Understanding the Group Policy Feature Set. *Msdn* [online]. Microsoft, c2017 [cit. 2017-03-29]. Dostupné z: <https://msdn.microsoft.com/en-us/library/bb742376.aspx>
15. Group Policy for Beginners. *Technet* [online]. Microsoft, c2017 [cit. 2017-04-12]. Dostupné z: [https://technet.microsoft.com/en-us/library/hh147307\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/hh147307(v=ws.10).aspx)
16. Domain Name System. *Msdn* [online]. Microsoft, c2017 [cit. 2017-04-12]. Dostupné z: [https://msdn.microsoft.com/en-us/library/windows/desktop/ms682100\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/desktop/ms682100(v=vs.85).aspx)

17. PANEK, William. MCSA Windows Server 2012 R2 complete study guide. 2nd edition. Sybex, 2015. ISBN 978-1118859919.
18. Understanding Zone Types. *Technet* [online]. Microsoft, c2017 [cit. 2017-04-08]. Dostupné z: [https://technet.microsoft.com/en-us/library/cc771898\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/cc771898(v=ws.11).aspx)
19. Managing the File Services Role. *Msdn* [online]. Microsoft, c2017 [cit. 2017-04-12]. Dostupné z: <https://msdn.microsoft.com/en-us/library/dd163554.aspx>
20. File and Storage Services Overview. *Technet* [online]. Microsoft, c2017 [cit. 2017-03-29]. Dostupné z: [https://technet.microsoft.com/en-us/library/hh831487\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/hh831487(v=ws.11).aspx)
21. Prostory úložiště – přehled. *Technet* [online]. Microsoft, c2017 [cit. 2017-03-29]. Dostupné z: <https://technet.microsoft.com/library/hh831739.aspx>
22. Přehled Přesměrování složky, Offline souborů a Cestovních profilů uživatelů. *Technet* [online]. Microsoft, c2017 [cit. 2017-03-29]. Dostupné z: <https://technet.microsoft.com/library/hh848267.aspx>
23. Pracovní složky – přehled. *Technet* [online]. Microsoft, c2017 [cit. 2017-03-29]. Dostupné z: <https://technet.microsoft.com/library/dn265974.aspx>
24. Advantages of NTFS. *Technet* [online]. Microsoft, c2017 [cit. 2017-03-29]. Dostupné z: <https://technet.microsoft.com/en-us/library/cc976817.aspx>
25. Backing Up Your Server. *Technet* [online]. Microsoft, c2017 [cit. 2017-03-29]. Dostupné z: [https://technet.microsoft.com/en-us/library/cc753528\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/cc753528(v=ws.11).aspx)

26. Backup Types: Full, Incremental, Differential. *EnterpriseFeatures* [online]. Enterprise Features Staff, 2015 [cit. 2017-04-09]. Dostupné z: <http://www.enterprisefeatures.com/backup-types-full-incremental-differential/>
27. Full, incremental or differential: How to choose the correct backup type. *SearchDataBackup* [online]. Techtarget, 2008 [cit. 2017-03-29]. Dostupné z: <http://searchdatabackup.techtarget.com/feature/Full-incremental-or-differential-How-to-choose-the-correct-backup-type>
28. Configuring a DHCP Scope. *Technet* [online]. Microsoft, c2017 [cit. 2017-04-12]. Dostupné z: [https://technet.microsoft.com/en-us/library/dd759218\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/dd759218(v=ws.11).aspx)
29. Server Manager. *Technet* [online]. Microsoft, 2008 [cit. 2017-04-08]. Dostupné z: [https://technet.microsoft.com/en-us/library/cc732131\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc732131(v=ws.10).aspx)
30. Directory Services Restore Mode (DSRM). *SearchWindowsServer*[online]. Techtarget, 2008 [cit. 2017-04-08]. Dostupné z: <http://searchwindowsserver.techtarget.com/definition/Directory-Services-Restore-Mode-DSRM>
31. NetBIOS Domain Names. *Technet* [online]. Microsoft, c2017 [cit. 2017-04-08]. Dostupné z: <https://technet.microsoft.com/en-us/library/cc961556.aspx>
32. Group scope. *Technet* [online]. Microsoft, c2017 [cit. 2017-04-08]. Dostupné z: [https://technet.microsoft.com/en-us/library/cc755692\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc755692(v=ws.10).aspx)

Anotace

Jméno a příjmení:	Michal Chmel
Katedra:	Katedra technické a informační výchovy
Vedoucí práce:	doc. PhDr. Milan Klement, Ph.D.
Rok obhajoby:	2017

Název práce:	Správa počítačové učebny pomocí Active Directory Domain Services
Název v angličtině:	Administering a computer lab using Active Directory Domain Services
Anotace práce:	<p>Tato práce si klade za cíl ukázat některé výhody, které nabízí využití platformy Microsoft Windows Server, zejména služeb Active Directory Domain Services, pro správu počítačové učebny.</p> <p>Teoretická část se zabývá popisem základních poznatků potřebných k pochopení podstaty jednotlivých funkcí.</p> <p>Praktická část vysvětluje na názorném příkladu proces instalace a konfigurace těchto komponent.</p>
Klíčová slova:	Windows, Server, Microsoft, Active Directory, správa, služba, funkce, počítač, učebna

Anotace v angličtině:	<p>The aim of this work is to show some of the advantages of using Microsoft Windows Server, especially one of its roles Active Directory Domain Services to administer a computer lab.</p> <p>The theoretical part focuses on describing the essential basics of the individual functions.</p> <p>The practical part explains the process of installation and configuration of these functions.</p>
Klíčová slova v angličtině:	<p>Windows, Server, Microsoft, Active Directory, management, service, feature, computer, lab</p>
Přílohy:	<p>CD s elektronickou verzí kvalifikační práce</p>
Rozsah práce:	<p>54 stran</p>
Jazyk práce:	<p>CZ</p>