UNIVERZITA PALACKÉHO V OLOMOUCI

PEDAGOGICKÁ FAKULTA

Katedra technické a informační výchovy

Bakalářská práce

Tomáš Kubíček

Optimalizace služeb datové sítě postavené na technologii Microsoft Active Directory

Olomouc 2018 Vedoucí práce: doc. PhDr. Milan Klement, Ph.D.

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně a použil výhradně uvedenou literaturu a zdroje.

V Olomouci dne _____ …….

Podpis

Poděkování

Děkuji autorům všech použitých zdrojů, díky jejichž znalostem mohla tato práce vzniknout. Největší poděkování však patří doc. PhDr. Milanu Klementovi, Ph.D. za jeho cenné rady, konstruktivní kritiku, a velmi vstřícný přístup po celou dobu tvorby této práce.

Obsah

Úvod

Datová síť je v dnešní době jedním ze základních stavebních kamenů každé organizace. V korporátním světě je optimalizaci jejích služeb, tedy zajištění její bezproblémové, efektivní a bezpečné funkce, přikládána značná důležitost, protože i malý technický problém může být v tomto prostředí příčinou značných finančních ztrát.

Ve školách však v současné době můžeme pozorovat spíše opačný trend. Školní datové sítě bývají často neoptimalizované. Struktura datových sítí zde často bývá chaotická a jejich správa necentralizovaná, což je způsobeno především tím, že školy nechtějí příliš investovat do IT infrastruktury, a také skutečností, že na školách chybí IT specialisti, kteří by pohotově reagovali na nové trendy a stále se ve svém oboru rozvíjeli. Nedostatečná optimalizace služeb datové sítě se projevuje časově neefektivní správnou datové sítě, zvýšenými bezpečnostními riziky souvisejícími s jejím využíváním a také tím, že odstranění technických problémů zabere mnohdy poměrně hodně času. Znepokojeni současnou situací, rozhodli jsme se pro bakalářskou práci zvolit téma optimalizace služeb datové sítě, s cílem zvýšit kvalitu školních datových sítí vytvořením užitečného a dostupného zdroje informací, který je možno pro účely optimalizace školní datové sítě efektivně použít.

Nejobecnějším z cílů práce je zvýšit povědomí o technologii Microsoft Active Directory a o možnostech jejího využití za účelem optimalizace služeb datové sítě. Dalším cílem je poskytnout návrh konkrétní struktury Active Directory pro vybranou školu, který je však jednoduše upravitelný a lze jej tedy použít i jako předlohu pro tvorbu struktur Active Directory pro jiné školy. Posledním z cílů práce je poskytnout jakýsi manuál, popisující praktickou realizaci navrženého řešení a rovněž možnosti využití tohoto řešení za účelem optimalizace služeb datové sítě. Cílovou skupinou práce jsou především správci školních datových sítí, případně další osoby se zájmem o zvolené téma, které disponují obecným přehledem v oboru informačních technologií.

V práci nejprve uvádíme kapitoly, které lze na základě jejich obsahu označit za teoretické. V těchto kapitolách, vytvořených na základě studia odborné literatury a rovněž autorových osobních zkušeností z oboru informačních technologií, je rozebráno, co je podstatou technologie Active Directory. Jsou zde osvětleny základní pojmy, které je v souvislosti s pochopením této technologie nutné znát a uvádíme zde rovněž další informace, které považujeme za důležité z hlediska tvorby návrhu struktury Active Directory. Na základě všech

získaných informací a rovněž vstupních údajů, charakterizujících vybranou školu, se poté zabýváme tvorbou zmíněného návrhu. Dále se v práci nachází kapitola, věnovaná oblasti požadavků k provozování Active Directory. Zde uvádíme, co vše je pro implementaci navrženého řešení potřeba zajistit.

Po teoreticky orientovaných kapitolách je v práci zařazena kapitola, kterou považujeme za praktickou. Ta se zabývá praktickou realizací dříve vytvořeného návrhu. Jsou zde přesně popsány jednotlivé kroky, vedoucí k jeho úspěšné implementaci do datové sítě školy. V této kapitole lze rovněž nalézt informace o konkrétních možnostech využití navrženého řešení za účelem optimalizace služeb datové sítě.

Poslední kapitolu práce považujeme spíše za doplňkovou. V ní se zabýváme open source alternativami Active Directory, protože se domníváme, že jejich použití může být pro některé školy výhodnou volbou.

1 Charakteristika technologie Microsoft Active Directory

Tématem této práce je optimalizace služeb datové sítě postavené na technologii Active Directory. Domníváme se však, že je nejprve důležité charakterizovat, co se pod pojmem Active Directory (dále jen AD) skrývá, pochopit, jak tato technologie souvisí s datovou sítí a její optimalizací a rovněž vymezit základní terminologii, která se souvislosti s AD používá a jejíž znalost je pro pochopení principů technologie AD důležitá. Teprve poté se můžeme zabývat tvorbou návrhu vhodné struktury AD pro vybranou školskou instituci s cílem optimalizovat služby poskytované její datovou sítí. Nejprve tedy uvedeme stručnou definici AD jednoho z uznávaných autorů odborné IT literatury, kterou si pro potřeby naší práce rozvedeme.

„Active Directory je adresářová služba obsažená v systému Windows Server. Active Directory zahrnuje adresář, v němž jsou uloženy informace o vašich distribuovaných prostředcích, stejně jako o službách, díky nimž jsou tyto informace užitečné a dostupné.“ (Stanek, 2009, s. 23)

AD je tedy služba, která eviduje informace o distribuovaných prostředcích datové sítě. Zde je ovšem potřeba uvedenou definici doplnit, protože v AD jsou mimo distribuované prostředky evidováni rovněž uživatelé a informace o nich. Distribuované prostředky a uživatelé datové sítě bývají v souvislosti s AD zařazovány do tzv. **objektů**, kterým níže věnujeme samostatnou kapitolu. Informace o nich, tedy jejich vlastnosti, označujeme jako **atributy.** Celá tato evidence objektů je uložena v takzvaném **adresáři**. To potvrzuje například Štěrba ve své definici adresáře, podle níž je adresář *„databáze, v níž jsou uloženy všechny informace o objektech sítě.“* (Štěrba, 2014, s. 16)

Dále je pro účely pochopení AD a pozdějšího návrhu struktury AD nutné uvést pojem **řadič domény**. Řadiče domény jsou servery, na kterých je uložen adresář a které tedy tvoří jakési základní kameny AD. Těmito servery se budeme více zabývat později, v samostatné kapitole.

Pochopení služby AD jako ústřední služby, evidující informace o objektech v datové síti je velmi důležité pro pochopení její využitelnosti pro naše účely, protože z této charakteristické vlastnosti vycházejí prakticky veškeré její další funkce. Z těchto funkcí považujeme za vhodné uvést, že služba AD plní významnou funkci bezpečnostní, a to z toho důvodu, že se vůči ní ověřují objekty datové sítě. V nástrojích služby AD máme možnost určit způsoby tohoto ověřování a dále pak můžeme na základě ověření objektů definovat oprávnění uživatelů a počítačů, například ohledně přístupu k různým sdíleným prostředkům, či možnosti měnit

různá nastavení. Za velkou výhodu služby AD považujeme fakt, že nám dává možnost definovat tato oprávnění na jednom místě, což činí správu datové sítě centralizovanou a přehlednou. To usnadňuje práci administrátora, což ve svém díle rovněž uvádí Stanek (2009, s. 24). Dále je v AD možné seskupovat objekty a poté pracovat s těmito skupinami, což nám dává možnost efektivní správy objektů datové sítě.

Poslední, avšak neméně důležitou množinou pojmů, které se v souvislosti AD používají, jsou názvy protokolů, kterých AD využívá ke své funkci. Z těchto protokolů považujeme za důležitý aplikační protokol **LDAP 3** (Lightweight Directory Access Protocol 3), který poskytuje přenos dat ve standardizovaném formátu a jejich kódování (Štěrba, 2014, s. 17). Dalším důležitým protokolem, který zajišťuje funkčnost AD, je protokol **Kerberos 5**, využívaný autentizačními a autorizačními službami k ochraně dat a při maximalizaci flexibility (Stanek, 2009, s. 24).

V této kapitole jsme tedy krátce definovali technologii AD, popsali její funkci uvnitř datové sítě a možnosti, které nám v datové síti nabízí, a rovněž uvedli základní pojmy, které se v souvislosti s AD používají. Z výše uvedených informací lze do značné míry vyvodit, jakým způsobem můžeme tuto službu využít k zefektivnění správy školní datové sítě a k optimalizaci jejích služeb. Z hlediska zefektivnění správy datové sítě považujeme za klíčovou pečlivě vedenou evidenci o objektech datové sítě, obsahující jejich atributy, tedy například jejich název, typ, umístění, funkce a jméno vlastníka. Důležitým faktem z hlediska efektivity správy je dále to, že v AD můžeme na základě této evidence zmíněné objekty vhodně seskupovat a pracovat poté s díky vytvořeným skupinám s objekty hromadně, což může dle našeho názoru administrátorovi školní datové sítě velmi usnadnit práci. Tímto seskupováním se bude zabývat náš pozdější návrh struktury AD. V souvislosti s optimalizací služeb datové sítě jsou pro nás důležité možnosti nastavení autentizace objektů vůči AD a rovněž řízení přístupů ke sdíleným prostředkům (sdílené adresáře, přístupy k aplikacím na serveru, k tiskárnám, apod.), protože těmito nastaveními můžeme zamezit neoprávněnému přístupu k prostředkům datové sítě a rovněž zajistit jejich optimální vytížení.

Nyní jsme tedy ze získaných informací vyvodili možnosti, které nám služba AD nabízí k zefektivnění správy datové sítě a k optimalizaci jejích služeb a máme tedy základní představu o tom, čím se bude zabývat náš pozdější návrh. Domníváme se, že nyní již můžeme přejít k dalšímu důležitému tématu, které s AD souvisí, a tím jsou řadiče domény.

2 Řadiče domény

K porozumění AD a tedy i k pozdější tvorbě optimálního návrhu struktury AD potřebujeme hlouběji porozumět rovněž řadičům domény (domain controller – dále jen DC) a základním principům jejich funkce. DC jsou, jak jsme již dříve zmínili, servery, na kterých je uložen adresář. Jakožto nositelé adresáře jsou to rovněž servery, vůči kterým se objekty datové sítě ověřují. S tohoto faktu můžeme vyvodit, že na efektivitu funkce a správy datové sítě má zásadní vliv jejich rozmístění. Pokud by se například některé objekty ověřovaly vůči vzdálenému DC, se kterým by byly spojeny síťovým připojením s příliš nízkou propustností, znamenalo by to značná omezení při využívání služeb datové sítě.

Z hlediska porozumění principům funkce AD pokládáme za důležitou informací také to, že DC nemají žádnou hierarchii – nerozlišujeme nadřazené a podřazené DC. Systém Windows Server využívá model **replikace multimaster** a proto mohou být změny adresáře zpracovány jakýmkoliv DC. DC, na kterém byly provedeny změny, nové údaje replikuje na ostatní DC. Administrativu datové sítě tedy můžeme provádět na libovolném DC. Důležitost tohoto faktu nejvíce doceníme ve čtvrté kapitole, která se zabývá strukturami AD.

V této stručné kapitole jsme uvedli základní informace o DC, popsali základní principy jejich funkce a rovněž objasnili jejich význam v rámci datové sítě a důležitost jejich správného rozmístění. Nyní uvedeme další stručnou kapitolu, jejímž tématem jsou objekty, jejichž znalost má dle našeho názoru z hlediska pochopení a následného návrhu struktury AD zásadní význam.

3 Objekty

Jednou z oblastí, které je již na začátku naší práce potřeba rozvést, je oblast objektů, protože se s nimi budeme v celé této práci setkávat. Objekty jsou prostředky, jež v AD spravujeme. Rozdělujeme je na **koncové objekty stromové struktury** (které bývají někdy označovány jako listy – uživatelé, počítače apod.) a **objekty kontejneru** (často zkráceně označovány jako kontejnery – doména, organizační jednotka, apod.). Kontejnery jsou specifické tím, že mohou, na rozdíl od koncových objektů, obsahovat další objekty.

Dále považujeme za důležité uvést, že jsou objekty v AD rozděleny do takzvaných **tříd** se specifickými možnostmi využití a specifickými vlastnostmi. Tyto třídy jsou **uživatel, počítač, tiskárna** a **skupina**. Vlastnostem objektů se, jak jsme již dříve uvedli, v AD říká atributy.

Jak tedy vidíme, objekty lze v AD dělit dle různých kritérií a vlastností. To nám umožňuje jejich snadné třídění a procházení. Za nejdůležitější z informací, které v této kapitole uvádíme, však pokládáme, že existují kontejnery, které mohou seskupovat objekty. Z této informace můžeme vyvodit, že nám AD dává možnost vytvořit hierarchickou strukturu kontejnerů a do této struktury následně třídit koncové objekty, čímž lze učinit jejich evidenci a rovněž správu přehlednější. Využitím kontejnerů k seskupování objektů se budeme podrobně zabývat v navazující kapitole, věnující se strukturám AD, a to konkrétněji v podkapitole 4.2, věnující se tzv. logické struktuře v AD, jíž jsou kontejnery součástí.

4 Struktury v Active Directory

Nyní jsme již ve fázi, kdy jsme pronikli do základních principů AD a rovněž rozvedli obsah základních pojmů, které se v souvislosti s AD používají. Tyto znalosti považujeme za nezbytné k pochopení tématu, kterým se budeme nyní zabývat a které přímo souvisí s tvorbou našeho návrhu, a tím jsou struktury v AD.

Hned na začátku této kapitoly považujeme za vhodné uvést fakt, že služba AD rozlišuje **fyzickou** a **logickou** strukturu datové sítě. To má hned několik výhod, jak ve své práci uvádí rovněž Klement (2015, s. 42), který tyto výhody spatřuje v tom, že máme možnost navrhovat a udržovat fyzické a logické struktury nezávisle na sobě a rovněž v tom, že při vytváření oborů názvů domény nejsme závislí na struktuře fyzické sítě. Zmíněné rozlišování fyzické a logické struktury datové sítě dále dle Klementa (2015, s. 42) přináší výhody při zavádění DC. V souvislosti s rozlišovanými strukturami je důležité uvést fakt, že AD v adresáři pracuje s logickou strukturou. To ve své práci uvádí rovněž Stanek (2009, s. 34), který tento fakt odůvodňuje tím, že běžný obor názvů AD neobsahuje součásti fyzické struktury.

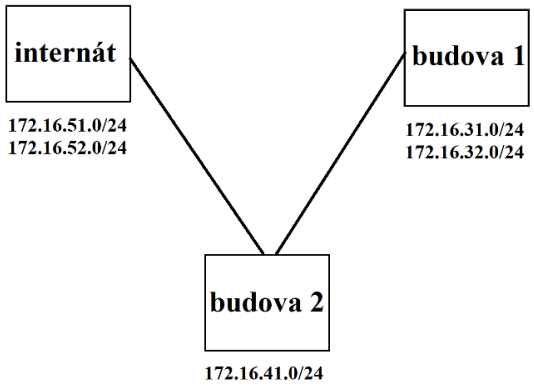
Domníváme se, že jsme nyní zmínili důležité základní informace o strukturách, které AD rozlišuje, a rovněž uvedli základní výhody tohoto rozlišování. Z informace zmíněné na konci předchozího odstavce lze vyvodit, že je pro naše potřeby důležité pochopit zejména strukturu logickou. Dle našeho názoru je však vhodné uvést alespoň základní informace o fyzické struktuře v AD a základní pojmy, které se ve spojitosti s touto strukturou používají, protože i tyto znalosti jsou při práci s AD mnohdy důležité.

4.1 Fyzická struktura v AD

V této podkapitole se budeme pohybovat na samotné hranici tématu práce, protože se budeme zabývat nejen reprezentací fyzické struktury v AD, ale rovněž fyzickou strukturou datové sítě samotnou, ze které její reprezentace v AD vychází. Pokládáme však za důležité se s touto oblastí krátce seznámit, protože i těchto znalostí budeme v dalších kapitolách práce využívat. Fyzická struktura v AD vychází, jak už bylo zmíněno, z fyzické struktury datové sítě. Je rozdělena do **sítí** (někdy označováno jako lokality) a **podsítí**. Síť může obsahovat jednu či více podsítí. Z hlediska kvality služeb datové sítě je velmi důležité, aby byly podsítě spolehlivě propojeny. Pro úplnost ještě považujeme za vhodné uvést jednoduchou definici podsítí. Podsítě jsou skupiny IP adres přesně určeného rozsahu, jejichž název je dán IP adresou sítě a bitovou maskou, například 172.16.33.0/24.

Fyzická struktura AD bývá v praxi vytvářena tak, že kopíruje fyzickou strukturu datové sítě. Domníváme se, že se v případě většiny škol nesetkáme s tím, že by působily ve více městech a proto budou v rámci fyzické struktury datové sítě školy pravděpodobně existovat separátní sítě zejména pro jednotlivé budovy školy, či pro jejich části. Tuto strukturu tedy bude fyzická struktura v AD kopírovat.

Pro lepší pochopení tématu fyzických struktur zde nabízíme příklad. Ten je tematicky záměrně orientován na školu.



Obrázek 1: Fyzická struktura v AD

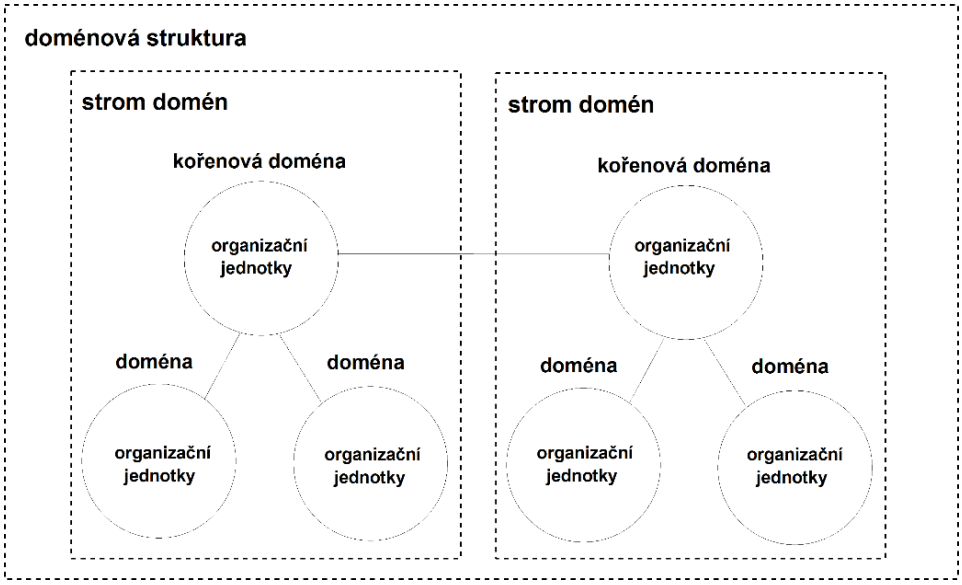
Na obrázku 1 vidíme fyzickou strukturu školy, která obsahuje tří sítě. Síť budovy 2 obsahuje jednu podsíť. Zbylé sítě mají podsítě dvě.

V souvislosti s fyzickou strukturou v AD považujeme za zajímavé doporučení, které někteří autoři, jako například Stanek (2009, s. 34) ve svých publikacích poskytují, a to, že do jednotlivých sítí (lokalit) je výhodné umisťovat DC, z důvodu optimalizace ověřování a replikace. Domníváme se, že toto doporučení bylo poskytováno z důvodu mnohdy nízké propustnosti síťového propojení lokalit v době, kdy tito autoři své publikace vydali. V současné době, z důvodu rychlého vývoje v oblasti informačních technologií a souvisejícího vývoje datových sítí, již ono doporučení nepokládáme za tolik důležité.

Z informací, uvedených v této podkapitole můžeme vyvodit, že návrh fyzické struktury v AD nebude prioritou této práce. Fyzická struktura datové sítě, kterou fyzická struktura v AD kopíruje, bývá již z pravidla dána před implementací služby AD do datové sítě. K optimalizaci služeb datové sítě tedy využijeme strukturu logickou a návrhem této struktury se budeme později zabývat.

V tuto chvíli považujeme informace, uvedené o fyzické struktuře v AD za dostatečné, a proto můžeme přejít k podkapitole, věnující se struktuře logické. Znalosti, které v následující kapitole získáme, považujeme z hlediska pozdějšího návrhu za nezbytně nutné.

4.2 Logická struktura v AD



Obrázek 2: Logická struktura v AD

V této podkapitole se dostáváme k tématu, které s přihlédnutím k tématu práce, kterým je optimalizace služeb datové sítě, považujeme za velmi důležité, a tím je logická struktura v AD. Právě jejím návrhem se budeme, jak jsme již vyvodili v podkapitole 4.1, později zabývat. V této podkapitole si rozebereme obsah pojmu logická struktura, možnosti jejího využití a také to, jakých prvků můžeme využít při její tvorbě. Rovněž v této kapitole zvolíme prvky, vhodné pro potřeby pozdějšího návrhu logické struktury pro vybranou školu.

Fyzická struktura v AD nám neposkytuje dostatečné možnosti správy, protože v praxi často potřebujeme aplikovat určitá pravidla pro specifickou skupinu objektů, která je ne vždy dána jejich fyzickým umístěním. Pro tyto potřeby je vhodné využít strukturu logickou. Základním rozdílem logické struktury od struktury fyzické je skutečnost, že tato struktura nevychází z fyzické struktury datové sítě. Logickou strukturu v AD tvoří sám administrátor datové sítě na základě specifikací dané instituce. Může tak vytvořit skupiny objektů (kontejnery) na základě určitých kritérií a usnadnit si tak správu objektů datové sítě. Samotné skupiny bývají zpravidla uspořádány do vhodně vytvořené hierarchické struktury, která umožňuje snadnou orientaci v těchto skupinách. Tvorbou těchto struktur pro konkrétní školu se budeme zabývat v šesté kapitole této práce. Jakmile máme objekty seskupené v kontejnerech, můžeme na tyto objekty aplikovat určitá společná pravidla hromadně, a ušetřit tak mnoho času.

Z výše uvedených informací můžeme tedy vyvodit, že hlavním účelem logické struktury je zjednodušit administraci datové sítě a rovněž optimalizaci jejích služeb.

Pro lepší pochopení toho, jakým způsobem je možné logickou strukturu datové sítě využít považujeme za vhodné uvést konkrétní příklad. Tento příklad bude opět tematicky vztažen na školu. Řekněme, že velká střední škola, jejíž datová síť je postavená na technologii AD, má pouze jednoho správce sítě. Tento správce má však mnoho povinností a proto se rozhodne využít technologii AD k tomu, aby si usnadnil práci. Všem studentům, nezávisle na budově, ve které studují, nastaví vhodná oprávnění a nejrůznější restrikce znemožňující jim nežádoucí zásahy do konfigurace počítačů a přístup k sdíleným prostředkům, jejichž využívání studenty je nežádoucí. Vhodná oprávnění a vhodné restrikce rovněž nastaví všem zaměstnancům školy. Dále po dohodě s vedením školy deleguje administrátorská oprávnění k počítačům ve vybraných počítačových učebnách a rovněž k některým sdíleným prostředkům na škole na některého z učitelů IT, který tak může se správou zvolených zařízení pomáhat. Takovéto změny lze efektivně provádět pouze s využitím vhodně vytvořené logické struktury v AD. Jak je tedy z tohoto příkladu zřejmé, logická struktura v AD nám nabízí široké možnosti v oblasti administrace datové sítě a rovněž v oblasti optimalizace jejích služeb.

Výše jsme uvedli, čím se vyznačuje logická struktura v AD. Rovněž jsme nastínili možnosti jejího praktického využití. Z uvedeného textu je zřejmé, že existence vhodně vytvořené logické struktury usnadňuje správu datové sítě a rovněž poskytuje široké možnosti optimalizace jejích služeb. V tuto chvíli již považujeme za vhodné přejít ke konkrétním prvkům logické struktury, kterých lze využít při jejím návrhu.

4.2.1 Doména

Domény jsou základními prvky logické struktury datové sítě v AD, které obsahují účty objektů. Každá datová síť postavená na technologii AD musí mít minimálně jednu doménu. Podobné definice uvádí mnoho autorů. My zde jednu takovou uvedeme.

„Domény jsou logickými seskupeními objektů, které sdílí společné databáze služby Active Directory. V adresáři jsou domény reprezentovány jakožto objekty kontejneru.“ (Stanek, 2009, s. 35)

Doména je tedy objektem adresáře a rovněž nadřazeným objektem k objektům, které obsahuje. V síti, ve které je vytvořena (v privátní síti, či v internetu) musí mít unikátní název.

Tímto jsme krátce vymezili obsah pojmu doména. Mnozí autoři se ve svých dílech zabývají jejím popisem podrobněji a poskytují například vymezení jejích komponent, jako to můžeme vidět v díle bratří Allenů (2005, s. 33). Pro naše potřeby však pokládáme uvedené vymezení za dostatečné.

S přihlédnutím k tématu této práce považujeme už nyní za důležité nastínit praktické využití domén. Veškeré objekty uvnitř domény se vůči doméně ověřují. Díky existenci tohoto ověřování může administrátor objektům v datové síti nastavovat různá pravidla, která poté bývají na základě zmíněného ověřování vynucována. Objektům v doméně takto může nastavovat například přístupová práva k různým sdíleným prostředkům, či nejrůznější restrikce, přispívající k optimalizaci služeb datové sítě.

Z hlediska pozdějšího návrhu považujeme dále za důležité uvést, že každá doména musí obsahovat minimálně jeden DC. V běžné praxi se však většinou setkáváme s doménami, které obsahují více DC. Díky tomu je v případě poruchy jednoho z DC zachována funkčnost domény. Dále je potřeba uvést, že jeden DC nemůže hostovat více než jednu doménu.

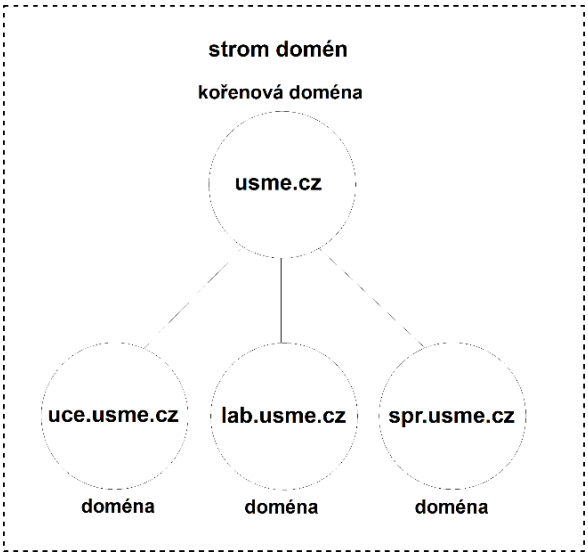
Z výše uvedeného je tedy zřejmé, že náš návrh logické struktury datové sítě bude muset obsahovat minimálně jednu doménu. Dále lze z textu této podkapitoly vyvodit, že domény mají velký význam z hlediska optimalizace služeb datové sítě a z tohoto důvodu je považujeme za důležité. Nyní jsme již dle našeho názoru dostatečně pronikli do obsahu pojmu doména, a proto můžeme přistoupit k těm součástem logické struktury v AD, které jsou doménami tvořeny.

4.2.2 Strom domén

Strom domén je seskupení souvisejících domén. Zde si rovněž uvedeme jednu z možných definic. Podle Allenů (2005, s. 33) je to *„řada domén, spojených dohromady hierarchicky, přičemž všechny používají souvislé jmenné schéma.“*

V souvislosti se stromem domén považujeme za vhodné uvést pojem **kořenová doména**. Jde o první doménu, která byla v adresáři vytvořena. Tato doména je v hierarchické struktuře nadřazena ostatním doménám. Jak již víme z výše uvedené definice, domény stromu domén používají souvislé jmenné schéma. Z tohoto důvodu názvy všech podřazených domén obsahují název kořenové domény. K tomuto názvu se z levé strany připojuje textový řetězec, který identifikuje podřazenou doménu. Ten je od názvu kořenové domény oddělen tečkou.

Pro lepší pochopení zmíněného jmenného schématu uvedeme příklad. Vytvoříme strom domén pro velkou, fiktivní vysokou školu – Univerzitu Smetany. Kořenová doména ponese název usme.cz. Tato doména bude mít podřazené domény pro učebny, laboratoře a správní obor. Dle principu souvislého jmenného schématu, který stromy domén v AD používají, můžeme těmto doménám dát názvy: uce.usme.cz, lab.usme.cz a spr.usme.cz. Vidíme tedy, že každá podřazená doména má ve svém názvu název kořenové domény.



Obrázek 3: Strom domén

Nyní jsme tedy pronikli do obsahu pojmu strom domén a rovněž jsme uvedli základní principy, které se ve stromech domén používají. Z hlediska našeho pozdějšího návrhu považujeme nyní za nutné připomenout informace, které jsme uvedli v podkapitole 4.2.1, věnované doménám, a to že každá doména musí obsahovat minimálně jeden DC a že jeden DC nemůže hostovat více než jednu doménu. Z toho odvozujeme, že pokud by náš návrh obsahoval strom domén, bylo by potřeba mít více DC než v případě použití pouze jedné domény, což by negativním způsobem ovlivnilo cenu a prostorovou náročnost tohoto řešení, nemluvě o negativním vlivu na časovou náročnost správy datové sítě. Na základě těchto skutečností se domníváme, že bude pro účely našeho pozdějšího návrhu logické struktury nejvýhodnější použít pouze jednu doménu. Použití jedné domény považujeme za vhodné řešení pro většinu běžných škol.

Přestože jsme z dříve získaných informací vyvodili, že bude pro účely pozdějšího návrhu logické struktury nejvýhodnější využít pouze jednu doménu, jsme toho názoru, že je pro úplnost této podkapitoly, věnované logické struktuře v AD, potřeba uvést rovněž základní informace o doménových strukturách. Doménovým strukturám se tedy budeme nyní věnovat.

4.2.3 Doménové struktury

Doménové struktury (také často označovány jako lesy) jsou, jak rovněž uvádí Price (2005, s. 23), nejvyšším kontejnerem AD. Jde o seskupení souvisejících stromů domén. Tyto stromy jsou do značné míry nezávislé. Je však potřeba zdůraznit, že nejsou nezávislé úplně. Jak uvádí Allenovi (2005, s. 34), mezi všemi stromy doménové struktury existuje vzájemná důvěra (tzv. trust lesa).

Doménové struktury mají, stejně jako stromy domén, svou kořenovou doménu. Jde o doménu, která byla v doménové struktuře vytvořena nejdříve. Podle této domény je doménová struktura vždy pojmenována. V souvislosti s kořenovou doménou doménové struktury však považujeme za důležité uvést, že doménová struktura nepoužívá v případě názvů stromů domén, které obsahuje, souvislé jmenné schéma. Souvislé jmenné schéma používají pouze jednotlivé stromy domén, nacházející se uvnitř doménové struktury, a to v souvislosti s doménami, které obsahují. Tento princip jsme vysvětlili v předchozí podkapitole 4.2.2.

V souvislosti s doménovými strukturami považujeme za důležité zmínit důležitý pojem, kterým je **globální katalog**, protože jde o jeden z pojmů, se kterým se v souvislosti s AD běžně setkáváme. Uvedeme si zde jeho definici, kterou uvádí jeden z významných autorů odborné IT literatury.

„Globální katalog je řadič domény, který hostuje objekty ze všech názvových kontextů domén v celé doménové struktuře.“ (Price, 2005, s. 26-27)

Globální katalog tedy obsahuje záznam každého z objektů doménové struktury. Záznamy ovšem z důvodu optimalizace obsahují jen některé atributy objektů. Server globálního katalogu je nutnou součástí všech doménových struktur, protože nám poskytuje možnost vyhledávání objektů v rámci doménové struktury. Pokud vyhledáváme objekt uvnitř doménové struktury, je nutné nejprve učinit dotaz na server globálního katalogu, abychom zjistili, ve které doméně se objekt nachází.

Domníváme se, že jsme nyní uvedli dostatek informací o doménových strukturách. S přihlédnutím k potřebám našeho návrhu můžeme konstatovat, že doménovou strukturu zcela jistě nevyužijeme. Doménová struktura má své využití v datových sítích velkých korporací, disponujících rozsáhlou datovou síti, které rovněž mají velký tým IT specialistů, nutný pro správu takové sítě. Pro naše potřeby však považujeme využití doménové struktury,

ze stejných důvodů, jež jsme uvedli v podkapitole 4.2.2 v případě stromům domény, za nevýhodné.

Do této chvíle jsme se v kapitole věnované logické struktuře AD věnovali doménám, a kontejnerům, které jsou doménami tvořeny. Nyní se zaměříme prvky, které lze využít k seskupování objektů uvnitř domény. Toto seskupování považujeme pro náš pozdější návrh logické struktury datové sítě za velmi důležité.

4.2.4 Organizační jednotky

Organizační jednotky (organizational units, dále jen OU) jsou kontejnery uvnitř domény, do kterých můžeme zařazovat objekty v doméně. Používají se k seskupování objektů s cílem zpřehlednění a zefektivnění jejich správy. Dle Allenů (2005, s. 31) se jedná o nejčastěji využívaný typ kontejneru.

S těmito skupinami objektů poté můžeme dále pracovat. Můžeme nastavovat různá pravidla, společná pro všechny objekty dané OU najednou, jejich aplikací na celou OU. Tímto se budeme zabývat v osmé kapitole, konkrétně v její podkapitole 8.7, která se zabývá skupinovou politikou. Dále můžeme například určit množinu uživatelů, kteří mají právo spravovat objekty dané OU. Rovněž považujeme za důležité zmínit, že máme možnost vytvářet OU uvnitř OU a vytvořit tak hierarchickou strukturu.

Běžně se OU používají tak, aby kopírovaly strukturu společnosti (ať už geografickou, či v rámci útvarů). V takovém případě dávají možnost efektivní delegace administrátorských oprávnění, jak ve svém díle nepřímo sděluje Stanek (2009, s. 40). V organizaci, ve které využíváme OU, můžeme tedy jednoduše mít více administrátorů, z nichž každému přidělíme určité pravomoci. Tyto pravomoci poté můžeme, na základě aktuální potřeby, jednoduše měnit (správcům můžeme jednotlivá oprávnění k OU jednoduše přidávat i odebírat). Dále nám struktura OU kopírující strukturu společnosti dává možnost hromadně nastavovat pravidla skupinám objektů, které spolu souvisejí.

Již nyní usuzujeme, že OU budou mít pro náš pozdější návrh logické struktury zásadní význam. Dávají nám možnost seskupovat objekty bez nutnosti zavádění dalších DC, tedy bez dalších investic a umožňují nám poté s vytvořenými skupinami objektů efektivně pracovat. Možnosti, které nám OU poskytují, vedou k zefektivnění správy datové sítě a nabízejí značné možnosti, kterých lze využít při optimalizaci jejích služeb. Je tedy zřejmé, že budou důležitými prvky našeho návrhu logické struktury datové sítě.

V souvislosti se seskupováním objektů považujeme za vhodné rozvést ještě jeden pojem, týkající se logické struktury v AD, a tím je pojem skupina.

4.2.5 Skupiny

Jak rovněž uvádí Štěrba (2014, s. 50), použití vhodné struktury skupin může zefektivnit správu celé datové sítě. Skupiny v AD slouží k seskupování objektů, které mohou být umístěny jak ve stejné OU, tak v různých OU. S těmito skupinami se dá poté dále pracovat. Můžeme jim nastavovat různá pravidla, jako jsou například přístupová práva k různým sdíleným prostředkům. Skupiny mohou obsahovat nejen objekty, ale i další skupiny a díky tomu lze vytvářet jejich hierarchické struktury, podobně jako tomu bylo v případě OU.

Na základě uvedených informací pokládáme skupiny za další z užitečných prostředků, které lze využít k zefektivnění správy datové sítě a rovněž k optimalizaci jejích služeb. V případě našeho návrhu považujeme za ideální jejich využití v kombinaci s OU, a to v případech kdy potřebujeme vytvořit takové skupiny objektů, které nejsou vytvořeny na úrovni OU.

4.3 Závěr

Touto podkapitolou jsme uzavřeli část věnovanou strukturám v AD, ve které jsme dle našeho názoru získali mnoho cenných informací, a to nejen pro náš pozdější návrh, ale rovněž pro pochopení služby AD a jejích principů obecně. Vyvodili jsme, že se při tvorbě struktury datové sítě v AD budeme zabývat tvorbou logické struktury, a to s využitím domény a OU. Rovněž můžeme ve specifických případech vhodně využít skupin.

Domníváme se, že je nyní vhodné přejít k tématu, které nám pomůže prohloubit naše porozumění technologii AD a rovněž poznat další možnosti, které nám tato technologie nabízí k optimalizaci služeb datové sítě, a tím je vývoj AD.

5 Vývoj Active Directory

Vývoj AD, je dle našeho názoru velmi obsáhlým tématem, na které by si zasloužilo samostatnou publikaci. My se zde zaměříme zejména na informace, které jsou důležité s přihlédnutím k tématu a k cílům práce, tedy informace spojené s optimalizací služeb datové sítě a rovněž využitelné při návrhu logické struktury školní datové sítě a jeho následné realizaci. Nejprve si však uvedeme některá obecná fakta.

Služba AD je podporována všemi operačními systémy Microsoft Windows Server od verze 2000. Je ovšem potřeba zmínit, že předchůdce této služby - Windows NT NOS se objevil již v roce 1990 s příchodem operačního systému Windows NT 3.0. Ten kombinoval funkce protokolů z LAN Manageru a operačního systému OS/2. Měl však řadu nedostatků, jako například jednoduché domény s počtem objektů, omezeným přibližně na 40 000 a s omezenými možnostmi delegování administrace (Allen, 2005, s. 22).

S každou verzí operačního systému Microsoft Windows Server se služba AD vyvíjela a dále vyvíjí. Z tohoto důvodu nabízí stále více využitelných funkcí. Z hlediska pozdější využitelnosti informací považujeme za nejvhodnější tento vývoj prezentovat na tzv. **úrovních funkčnosti domény**. Rovněž se v této kapitole stručně zmíníme i o tzv. **úrovních funkčnosti doménové struktury**, které však již nejsou s přihlédnutím k cílům této práce natolik důležité. Získané znalosti využijeme zejména k volbě vhodné úrovně funkčnosti domény, kterou využijeme při praktické realizaci návrhu logické struktury datové sítě v osmé kapitole práce a rovněž k volbě operačního systému, kterým později vybavíme DC.

5.1 Úrovně funkčnosti domény

Jak rovněž uvádí Price (2005, s. 33), každá vyšší úroveň funkčnosti domény přináší nové funkce. Úroveň funkčnosti domény tedy přímo určuje, které funkce AD máme k dispozici. Volíme ji již při instalaci prvního DC a dodatečně je možné pouze její zvýšení. Pro úplnost považujeme za vhodné zmínit, že domény v doménové struktuře mohou mít různé úrovně funkčnosti.

V současné době existuje celkem osm úrovní funkčnosti domény, z nichž každá umožňuje používat pouze DC s vybranými verzemi operačního systému. Tyto úrovně si zde vypíšeme, uvedeme funkce, které daná úroveň oproti úrovni předchozí nově nabízí, a rovněž to, kterými verzemi operačního systému je možné DC při jednotlivých úrovních funkčnosti domény vybavit. V případě každé z úrovní dále zhodnotíme přínos nových funkcí z hlediska pozdějšího

návrhu. Na základě získaných informací dále v této podkapitole vybereme úroveň funkčnosti vhodnou pro realizaci návrhu logické struktury a operační systém, kterým vybavíme naše DC. Přehled úrovní funkčnosti a jejich funkcí, který nám poslouží jako podklad pro většinu podkapitol této podkapitoly, byl nalezen na webu TechNet (Microsoft, 2014).

5.1.1 Windows 2000 mixed

Tato úroveň nabízí základní funkce služby AD a v operačním systému Windows Server 2003 byla nastavena jako výchozí. K těmto funkcím jsou s každou vyšší úrovní funkčnosti přidávány funkce nové. Ve své době šlo o poměrně efektivní a využitelné řešení.

Podporované operační systémy pro DC: Windows NT 4 (pro záložní DC), Windows 2000 Server, Windows Server 2003

V dnešní době považujeme tuto úroveň funkčnosti za nevýhodnou, a to zejména s přihlédnutím k operačním systémům, využitelným pro DC, které již nejsou v prodeji a rovněž nejsou ze strany společnosti Microsoft dále podporovány.

5.1.2 Windows 2000 native

V případě úrovně Windows 2000 native máme nově možnost vytvářet univerzální skupiny, převádět typy skupin (convention a distribution groups), vnořovat skupiny a můžeme také provádět migraci objektů zabezpečení.

Podporované operační systémy pro DC: Windows 2000 Server, Windows Server 2003, Windows Server 2008, Windows Server 2008 R2

Funkce, které tato úroveň funkčnosti nově přináší, považujeme za užitečné. Nové funkce nám poskytují zejména větší volnost při tvorbě skupin a při práci s nimi, díky čemuž můžeme učinit správu datové sítě efektivnější. Nevýhodou však je, podobně jako v případě předchozí úrovně, že lze pro DC využít pouze starších verzí operačního systému Windows Server.

5.1.3 Windows Server 2003

Při této úrovni funkčnosti domény může administrátor datové sítě využít několik nových funkcí, včetně snadného přejmenování DC, omezeného delegování, ukládání zásad autentizace a možnosti přesměrování kontejnerů Users a Computers. Zde považujeme za vhodné osvětlit poslední ze zmíněných funkcí. Ve výchozím nastavení AD máme k dispozici pouze dva známé kontejnery, a to Users a Computers. Možností přesměrování kontejnerů Users a Computers

je myšleno to, že máme možnost definovat nová známá umístění pro účty uživatelů a počítačů, do kterých poté můžeme tyto účty ukládat.

Podporované operační systémy pro DC: Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2

Nové funkce této úrovně nám opět dávají možnost efektivnější právy datové sítě. Za nejdůležitější z funkcí považujeme možnost přesměrování kontejnerů Users a Computers, která je z hlediska návrhu logické struktury datové sítě velmi důležitá. Další ze zmíněných funkcí přinášejí nové možnosti, kterých lze využít pro účely administrace datové sítě a s tím související optimalizace jejích služeb. Dále můžeme z uvedených informací říci, že tato úroveň funkčnosti umožňuje vybavit DC operačním systémem Windows Server 2012 R2, který má být, dle informací z webových stránek společnosti Microsoft (2018) podporován až do listopadu roku 2023, což považujeme za výhodu této úrovně oproti úrovním předchozím. V současnosti nejnovější verzi, Windows Server 2016, však tato úroveň funkčnosti nepodporuje.

5.1.4 Windows Server 2008

Úroveň funkčnosti Windows Server 2008 přináší možnost nastavení podrobných zásad pro hesla. To umožňuje administrátorovi mimo jiné nastavit pravidla pro uzamykání účtů a rovněž pravidla pro uzamykání hesel uživatelů a globálních skupin zabezpečení. Z dalších funkcí, které tato úroveň funkčnosti přináší, můžeme zmínit podporu standardizovaného šifrovacího algoritmu Advanced Encryption Standard, což má pozitivní vliv na bezpečnost komunikace v rámci datové sítě.

Podporované operační systémy pro DC: Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016

Z uvedených informací lze vyvodit, že se nové funkce úrovně funkčnosti Windows Server 2008 týkají zejména zabezpečení datové sítě. Z těchto funkcí považujeme pro účely optimalizace služeb datové sítě za důležitou zejména možnost nastavení podrobných zásad pro hesla. Domníváme se, že pokud administrátor tyto zásady nastaví správně, může do značné míry zvýšit úroveň bezpečnosti datové sítě a optimalizovat tak služby, které tato síť poskytuje. Z hlediska samotného návrhu logické struktury datové sítě však nepovažujeme nové funkce, které tato úroveň funkčnosti přináší, za příliš důležité. Výhodou této úrovně oproti úrovním

předchozím je podpora v současnosti nejnovější verze operačního systému Windows Server, kterou je verze Windows Server 2016.

5.1.5 Windows Server 2008 R2

Tato úroveň funkčnosti přidává mimo jiné funkci záruky ověřovacího mechanizmu, (autentication mechanism assurance), která ukládá informaci o metodě autentizace doménového uživatele (užití čipové karty, uživatelského jména a hesla, apod.) do všech tokenů protokolu Kerberos daného uživatele. Tato informace může být použita pro určení autorizace v aplikacích, které toto podporují. Další z nových funkcí, které úroveň funkčnosti Windows Server 2008 R2 přináší, již nepovažujeme s přihlédnutím k cílům této práce za příliš důležité.

Podporované operační systémy pro DC: Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016

Úroveň Windows Server 2008 R2 dle našeho názoru neposkytuje žádné nové funkce, které by zásadním způsobem přispívali k zefektivnění správy datové sítě, a tedy ovlivňovali náš pozdější návrh logické struktury datové sítě. Zmíněná funkce záruky ověřovacího mechanizmu však může být užitečná, pokud škola využívá aplikace, které tuto funkci podporují, protože může uživateli usnadnit využívání služeb datové sítě (uživatel nemusí zadávat přihlašovací údaje pro přístup zmíněných aplikací). Za určitých okolností tedy může být využití této úrovně funkčnosti, v porovnání s úrovní předchozí, z hlediska optimalizace služeb datové sítě výhodnější.

5.1.6 Windows Server 2012

Úroveň funkčnosti Windows Server 2012 přidává zejména podporu služby key distribution center (dále jen KDC), složenou autentizaci a obrňování Kerberosu. Zde považujeme za nutné vysvětlit, co je pojmem KDC myšleno. KDC je služba, která slouží ke snížení rizik spojených s vyměňováním klíčů. KDC bezpečně distribuuje klíče konkrétním uživatelům, kteří je poté mohou používat za účelem přístupu k různým prostředkům.

Podporované operační systémy pro DC: Windows Server 2012, Windows Server 2012 R2, Windows Server 2016

Domníváme se, že tato úroveň funkčnosti rovněž neposkytuje žádné nové funkce, které by v souvislosti s pozdějším návrhem logické struktury datové sítě měly zásadní význam. Zmíněné funkce však přináší řadu vylepšení z hlediska zabezpečení datové sítě a přispívají tedy

k optimalizaci jejích služeb. S přihlédnutím k cílům práce tedy považujeme využití této úrovně funkčnosti za výhodnější, než využití úrovní předchozích.

5.1.7 Windows Server 2012 R2

Tato úroveň funkčnosti nově nabízí možnost nastavovat autentizační politiky na úrovni doménové struktury, které mohou být použity například pro určení, ze kterých zařízení se uživatel může přihlásit k datové síti. Přináší rovněž celou řadu různých bezpečnostní vylepšení, mimo jiné několik ochranných opatření ze strany DC pro skupinu Chránění uživatelé (Protected Users), která pro členy této skupiny znamenají jistá omezení.

Podporované operační systémy pro DC: Windows Server 2012 R2, Windows Server 2016

Stejně jako v případě tří předchozích úrovní se domníváme, že úroveň funkčnosti domény Windows Server 2012 R2 nepřináší žádné nové funkce, které by byly vzhledem k pozdějšímu návrh logické struktury datové sítě důležité. Díky novým bezpečnostním vylepšením, která tato úroveň poskytuje, však považujeme její využití za výhodnější, než využití některé z předchozích úrovní.

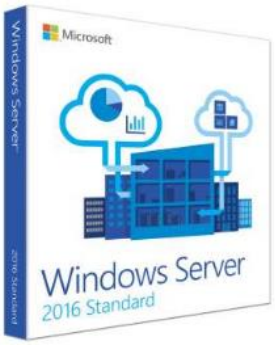
5.1.8 Windows Server 2016

Zatím nejvyšší úroveň funkčnosti přináší dle našeho názoru zejména vylepšení spojené s bezpečností. Tato vylepšení se týkají například ochrany přihlašovacích údajů a autentizace Kerberosu.

Podporované operační systémy pro DC: Windows Server 2016

Z doposud získaných informací usuzujeme, že je tato úroveň pro naše potřeby úrovní nejvýhodnější, přestože nepřináší žádné nové funkce, které by mohly ovlivnit náš pozdější návrh logické struktury datové sítě. Úroveň považujeme za nejvýhodnější zejména díky novým funkcím, zlepšujícím bezpečnost datové sítě. Pro praktickou realizaci našeho pozdějšího návrhu tedy volíme úroveň funkčnosti domény Windows Server 2016. Tato volba nám rovněž přímo určuje operační systém, kterým bude potřeba vybavit DC, protože zvolená úroveň funkčnosti v tuto chvíli podporuje pouze operační systém Windows Server 2016. Za výhodu použití tohoto operačního systému považujeme fakt, že jde v současnosti o nejnovější serverový operační systém společnosti Microsoft a z tohoto důvodu bude ze současné nabídky serverových operačních systémů tohoto výrobce podporován nejdéle. Podpora tohoto operačního systému

by dle informací, dostupných na webových stránkách společnosti Microsoft (2018), měla skončit v listopadu roku 2027.



Obrázek 4: Windows Server 2016 (Microsoft, 2017)

Domníváme se, že jsme se v této kapitole dostatečně seznámili s úrovněmi funkčnosti domény a rovněž s funkcemi, které jednotlivé úrovně nabízejí. Nyní tedy můžeme přejít k dalšímu tématu, kterým jsou úrovně funkčnosti doménové struktury.

5.2 Úrovně funkčnosti doménové struktury

Úrovně funkčnosti doménové struktury popisují funkce doménové struktury jako celku. Především se jedná o funkce, týkající se práce s celými doménami, vzájemných vztahů domén a jejich vzájemné komunikace. Těchto úrovní je opět několik a jsou nazývány analogicky k úrovním funkčnosti domény, tedy například Windows Server 2003, Windows Server 2008, apod.. Každá vyšší úroveň funkčnosti doménové struktury přináší, stejně jako tomu je v případě úrovní funkčnosti domény, nové funkce a nová vylepšení.

S přihlédnutím k faktu, který jsme vyvodili ve čtvrté kapitole práce, a to že v pozdějším návrhu logické struktury datové sítě pro vybranou školu doménovou strukturu nevyužijeme, považujeme výše uvedené informace o úrovních funkčnosti doménové struktury za dostatečné.

5.3 Závěr

V této kapitole jsme tedy na základě úrovní funkčnosti domény a jejich funkcí stručně popsali vývoj služby AD. Na základě zhodnocení přínosu nových funkcí, které každá z úrovní přináší, jsme vyvodili, že pro potřeby realizace našeho pozdějšího návrhu bude nejvýhodnější použít úroveň funkčnosti domény Windows Server 2016. Na základě této volby jsme dále stanovili, že při praktické realizaci návrhu budou DC vybaveny operačním systémem Windows Server 2016. Rovněž jsme pro úplnost uvedli základní informace o úrovních funkčnosti doménové

struktury, se kterými se při praktické realizaci našeho návrhu v osmé kapitole této práce okrajově setkáme.

Domníváme se, že jsme nyní ve fázi, kdy jsme již vytvořili dostatečný teoretický základ pro pochopení základních principů technologie AD a rovněž pro tvorbu návrhu logické struktury datové sítě. V další kapitole se tedy tvorbě tohoto návrhu věnovat.

6 Návrh logické struktury školní datové sítě

V této kapitole vytvoříme návrh logické struktury školní datové sítě. Jak jsme již zmínili v úvodu práce, půjde o návrh konkrétní struktury, určený pro vybranou školu. Nejprve tedy pokládáme za důležité tuto školu představit, a to zejména z hlediska uživatelů a zařízení, využívajících její datovou síť, a rovněž stanovit cíle, kterých chceme tvorbou a pozdější realizací návrhu, dosáhnout. Dále stanovíme základní princip návrhu, který využijeme při tvorbě samotných OU. Na základě těchto podkladů a informací, získaných v předchozích kapitolách, poté vytvoříme návrh logické struktury datové sítě. Při tvorbě návrhu také uvedeme, jakým způsobem jej lze přizpůsobit pro použití v jiných školách, majících rozdílnou strukturu. Rovněž se v této kapitole budeme zabývat stanovením jmenných konvencí, kterých využijeme pro pojmenování objektů naší datové sítě.

6.1 Vstupní údaje

6.1.1 Škola

Jakožto předloha pro realizaci tohoto návrhu nám poslouží **Základní škola Odry Komenského**. Autor práce si tuto školu zvolil, protože zde působí jako učitel angličtiny a informatiky a od příštího roku mu rovněž byla přislíbena pozice ICT koordinátora. V budoucnu by zde chtěl podobné řešení implementovat.

Nyní tedy uvedeme základní vstupní údaje, které poslouží jako podklad pro tvorbu našeho návrhu. Tyto údaje se týkají uživatelů a počítačů, coby základních objektů datové sítě. K tomuto účelu využijeme dvojici tabulek s popisem.

6.1.2 Uživatelé

V této části si uvedeme ty informace o budoucích uživatelích naší datové sítě, které považujeme za důležité jakožto podklad pro tvorbu OU našeho návrhu. Jakožto vhodné vyjádření těchto informací pokládáme níže uvedenou tabulku, udávající skupiny uživatelů, vytvořené na základě jejich pracovních pozic. Tato tabulka, vytvořená na základě informací, uvedených na webových stránkách Základní školy Odry Komenského (2018) a na základě autorových znalostí personálního uspořádání školy, obsahuje také počty uživatelů v jednotlivých skupinách. Pracovníci školy, kteří nemají potřebu využívat služeb školní datové sítě (například uklízečky či kuchařky) nejsou v tabulce zahrnuti.

Pracovní pozice:	Počet	Poznámka
Ředitel	1	
Zástupce ředitele	1	
Správní zaměstnanci	4	sekretářka, ekonomka, školník, projektový koordinátor
Pedagogičtí pracovníci - 1. stupeň	13	
Pedagogičtí pracovníci - 2. stupeň	22	
Speciální pedagogové	2	
Asistenti	11	asistenti pedagogů a školní asistenti
Školní psycholožka	1	
Pracovníci školní družiny	4	jeden je také asistentem (v celkovém počtu níže jsou tedy započítáni pouze tři pracovníci)
Pracovníci školní jídelny	2	vedoucí školní jídelny a referentka stravování
Žáci	450	počet žáků je přibližný
Uživatelů celkem (bez žáků)	**60**	

Tabulka 1: Uživatelé školní datové sítě

V tuto chvíli jsme uvedli důležité informace o uživatelích datové sítě školy. V další podkapitole uvedeme důležité informace o počítačích, které nám, stejně jako informace o uživatelích, poslouží jakožto podklad pro tvorbu OU našeho návrhu.

6.1.3 Počítače

Základní informace o počítačích školy pokládáme za další z důležitých podkladů pro tvorbu našeho návrhu. Počítače seskupíme dle jejich umístění a rovněž stručně uvedeme jejich využití. K tomu nám, stejně jako v předchozí podkapitole, poslouží přehledná tabulka. Tabulka byla vytvořena na základě autorovy vlastní evidence školní techniky, kterou, jakožto zaměstnanec školy, dříve pro jiné účely vytvořil.

Umístění	Počet	Využití
Vedení a správa školy	5	MS Office, ekonomický SW, tisk dokumentů, multimediální tvorba, internet
Sborovna 1 - nižší stupeň	1	MS Office, tisk dokumentů, internet
Sborovna 2 - vyšší stupeň	2	MS Office, tisk dokumentů, internet
PC učebna 1	11	MS Office, multimediální tvorba, programování, internet, **přímá činnost žáků**
PC učebna 2	12	MS Office, multimediální tvorba, programování, internet, **přímá činnost žáků**
Komunikační centrum	11	MS Office, multimediální tvorba, programování, internet, **přímá činnost žáků**
Třídy	18	Přehrávání videí, prezentace, interaktivní tabule, internet
Jídelna	2	MS Office, ekonomický SW, tisk dokumentů, internet
Školní družina	5	MS Office, multimediální tvorba, hry, internet, **přímá činnost žáků**
Spec. ped. a psycholožka	2	MS Office, tisk dokumentů, internet
Počítačů celkem:	**69**	

Tabulka 2: Počítače školní datové sítě

Kromě informací v tabulce považujeme za vhodné zmínit, že počítače disponují širokou škálou verzí operačního systému Microsoft Windows. Seskupováním počítačů na základě jejich operačních systémů se však budeme zabývat až později, a to na úrovni skupin.

Nyní jsme si uvedli všechny potřebné vstupní údaje, které využijeme při tvorbě OU našeho návrhu. Dále považujeme za vhodné stanovit cíle samotného návrhu a poté zvolit základní princip, na základě kterého budeme tvořit OU.

6.2 Stanovení cílů a základních principů návrhu

6.2.1 Stanovení cílů návrhu

Jak je již patrné z názvu práce, hlavním cílem návrhu je optimalizace služeb datové sítě. V úvodu jsme stanovili, že problémy, spojené s neoptimalizovanou datovou sítí, kterou školy v současné době mnohdy disponují, jsou časově neefektivní správa sítě, zvýšená bezpečnostní rizika, související s využíváním jejích služeb a rovněž neefektivní odstraňování problémů. **Zefektivnění správy** školní datové sítě a **minimalizaci bezpečnostních rizik** považujeme

za dva klíčové cíle našeho návrhu. Jejich dosažením dále nejenže zefektivníme odstraňování problémů, ale rovněž zajistíme prevenci jejich vzniku.

V první kapitole, věnované charakteristice AD jsme zjistili, že lze tuto službu využít k centralizaci správy datové sítě. Tato centralizace, tedy možnost spravovat objekty z jednoho místa, vede k zefektivnění správy datové sítě. Dále již víme, že pomocí OU logické struktury v AD můžeme docílit seskupení objektů do skupin, pomocí kterých lze s objekty pracovat hromadně. Díky těmto skupinám máme možnost jednoduché, přehledné, a tedy efektivní správy objektů datové sítě. Zmíněné seskupování nám rovněž dává možnost řídit oprávnění objektů v rámci datové sítě. Správným využitím dostupných nastavení můžeme zajistit minimalizaci rizik s užíváním datové sítě spojených. Z uvedených informací je zřejmé, že s využitím vhodně navržené logické struktury v AD můžeme splnit cíle, stanovené v předchozím odstavci.

V této podkapitole jsme tedy stanovili základní cíle našeho návrhu. Na základě informací, nashromážděných dříve v textu, jsme rovněž vyvodili, že pomocí vhodně navržené logické struktury datové sítě můžeme splnit stanovené cíle a tímto zvýšit kvalitu služeb, poskytovaných datovou sítí. V tuto chvíli přejdeme k volbě vhodné metodiky a stanovení základního principu, který použijeme při tvorbě naší logické struktury datové sítě.

6.2.2 Princip návrhu

Na začátku této podkapitoly považujeme za nutné připomenout fakt, který jsme vyvodili ve čtvrté kapitole práce. V našem návrhu využijeme pouze jednu doménu. Rozhodli jsme se tak mimo jiné s přihlédnutím k ceně celého řešení. K dalšímu seskupování našich objektů tedy využijeme OU.

V souvislosti s tvorbou OU se dostáváme k volbě, kterou považujeme z hlediska logické struktury našeho návrhu za zásadní, a to zda vytvořit jednu strukturu OU, zahrnující uživatele i počítače, nebo struktury dvě, jednu pro uživatele a druhou pro počítače. Mnozí autoři, jako například Štěrba (2014, s. 33), ve svých dílech popisují řešení, založené pouze na jedné struktuře, zahrnující jak uživatelé, tak počítače. Autor této práce však několik let pracoval jako IT specialista u nejmenované bankovní instituce, kde existovaly struktury dvě. Jedna, zahrnující uživatelé a druhá počítače. Po konzultaci této skutečnosti s vedoucím práce – doc. PhDr. Milanem Klementem, Ph.D., kterého považujeme za zkušeného systémového administrátora, s mnoha praktickými zkušenostmi, jsme se rozhodli, že k tomuto návrhu přistoupíme způsobem, který jsme viděli ve firemní praxi. S vedoucím práce jsme se shodli, že takovéto řešení nabízí možnost efektivnější správy datové sítě.

V této chvíli jsme se dostali do fáze, kdy máme zodpovězeny všechny důležité otázky týkající se cílů návrhu a zvolen základní princip, kterého využijeme při tvorbě OU, a nyní už tedy můžeme začít s návrhem samotným. Dle našeho názoru je vhodným začátkem práce na návrhu stanovení názvu domény. V další podkapitole se tedy volbou vhodného názvu domény budeme zabývat.

6.3 Stanovení názvu domény

Stanovení názvu domény pokládáme za velmi důležitý krok, protože jde o údaj, který budeme při realizaci a pozdější administraci logické struktury datové sítě poměrně často používat. Vhodnou volbou doménového jména se také můžeme vyhnout řadě komplikací, jako například jevu nazývanému split DNS či vlastnickým konfliktům s jinými institucemi, které zmiňuje mimo jiné NG (2014). Abychom podobným problémům předešli, rozhodli jsme se zjistit, jaká doporučení pro volbu vhodného doménového jména poskytuje společnost, vyvíjející službu AD. Z doporučení, nalezených na stránkách společnosti Microsoft (2017) pokládáme za nejdůležitější tato:

- Název domény by měl být krátký a jednoduše zapamatovatelný
- Je vhodné použít doménu, příbuznou k registrované internetové DNS doméně společnosti
- Je důležité jako název domény nezvolit jméno existující společnosti či produktu
- Je vhodné vyvarovat se obecný názvům
- Je vhodné vyvarovat se použití podtržítka v názvu domény

Rovněž považujeme za důležité zmínit, že není vhodné, aby se název AD domény shodoval s názvem veřejně dostupné domény společnosti, a to z důvodu prevence proti již zmíněnému jevu split DNS.

Dále existují jistá pravidla, definující povolenou délku názvu domény a povolené znaky. Ta zde však nepovažujeme za důležité rozebírat, protože nám samotná služba AD při pokusu o vytvoření nové domény, jejíž název nesplňuje stanovená pravidla, vypíše chybovou hlášku a takovou doménu nám neumožní vytvořit.

Námi zvolená škola, Základní škola Odry Komenského, má zaregistrovánu internetovou doménu **komenska.com**. My tedy dle dříve uvedených doporučení volíme jako název

AD domény **ad.komenska.com**. Podobným způsobem může vytvořit název své AD domény kterákoliv jiná škola.

Domníváme se, že jsme v této podkapitole dostatečně pronikli do problematiky volby vhodného názvu AD domény. Na základě získaných informací jsme rovněž zvolili název AD domény, která bude součástí našeho návrhu. V tuto chvíli nám tedy již nic nebrání v tvorbě dvou struktur, zmíněných v předchozí podkapitole, které budou dohromady tvořit návrh logické AD struktury zvolené školy.

6.4 Návrh uživatelské struktury

Prvnímu hierarchickému seskupení jsme zvolili pracovní název **uživatelská struktura**. Tato struktura v sobě bude zahrnovat všechny uživatele školní datové sítě. Jelikož nám má naše struktura pomoci k zefektivnění správy datové sítě a rovněž k minimalizaci bezpečnostních rizik, považujeme za vhodné uživatele seskupovat do OU podle jejich pracovní pozice a pracovní náplně. To nám umožní pracovat se skupinami uživatelů, z nich každá využívá specifické služby a prostředky datové sítě a má rovněž specifické potřeby, související s bezpečností (s přístupovými právy). Na tyto skupiny uživatelů poté můžeme jednoduše aplikovat vhodná pravidla reflektující zmíněné potřeby, což považujeme za mnohem efektivnější metodu, než tato pravidla aplikovat na každého z uživatelů jednotlivě.

Před tvorbou samotné struktury ještě považujeme za vhodné zmínit pravidla pro volbu názvu OU. V případě volby názvu OU nejsme limitováni, co se povolených znaků týče - jsou povoleny všechny znaky. Je však potřeba respektovat, že maximální délka názvu OU je 64 znaků. Společnost Microsoft (2017) doporučuje, aby názvy OU byly jednoduché a vystihovali jejich účel.

Nyní však již začneme se samotným návrhem. Při jeho tvorbě budeme vycházet z **tabulky 1**, kterou jsme uvedli v podkapitole 6.1.2. Nejprve je vhodné vytvořit OU zahrnující všechny uživatele naší datové sítě, na kterou bude později možné aplikovat pravidla, společná pro všechny uživatele. Dle dříve uvedeného principu seskupování uživatelů dále na základě tabulky 1 vytvoříme OU zahrnující skupiny uživatelů s navzájem podobnou pracovní náplní (s navzájem podobnými potřebami z hlediska využívání služeb datové sítě), které budou součástí OU zahrnující všechny uživatele.

Výše uvedeným způsobem jsme vytvořili následující návrh uživatelské struktury. Níže rovněž uvádíme stručné vysvětlení tohoto návrhu.

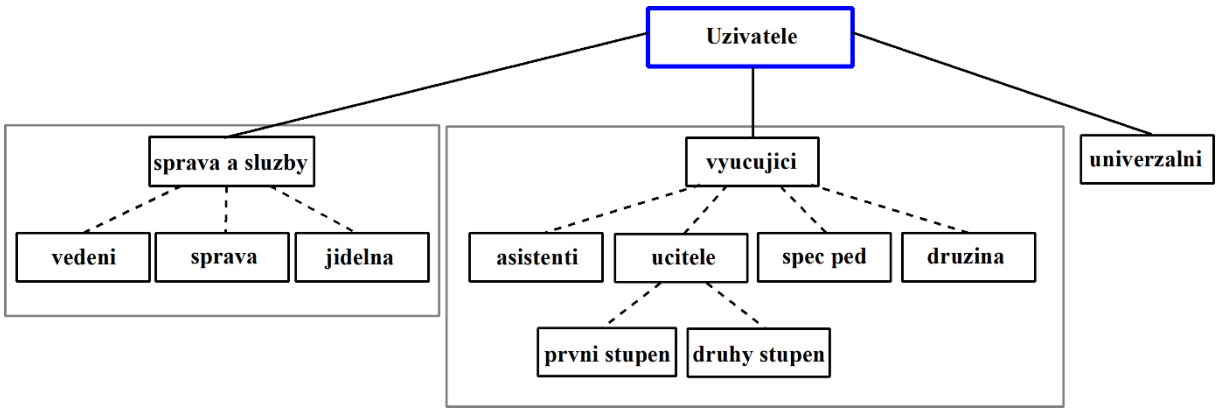


Schéma 1: Návrh uživatelské struktury

Do jednotlivých OU budeme později rozdělovat uživatelské účty na základě pracovní náplně uživatelů. Jedinou pracovní pozicí, jejíž umístění nelze při porovnání tabulky 1 a výše uvedeného návrhu snadno určit, je pozice **školní psycholožky**. Tu bychom, dle její pracovní náplně, zařadili do OU **spec ped**, která je určena pro speciální pedagogy.

Dále považujeme za důležité uvést, kde jsou v návrhu začleněni žáci školy. Zde je potřeba vysvětlit, jakou funkci má OU **univerzalni**. Jde o OU, která je určena pro uživatelské účty, používané v počítačových učebnách a ve třídách, které si konkrétně pojmenujeme **zak** a **ucitel**. Pro žáky školy považujeme za výhodné využít jeden univerzální uživatelský účet. To je dáno skutečností, že vždy před začátkem školního roku dojde k výměně desítek žáků, nemluvě o změnách v jeho samotném průběhu, a na tyto změny by v případě, že by každý žák měl osobní uživatelský účet, bylo nutné reagovat. Hlavní náplní práce administrátora školní datové sítě však často nebývá administrace datové sítě, ale pedagogická činnost, a proto se domníváme, že nemusí mít dostatečný časový prostor pro reakci na podobné změny.

Rovněž je nutné objasnit, proč v našem návrhu figuruje nejen univerzální účet ucitel, ale rovněž osobní účty pedagogů. Důvodem je řada možností a výhod, které toto řešení přináší. Mimo jiné můžeme zmínit možnost vytvořit každému osobnímu účtu vlastní síťový adresář, kde jen on bude mít právo zápisu, a ze kterého bude moci univerzální účet ucitel pouze číst, což umožňuje bezpečně zpřístupnit data univerzálnímu účtu bez rizika jejich ztráty (například chybou některého z jiných pedagogických pracovníků) a zároveň se učitelé nebudou muset v učebně přihlašovat ke svému osobnímu účtu a tím ztrácet čas a vystavovat svá data bezpečnostnímu riziku, zapříčiněnému možností, že se z počítače zapomenou odhlásit. Dále můžeme uvést například výhody spojené s konfigurací počítače (každý uživatel může například

přizpůsobit uživatelské rozhraní počítače ve sborovně svým potřebám, aniž by omezoval potřeby jiných uživatelů) a s řízením tisku.

Nyní tedy již máme vytvořenu vhodnou uživatelskou strukturu, navrženou tak, aby se dala efektivně spravovat. OU jsou vytvořeny způsobem, který umožňuje jednoduchou aplikaci nastavení spojených s řízením přístupu ke sdíleným prostředkům v datové síti a s minimalizací bezpečnostních rizik v datové síti obecně. Strukturu je rovněž možné jednoduše měnit přidáváním či odebíráním OU na základě potřeb dané školy a proto ji považujeme za relativně univerzální. Tento fakt si předvedeme na příkladu. Kdyby se například zvolená základní škola spojila se střední školou, disponující internátem, mohli bychom naši strukturu této změně jednoduše přizpůsobit přidáním nových OU. Pod OU **ucitele** bychom v takovém případě přidali OU **stredni skola** a pod OU **sprava a sluzby** bychom v naší hierarchii přidali OU **internat**. Tento příklad vychází z předpokladu, že by bylo zachováno pouze vedení základní školy. Návrh by však samozřejmě bylo možné přizpůsobit i jiné situaci. Vidíme tedy, že strukturu, jejíž princip i návrh je popsán v této podkapitole, je možné poměrně jednoduše přizpůsobit potřebám prakticky jakékoli školy.

V této chvíli jsme ve fázi, kdy máme vytvořenu strukturu OU vhodnou pro správu uživatelských účtů. V další podkapitole považujeme za vhodné provést návrh struktury, zahrnující počítače.

6.5 Návrh struktury pro počítače

Při tvorbě druhé struktury, která bude sloužit pro administraci počítačů, připojených k datové síti vybrané školy, budeme postupovat podobně, jako tomu bylo v případě tvorby struktury předchozí. Budeme vycházet z **tabulky 2**, kterou jsme uvedli v podkapitole 6.2.3. Počítače, uvedené v tabulce, budeme seskupovat do OU dle jejich využívání a částečně rovněž dle jejich umístění v rámci budovy. Tuto metodu považujeme za výhodnou, protože na takto vytvořené skupiny počítačů můžeme poté snadno aplikovat pravidla, které budou reflektovat zmíněný způsob využívání počítačů a zajistí tak vhodné podmínky, potřebné k jejich efektivnímu, bezpečnému a zároveň dlouhodobému provozu. Vzniklá struktura bude navíc díky tomu, že bude do jisté míry reflektovat také umístění počítačů, rovněž přehledná a v případě změn snadno upravitelná.

Pravidla a doporučení, vztahující se k volbě názvů OU, jsme již uvedli v předchozí podkapitole 6.4, a proto se domníváme, že máme dostatek teoretických znalostí, abychom mohli zmíněnou strukturu vytvořit. Opět považujeme za výhodné začít vytvořením souhrnné OU, zahrnující všechny počítače v naší datové síti, která nám poskytne možnost efektivně aplikovat pravidla,

společné pro všechny počítače. Dále si na základě již zmíněné metody seskupování počítačů vytvoříme OU, které budou součástí souhrnné OU.

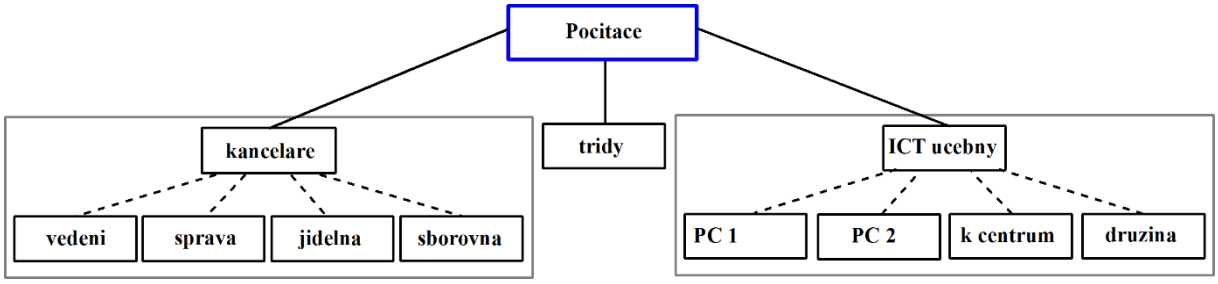


Schéma 2: Návrh struktury pro počítače

Stejně jako v případě uživatelské struktury však považujeme za vhodné objasnit možné nejasnosti, které mohou bránit ve správném pochopení struktury. K jejich objasnění a k jistému vysvětlení principu struktury, jsme se však tentokrát rozhodli přistoupit jiným způsobem. Učiníme to ve spojení s prezentací výhod nově vytvořené struktury.

Mezi hlavní výhody této struktury řadíme fakt, že jsou v ní odděleny počítače, využívané pouze zaměstnanci školy (OU kancelare) od počítačů, které jsou k dispozici žákům (ICT ucebny). Z vlastní zkušenosti víme, že na počítačích, které se nacházejí ve špatně optimalizovaných datových sítích, žáci často nevhodným chováním (ať už úmyslným, jako například změny různých nastavení počítače, nebo neúmyslným, jako například způsobením virové infiltrace) způsobí nemalé problémy. Tyto problémy nejen že omezují další uživatele počítačů, vystavují počítače zvýšenému riziku a snižují jejich životnost, ale rovněž mohou mít negativní důsledek na kvalitu služeb, poskytovaných datovou sítí. Jejich vznik také přidává práci ICT koordinátorovi dané školy, který je musí řešit. Toto logické oddělení počítačů nám později umožní předejít zmíněným problémům vhodným nastavením pravidel a restrikcí, reflektujícím typ uživatelů, kteří počítače dané OU využívají.

Počítače v OU **tridy** budou z hlediska nastavení specifické, protože k nim mají přístup jak učitelé, tak i žáci. K těmto počítačům bývá často připojeno některé z přenosných paměťových médií s nejrůznějším obsahem (prezentace, videa, ale rovněž hrozí zvýšené riziko virové infiltrace, stejně jako je tomu v případě počítačů v OU ICT ucebny). Dalším charakteristickým znakem těchto počítačů je fakt, že jsou všechny připojeny buďto k projektoru, nebo k interaktivní tabuli. Kvůli těmto a dalším specifickým vlastnostem těchto počítačů považujeme za vhodné mít tyto počítače oddělené od ostatních a tedy mít možnost tuto skupinu počítačů samostatně spravovat.

Další výhodou je fakt, že návrh seskupuje počítače stejného využití či umístění do dalších OU, podřazených OU ICT ucebny a kancelare. To umožňuje efektivnější správu počítačů a to proto, že máme možnost aplikovat specifická pravidla i na menší skupiny počítačů, než jsou OU ICT ucebny a kancelare, což je mnohdy žádoucí. V souvislosti s tímto faktem považujeme za důležité zmínit, že počítače umístěné v obou sborovnách, společně s počítači speciální pedagožky a psycholožky byly seskupeny do OU **sborovna**. Tento krok byl učiněn na základě tabulky 2, ze které je patrné, že tyto počítače mají prakticky totožné využití. Počítače poté můžeme pro snadnou identifikaci odlišit pomocí jejich názvů.

Poslední výhodou je, stejně jako při návrhu organizační struktury pro uživatele, že je tato struktura jednoduše upravitelná. Pokud bychom se například rozhodli do naší datové sítě připojit tablety, využívané pro vzdělávání žáků, mohli bychom v OU **ICT ucebny** vytvořit OU **tablety**. Domníváme se tedy, že i tuto strukturu je možné poměrně jednoduše přizpůsobit jakýmkoliv změnám, a je rovněž možné ji upravit pro využití v datové síti prakticky jakékoliv jiné školy.

V této chvíli jsme tedy vytvořili dvě hierarchické struktury OU, které dohromady tvoří návrh logické AD struktury. Obě struktury dle našeho názoru seskupují objekty datové sítě tak, aby byla zajištěna jejich co nejefektivnější správa a rovněž co nejjednodušší aplikace nejrůznějších nastavení, vedoucích k minimalizaci rizik spojených s využíváním služeb datové sítě. Domníváme se tedy, že návrh splňuje cíle návrhu, stanovené v podkapitole 6.2.1, a proto jej považujeme za vhodný k nasazení za účelem optimalizace služeb datové sítě. Nyní nám však zbývá ještě jedna důležitá oblast, kterou bychom při návrhu logické struktury datové sítě neměli opomenout, a tou je oblast stanovení názvů účtů. Právě této oblasti se tedy budeme věnovat v další podkapitole.

6.6 Stanovení názvů účtů

V této podkapitole se budeme zabývat nazýváním účtů počítačů a uživatelů, které budou později obsahem OU výše navržené logické AD struktury. Stanovíme si takzvané **jmenné konvence**. Jmenné konvence, jak rovněž zmiňuje například Allen (2016), zjednodušují práci administrátora datové sítě, protože každý z účtů musí mít svůj unikátní název a administrátor díky těmto konvencím bude mít pevně stanoven způsob, jakým bude tyto názvy volit. Nemusí tak sám vymýšlet unikátní název pro každý z účtů, což nejenže může zabrat poměrně mnoho času, ale rovněž může vést k neefektivní správě datové sítě, způsobené problémy s dohledáním objektů na základě jejich názvů. Před samotným stanovením jmenných konvencí

ještě považujeme za vhodné zmínit, že neexistuje žádná jmenná konvence, která je vhodná či nejvhodnější pro všechna prostředí, jak rovněž uvádějí ve svých odborných článcích Allen (2016) a Pytko (2015), a proto je pouze na nás, abychom zvolili jmenné konvence, odpovídající našim potřebám.

6.6.1 Jmenná konvence uživatelských účtů

Jmenná konvence účtů v AD nám musí umožnit splnění podmínky, kterou jsme uvedli výše, a to, že každý z účtů musí mít unikátní název. Při zakládání uživatelských účtů v AD máme možnost zadat **jméno** a **příjmení** uživatele, který bude účet využívat. Těmito dvěma údaji je tvořeno **celé jméno** uživatele (tzv. full name), kterým je poté uživatel v AD identifikován. Způsob nazývání uživatelských účtů, založený pouze na principu jména a příjmení uživatele nám však sám o sobě nadává možnost za každých okolností stanovit unikátní název uživatelského účtu. Představme si situaci, kdy máme v naší škole dva uživatele, kteří se jmenují **Jiří Novotný**. Oba uživatelé by tedy v AD měli celé jméno Jiří Novotný, což však není možné. Proto musíme tyto uživatele odlišit. My jsme se z tohoto důvodu rozhodli, že v případě shodných uživatelských jmen přidáme do celého uživatelského jména druhého z uživatelů číslici 2 (či vyšší, v závislosti na počtu již vytvořených uživatelů se shodným jménem). Náš v pořadí druhý Jiří Novotný by tedy v takovémto případě měl celé uživatelské jméno v rámci AD **Jiří Novotný2** a tímto by tedy byl jasně odlišen od svého jmenovce.

Další oblastí, které se musíme při stanovení jmenné konvence uživatelských účtů věnovat, je oblast **přihlašovacího jmena uživatelů** (tzv. user logon name). Jde o jméno, pomocí kterého se bude uživatel přihlašovat k počítačům a další zařízením uvnitř domény. Toto jméno by dle našeho názoru mělo splňovat následující tři podmínky. Musí být, stejně jako celé uživatelské jméno, unikátní. Dále by mělo být jednoduché a snadno zapamatovatelné. Jednoduché přihlašovací jméno umožní rychlé přihlášení uživatele k zařízení v doméně a dále se domníváme, že pokud bude toto jméno snadno zapamatovatelné, uživatelé to jistě ocení.

Na základě výše zmíněných podmínek jsme se rozhodli v naší jmenné konvenci uživatelských účtů využít následující princip tvorby přihlašovacích jmen, který ve svém článku rovněž zmiňuje Pytko (2015). Přihlašovací jméno se bude skládat z jeho celého příjmení uživatele a počátečních tří písmen jeho křestního jména, a to bez diakritiky a velkých písmen. Pro ilustraci uvedeme příklad. V případě, že bychom zakládali účet uživateli jménem **Jiří Novotný**, jeho přihlašovací jméno bude **novotnyjir**. Pokud bychom později vytvářeli účet uživateli se stejným jménem, jako má některý z uživatelů již vytvořených, jeho přihlašovací

jméno by na konci obsahovalo číslici 2 (či vyšší, v závislosti na počtu již vytvořených uživatelů se shodným jménem). Kdybychom tedy vytvářeli uživatelský účet dalšímu uživateli se jménem Jiří Novotný, zvolili bychom mu přihlašovací jméno **novotnyjir2**.

Domníváme se, že máme v této chvíli stanovenu vhodnou jmennou konvenci, týkající se uživatelských účtů, a proto můžeme přistoupit ke stanovení jmenné konvence pro účty počítačů.

6.6.2 Jmenná konvence účtů pro počítače

V případě stanovení jmenné konvence účtů počítačů máme, dle našeho názoru, větší volnost, než v případě jmenné konvence uživatelských účtů. Je to z toho důvodu, že s názvy účtů počítačů bude ve většině případů pracovat pouze administrátor datové sítě. I zde však musíme splnit podmínku, že každý objekt datové sítě musí mít svůj unikátní název. My jsme se rozhodli využít řešení, které ve svém odborném článku zmiňuje rovněž Thompson (2011), a to dle fyzického umístění počítače. Tato jmenná konvence je do značné míry v souladu s dříve navrženou logickou AD strukturou a také nám dává možnost zjistit základní informaci o umístění počítače již při pohledu na název jeho účtu, což považujeme než užitečné.

Název účtu počítače, připojeného k datové síti, tedy bude tvořen z údaje o umístění počítače a rovněž z jeho čísla v rámci tohoto umístění, a to ve tvaru **umisteni-pcislo**. Pro lepší pochopení považujeme za vhodné uvést několik příkladů. Při vytváření účtu prvního z počítačů, který se nachází v učebně **PC 1** (a rovněž v OU PC 1 našeho návrhu), bude tomuto účtu zvoleno jméno **pc1-p01**. Účet dalšího počítače, umístěného v učebně PC 1 bude mít název **pc1-p02** a tímto způsobem lze volit názvy účtů dalších počítačů v učebně. V návaznosti na náš dříve vytvořený návrh struktury pro počítače dále uvedeme příklad počítače, umístěného ve sborovně 2 (malá budova) a počítače, umístěného v pracovně speciálních pedagogů. Oba tyto počítače jsou umístěny v OU **sborovna**. My si je pomocí názvů jejich účtů můžeme snadno odlišit, což nám zjednoduší jejich identifikaci a správu. Počítači ve sborovně 2 bychom zvolili název **sborovna2-p01** a počítači v pracovně speciálních pedagogů název **specped-p01**.

Zvolená jmenná konvence nám tedy poskytne nejen princip pro stanovování unikátních názvů účtů počítačů, ale také možnost z těchto názvů přibližně určit umístění počítače. Z těchto důvodů považujeme zvolenou jmennou konvenci za výhodnou.

6.7 Závěr

V této kapitole jsme si tedy na základě informací z předchozích kapitol a na základě vstupních údajů, uvedených v podkapitole 6.1, vytvořili návrh logické AD struktury. Dále jsme zvolili vhodné jmenné konvence, na základě kterých budeme volit názvy účtů objektů naší datové sítě, což využijeme zejména v osmé kapitole, věnované praktické realizaci našeho návrhu. Před praktickou realizací návrhu však považujeme za vhodné nejprve prozkoumat požadavky k provozování AD, které s praktickou realizací návrhu přímo souvisí. Těmto požadavkům se budeme věnovat v následující kapitole.

7 Požadavky k provozování Active Directory

Poslední důležitou oblastí, které je potřeba před praktickou realizací našeho návrhu věnovat pozornost, je oblast požadavků k provozování AD, která s realizací návrhu přímo souvisí. Tyto požadavky si zde tedy uvedeme, a v případě požadavků, kde existuje více možností, vedoucích k jejich splnění, vždy zvolíme alternativu, která je z hlediska realizace našeho návrhu tou nejvhodnější.

7.1 Server

Z dříve získaných informací je zřejmé, že jedním z důležitých požadavků k provozování AD je nejméně jeden server, který bude sloužit jako DC. S vedoucím práce jsme se však na jedné z konzultací shodli, že pro zajištění spolehlivosti navrženého řešení bude vhodné pro jeho praktickou realizaci použít servery dva. Toto rozhodnutí bylo učiněno na základě skutečnosti, zmíněné v podkapitole 4.2.1, a to sice, že v případě poruchy jednoho z DC bude funkce domény díky DC zachována. Oprava nefunkčního DC tak nebude mít zásadní vliv na kvalitu služeb, poskytovaných ze strany datové sítě.

Dále považujeme za vhodné připomenout skutečnost, kterou jsme určili v podkapitole 5.1.8, a to, že naše DC budou disponovat operačním systémem **Windows Server 2016**. Při výběru serverů proto musíme zohlednit **systémové požadavky**, které musí servery splňovat pro instalaci a následný bezproblémový chod zvoleného operačního systému. Níže si uvedeme tabulku, vytvořenou na základě informací z webových stránek společnosti Microsoft, která tyto požadavky obsahuje.

Procesor:	64-bitový procesor s frekvencí 1,4 GHz Kompatibilita s instrukční sadou x64 Podpora technologií NX a DEP (data execution prevention) Podpora instrukcí CMPXCHG16b, LAHF/SAHF a PrefetchW Podpora překladu adres druhé úrovně
Paměť RAM:	Kapacita minimálně 512 MB (2 GB pro server s možností instalace desktopového prostředí) Typ ECC (Error Correcting Code) nebo podobná technologie
Řadič paměťového zařízení:	Adaptér úložiště kompatibilní se specifikací architektury PCI Express Trvalá úložiště s klasifikací pevných disků nemohou mít rozhraní PATA Pro spouštěcí, stránkovací nebo datové jednotky nejsou povolena rozhraní SATA/PATA/IDE a EIDE
Kapacita pevného disku:	Minimálně 32 GB pro instalaci v režimu Jádro serveru Minimálně 36 GB pro instalaci v režimu Server s grafickým uživatelským rozhraním Při instalaci přes síť či u serverů s velikostí paměti RAM nad 16 GB jsou nároky na kapacitu vyšší
Síťový adaptér:	Adaptér sítě Ethernet s minimálně gigabitovou propustností Kompatibilita se specifikací architektury PCI Express Podpora technologie PXE (preboot execution environment)
Další požadavky:	Jednotka DVD (při instalaci z disku DVD) Grafické zařízení a monitor rozlišením minimálně Super VGA (1 024 x 768) v případě instalace desktopového prostředí Další požadavky, v závislosti na požadovaných funkcích

Tabulka 3: Minimální požadavky systému Windows Server 2016 (Microsoft, 2017)

Kromě požadavků, souvisejících s instalací a chodem zvoleného operačního systému, musíme při volbě vhodných serverů rovněž přihlédnout k předpokladům pro jejich spolehlivost. Z těchto předpokladů považujeme za důležité zmínit **počet zdrojů**, kterými server disponuje. S vedoucím práce jsme se shodli, že servery, optimální pro použití jako DC, by měly disponovat dvěma zdroji. Díky této redundanci zdrojů je v případě poruchy jednoho z nich funkce serveru zachována. S přihlédnutím k bezpečnému chodu serverů jsme se dále shodli, že je potřeba mít tyto servery, z důvodu možného výpadku elektrického proudu, připojeny k UPS stanici.

Zmíněná kritéria pro výběr, tedy požadavky pro instalaci a provoz zvoleného operačního systému a rovněž vhodný počet zdrojů, splňuje celá řada serverů, které jsou v současné době na trhu. Jako příklad můžeme uvést server **Dell PowerEdge R330**, který díky tomu, že splňuje

zmíněná kritéria, považujeme za vhodný pro účely realizace našeho návrhu. Pro představu uvádíme, že cena tohoto serveru k datu 7. 4. 2018 začíná na 32 000 Kč (Czech Computer, 2018) a v závislosti na konfiguraci může být vyšší.

V této podkapitole jsme určili, že pro potřeby praktické realizace našeho návrhu bude vhodné mít k dispozici dva servery. Rovněž jsme uvedli, jaká kritéria je potřeba zvážit při výběru serverů, vhodných pro použití jako DC, a poskytli příklad jednoho z mnoha nabízených modelů, který splňuje uvedená kritéria. Nyní již přejdeme k dalším z požadavků na provoz AD, kterými jsou operační systém a klientské licence.

7.2 Operační systém a klientské licence

Jako vhodný operační systém pro realizaci našeho návrhu jsme v podkapitole 5.1.8 zvolili Windows Server 2016. Microsoft nám dává na výběr ze tří edic tohoto operačního systému, z nichž každá je specifická svým určením a svými funkcemi a každá má rozdílnou cenu. Kteroukoliv z nich však lze ke zprovoznění AD použít. My v této kapitole jednotlivé edice prozkoumáme s cílem stanovit, která z nich bude nejvhodnější pro realizaci našeho návrhu. Edice si uvedeme v pořadí od nejlevnější po nejdražší. U každé edice rovněž poskytneme informaci o ceně za její nejlevnější variantu, uváděnou na stránkách společnosti Microsoft, která je aktuální k datu 23. 12. 2017.

7.2.1 Windows Server Essentials

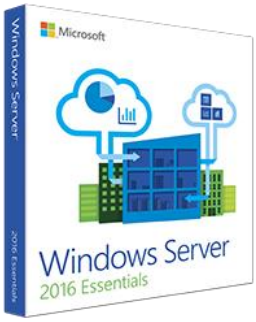
Edice Essentials je určena pro malé organizace. Tomu je přizpůsoben licenční model a také jistá omezení, která tuto edici činí nevhodnou pro větší organizace. Licence je vázána na konkrétní server a pro připojení k serveru nejsou potřeba klientské licence CAL (client access license). Fakt, že pro připojení k serveru, vybavenému operačním systémem Windows Server 2016 Essentials, nejsou potřeba klientské licence, činí využití této edice cenově výhodným.

K této verzi se však váží již zmíněná omezení. V souvislosti s potřebami našeho návrhu je největším omezením fakt, že k tomuto serveru můžeme připojit maximálně 50 počítačů a 25 uživatelů (Microsoft, 2017). Z dalších omezení považujeme za vhodné zmínit, že edice Essentials rovněž stanovuje jisté limity ve vztahu k serveru. Podporuje totiž maximálně 64 GB paměti RAM a maximálně dva procesory, jak na svých webových stránkách uvádí společnost Microsoft (2013). Tyto limity dle našeho názoru nejsou příliš důležité, pokud má daný server sloužit pouze jako DC. V takovém případě by totiž byl dostačující i server s podstatně nižším výkonem.

Další omezení edice Essentials již nejsou s přihlédnutím k potřebám našeho návrhu zásadní. Z hlediska AD jsou dány převážně tím, že některé role (Active Directory Domain Services a další) mají automatickou instalaci a jsou automaticky konfigurovány, jak lze vyvodit z Obernedova srovnání edic (2017). Jako příklad takového omezení můžeme uvést, že DC, vybavený touto edicí operačního systému, musí být vždy kořenem doménové struktury. Toto omezení však, pro potřeby realizace návrhu logické AD struktury školní datové sítě, nepokládáme za důležité, protože nepředpokládáme, že by logická AD struktura v případě školy, používající 50 počítačů, obsahovala více než jednu doménu.

Cena: $501 (Microsoft, 2017)

Z výše uvedeného usuzujeme, že tato licence může být, díky své licenční politice a relativně nízké ceně, výhodná pro malé školy s nízkým počtem počítačů a uživatelů. Pro naše potřeby však, zejména z důvodu omezeného počtu uživatelů a počítačů, není vhodná.



Obrázek 5: Windows Server 2016 Essentials (TechSoup, 2017)

7.2.2 Windows Server Standard

Edice standard se zdá být edicí vhodnou pro využití ve většině firem a institucí. Tento závěr jsme vyvodili nejen dle jejího názvu, ale i dle popisu výrobce. Microsoft uvádí, že je tato edice vhodná pro nevirtualizovaná prostředí, nebo pro prostředí s nízkou hustotou virtualizace (Microsoft, 2017), což je popis, kterému odpovídají datové sítě většiny škol.

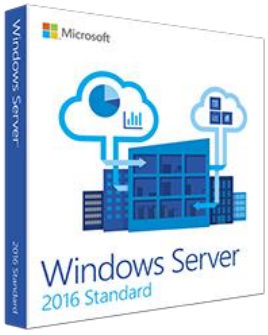
V případě této edice pokládáme licenční model za složitější, než tomu bylo u edice předchozí, a proto považujeme za vhodné jej krátce vysvětlit. Microsoft zde zvolil licencování na základě počtu jader procesoru. Nejnižší počet jader serveru, pro něž lze zakoupit licenci, je 16. Proto můžeme říci, že z hlediska licenční politiky Microsoftu neexistuje server s nižším počtem jader než 16, jak rovněž ve svém odborném článku uvádí Novák (2017). To pokládáme, s přihlédnutím k potřebám realizace našeho návrhu, za nevýhodné, protože server, využívaný jako DC, nepotřebuje disponovat takto vysokým počtem jader. Služba AD nevyžaduje

od serveru mnoho prostředků, a proto bychom uvítali možnost zakoupení levnější licence pro server s nižším počtem jader. Dále považujeme za důležité zmínit, že v případě edice Standard již je potřeba dokoupit klientské licence CAL pro uživatele či počítače, připojující se k serveru (Microsoft, 2017), což se samozřejmě projeví zvýšením celkových nákladů, spojených s realizací navrženého řešení. Licencemi CAL se budeme podrobněji zabývat později.

Z hlediska potřeb našeho návrhu je zásadním faktem, že u této edice již není stanoven maximální počet uživatelů a počítačů (Microsoft, 2017). Rovněž limity ve vztahu k serveru jsou přívětivější. V případě edice Standard máme stanoveno, že maximální množství paměti RAM, kterým může server disponovat, je 24 TB a maximální počet jeho procesorových jader je 512. To jsou hodnoty, které nás z hlediska použití serverů jako DC zcela jistě neomezí. Dále nám u této edice odpadají omezení související s automatickou instalací a automatickou konfigurací rolí, které jsme zmínili v případě předchozí edice.

Cena: $882 (Microsoft, 2017)

Ze zjištěných skutečností můžeme vyvodit, že je tato edice pro potřeby našeho návrhu vhodná. Hlavní výhodu oproti edici Essentials shledáváme v tom, nejsme limitovaní omezeným počtem uživatelů či stanic.



Obrázek 6: Windows Server 2016 Standard (Microsoft, 2017)

7.2.3 Windows Server Datacenter

Poslední z nabízených edic operačního systému Windows Server 2016 má mnoho společného s edicí Standard. Dle výrobce je však určena pro *„Vysoce virtualizovaná a softwarově definovaná prostředí datacenter.“* (Microsoft, 2017). To naznačuje, že pro potřeby našeho návrhu pravděpodobně nebude edicí nejvhodnější. Přesto jí však, pro úplnost, z hlediska našeho návrhu posoudíme.

Nejprve považujeme za vhodné uvést společné rysy edicí Standard a Datacenter, kterých je hned několik. Společnost Microsoft pro edici Datacenter zvolila stejný licenční model, jako pro edici Standard. Dále nás tato edice, stejně jako edice Standard, neomezuje z hlediska maximálního počtu uživatelů a počítačů, což je z hlediska potřeb návrhu důležité. Limity ve vztahu k serveru jsou u obou zmíněných edic rovněž totožné.

Dále si zde uvedeme rozdíly mezi edicemi Standard a Datecenter. Rozdílem edice Datacenter oproti edici Standard jsou funkce, které v jiných edicích operačního systému Windows Server 2016 nejsou dostupné. Za účelem uvedení funkcí, které nám edice Datacenter oproti edici Standard navíc přináší, považujeme za vhodné použít tabulku, která je k dispozici na stránkách společnosti Microsoft.

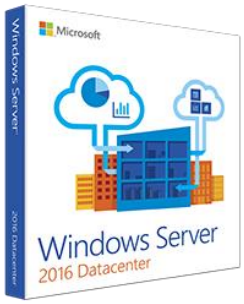
Funkce	Datacentrum	Standard
Základní funkce systému Windows Server	●	●
Prostředí OSE / kontejnery Windows Server s izolací Hyper-V	Neomezeno	2
Prostředí OSE / kontejnery Windows Server bez izolace Hyper-V	Neomezeno	Neomezeno
Služba ochrany hostitelů	●	●
Funkce úložiště včetně úložiště dat s přímým přístupem a repliky úložiště dat	●	
Stíněné virtuální počítače	●	
Sada síťových protokolů	●	

Tabulka 4: Srovnání funkcionality edic Datacenter a Standard (Microsoft, 2016)

Z informací, uvedených v tabulce, se domníváme, že nám edice Datacenter ve srovnání s edicí Standard nepřináší žádné funkce, které by pomohly s realizací našeho návrhu, či by významným způsobem přispěly k vyšší kvalitě výsledného řešení.

Cena: $6,155 (Microsoft, 2017)

Z výše uvedených informací usuzujeme, že tato edice není příliš vhodná k realizaci našeho návrhu. Edice Datacenter je výrazně dražší a její použití nepřináší žádné významné výhody oproti použití edice Standard.



Obrázek 7: Windows Server 2016 Datacenter (TechSoup, 2017)

Myslíme si, že jsme nyní dostatečně prozkoumali edice zvoleného operačního systému. Z dostupných edic jsme, jakožto nejvhodnější pro účely praktické realizace našeho návrhu, zvolili edici **Standard**, která je nejlevnější z edic, splňujících požadavky navrženého řešení. Nyní přejdeme k tématu, které se zvolenou edicí přímo souvisí, a tím jsou klientské licence CAL.

7.2.4 CAL licence

Jak již víme z podkapitoly 7.2.2, použití námi zvolené edice operačního systému Windows Server 2016, kterým budou vybaveny naše DC, vyžaduje nákup licencí CAL. Z tohoto důvodu považujeme za vhodné vysvětlit, k čemu licence CAL slouží, uvést, jaké typy těchto licencí společnost Microsoft nabízí a rovněž určit, jakým způsobem bude v případě praktické realizace našeho návrhu nejvýhodnější licencí CAL využít.

CAL je klientská licence, nutná k využívání služeb serveru. Tyto licence se dají pořídit pro jednotlivé **počítače**, nebo pro jednotlivé **fyzické uživatele** a obě možnosti lze rovněž kombinovat. Je ovšem nutné zajistit, aby každý klient, připojující se k serveru, měl svou vlastní CAL licenci (nehledě na to, zda vázanou na počítač, nebo na uživatele).

Fakt, že existuje více typů CAL licencí, nás dovedl k úvaze, kterého typu je pro realizaci našeho návrhu výhodnější využít. Dle údajů, získaných na webových stránkách Heureka (2017) je běžná CAL licence pro počítač o několik desítek procent levnější, než běžná CAL licence pro uživatele. To však můžeme v případě realizace našeho návrhu zanedbat, protože Microsoft tyto licence pro neziskové a školské instituce nabízí za zvýhodněnou a hlavně jednotnou cenu.

Cena za jednu licenci pro školy: 249 Kč (Heureka, 2017)

Po ceně je dalším důležitým faktorem, ovlivňujícím volbu vhodného typu CAL licencí, rovněž jejich počet, nutný pro připojení všech klientů k serveru. Úvahou jsme vyvodili, že na pracovištích, kde jeden uživatel využívá více zařízení, připojených k serveru,

je výhodnější využít licencí pro uživatele, kdežto na pracovištích, kde se na jednom počítači denně střídá více uživatelů, je výhodnější využít licencí pro počítače.

Na základě zmíněné úvahy, a rovněž s přihlédnutím k jednotné ceně obou typů licencí se domníváme, že pro využití v datových sítích škol existují dvě výhodná řešení nákupu CAL licencí. Prvním z těchto řešení je využit pouze licencí pro počítače. To pokládáme za výhodné, protože se na počítačích, zvláště v počítačových učebnách, střídá velké množství uživatelů, a je tedy levnější zajistit licenci pro každý počítač, než pro každého uživatele. Druhým řešením, které by pro školy mohlo být výhodné, je řešení kombinované. Máme na mysli řešení, kdy by pro administrativní pracovníky školy (ředitel, zástupce ředitele, účetní, apod.), kteří běžně využívají více než jedno zařízení, připojené ke školní datové síti, byly využity licence pro uživatele. Pro počítače, nenalézající se v administrativní sekci školy, by však byly využity licence pro počítače (máme na mysli zejména počítače v počítačových učebnách). Podobné řešení, ovšem aplikované na výrobní společnosti a nemocnice, zmiňuje rovněž Novák (2017).

My jsme se rozhodli, že pro realizaci našeho návrhu použijeme první ze dvou výše zmíněných řešení. Rozhodli jsme se tak zejména z toho důvodu, že na ZŠ Odry Komenského využívá každý administrativní pracovník zpravidla pouze jedno zařízení připojené do školní datové sítě. Druhým důvodem je rovněž menší náročnost zvoleného řešení z hlediska správy licencí. Školským institucím, kde administrativní pracovníci ke své práci využívají více než jedno zařízení na osobu, doporučujeme zvážit rovněž řešení druhé. Zde je však vhodné připomenout, že v takovém případě musí administrátor školní datové sítě zajistit, aby každý klient, připojujícímu se k serveru, měl přiřazenu CAL licenci (ať už pro počítač, nebo pro uživatele), což s sebou přináší zvýšenou administrativní náročnost.

V této podkapitole jsme získali všechny potřebné informace týkající se CAL licencí a jejich využití. Na základě těchto informací jsme poté zvolili způsob jejich využití, který považujeme z hlediska praktické realizace našeho návrhu za nejvýhodnější. Nyní přistoupíme k poslednímu z požadavků na provoz AD této kapitoly, a tím je služba Domain Name System.

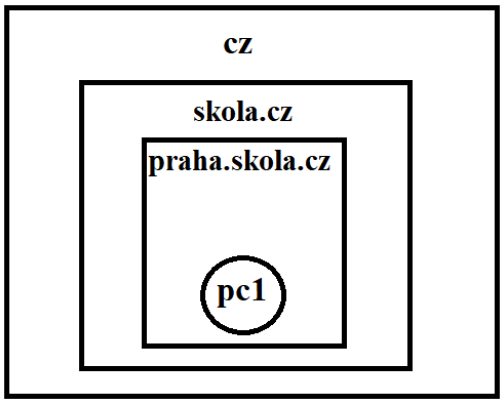
7.3 Domain Name System

Domain Name System (dále jen DNS) je službou, kterou služba AD využívá ke své funkci. Je tedy jedním z nezbytných požadavků k provozování AD. Účelem této kapitoly však nebude podrobně vysvětlit principy fungování služby DNS, protože to s přihlédnutím k cílům práce nepovažujeme za důležité. Zaměříme se zejména na to, jakým způsobem AD službu DNS

využívá, tedy na vzájemné souvislosti obou služeb. Tyto informace považujeme, z hlediska pozdější praktické realizace návrhu, za důležité, protože se se službou DNS v průběhu tohoto procesu zcela jistě setkáme. Rovněž nám osvětlení těchto souvislostí pomůže v hlubším pochopení zákonitostí služby AD.

Služba DNS nám v souvislosti s AD poskytuje možnost pracovat s pro nás jednoduchými názvy hostitelů, namísto používání dlouhých číselných identifikátorů – IP adres. K tomu služba DNS využívá protokol DNS, sloužící k vzájemnému překladu IP adres a doménových jmen. Díky službě DNS mohou klienti služby AD nacházet prostředky v datové síti, jak uvádí rovněž Stanek (2012, s. 24)

Služba DNS dále poskytuje AD **hierarchickou strukturu doménových jmen**. Pro pochopení, se za pojmem hierarchická struktura doménových jmen skrývá, uvedeme podobný příklad, jako ve svém díle uvádí například Minasi (2014, s. 212).



Obrázek 8: Hierarchická struktura doménových jmen

Na obrázku 8 vidíme příklad hierarchické struktury doménových jmen. Nejvyšší doménou je doména **cz**. Součástí domény **cz** je doména **skola** a uvnitř domény škola se nalézá doménu **praha**. Důležitým poznatkem, který lze z uvedeného obrázku vyvodit, je, že identifikátor každé domény obsahuje nejen název dané domény, ale také názvy domén vyšších. Tyto názvy jsou v identifikátoru odděleny tečkou.

V této chvíli dále považujeme za vhodné uvést pojem **plně kvalifikované doménové jméno** (fully qualified domain name – dále jen FQDN), a to z toho důvodu, že se s ním při administraci logické struktury datové sítě lze běžně setkat. Jedná se o jednoznačný identifikátor každého zařízení v datové síti. FQDN obsahuje nejen název počítače samotného, ale rovněž jeho umístění v rámci doménové struktury. Pro lepší pochopení považujeme za vhodné uvést

příklad FQDN. Na obrázku 8 vidíme počítač **pc1**, který je součástí domény s identifikátorem praha.skola.cz. Jeho FQDN by bylo **pc1.praha.skola.cz**.

Toto krátké nastínění principů služby DNS a souvislostí s této služby se službou AD považujeme, pro naše potřeby, za dostatečné. Z uvedených informací je zřejmá úzká provázanost služeb AD a DNS. Naše datová síť tedy bude muset službou DNS disponovat. Nyní uvedeme krátké shrnutí této kapitoly.

7.4 Závěr

V této kapitole jsme prozkoumali požadavky k provozování AD. Pronikli jsme do problematiky volby vhodného serveru a rovněž zvolili řešení, vhodné pro účely realizace našeho návrhu. Rovněž jsme se seznámili s edicemi operačního systému Windows Server 2016 a na základě získaných informací vybrali edici, nejhodnější pro naše potřeby. Dále jsme získali mnoho důležitých poznatků ohledně klientských licencí CAL, které jsou pro praktickou realizaci našeho návrhu nutné, a na jejich základě vybrali pro naše potřeby nejvýhodnější variantu nákupu těchto licencí. U všech výše zmíněných požadavků jsme neopomněli zmínit údaje, týkající se pořizovacích cen. Na základě těchto údajů odhadujeme, že by se výsledná cena implementace AD do datové sítě zvolené školy v případě, že škola nedisponuje žádným serverem, použitelným jako DC a rovněž žádnými z potřebných licencí, pohybovala mezi 85 000 – 100 000 Kč. V podkapitole 7.3 jsme rovněž blíže prozkoumali službu DNS, která je pro provoz služby AD nezbytně nutná, a to zejména z hlediska jejích souvislostí se službou AD, což nám, dle našeho názoru, dotvořilo teoretický základ, nutný pro dostatečné porozumění principům služby AD.

Domníváme se, že jsme získali dostatek informací ohledně požadavků k provozování AD, a proto nyní přejděme k praktické realizaci našeho návrhu.

8 Praktická realizace návrhu logické struktury školní datové sítě

V této kapitole se budeme zabývat procesem implementace AD do datové sítě školy a rovněž praktickou realizací návrhu logické struktury školní datové sítě, který byl vytvořen v šesté kapitole této práce. Dále zde uvedeme postupy, vedoucí k vytvoření a k nastavení účtů objektů datové sítě a rovněž k vytvoření skupin. V souvislosti s tématem práce také uvedeme jednu s možností, kterou AD nabízí ke správě objektů datové sítě, kterou jsou tzv. skupinové politiky, jejichž správné použití může významným způsobem přispět k optimalizaci služeb datové sítě. Nezapomeneme také na možnosti propojení AD s dalšími zařízeními, aplikacemi a službami, protože správným využitím těchto možností lze rovněž dosáhnout optimalizace některých služeb datové sítě.

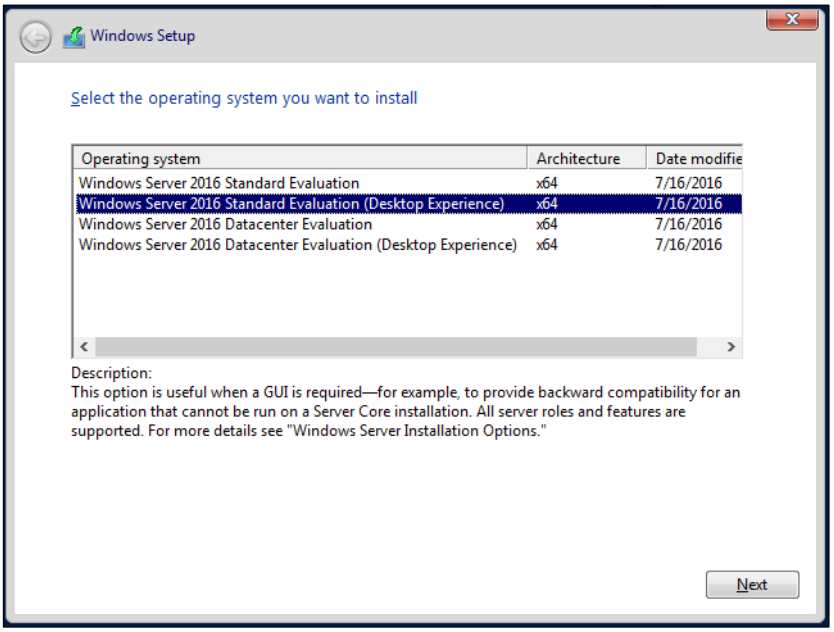
Nyní jsme nastínili, čím se v této kapitole budeme zabývat. Úvodem ještě považujeme za vhodné zmínit, že realizaci návrhu budeme provádět pomocí **virtuálních stanic**, vytvořených pomocí aplikace **VirtualBox**, které nám poslouží jakožto simulace skutečných stanic, tvořících datovou síť školy. V textu této kapitoly jsou, za účelem zvýšení jeho přehlednosti, kurzívou vyznačeny názvy nástrojů, které nám zvolený operační systém nabízí a rovněž přesná znění voleb, které v průběhu praktické realizace návrhu učiníme. V tuto chvíli již přistoupíme k prvnímu z kroků, vedoucích k praktické realizaci našeho návrhu.

8.1 Instalace a konfigurace prvního doménového řadiče

Jak jsme již stanovili v páté kapitole práce, naše DC budou disponovat operačním systémem **Microsoft Windows Server 2016**. V kapitole sedmé jsme dále jako vhodnou edici tohoto operačního systému zvolili edici **Standard**. Nyní tedy tento operační systém využijeme pro zprovoznění prvního z našich DC. Považujeme za vhodné zmínit, že na oba DC nainstalujeme zvolený operační systém ve verzi **Evaluation**, kterou společnost Microsoft nabízí k vyzkoušení na dobu 180 dní zdarma, a rovněž to, že zvolená verze neobsahuje českou lokalizaci, a proto budeme pracovat s anglickou verzí systému. Tento fakt by však neměl negativním způsobem ovlivnit čtenářovo porozumění textu, protože se v něm bude setkávat zejména s anglickými pojmy, které mají spojitost s IT problematikou, a které by tedy cílová skupina práce měla znát. V případech, kdy to považujeme za vhodné, však v závorce za textem v anglickém jazyce přidáváme jeho překlad do češtiny.

8.1.1 Instalace operačního systému

Začneme tedy instalací operačního systému. Tato část bude spíše stručná, a to z toho důvodu, že se postup instalace zvoleného serverového operačního systému příliš neliší od postupu instalace operačních systémů společnosti Windows, určených pro klientské stanice, který by cílová skupina této práce měla dobře znát. Zmíníme však jednu důležitou volbu, kterou nám instalace serverového operačního systému na rozdíl od instalace klientských operačních systémů nabízí, a tou je volba prostředí, které si přejeme nainstalovat. Součástí instalace zvoleného operačního systému je tabulka, kterou uvádíme níže.



Obrázek 9: Volba operačního systému k instalaci

Na obrázku 9 vidíme, že máme na výběr dvě varianty (pro zvolenou edici Standard). První varianta nabízí možnost nainstalovat **pouze jádro** operačního systému, bez desktopového, tedy grafického, prostředí. Volbou druhé varianty dojde k instalaci zvoleného operačního systému **včetně desktopového prostředí**.

Za výhodu první volby považujeme nižší nároky na HW prostředky, jak lze vidět v **tabulce 3**, která je k nalezení v podkapitole 7.1 této práce. Významnou nevýhodu této volby však shledáváme ve faktu, který ve svém díle rovněž uvádí Minasi (2014, s. 26), a to, že pro práci s jádrem operačního systému je předpokladem schopnost administrátora obsluhovat server pomocí příkazového řádku a rovněž znalost technik pro vzdálenou správu serveru, což vzhledem k cílové skupině této práce (správci školních datových sítí, případně další osoby disponující obecným přehledem v oboru IT) nepovažujeme za samozřejmost. Další nevýhodou instalace pouze jádra operačního systému, která je zmíněna v průběhu instalace, a kterou rovněž

uvádí například Štěrba (2014, p. 5) je, že operační systém v takovém případě nepodporuje všechny role, které by podporoval v případě instalace úplné (instalace včetně desktopového prostředí).

Vzhledem k uvedeným informacím volíme druhou z variant – **instalaci operačního systému včetně desktopového prostředí**. Mírně vyšší nároky na HW vybavení serveru považujeme, vzhledem k výkonu většiny dnes prodávaných serverů, za zanedbatelné.

Po učinění zmíněné volby již instalace probíhá podobným způsobem, jako v případě klientských operačních systémů řady Microsoft Windows. Jediným z rozdílů, který považujeme za důležitý, je fakt, že na konci instalace je potřeba povinně zvolit heslo pro účet administrátora, což v případě klientských operačních systému zmíněného výrobce není běžné. Tento účet má rovněž stanovené uživatelské jméno **Administrator**, které není možné změnit.

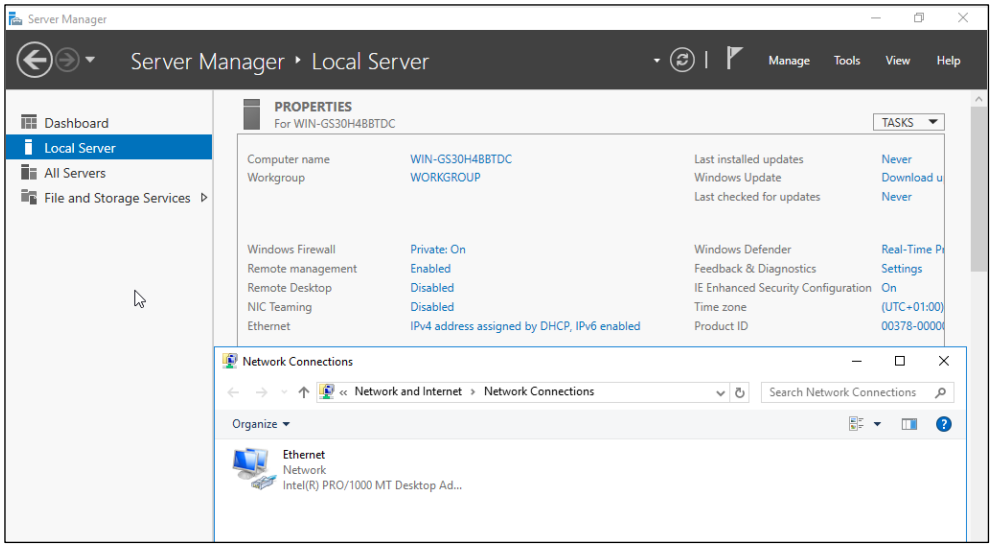
Dále budeme vycházet ze stavu, kdy máme nainstalován server s operačním systémem Windows Server 2016 Standard včetně desktopového prostředí. Domníváme se, že nám nyní nic nebrání v tom, abychom přistoupili ke konfiguraci serveru.

8.1.2 Nastavení statické IP adresy a názvu serveru

Prvními důležitými kroky, které je potřeba po instalaci serveru učinit, jsou nastavit serveru statickou IP adresu a změnit jeho název, což například Minasi uvádí mezi takzvanými *„Common Configuration Tasks“* (2014, p. 45), tedy běžnými konfiguračními úkoly, které je potřeba provést vždy při konfiguraci nového serveru. Mezi těmito úkoly autor dále uvádí, mimo jiné, také aktivaci operačního systému. To je však záležitost, kterou pokládáme za samozřejmou po instalaci kteréhokoliv z operačních systémů Windows (nejen serverových), a proto se jí zde nebudeme zabývat.

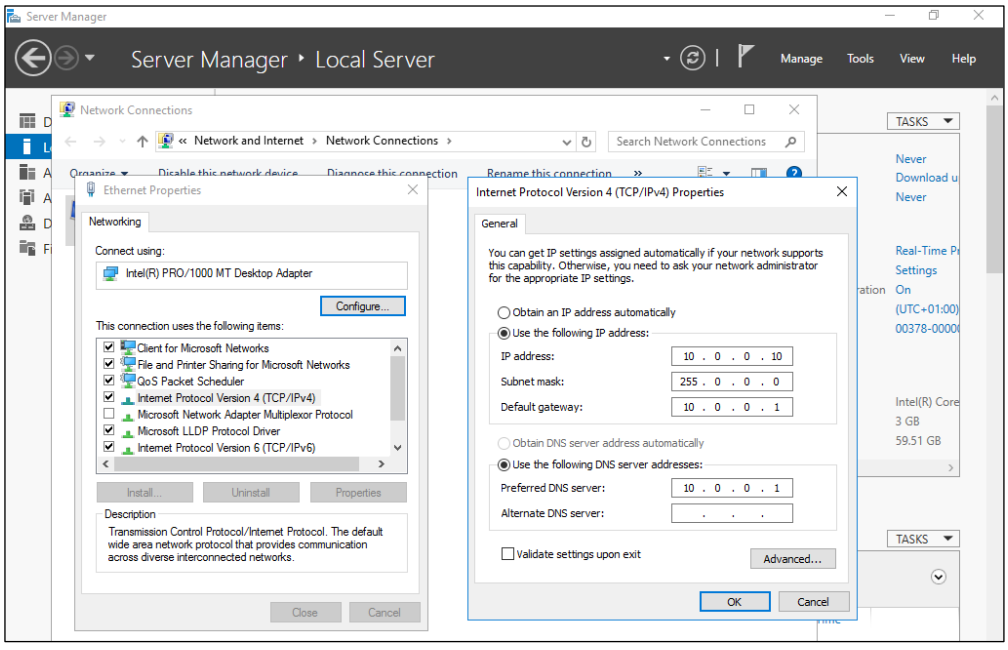
Nastavení statické IP adresy je důležité z toho důvodu, aby bylo možné server v datové síti jednoznačně identifikovat. Po instalaci zvoleného operačního systému je defaultně nastaveno získávání IP adresy z DHCP serveru. Toto nastavení je tedy potřeba změnit. Před tím, než zvolíme IP adresu, kterou použijeme pro náš server, považujeme za vhodné zmínit dvě základní podmínky, které musí být pro volbu vhodné IP adresy splněny. Zvolená IP adresa musí být z adresního rozsahu, který je vyhrazen pro zařízení v síti. Dále bychom se měli vyhnout adresám, které jsou již přiděleny jiným síťovým prvkům (například výchozí brána bývá často první adresou rozsahu adres a adresa DHCP serveru je často adresou poslední), abychom se vyhnuli konfliktu IP adres. My jsme pro náš server zvolili IP adresu **10.0.0.1**.

Nyní přejdeme k samotnému nastavení statické IP adresy. To lze učinit s pomocí nabídky *Server Manager*, která se nám zobrazí hned po přihlášení administrátora do operačního systému. Toto okno se dá rovněž vyvolat tak, že klikneme na ikonu *Start* a vybereme volbu *Server Manager*. V levém menu okna *Server Manager* klikneme na položku *Local Server* a poté na odkaz, který se nachází vedle nápisu *„Ethernet“*.



Obrázek 10: Nastavení Ethernet připojení

Zde klikneme pravým tlačítkem na ikonu *Ethernet* a zvolíme možnost *Properties*. Objeví se nám okno, kde potřeba označit možnost *Ethernet Protocol Version 4 (TCP/IPv4)* a poté kliknout na tlačítko *Properties*. Tato volba vyvolá tabulku, kde můžeme nastavit statickou IP adresu a rovněž další údaje, nutné pro komunikaci serveru v rámci datové sítě školy.

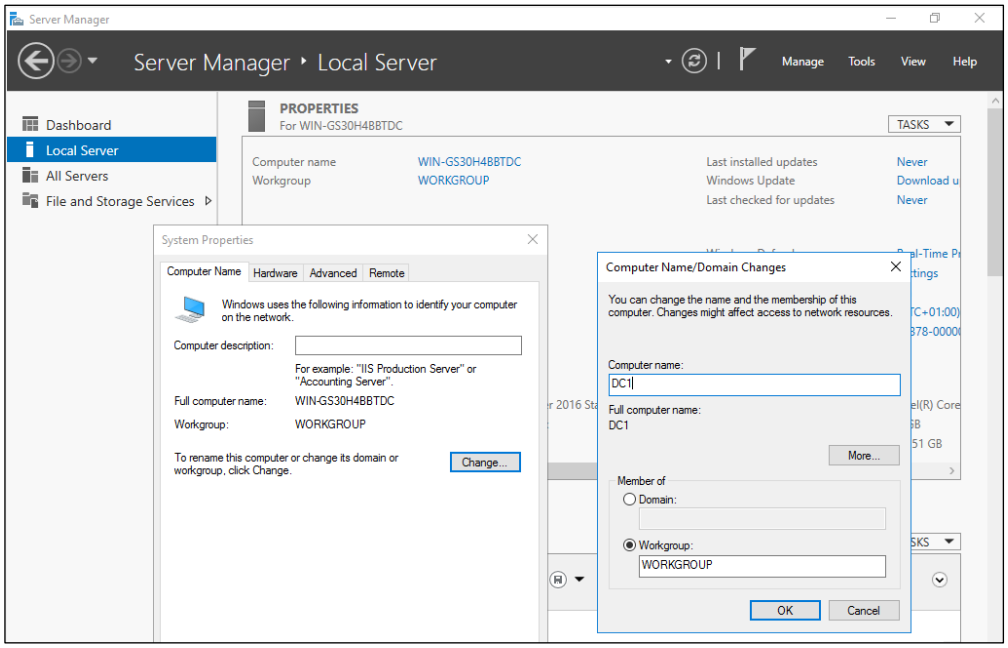


Obrázek 11: Nastavení síťových údajů

Nastavené hodnoty poté potvrdíme kliknutím na tlačítko *OK*. Po tomto potvrzení má náš server nastavenu statickou IP adresu. Nyní přistoupíme k volbě a nastavení názvu serveru.

Důležitým faktem, který v této chvíli považujeme za nutné zmínit, je, že každé zařízení v datové síti musí mít svůj **unikátní název**, aby mohlo být jasně identifikováno ze strany služby DNS, díky čemuž je poté možno s tímto zařízením jednoduše pracovat v AD. Při volbě názvu serveru nejsme omezeni žádnou stanovenou konvencí, a máme tedy mnoho možností, jak server pojmenovat. To potvrzuje rovněž Minasi (2014, p. 50), který uvádí, že každá firma má své vlastní způsoby, které využívá při volbách názvů serverů. My se domníváme, že by název serveru měl být jednoduchý a výstižný, a proto jsme zvolili název **DC1**.

K možnosti změny názvu serveru se lze dostat následujícím způsobem. V záložce *Local Server* nabídky *Server Manager* klikneme na odkaz, který se nachází vedle nápisu *„Computer name“*. Na obrazovce se poté objeví okno, ve kterém klikneme na tlačítko *Change*. To vyvolá další tabulku, kde lze dříve zvolený název serveru nastavit.



Obrázek 12: Změna názvu serveru

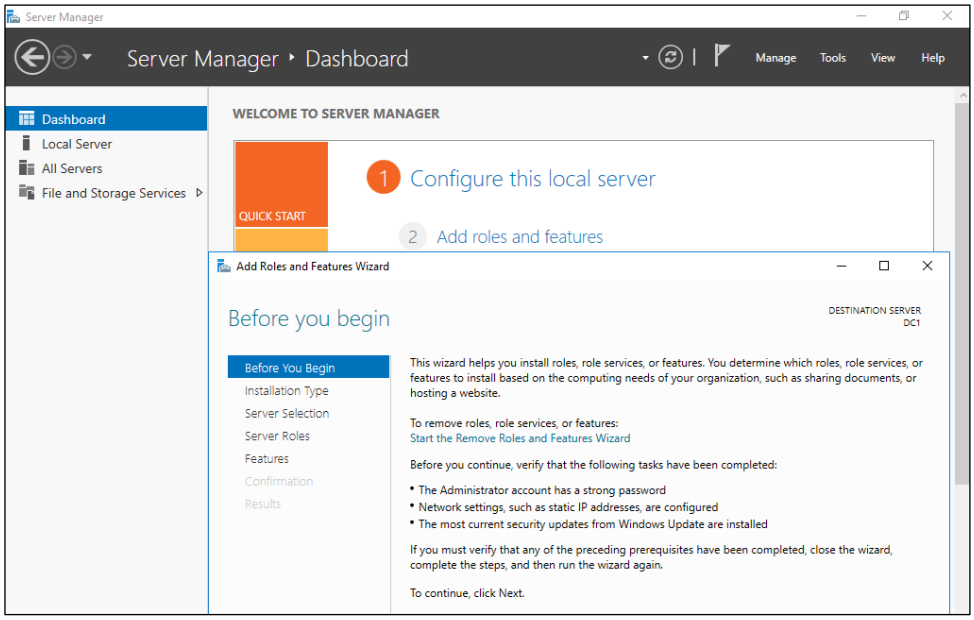
Po kliknutí na tlačítko *OK* jsme vyzváni k restartování počítače. Po opětovném načtení operačního systému je změna názvu serveru dokončena.

V této podkapitole jsme provedli základní nastavení, která je potřeba před další konfigurací serveru provést. Domníváme se, že nyní již můžeme provést první z částí konfigurace serveru, které jsou specifické pro přípravu DC.

8.1.3 Přidání role Active Directory Domain Services (AD DS)

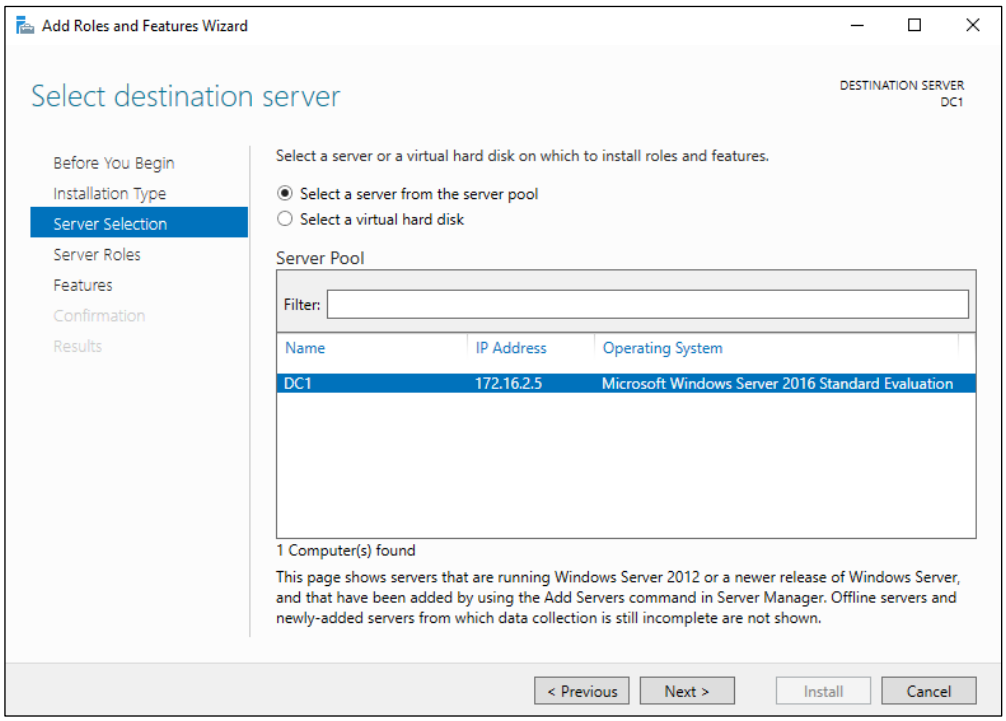
V této chvíli jsme ve fázi, kdy máme server s nainstalovaným operačním systémem, nastavenou statickou IP adresou, a vhodně zvoleným a nastaveným názvem. Abychom však mohli tento server později povýšit na DC, potřebujeme mu přidat roli Active Directory Domain Services (dále jen AD DS). Přidáním této role se budeme nyní zabývat.

Vyvoláme nabídku *Server Manager* a otevřeme její záložku *Dashboard*. Zde vybereme možnost *Add roles and features*. Kliknutím na zmíněnou možnost se nám objeví okno *Add Roles and Features Wizard*.



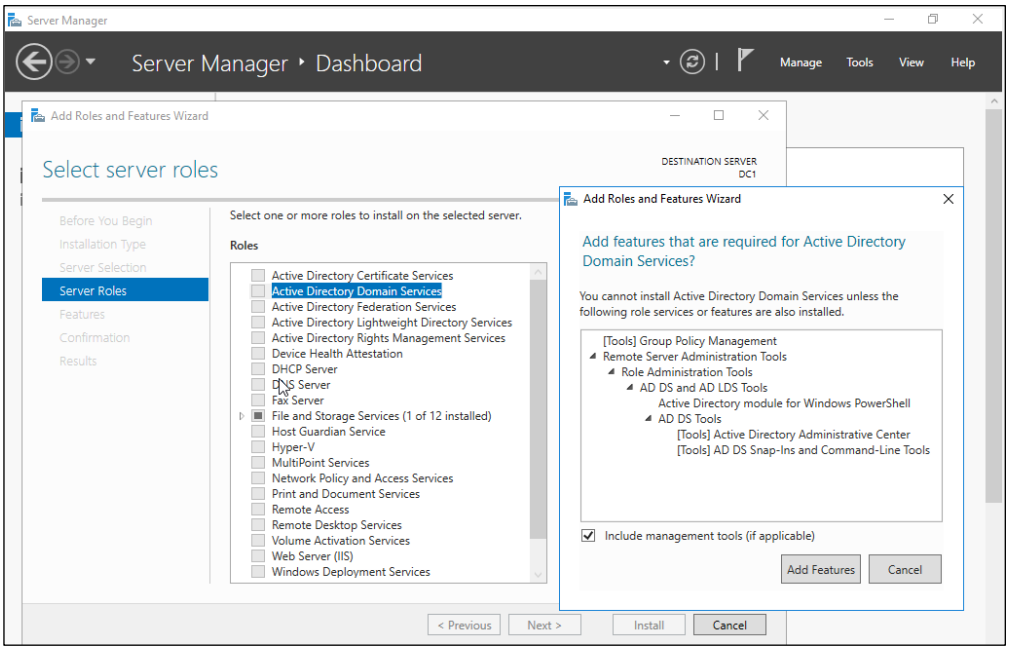
Obrázek 13: Přidání role AD DS serveru DC1 - 1

V menu na levé straně okna jsou k vidění záložky obsahující nastavení, kterých lze využít při přidávání rolí serveru. Lze mezi nimi přepínat pomocí tohoto menu, nebo pomocí tlačítek v dolní části okna. V záložce *Installation Type* ponecháme zvolenu možnost *Role-based or feature-based installation* a pokračujeme do záložky *Server Selection*. Zde pouze zvolíme náš server.



Obrázek 14: Přidání role AD DS serveru DC1 - 2

Poté pokračujeme do záložky *Server Roles*, kde vybereme možnost *Active Directory Domain Services*. Zatržením příslušného políčka vyvoláme okno s výpisem všech funkcí a služeb, které se nám nainstalováním role AD DS nainstalují. Jak vidíme na obrázku 15, nenainstaluje se pouze role AD DS, ale rovněž s ní související funkce a služby.

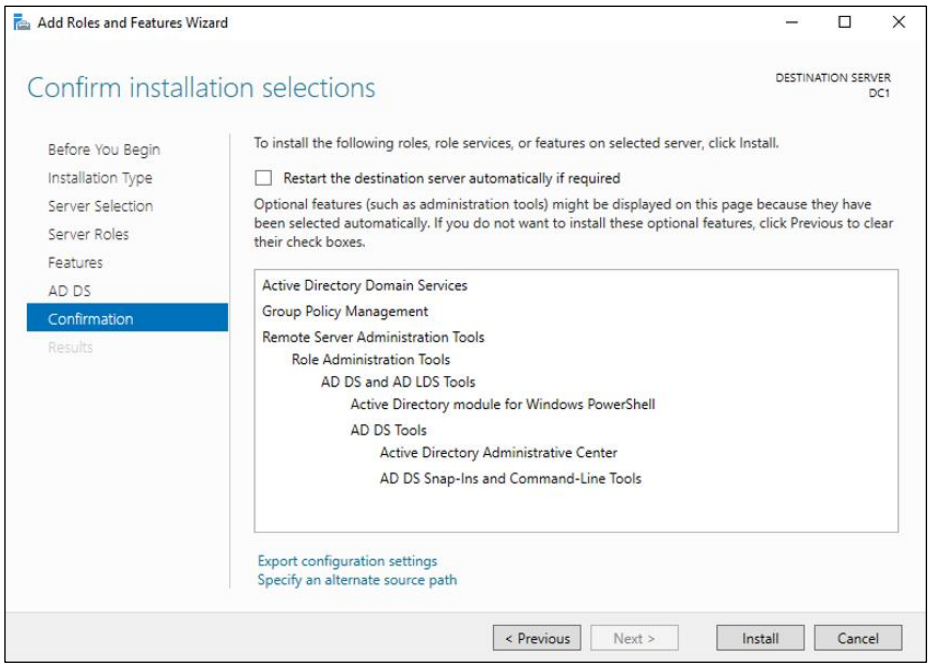


Obrázek 15: Přidání role AD DS serveru DC1 - 3

Ve vyvolaném okně klikneme na tlačítko *Add Features*. Poté se nám v levém menu okna *Add Roles and Features Wizard* objeví nová volba *AD DS*.

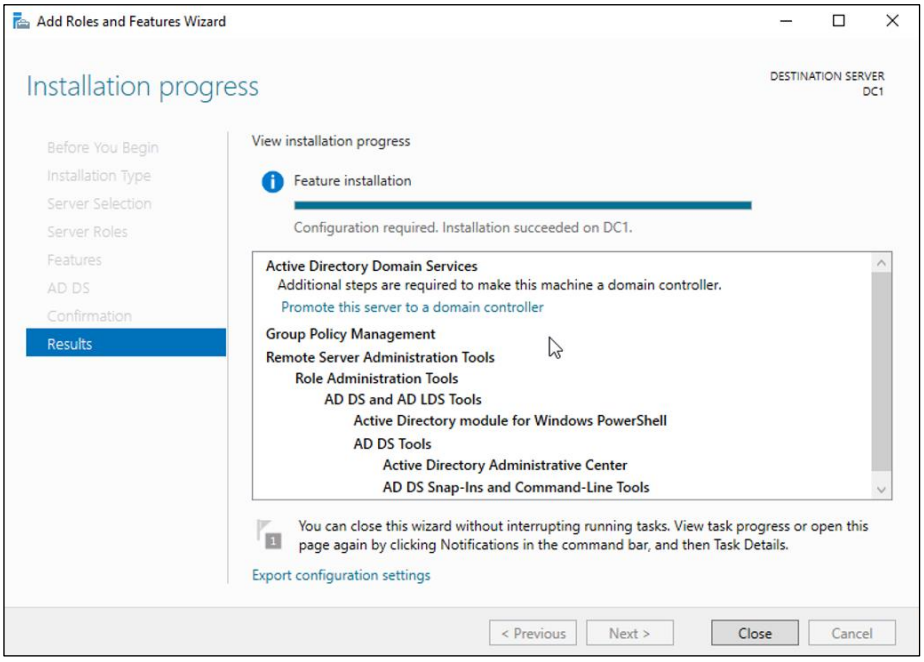
Nastavení v záložkách *Features* a *AD DS* ponecháme beze změny. Považujeme však za vhodné zmínit, že v záložce AD DS lze nalézt užitečné informace ohledně funkcionality a provozu instalované služby.

V záložce *Confirmation* vidíme výpis všech rolí, funkcí a služeb, připravených k instalaci. Kliknutím na tlačítko *Install* instalaci potvrdíme.



Obrázek 16: Přidání role AD DS serveru DC1 - 4

Tímto potvrzením dojde ke spuštění instalace. Po jejím dokončení zvolíme tlačítko *Close*.



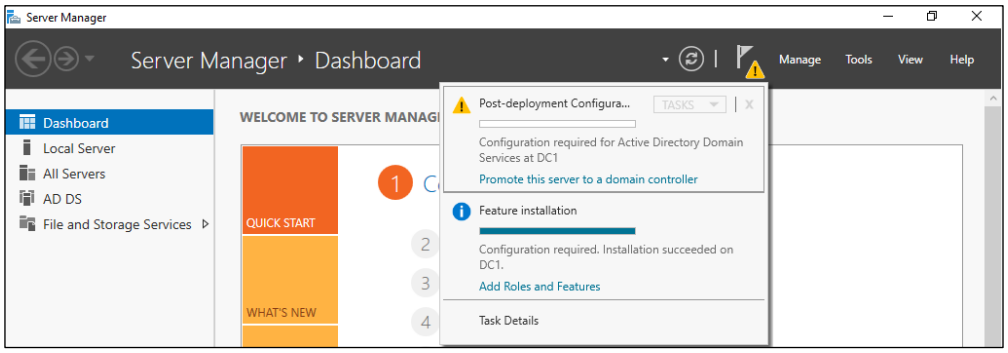
Obrázek 17: : Přidání role AD DS serveru DC1 - 5

Tímto jsme dokončili proces přidání role AD DS serveru DC1. Domníváme se, že je nyní vše připraveno k povýšení serveru na DC a rovněž k vytvoření domény.

8.1.4 Povýšení serveru na doménový řadič a vytvoření domény

V této podkapitole povýšíme server DC1 na DC a rovněž vytvoříme doménu, která je součástí návrhu logické struktury školní datové sítě, vytvořeného v šesté kapitole práce. Postup tentokrát uvedeme v bodech, na které budeme později, v průběhu přípravy druhého DC, odkazovat.

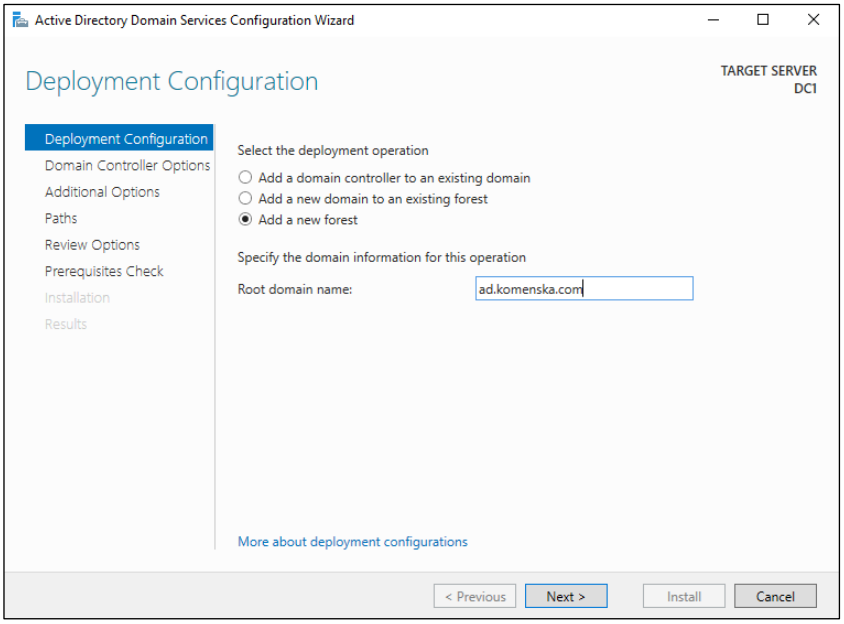
1. Klikneme na ikonu *Notifications*, která je umístěna na horním panelu nabídky *Server Manager*, a zde zvolíme odkaz s textem *„Promote this server to a domain controller“*.



Obrázek 18: Povýšení serveru DC1 na DC - 1

Kliknutím na odkaz vyvoláme okno *Active Directory Domain Services Configuration Wizard*. Toto okno, stejně jako okno *Add Roles and Features Wizard*, obsahuje menu se záložkami, nabízejícími různá nastavení, umístěné na levé straně.

2. V záložce *Deployment Configuration* zvolíme možnost *Add a new forest*, protože zatím nemáme vytvořen žádný doménový strom. Do pole, nacházejícího se vedle textu *„Root domain name“* (název kořenové domény) zadáme název domény našeho návrhu, stanovený v podkapitole 6.3 této práce.

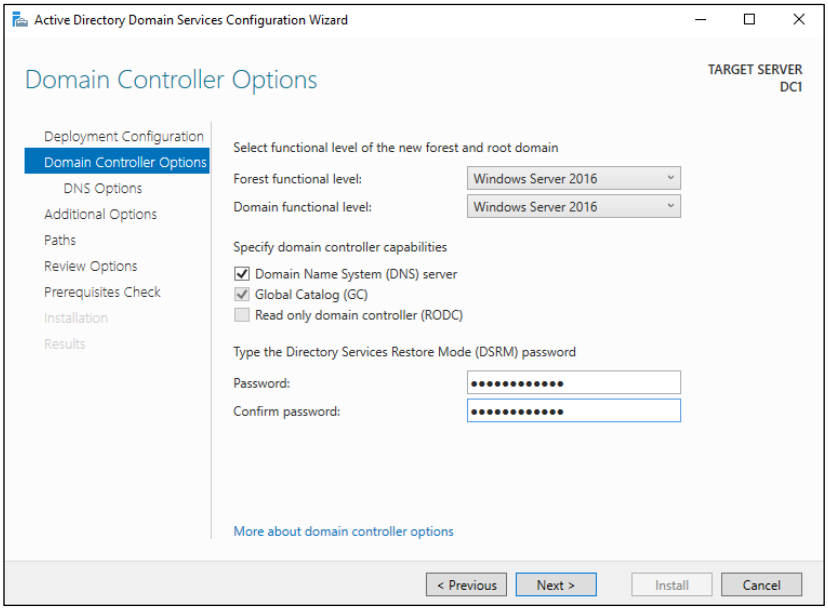


Obrázek 19: Povýšení serveru DC1 na DC - 2

3. Pokračujeme do záložky *Domain Controller Options*. Zde máme možnost nastavit *Forest functional level (*úroveň funkčnosti doménové struktury) a rovněž *Domain functional level* (úroveň funkčnosti domény). V páté kapitole jsme jako nejvýhodnější z úrovní funkčnosti domény zvolili úroveň **Windows Server 2016** a tu tedy v příslušném boxu zvolíme. Jako úroveň funkčnosti doménové struktury zvolíme rovněž úroveň **Windows Server 2016**.

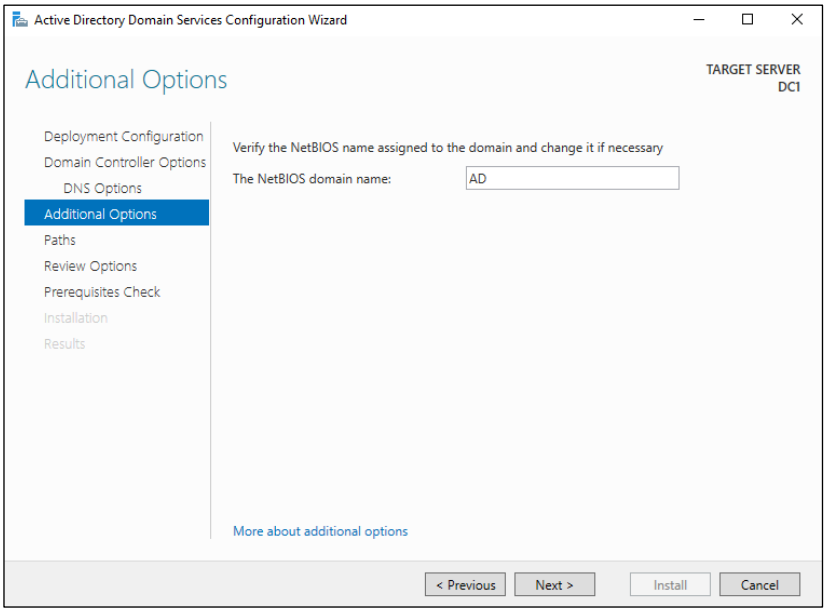
   Dále máme v této záložce možnost nastavit, zda má být na server nainstalována služba DNS, či nikoliv. Jak jsme uvedli v podkapitole 7.3, služba AD využívá službu DNS ke své funkci, a proto ji na server nainstalujeme. Zkontrolujeme proto, zda je zatržena možnost *Domain Name System (DNS) server*. Zde považujeme za důležité zmínit, že pokud by se naší datové síti DNS server již nalézal, nebylo by nutné službu DNS na server instalovat.

   Posledním úkonem, který musíme v této záložce provést, je nastavení takzvaného **Directory Services Restore Mode password**. Toto heslo je vyžadováno pro některé servisní zásahy, a proto je potřeba si jej dobře zapamatovat.



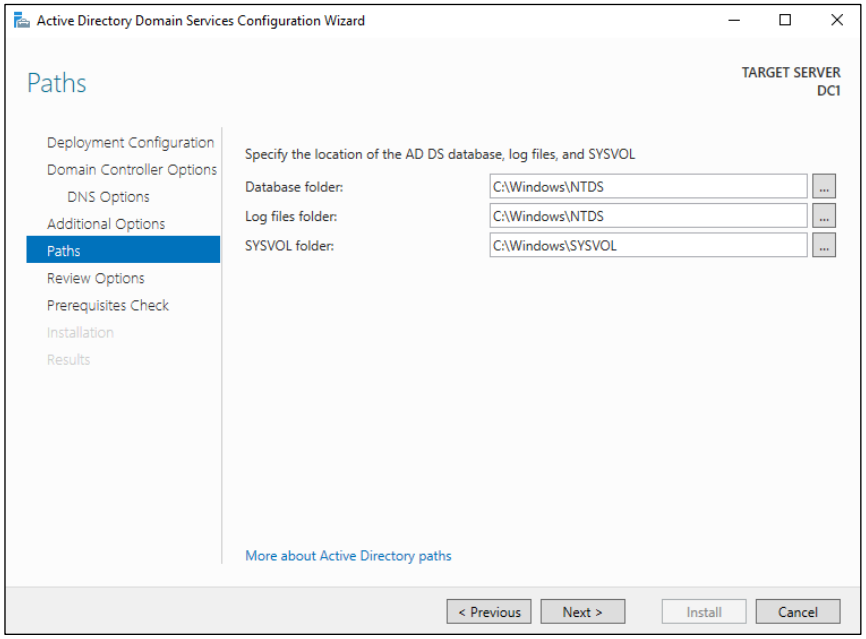
Obrázek 20: Povýšení serveru DC1 na DC - 3

4. V záložkách *DNS Options* a *Additional Options* není potřeba cokoli nastavovat. V záložce *Additional Options* pouze potvrdíme vygenerované **NetBIOS domain name**.



Obrázek 21: Povýšení serveru DC1 na DC - 4

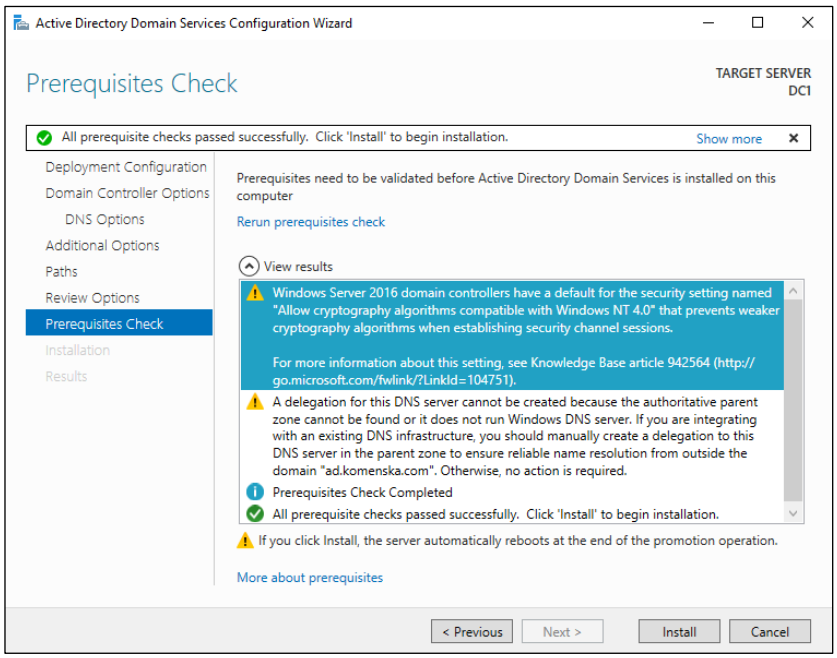
5. V záložce *Paths* máme možnost nastavit cesty pro ukládání databáze, souborů s logy a SYSVOL (system volume). V této chvíli považujeme za vhodné ponechat defaultně nastavené hodnoty, a proto rovnou přejdeme do další záložky.



Obrázek 22: Povýšení serveru DC1 na DC - 5

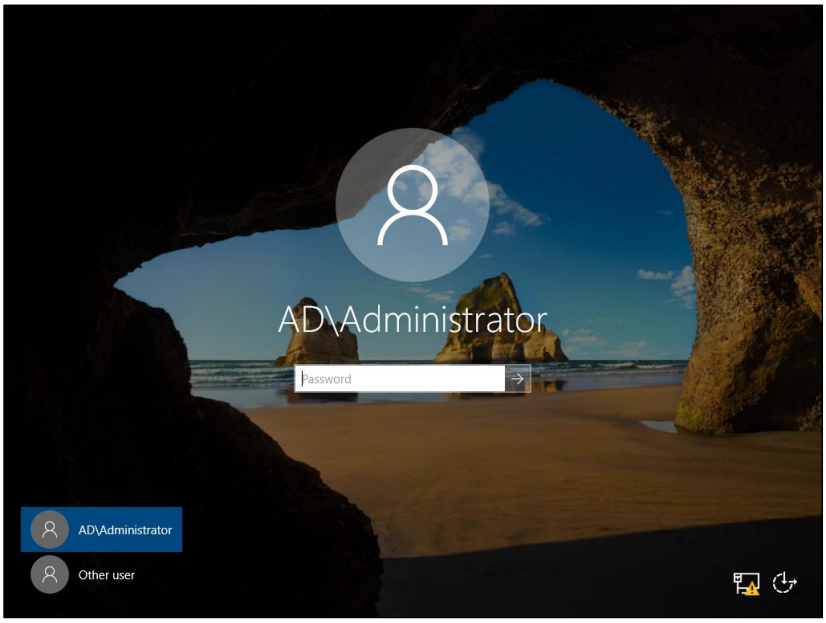
6. Záložka *Review Options* nabízí k nahlédnutí shrnutí provedených nastavení. Za zmínku zde stojí možnost vyexportovat PowerShell skript, obsahující námi dříve provedená nastavení, který může být použit pro povýšení dalších serverů na DC, a to včetně serverů, které disponují pouze jádrem operačního systému. Přehled potvrdíme a pokračujeme k záložce *Prerequisites Check*.

7. V záložce *Prerequisites Check* proběhne kontrola předpokladů pro povýšení serveru na DC. V případě úspěšné kontroly můžeme kliknout na tlačítko *Install*, kterým spustíme proces, vedoucí k povýšení serveru na DC. V případě neúspěšné kontroly je potřeba nejprve odstranit problémy a až poté je možnost server povýšit. V tuto chvíli ještě považujeme za vhodné zmínit, že v průběhu instalace dojde k restartování serveru.



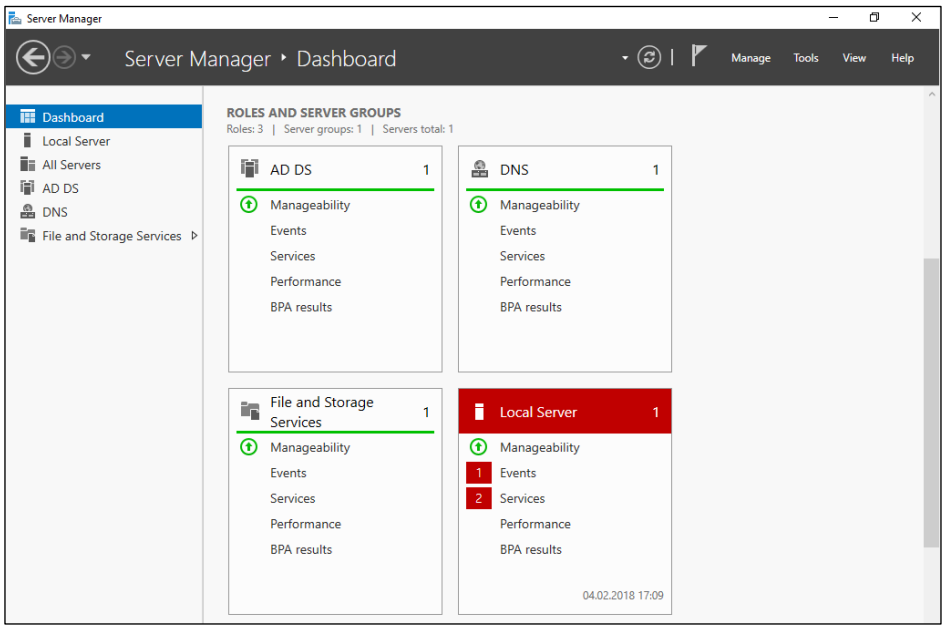
Obrázek 23: Povýšení serveru DC1 na DC - 6

8. Po restartu serveru již na úvodní obrazovce vidíme, že je nám nabídnuto přihlášení k doméně **AD**. To značí, že byl proces povýšení serveru na DC úspěšný.



Obrázek 24: Obrazovka pro přihlášení k doméně

9. Po přihlášení do operačního systému vidíme v záložce *Dashboard* nabídky *Server Manager* nově přidané role.



Obrázek 25:Nabídka Server Manager s nově přidanými rolemi

Instalace proběhla úspěšně, čímž máme připraven první z plánovaných DC a rovněž vytvořenu doménu. Nyní považujeme za vhodné přejít k přípravě druhého DC, jehož použití, jak jsme již uvedli v podkapitole 7.1, zajistí vyšší spolehlivost našeho řešení.

8.2 Instalace a konfigurace druhého doménového řadiče

V této podkapitole si připravíme druhý z dvojice DC. Druhý DC bývá někdy označován jako **replica domain controller**, tedy DC repliky. Jak už toto označení napovídá, mezi oběma DC bude probíhat pravidelná **replikace dat**. Díky tomu nebude mít výpadek kteréhokoliv z dvojice DC zásadní vliv na kvalitu služeb, poskytovaných ze strany datové sítě. Úvodem považujeme za vhodné zmínit, že instalace i konfigurace druhého DC mají do značné míry stejný průběh, jako instalace a konfigurace toho prvního, a proto se v této kapitole budeme zabývat zejména úkony, pro přípravu druhého DC specifické.

Postup instalace operačního systému je v případě druhého serveru stejný, jako tomu bylo v případě serveru prvního, a proto nepovažujeme za důležité se jím zde příliš zabývat. Pouze zmíníme, že i zde zvolíme variantu **instalace včetně desktopového prostředí**, a to ze stejných důvodů, jako jsme uvedli v podkapitole 8.1.1.

Našemu druhému serveru bude opět potřeba nastavit **statickou IP adresu** a **vhodný název**. Postup těchto úkonů je detailně popsán v podkapitole 8.1.2. My zde tedy pouze zmíníme údaje, které druhému serveru nastavíme. IP adresa druhého serveru bude **10.0.0.11**. Jako *preferred DNS server* (upřednostňovaný DNS server) je v tomto případě potřeba nastavit server DC1. Do příslušného pole tedy zadáme IP adresu 10.0.0.10. Jako *alternate DNS server* (alternativní

DNS server) nastavíme IP adresu právě konfigurovaného serveru. Do příslušného pole zadáme IP adresu 10.0.0.11. Další údaje, týkající se komunikace serveru v rámci datové sítě, použijeme stejné, jako jsme použili v podkapitole 8.1.2. Serveru jsme dále zvolili název **DC2**.

Aby mohl být druhý server povýšen na DC, musíme mu, stejně jako dříve prvnímu serveru, přidat roli **AD DS**. To učiníme způsobem, který byl detailně popsán v podkapitole 8.1.3.

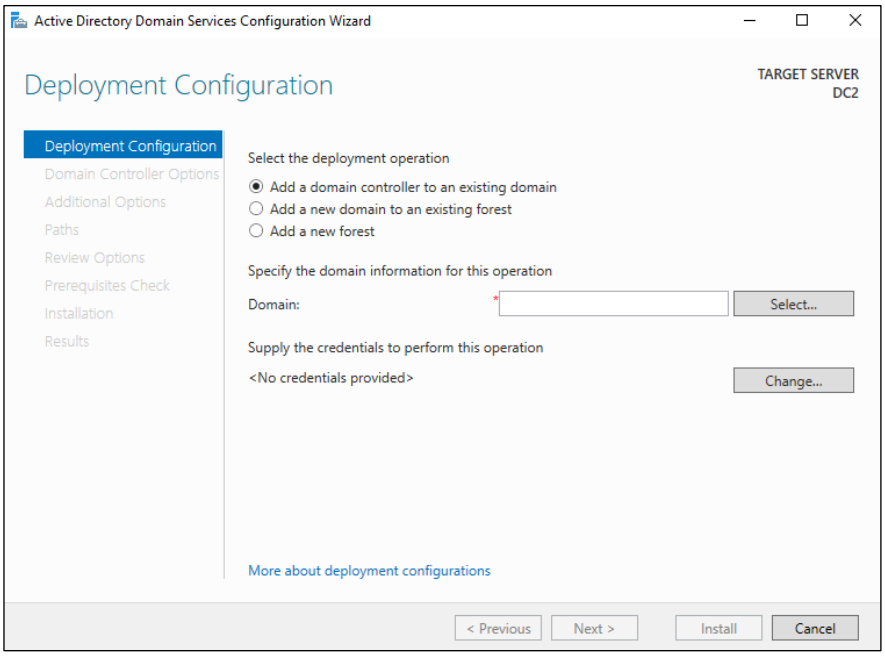
Až do této chvíle byl postup přípravy druhého serveru totožný s postupem přípravy toho prvního. Nyní se však dostáváme do bodu, kdy musíme pro dosažení kýženého výsledku zvolit postup odlišný.

8.2.1 Povýšení serveru na doménový řadič a přidání serveru do domény

Nyní tedy povýšíme náš dříve připravený server na DC a rovnou jej přidáme do dříve vytvořené domény.

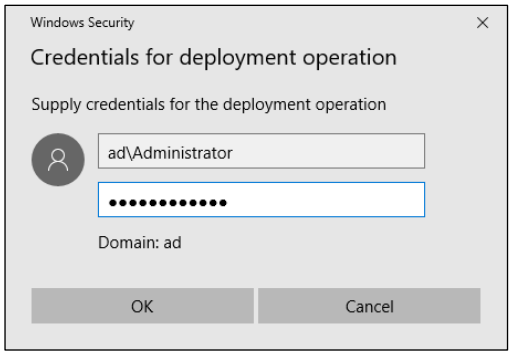
Nejprve způsobem, popsaným v prvním bodě postupu povýšení serveru DC1 na DC v podkapitole 8.1.4, otevřeme okno *Active Directory Domain Services Configuration Wizard*.

V záložce *Deployment Configuration* však tentokrát ponecháme defaultně zvolenou možnost *Add a domain controller to an existing domain*, protože nechceme vytvářet novou doménu, jako tomu bylo v podkapitole 8.1.4, ale přidat tento DC do domény již vytvořené. Poté klikneme na tlačítko *Select…*, umístěné vedle nápisu *„Domain:“*, abychom vybrali dříve vytvořenou doménu.



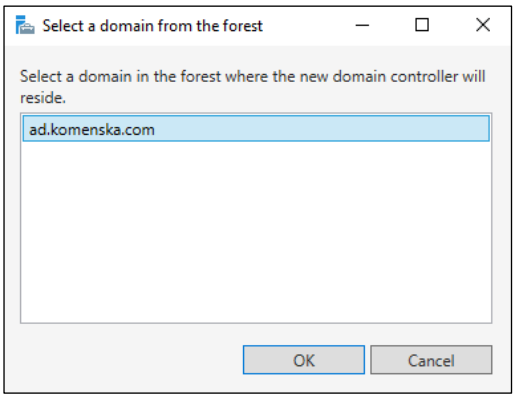
Obrázek 26: Povýšení serveru DC2 na DC - 1

Stisknutí zmíněného tlačítka vyvolá tabulku, žádající nás o **uživatelské jméno** a **heslo**. Zde zadáme přihlašovací údaje doménového administrátora. V našem případě je to uživatelské jméno **Administrator** a heslo, které jsme zvolili při instalaci operačního systému na první z dvojice serverů. V tuto chvíli považujeme za vhodné zmínit, že pro přihlášení k doméně je potřeba před uživatelským jménem uvést název dané domény. Tento název musí být od uživatelského jména oddělen pomocí zpětného lomítka. Stačí uvést pouze jeho první část. Zbytek názvu domény za nás doplní služba DNS.



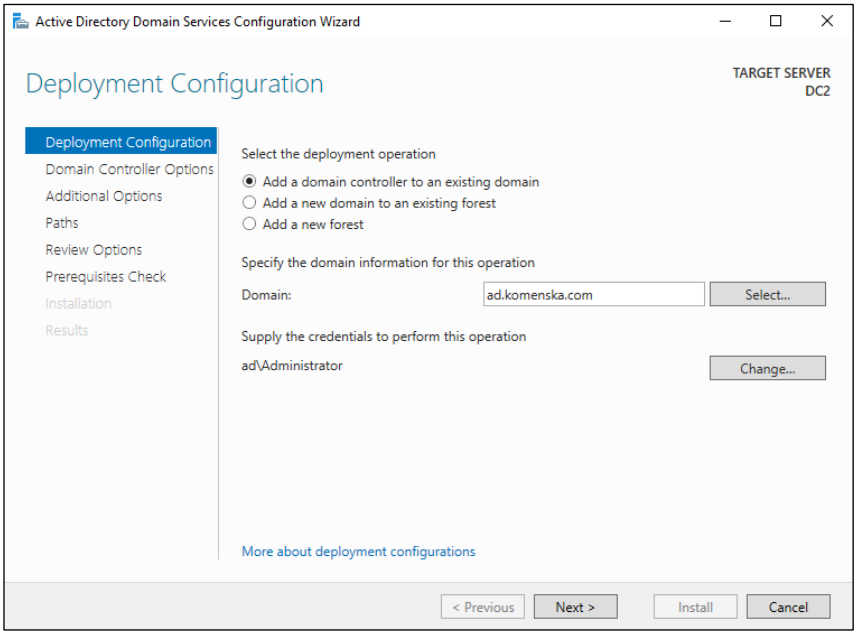
Obrázek 27: Povýšení serveru DC2 na DC - 2

Jakmile zadáme potřebné údaje, klikneme na tlačítko *OK*. Pokud jsou zadané přihlašovací údaje správné, zobrazí se nám tabulka, kde je potřeba zvolit doménu, do které chceme náš server DC2 přidat. Zvolíme tedy naši dříve vytvořenou doménu a klikneme na tlačítko *OK*.



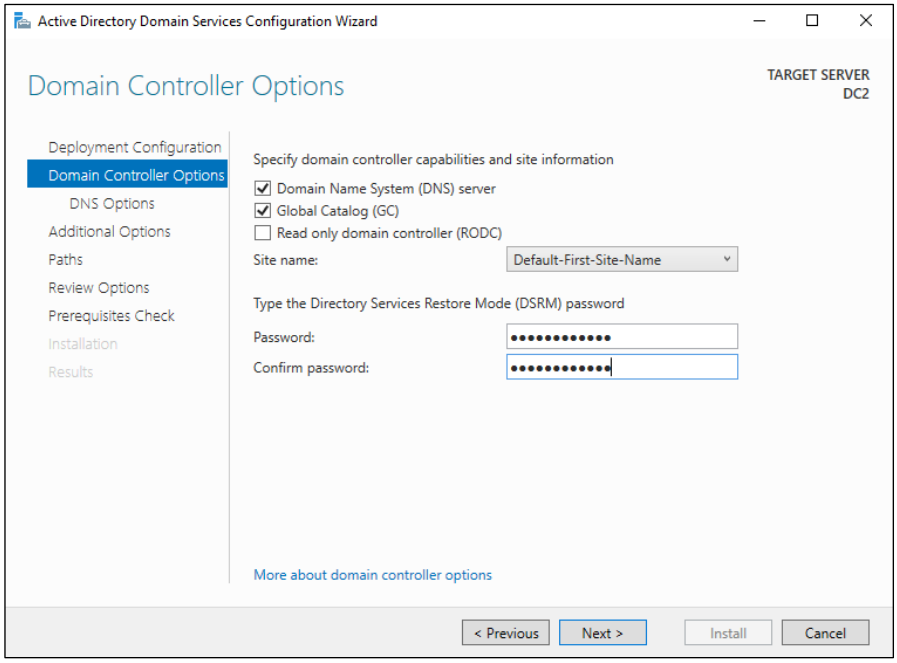
Obrázek 28: Povýšení serveru DC2 na DC - 3

Na obrázku 29 vidíme záložku *Deployment Configuration* po vyplnění všech potřebných údajů. Nyní můžeme přejít do další záložky.



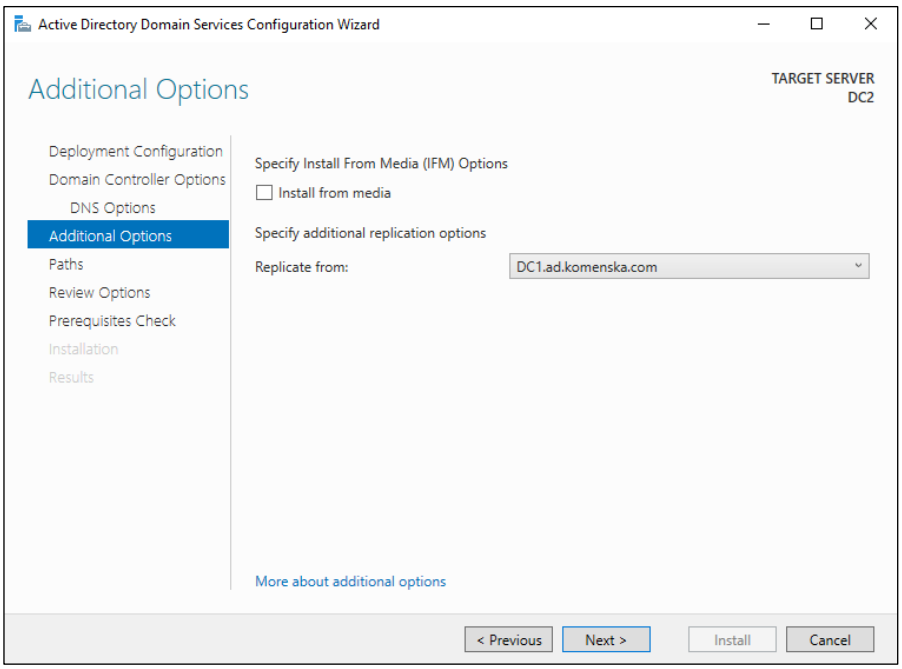
Obrázek 29: Povýšení serveru DC2 na DC - 4

V záložce *Domain Controller Options* považujeme za vhodné ponechat zatrženu možnost *Domain Name System (DNS) server*, která nám zajistí, že náš server DC2 bude, stejně jako server DC1, DNS serverem. Díky tomu zůstane dostupnost služby DNS v případě výpadku kteréhokoliv ze dvojice serverů zachována. Rovněž necháme zatrženu možnost *Global Catalog (GC)*, a to z důvodu zachování dostupnosti globálního katalogu v případě výpadku jednoho ze serverů. Dále ponecháme nezatrženu možnost *Read only domain controller (RDOC)*, přestože je jí někdy v případě DC repliky doporučeno využít. DC pouze pro čtení jsou vhodné pro lokality, kde není zajištěno fyzické zabezpečení DC, jak rovněž uvádí například Stanek (2009, s. 119). Oba naše servery však pravděpodobně budou umístěny ve stejné serverovně, a proto toto nastavení v našem případě postrádá svůj smysl. Dále v této záložce už pouze zadáme *Directory Services Restore Mode password* a přesuneme se do další záložky.



Obrázek 30: Povýšení serveru DC2 na DC - 5

V záložce *DNS Options* není potřeba cokoliv nastavovat, a proto se hned přesuneme do záložky *Additional Options*. Zde pouze nastavíme server DC1 jako server pro replikaci. Tuto možnost pokládáme z hlediska zabezpečení datové sítě za výhodnější, než defaultně zvolenou možnost *Any domain controller* (jakýkoli DC). Poté pokračujeme do další záložky.



Obrázek 31: Povýšení serveru DC2 na DC - 6

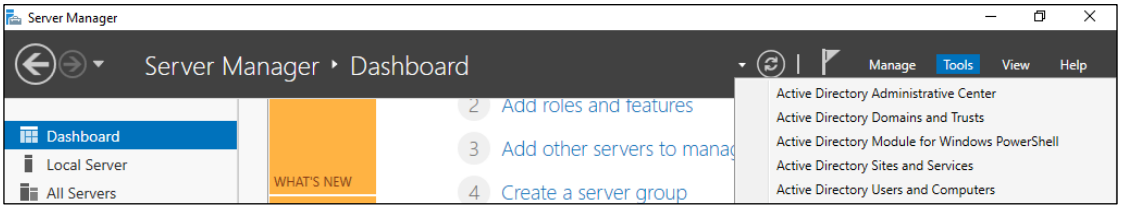
Dále už je postup povýšení serveru DC2 na DC stejný, jako v pátém až devátém bodě postupu povýšení serveru DC1 na DC, uvedeného v podkapitole 8.1.4. Z tohoto důvodu jej zde nebudeme znovu uvádět.

V této fázi tedy máme zprovozněny oba DC, a proto můžeme přejít k realizaci návrhu logické struktury školní datové sítě, který byl vytvořen v šesté kapitole této práce.

8.3 Vytvoření logické struktury školní datové sítě

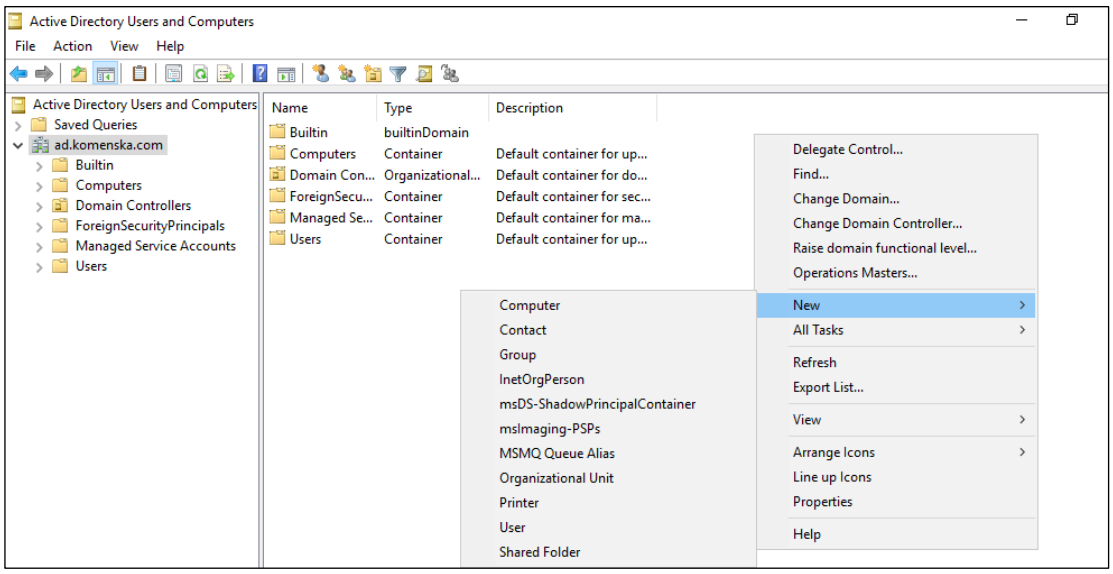
Cílem této podkapitoly je vytvořit logickou strukturu datové sítě, navrženou v šesté kapitole práce. Vytvoříme si zde tedy dvojici struktur, které zmíněnou strukturu tvoří.

K tvorbě struktur použijeme nástroj *Active Directory Users and Computers*, který slouží k jednoduché správě uživatelů a počítačů v AD. Tento nástroj lze vyvolat skrze horní menu nabídky *Server Manager*, kde se nalézá pod položkou *Tools*.



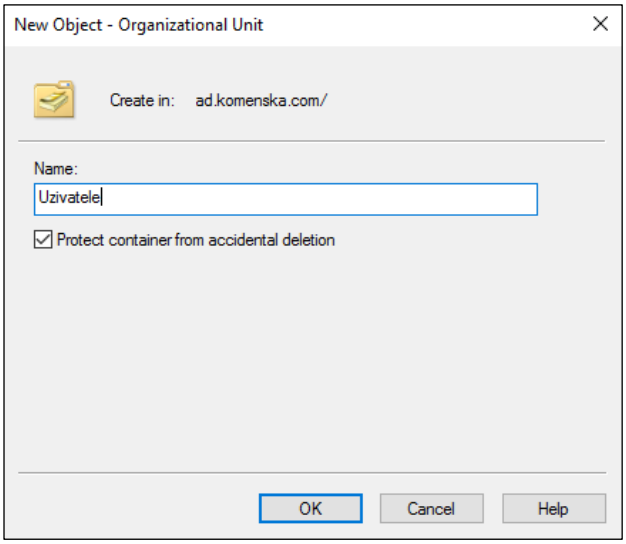
Obrázek 32: Spuštění nástroje Active Directory Users and Computers

V menu, které se nalézá na levé straně nově vyvolaného okna, klikneme na položku, která nese název naší domény. Tímto se dostaneme do náhledu, ve kterém máme možnost vytvářet OU logické struktury datové sítě. Klikneme tedy pravým tlačítkem do volného prostoru a poté zvolíme *New* a *Organizational Unit*.



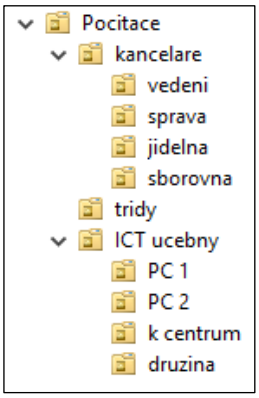
Obrázek 33: Vytvoření OU - 1

Kliknutím na položku *Organizational Unit* dojde k vyvolání okna s možností zadat název nové OU. Dále máme také možnost tuto OU zabezpečit proti odstranění z nepozornosti zatržením možnosti *Protect container from accidental deletion*. Doporučujeme toto zabezpečení využívat. V této chvíli vytvoříme první z OU navržené struktury – OU **Uzivatele**. Do pole pod textem *„Name:“* tedy zadáme název této OU a poté klikneme na tlačítko *OK*.

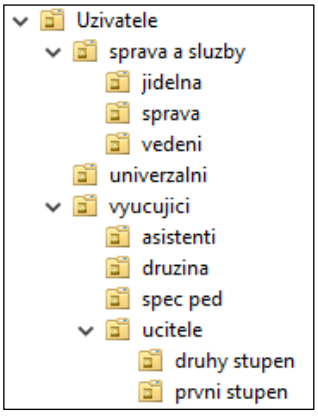


Obrázek 34: Vytvoření OU - 2

Nyní máme vytvořenu první z organizačních jednotek navržené logické struktury. Stejným způsobem vytvoříme OU, s názvem **Pocitace** a poté do každé z dvojice vytvořených OU vytvoříme, na základě dřívějšího návrhu, příslušnou strukturu.



Obrázek 36: Vytvořená struktura pro počítače



Obrázek 35: Vytvořená uživatelská struktura

Výsledek našeho počínání je k nahlédnutí výše. Vidíme, že jsme vytvořili navrženou logickou strukturu. Ta je tedy nyní připravena k použití. V tuto chvíli považujeme za vhodné přejít k tvorbě obsahu OU, kterým jsou účty objektů datové sítě.

8.4 Tvorba uživatelských účtů a nastavování jejich vlastností

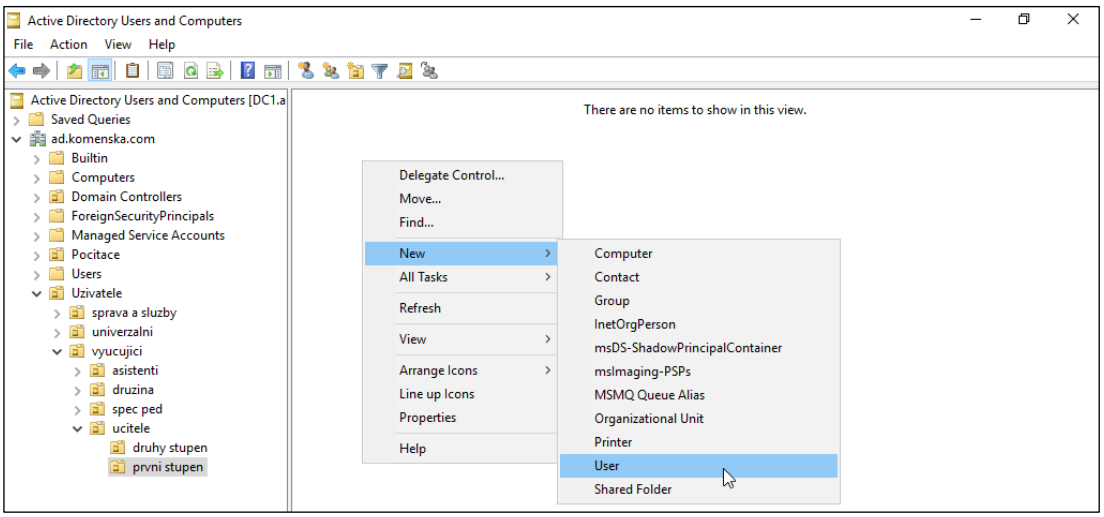
V této podkapitole se budeme zabývat nejen vytvářením uživatelských účtů, ale rovněž si nastíníme, jakým způsobem lze nastavovat jejich základní vlastností, protože se domníváme, že vhodné nastavení těchto vlastností může přispět k zefektivnění správy datové sítě a rovněž k minimalizaci bezpečnostních rizik, souvisejících s využíváním jejich služeb. Jejich nastavení tedy je, jak vidíme, v souladu s cíli navržené struktury, které jsme stanovili v podkapitole 6.2.1, a proto tato nastavení považujeme za žádoucí.

Nyní vytvoříme vzorový uživatelský účet a rovněž ukážeme, jakým způsobem se lze dostat k nastavení jeho vlastností.

8.4.1 Tvorba uživatelských účtů

K vytváření uživatelských účtů lze využít několika způsobů. Z nástrojů desktopového prostředí operačního systému Windows Server 2016 jsou to nástoje *Active Directory Users and Computers* a *Active Directory Administrative Centre*. My jsme se rozhodli využít prvního ze zmíněných nástrojů, protože považujeme jeho uživatelské rozhraní za intuitivnější a také proto, že jej dobře známe.

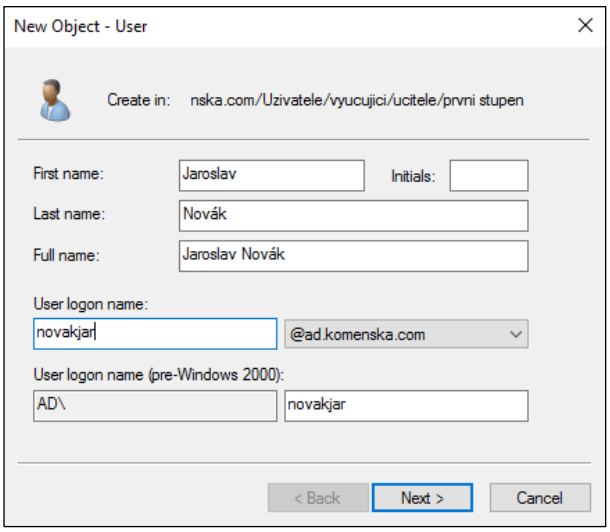
Jako vzorový uživatelský účet, na kterém si tvorbu účtů ukážeme, jsme se rozhodli vytvořit účet fiktivního uživatele **Jaroslava Nováka**, učitele prvního stupně. Otevřeme si tedy zvolený nástroj a přesuneme se do OU, do které spadá náš uživatel. Zde klikneme pravým tlačítkem do volného prostoru, a ve vyvolaném menu zvolíme *New* a poté *User*.



Obrázek 37: Tvorba uživatelského účtu - 1

Volba položky *User* vyvolá okno, kde je možné vyplnit některé základní údaje o novém uživateli. Zde považujeme za důležité vyplnit pole *First name* (křestní jméno) a *Last name*

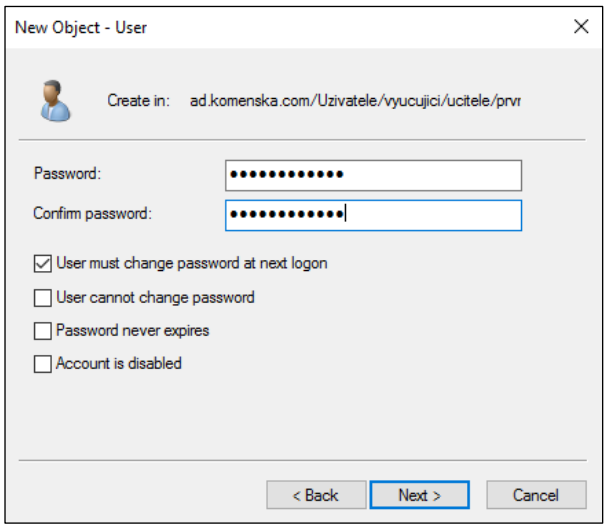
(příjmení) uživatele. Dále vyplníme pole *User logon name* (uživatelovo přihlašovací jméno), což je údaj, který bude náš nový uživatel používat pro přihlašování do domény. Pro jeho stanovení využijeme jmenné konvence, zvolené v podkapitole 6.6.1 této práce. V případě uživatele Jaroslava Nováka do pole *User logon name* zadáme *„novakjar“*.



Obrázek 38: Tvorba uživatelského účtu - 2

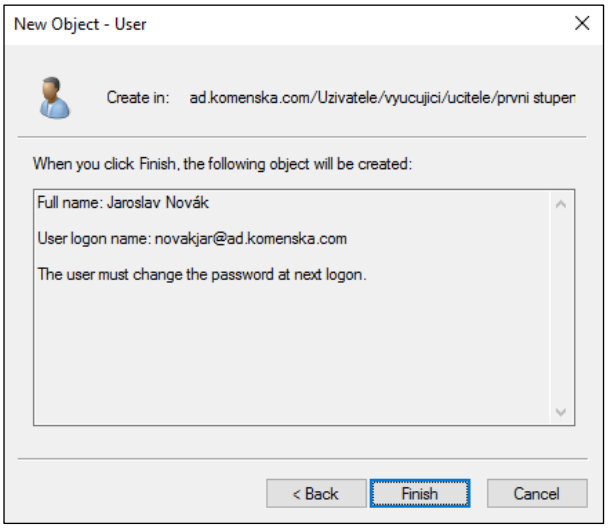
Jak vidíme na obrázku 38, po nastavení zmíněných údajů se nám automaticky doplnila pole *Full name* (celé jméno) a *User logon name (pre-Windows 2000)*. Pole *Inicials* nepovažujeme za důležité, a proto jej necháme prázdné. Nyní klikneme na tlačítko *Next*.

Nastavení, které nám nabízí další náhled, považujeme za velmi důležitá. Zde uživateli nastavujeme heslo pro přihlašování k doméně a rovněž základní pravidla, které s tímto heslem a rovněž s přihlašováním obecně souvisí. Domníváme se, že v tomto okně je vhodné uživateli nastavit heslo pouze pro první přihlášení s tím, že si po tomto přihlášení uživatel zvolí heslo vlastní. Vymyslíme tedy libovolné heslo a zatrhneme první možnost *User must change password at next logon* (uživatel musí heslo při příštím přihlášení změnit). Poté klikneme na tlačítko *Next*.



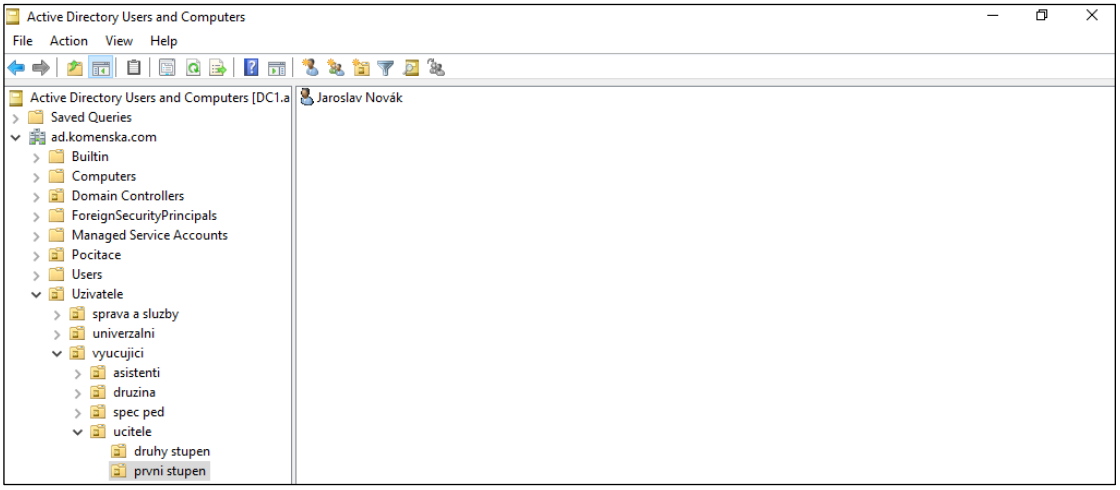
Obrázek 39: Tvorba uživatelského účtu - 3

V následující tabulce je uvedeno shrnutí nastavených údajů. Zde tedy můžeme tyto údaje zkontrolovat. Po provedení kontroly klikneme na tlačítko *Finish*.



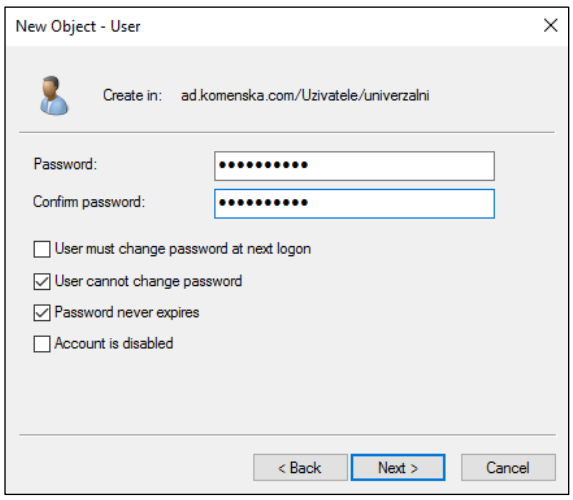
Obrázek 40:Tvorba uživatelského účtu - 4

Skutečnost, že nyní máme vytvořen náš první uživatelský účet, je zřejmá z následujícího obrázku. Stejného postupu lze využít k vytváření dalších uživatelských účtů.



Obrázek 41: Tvorba uživatelského účtu - 5

V souvislosti s tvorbou uživatelských účtů ještě považujeme za vhodné zmínit, že v případě účtů OU **univerzalni** doporučujeme ve spojení s přihlašováním využít následujících nastavení.



Obrázek 42: Nastavení přihlašování pro univerzální účty

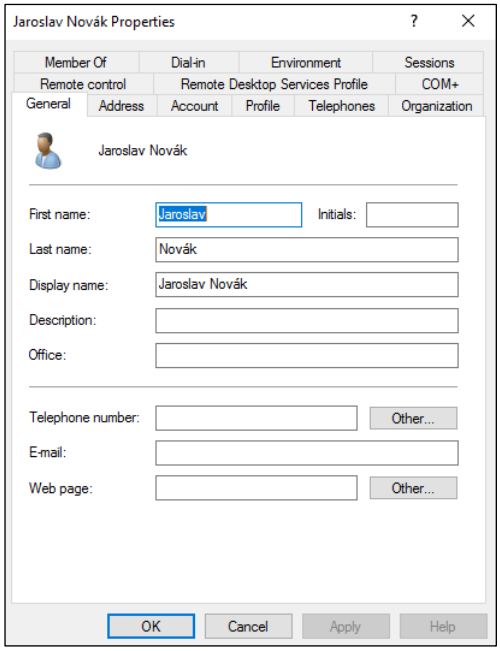
Nastavení *User cannot change password* zajistí, že žádný z fyzických uživatelů, využívajících daného univerzálního účtů, nebude mít možnost změnit přihlašovací heslo, a tedy znemožnit ostatním fyzickým uživatelům přihlášení k doméně. Dále je vhodné zvolit možnost *Password never expires*, aby mělo heslo neomezenou délku platnost.

Nyní jsme se, dle našeho názoru, dostatečně seznámili s tvorbou uživatelských účtů v AD. Dále uvedeme, jakým způsobem se lze dostat k nastavení vlastností vytvořených uživatelských účtů.

8.4.2 Nastavení vlastností uživatelských účtů

V této podkapitole si ukážeme, kde lze v nástroji *Active Directory Users and Computers* nalézt možnost nastavení vlastností vytvořených uživatelských účtů.

Klikneme nyní pravým tlačítkem na vytvořený uživatelský účet, a ve vyvolaném menu zvolíme položku *Properties*. Po kliknutí na zmíněnou položku se objeví tabulka s řadou záložek, ve kterých lze nastavovat vlastnosti uživatelského účtu.



Obrázek 43: Vlastnosti uživatelského účtu

Doporučujeme všechna dostupná nastavení prozkoumat, a zamyslet se, zda chceme uživatelskému účtu (a dalším uživatelským účtům) zejména z důvodů zefektivnění správy datové sítě a minimalizace bezpečnostních rizik, spojených s využíváním jejích služeb, některé z těchto vlastností nastavit.

8.4.3 Závěr

V této podkapitole jsme se seznámili s tvorbou uživatelských účtů, a to jak osobních, tak univerzálních, a rovněž jsme zde uvedli, jakým způsobem se lze dostat k nastavení vlastností vytvořených uživatelských účtů. Nyní přejdeme k tvorbě účtů pro počítače.

8.5 Tvorba účtů pro počítače a nastavování jejich vlastností

V této podkapitole přistoupíme k tvorbě doménových účtů pro počítače a stejně jako u tvorby uživatelských účtů rovněž zmíníme, jakým způsobem jim po vytvoření lze nastavovat vlastnosti. V případě tvorby účtů pro počítače máme dvě možnosti.

První z možností, kterými lze vytvořit účet počítače, je jeho vytvoření **po prvním přihlášení** počítače k doméně. Ve chvíli, kdy počítač poprvé přihlásíme k doméně, vytvoří se automaticky doménový účet se shodným názvem, jako má samotný počítač. Jako umístění, ve kterém se účet

počítače, vytvořený tímto způsobem, objeví je defaultně nastavena OU **Computers**, odkud účet poté můžeme přesunout, kam potřebujeme.

Druhou možností je vytvořit doménový účet počítače **před** jeho **prvním přihlášením** k doméně. Toto řešení má dle našeho názoru řadu výhod. První z nich je fakt, že pokud se rozhodneme využít této možnosti vytváření účtů pro počítače, máme rovněž možnost využít nastavení, zajišťující aby se k doméně mohly připojovat pouze počítače s již vytvořenými účty. To se nám zdá být výhodné z hlediska bezpečnosti v rámci datové sítě. Z dalších výhod můžeme zmínit například tu, že počítač, který má dopředu vytvořen účet s určitými vlastnostmi, si tyto vlastnosti již při prvním přihlášení k doméně osvojí. Můžeme tedy provést vhodná nastavení počítače s předstihem a počítač je hned po jeho prvním přihlášení k doméně vhodně nakonfigurován.

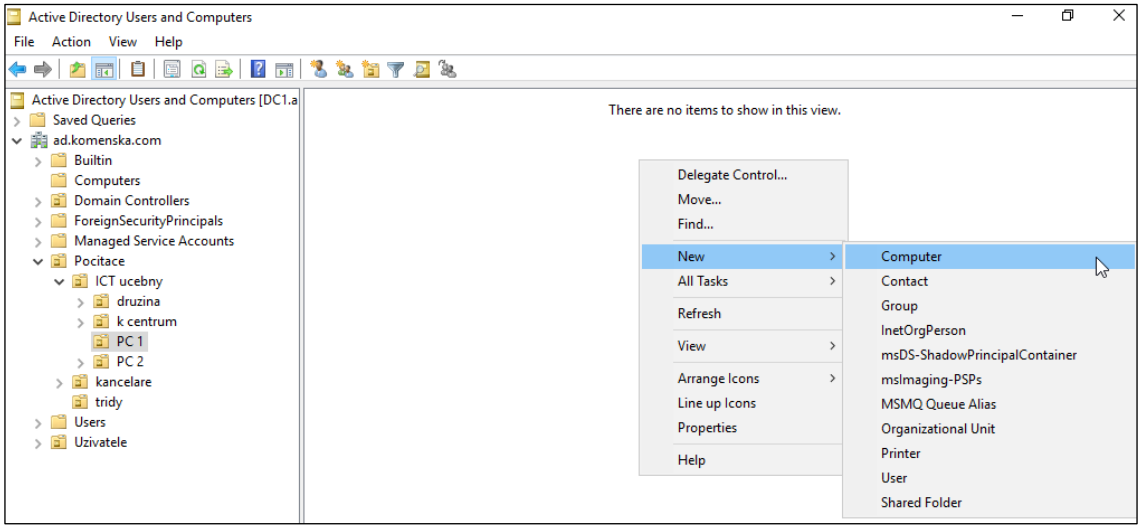
Vzhledem k cílové skupině práce nepovažujeme za nutné zabývat se prvním ze zmíněných způsobů, protože postup připojení počítače do domény by měl být čtenářům, kterým je tato práce určena, znám. Zaměříme se na druhý ze zmíněných způsobů, tedy na vytváření účtů pro počítače **před** jejich **prvním přihlášením** k doméně.

8.5.1 Tvorba účtů pro počítače

Pro tvorbu účtů pro počítače jsme se, stejně jako tomu bylo v případě tvorby uživatelských účtů, rozhodli použít nástroj *Active Directory Users and Computers*, a to ze stejných důvodů, jako jsme uvedli v podkapitole 8.4.1.

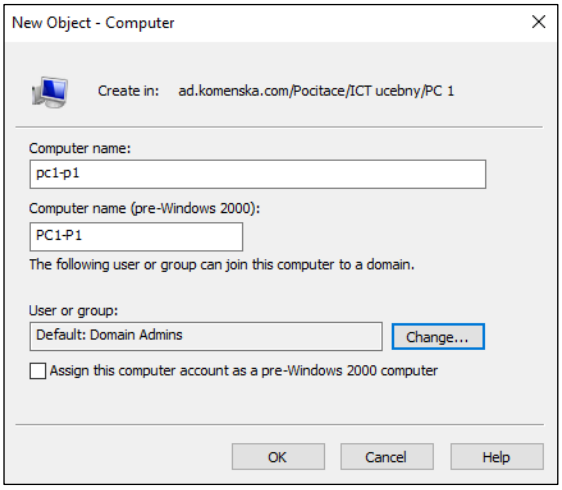
Nyní si pomocí zmíněného nástroje vytvoříme vzorový účet jednoho z počítačů, umístěných v počítačové učebně **PC 1**. Tomuto počítači na základě jmenné konvence, popsané podkapitole 6.6.2 této práce, zvolíme název **pc1-p01**.

Vyvoláme tedy nástroj *Active Directory Users and Computers* a otevřeme OU *PC 1*, kam vzorový počítač dle našeho návrhu patří. Zde klikneme pravým tlačítkem do volného prostoru a v příslušném menu zvolíme položku *New* a poté *Computer*.



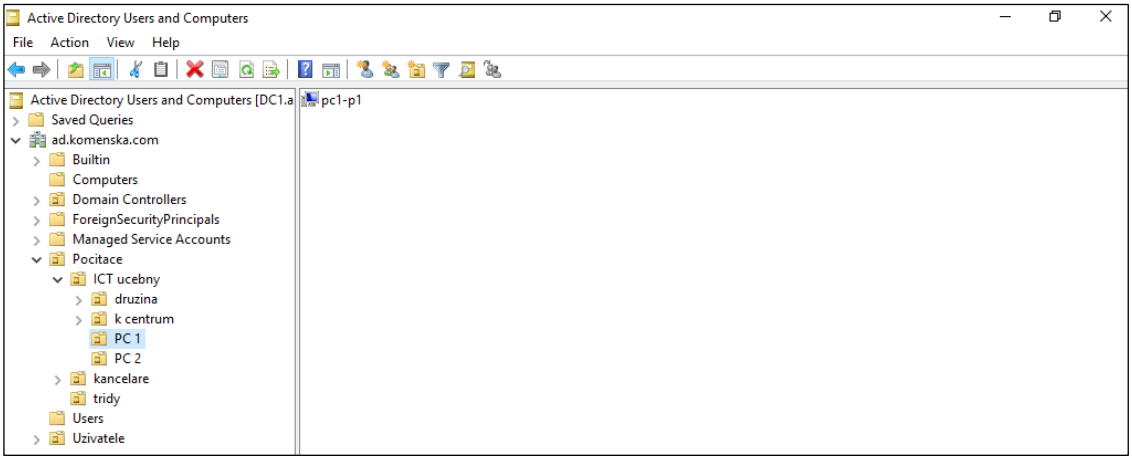
Obrázek 44: Tvorba účtu pro počítač - 1

Po kliknutí na položku *Computer* dojde k vyvolání okna, ve kterém máme možnost zadat název účtu počítače a rovněž určit, který uživatel či která skupina uživatelů může počítač, jehož název odpovídá názvu tohoto účtu, připojit k doméně. Nejprve tedy do boxu pod textem *„Computer name“* zadáme zvolený název počítače.



Obrázek 45: Tvorba účtu pro počítač - 2

Dále zde vidíme, že je v poli *User or group* nastavena hodnota *„Default: Domain Admins“*. Toto nastavení zajistí, že počítač se shodným názvem, jako je název vytvářeného účtu, může připojit do domény pouze uživatel s účtem doménového administrátora. Toto nastavení pokládáme za vhodné, a proto pokračujeme kliknutím na tlačítko *OK*. Tímto máme vytvořen náš první účet pro počítač. Nový účet se nyní zobrazí v příslušné OU.



Obrázek 46: Tvorba účtu pro počítač - 3

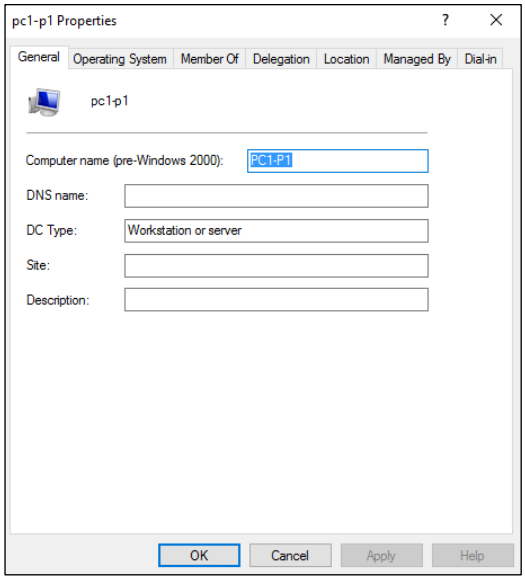
Výše zmíněný způsob lze využít k tvorbě účtů dalších počítačů, připojených k datové síti školy.

Domníváme se, že jsme v tuto chvíli dostatečně pronikli do procesu tvorby účtu pro počítače a příslušných nastavení. Dále ještě popíšeme, jakým způsobem se lze dostat k nastavení vlastností již vytvořených účtů pro počítače.

8.5.2 Nastavení vlastností účtů pro počítače

Stejně jako u uživatelských účtů máme i v případě účtů pro počítače možnost nastavovat jejich vlastnosti. V této podkapitole si ukážeme, jakým způsobem se lze k těmto nastavením dostat.

Klikneme pravým tlačítkem na existující účet počítače a zvolíme *Properties*.



Obrázek 47: Vlastnosti účtu pro počítač

Zobrazí se nám podobné okno, jako v případě nastavování vlastností uživatelského účtu. Záložky, dostupné v horní části okna, obsahují mnoho různých nastavení, spojených

se zvoleným účtem. Stejně jako v případě uživatelských účtů doporučujeme i zde prozkoumat všechna dostupná nastavení a zamyslet se, kterých nastavení si přejeme v případě účtů počítačů využít.

8.5.3 Závěr

V tuto chvíli jsme, dle našeho názoru, dostatečně pronikli do tvorby a nastavení účtů pro počítače a proto je vhodná chvíle přejít k dalšímu důležitému tématu této kapitoly, kterým je tvorba skupin.

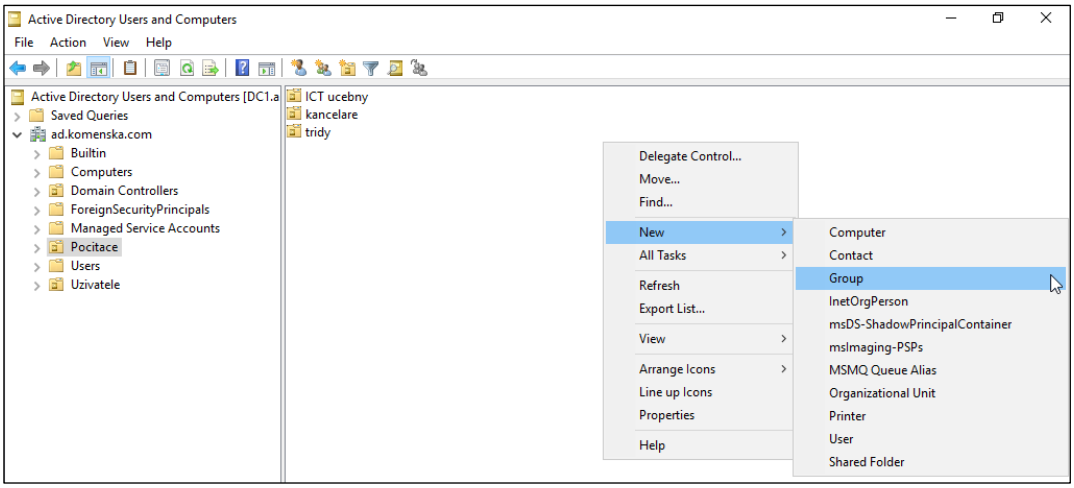
8.6 Tvorba skupin

V této podkapitole se seznámíme s tvorbou skupin, které, jak jsme rovněž uvedli v podkapitole 4.2.5, pokládáme za užitečný prostředek, který lze využít k zefektivnění správy datové sítě a k optimalizaci jejích služeb. Rovněž zde popíšeme, jakým způsobem je možné do skupin přidávat objekty.

V podkapitole 6.1.3 jsme zmínili, že se na úrovni skupin budeme zabývat **seskupováním počítačů na základě jejich operačního systému**, a proto si v této podkapitole jako příklad tvorby skupin vytvoříme skupinu pro počítače, disponující operačním systémem **Microsoft Windows 10**. Rovněž zde popíšeme postup, vedoucí k přidání počítače do této skupiny.

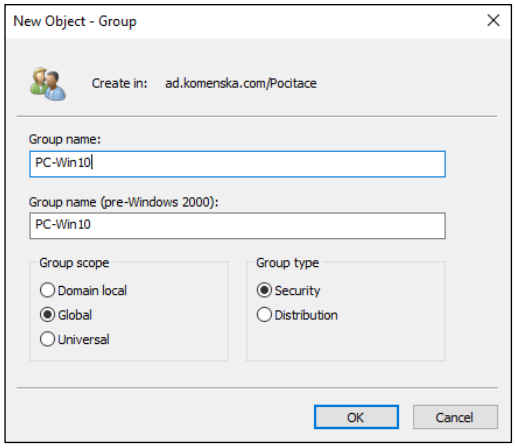
8.6.1 Vytvoření skupiny

Pro účely tvorby skupiny využijeme nám již známý nástroj *Active Directory Users and Computers*. Nástroj spustíme a přejdeme do OU *Pocitace*, kde klikneme pravým tlačítkem do volného prostoru. Tím vyvoláme menu, ve kterém zvolíme položku *New* a poté *Group*.



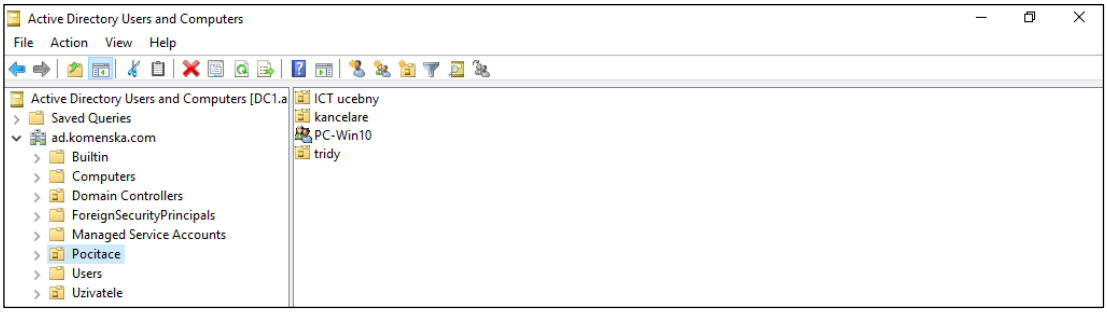
Obrázek 48: Tvorba skupiny - 1

V nově zobrazeném okně máme možnost specifikovat vlastnosti nové skupiny. Do pole *Group name* je potřeba zadat název skupiny. My jsme pro tuto skupinu zvolili název **PC-Win10**. Dále okno nabízí možnost nastavit *Group scope* (rozsah skupiny) a rovněž *Group type* (typ skupiny). Zde ponecháme výchozí hodnoty. Nastavení potvrdíme kliknutím na tlačítko *OK*.



Obrázek 49: Tvorba skupiny - 2

Nově vytvořená skupina se poté zobrazí v příslušné OU.



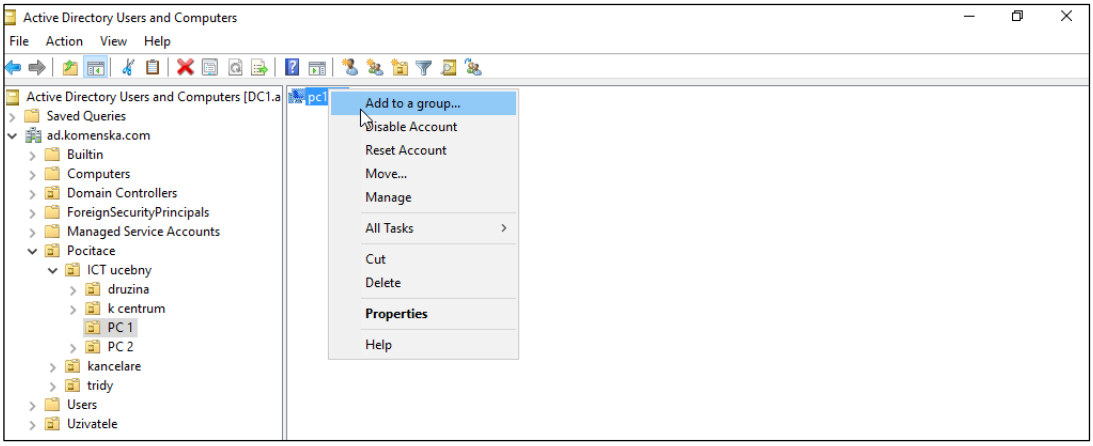
Obrázek 50: Tvorba skupiny - 3

V tuto chvíli máme vytvořenu první skupinu, do které je nyní možné vkládat objekty. Stejným způsobem lze vytvořit další skupiny, využitelné k seskupování počítačů dle jejich operačního systému, či jakékoliv jiné skupiny, seskupující objekty na základě našich potřeb. Dále se budeme zabývat přidáváním objektů do skupin.

8.6.2 Přidávání objektů do skupiny

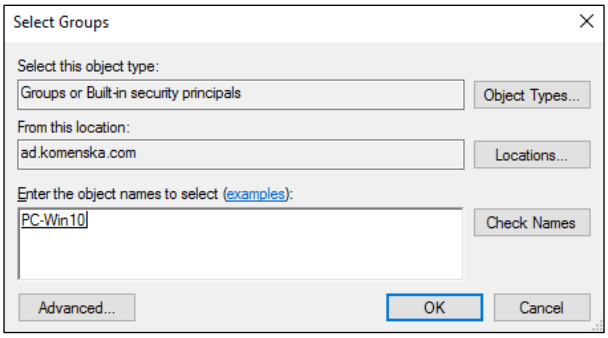
Existuje několik způsobů, kterými lze přidávat objekty do skupin. My si zde jeden z těchto způsobů ukážeme. Pomocí zvoleného způsobu přidáme účet počítače **pc1-p01**, vytvořený v podkapitole 8.5.1, do skupiny ***PC-Win10***, vytvořené v podkapitole 8.6.1.

Nejprve v naší logické struktuře vyhledáme dříve vytvořený účet počítače pc1-p01. Na tento účet klikneme pravým tlačítkem myši a zvolíme možnost *Add to a group…*.



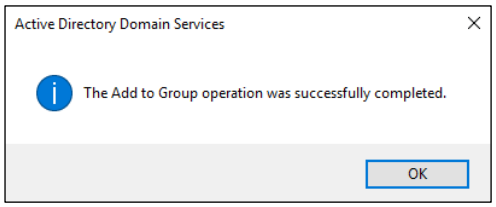
Obrázek 51: Přidání objektu do skupiny - 1

Tímto vyvoláme tabulku, v jejíž dolní části se nachází textové pole. Do tohoto pole napíšeme název dříve vytvořené skupiny a poté klikneme na tlačítko *Check Names* (zkontrolovat jména). V případě, že kontrola jména proběhne v pořádku, dojde k jeho podtržení.



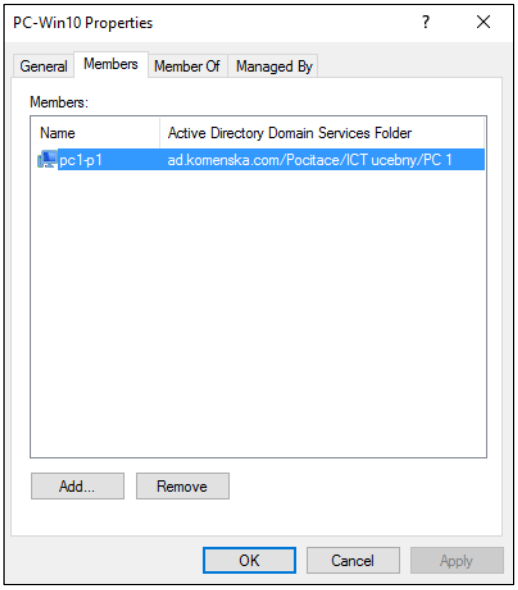
Obrázek 52: Přidání objektu do skupiny - 2

V této fázi můžeme kliknout na tlačítko *OK*, pomocí kterého potvrdíme přidání počítače do skupiny. Po chvíli se nám zobrazí informativní okno, sdělující, že operace proběhla úspěšně.



Obrázek 53: Přidání objektu do skupiny - 3

Pokud chceme přidání počítače (či jiného objektu) do skupiny zkontrolovat, klikneme v nástroji Active Directory Users and Computers pravým tlačítkem myši na danou skupinu a zvolíme možnost *Properties*. V nově vyvolaném okně se přepneme do záložky *Members*, kde vidíme seznam členů skupiny a tedy i to, zda bylo přidání objektu do skupiny úspěšné.



Obrázek 54: Vlastnosti skupiny – kontrola přidání objektu do skupiny

8.6.3 Závěr

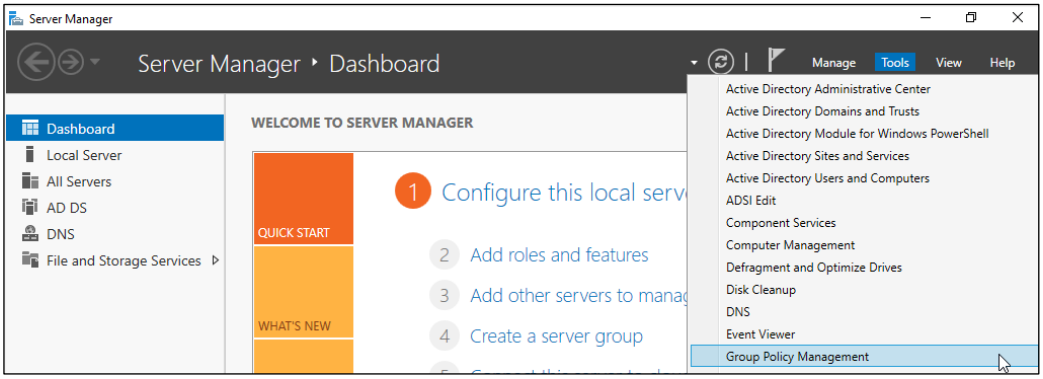
V této podkapitole jsme na konkrétním příkladu ukázali postup, vedoucí k vytvoření skupiny a rovněž postup přidávání objektů do skupiny. Nyní považujeme za vhodné přejít k dalšímu tématu této kapitoly, kterým je správa objektů pomocí skupinových politik.

8.7 Správa objektů pomocí skupinových politik

V tuto chvíli se dostáváme k takzvaným skupinovým politikám (group policies, dále jen GPO), které jsou jednou z velmi využívaných možností, které AD nabízí ke správě objektů datové sítě. Pomocí GPO lze hromadně nastavovat pravidla pro objekty, které jsou součástí určité OU. Je tedy zřejmé, že jejich vhodné využití vede k zefektivnění správy datové sítě. Dále považujeme za vhodné zmínit, že nám GPO nabízí široké možnosti správy objektů, což potvrzuje rovněž Desmond (2013, s. 283), který uvádí, že díky GPO máme možnost využít desítek tisíc nastavení, které můžeme aplikovat na uživatele a počítače.

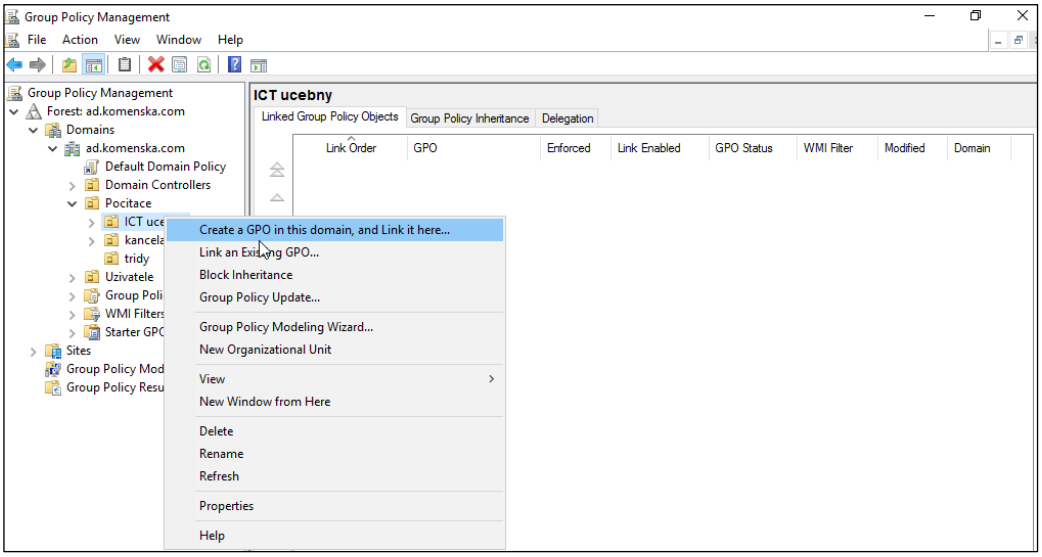
V této podkapitole si na konkrétním příkladu ukážeme, jakým způsobem lze vytvořit GPO pro určitou OU, a rovněž jakým způsobem se lze dostat k nastavení jejích pravidel. Vytvoříme si zde GPO pro OU **ICT ucebny**, tedy takovou, pomocí které lze nastavovat společná pravidla pro všechny počítače, umístěné v počítačových učebnách.

K tomu nám poslouží nástroj *Group Policy Management*, který lze nalézt pod položkou *Tools* v horním menu nabídky *Server Manager*. Tento nástroj tedy nyní spustíme.



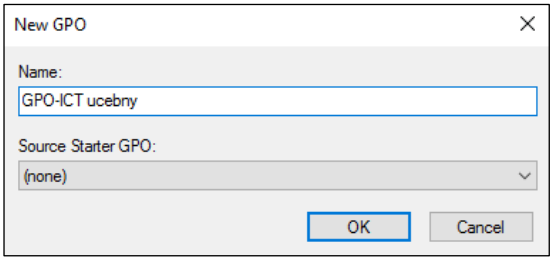
Obrázek 55: Tvorba GPO - 1

V levém menu nástroje *Group Policy Management* je možné, stejně jako v případě nástroje *Active Directory Users and Computers*, pracovat s logickou strukturou datové sítě. V tomto menu vyhledáme OU, pro kterou chceme vytvořit GPO a klikneme na ni pravým tlačítkem. V nově vyvolaném menu poté zvolíme položku *Create a GPO in this domain, and Link it here…* (vytvořit GPO v této doméně a připojit ji zde).



Obrázek 56: Tvorba GPO - 2

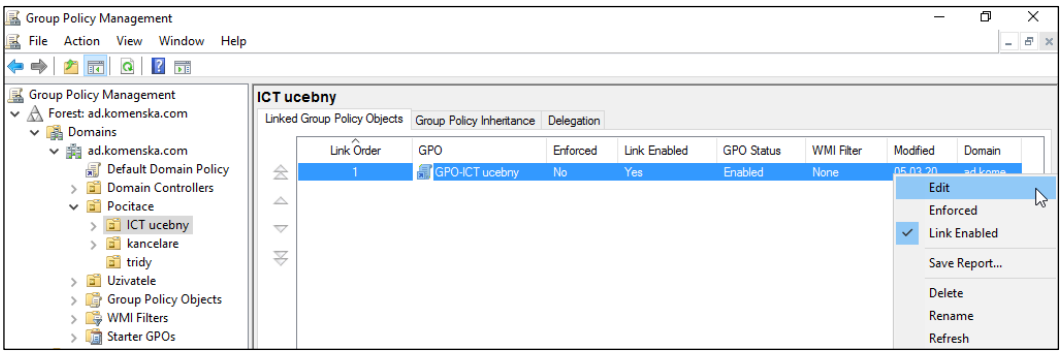
Kliknutí na zmíněnou položku vyvolá tabulku, ve které je potřeba zadat název nové GPO. My považujeme za vhodné při volbě názvu GPO vycházet z názvu OU, pro kterou GPO vytváříme. Proto volíme název **GPO-ICT ucebny**. Ten zadáme do pole pod nápisem *„Name:“*.



Obrázek 57: Tvorba GPO - 3

Nyní klikneme na tlačítko *OK*.

Tímto jsme vytvořili první GPO. Úspěch našeho počínání potvrzuje fakt, že se nová GPO zobrazila v pravé části okna *Group Policy Management* v kartě *Linked Group Policy Objects*.



Obrázek 58: Tvorba GPO – 4

Jakmile máme v OU vytvořenu GPO, můžeme začít s nastavováním pravidel, společných pro objekty dané OU. K možnosti nastavit pravidla GPO se lze dostat následujícím způsobem.

Klikneme pravým tlačítkem na příslušnou GPO a zvolíme možnost *Edit*. Volbou této možnosti vyvoláme tabulku, která nabízí **dvě kategorie pravidel**. Kategorii pravidel **pro uživatele** a kategorii pravidel **pro počítače**. Doporučujeme každému administrátorovi datové sítě, aby se seznámit s možnostmi, které jsou mu v těchto kategoriích nabízeny, a to ať už vlastním průzkumem a testováním těchto pravidel, nebo s využitím odborné literatury.

V této podkapitole jsme se na konkrétním příkladu seznámili s tvorbou GPO. Rovněž jsme uvedli, kde lze nalézt možnost nastavení jejích pravidel. Vhodné využití GPO může významným způsobem přispět k optimalizaci služeb datové sítě, a proto považujeme informace, uvedené v této podkapitole za velmi přínosné. Nyní již přejdeme k poslednímu tématu této kapitoly.

8.8 Možnosti propojení Active Directory s dalšími zařízeními, aplikacemi a službami

Domníváme se, že plného potenciálu technologie AD v oblasti optimalizace služeb datové sítě využijeme až teprve po propojení služby AD s dalšími zařízeními, aplikacemi a službami. Proto jsme se rozhodli zařadit do práce tuto podkapitolu, ve které nastíníme některé z nejpoužívanějších služeb, které lze propojit s technologií AD, jimiž jsou **souborový server** a **tiskové řešení**, a také zde zmíníme možnost využití autentizace **Single Sign On** (dále jen SSO), kterou nám využití technologie AD nabízí. Rovněž uvedeme některé způsoby, jak lze uvedených možností propojení AD s dalšími zařízeními, aplikacemi a službami využít v prostředí běžné školy a také se zamyslíme nad realizací některých z těchto způsobů.

8.8.1 Souborový server

Velmi často se lze v běžné praxi setkat s využitím AD k řízení přístupu ke sdíleným souborům a složkám, vytvořeným na souborovém serveru. My zde nastíníme dvě z možností využití takového řešení a v případě jedné z těchto možností se rovněž zamyslíme nad její realizací v prostředí navržené logické struktury datové sítě.

Domníváme se, že ve vyučování je mnohdy užitečná možnost efektivní výměny dat mezi učitelem a žákem. To platí obzvláště v hodinách informatiky, kdy učitel mnohdy potřebuje studentům předat podklady k práci (zadání, vstupní data, před-vytvořený projekt, a podobně). Je tedy výhodné vytvořit sdílenou složku, ke které budou mít učitelé právo čtení i zápisu, zatímco žáci pouze právo čtení. Učitelé tak budou moci žákům předávat podklady a žáci nebudou mít možnost vstupní podklady ať už nedopatřením, či záměrně, mazat nebo nevhodně upravovat.

Pokud bychom toto řešení chtěli zprovoznit v prostředí námi navržené logické struktury datové sítě, mohli bychom na souborovém serveru vytvořit sdílenou složku s názvem **zadani**, a poté nastavit, aby měl univerzální uživatelský účet **ucitel** ke složce právo čtení i zápisu, zatímco univerzální účet **zak** pouze právo čtení.

Z uvedeného příkladu je zřejmé, že pomocí technologie AD lze efektivně řídit přístup ke sdíleným souborům a složkám. Dalším z možných využití propojení AD a souborového serveru je například každému uživateli vytvořit na souborovém serveru osobní složku, ke které bude mít přístup pouze daný uživatel. Dále můžeme pomocí vhodného nastavení v AD zajistit, aby se každému uživateli přimapovala jeho osobní složka po každém přihlášení k doméně jakožto síťová jednotka.

Možností, poskytovaných kombinací AD a souborového serveru je celá řada a jejich využití závisí pouze na potřebách dané školy.

8.8.2 Tiskový server

Propojení AD s tiskovým serverem je další poměrně často využívané řešení. Z tohoto důvodu považujeme za vhodné zde zmínit možnosti, které nám propojení služby tiskového serveru se službou AD nabízí.

Pomocí služby AD můžeme řídit přístup k tiskárnám, a to tak, že můžeme s využitím GPO určit, kteří uživatelé mohou využívat služeb konkrétní tiskárny. Ostatní uživatelé nemohou služeb této tiskárny využívat a tiskárna je tedy zabezpečena proti zneužití jakoukoli neoprávněnou osobou.

V prostředí námi navržené logické struktury datové sítě můžeme například zajistit, aby **tiskárna ve sborovně 2** (vyšší stupeň) byla k dispozici pouze učitelům, kteří jsou součástí OU **druhy stupen** a tímto tedy přesně definovat, kdo může využívat služeb této tiskárny. Podobným způsobem můžeme řídit přístup k dalším tiskárnám, připojeným k datové síti školy.

Dále nám kombinace AD a tiskového serveru například umožňuje využít možnosti zvané **Location-Based Printing**. Tuto možnost však nepokládáme v prostředí běžných škol za příliš využitelnou.

8.8.3 Autentizace SSO

Autentizace SSO je výhodnou funkcí, pomocí které lze uživatelům zpříjemnit využívání služeb datové sítě. Jejím základním principem, který je rovněž uveden v odborném článku na webu Živě.cz (2014) je, že uživatel zadá své přihlašovací údaje pouze jednou, a autentizace k dalším aplikacím a službám již proběhne automaticky, bez nutnosti jejich opětovného zadávání. Tato metoda autentizace využívá protokolu **Kerberos**, který, jak již víme z první kapitoly této práce, je využívám samotnou službou AD. Jednou z podmínek k zprovoznění autentizace SSO tedy je, že aplikace, pro kterou chceme SSO nasadit, podporuje protokol Kerberos.

Využití autentizace SSO ve školách závisí zejména na konkrétních aplikacích, které daná škola využívá. Pokud škola využívá řadu aplikací, které autentizaci SSO podporují, doporučujeme nastavení této metody autentizace věnovat čas. S její pomocí lze uživatelům významným způsobem usnadnit využívání služeb datové sítě.

8.8.4 Závěr

V této podkapitole jsme si krátce nastínili některé možnosti propojení technologie AD s dalšími zařízeními, aplikacemi a službami. Z výše uvedených informací je zřejmé, že uvedené možnosti přispívají, a to zejména poskytnutím možnosti efektivního řízení přístupu k prostředkům a službám datové sítě a rovněž usnadněním autentizace uživatelům, k optimalizaci služeb datové sítě. Toto nastínění považujeme pro potřeby naší práce za dostatečné. V případě vážné úvahy o nasazení některého z těchto řešení však doporučujeme nejprve prostudovat některou z odborných publikací, věnujících se zvolenému řešení.

8.9 Závěr

Podkapitolou o možnostech propojení s dalšími zařízeními, aplikacemi a službami jsme uzavřeli kapitolu, věnovanou praktické realizaci navržené logické struktury datové sítě. Dle našeho názoru jsme v této kapitole uvedli všechny informace, nutné pro implementaci technologie AD do školní datové sítě a pro rovněž vytvoření dříve navržené logické struktury. Dále jsme popsali postup, vedoucí k vytvoření a nastavení účtů objektů datové sítě a skupin. Také jsme se seznámili s tvorbou GPO a rovněž s některými možnostmi propojení AD s dalšími zařízeními, aplikacemi a službami. Tyto znalosti považujeme s přihlédnutím k tématu práce za velmi důležité.

Domníváme se, že jsme v této kapitole vytvořili dostatečný informační základ pro efektivní využití technologie AD za účelem optimalizace datové sítě. K hlubšímu průzkumu uvedených možností AD, vedoucích k optimalizaci služeb datové sítě, či k objevení možností dalších však doporučujeme prostudovat i jiné odborné práce či publikace, věnující se této technologii. Nyní přejdeme k poslední kapitole práce, věnující se open source alternativám AD.

9 Open source alternativy Active Directory

Jak uvádí rovněž Stani (2014), v běžné praxi se z adresářových služeb nejčastěji setkáváme se službou AD. Domníváme se, že mezi důvody tohoto fenoménu patří zejména **profesionální technická podpora** ze strany společnosti Microsoft (zdokonalování služby, poradenství), **velká online komunita** IT specialistů, z nichž mnozí pracují s AD na denní bázi, a rovněž fakt, že tuto službu vyvíjí věhlasná **firma Microsoft**, jejíž operační systémy jsou ve firmách mnohdy jedinými používanými. Použití technologie AD však není jedinou variantou, využitelnou k optimalizaci služeb datové sítě. Existuje celá řada alternativ AD, a to jak placených, vyvíjených různými společnostmi, tak open source, dostupných bezplatně. A právě open source alternativami AD se v této kapitole budeme zabývat. Tuto kapitolu jsme do práce zařadili, protože ne každá škola disponuje dostatkem financí, aby pokryla výdaje, spojené s implementací technologie AD do své datové sítě. Přesně pro takové školy může být využití některé z open source alternativ AD vhodnou volbou.

Zaměříme se zejména na nástroj **OpenLDAP**, který nás z dostupných alternativ AD zaujal nejvíce. Zmíníme však i další open source řešení, která je možné místo AD použít.

9.1 OpenLDAP

Z open source nástrojů, které lze považovat za alternativu AD, je Open LDAP pravděpodobně tím nejčastěji zmiňovaným. Tento nástroj je k dispozici zdarma, jak je uvedeno na jeho webových stránkách (OpenLDAP, 2018). Jedná se o nástroj multiplatformní, který je možné provozovat v prostředí operačních systémů Microsoft Windows, Mac OS X, Linux, a dalších. Z tohoto faktu lze odvodit, že v případě použití OpenLDAP v prostředí některého z bezplatných operačních systémů odpadají jakékoliv náklady, spojené s nákupem licencí, a proto může být jeho použití z ekonomického hlediska velmi výhodné. Důležitou skutečností je také to, že je nástroj stále vyvíjen a zdokonalován. Lze tedy očekávat, že budou vývojáři v budoucnosti stále reagovat na nové trendy, jakými jsou nové potřeby, spojené se správou datové sítě, či nové bezpečnostní hrozby. Z tohoto důvodu se domníváme, že se jedná o dlouhodobě využitelné řešení. Dále nás ve spojitosti s nástrojem zaujal fakt, zjištěný na jeho stránkách (OpenLDAP, 2018), a to, že existuje několik poskytovatelů technické podpory pro firmy, které tento nástroj využívají, což v případě open source software není běžné. Nejbližší firmou, která v současné době nabízí technickou podporu, spojenou s nástrojem OpenLDAP, je německá firma **New Elements GmbH**.

Z výše uvedených informací je zřejmé, že využití nástroje OpenLDAP může při správném využití přinést poměrně velkou ekonomickou úsporu. K dosažení maximální úspory nákladů, spojených implementaci OpenLDAP do datové sítě je však potřeba, aby správce školní datové sítě disponoval znalostí prostředí některého z bezplatných operačních systémů, což vzhledem k nízké rozšířenosti těchto systémů není samozřejmostí. Nedostatečná znalost prostředí bezplatného operačního systému může mít za následek zvýšené náklady, spojené s potřebou technické podpory od některé ze společností, které se tímto zabývají. Nicméně, neustálý vývoj a rovněž existence firem, poskytujících technickou podporu, dělají z tohoto nástroje, dle našeho názoru, důstojnou konkurenci pro službu AD a domníváme se, že jeho využití může být pro některé školy výhodné.

9.2 Další open source alternativy Active Directory

Další open source alternativou AD je nástroj **389 Directory Server**, který ve svém článku uvádí Stani (2014), a který je rovněž zmíněn v odborných článcích na webových stránkách MeraBheja (2018) a Top Best Alternatives (2014). Jedná se o nástroj, určený pro operační systém Linux. Mezi výhody 389 Directory Server patří podpora replikace multimaster a také fakt, že je nástroj neustále ve vývoji, jak je zřejmé z informací, uvedených na jeho oficiálních webových stránkách (389 Directory Server, 2018).

Z dalších používaných alternativ AD považujeme dále za vhodné zmínit nástroje **Apache Directory** a **Open DJ**. Nástrojů, které lze použít jakožto alternativu AD, je mnohem více.

9.3 Závěr

V této kapitole jsme se krátce seznámili s některými open source alternativami technologie AD. Z uvedených informací lze vyvodit, že použití open source alternativy může pro některé školy výhodné. Volbu mezi AD a některou ze zmíněných alternativ však doporučujeme dobře promyslet, protože obě varianty mají své kladné i záporné stránky. Zejména v případě bezplatných alternativ doporučujeme správci školní datové sítě před konečným rozhodnutím nejprve zvolenou alternativu důkladně vyzkoušet ve virtualizovaném prostředí. Testování ve virtualizovaném prostředí poskytne správci datové sítě možnost zhodnotit nejen zvolenou alternativu, ale také to, zda je schopen řešení implementovat do datové sítě školy a poté jej rovněž spravovat.

Nyní jsme uzavřeli poslední kapitolu, a proto přejdeme k závěru práce.

Závěr

V úvodu práce jsme stanovili tři cíle práce, kterých jsme chtěli dosáhnout. Dosažení prvního a rovněž nejobecnějšího cíle, tedy zvýšit povědomí o technologii Microsoft AD a o možnostech jejího využití za účelem optimalizace služeb datové sítě, bude možné zhodnotit teprve s odstupem času, po zveřejnění práce. Věříme však, že si práce díky svému zaměření na využití technologie AD ve školách najde své čtenáře a tedy, že tento cíl bude splněn.

Druhým z dříve stanovených cílů bylo poskytnout návrh konkrétní struktury AD pro vybranou školu, který je jednoduše upravitelný a může sloužit jako předloha pro tvorbu struktur AD pro jiné školy. Tento cíl byl dle našeho názoru splněn. V práci jsme nejprve poskytli teoretický základ, nutný k pochopení základních principů technologie AD, a poté jsme na základě získaných informací, a rovněž vstupních údajů, charakterizujících vybranou školu, vytvořili zmíněný návrh. Návrh je snadno upravitelný, což jsme prezentovali na konkrétních příkladech, a proto se domníváme, že je vhodný jako předloha pro tvorbu AD struktur jiných škol.

Posledním z cílů práce bylo poskytnout jakýsi manuál, popisující praktickou realizaci navrženého řešení a rovněž možnosti využití tohoto řešení za účelem optimalizace služeb datové sítě. Z důvodu tvorby samotného manuálu jsme do práce zakomponovali kapitolu, věnující se požadavkům k provozování AD, která nám dala odpovědi na řadu otázek, spojených s tvorbou manuálu, a také nám poskytnula přibližnou představu o výši nákladů, spojených s realizací navrženého řešení. Na základě těchto informací a rovněž na základě studia odborné literatury jsme vytvořili zmíněný manuál, čímž jsme splnili poslední z cílů, stanovených v úvodu práce.

Při zjištění výše nákladů, spojených s realizací navrženého řešení, jsme v průběhu tvorby práce dospěli k názoru, že ne každá škola má dostatečné finanční prostředky k jejich pokrytí. Proto jsme se rozhodli do práce přidat stručnou kapitolu, věnující se open source alternativám, jejichž využití může být pro tyto školy výhodné.

Domníváme se, že jsme splnili všechny z cílů, stanovených v úvodní kapitole práce, jejichž splnění je v současné době možné zhodnotit. Existuje však několik oblastí, ve kterých by bylo možné práci dále rozšířit. Mohli bychom například rozebrat nejdůležitější z nastavení GPO, která nám AD pro správu objektů datové sítě dává k dispozici a rovněž vytvořit konkrétní GPO pro každou z OU vytvořené struktury. Práci by rovněž bylo možné obohatit uvedením popisu

praktických procesů, vedoucích k propojení technologie AD s dalšími zařízeními, aplikacemi a službami. Je pravděpodobné, že těchto myšlenek využijeme při tvorbě diplomové práce.

Seznam použité literatury

Monografie

[1] ALLEN, Robbie a Alistair G. LOWE-NORRIS. *Active Directory: implementace a správa Microsoft Active Directory*. Praha: Grada, 2005. ISBN 80-247-0973-2.

[2] DESMOND, Brian, Joe RICBARDS, Robbie ALLEN a Alistair G. LOWE-NORRIS. *Active Directory*. 5th edition. Sebastopol: O'Reilly Media, 2013. ISBN 978-1-449-32002-7.

[3] KLEMENT, Milan. *Služby spojené s Active Directory*. Olomouc: Univerzita Palackého v Olomouci, 2015. ISBN 978-80-244-4572-4.

[4] MINASI, Mark. *Mastering Windows server 2012 R2*. Indianapolis, Indiana: Sybex, 2014. ISBN 978-1-118-28942-6.

[5] PRICE, Brad. *Active Directory: optimální postupy a řešení problémů*. Brno: CP Books, 2005. ISBN 80-251-0602-0.

[6] STANEK, William R. *Active Directory: kapesní rádce administrátora*. Brno: Computer Press, 2009. Microsoft (Computer Press). ISBN 978-80-251-2555-7.

[7] STANEK, William R. *Windows Server 2012: Pocket Consultant*. Redmond, Wash.: Microsoft Press, 2012. ISBN 978-0-7356-6633-7.

[8] ŠTĚRBA, Petr. *Instalace operačního systému a jeho konfigurace*. Orlová: Obchodní akademie Orlová, 2014. ISBN 978-80-87477-16-8.

Webové stránky a příspěvky na webu

[9] *389 Directory Server* [online]. Raleigh: Red Hat, c2018 [cit. 2018-02-20]. Dostupné z: http://directory.fedoraproject.org/

[10] 8 Microsoft Active Directory Alternatives and Competitors. In: *Top Best Alternatives* [online]. Top Best Alternatives, 2014-09-26 [cit. 2018-02-20]. Dostupné z: https://www.topbestalternatives.com/microsoft-active-directory/

[11] ALLEN, Robert. Active Directory user naming conventions. In: *Active Directory Training - Beginner to Expert Skills* [online]. October 25, 2016 [cit. 2018-04-14]. Dostupné z: https://activedirectorypro.com/active-directory-user-naming-convention/

[12] *CZC.cz* [online]. Příbram: Czech Computer, c2018 [cit. 2018-04-07]. Dostupné z: https://www.czc.cz/

[13] *Heureka.cz* [online]. Liberec: Heureka Shopping, c2000-2017 [cit. 2017-12-23]. Dostupné z: https://www.heureka.cz/

[14] CHRISTOPHER. 22 Best Alternatives to Microsoft Active Directory. In: *MeraBheja* [online]. January 20, 2018 [cit. 2018-02-20]. Dostupné z: https://merabheja.com/22-best-alternatives-to-microsoft-active-directory/

[15] Kerberos, část 2 – popis metody SSO a protokolu Kerberos. In: *Živě.cz* [online]. Praha: CN Invest, 7. července 2014 [cit. 2018-04-14]. Dostupné z: https://www.zive.cz/clanky/kerberos-cast-2--popis-metody-sso-a-protokolu-kerberos/sc-3-a-174389/default.aspx

[16] Licencování a ceny pro Windows Server 2016. *Microsoft* [online]. Redmond: Microsoft, c2017 [cit. 2017-12-23]. Dostupné z: https://www.microsoft.com/cs-cz/cloud-platform/windows-server-pricing

[17] Naming conventions in Active Directory for computers, domains, sites, and OUs. In: *Microsoft Support* [online]. Redmond: Microsoft, 26 Jul 2017 [cit. 2017-12-28]. Dostupné z: https://support.microsoft.com/en-gb/help/909264/naming-conventions-in-active-directory-for-computers-domains-sites-and

[18] NG, Cindy. Best Practices for Naming an Active Directory Domain. In: *Inside Out Security* [online]. 11/16/2017 [cit. 2017-12-28]. Dostupné z: https://blog.varonis.com/active-directory-domain-naming-best-practices/

[19] NOVÁK, Lubomír. Kterak správně zalicencovat Windows Server 2016. In: *CDL SYSTEM* [online]. 27. 4. 2017 [cit. 2017-12-23]. Dostupné z: http://www.cdl.cz/cs/blog/kterak-spravne-zalicencovat-windows-server-2016

[20] OBERNEDER, Armin. Windows Server 2016 Editions comparison. In: *Thomas-Krenn-Wiki* [online]. 28 September 2017 [cit. 2018-02-07]. Dostupné z: https://www.thomas-krenn.com/en/wiki/Windows_Server_2016_Editions_comparison

[21] *OpenLDAP* [online]. Minden: The OpenLDAP Foundation, c2014-2018 [cit. 2018-02-20]. Dostupné z: http://www.openldap.org/

[22] Zásady životního cyklu společnosti Microsoft. *Microsoft Support* [online]. Redmond: Microsoft, c2018 [cit. 2018-04-14]. Dostupné z: https://support.microsoft.com/cs-cz/lifecycle/search

[23] PYTKO, Krzysztof. Active Directory objects naming convention. In: *ISiek's blog about Microsoft Windows services* [online]. January 31, 2015 [cit. 2018-02-18]. Dostupné z: http://kpytko.pl/active-directory-domain-services/active-directory-objects-naming-convention/

[24] STANI, Emidio. Top 4 open source LDAP implementations. In: *Opensource.com* [online]. 28 May 2014 [cit. 2018-02-20]. Dostupné z: https://opensource.com/business/14/5/top-4-open-source-ldap-implementations

[25] Systémové požadavky. In: *Microsoft Docs* [online]. Redmond: Microsoft, 17. 10. 2017 [cit. 2018-04-15]. Dostupné z: https://docs.microsoft.com/cs-cz/windows-server/get-started/system-requirements

[26] System Requirements for Windows Server Essentials. In: *Microsoft Docs* [online]. Redmond: Microsoft, 31. 10. 2013 [cit. 2017-12-23]. Dostupné z: https://docs.microsoft.com/cs-cz/windows-server-essentials/get-started/system-requirements

[27] THOMPSON, Martin. IT Asset Naming Conventions. In: *The ITAM Review* [online]. Jan 17th, 2011 [cit. 2018-02-18]. Dostupné z: https://www.itassetmanagement.net/2011/01/17/asset-naming-conventions/

[28] Understanding Active Directory Functional Levels. In: *TechNet* [online]. Redmond: Microsoft, 60/18/2014 [cit. 2017-09-13]. Dostupné z: https://technet.microsoft.com/en-us/library/understanding-active-directory-functional-levels(v=ws.10).aspx

[29] Windows Server 2016 Functional Levels. In: *Microsoft Docs* [online]. Redmond: Microsoft, 31. 05. 2017 [cit. 2017-09-13]. Dostupné z: https://docs.microsoft.com/cs-cz/windows-server/identity/ad-ds/windows-server-2016-functional-levels

[30] Zaměstnanci. *Základní škola, - Komenského 6, Odry* [online]. Odry: Základní škola Odry Komenského, [2018] [cit. 2018-03-17]. Dostupné z: http://komenska.com/?page_id=15740

Zdroje použitých obrázků a tabulek

[31] Buy Windows Server 2016 Standard - Microsoft Store. *Microsoft Store* [online]. Redmond: Microsoft, c2017 [cit. 2017-09-13]. Obrázek ve formátu WebP. Dostupné z: https://www.microsoft.com/en-us/store/d/windows-server-2016-standard/dg7gmgf0ds12/0004

[32] Licencování a ceny pro Windows Server 2016. *Microsoft* [online]. Redmond: Microsoft, c2017 [cit. 2017-12-23]. Tabulka. Dostupné z: https://www.microsoft.com/cs-cz/cloud-platform/windows-server-pricing

[33] Windows Server Essentials. *TechSoup* [online]. San Francisco: TechSoup, c2017, [cit. 2017-12-23]. Obrázek ve formátu PNG. Dostupné z: http://www.techsoup.org/products/windows-server-essentials--LVS-48293--

[34] Windows Server Datacenter. *TechSoup* [online]. San Francisco: TechSoup, c2017, [cit. 2017-12-23]. Obrázek ve formátu PNG. Dostupné z: http://www.techsoup.org/products/windows-server-datacenter--LVS-47823--

Seznam použitých zkratek

AD	Active Directory
DC	domain controller
DNS	domain name system
SSO	single sign on
KDC	key distribution center
OU	organizational unit
FQDN	fully qualified domain name
AD DS	Active Directory Domain Services
GPO	group policy
LDAP	lightweight directory access protocol
CAL	client access license

Poznámka: V seznamu nejsou uvedeny všeobecně známé zkratky, zkratky, které pokládáme za součást všeobecného přehledu v oblasti IT (označení jednotek, a podobně) a rovněž zkratky, které jsou v textu použity pouze ojediněle s vysvětlením v textu.

Seznam obrázků

Seznam schémat

Seznam tabulek

ANOTACE

Jméno a příjmení:	Tomáš Kubíček
Katedra:	Katedra technické a informační výchovy
Vedoucí práce:	doc. PhDr. Milan Klement, Ph.D.
Rok obhajoby:	2018

Název práce:	Optimalizace služeb datové sítě postavené na technologii Microsoft Active Directory
Název v angličtině:	Optimization of Services Provided by a Data Network Based on Microsoft Active Directory
Anotace práce:	Bakalářská práce se zabývá adresářovou službou Microsoft Active Directory a jejím využitím k optimalizaci služeb datové sítě a zjednodušení její správy. Práce je orientovaná především na využití Active Directory ve školních datových sítích. Mimo teoretického popisu této služby a její funkce je zde k dispozici také návrh konkrétního řešení, které lze do školní datové sítě implementovat a které je do značné míry univerzálně využitelné. Tento návrh je popsán pomocí textu a schémat. Dále se práce věnuje postupu samotné implementace navrženého řešení do školní datové sítě prováděné v prostředí operačního systému Microsoft Server 2016, a také možnostem jeho využití za účelem optimalizace datové sítě. Rovněž je v práci zmínka o open source alternativách služby Active Directory.
Klíčová slova:	Informační technologie, Active Directory, datová síť, správa školní sítě, Windows Server 2016
Anotace v angličtině:	The bachelor thesis focuses on a directory service Microsoft Active Directory and its usage for optimization of data network services and for facilitation of data network administration. It is oriented mainly on the school data networks. It provides not only a theoretical description of the service and its function but also a concrete design of a solution which can be implemented in school data network and which is relatively universal. The structure of the design is described by the usage of text and schemes. The thesis also provides a description of the practical process of its implementation to a school data network in the environment of Microsoft Server 2016 and mentions possible ways of how to use the implemented solution to optimize the data network. In the thesis, there are also mentioned the open source alternatives to Microsoft Active Directory.

Klíčová slova v angličtině:	Information technology, Active Directory, data network, school network administration, Windows Server 2016
Přílohy vázané v práci:	Práce neobsahuje žádné přílohy.
Rozsah práce:	103 stran (157 304 znaků)
Jazyk práce:	CZ