ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

PROSTŘEDÍ MICROSOFT WINDOWS SERVER

Autor: **Jan Balvín**

Vedoucí práce: **Ing. Jiří Vaněk, Ph.D.**

Prohlášení

Prohlašuji, že jsem bakalářskou práci na téma Prostředí Microsoft Windows Server vypracoval samostatně a použil jen pramenů, které cituji a uvádím v seznamu použitých zdrojů.

Jsem si vědom, že odevzdáním bakalářské práce souhlasím s jejím zveřejněním dle zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů, ve znění pozdějších předpisů, a to i bez ohledu na výsledek její obhajoby.

Jsem si vědom, že moje bakalářská práce bude uložena v elektronické podobě v univerzitní databázi a bude veřejně přístupná k nahlédnutí.

Jsem si vědom že, na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, ve znění pozdějších předpisů, především ustanovení § 35 odst. 3 tohoto zákona, tj. o užití tohoto díla.

.....

(podpis autora)

V ..... dne .....

Poděkování

Děkuji vedoucímu práce, panu Ing. Jiřímu Vaňkovi, Ph.D. za trpělivost, ochotu, za cenné rady a odborné vedení. Dále chci poděkovat rodině, přítelkyni a přátelům za podporu a poskytnutí podkladových materiálů pro tvorbu této práce.

PROSTŘEDÍ MICROSOFT WINDOWS SERVER

Souhrn

Tématem této práce je přiblížení serverového prostředí Microsoft Windows. V teoretické části je charakterizován server a jeho edice. Dále jsou vylíčeny jeho důležité role v síti a je přiblíženo prostředí domény Active Directory. Další kapitoly jsou věnovány uživatelským účtům a účtům Active Directory a jejich slučování do skupin. Poté proběhne seznámení se zásadami skupin a jejich možností aplikace na uživatele či skupiny. Analytická část se zabývá praktickým nasazením serveru a nastavení jeho rolí, vytvoření doménového uživatelského účtu a jeho přiřazení do skupiny a aplikace zásad skupiny na něj. Dále se zabývá srovnáním s novějším serverovým systémem a zhodnocením obou zmíněných systémů.

Klíčová slova:

Microsoft Windows Server, doména, Active Directory, DHCP, DNS, zásady skupiny, uživatelské účty, TCP/IP, příkazový řádek

MICROSOFT WINDOWS SERVER ENVIROMENT

Summary

The theme of this bachelor paper work is a description of Microsoft Windows Server enviroment. In the theoretical part, there is characterized server and his editions. Further, there are subscribed his important roles and it is aimed to Active Directory domain enviromental. The following chapters are dedicated to user accounts and Active Directory accounts and their merging into the groups. Next chapters are going to acquaint to the readers Group Policy Objects and their application to user or group accounts. Analytical part of the paper work is following up the practical instalation of server and setting his roles, creating domain user accounts and their assignment to the groups and application Group Policy Objects. Following work is dedicated to comparing with newer serever systém and evaluation of both mentioned systems.

Key words:

Microsoft Windows Server, domain, Active Directory, DHCP, DNS, Group Policy Objects, user Accounts, TCP/IP, CMD line

Obsah

1. Úvod

Ačkoliv systém Microsoft Windows Server 2003 pomalu dostává ke konci své životnosti, přes jedenáct let sloužil spolu se systémem Microsoft Windows XP na počítačích doma i v práci. Ze statistik se dá vyčíst, že od jeho vydání do konce roku 2011 byl stále nejoblíbenější operační systém Microsoft Windows XP, který je dodnes nainstalován na skoro 40 procentech počítačů. Teprve v červenci roku 2012 překonal Windows 7 tržní podíl Windows XP.[1] Pravděpodobně finanční náročností přechodu na novější systém je dáno, že ho většina firem stále používá.

Dnes pomalu, ale jistě, vytlačuje Windows XP jiný operační systém od společnosti Microsoft, a to Windows 7 a jeho serverová verze Windows Server 2008 (R2). S nástupem nyní nejnovějšího operačního systému od společnosti Microsoft, Windows 8 a serveru Microsoft Windows Server 2012, a s již zmiňovaným koncem životnosti (koncové datum podpory Windows Server 2003 je stanoveno na 14. 7. 2015[2]) to bude s největší pravděpodobností konec zatím nejoblíbenějšího systému Windows XP a s ním i serverového systému Microsoft Windows Server 2003.

Vzhledem k těmto faktům, také trochu i z nostalgie, ale hlavně ze skutečnosti, že Microsoft Windows Server 2003 pracuje na stejném jádře jako v podstatě legendární systém Microsoft Windows XP a platí za nejrozšířenější serverový systém své doby, je za téma práce právě tento serverový operační systém a jeho srovnání s novější verzí Microsoft Windows Server 2008.

[1] CDR. *CDR.cz - vybráno z IT* [online]. 2012 [cit. 2012-11-12]. Dostupné z: http://cdr.cz/clanek/podil-windows-7-prekonal-windows-xp
[2] MICROSOFT. *Technická podpora Microsoft online* [online]. 2012 [cit. 2012-11-12]. Dostupné z: http://support.microsoft.com/lifecycle/?p1=3198

2. Cíl práce a metodika

Bakalářská práce je tematicky zaměřena na prostředí Microsoft Windows Server. Hlavním cílem této práce je představení prostředí síťového operačního systému Microsoft Windows Server 2003, srovnání s jednou z novějších verzí serverového operačního systému, zhodnocení výhod a uvážení přechodu na novější verze.

Dílčími cíli jsou:

- charakterizovat prostředí a role Microsoft Windows Server,
- seznámení s doménou Active Directory, uživatelskými účty a skupinami,
- vytvoření uživatelských účtů, cestovních profilů a jejich správa,
- vytváření zásad skupiny, jejich nastavení a implementace,
- závěry, hodnocení systémů a doporučení.

V úvodních kapitolách se bakalářská práce bude věnovat základním představení serverového operačního systému. Zodpoví otázku v čem je výhoda mít nainstalován server již v malé síti. Dále uvedení služeb výhodných pro tuto síť. V další kapitole se zaměří na doménu na serveru, její představení a použití služby Active Directory a vysvětlení stromů a lesů Active Directory. V následující kapitole se bakalářská práce zaměří na účty. Důraz bude kladen na doménové účty s cestovním profilem, nastavení jejich vlastností a přiřazování do určitých skupin. Příští kapitola vylíčí skupiny zásad (Group Policy Objects), k čemu nám jsou a jak se implementují. Dotkne se i jejich správy.

Analytická část práce bude věnována srovnání s novějším serverovým operačním systémem, a to Microsoft Windows Server 2008 a jeho výhodami oproti starší verzi. Přiblížení teoretických znalostí z úvodu práce do praxe, a to návrhem a implementací systému Microsoft Windows Server 2003 s jeho rolemi. Vytvoření uživatelských účtů a jejich přiřazení do skupin. Vytvoření určitých zásad skupiny a jejich použití. Z těchto poznatků a úvah pak bude vyveden závěr práce.

3. Přehled řešené problematiky

„Tak jako se lidské tělo neobejde bez srdce či fotbalový zápas bez rozhodčího, neobejdou se větší počítačové sítě bez serveru (nebo serverů). Server je tedy srdcem takové sítě. Jedná se o nejdůležitější počítač (počítače), který může mít různé úkoly od řízení chodu celé sítě přes uchování dat až po správu běhu aplikací.

Jedná se o počítač, který v síti, k níž je připojen, poskytuje služby (od slova „serve" - „sloužit"). Je úplně jedno, jakým operačním systémem daný počítač disponuje, taktéž nezáleží ani na hardwarové výbavě.

Protože se v každé síti vyskytují požadavky na sdílení souborů, na tisk na síťové tiskárny a další, měl by v každé síti existovat alespoň jeden server. Ten může samozřejmě dané služby kombinovat. Pokud to však jeho vytížení či nekompatibilita nedovolí, je nutné přidat další servery, pochopitelně se serverovými operačními systémy.“[3]

Proč si pořídit server do již malé sítě? Data jsou mnohem lépe uspořádaná a centralizovaná a získá se tak lepší přehled a kontrola nad informacemi, které jsou důležité pro chod společnosti. Výrazně přispěje k lepší spolupráci uvnitř společnosti, usnadní sdílení souborů a jiných dat mezi více počítači a zjednoduší se také přenos dat z jednoho počítače na druhý. Pokud je potřeba sdílet mezi dvěma či více počítači hardware, jako je tiskárna nebo fax, je server naprostou nutností. Dále umožňuje i používání podnikových aplikací na více počítačích. Server významně usnadňuje vytváření záloh a obnovu důležitých dat. Výrazně se tím zvyšuje zabezpečení a ochrana dat. Často se v dnešní době stává, že lidé jezdí na služební cesty nebo pracují z domova, v tomto případě potřebují mít možnost se připojit k síti společnosti, u které pracují. Server tedy umožňuje oprávněným pracovníkům získat vzdálený přístup k této síti. V případě růstu a rozvoje společnosti, bude potřeba snadno a rychle nainstalovat nové počítače a přidávat další

[3] ŠETKA, Petr. *Mistrovství v Microsoft Windows Server 2003*. Vyd. 1. Brno: Computer Press, 2003. ISBN 80-251-0036-7.

uživatele. Při správě dat z centrálního místa je přidávání počítačů a softwarových licencí mnohem jednodušší.[4]

3.1 Microsoft Windows Server 2003

Tato část je zpracována podle [3][5][7][12]

Tento serverový systém byl vydán v několika variantách. Dělí se podle funkcí, které zastávají.

- Windows Server 2003 Web Edition
- Windows Server 2003 Standard Editon
- Windows Server 2003 Enterprise Edition
- Windows Server 2003 Datacenter Edition

3.1.1 Web Edition

Největší nevýhodou této verze je, že postrádá některé důležité funkce a služby, které by se dozajista hodily, jako například internetová brána, DHCP, nemůže to být řadič domény atp. Je to ochuzený server, který poskytuje jednoduché zavádění i správu, je speciálně navržen jen pro webové služby a není proto vhodný pro malé podnikové sítě.

3.1.2 Standard Editon

Tato verze je univerzální a je schopna nám poskytovat nejširší pole služeb pro všechny společnosti, malé i střední. Může zastávat funkci doménového řadiče či serveru DNS, zejména však poskytuje služby pro sdílení tiskáren a souborů. Jednoduše jej lze připojit i k internetu a využít tak pro správu aplikací klient-server.

3.1.3 Enterprise Edition

Zde je představená verze, která je již určena pro střední a větší sítě a společnosti. Použije se, když už svou kapacitou nestačí standardní edice. Podporuje technologii clustering a je určena pro zastávání kritických aplikací.

[4] PCCOMP.eu. *PC Comp s.r.o. - Internet, VoIP, Správa sítí, Výpočetní technika, Webhosting* [online]. 2007 [cit. 2012-11-22]. Dostupné z: http://www.pccomp.eu/cs/pc-comp/serverova-reseni/

3.1.4 Datacenter Edition

Tato verze se hodí do prostředí s vysokými požadavky na bezpečnost, poskytuje nesmírnou škálovatelnost a rychlost. Jeho výhoda je bezesporu ve zpracování velkého množství transakcí v reálném čase.

Požadavky na hardware pro tyto systémy jsou v dnešní době, řekněme, skromné. Stejně výkonné stroje, jak již bylo zmíněno, se dají najít i v noteboocích, či tabletech a snad i smartphonech, i když se v nich používají procesory s jinou architekturou. Pro upřesnění, minimální požadavky na Microsoft Windows Server 2003 a jeho edic jsou, CPU 133 – 400 MHz, 128 MB RAM, 1,5 GB místo na disku. Různé edice podporují různý maximální počet paměti RAM, nebo procesorů. Web Edition podporuje nejvíce 2 procesory, oproti tomu Datacenter Edition přímo vyžaduje nejméně 8 a zvládá nejvíce až 32 procesorů.

Následující Tabulka 1[5] ujasní systémové požadavky pro všechny edice Microsoft Windows Server 2003.

Verze systému	**Minimální systémové požadavky**
Windows Server 2003, Web Edition	CPU min. 133 MHz (doporučeno 550 MHz), 128 MB RAM (doporučeno 256 MB), 1,5 GB místa na disku Systém podporuje maximálně 2 GB paměti RAM a nejvíce 2 procesory
Windows Server 2003, Standard Edition	CPU min. 133 MHz (doporučeno 550 MHz), 128 MB RAM (doporučeno 256 MB), 1,5 GB místa na disku Systém podporuje maximálně 4 GB paměti RAM a nejvíce 4 procesory
Windows Server 2003, Enterprise Edition	CPU min. 133 MHz (doporučeno 733 MHz), 128 MB RAM (doporučeno 256 MB), 1,5 GB místa na disku Systém podporuje maximálně 32 GB paměti RAM a nejvíce 8 procesorů
Windows Server 2003, Datacenter Edition	CPU min. 400 MHz (doporučeno 733 MHz), 512 MB RAM (doporučeno 1 GB), 1,5 GB místa na disku Systém podporuje maximálně 64 GB paměti RAM a vyžaduje nejméně 8, nejvíce 32 procesorů

Tabulka 1- Systémové požadavky Microsoft Windows Server 2003

[5] ŠETKA, Petr. *Mistrovství v Microsoft Windows Server 2003*. Vyd. 1. Brno: Computer Press, 2003, 680 s. ISBN 80-251-0036-7.

3.1.5 Podpora procesorů Itanium a AMD64

První, kdo vydal procesory pro 64-bitovou architekturu, byla firma Intel a jejich procesor s názvem Itanium. Klíč není jenom v podpoře 64-bitové architektury, ale hlavně v tom, že používá instrukční sadu zvanou „EPIC“ (Explicitly Parallel Instruction Computing). Tato sada byla navržena tak, aby zvýšila schopnost mikroprocesorů vykonávat paralelně více instrukcí. Se změnou softwarového kompilátoru místo za pomoci komplexních logických obvodů na procesoru, se podařilo zvýšit počet vykonaných instrukcí za jeden takt procesoru a tím zvýšit i celkový výkon procesoru. Firma AMD také podporuje 64-bitovou architekturu. Nicméně firma AMD šla vlastní cestou a výsledek je architektura s názvem „AMD64“, dnes známé jako „X64“., který je oproti procesoru Itanium zpětně kompatibilní s X86 architekturou. Microsoft vytvořil další verze systému Microsoft Windows Server 2003 s přízviskem 64 bit. Byly to edice Windows Server 2003 Enterprice a Windows Server 2003 Datacenter.[6]

[6] MICROSOFT. *Technická podpora Microsoft online* [online]. 2012 [cit. 2012-11-24]. Dostupné z: http://technet.microsoft.com/cs-cz/bb291006.aspx

3.2 Role Microsoft Windows Server 2003

Tato část je zpracována podle [2][3][5][12]

Na Obrázku 1 je vidět možnost přidání rolí na server. Role, které se dají přidat na server, se liší od požadavků společnosti či administrátora, a je to vlastně služba serveru, kterou poskytuje v síti.

Obrázek 1 - Vytvoření role na serveru

3.2.1 Souborový server

Pokud na serveru poběží tato role, poskytne pohodlný a hlavně centralizovaný přístup k adresářům a souborům, a to jak pro jednotlivé uživatele, skupiny uživatelů nebo pro celou společnost. Výhodou je pak snadnější údržba a zálohování, správa, vyhledávání, sdílení dat a podobně.

3.2.2 Server DHCP

DHCP (Dynamic Host Configuration Protokol) zjednodušuje správu IP adres a související konfigurační data. Tato služba poskytuje automaticky IP adresu všem klientským počítačům, které mají nastaveno použití dynamického adresování, a dále zamezuje použití stejné IP adresy u dvou počítačů

3.2.3 Doménový řadič (Active Directory)

Poskytuje adresářové služby pro klienty v síti. Active Directory umožňuje administrátorům nastavovat politiku, instalovat programy na mnoho počítačů nebo aplikovat kritické aktualizace v celé organizační struktuře. Active Directory ukládá své informace a nastavení v centrální organizované databázi.

3.2.4 DNS server

Domain Name System, tedy DNS, je internetový standard zahrnutý do TCP/IP a slouží k překladu jmen objektů na IP adresy a zpět. Tyto jména se označují jako doménová jména (domain name) a nejčastěji jsou zastoupena jmény hostitelů (hostname). Většina lidí si nebude pamatovat IP adresu 77.75.72.3, ale spíše adresu www.seznam.cz.

3.2.5 Terminálový server

Umožňuje přístup k aplikacím v síti, které jsou nainstalovány na terminálovém serveru tak, jako kdyby byly nainstalovány na jednom z lokálních počítačů. Přes vzdálenou plochu tak může pracovat více pracovníků v jedné aplikaci, či ukládat soubory a používat síťové prostředky.

3.2.6 Server POP3 či IMAP4

POP3 protokol poskytuje pomocí služby SMTP přístup k e-mailům na serveru. Tyto e-maily jsou pak stahovány ke klientským počítačům najednou a tím je zaručeno pohodlné ovládání a čtení e-mailů.

Dále také:

- Webový server
- Terminálový server
- Aplikační server (IIS, ASP. NET)
- WINS server
- Server pro vzdálené připojení / VPN server
- Server FTP
- Tiskový server
- Stream Media Center
- Server se službou vzdálené instalace

a další…

3.3 Doména a Active Directory Microsoft Windows Server 2003

Tato část je zpracována podle [1][3][5][8][12]

Administrace počítačů v pracovní skupině je nereálná po překročení určitého množství počítačů v síti. Pro toto prostředí, se hodí doména.

„Doménu lze definovat jako logické seskupení prostředků v síti. Prostředky se rozumí počítače, uživatelské účty, skupiny uživatelů atd. Jak se bude doména tvářit v porovnání s pracovní skupinou?

- *V doméně existuje částečné hierarchické uspořádání počítačů. Na vrcholu hierarchie je počítač, který udržuje doménovou databázi, tzv. řadič domény. Nejedná se tedy o síť typu peer-to-peer, ve které jsou si všechny počítače rovny.*
- *Uživatel má pouze jediný, takzvaný doménový účet. Ten může standardně použít k přihlášení ke každému počítači v doméně.*
- *Účet uživatele je uložen v doménové databázi. Doménovou databázi udržuje řadič domény. Pokud je řadičů domény více, vyměňují si repliku doménové databáze (pro případ, že by některý z nich vypadl nebo pokud je v síti velký počet uživatelů a jeden řadič by takový počet nezvládal).*
- *Přístup k prostředkům v jiných počítačích v doméně může být řízen doménovým účtem uživatele. Místní účty v daných počítačích nejsou nutné.*
- *Pokud uživatel mění heslo, týká se to jeho doménového účtu. Se změněným heslem je tedy schopen se ihned poté přihlásit k jinému počítači.*
- *Počítače v doméně lze zabezpečit pomocí nastavení Zásad skupiny definovaných pouze jednou pro celou doménu.*

Doménové prostředí je jedinou rozumnou volbou pro střední až velká prostředí. Umožňuje mnohem efektivnější správu, poskytuje větší zabezpečení prostředí a ve svém důsledku snižuje celkové náklady na výpočetní techniku.“[7]

3.3.1 Active Directory

Active directory je adresářová služba, ve které jsou objekty hierarchicky členěny a přistupuje se k nim pomocí protokolu LDAP. Tato služba pak využívá databázi, kde se nacházejí všechny objekty sítě a měla by obsahovat všechny záznamy o nich - o počítačích, účtech uživatelů či skupin uživatelů, informace o tiskárnách a jiných objektech a všechny jejich atributy jako název nebo přihlašovací jméno, datum vytvoření účtu apod. Je to také služba, která propojuje všechny počítače uvnitř sítě a poskytuje jim všechny adresáře všech počítačů a informace o nich v jednom bodě. Active Directory umí také omezovat přístup k těmto informacím různým uživatelům přes ACL (Access Control List). Access Control List je seznam, ve kterém jsou uvedeny SID a jejich oprávnění (jeden záznam v tomto seznamu je ACE – Access Control Entry). Je to vlastně logické seskupení objektů v síti, kde není podstatné, na kterém místě jsou fyzicky umístěny.

Nejdůležitější funkcí je tedy jednoduché vyhledávání informací o objektech a jejich jednoduchá správa, jelikož je všechno soustředěno do jednoho bodu. K tomu tedy je potřeba mít tento bod, kde je služba Active Directory nainstalována, jinými slovy doménový řadič.

Funkční úroveň domény Active Directory

Pokud je v síti více domén s různými instalovanými serverovými systémy, nemůže se používat stejná úroveň funkčnosti domény Active Directory. V ideálním případě mají všechny doménové řadiče nainstalovanou stejnou verzi operačního systému, ale ne vždy tak tomu je. Každá verze serverového operačního systému má svojí vlastní úroveň a v důsledku to znamená, že administrátoři nemohou používat všechny funkce domény Active Directory.

Existují tři úrovně funkčnosti domény a následující Tabulka 2[8] je shrnuje.

[7] ŠETKA, Petr. *Mistrovství v Microsoft Windows Server 2003*. Vyd. 1. Brno: Computer Press, 2003, s. 54. ISBN 80-251-0036-7.

	Windows 2000 mixed	**Windows 2000 native**	**Windows server 2003**
Možné operační systémy na řadiči domény	▪ Windows NT 4.0 Server ▪ Windows 2000 ▪ Windows Server 2003	▪ Windows 2000 ▪ Windows Server 2003	▪ Windows Server 2003
Povolené rozsahy	▪ Globální ▪ Místní doménové ▪ Univerzální	▪ Globální ▪ Místní doménové	▪ Globální ▪ Místní doménové ▪ Univerzální

Tabulka 2 - Úrovně funkčnosti domény

Za zmínku stojí i úroveň Windows Server 2003 Interim, který se používá k přechodu z Windows NT Server na verzi Windows Server 2003.

Při funkční úrovni Windows 2000 native, jsou k dispozici všechny základní vlastnosti domény a navíc je možno využívat vlastnosti jako:

- univerzální skupina pro distribuční i skupinu se zabezpečením,
- seskupování skupin,
- převod skupin, který umožňuje konverzi mezi distribuční a skupinou se zabezpečením,
- SID historie.

V úrovni Windows server 2003 jsou navíc, k základním vlastnostem a vlastnostem úrovně Windows 2000 native, vlastnosti:

- doménový nástroj Netdom.exe, který umožňuje přejmenovat řadiče domény,
- aktualizace časových razítek přihlášení,
- časové razítko LastLogon (poslední přihlášení), které se replikuje v rámci domény,
- možnost nastavení atributu userPassword (uživatelské heslo) jako efektivního hesla na InetOrgPerson a uživatelské objekty,
- schopnost přesměrování uživatelů a kontejnerů počítačů,

[8] ŠETKA, Petr. *Mistrovství v Microsoft Windows Server 2003*. Vyd. 1. Brno: Computer Press, 2003, 680 s. ISBN 80-251-0036-7.

- optimalizovaná delegace, která umožňuje aplikacím využít zabezpečené delegace na základě ověřování Kerberos[9]

a další…

Funkční úroveň lesů domény Active Directory

Nejen doména má funkční úrovně. Musí se zmínit i úrovně funkčnosti lesa (Forest Functional Level) a to jsou Windows 2000 a Windows 2003. Úroveň funkčnosti lze pouze zvyšovat a tyto změny jsou nevratné. Pokud se nastaví úroveň funkčnosti lesa na určitou úroveň, nelze nastavit funkční úroveň domény na nižší úroveň než na úroveň lesa. V případě, že doménová struktura neobsahuje žádné domény staršího typu Windows NT 4.0 nebo Windows 2000, lze doporučit úroveň funkčnosti Windows 2003. Při úrovni Windows 2000 jsou k dispozici pouze všechny základní vlastnosti domény. Při úrovni Windows 2003 jsou navíc k dispozici tyto vlastnosti jako:

- přejmenování domén,
- inkrementální replikace,
- používání univerzálních skupin,
- vztahy důvěryhodnosti mezi lesy,
- možnost instalace doménového řadiče „jen pro čtení“,

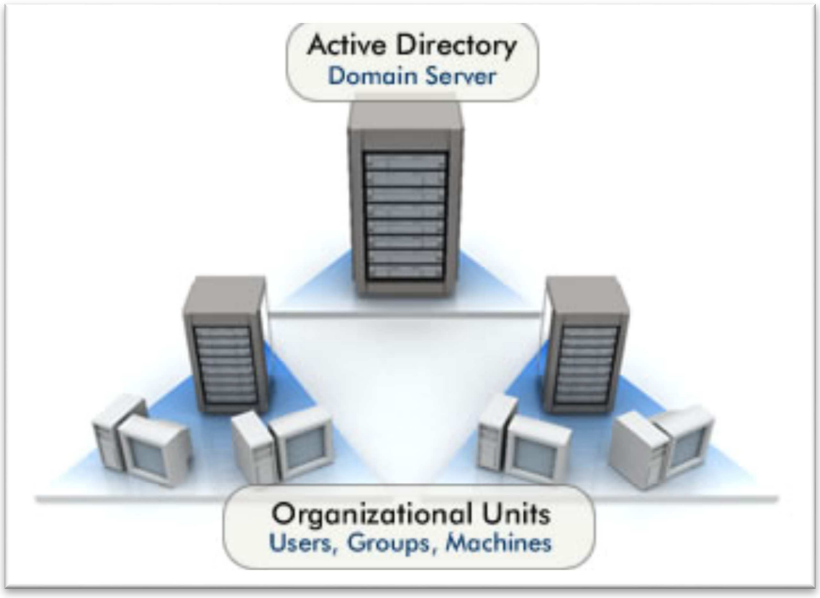
a další…

3.3.2 Doménový řadič

S prvním vytvořeným doménovým řadičem, se zároveň vytváří doména, les a instaluje se Active Directory. Jelikož jsou na řadiči domény uloženy všechny informace a databáze Active Directory, vyřizuje tak veškeré dotazy uživatelů. Proto se takovému počítači v organizaci věnují více než normálnímu. Doménový řadič by měl být nainstalován na velmi stabilním a dále rozšířitelným hardware a měl

[9] MICROSOFT. *Technická podpora Microsoft Online* [online]. 2012 [cit. 2012-11-26]. Dostupné z: http://technet.microsoft.com/en-us/library/understanding-active-directory-functional-levels(WS.10).aspx

by být lépe zabezpečený. Většinou se tento řadič nepoužívá současně s jinými rolemi serveru. Následující obrázek (obrázek č. 2) napovídá rozložení doménové struktury.



Obrázek 2 – Rozložení domény

Pokud by selhala jedna z hardwarových součástí serveru, která by jakkoliv poškodila data, bylo by vše ztraceno. Z tohoto důvodu, nebo z důvodu restartu, či výpadku serveru se většinou instaluje další řadič domény. Na serveru, kde je nainstalován Microsoft Windows Server 2003 a vyšší, lze propojit více doménových řadičů, které spolu komunikují, spolupracují, neboli se replikují. Pokud by jeden ze serverů přestal z jakéhokoliv důvodu pracovat, či odpovídat do sítě, převezme jeho roli druhý doménový řadič bez následků na uživatele.

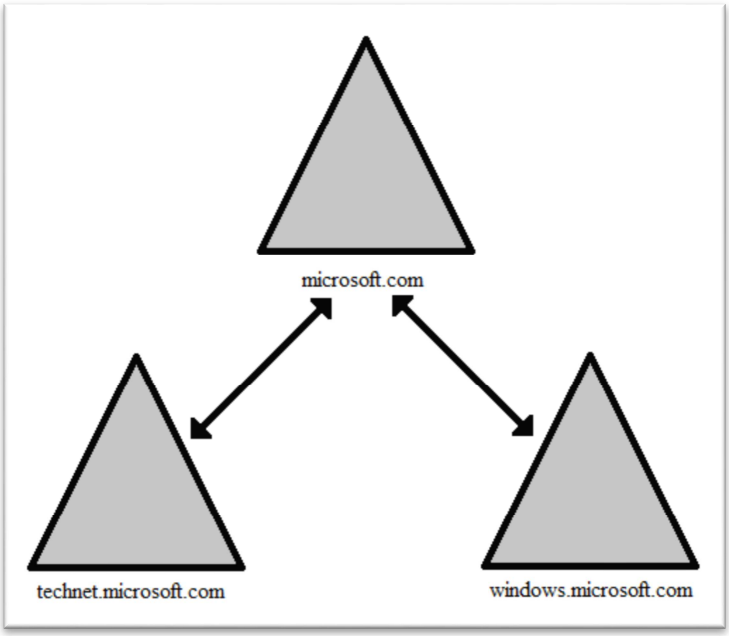
3.3.3 Stromy a lesy Active Directory

Pokud má tedy společnost více doménových řadičů a domén, musí spolu nějak koexistovat. Je na výběr více voleb, jak spolu mohou tyto domény spolupracovat. Záleží na již určených podmínkách nebo podmínkách při vytváření společnosti.

Poté co se nainstaluje první doménový řadič, bude zastávat funkci kořene domény a zároveň to bude první strom. Tím pádem všechny domény v tomto stromu, budou mít také stejný kořen domény neboli obor názvů. Dá se vzít příklad z domény, kde kořen této domény je microsoft.com a všechny v tomto stromu budou

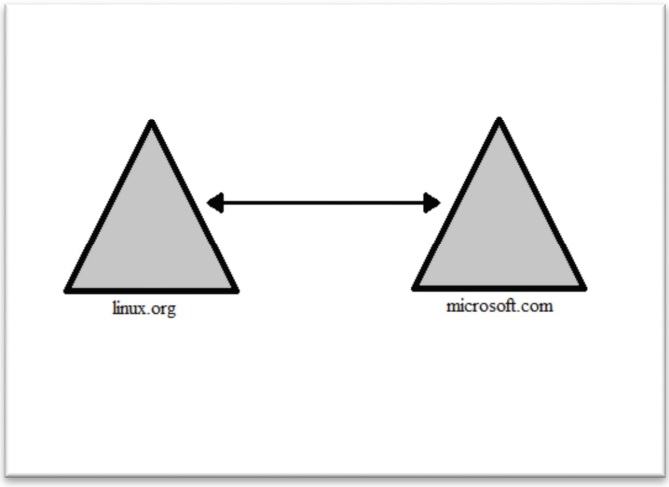
zachovávat stejný jmenný prostor, tedy microsoft.com. Například technet.microsoft.com, nebo windows.microsoft.com (obrázek č. 3). Všechny tyto domény se slučují do takzvaných lesů. Tato podoba se hodí do většiny malých, středních, ale někdy i větších společností. Jedná se o společnost, která má jeden název, který kopírují jednotlivé pobočky, a vše je soustředěno do jednoho místa společnosti.

V opačném případě se domény rozkládají na větším prostoru. Teď není myšleno velikost početní, ale fyzická. Společnost, která má pobočky rozesety po určitém místě, státu nebo kontinentu, bude pravděpodobně používat model stejný, akorát pojmenování jeho domén je rozdílné. To se odvíjí podle geografického rozdělení Active Directory struktury. Například v rámci měst budou domény, například odb.cz, pojmenovány takto – praha.odb.cz, brno.odb.cz, ostrava.odb.cz apod.



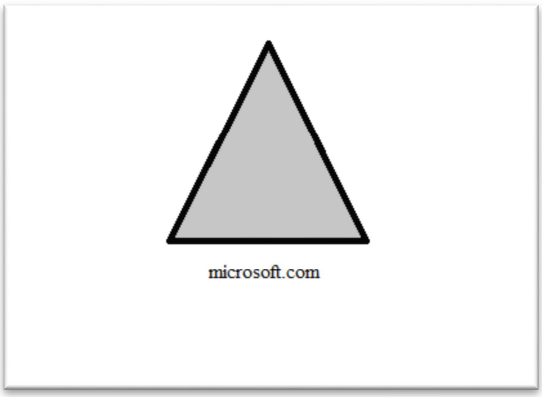
Obrázek 3 – Model s jedním stromem, jedním lesem a jedním kořenem domény

Společnosti, která koupí jinou společnost a bude chtít mít propojenou svojí síťovou infrastrukturu, již nebude vyhovovat předchozímu modelu propojení domén. V tomto případě budou mít obě společnosti vlastní strom a vlastní Active Directory, pokud si ponechají své názvy domén. Budou se však nacházet pořád v jednom lese (obrázek č 4).



Obrázek 4 – Model se dvěma stromy, dvěmi doménami a jedním lesem

Poslední model, který bude představen, je nejjednodušší. Je to model s jedinou doménou, tudíž je sestavena z jednoho stromu a jednoho lesa (obrázek č. 5).



Obrázek 5 – Model s jedním stromem, jedním lesem a jednou doménou

Vztahy důvěryhodnosti

Mezi doménami existuje určitý vztah důvěryhodnosti. V doméně Microsoft Windows Server jsou dva typy těchto vztahů, a to jednosměrný a obousměrný. Když přijde požadavek o přístup k určitému objektu z jiné domény, musí tento požadavek projít cestou důvěryhodnosti. Pokud je mezi doménami A a B nastavena jednosměrná cesta (A → B), můžou uživatelé domény A získat přístup k prostředkům v doméně B (doména B musí důvěřovat doméně A). Opačně to již však nepůjde. U obousměrného vztahu si domény věří navzájem. Uživatelé mohou přistupovat k prostředkům obou domén podle ACL (Access Control List).

„Doména systému Microsoft Windows Server může navázat jednosměrný nebo obousměrný vztah důvěryhodnosti:

- *s doménami systému Windows Server 2003 ve stejné doménové struktuře,*
- *s doménami systému Windows Server 2003 v jiné doménové struktuře,*
- *s doménami systému Windows NT 4.0,*
- *se sférami protokolu Kerberos V5.*[10]

Kerberos V5 je primární protokol zabezpečení pro ověřování v rámci domény. Protokol Kerberos V5 ověřuje identitu uživatele požadujícího ověření i identitu serveru provádějícího požadované ověření. Toto duální ověřování je označováno také jako vzájemné ověření.

Každý řadič domény funguje jako služba KDC. Klient vyhledá pomocí vyhledávání služby DNS (Domain Name Service) nejbližší dostupný řadič domény. Nalezený řadič domény poté tomuto uživateli slouží v průběhu relace přihlášení uživatele jako upřednostňovaná služba KDC. Pokud se upřednostňovaná služba KDC stane nedostupnou, vyhledá systém pro ověřování jinou službu KDC.“[11]

Musí být také zmíněno, že nemusí být jednoduché pojmenovat různé větve stromu. Jsou způsoby, které odpovídají pojmenování podle geografického umístění a dále pojmenování organizační. Každé má své výhody i nevýhody.

Názvy větví podle geografického umístění nabízí větší flexibilitu a rozmanitost. Z jednoho kořene, třeba microsoft.com, můžou vzejít v první úrovni větve jako us.microsoft.com, eu.microsoft.com, asia.microsoft.com atp. Nevýhody mohou nastat při pohledu na strom s větvemi a povahy společnosti, kdy spolu nemusí tyto dva pohledy souviset.

Oproti tomu organizační pojmenování přímo reflektuje strukturu společnosti do těchto názvů. Například opět kořen microsoft.com a jeho větve products.microsoft.com, office.microsoft.com, partners.microsoft.com atp. Z toho

[10] MICROSOFT. *Technická podpora Microsoft Online* [online]. 2012 [online]. 2012 [cit. 2012-11-16]. Dostupné z: http://technet.microsoft.com/cs-cz/library/cc728024(WS.10).aspx
[11] MICROSOFT. *Technická podpora Microsoft Online* [online]. 2012 [online]. 2012 [cit. 2012-11-16]. Dostupné z: http://technet.microsoft.com/cs-cz/library/cc783708(WS.10).aspx

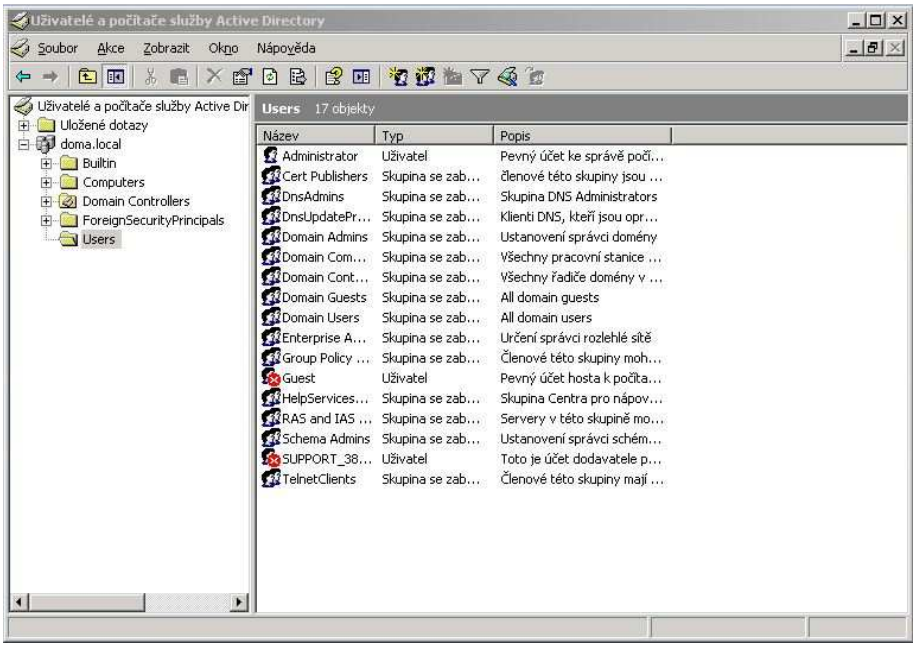
vyplývá, že tento strom je velice přehledný a srozumitelný. Na druhou stranu jej lze obtížně upravovat či rozdělovat.

3.4 Uživatelské účty v Active Directory

Tato část je zpracována podle [1][4][7][12]

Účty zastupují na počítači a v síti jednotlivé objekty nebo fyzické entity neboli počítače nebo osoby. V určitých případech mohou sloužit také pro určité služby nebo aplikace. Někdy jsou také označovány jako objekty zabezpečení. Základní vlastností je tedy přihlášení uživatelů do počítače, kde bude mít každý svůj vlastní prostor, profil. Účty zastupující počítače jdou stejně, tak jako účty uživatelů, ověřovat v síti, proto musí být každý účet počítače unikátní.

Je potřeba, aby se daly tyto objekty a entity neboli účty, jednoznačně rozlišovat. Proto každý účet dostane při vytvoření vlastní identifikátor zabezpečení (SID - Security Identifier), který se pak používá při autorizaci. Všechny tyto účty jsou ve společné databázi Active Directory (obrázek č. 6).



Obrázek 6 – Uživatelské účty a skupiny v Active Directory

Identifikátor zabezpečení pak umožňuje a opravňuje k ověření uživatele nebo počítače v síti. Každý uživatel, by měl mít kvůli bezpečnosti vlastní účet a tím i vlastní kód zabezpečení, se kterým se bude prokazovat při připojení do domény

a dále k přístupu k doménovým prostředkům. Uživateli může být přístup po ověření buď uděleno nebo odepřeno, a to podle nastavených práv a členství ve skupinách.

3.4.1 Profily uživatelů

Po přihlášení do svého uživatelského profilu si tedy může uživatel nastavit prostředí, ve kterém bude pracovat. Například změnou pozadí, velikosti a barvy písma apod., uvidí své dokumenty, bude listovat ve své historii na internetu apod. Je důležité, aby z pohledu bezpečnosti měl každý uživatel nastaveno heslo na svém účtu.

Výčet možností, kam se ukládá uživatelský profil a kde může uživatel měnit svá data:

- Konfiguraci aplikace Průzkumník Windows (například skrytí přípon známých typů souborů či připojené síťové jednotky).
- Nastavení hlavního panelu (například přítomnost panelu Snadné spuštění).
- Nastavení tiskáren (veškeré síťové tiskárny).
- Ovládací panely (veškeré změny v okně Ovládací panely).
- Příslušenství (nastavení aplikací a programů tvořících příslušenství systému Windows - kalkulačka a další).
- Nastavení aplikací (Některé aplikace si ukládají své nastavení - příkladem budiž hlavní panel aplikace Microsoft Word 2000).
- Cookies Soubory (Cookie aplikace Internet Explorer).
- Data aplikací (Data konkrétních aplikací, jako například vlastní slovník aplikace pro zpracování textu. O datech, která se zde budou ukládat, rozhodují sami aplikace).
- Dokumenty:
  - Hudba
  - Obrázky

- Local Settings (Nastavení a data aplikací, jež necestují s profilem uživatele. Jedná se o data specifická pro daný počítač nebo například o velké objemy, jejichž přenos v síti by nebyl efektivní).
  - Data aplikací (Data aplikací závislá na daném počítači).
  - History (Historie aplikace Internet Explorer).
  - Temp (Dočasné soubory).
  - Temporary Internet Files (Mezipaměť offline aplikace Internet Explorer).
- Nabídka Start (Zástupci k programům a aplikacím, např. obsah, který se zobrazí po klepnutí na tlačítko Start).
- Oblíbené položky (Oblíbené položky aplikace Internet Explorer).
- Okolní síť (Zástupci na položky okna Místa v síti).
- Okolní tiskárny (Zástupci na položky okna Tiskárny).
- Plocha (Položky plochy včetně zástupců na ploše).
- Poslední dokumenty (Zástupci k naposledy otevřeným dokumentům).
- SendTo (Zástupci k úložišti dokumentů a k aplikacím).
- Šablony (Zástupci na položky šablon).[12]

V prostředí Microsoft Windows se rozlišují tři základní typy profilů – místní, cestovní a povinné profily.

Místní profil

Místní profil je záležitostí jen určitého počítače. Každý uživatel má svůj a do něj se přihlašuje. Profil je uložen na disku počítače.

[12] ŠETKA, Petr. *Mistrovství v Microsoft Windows Server 2003*. Vyd. 1. Brno: Computer Press, 2003, s. 135-136. ISBN 80-251-0036-7.

Cestovní profil

Oproti tomu, cestovní profil je uložen centrálně na serveru a je vytvořen správcem. Výhoda tohoto profilu je v možnosti použití. K profilu, který byl vytvořen jako cestovní, se může uživatel připojit z kteréhokoliv počítače v doméně. Při přihlášení uživatele ke svému cestovnímu profilu, se mu data uložená na serveru zkopírují na lokální disk počítače. Po jakékoliv změně se opět data ukládají na server. To znamená, že se změna projeví kdekoliv, kde se uživatel přihlásí svým doménovým profilem.

Povinný profil

Povinné profily mají výhodu v tom, že je může používat více uživatelů a při tom zůstanou vždy takové, jako když se vytvořily. Jednoduchým přepsáním koncovky u skrytého souboru Ntuser.dat na NTuser.man v cestovním profilu, se změní chování zápisu souborů na server. Při prvním přihlášení se stáhne profil na disk, ale po odhlášení se již neposílají změny na server a nastavení profilu jsou obnovena do stejného stavu, jako při prvním přihlášení.

3.5 Skupiny uživatelů Active Directory

Cílem spojení uživatelských účtů do skupin je zjednodušení jejich správy. Například, pokud nastane situace, kdy se bude muset aplikovat změna na více počítačů nebo uživatelů najednou. Je poté lepší, když se aplikuje jednou, než když se bude muset nastavovat několikrát. Většinou se spojují uživatelé, kteří mají ve společnosti stejnou nebo podobnou práci. Přistupují do stejných složek, tisknou na stejné tiskárny nebo mají stejná omezení. Například lidé z právního oddělení budou přistupovat do jiných složek, než lidé z obchodního oddělení, nebo finančního.

V Active Directory jsou dvě základní typy skupin. Skupiny se zabezpečením a distribuční skupiny. Ve většině případů se pracuje se skupinami se zabezpečením, a to z důvodu, že se jim dají udělovat práva a oprávnění. Stejně tak jako uživatelské účty i skupiny se zabezpečením mají svůj SID kód. Ten zajistí bezpečnost v síti a určí, kdo má kam přístup a co může člen této skupiny provádět v doméně. Distribuční skupiny se používají výhradně k odesílání e-mailů a nemají SID kód.

3.5.1 Rozsahy skupin

Každé skupině se zabezpečením je přiřazen rozsah skupiny, který říká, do jaké míry lze skupinu použít v doménové struktuře. Rozlišují se tři rozsahy – globální, místní a univerzální.

3.5.2 Globální rozsah

Globální je v tom smyslu, že oprávnění lze přidělovat k prostředkům umístěným v libovolné doméně. Na druhou stranu členové této skupiny mohou pocházet jenom z domény, v níž je skupina vytvořena. Do ní se pak budou řadit nejvíce používané objekty a objekty, které vyžadují častou údržbu. Nejčastěji to tedy budou uživatelské účty a účty počítačů. Tyto účty je možné často měnit, jelikož negenerují replikace do globálního katalogu.

3.5.3 Místní rozsah

Tento rozsah je přímo opakem skupiny globální. Členové této skupiny mohou pocházet z jakékoliv domény, ale přidělení oprávnění lze jenom k prostředkům v doméně, v níž je skupina vytvořena. Například pro přístup k jedné tiskárně pro několik uživatelů, postačí skupina s místním rozsahem.

3.5.4 Univerzální rozsah

Skupina uživatelů s univerzálním zabezpečením může obsahovat členy libovolné domény a mohou jim být přiřazena oprávnění k prostředkům v libovolné doméně. Toto se zdá jako optimální rozsah, ne vždy tomu tak ale je. Tento rozsah může mít za následek zpomalování sítě. Je to důsledek toho, že tyto skupiny jsou se svými členy uvedeny v globálním katalogu a jejich dotazy se musí porovnat s každým objektem těchto skupin.

Tabulka 3[13] shrnuje tyto rozsahy. Jaké členy mohou obsahovat, jaké oprávnění lze přiřadit a na jaký rozsah lze převést.

[13] MICROSOFT. *Technická podpora Microsoft Online* [online]. [cit. 2012-11-14]. Dostupné z: http://technet.microsoft.com/cs-cz/library/cc755692(v=ws.10).aspx

Rozsah skupiny	Skupina může jako členy obsahovat…	Skupině lze přiřadit oprávnění v…	Rozsah skupiny lze převést na…
Univerzální	▪ Účty z libovolné domény v doménové struktuře, ve které se nachází tato univerzální skupina. ▪ Globální skupiny z libovolné domény v doménové struktuře, ve které se nachází tato univerzální skupina. ▪ Univerzální skupiny z libovolné domény v doménové struktuře, ve které se nachází tato univerzální skupina.	Libovolná doména nebo doménová struktura	▪ Místní doménová ▪ Globální (pokud žádné jiné univerzální skupiny neexistují jako členové)
Globální	▪ Účty ze stejné domény jako nadřazená globální skupina ▪ Globální skupiny ze stejné domény jako nadřazená globální skupina	Oprávnění členů lze přiřazovat v libovolné doméně.	Univerzální (pokud není členem žádné jiné globální skupiny)
Místní doménová	▪ Účty z libovolné domény ▪ Globální skupiny z libovolné domény ▪ Univerzální skupiny z libovolné domény ▪ Místní skupiny domény, ale pouze ze stejné domény jako nadřazená místní skupina domény	Oprávnění členů lze přiřazovat pouze v rámci domény, v jaké se nachází nadřazená místní skupina domény	Univerzální (pokud žádné jiné místní skupiny domény neexistují jako členové)

Tabulka 3 - Rozsah skupin

3.6 Group Policy Objects

Tato část je zpracována podle [4][5][7][12]

Group Policy Objects (dále jen GPO) jsou skupiny zásad pro hromadnou správu oprávnění a nastavení objekty uživatelů nebo počítačů umístěných v Active Directory. V těchto skupinách lze vytvářet kolekce nastavení, kterým se říká GPO. Díky nim se dokáže měnit chování počítače nebo uživatele. Jednou aplikací GPO na organizační jednotku v Active Directory lze spravovat potenciálně tisíce počítačů nebo uživatelů.[14]

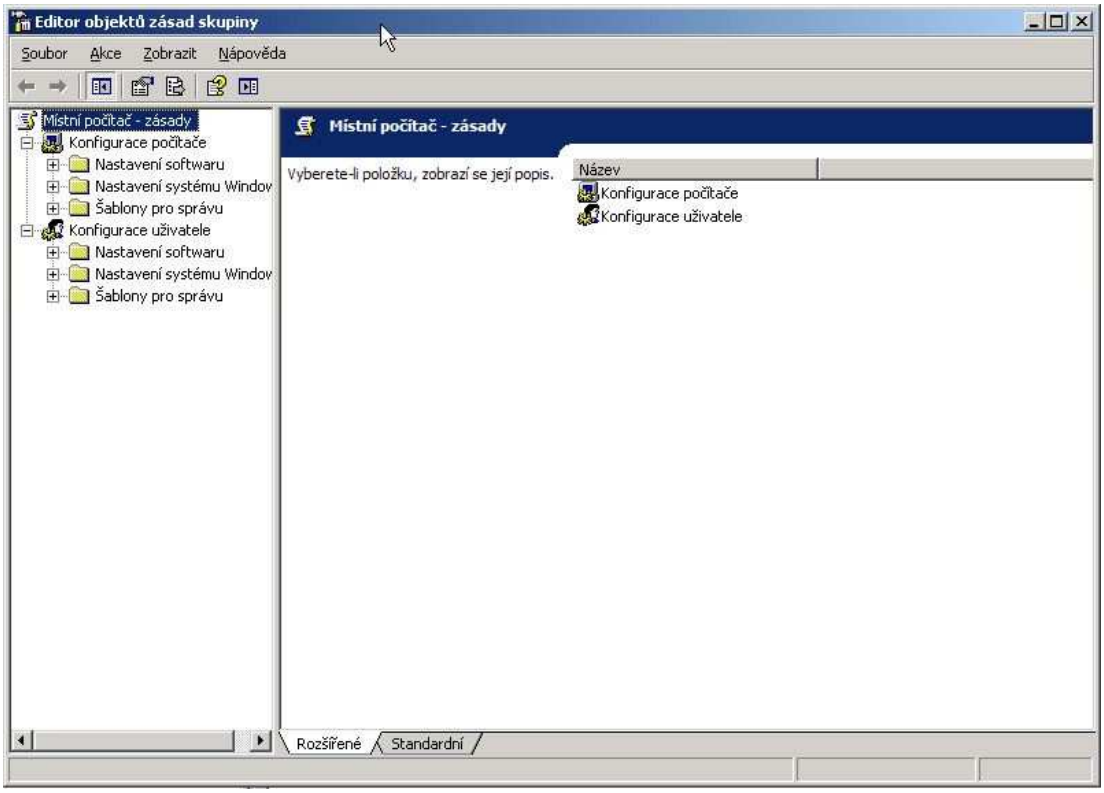
Aplikace zásad je možná dvěma způsoby. První je spuštění počítače a přihlášení uživatele do domény. Druhou možností je aplikace zásad přes automatickou aktualizaci. Ta je ve výchozím nastavení konfigurována tak, že se aplikuje každých 90 minut a musí být provedena v rámci 30 minut, aby nedocházelo k přetížení sítě či doménového řadiče. Aktualizace zajistí, že administrátoři nemusí čekat na aplikaci GPO na další přihlášení počítače nebo uživatele do domény.[15]

Téměř každá zásada má tři možnosti konfigurace, a to – Není nakonfigurováno, povoleno a zakázáno. Pokud v zásadě je nastaveno „Není nakonfigurováno“, platí nastavení nadřazené zásady. Toto je výchozí konfigurace. Při nastavení na „Povoleno“ je zásada platná a platí to, co je uvedeno v její charakteristice. Třetí možnost „Zakázáno“ říká, že je zásada v neplatném stavu.

[14] IT-BLOGUJE. *Blog plný rad a návodů ze světa IT* [online]. 2012 [cit. 2012-11-26]. Dostupné z: http://www.it-bloguje.cz/windows-server/active-directory/70-co-jsou-skupiny-zasad-group-policy.html

[15] OSIF, Michal. *Windows Server 2003*. 1. vyd. Praha: Grada, 2003, 612 s. ISBN 80-247-0396-3.

Všechna nastavení zásad jsou uložena v Active Directory Group Policy Objects a ve složce SYSVOL na doménovém řadiči. Každý objekt zásad se skládá ze dvou částí. Jedna obsahuje nastavení pro počítač a druhá nastavení pro uživatele (obrázek č. 7). Při konfiguraci jedné ze zásad, je možné jedu z částí vypnout pro lepší a rychlejší práci a načítání. Veškerá nastavení provedená v části „Konfigurace počítače“ platí pro každý počítač, bez ohledu na to, který uživatel se k němu přihlásí. Stejně tak, když se provede konfigurace v části „Konfigurace uživatele“, nastavení platí pro každého uživatele, bez ohledu na to, na kterém počítači se přihlásí. V nastavení obou částí je možno se setkat s duplikací nastavení, v tomto případě pak platí to z části „Konfigurace počítače“.



Obrázek 7 - Editor objektů zásady skupiny

Pomocí zásad skupiny lze provádět mnoho nastavení. Microsoft tyto zásady sjednotil do jedné tabulky. Tato tabulka má 1691 řádků a každý z nich zastupuje jedno nastavení. Souhrn lze napsat takto:

- Správa zásad založených na registru pomocí nástroje „Šablony pro správu“. (V modulu „Zásady skupiny“ se vytvoří soubor obsahující nastavení registru, která jsou potom zapsána do částí

databáze registru týkajících se uživatele a místního počítače. Nastavení uživatelského profilu specifické pro uživatele, který se připojuje k dané pracovní stanici nebo serveru, je zapsáno do klíče registru HKEY_CURRENT_USER (HKCU) a nastavení specifické pro počítač je zapsáno do klíče HKEY_LOCAL_MACHINE (HKLM)).

- Přiřazování skriptů. (Tato možnost zahrnuje například skripty pro spuštění a vypnutí počítače nebo přihlášení a odhlášení uživatele.)
- Přesměrování složek. (Můžete přesměrovat složky, například složky Dokumenty a Obrázky, ze složky Documents and Settings v místním počítači do umístění v síti.)
- Správa aplikací. (Pomocí rozšíření Instalace softwaru modulu „Zásady skupiny“ můžete přiřazovat, publikovat, aktualizovat nebo opravovat aplikace.)
- Nastavení zabezpečení. (Nastavení zabezpečení umožňuje administrátorům změnit nastavení zabezpečení přiřazené objektům v Group Policy.)[16]

3.6.1 Implementace Group Policy Objects

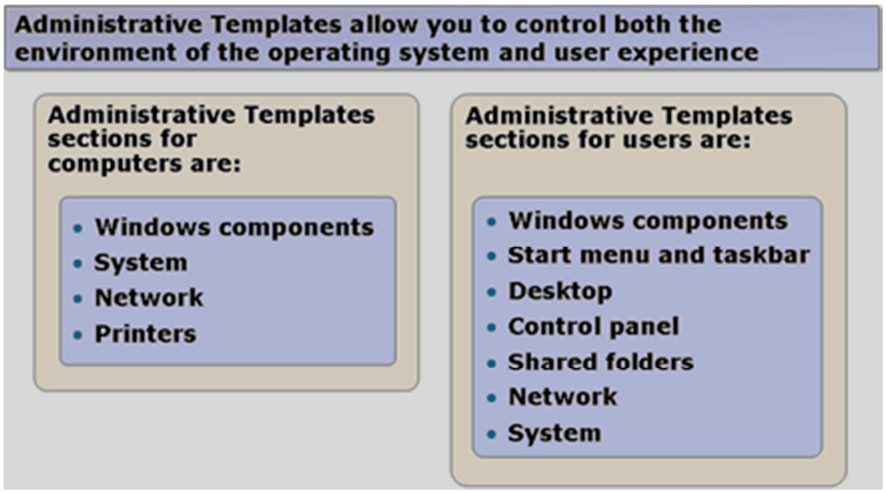
Při aplikaci Group Policy Objects jsou na výběr tři možnosti, kam se umístí. Může se aplikovat na úrovni domény, sítě nebo jednotlivých organizačních jednotek. Skupiny zásad lze také aplikovat i na členské servery a řadiče domény.

Vzhledem k hierarchickému složení Active Directory se můžou tyto zásady skládat, anebo také dědit. Předávají se z nadřazených kontejnerů do podřízených v rámci domény. Při přihlašování uživatele nebo počítače do sítě se zásady aplikují v logickém pořadí. Toto pořadí je „Local Policy“ (místní zásady), zásady pro skupiny sítě, „Domain Policy“ (zásady domény) a nakonec „OU Policy“ (zásady skupiny organizačních jednotek). Největší prioritu pak mají zásady nejblíže k dotčenému objektu. To znamená, že pokud se aplikuje zásada na kontejner vyšší úrovně, tak pro všechny kontejnery, počítače a organizační jednotky pod tímto

[16] MICROSOFT. *Technická podpora Microsoft Online* [online]. [cit. 2012-11-18]. Dostupné z: http://technet.microsoft.com/cs-cz/library/dd349323(en-us,WS.10).aspx

kontejnerem, bude tato zásada platit také. Pokud se poté změní stejná zásada v nějakých podřízených objektech, pak bude platit tato zásada.

Když chtějí administrátoři konfigurovat nastavení v konfiguraci počítače nebo uživatele, můžou jim v tom pomoct takzvané šablony pro správu (soubory ADM). Tyto soubory ADM jsou standardně implementovány v každém operačním systému. Jsou to přednastavené parametry, které umožňují ovládat prostředí operačního systému (obrázek č. 8).[17]



Obrázek 8 – Soubory ADM

V systému Microsoft Windows Server 2003 jsou následující soubory ADM:

- System.adm (Nastavení systému, které řídí funkce, jako jsou plocha, síťová připojení, sdílené složky a Ovládací panely.)
- Inetres.adm (Nastavení aplikace Internet Explorer, které ovládá funkce, jako jsou zóny zabezpečení, nastavení serveru proxy, vyhledávání a dočasné soubory Internetu.)
- Wmplayer.adm (Nastavení programu Windows Media Player, které ovládá funkce, jako jsou nastavení serveru proxy, kodek a vyrovnávací paměť pro síť. Tento nástroj není k dispozici v operačních systémech Windows pro počítače s procesorem Itanium. Tento nástroj není k dispozici v operačních systémech Windows pro počítače s procesorem řady x64.)

[17] IT-BLOGUJE. *Blog plný rad a návodů ze světa IT* [online]. [cit. 2012-11-18]. Dostupné z: http://www.it-bloguje.cz/windows-server/active-directory/72-konfigurace-uzivatelskeho-prostredi-skupiny-zasad.html

- Conf.adm (Nastavení programu NetMeeting, které ovládá funkce, jako jsou sdílení aplikací, zvuk, video a konverzace. Tento nástroj není k dispozici v operačních systémech Windows pro počítače s procesorem Itanium. Tento nástroj není k dispozici v operačních systémech Windows pro počítače s procesorem řady x64.)
- Wuau.adm (Nastavení systému Windows Update, které ovládá funkce, jako jsou automatické aktualizace softwaru prostřednictvím Internetu.)[18]

„Je důležité pochopit, že soubory ADM nepředstavují skutečné nastavení zaváděné do operačních systémů klientů. Soubor ADM je pouze soubor šablony (implementovaný jako textový soubor s příponou ADM) poskytující popisný název pro nastavení a vysvětlení. Tento soubor šablony se používá k naplnění uživatelského rozhraní. Nastavení zaváděné do klientů je obsaženo v souboru registry.pol v rámci objektu zásad skupiny. V systému Windows XP a Windows Server 2003 obsahuje každé nastavení registru informace Supported on (Podporováno v) označující, ve kterých verzích operačního systému je dané nastavení zásad podporováno. Pokud je nastavení zadáno a zavedeno do operačního systému klienta, který nastavení nepodporuje, je toto nastavení ignorováno. Tyto soubory ADM se ve výchozím nastavení ukládají ve dvou umístěních: v rámci objektů zásad skupiny a ve složce %adresář_systému_Windows%\inf v místním počítači.“[19]

3.6.2 Možnosti aplikování Group Policy Objects

Při pohledu na Active Directory a jeho složení z úrovní a při pohledu na její objekty je jasné, že je více přístupů jak aplikovat zásady skupiny GPO. První pohled je ten, že se zásady skupiny aplikují na jednotlivé úrovně, na celou doménu, na celou síť nebo na organizační jednotky. Druhý pohled se odehrává na úrovni omezení přístupu oprávnění pro konkrétní uživatele, nebo dle členství ve skupině. Každý má svá specifika, výhody a nevýhody.

[18] MICROSOFT. *Technická podpora Microsoft Online* [online]. [cit. 2012-11-18]. Dostupné z: http://technet.microsoft.com/cs-cz/library/cc779058(WS.10).aspx
[19] MICROSOFT. *Technická podpora Microsoft Online* [online]. [cit. 2012-11-18]. Dostupné z: http://technet.microsoft.com/cs-cz/library/cc779058(WS.10).aspx

Když se aplikují zásady organizačnímu útvaru, tím pádem všem podřízeným útvarům a objektům, aplikují se díky pouhé příslušnosti uživatelů v těchto útvarech. Toto nastavení je výchozí a je vhodné například pro geografické rozložení domény nebo při rozložení organizačních jednotek podle funkcí v organizaci. Horší je pak pro administrátory vytváření těchto zásad, jelikož musí vyhovět všem dotčeným objektům.

Zásady se většinou aplikují na velký počet uživatelů a objektů. Pokud je však potřeba, aby jeden z této skupiny tyto zásady neměl aplikované, může se buď vyčlenit z dosahu této zásady, nebo se mu omezí přístup k nim. Potom se mu aplikují jenom ty zásady, u kterých má nastaveno oprávnění „Apply Group Policy“ (aplikovat zásady skupiny). To má výhodu v tom, že lze zásady aplikovat nezávisle na umístění uživatele nebo objektu ve struktuře domény.

Lze doporučit použití obou dvou pohledů najednou. Pominou nevýhody jednoho či druhého pohledu a je to mnohem efektivnější. Menší nevýhodou je potřeba stanovení pravidel, kterým zásadám skupin jsou a kterým nejsou definována přístupová oprávnění.

4. Analytická část

V této kapitole budou řečeny výhody novějšího serverového systému Microsoft Windows Server 2008 oproti výše hodnocenému Microsoft Windows Server 2003. Nejdříve však uvedení teorie z předchozí části práce do praxe.

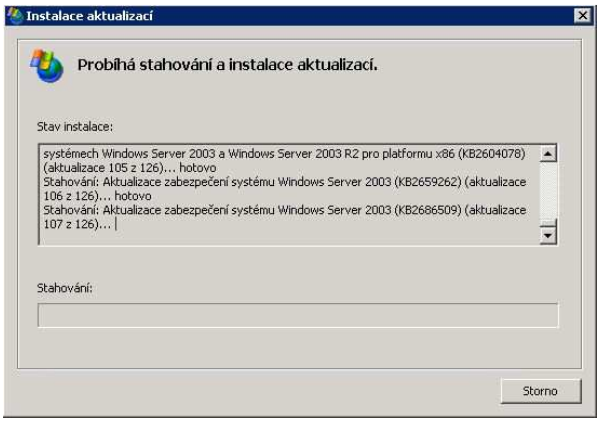
4.1 Vytvoření serverového prostředí

V této části je podrobněji vysvětleno, jak se nainstaluje server a jeho prostředí tak, aby byl schopen obsluhovat jak pár počítačů, tak menší společnost.

4.1.1 Instalace serveru Microsoft Windows Server 2003

Instalace začíná vložením CD do mechaniky nebo z ISO souboru při instalaci na virtuální počítač a poté se pokračuje podle pokynů na obrazovce. Po dokončení kopírování souborů pro instalaci a restartu se instalace dostane do příjemnější oknové podoby. V místním a jazykovém nastavení se nastaví jazykové prostředí a klávesnice. Poté se zadá „Produkt Key“ (klíč k produktu) a na další stránce způsob licencování. Dalším krokem je pojmenování stanice a nastavení hesla administrátora. Pokud heslo nesplňuje požadavky na náročnost, je požádáno o nové, případně se dá pokračovat dále na „vlastní nebezpečí“, což autor nedoporučuje (u verze Microsoft Windows Server 2008 již tato volba není a musí se zadat bezpečné heslo). V následujícím kroku se může nastavit síť, jelikož ale bude podrobněji nastavena v další části práce, je ponecháno „Typické nastavení“ sítě. Počítač se nebude připojovat do domény, neboť z něj bude jediný doménový řadič s vlastní doménou.

Po dokončení instalace, restartu a prvním přihlášení vyskočí tabulka s důrazným varováním a žádostí o instalaci kritických aktualizací (obrázek č. 9). Autor doporučuje je nainstalovat zároveň i s balíčky záplat, pokud nějaké jsou.



Obrázek 9 - Instalace kritických aktualizací

Poté co je nainstalován a aktualizován systém je nutné nastavit síťové prostředí, viz následující kapitola.

Nastavení sítě

Tato část je zpracována s pomocí zdrojů [2][6]

Je více možností jak nastavit síť. Pro účely této práce bude stačit jeden z privátních rozsahů IP adres:

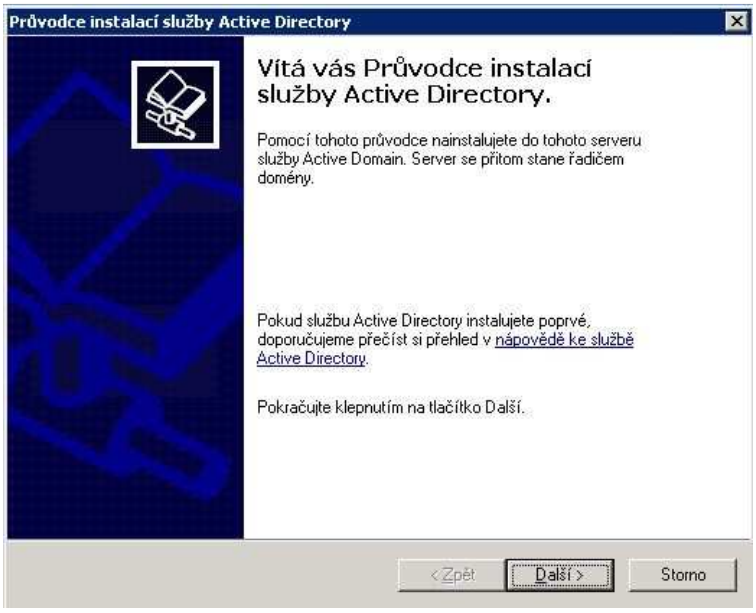
- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255[20]

Server DHCP bude autor nastavovat tak, aby IP adresy byly v posledním privátním rozsahu, se kterým se dá vytvořit nejvíc omezený počet adres.

Vytvoření rolí

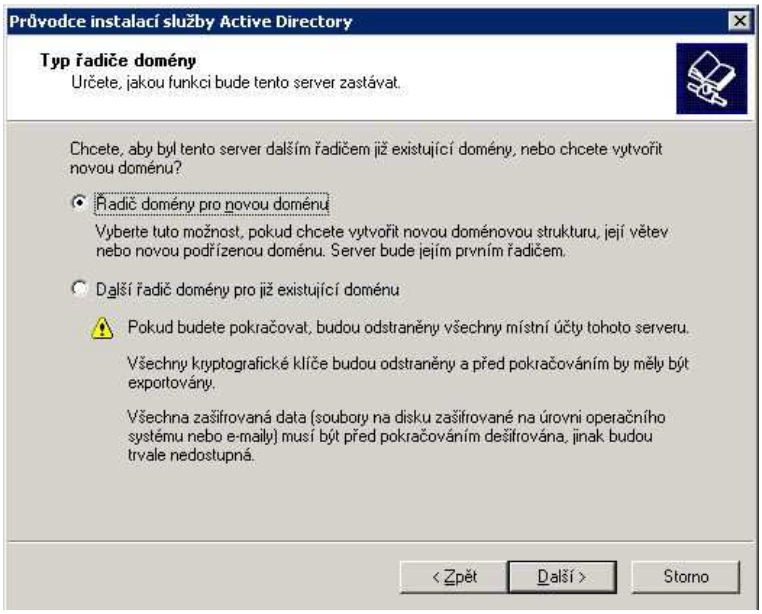
První se bude instalovat adresářová služba Active Directory a s ní služba DNS. Klávesovou zkratkou tlačítek Win+R se spustí konzole „spustit“ a do té se vepíše příkaz „dcpromo“. Tímto začne instalační proces služby Active Directory (obrázek 10).

[20] DOSTÁLEK, Libor a Sharon CRAWFORD. *Velký průvodce protokoly TCP/IP a systémem DNS: hotová řešení*. 3. aktualiz. a rozš. vyd. Praha: Computer Press, 2002, xiv, 542 s. Administrace (Computer Press). ISBN 80-722-6675-6.



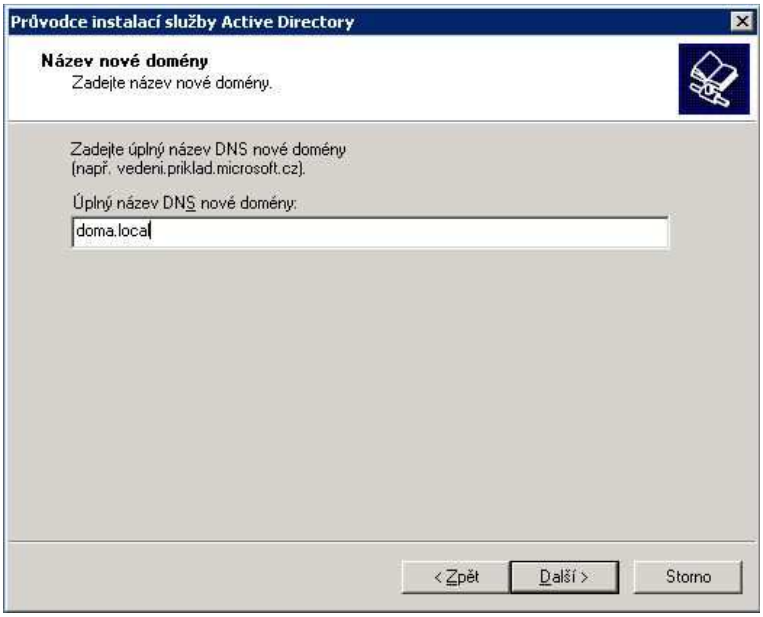
Obrázek 10- Spuštění instalace Active Directory

V dalším kroku je pak na výběr jestli chce uživatel vytvořit nový doménový řadič nebo ho přidat do již existující domény (obrázek č. 11).



Obrázek 11 - Typ řadiče domény

Následující krok žádá o upřesnění typu domény – Doména v nové struktuře (první doména), podřízená doména v existující větvi, Větev v existující doménové struktuře. Je vybráno „Doména v nové doménové struktuře“, neboť to bude nový doménový řadič s jednou doménou. V dalším kroku se zadá úplný název nové domény (obrázek č. 12) a hned na to se pojmenuje doména pro systém NetBIOS.



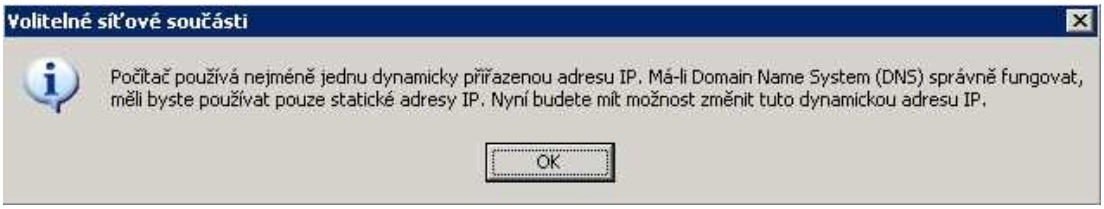
Obrázek 12 - Úplný název nové domény

Následně se určí umístění databáze NTDS a souboru jeho protokolu, standardně to je „C:\windows\NTDS“ a to je ponecháno. Stejně tak i umístění složky SYSVOL.

V dalším kroku je nutné nainstalovat a nakonfigurovat službu DNS. Vybere se výchozí oprávnění pro uživatele skupiny, a to „Oprávnění kompatibilní pouze s operačními systémy řady Windows 2000 Server nebo Windows Server 2003“, neboť opět není v plánu instalovat jiné servery. Další krok vyzývá k vytvoření hesla pro obnovení adresářových služeb. Je tedy zadáno a pokračuje se dále. Nyní se již počká na dokončení procesu instalace (obrázek č. 13).

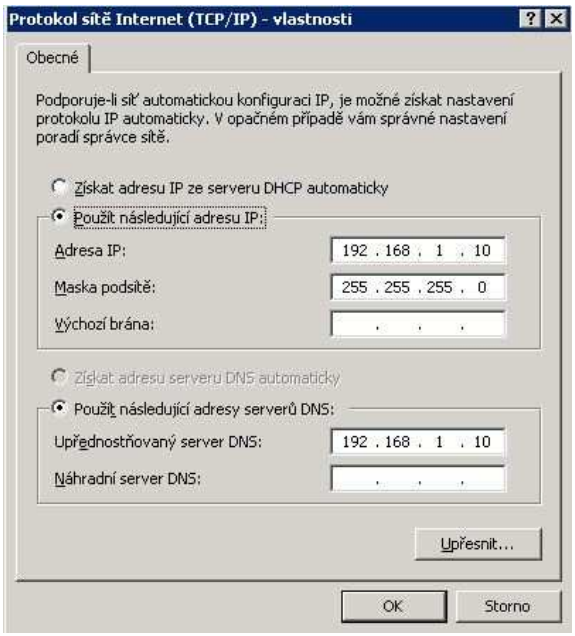
Obrázek 13 - Dokončení instalace Active Directory

Jelikož nebyla služba DNS nainstalována a konfigurována před instalací Active Direcotory, musí se nastavit nyní (obrázek č. 14).



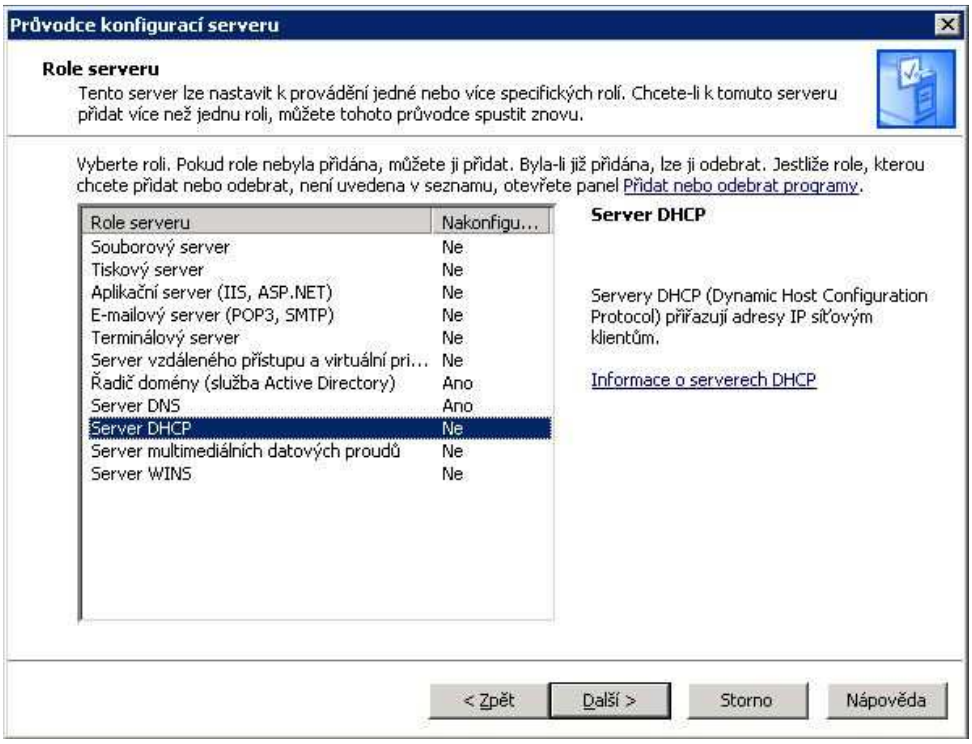
Obrázek 14 - Konfigurace IP adres

Nastavení bude řešeno pomocí privátního rozsahu 192.168.0.0/16, tudíž adresa a maska podsítě bude nastavena takto (obrázek č. 15). DNS server bude odkazovat zpět na tento server, aby byl sám sobě DNS klientem.



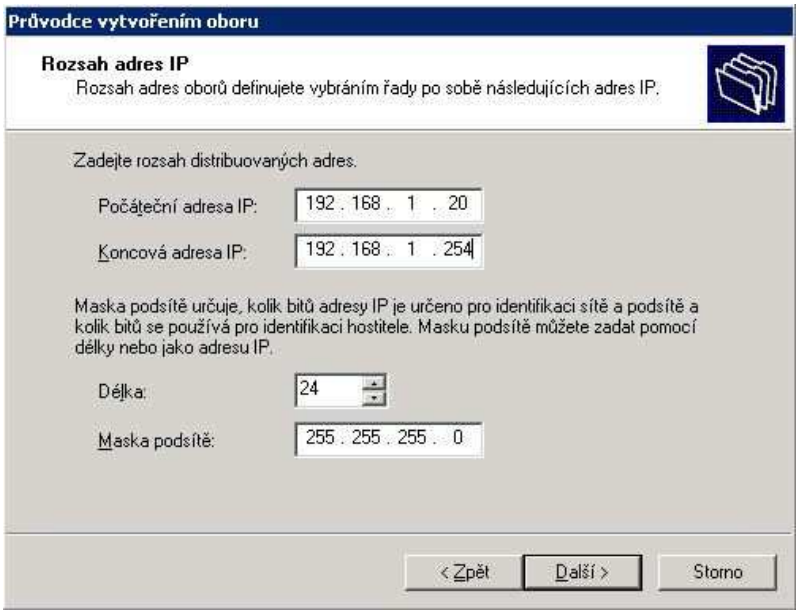
Obrázek 15 - Nastavení protokolu TCP/IP

Poté již stačí jen dokončit instalaci a restartovat server. Pokud je potřeba, aby počítače v síti dostávaly automaticky IP adresu a nemusela se zadávat ručně, je nezbytné ještě nainstalovat služba DHCP (obrázek č. 16).



Obrázek 16 - Spuštění instalace serveru DHCP

Při instalaci služby DHCP je nutné vytvořit nový obor. Vytvoří se jeden obor, který autorovi pro tuto práci bude stačit, přitom se zadá rozsah adres, které budou automaticky přiřazovány počítačům v doméně (obrázek č. 17).



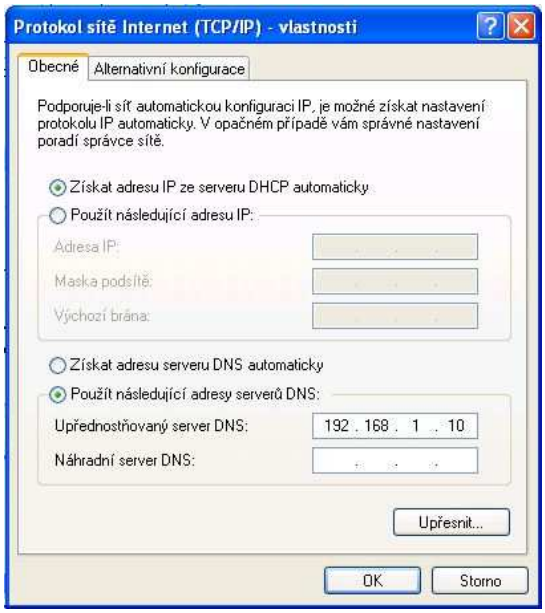
Obrázek 17 - Rozsah IP adres pro počítače v doméně

Na následující obrazovce lze nastavit rozsah IP adres, které nebude server distribuovat. Většinou to bývá z důvodu přiřazení těchto adres serverům, tiskárnám, přenosným zařízením apod. To nyní není třeba nastavovat. Výchozí brána taktéž není potřeba nastavovat, jelikož počítače budou v jednom IP rozsahu. Po dokončení je nutné autorizovat DHCP a aktivovat nový rozsah (obrázek č. 18 a obrázek č 19).

Obrázek 18 - Autorizace DHCP

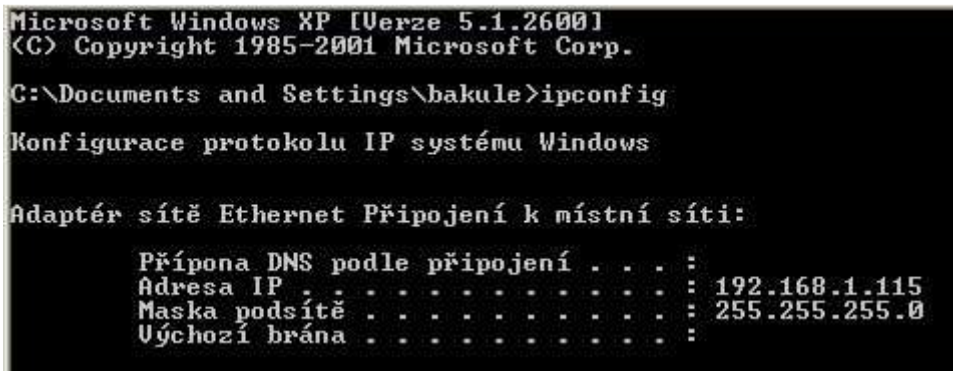
Obrázek 19 - Aktivace rozsahu DHCP

Nyní je vše připraveno k užívání ze strany serveru. Jelikož je žádoucí, aby se daly počítače obsluhovat, musí se k doméně nejdříve připojit. Tyto počítače musí mít správně nastaven protokol TCP/IP k připojení do sítě. Jelikož už běží na serveru služba DHCP a DNS, nastavení bude vypadat takto (obrázek č. 20).



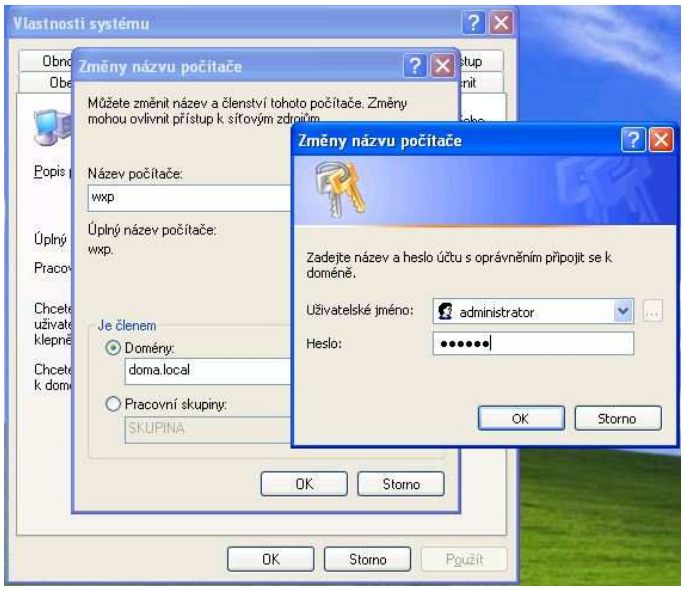
Obrázek 20 - Nastavení TCP/IP na uživatelském počítači

Toto nastavení lze ověřit přes příkazový řádek (Command line, dále již jen CMD). Na uživatelském počítači se spustí CMD, přes již známou zkratku Win+R a konzoli „spustit“. Po otevření se do ní vepíše příkaz „ipconfig“ a potvrdí klávesou Enter. Následující obrazovka (obrázek č 21) zobrazí nastavení TCP/IP s adresou, kterou mu přidělil server DHCP.



Obrázek 21 - Výpis přidělené IP adresy serverem v CMD

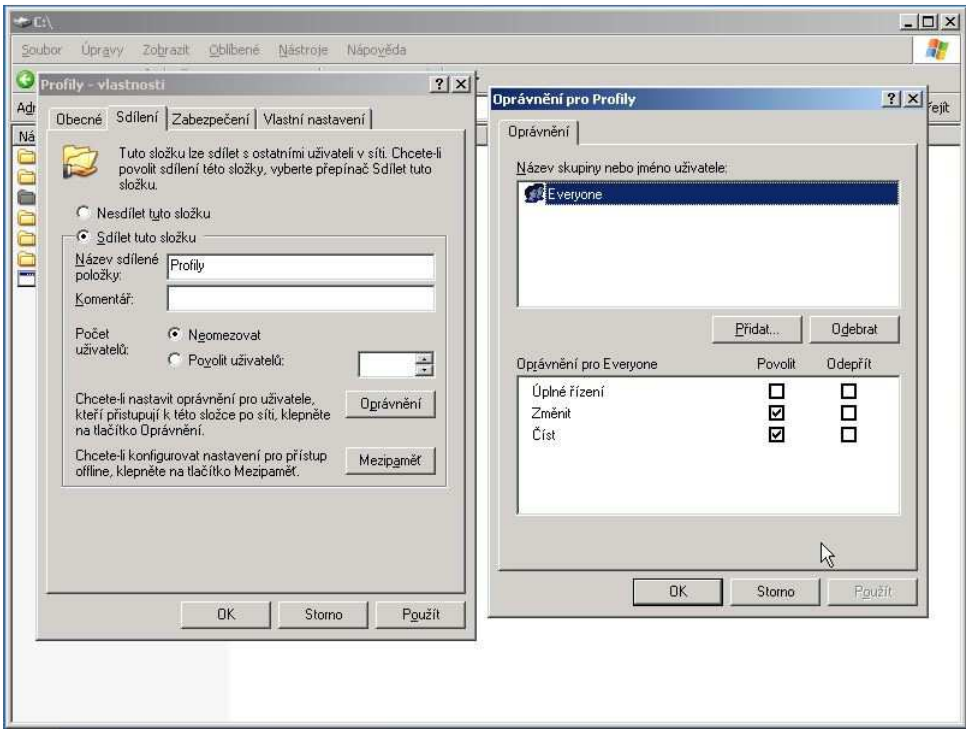
Připojení k doméně provádí uživatel, který má povoleno přidávat počítače do domény. Většinou to je člen skupiny doménových administrátorů. Po přihlášení uživatele s lokálními administrátorskými právy, který může měnit členství počítače ve skupinách, zobrazení vlastností tohoto počítače a přechodu na kartu „Název počítače“, se klikne na tlačítko „Změnit“. Poté bude zobrazeno okno, kam se zadá název domény, ke které je potřeba počítač připojit a následně v dalším okně se ověří uživatel s doménovými právy, který dokončí připojení počítače do domény (obrázek č. 22). Po následném restartu je počítač připojen do domény.



Obrázek 22 - Připojení počítače do domény

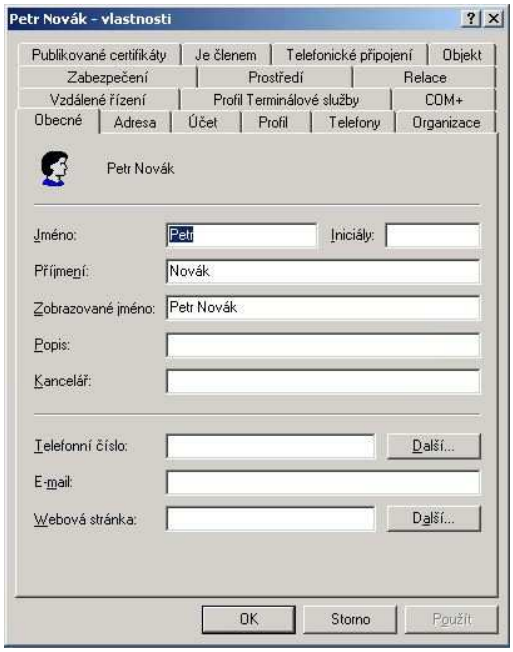
4.1.2 Vytvoření doménového cestovního profilu

V první řadě, při vytváření cestovního profilu, se musí vytvořit sdílené umístění někde v síti, kam mají všichni uživatelé přístup. Většinou to je jeden ze serverů. Do tohoto umístění se pak ukládá profil uživatele. Při vytváření nesmí být zapomenuto na zabezpečení složky. Uživatelé, kteří budou přistupovat k této složce, musí mít povoleno minimálně čtení a změny obsahu složky (obrázek č. 23).



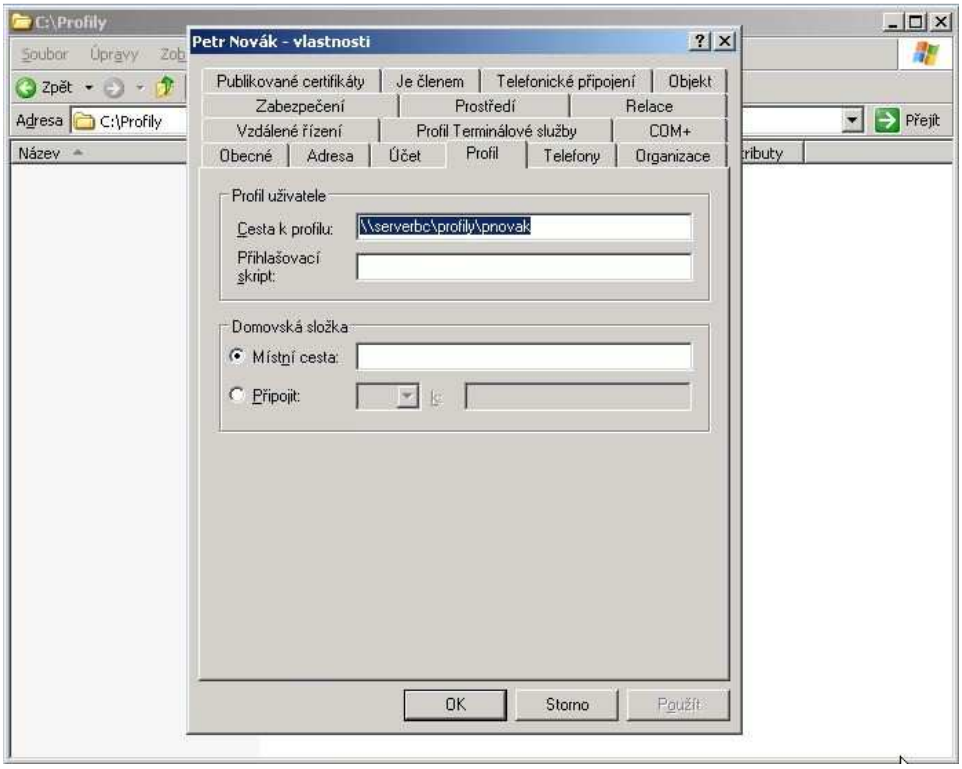
Obrázek 23 - Vytvoření cestovního profilu

V konzoli „Uživatelé a počítače služby Active Directory“ na doménovém řadiči, v kontejneru Users (uživatelé), se vytvoří požadovaný uživatel. Obrázek 24 poskytuje pohled na vlastnosti uživatelského účtu.



Obrázek 24 - Karta vlastností uživatelského účtu

Poté co je vytvořen uživatel a doplněny všechny patřičné vlastnosti účtu, je potřeba doplnit cestu k profilu. V záložce „Profil“ je políčko „Cesta k profilu“, kam se doplní UNC (Universal Naming Convention) cesta k již vytvořené sdílené složce na serveru (obrázek č. 25).

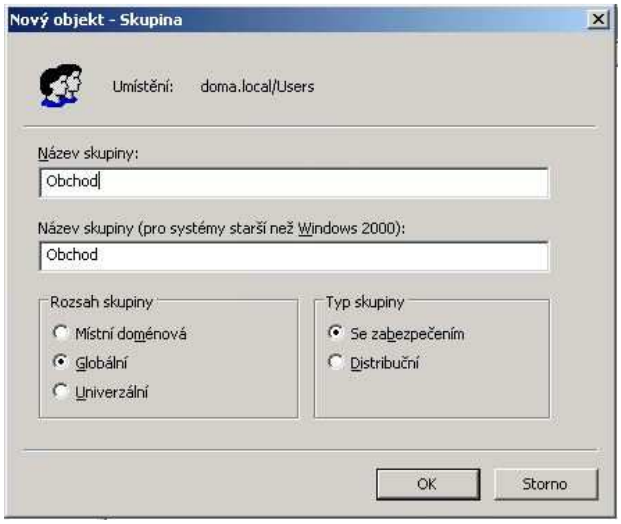


Obrázek 25 - UNC cesta k profilu

V tuto chvíli je vytvořen panu Novákovi účet s cestovním profilem, který, jak je vidět na Obrázku 25 (okno s adresářem C:\Profily je prázdné), zatím není na serveru uložen. To se stane po prvním přihlášení uživatele na počítač.

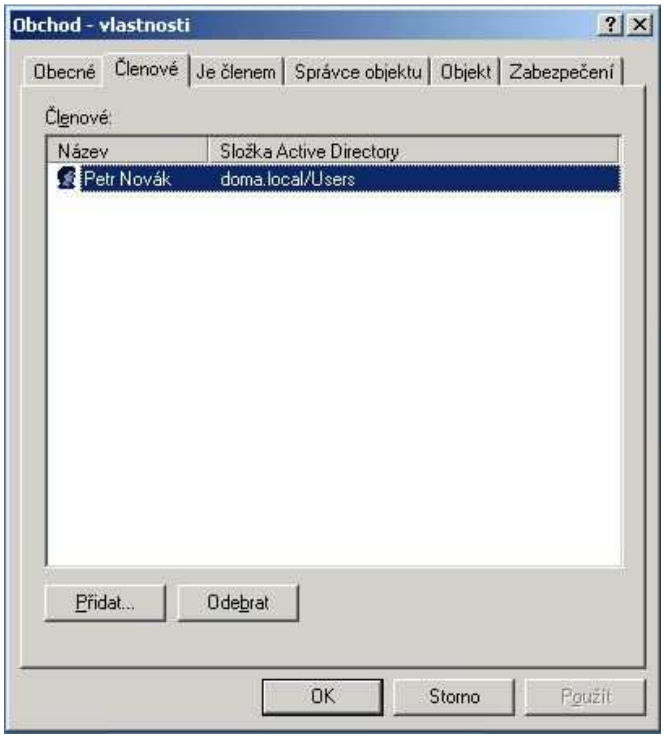
4.1.3 Přiřazení uživatelského účtu ke skupinám

Po otevření konzole s uživatelskými účty a skupinami Active Directory (obrázek č. 26), jsou vidět již přednastavené skupiny. Pokud je potřeba vytvořit novou skupinu, může se použít postup přes tlačítko „Akce“, dále „Nová položka“, kde se vybere „Skupina“. Je nutné vyplnit název skupiny, její rozsah a typ. Ten bude většinou označen na políčku skupiny se zabezpečením. Rozsah je na uvážení, viz kapitola 3.5. Obrázek 27 přiblíží vzhled okna při vytváření skupiny.



Obrázek 26 - Vytvoření skupiny v Active Directory

Po rozkliknutí vlastností nově vytvořené skupiny, je vidět, že má více možností k doplnění informací, stejně tak jako uživatelský účet. Není jich tolik, ale k detailnější charakteristice skupiny to stačí. Nejdůležitější je záložka „Členové“. Zde se dá upravovat kdo bude členem této skupiny a kdo ne. Kliknutím na tlačítko přidat a výběrem uživatele, se přidá uživatel (obrázek č. 27).



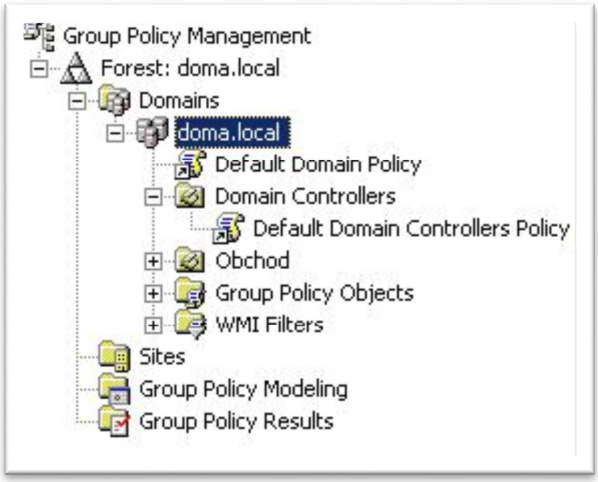
Obrázek 27 - Členové skupiny Obchod

V této záložce jsou vidět uživatelé nebo také jiné skupiny, kteří náleží do této skupiny. Další záložka „Je členem“ již napovídá, že se jedná o výpis nadřazených skupin, kterých je členem.

V takto omezeném prostředí autor nemusí dodržovat standardní strategie řazení do skupin, například AGDLP (Accounts, Global group, Domain local group, Permissions).

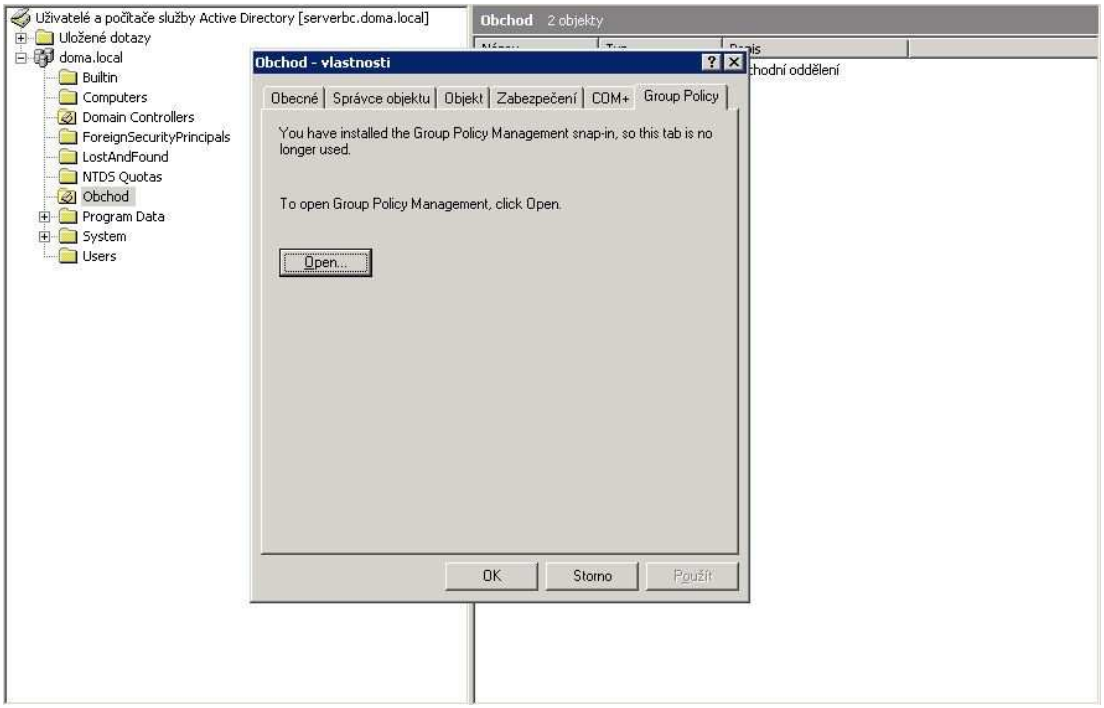
4.1.4 Vytvoření a použití Group Policy Objects

Pokud chce administrátor ovlivnit všechny počítače a všechny uživatele v doméně, pak nemusí vytvářet novou skupinu zásad, ale může použít přednastavenou, která se jmenuje Default Domain Policy, která se vytvoří automaticky po instalaci služby Active Directory. Další automaticky vytvořená zásada je Default Domain Controllers Policy. Ta je rovnou aplikována na kontejner, který obsahuje jenom doménové řadiče (obrázek č. 28).



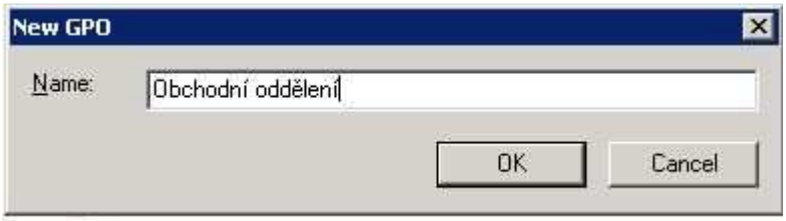
Obrázek 28 - Default Domain a Default domain Controller Policy

Pokud je potřeba vytvořit novou zásadu skupiny, například pro obchodní oddělení, najde se kontejner pro obchodní oddělení v konzoli „Uživatelé a počítače služby Active Directory“, otevřou se jeho vlastnosti a na záložce „Group Policy“ se klikne na tlačítko „Open“ (obrázek č. 29).



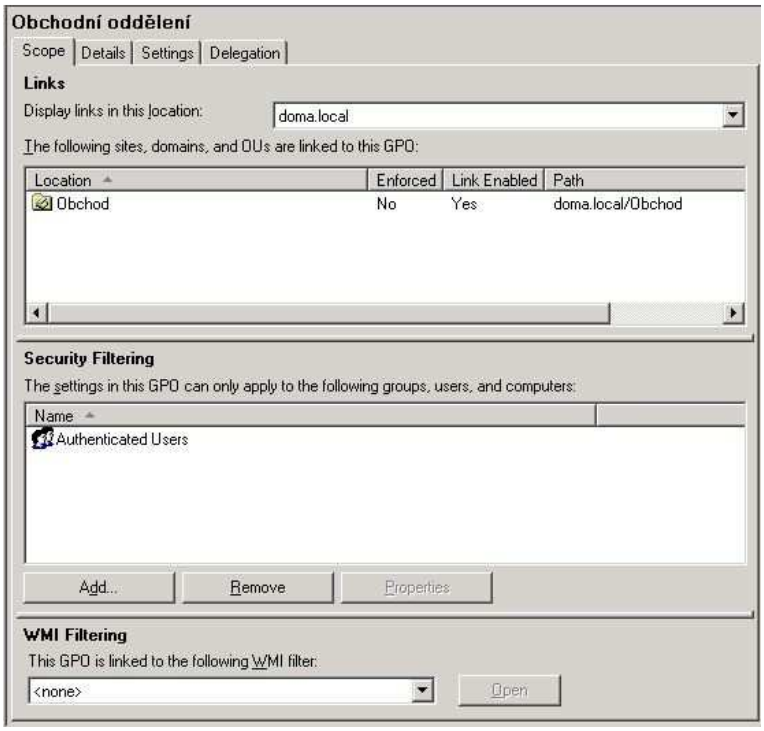
Obrázek 29 - Otevření Group Policy Objects pro určitou skupinu

Po těchto úkonech se otevře konzole „Group Policy Management“, kde se vytváří, upravují a aplikují zásady skupiny. Pravým klikem na složku „Group Policy Objects“ a rozkliknutí možnosti „New GPO“ (nová zásada skupiny) se otevře okénko vybízející k pojmenování nové zásady (obrázek č. 30).



Obrázek 30 - Pojmenování nové zásady skupiny

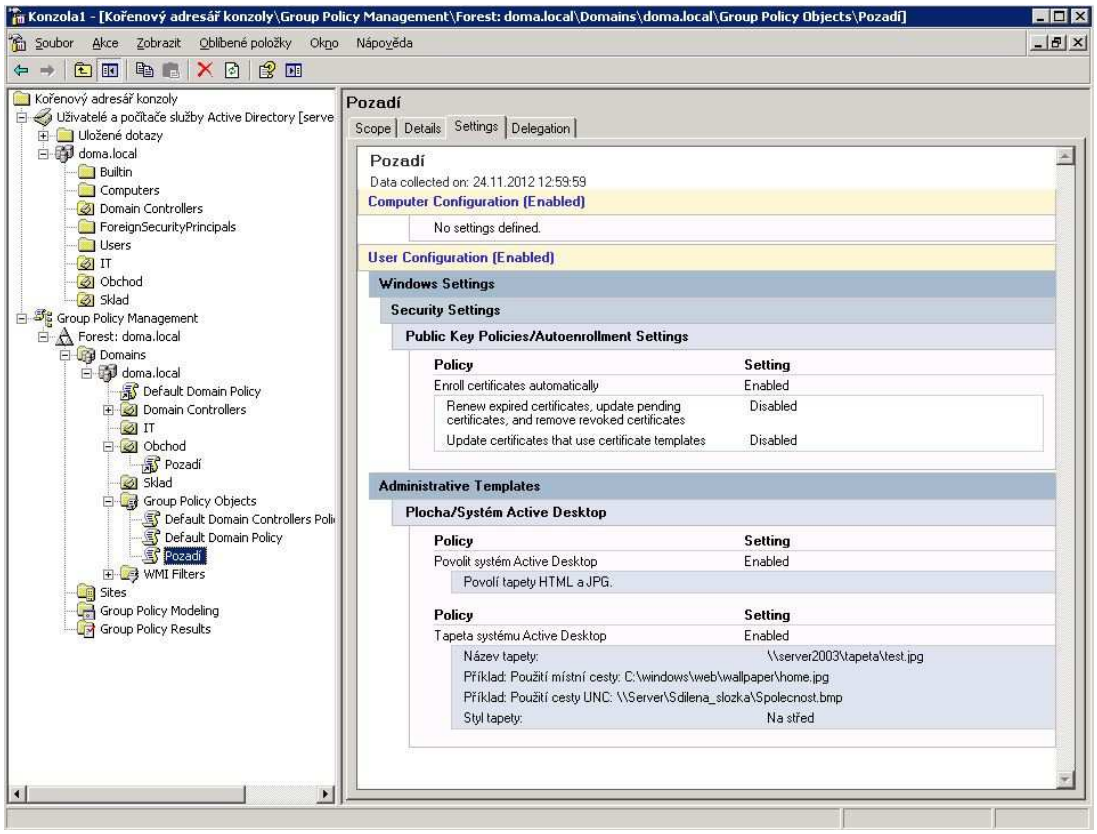
Tímto je vytvořena nová zásady skupiny pojmenovaná „Obchodní oddělení“. Na Obrázku 31 je vidět výčet nastavení zásady – „Scope“, „Details“, „Settings“ a „Delegation“.



Obrázek 31 - Detaily zásady skupiny pro Obchodní oddělení

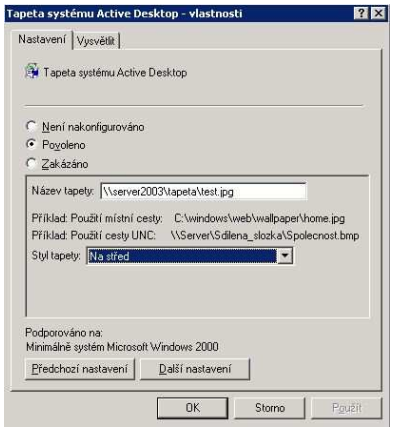
„Scope“ (rozsah nebo dosah) určuje, kde platí tato zásada, „Details“ (detaily) vypisují kdo a kdy vytvořil tuto zásadu, kdy byla modifikována, jestli je platná atp., záložka „Settings“ (nastavení) zobrazuje výčet provedených nastavení a poslední záložka „Delegation“ (delegace) zobrazuje výčet uživatelů a jejich oprávnění vztahujících se k této zásadě.

Pro příjemnější práci se zásady skupiny, autor doporučuje instalaci Group Policy Management Console (dále již jen GPMC). Přidáním modulů snap-in do konzole MMC se zjednoduší a zpřehlední správa zásady skupiny. Pokud se přidají ty správné moduly, tak je vidět struktura Active Directory a pod tím, struktura zásad skupiny. Podle mínění autora, je v takto vytvořené konzoli menší prostor pro chyby (obrázek č. 32).



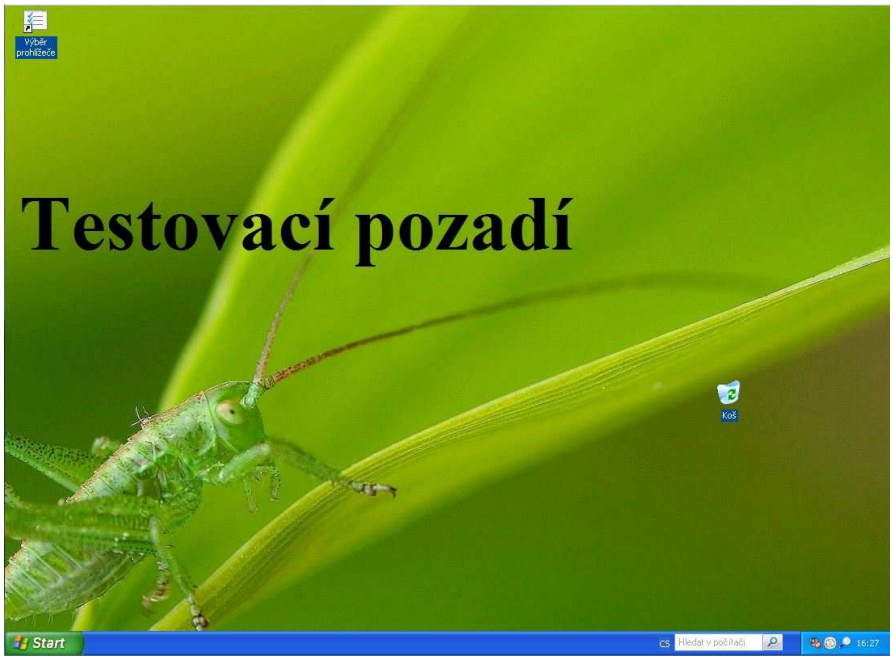
Obrázek 32 - Konzole MMC pro správu zásad skupiny

Nyní se vytvoří testovací zásada skupiny a aplikuje se na kontejner Obchod. Na kontejner „Group Policy Objects“ se klikne pravým tlačítkem a zvolí se nová zásada skupiny. V editaci této zásady lze nastavit například nové pozadí plochy (obrázek č. 33) a poté se nastavená GPO přetáhne na kontejner Obchod (obrázek č. 32).



Obrázek 33 - Nastavení pozadí v GPMC

Po přihlášení uživatele na počítač nebo po automatické aplikaci GPO se na pozadí zobrazí požadované pozadí (obrázek č. 34).



Obrázek 34 - Nastavené testovací pozadí přes GPO

4.2 Srovnání s Microsoft Windows Server 2008

Tento serverový systém spojuje to nejlepší z předchozího operačního systému s na jednu stranu ne moc povedeným, ale přesto pokrokovým, systémem Windows Vista. Pokrokovým, jelikož již od aktualizace Service Pack 1 pracuje na novém jádře NT 6.0[21]. Hlavní vylepšení je určitě opět v dalším nárůstu výkonu a dalším rozšíření nastavení a správy ve všech částech operačního systému.

4.2.1 Přehled Microsoft Windows Server 2008

Tato část je zpracována podle [5][9][11]

Stejně tak jako jeho předchůdce se vydává Microsoft Windows Server 2008 v podstatě ve stejných edicích se stejným účelem.

- Windows Web Server 2008
- Windows Server 2008 Standard
- Windows Server 2008 Enterprise

[21] STANEK, William R. *Mistrovství v Microsoft Windows Server 2008: [kompletní informační zdroj pro profesionály]*. Vyd. 1. Brno: Computer Press, 2009, 1364 s. ISBN 978-80-251-2158-0.

- Windows Server 2008 Datacenter

Dále jsou vydány ještě edice bez podpory technologie Hyper-V a opět 64bitové verze. Windows server 2008 je poslední z řady 32bitových serverových operačních systémů. Verze 2008 R2 je již výhradně 64bitový systém.

Windows Web Server 2008

Moc se neliší od předchozí verze, snad jen v podpoře novějších technologií jako IIS 7.0, .NET Framework atd. a podpoře více pamětí a procesorů.

Windows Server 2008 Standard

Základní verze operačního systému poskytující mnoho funkcí s několika vylepšeními, a to jsou – sítě SAN (Storage Area Network), oznamování úložišť, zdokonalené přístupové služby apod.

Windows Server 2008 Enterprise

Opět řešení pro větší organizace. Výhoda proti minulé verzi je v podpoře clusteringu až do osmi uzlů a konfigurace VLM (Very Large Memory) s podporou velmi velkých pamětí. Je to až 32 GB ve 32bitových systémech a 2 TB v případě 64bitových systémů.

Windows Server 2008 Datacenter

Nejvýkonnější verze obsahující vše co má verze Enterprise, navíc s podporou 64 procesorů a zdokonalené VLM, protože umožňuje nasadit konfigurace až do 64 GB paměti v 32bitových systémech a v 64bitových systémech až 2TB.

Změnou prošly i hardwarové požadavky na systém. V Následující Tabulce 4[22] jsou požadavky shrnuty a je k ní i přiřazen sloupec pro porovnání s verzí Windows Server 2003.

[22] MICROSOFT. *Microsoft Download Center* [online]. 2007 [cit. 2012-11-21]. Dostupné z: http://www.microsoft.com/en-us/download/default.aspx

Operační systém	Minimální rychlost procesoru	Podpora více procesorů	Místo na disku pro instalaci	Paměť	Minimální systémové požadavky Windows Server 2003 a jeho edic
Windows Server 2008 Standard Edition	1 GHz	Maximálně 4	8 GB	512 MB	CPU min. 400 MHz (doporučeno 733 MHz), 512 MB RAM (doporučeno 1 GB), 1,5 GB místa na disku Systém podporuje maximálně 64 GB paměti RAM a vyžaduje nejméně 8, nejvíce 32 procesorů
Windows Server 2008 Enterprise Edition	1 GHz	Maximálně 8	9 GB	513 MB	CPU min. 133 MHz (doporučeno 550 MHz), 128 MB RAM (doporučeno 256 MB), 1,5 GB místa na disku Systém podporuje maximálně 4 GB paměti RAM a nejvíce 4 procesory
Windows Server 2008 Datacenter Edition	1 GHz	Max. 32 pro platformu x86 a až 64 pro platformy x64 a Itanium	10 GB	514 MB	CPU min. 133 MHz (doporučeno 733 MHz), 128 MB RAM (doporučeno 256 MB), 1,5 GB místa na disku Systém podporuje maximálně 32 GB paměti RAM a nejvíce 8 procesorů
Windows Server 2008 Web Edition	1 GHz	Maximálně 4	11 GB	515 MB	CPU min. 133 MHz (doporučeno 550 MHz), 128 MB RAM (doporučeno 256 MB), 1,5 GB místa na disku Systém podporuje maximálně 2 GB paměti RAM a nejvíce 2 procesory
Windows Server 2008 Itanium a IA 64 Edition	1 GHz	Maximálně 64	12 GB	516 MB	

Tabulka 4 - Systémové požadavky pro Microsoft Windows Server 2008

Jedna z největších výhod dle autora je určitě možnost virtualizace serverů. Virtualizace byla možná i do doby než přišel Microsoft Windows Server 2008, ale nyní je virtualizace vestavěna přímo v systému. Další výhodou je určitě možnost instalace jádra serveru, kde se nainstaluje jen omezené prostředí s vysokým zabezpečením. Je zde zcela vynecháno grafické rozhraní a pro správu je tedy nutno používat příkazový řádek nebo skripty. Další možnost je správa pomocí MMC z jiného počítače. Po instalaci takovéhoto serveru se nabízí instalace rolí jako například DHCP server, server DNS, IIS, tiskový server, souborový server, služba Active Directory apod. Neméně důležitou novinkou je prostředí PowerShell, kde je možné vytvářet skripty a výrazné vylepšení terminálových služeb, kde již není potřeba sdílet celou plochu připojeného počítače, ale stačí sdílet samotnou aplikaci.

4.2.2 Role Microsoft Windows Server 2008

Tato část je zpracována podle [5][9][11]

Z předchozí verze systému jsou přebrány veškeré role. Některé jsou jen pozměněny, některé vylepšeny a některé jsou úplně nové. Následný seznam bude obsahovat některé vylepšené nebo nové role:

- AD CS (Active Directory Certificate Servies)
- AD DS (Active Directory Domain Services)
- AD LDS (Active Directory Lightweigh Directory Services)
- AD RMS (Active Directory Rights Management Services)
- Aplikační server
- Souborové služby
- Terminálové služby
- Virtualizace

a další jako Clustering, zásady skupiny, brána Firewall s pokročilým zabezpečením, prostředí PowerShell apod.

Pro autora jsou zásadní změny ve virtualizaci, rozšíření MMC konzole a služeb Active Directory.

Virtualizace

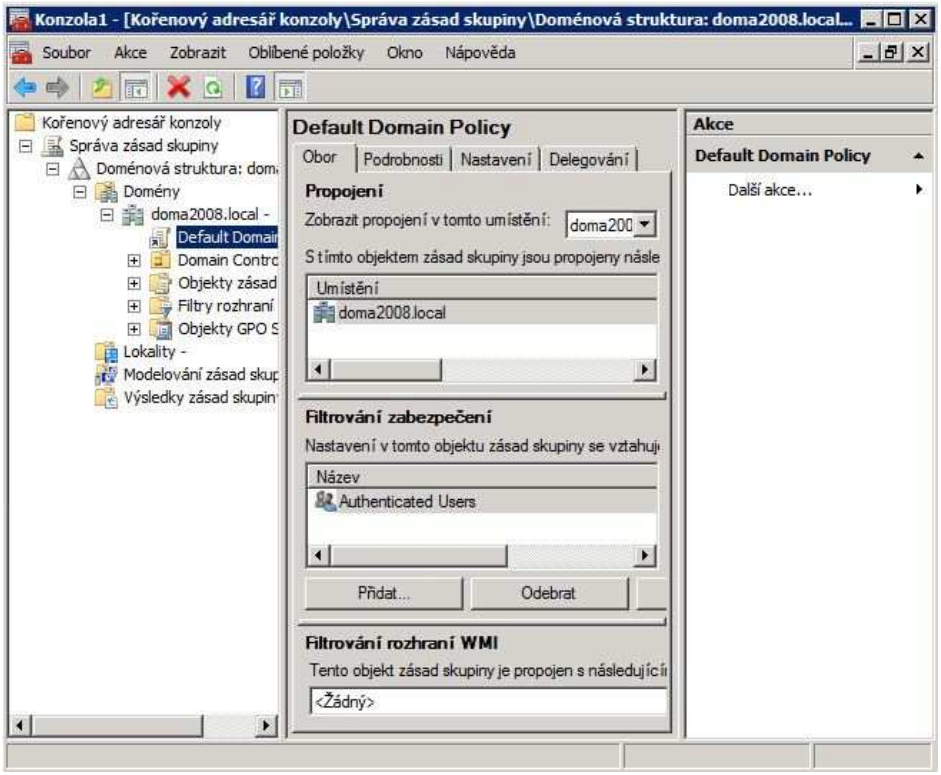
Virtualizace umožňuje vytvářet virtualizované prostředí serveru pomocí technologie, která je součástí operačního systému Windows Server® 2008. Toto řešení je poskytováno prostřednictvím nástroje Hyper-V™. Virtualizované počítačové prostředí lze použít k efektivnější práci s počítačem lepším využitím hardwarových prostředků.[23]

Technologie Hyper-V vychází z technologií Virtual PC a Virtual Server a pracuje obdobně. Počet počítačů nainstalovaných do virtuální podoby závisí na hardwarové výbavě daného stroje. Další výhodou je možnost instalací jiných operačních systémů, než jenom ty od společnosti Microsoft. Pokud se společnost rozhodne pro instalaci systému UNIX, není potřeba nového stroje, ale stačí ho nainstalovat do virtuální podoby.

[23] MICROSOFT. *Technická podpora Microsoft Online* [online]. [cit. 2012-11-24]. Dostupné z: technet- http://technet.microsoft.com/cs-cz/library/cc755090(WS.10).aspx

MMC konzole

V MMC konzoli bylo přidáno podokno Akce pro přehlednější a snadnější zjištění dostupných akcí pro vybranou položku (obrázek č. 35). Toto podokno lze i případně skrýt.



Obrázek 35 - Nová MMC konzole 3.0

Je zde zdokonalené oznamování o chybách a nyní konzole poskytuje i řešení chyb, které by mohly způsobit její selhání. Anebo zjednodušené přidávání modulů snap-in a rozšíření jejich dostupnosti. (Staněk 2008)

Autorovi se zejména líbí ovládání serveru a jeho částí přes MMC konzoli, aniž by musel přistupovat na server. Jednoduše se MMC konzole nainstaluje na počítač a vzdáleně obsluhuje například službu DNS.

4.2.3 Doména Active Directory Microsoft Windows Server 2008

Jedna z nejdůležitějších změn je podle autora možnost restartu nebo zastavení služby Active Directory. Dává to možnost zlepšení údržby databáze, instalace aktualizací apod. Další vhodná změna je v možnosti definovat politiky pro hesla. Lze nastavovat komplexnost, délku hesla atp. a tyto politiky následně přiřazovat

jednotlivým kontejnerům, či uživatelům. Co také může potěšit je možnost instalace doménového řadiče jen pro čtení.[24]

4.2.4 Group Policy Objects

Pro autora je největší navýšení počtu položek nastavení zásad skupiny. V předchozí verzi serverového systému jich bylo kolem 1600, nyní jich je již přes 3000. V příloze jsou obě tabulky pro porovnání. S tím souvisí i další vylepšení a to je filtrování těchto zásad.

Nemenší změnou prošla i GPMC a novinkou je konzole GPP (Group Policy Preferences). Výhody této nové konzole vidí autor například ve snadnějším mapování síťových disků pro uživatele, práce s registry, nastavení vlastností složek apod.

[24] MICROSOFT. *TechNet Blog CZ/SK* [online]. [cit. 2012-11-24]. Dostupné z: http://blogs.technet.com/b/technetczsk/archive/2007/09/20/novinky-ad-serveru-windows-serveru-2008-v-kostce.aspx

5. Zhodnocení výsledků a závěr

Cílem autora bylo přiblížení a charakteristika serverových operačních systémů od společnosti Microsoft. Jmenovitě to byl Microsoft Windows Server 2003 a jeho srovnání s novějším systémem. Snahou bylo vystižení důležitých funkcí pro chod serveru v síti a zároveň průřez jeho rolí. Tyto role jsou důležité pro základ síťové struktury, ale samozřejmě je nutné brát v úvahu další role, nebo rozrůstání počtu počítačů, nebo serverů v síti. To by však znamenalo instalaci dalších rolí, případně doménových řadičů apod.

Názorně byla provedena instalace serveru a jeho konfigurace, instalace rolí popsaných v teoretické části práce, vytvoření doménových uživatelských účtů a aplikace zásad omezení skupiny. Na závěr práce byly vylíčeny výhody novějšího systému a to Microsoft Windows Server 2008. Zhodnocení těchto poznatků by mělo vyústit ve volnou diskuzi čtenářů na téma přechodu na novější verzi systému. Případně by práce měla dát námět na hlubší poznání novějšího systému.

Pro osvojení centralizované správy počítačů a doménového prostředí si autor myslí, že byl vybrán dostačující serverový systém. Jelikož není úplně tak zastaralý (stále se v současné době používá), je jednoduchý a účinný, vychází z něj další řada dalších nových systémů a obsahuje důležité funkce, které ale nejsou ještě zdaleka tak komplikované jako v prostředí novějšího serverového systému.

Je jasné, že jde vývoj rychle dopředu a novější funkce jsou žádané. Sice zjednodušují v některých situacích úkony administrátora, může být ale mnohem složitější si je osvojit. Rozdíl mezi popsanými systémy je, dá se říci, skoro generační, přesto ten starší systém je důstojný zástupce serverové řady operačních systému od společnosti Microsoft.

Tato práce se nesnažila o dokonalé přiblížení prostředí serverů, ale o pochopení alespoň základních úkonů práce se serverem a prostředí centralizované správy. Obsah této bakalářské práce je tedy úměrně daný její velikosti.

6. Seznam použitých zdrojů

1) CAFOUREK, Bohdan a Sharon CRAWFORD. *1001 tipů a triků pro Microsoft Windows Server 2003: hotová řešení*. Vyd. 1. Brno: Computer Press, 2004, 415 s. Administrace (Computer Press). ISBN 80-251-0351-X.

2) DOSTÁLEK, Libor a Sharon CRAWFORD. *Velký průvodce protokoly TCP/IP a systémem DNS: hotová řešení*. 3. aktualiz. a rozš. vyd. Praha: Computer Press, 2002, xiv, 542 s. Administrace (Computer Press). ISBN 80-722-6675-6.

3) HOLME, Dan a Orin THOMAS. *MCSA/MCSE Self-paced training kit (Exam 70-290): managing and maintaining a Microsoft Windows Server 2003 environment*. Vyd. 1. Washington: Microsoft Press, 2004, xxxiv, [760] s. Administrace (Computer Press). ISBN 07-356-1437-7.

4) MALINA, Patrik a Sharon CRAWFORD. *Microsoft Windows Server 2003: hotová řešení*. Vyd. 1. Brno: Computer Press, 2006, 358 s. Administrace (Computer Press). ISBN 80-251-1096-6.

5) MICROSOFT. *Resources and Tools for IT Professionals | TechNet* [online]. 2012. Dostupné z: http://technet.microsoft.com/en-us/

6) MUELLER, John a Sharon CRAWFORD. *Příkazový řádek Windows pro Windows Vista, 2003, XP a 2000: hotová řešení*. Vyd. 1. Brno: Computer Press, 2008, 656 s. Administrace (Computer Press). ISBN 978-80-251-1961-7.

7) OSIF, Michal a Orin THOMAS. *Windows Server 2003: managing and maintaining a Microsoft Windows Server 2003 environment*. 1. vyd. Praha: Grada, 2003, 612 s. Administrace (Computer Press). ISBN 80-247-0396-3.

8) RUSSEL, Charlie a Orin THOMAS. *Microsoft windows server 2003: velký průvodce administrátora*. Vyd. 1. Brno: Computer Press, 2005, 1374 s. Administrace (Computer Press). ISBN 80-251-0579-2.

9) RUSSEL, Charlie a Sharon CRAWFORD. *Microsoft Windows Server 2008: velký průvodce administrátora*. Vyd. 1. Brno: Computer Press, 2009, 1271 s. Administrace (Computer Press). ISBN 978-80-251-2115-3.

10) SAMURAJ-CZ.COM. *Počítačové sítě, Cisco, administrace a webcoding* [online]. 2012. Dostupné z: http://www.samuraj-cz.com/

11) STANEK, William R a Sharon CRAWFORD. *Mistrovství v Microsoft Windows Server 2008: [kompletní informační zdroj pro profesionály]*. Vyd. 1. Brno: Computer Press, 2009, 1364 s. Administrace (Computer Press). ISBN 978-80-251-2158-0.

12) ŠETKA, Petr. *Mistrovství v Microsoft Windows Server 2003*. Vyd. 1. Brno: Computer Press, 2003, 680 s. ISBN 80-251-0036-7.

6.1 Seznam obrázků

6.2 Seznam Tabulek

6.3 Seznam použitých zkratek

ACE (Access Control Entry) - záznam v seznamu přístupových práv

ACL (Access Control List) - seznam přístupových práv

AD CS (Active Directory Certificate Servies) – služba, která poskytuje přizpůsobitelné služby pro vytváření a správu certifikátů veřejných klíčů

AD DS (Active Directory Domain Services) – služba, která ukládá informace o uživatelích, počítačích a dalších zařízeních v síti

AD LDS (Active Directory Lightweigh Directory Services) – služba, která Zajišťuje ukládání a načítání dat pro aplikace s povolenými adresáři

AD RMS (Active Directory Rights Management Services) – služba, která má za cíl ochranu informací bez ohledu na jejich umístění

AGDLP (Accounts, Global, Domain Local, Permissions) – strategie přiřazování zabezpečení uživatelských účtů

AMD (Advanced Micro Devices) - americká firma vyvíjející CPU, GPU, čipsety a technologie

ASP .NET - je součást aplikace .NET Framework pro tvorbu webových aplikací a služeb

CD (Compact Disk) – disk na přenos dat

CMD (Command line) – příkazový řádek

CPU (Central Processing Unit) - procesor

DHCP (Dynamic Host Configuration Protocol) - server přidělující automaticky IP-adresy

DNS (Domain Name Systém) - hierarchický systém doménových jmen

EPIC (Explicitly parallel instruction computer) - architektura 64-bitových procesorů

FTP (File Transfer Protocol) - protokol pro přenos souborů mezi počítači

GPMC (Group Policy Management Console) – konzole pro správu zásad skupiny

GPP (Group Policy Preferences) - rozšíření Group Policy

IMAP4 (Internet Message Access Protocol verze 4) – protokol pro přístup k emailovým zprávám

IIS (Internet Information Services) - webový server s kolekcí rozšiřujících modulů

ISO - soubor obsahující digitální kopií dat na optickém disku

KDC (Key Distribution Center) - spravuje databázi uživatelů a přiděluje jim tikety

LDAP (Lightweight Directory Access Protocol) - protokol pro ukládání a přístup k datům na adresářovém serveru

MB, GB, TB (MegaByte, GigaByte, TeraByte) – měrné jednotky objemu dat v IT

MHz (MegaHertz) – jednotky frekvence

MMC (Microsoft Management Console) – konzole pro správu nástrojů počítačů

NTDS (Windows NT Directory Services) – úložiště pro Active Directory

POP3 (Post Office Protocol) - internetový protokol, který se používá pro stahování emailových zpráv ze vzdáleného serveru na klienta

RAM (Random Access Memory) – operační paměť počítače

SID (Security Identifier) – identifikační číslo

SAN (Storage Area Network) – oddělená datová síť, která slouží pro připojení externích zařízení k serverům

SMTP (Simple Mail Transfer Protocol) - internetový protokol určený pro přenos emailů

TCP/IP (Transmission Control Protocol/Internet Protocol) - sada protokolů pro komunikaci v počítačové síti a

UNC (Universal Naming Convention) - Jedná se o cestu ve formátu. \\<computername>\<sharename>\<filename>

VLM (Very LArge Memory) – metoda pro využití většího počtu paměti v počítači

VPN (Virtual Private Network) - propojení mezi dvěma počítači realizovaná přes privátní nebo veřejnou síť

WINS (Windows Internet Naming Service) - slouží jako name server pro jména počítačů v síťovém prostředí NetBIOS

6.4 Rejstřík pojmů

Clustering – spojování více serverů tak, že navenek vypadají jako jeden

Hardware – fyzický materiál, z něhož se sestavují počítače

Internetová brána - uzel, který spojuje dvě sítě s odlišnými protokoly

Software – počítačové programy v počítači

PowerShell – prostředí pro vytváření skriptů

7. Přílohy

Karta	Popis
Obecné	Obsahuje jméno uživatele, popis, umístění kanceláře, telefonní číslo, e-mailovou adresu a adresy webových stránek
Adresa	Obsahuje fyzickou adresu uživatele
Účet	Obsahuje přihlašovací jméno, omezení pro přihlášení, možnosti hesla a zda vyprší platnost účtu
Profil	Zobrazuje cestu k profilu uživatele, cestu ke skriptu spouštěnému při přihlašování uživatele, cestu k domovské složce a všechna automatická připojení jednotek
Telefony	Udává další telefonní čísla, např. operátoru, mobilního telefonu a telefonu IP
Organizace	Obsahuje titul uživatele, oddělení, společnost, nadřízeného pracovníka a přímé podřízené pracovníky
Vzdálené řízení	Slouží ke konfiguraci úrovně, na které může správce zobrazovat nebo řídit relace Terminálové služby uživatele
Profil Terminálové služby	Obsahuje profil Terminálové služby uživatele
COM+	Obsahuje členství uživatele v sadách oddílů modelu COM+
Je členem	Udává členství uživatele ve skupinách
Telefonické připojení	Obsahuje údaje o telefonickém připojení uživatele
Prostředí	Nastavení prostředí Terminálové služby u uživatele
Relace	Nastavení odpojení a obnovení Terminálové služby

Tabulka 5 - Karty uživatelských účtů