Služby systému Windows Server 2008 a jejich konfigurace

Services of Windows Server 2008 and their configuration

Zdeněk Habrman

Bakalářská práce
2011

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2010/2011

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Zdeněk HABRMAN**
Osobní číslo:	**A08596**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Informační a řídicí technologie**
Téma práce:	**Služby systému Windows Server 2008 a jejich konfigurace**

Zásady pro vypracování:

1. **Popište, nainstalujte a zprovozněte základní síťové služby (DHCP, DNS, File Server).**
2. **Server využijte k připojení vnitřní LAN k Internetu a zprovozněte Active Directory.**
3. **Nakonfigurujte automatické pravidelné zálohování serveru.**
4. **Popište a vyzkoušejte sledování aktualizací systému MS Windows na pracovních stanicích (WSUS).**
5. **Uveďte nejběžnější útoky na počítačovou síť a možné způsoby obrany.**

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **HORÁK, Jaroslav; KERŠLÁGER, Milan. Počítačové sítě pro začínající správce. 4., aktualiz. a rozš. vyd. Brno : Computer Press, 2008. 327 s. ISBN 978-80-251-2073-6.**
2. **SOSINSKY, Barrie. Mistrovství - počítačové sítě : [vše, co potřebujete vědět o správě sítí]. Vyd. 1. Brno : Computer Press, 2010. 840 s. ISBN 978-80-251-3363-7.**
3. **LUDVÍK, Miroslav; ŠTĚDROŇ, Bohumír. Teorie bezpečnosti počítačových sítí. 1. vyd. Kralice na Hané : Computer Media, 2008. 98 s. ISBN 978-80-86686-35-6.**
4. **STANEK, William R. Microsoft Windows Server 2008 : kapesní rádce administrátora. Vyd. 1. Brno : Computer Press, 2008. 704 s. ISBN 978-80-251-1936-5.**
5. **ALLEN, Robbie; LIŠKA, Alois; LOWE-NORRIS, Alistair G. Active Directory : implementace a správa Microsoft Active Directory. 1. vyd. Praha : Grada, 2005. 644 s. ISBN 8024709732.**
6. **PRICE, Brad. Active Directory : optimální postupy a řešení problémů. Vyd. 1. Brno : CP Books, 2005. 381 s. ISBN 80-251-0602-0.**

Vedoucí bakalářské práce: **Ing. Jiří Korbel**
Ústav počítačových a komunikačních systémů

Datum zadání bakalářské práce: **25. února 2011**

Termín odevzdání bakalářské práce: **7. června 2011**

Ve Zlíně dne 25. února 2011

prof. Ing. Vladimír Vašek, CSc.
děkan

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.
①

prof. Ing. Vladimír Vašek, CSc.
ředitel ústavu

ABSTRAKT

Cílem této bakalářské práce je návrh implementace *Windows Server 2008 R2 Foundation* a jeho služeb pro malou firmu.

Teoretická část se věnuje obecnému popisu vybraných síťových služeb, rozebírá jejich funkci a přínosy při použití v počítačové síti.

Praktická část navazuje na teoretickou, popisuje instalaci a konfiguraci zmíněných služeb. Závěr se věnuje nejčastějším útokům na síť a možnosti ochrany proti nim.

Klíčová slova: Windows Server 2008 R2, DHCP, DNS, Active Directory Domain Services, WSUS

ABSTRACT

The aim of this bachelor thesis is implementation of *Windows Server 2008 R2 Foundation* and its roles for a small company.

The theoretical part contains general description of selected network services, their functions and benefits when they are used in the network.

The practical part follows the theoretical and describes the installation and configuration of those services. The conclusion is focused on the most common network attacks and possible protection against them.

Keywords: Windows Server 2008 R2, DHCP, DNS, Active Directory Domain Services, WSUS

PODĚKOVÁNÍ

Rád bych poděkoval následujícím osobám:

Ing. Jiřímu Korbelovi, Ph.D, vedoucímu mé bakalářské práce, který mi vždy poradil a vedl tuto práci k úspěšnému konci.

Ing. Martinu Kubíčkovi, za důvěru a prostor při implementaci celého projektu a aplikování této bakalářské práce.

A mým rodičům, za obrovskou podporu při studiu.

MOTTO:

„Každá lidská činnost se nakonec musí nějak projevit v číslech.“

Tomáš Baťa

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, 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 (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….

podpis diplomanta

Obsah

ÚVOD

Informační technologie jsou nedílnou součástí každodenního života, jak pracovního tak osobního, a nároky na ně stále rostou. Cennější nežli samotné přístroje jsou ovšem zpracovávané informace. Proto se v poslední době klade velký důraz na bezpečnost a obnovitelnost informace. Také někdy vzniká potřeba pracovat s těmito informacemi z jiného místa než obvykle, a to s důrazem na stejnou bezpečnost.

Takové potřeby jsou samozřejmostí ve firemním prostředí. Pro firmu jsou stabilní a rychlá síť, sdílené prostředky, rychlé pracovní stanice stejně důležité jako pro lékaře kvalitní nástroje a spolehlivé přístroje. Nejen že zrychlují, ale také zefektivňují práci programů, šetří náklady. Vše musí být pod dohledem administrátora, který se o celý provoz stará.

Jádrem firemní sítě je server, který musí být po hardwarové stránce velice výkonný. Těchto systémů je celá řada od různých výrobců. V této práci byl vybrán nejnovější produkt od Microsoftu.

Cílem této bakalářské práce je popsat instalaci, zprovoznění a správu základních služeb Windows Serveru 2008 R2 Foundation. Tento systém obsahuje kompletní řešení pro malou firmu a velkou mírou přispívá k zabezpečení dané sítě, a tím i samotných dat.

V teoretické části jsou popsány jednotlivé základní služby systému, které jsou součásti implementace pro firmu.

V praktické části jsou popsány jednotlivé instalace a konfigurace těchto služeb s ohledem na požadavky zadavatele. Jelikož se nevyužijí všechny služby systému, lze jeho využití v budoucnu ještě rozšířit. Popis všech služeb, které Windows Server nabízí, je obsahově nad rámec této práce, a proto je pozornost věnována funkcím důležitým pro základní chod serveru pro malou firmu.

I. TEORETICKÁ ČÁST

1 MICROSOFT WINDOWS SERVER 2008 R2

Systém Windows Server 2008 R2 představuje dosud nejpokročilejší operační systém Windows Server, navržený pro podporu nové generace sítí, aplikací a webových služeb. Pomocí systému WS je možné vyvíjet, distribuovat a spravovat komfortní uživatelská prostředí i aplikace, zajišťovat zabezpečenou síťovou infrastrukturu a zvyšovat technologickou vyspělost nebo hodnotu organizace. Systém WS staví na úspěších a pevných základech předchozích verzí platformy WS, ale zároveň přináší cenné nové funkce i významná vylepšení základního operačního systému. Nové webové nástroje, virtualizační technologie, vylepšení zabezpečení a nástroje pro správu přináší úsporu času, snižují náklady a vytváří pevný základ IT infrastruktury. [10]

Jedná se tedy o přímého nástupce Windows Server 2003. Jeden z nejzásadnějších rozdílů je, že verze 2008 je pouze 64bitová. Vylepšení je celá řada, např. virtualizace pomocí technologie Hyper-V, vylepšený výkon sítí, zvýšené zabezpečení a lepší plnění požadovaných pravidel, zdokonalené skriptování pomocí PowerShellu, ochrana sítě před připojením počítačů s nevyhovující konfigurací zabezpečení a také optimalizace se systémem Windows 7, dále došlo k vylepšení Terminálové služby.

1.1 Jednotlivé edice Windows Server 2008 R2

Existence několika vydání softwaru je naprosto běžná věc, nejen z hlediska finančního, ale také z hlediska hardwarové náročnosti. Každá edice má tedy své určené použití.

- Edice Windows Server 2008 R2 Foundation představuje nákladově efektivní základní úroveň, jež nabídne technologický základ pro podnikání. Je určena majitelům malých firem a IT specialistům, kteří tyto firmy podporují. Edice Foundation je nenákladná, osvědčená a spolehlivá technologie nabízející snadné nasazení. Organizacím poskytuje základ pro provozování nejčastěji používaných podnikových aplikací i pro sdílení informací a prostředků.
- Windows Server 2008 R2 Standard je nejrobustnějším serverovým operačním systémem Windows v historii. Obsahuje integrované vylepšené technologie pro web a virtualizaci, které umožňují zvýšit spolehlivost i flexibilitu serverové infrastruktury a zároveň ušetřit čas i snížit náklady. Výkonné nástroje nabízejí větší kontrolu nad servery, optimalizují konfiguraci i správu. Rozšířené funkce pro zabezpečení posilují

ochranu operačního systému, dat i sítě a zároveň vytvářejí pevnou, vysoce spolehlivou funkční základnu pro každou organizaci.

- Windows Server 2008 R2 Enterprise představuje pokročilou serverovou platformu, které poskytuje nákladově efektivnější a spolehlivější podporu nejdůležitějších úloh. Nabízí inovativní funkce pro virtualizaci, úsporu energie a snadnou správu, pomáhá usnadnit přístup mobilních pracovníků k firemním prostředkům.
- Windows Server 2008 R2 Datacenter představuje platformu pro nasazení nepostradatelných podnikových aplikací a rozsáhlou virtualizaci na malých i velkých serverech. Nabízí lepší dostupnost, vylepšené řízení spotřeby a integrovaná řešení pro pracovníky v terénu a v pobočkách. Konsolidací aplikací na základě neomezených licenčních práv k virtualizaci umožňuje snížení nákladů na infrastrukturu. Podporuje škálování od 2 do 64 procesorů. Windows Server 2008 R2 Datacenter představuje pevný základ, na kterém je možné budovat podniková řešení pro virtualizaci a škálování.
- Windows Web Server 2008 R2 představuje výkonnou platformu pro webové aplikace a služby. Tato edice obsahuje službu Internet Information Services (IIS) 7.5 a je navržena výhradně jako server připojený k Internetu. Nabízí vylepšenou správu nebo diagnostické nástroje, které při použití na mnoha oblíbených vývojářských platformách pomohou snížit náklady na infrastrukturu. Protože tato platforma zahrnuje role webového serveru i serveru DNS, zaznamenala vylepšení spolehlivosti a škálovatelnosti, umožňuje spravovat i ta nejnáročnější prostředí – od vyhrazeného webového serveru po celou farmu těchto serverů.
- Edice Windows Server 2008 R2 pro systémy s procesorem Itanium představuje platformu pro nasazení nepostradatelných podnikových aplikací. Podporuje škálování databází, podnikových a vlastních aplikací tak, aby splňovaly rostoucí potřeby podniku. Pomáhá zvýšit dostupnost díky clusteringu s podporou převzetí služeb při selhání i funkci dynamického dělení hardwaru. Virtualizuje nasazení s možností spouštět neomezený počet virtuálních instancí systému Windows Server. Edice Windows Server 2008 R2 pro systémy s procesory Itanium pomáhá vytvořit základ vysoce dynamické infrastruktury IT. [1]

Microsoft na svých stránkách udává i hlavní rozdíly v edicích, respektive v jejich službách. Microsoft služby serveru označuje jako role.

Server Role	Enterprise	Datacenter	Standard	Itanium	Web	Foundation	HPC
Active Directory Certificate Services	✓	✓	✓[1]	○	○	✓[1]	✓[1]
Active Directory Domain Services	✓	✓	✓	○	○	✓	✓
Active Directory Federation Services	✓	✓	○	○	○	○	○
Active Directory Lightweight Directory Services	✓	✓	✓	○	○	✓	○
Active Directory Rights Management Services	✓	✓	✓	○	○	✓	○
Application Server	✓	✓	✓	✓	○	✓	✓
DHCP Server	✓	✓	✓	○	○	✓	✓
DNS Server	✓	✓	✓	○	✓	✓	✓
Fax Server	✓	✓	✓	○	○	✓	○
File Services	✓	✓	✓[1]	○	○	✓[1]	✓[1]
Hyper-V	✓	✓	✓	○	○	○	✓
Network Policy and Access Services	✓	✓	✓[1]	○	○	✓[1]	✓[1]
Print and Document Services	✓	✓	✓	○	○	✓	○
Remote Desktop Services	✓	✓	✓[1]	○	○	✓[1]	✓[1]
Web Services (IIS)	✓	✓	✓	✓	✓	✓	✓
Windows Deployment Services	✓	✓	✓	○	○	✓	✓
Windows Server Update Services (WSUS)	✓	✓	✓	○	✓	✓	✓

Tabulka 1: Jednotlivé služby edic Windows Server 2008 R2

[1] určitá omezení dané verze. [2]

1.2 Hardwarové nároky Windows Server 2008 R2

Součást	Požadavek
Procesor	Minimum: 1.4 GHz (x64) Poznámka: Systém Windows Server 2008 R2 pro počítače s procesorem Itanium požaduje procesor Intel Itanium 2.
Paměť	Minimum: 512 MB RAM Maximum: 8 GB (Foundation) nebo 32 GB (Standard) nebo 2 TB (Enterprise, Datacenter a systémy s procesorem Itanium)
Volné místo na pevném disku	Minimum: 32 GB nebo více Foundation: 10 GB Poznámka: Počítače s více než 16 GB paměti RAM budou potřebovat více volného místa na pevném disku pro stránkování, hibernaci a odkládací soubory.
Zobrazení	Monitor s rozlišením Super VGA (800 × 600) nebo vyšším
Ostatní	Jednotka DVD-ROM, klávesnice a myš Microsoft Mouse nebo kompatibilní polohovací zařízení, připojení k síti Internet (může být zpoplatněno)

Tabulka 2: Hardwarové nároky Windows Server 2008 R2

Jedná se o minimální konfigurace. Pokud je potřeba provozovat všechny služby dané edice nebo ve větším provozu, může se minimální konfigurace lišit. [3]

2 DHCP SERVER

DHCP server přiděluje takové parametry, které klientským stanicím umožní komunikaci v síti. V dané síti by měl být pouze jeden DHCP server, aby bylo zaručené spolehlivé přidělování IP adres. Není ovšem nutné, aby stanice byla klientem DHCP serveru. Stanice může být, v některých případech musí být, nastavena ručně. Ručně se většinou nastavují servery, síťové tiskárny, routery atd., čili zařízení, u kterého se vyžaduje pevná IP adresa.

V současné době je nejpoužívanější protokol TCP s IPv4, což znamená použití 32bitové IP adresy a 32bitové masky sítě. Tento protokol časem v budoucnu nahradí novější protokol IPv6, jenž používá 128bitové adresování. Nástup IPv6 je zatím velice pozvolný.

2.1 Parametry DHCP Serveru

Pokud DHCP klient některému parametru nerozumí, ignoruje ho. DHCP server nastavuje na klientovi tyto parametry:

- **IP Adresa (IP address)** – 32bitová (pro IPv4) adresa stanice unikátní v dané síti. Klientským stanicím přiřazuje vždy adresu z určitého rozmezí. Pokud se stane, že by DHCP server již neměl IP adresu, kterou by mohl klientovi přiřadit, pak se klient nepřipojí do sítě. Velikost možného rozmezí závisí na masce sítě.
- **Maska sítě (Subnet mask)** – Stejná délka jako IP adresa. Podle druhu sítě určíme její velikost. Ve většině případů je dostačující 255.255.255.0 čili 254 IP adres v jedné síti, respektive podsítí.
- **Adresa výchozí brány** – Specifická IP adresa směrovače (routeru), přes který stanice komunikují s jinou sítí. Je to parametr nepovinný, ale vzhledem ke vzájemnému propojení většiny sítí, téměř vždy užívaný. Výjimku mohou tvořit experimentální či oddělené sítě.
- **DNS servery** – další nepovinná část, ale stejně jako výchozí brána, dnes prakticky nechybí na žádném klientovi. Jedná se o jednu či dvě IP adresy serverů DNS, které poskytují překlad doménových jmen na IP adresy.
- Další údaje mohou být servery pro NTP, WINS atd.

Nedílnou součástí konfigurace DHCP serveru je **doba zapůjčení** IP adresy (lease time), tedy doba, po kterou má stanice právo tuto adresu používat. DHCP server tedy IP adresu po dobu zapůjčení nepřiřadí jiné stanici. DHCP klient musí před vypršení této doby

požádat o prodloužení zapůjčení adresy. Pokud je žádost akceptována, DHCP klient může tuto adresu po novou dobu zapůjčení používat. Toho se využívá pouze u dynamického alokování adres.

2.2 Způsob přiřazování adres

DHCP server může adresy přiřazovat několika způsoby:

- **Statická alokace** – Podle seznamu (ke každé MAC adrese je přiřazená jedna IP adresa) přiřazuje každé stanici danou IP adresu. V praxi se používá výjimečně.
- **Dynamická alokace** – DHCP server má nastavené určité rozmezí IP adres, ze kterého čerpá pro jednotlivé stanice. Důležitým parametrem je tedy doba zapůjčení. Musíme vždy brát v úvahu, o jaké využití sítě se jedná a tudíž sladit počet adres a dobu zapůjčení.

V praxi se velmi často používá kombinace jednotlivých způsobů přiřazování.

2.3 Proč použít DHCP Server

V rozsáhlejších sítích je velmi obtížné ruční konfigurování a evidování všech IP adres. Pokud jde o samotné stanice, tak většinou není důležité, jakou IP adresu má. Při existenci DNS serveru je problém přiřazování dynamických adres vyřešen. V dnešní době, kdy se k síti připojuje mnoho zařízení (tablety, mobily, herní konzole atd.), je existence DHCP serveru v síti velice užitečná.

3 DNS SERVER

Tato služba byla vyvinuta pro Internet, v němž má každý počítač svou IP adresu, ale počítačů je mnoho a bylo by nemožné zapamatovat si, pod jakým číslem jsou skryty hledané údaje. Proto existuje DNS, který převádí lépe zapamatovatelné názvy na čísla a zpět. DNS rozděluje počítače do zón, nazývaných domény. Domény se dále řadí do stromové struktury. Musíme zadat IP adresu alespoň jednoho serveru, který DNS převod provede. [4]

3.1 Parametry DNS Serveru

- **Zóna dopředného vyhledávání** – v této zóně se převádí jednotlivé názvy na IP adresy. Obsahuje složky spravovaných domén a jejich záznamy typu A (resp. AAAA při použití IPv6). Pro každé sítové zařízení (jeden počítač může mít i vice síťových karet, čili několik IP adres) v doméně by měl existovat jeden záznam typu A (resp. AAAA).
- **Zóna zpětného vyhledávání** – v této zóně se převádí jednotlivé IP adresy na názvy.
- **SOA (Start Of Authority record)** – součást každé zóny a to na prvním místě a pouze jednou. Jsou zde uloženy základní informace o serveru DNS (jméno, třída záznamů, email zodpovědné osoby atd.)
- **Záznam o prostředku názvového serveru (NS)** – definuje názvy autoritativních serverů pro zóny DNS.
- **Záznam typu A** – překládá název na IP adresu počítače. Jedná se o 32bitovou adresu, tudíž se vztahuje k protokolu IPv4.
- **Záznam typu AAAA** – nachází se v něm také překlad názvu na IP adresu počítače, ale jedná se o 128bitovou adresu, tudíž se vztahuje k protokolu IPv6.
- **Alias (CNAME)** – Pokud existuje více názvů pro jeden počítač (jednu IP adresu), řeší se to pomocí těchto záznamů.
- **Mail Exchanger (MX)** – server určený pro obsluhu elektronické pošty. Může se zde uvést i více serverů, které potom slouží jako záložní. Pořadí využití je dáno prioritou.

- **Ukazatel (PTR)** – opak záznamu typu A (resp. AAAA), tudíž překládá IP adrese název.
- **A další záznamy**: TXT, SRV, SPF….

3.2 Proč použít DNS Server

Použití ve větších sítí má stejné opodstatnění jako server DHCP. Samotný internet by bez něj asi těžko mohl fungovat. S nástupem IPv6 bude nezbytný i pro menší sítě. Při implementování služby MS Active Directory Domain Services, je nutné mít server DNS zprovozněný.

4 FILE SERVER

Jedním z hlavních důvodů, proč vznikají sítě, je sdílení informací čili souborů. File Server poskytuje sdílení souborů a složek. A to modelem klient-server. Z tohoto modelu plyne, že každý uživatel má svá omezení (přístupová práva). Tato omezení mohou být odvozena z omezení skupiny (které je členem) nebo speciálně pro jednotlivé uživatele. Tato centrální správa je velmi výhodná pro zabezpečení, tak pro zálohování.

4.1 Oprávnění ke složkám a souborům

Je nutné stanovit, který uživatel bude moci se složkou pracovat, a co mu bude v konkrétní složce dovoleno. V operačních systémech Windows se možnosti práce jednotlivých uživatelů (a skupin) ve složkách definují prostřednictvím oprávnění. Přidělením oprávnění se definují přesné možnosti práce ve složce. [4]

Samotná oprávnění se dělí do dvou skupin. Jedna je lokální a druhá síťová. Lokální je závislá na použití souborového systému na disku (FAT32, NTFS, EXT4 atd.). Tato oprávnění platí nejen pro síťový přístup, ale také pro přístup uživatelů přímo ze stanice (serveru). Pro NTFS jsou to například tyto základní oprávnění: úplné řízení, měnit a spouštět, číst obsah složky, zobrazovat, číst, zapisovat. Síťová oprávnění, přesněji „Oprávnění ke sdílení“, platí pouze pro síťové uživatele nebo skupiny. Každé kategorii můžeme dát tři oprávnění a to: úplné řízení, změnit a číst. Jednotlivé stupně přístupu jsou vysvětleny v Tabulka 3.

Oprávnění	Umožňuje
Číst	Zobrazení názvu souborů a podsložek, přecházení do podsložek, zobrazení dat v souborech, spouštění souborů.
Měnit	Zahrnuje oprávnění Číst, a navíc umožňuje vytváření souborů a podsložek, změnu dat v souborech, odstraňování souborů a podsložek.
Úplné řízení	Je výchozí oprávnění každého nového sdílení, které vytvoříme. Úplné řízení zahrnuje všechna oprávnění Číst a Měnit.

Tabulka 3: Přehled Oprávnění ke sdílení [4]

Při síťovém přístupu se pak s těmito dvěma oprávněními udělá logický součin a dostane se výsledné oprávnění jednotlivého uživatele k dané složce. Některé literatury používají termín „efektivní oprávnění“.

5 ACTIVE DIRECTORY DOMAIN SERVICES

Služba Active Directory Domain Services (AD DS) v operačním systému Windows Server® 2008 ukládá informace o uživatelích, počítačích a dalších zařízeních v síti. Služba AD DS pomáhá správcům bezpečně spravovat tyto informace, usnadňuje sdílení prostředků i spolupráci uživatelů. Službu AD DS je také nutné mít nainstalovanou v síti, pokud je třeba instalovat aplikace pro práci s adresáři, jako je Microsoft Exchange Server, a pro použití ostatních technologií Windows Server jako jsou Zásady skupiny. [5]

AD DS poskytuje distribuované databáze, která ukládá a spravuje informace o síťových zdrojích i aplikacích. Správci mohou pomocí AD DS uspořádat prvky sítě (uživatelé, počítače a další zařízení) do hierarchické struktury. Hierarchická struktura zahrnuje omezení Active Directory: les, domény v lese a organizační jednotky (v každé doméně). Server se systémem AD DS se nazývá řadič domény.

5.1 Struktura Active Directory Domain Services

Active Directory Domain Services má přesně danou hierarchickou strukturu, která má spoustu výhod. Skládá se:

- **Les** – Nejvyšší v dané hierarchii, skládá se z minimálně jedné domény. Určuje pomyslné hranice, kde může správce zasahovat. V původním nastavení obsahuje les pouze jednu doménu, nazývaná jako kořenová doména.
- **Domény** – domény tvoří les a tím umožňují rozdělit data v AD DS. Doména obsahuje počítače, uživatele, tiskárny a organizační jednotky. Domény nemusí být v přesném souladu s fyzickou topologií sítě (domény mohou být propojeny například modemovým spojením, a pořád mohou tvořit jeden les). Domény také podporují mnoho základních funkcí pro správce jako totožnost uživatele, ověřování a vztahy důvěryhodnosti.
- **Organizační jednotka** – usnadní správu velkého množství objektů s pomocí delegování pravomocí. Vlastníci mohou skrz delegaci předávat plnou nebo částečnou pravomoc a to dalším uživatelům nebo skupinám. K distribuování řízení velkého počtu objektů k lidem, kterým věříme v řízení, slouží právě delegování.
- **Uživatel** – v AD DS je uživatel definován uživatelským jménem a heslem. Další nepovinné položky (atributy) jsou například telefon, adresa, email, povolení vzdáleného přístupu, skupiny (kterých je členem), atd.

- **Skupiny** – používají se pro hromadné nastavení práv a přístupů. Například přidělením jakéhokoliv oprávnění skupině, dědí toto oprávnění všichni členové. Toto přidělování oprávnění je mnohem efektivnější, než nastavovat každého uživatele zvlášť. Navíc je to velice přehledné. Tyto skupiny jsou dvě, a to *distribuční skupina* (*Distribution group*, nemá SID – *Security Identifiers*, využívá se pro nezabezpečené seznamy), *skupina zabezpečení* (*Security group*, má SID, vhodná pro řízení přístupu k prostředkům). Dále se skupiny dělí podle rozsahu platnosti skupiny. *Místní doménová skupina* (*Domain Local Group*) uplatňuje pravidla pouze na místní doménu. Zato *Globální skupina* (*Global Group*) umožňuje přidělit přístup do jakékoliv domény v doménové struktuře. Členovi *Univerzální skupiny* (*Universal Group*) lze nastavit oprávnění v rámci kterékoliv domény, které je členem.
- **Počítač –** je to objekt v AD DS reprezentující počítač, který se po přihlášení do domény vytvoří automaticky (ve většině případů). Ve speciálním případě se vytváří ručně.
- **Tiskárna –** pomocí těchto objektů v AD DS se vytvářejí či spravují sdílené nebo síťové tiskárny.

5.2 Řadič domény (Domain Controller)

V systému Windows Server 2008 R2 řadiče domény (DC) ukládají data adresářů. Také spravují interakci mezi uživatelem a doménou, včetně přihlášení uživatele, ověřování i vyhledávání v adresáři. Jelikož je prakticky srdcem služby AD DS, je pro něj velice důležitá bezpečnost a stabilita. Jakékoliv ztráty nebo poškození DC mají kritické důsledky pro klienty, servery, soubory, aplikace. Tedy všechno co využívá zásady ověřování skupin a adresáře protokolu LDAP (závislých na DC).

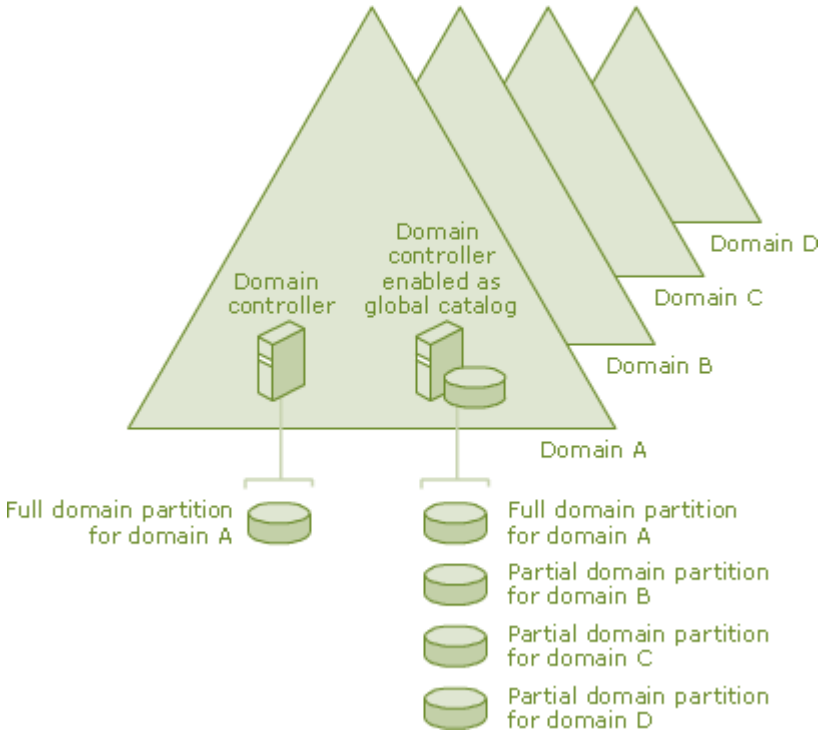
5.2.1 Řadič domény jen pro čtení (Read Only Domain Controller)

Řadič domény jen pro čtení je nový typ řadiče domény v operačním systému Windows Server® 2008. Prostřednictvím řadiče domény jen pro čtení mohou organizace snadno nasazovat řadiče domény v umístěních, kde nelze zaručit fyzické zabezpečení. Řadič domény jen pro čtení je hostitelem oddílů databáze služby AD DS (Active Directory® Domain Services) určených pouze pro čtení.

Před uvedením systému Windows Server 2008 neexistovala žádná skutečná alternativa v situaci, kdy uživatelé museli být ověřováni řadičem domény přes síť WAN. V mnoha případech se nejednalo o efektivní řešení. Pobočky často nemohou zajistit adekvátní fyzické zabezpečení požadované u řadiče domény s možností zápisu. Pobočky také při připojení k centrále mají často k dispozici omezenou šířku pásma. To může prodlužovat dobu, kterou trvá přihlašování. Může to také omezovat přístup k síťovým prostředkům. [7]

5.3 Globální katalog (Global Catalog)

Globální katalog je řadič domény, který ukládá kopie všech objektů služby Active Directory v doménové struktuře. Globální katalog ukládá úplné kopie všech objektů v adresáři hostitelské domény a částečné kopie všech objektů v ostatních doménách v doménové struktuře, jak je znázorněno na Obrázek 1: Funkce globálního katalogu.



Obrázek 1: Funkce globálního katalogu

Globální katalog obsahuje částečné kopie všech objektů domény, které byly nejčastěji používány ve vyhledávacích operacích uživatelů. Tyto atributy jsou v definici schématu označeny k zahrnutí do globálního katalogu. Ukládání nejčastěji hledaných atributů všech objektů domény do globálního katalogu umožňuje uživatelům efektivní vyhledávání, aniž by byl výkon sítě nepříznivě ovlivněn nepotřebnými odkazy na řadiče domény. [6]

5.4 Zásady skupiny (Group Policy)

Zásady skupiny lze použít k definování výchozího nastavení, které bude automaticky použito pro účty uživatele a počítače ve službě Active Directory. Pomocí nastavení zásad lze spravovat vzhled plochy, přiřadit skripty, přesměrovat složky z místních počítačů do umístění v síti, určit možnosti zabezpečení i určit, jaký software může být instalován v konkrétních počítačích nebo jaký software je k dispozici pro konkrétní skupiny uživatelů.

Nastavení zásad je uloženo v objektech zásad skupiny. V každé síti, doméně a organizační jednotce lze použít nastavení z více objektů zásad skupiny. Obsahuje-li například síť tři domény, může jeden objekt zásad skupiny řídit konfiguraci počítačů v celé síti. Samostatné zásady pro každou doménu mohou určit různé nastavení zabezpečení počítačů v těchto doménách. Obsahuje-li každá doména organizační jednotky Účtárna a Marketing, mohou další objekty zásad skupiny určit software, který bude nainstalován v počítačích používaných skupinami Účtárna a Marketing v rámci celé sítě. [8]

5.4.1 Zásady skupin dělení do složek

Zásady skupin můžeme rozdělit do 3 složek a 2 sad.

Složka Nastavení softwaru

Složka Konfigurace počítače\Nastavení softwaru obsahuje nastavení softwaru platné pro všechny uživatele, kteří se přihlásí k danému počítači. Tato složka obsahuje nastavení pro instalaci softwaru a může obsahovat další nastavení, které tam umístí nezávislí dodavatelé softwaru. Složka Konfigurace uživatele\Nastavení softwaru obsahuje nastavení softwaru platné pro uživatele bez ohledu na to, ke kterému počítači se přihlásí. Tato složka rovněž obsahuje nastavení pro instalaci softwaru a může obsahovat další nastavení, které tam umístí nezávislí dodavatelé softwaru.

Složka Nastavení systému Windows

Složka Konfigurace počítače\Nastavení systému Windows obsahuje nastavení systému platné pro všechny uživatele přihlášené k počítači. Tato složka obsahuje rovněž následující položky: *Nastavení zabezpečení* a *Skripty*.

Složka Nastavení zabezpečení

Nastavení zabezpečení nebo zásady zabezpečení jsou pravidla konfigurovaná v počítači nebo ve více počítačích za účelem ochrany prostředků v počítači nebo v síti. Pomocí nastavení zabezpečení můžete určit zásadu zabezpečení organizační jednotky, domény nebo sítě. [9]

5.4.2 Zásady skupin a sady zásad

Dělíme na 2 sady:

- *Zásady počítače* – nastavení pro počítače, nastavení zásad probíhá při startu počítače.
- *Zásady uživatele* – nastavení pro uživatele, nastavení probíhá při přihlášení uživatele.

6 WINDOWS SERVER UPDATE SERVICES

Za celým vývojem update pro produkty Microsoft (Windows Server, Windows 7 atd.) stojí Microsoft Security Response Center (MSRC). Je to tým, který dodává aktualizace a autoritativní bezpečnostní pokyny. MSRC identifikuje, monitoruje, řeší a reaguje na bezpečnostní incidenty v produktech od firmy Microsoft. Vydávají nejen aktualizace, ale také bulletin ke každé aktualizaci.

Postup MSRC při řešení případné hrozby je v následující tabulce:

Hodnocení	Vyhodnocení možný dopad hrozby pro zákazníky.
Šetření	Shromáždění informací k reprodukci zranitelnosti a určení, které produkty to ovlivní.
Přísnost	Hodnocení jednotlivých zranitelností v závislosti na závažnosti a pravděpodobnosti, že bude využíván.
Rozlišení	Rozhodnout, zda bude vydána ihned aktualizace, nebo až jej vyřeší následující Service Pack či novější verze produktu.

Tabulka 4: Postup řešení případné hrozby týmem MSRC

6.1 Microsoft Update

Server Microsoftu, na kterém se zveřejňují všechny aktualizace na všechny produkty od firmy Microsoft. Jsou zde přístupné nejen samotné informace, ale i samotné instalační soubory. Jedná se o jediný oficiální zdroj, na který jsou automaticky směřovány všechny operační systémy resp. jejich aktualizátory.

6.2 Windows Server Update Services

WSUS je role Windows Serveru, která se stará o distribuci a instalaci těchto aktualizací na samotné stanice. Integrovaná až od Windows Server 2008 jako jedna jeho služba, pokud je součástí dané edice. Viz Tabulka 1: Jednotlivé služby edic Windows Server 2008 R2. WSUS používá jako zdroj aktualizací server Microsoft Update.

Tato role umožňuje administrátorovi řídit aktualizace těmito možnostmi:

- nastavení času stahování aktualizací do stanic

- rozdělení stanic do skupin podle uvážení a nastavení různých pravidel pro uvolnění aktualizací na jednotlivé skupiny stanic.

6.3 Automatické aktualizace

Klientský program je součást každé verze Microsoft Windows. Program stahuje a instaluje aktualizace pro daný operační systém buď z WSUS serveru, pokud je přítomen, nebo přímo z Microsoft Update.

II. PRAKTICKÁ ČÁST

7 STÁVAJÍCÍ SITUACE A POŽADAVKY FIRMY

Ve firmě Elegante online s.r.o. vznikala nová pracovní místa a původní stav tří počítačů byl nedostačující. Také stav sítě (připojení pomocí wifi routeru přes usb wifi klíčenky) byl nevyhovující, i k vzhledem k nestálosti připojení. Operační systémy měli po jednom zástupci Windows XP Professional, XP Home edice a také nové sedmičky Professional. Všichni uživatelé byli zároveň správcové systému. Na každé stanici byl použit jiný softwarový firewall a antivirový program. Byla potřeba zajistit jak síťové účetnictví, tak přístup na toto účetnictví ze sítě Internet. Po konzultaci byl přidán požadavek na společný síťový prostor a síťový tisk.

7.1 Řešení sítě, stanic a serveru

Cílem bylo vytvořit stabilní síť, sjednotit operační systém a uvést do provozu nový server (respektive jeho služby). Při budování sítě bylo kalkulováno s budoucími pracovními pozicemi. V sídle firmy bylo použito přibližně 400 metrů kabelu UTP kategorie 5e a byl pořízen nový 24 portový 100Mb/s switch (do budoucna připraveno na rychlejší gigabit). Stávající wifi router byl ponechán v síti jako vstupní router s funkcí NAT. U internetového poskytovatele se zařídila statická veřejná IP adresa. Stanicím se doplnily operační paměti na dva gigabyty a byly na nich nainstalovány nové Windows 7 Professional ve 32 bitové verzi. Na všech stanicích byl použit antivirový program Microsoft Security Essentials.

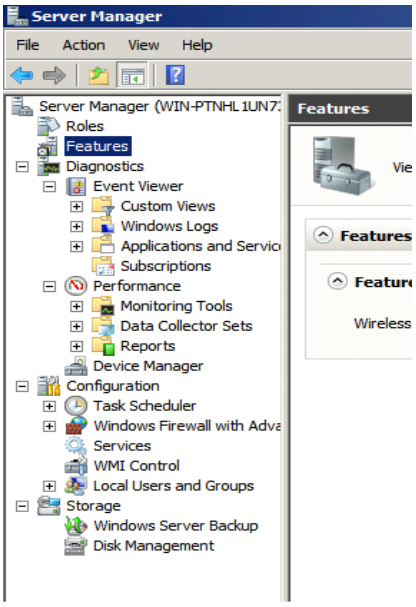
Jako server byl zakoupen FUJITSU PRIMERGY TX100 S1, ke kterému byl zdarma Microsoft Windows Server 2008 R2 Foundation OEM anglické verze. Tato edice má různá omezení (viz Tabulka 1: Jednotlivé služby edic Windows Server 2008 R2), která jsou dostatečná právě pro malé firmy do 15 uživatelů.

8 INSTALACE SERVERU

Před spuštěním samotné instalace, se ještě v biosu nastaví raid pole do modu 1 (zrcadlení dat na dva disky). Instalace z přiloženého DVD již probíhala způsobem běžným pro systémy Windows. Jediná odlišnost je nutnost zadání hesla administrátora, které splňuje defaultní principy uživatelského hesla. Tudíž musí obsahovat minimálně jedno velké a malé písmeno a jednu číslici. Minimální délka je stanovena na 8 znaků. Platnost administrátorského hesla je měsíc. Po ukončení instalace naběhne úvodní obrazovka Windows Serveru s výzvou k přihlášení.

8.1 Úvodní stav systému a prvotní nastavení

Ihned po přihlášení je zobrazeno okno se souhrnnými informacemi o systému, kde je uvedeno například: síťové jméno serveru, zda je vypnuta možnost připojení přes Remote Desktop, atd. Neboť je potřeba u serveru mít vzdálený přístup, je možné jej povolit přímo v úvodním okně (na přístup jen s nejnovějším klientem a nejlepším zabezpečením). Pro bezproblémový přístup je ještě nutné nastavit síťové jméno (*windows_server*) a také pevnou IP adresu (*192.168.0.100*). Po zavření úvodního okna se objeví další okno s názvem Server Manager. Toto okno je „brána“ do nastavení celého serveru. Na jednom místě je kompletní nastavení serveru, jednotlivých služeb, funkcí a dalších nastavení. Prohlížení (či nastavení) je úhledně seřazeno do stromové struktury (viz Obrázek 2).



Obrázek 2: Struktura Server Manageru

První program, který se nainstaluje, bude antivirový program Microsoft Security Essentials. Po nainstalování se dá aktualizovat a následně restartujeme server. Po té se může server spravovat vzdálenou plochou.

8.2 Role DHCP Server

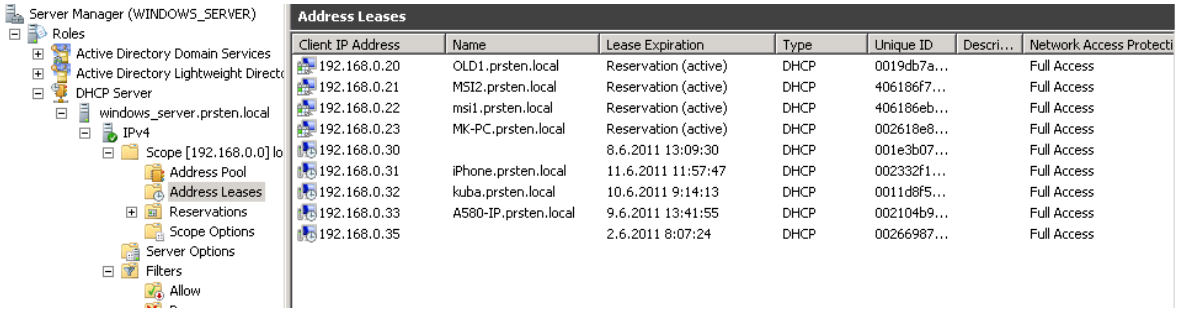
8.2.1 Instalace a konfigurace

Začátek přidání jakékoliv role je stejný. Otevření okna Server Manageru a kliknutí na odkaz *přidat roli*. Po té se vybere jedna role (nebo více rolí) a klikne se na tlačítko *další*. Takto bylo zatrhnuto přidání role DHCP Server. Další okno již popisuje funkci zvolené role, také upozorňuje na nutnost mít aspoň jednu statickou IP adresu a doporučuje mít rozvrhnuté podsítě, rozsahy i výjimky adres. Okno obsahuje také odkazy na další informaci o této službě. Následně se doplní název domény *prsten.local*. Do dvou textboxů se vyplní adresa primárního resp. sekundárního DNS serveru poskytovatele (172.16.34.17, 88.146.158.2), které se mohou nechat ověřit tlačítky u příslušné kolonky. Poté se zvolí, zda se budou používat WINS servery. Tato volba se ponechá vypnutá. Hned v dalším okně se nastaví rozsahy přidělovaných adres. Takových rozsahů může mít hned několik a nastaví se zde pojmenování rozsahu (*návštěvy*), začínající i končící adresu (*192.168.0.150-192.168.0.200*), druh připojení (*drátové* – jde o nastavení času rezervování adresy pro dané zařízení), masku podsítě (*255.255.255.0*) a nepovinný údaj výchozí bránu (*192.168.0.111*). Zakáže se *stateless mode* pro konfigurace klientů IPv6, takže zamezíme konfiguraci klientů s adresou IPv6. V předposledním okně se zkontroluje výpis nastavení DHCP Serveru a může se potvrdit tlačítkem *install*.

Po samotné instalaci nás systém upozorní na potřebu restartu, aby byla role spuštěna. Výzva k restartu se objeví i po zavření výsledku instalace. Další role nelze do restartu instalovat. Po restartu je DHCP Server plně funkční a pokud se nenachází v síti další DHCP server, funguje role spolehlivě. Tato role se spravuje v Server Manageru.

8.2.2 Otestování funkce

Po připojení jakéhokoliv zařízení do sítě se přidělí IP adresa a zařízení má přístup na Internet.



Obrázek 3: Výpis aktivních výpůjček IP adres

8.3 Role DNS Server

8.3.1 Instalace

Začne se stejně jako u role DHCP tedy přes Server Manager. První obrazovka instalace DNS Serveru je opět informativní, zobrazí se základní princip DNS Serveru a jeho možného propojení s Active Directory. Nechybí zde také odkazy na rozsáhlejší články týkající se této problematiky. Instalace proběhne po kliknutí na *install*. Poté se potvrdí zpráva o úspěšnosti instalace.

8.3.2 Konfigurace

Vybere se tedy v Server Manageru role DNS Server, záložku *DNS* a v ní náš server (ukazuje se pod síťovým jménem - *windows_server*). Rozkliknutí našeho serveru se zobrazí čtyři složky. První se nakonfiguruje dopředná zóna (*Forward Lookup Zones*). Klikne se pravým tlačítkem na složku *Forward Lookup Zones*, *vytvořit novou zónu*. Dále se vybere druh zóny. V našem případě se jedná o primární zónu, které se následně zadá název domény *prsten.local* a potvrdí se vytvoření podložek v dané zóně. Prozatím se zakážou dynamické aktualizace, protože zabezpečené dynamické aktualizace se umožní až po instalaci role AD DS. Posledním oknem se potvrdí vytvoření dopředné zóny.

Vytvoření reverzní zóny (*Reverse Lookup Zones*) je obdobné. Také se bude jednat o primární zónu pro IPv4. To se nastaví v prvních dvou oknech. Poté se zadá jednoznačné ID sítě, což je neměnná část IP adresy tedy „*192.168.0*“. Automaticky se vyplní celé jméno reverzní zóny „*0.168.192.in-addr.arpa*“. V příštím okně je vyplněné jméno souboru pro danou zónu, které se potvrdí. Stejně jako u dopředné zóny se zakážou dynamické aktualizace a potvrdíme vytvoření zóny.

8.3.3 Otestování role

Takové nastavení DNS Serveru je již kompletní ale bez záznamů. Jelikož jsou zakázané automatické aktualizace, tak by se musely jednotlivé záznamy dopsat ručně. Záznamy se nechají vytvořit až ve spolupráci s Active Directory. Tudíž testování proběhne v příštím bodě.

8.4 Role Active Directory Domain Services

8.4.1 Instalace

Návrh celé struktury v našem případě je velice jednoduchý, neboť se skládá pouze z jedné domény (tak se vyhoví omezení *edice Foundation*). Samotná instalace role je velice podobná roli DNS Serveru, přes průvodce se nainstaluje role.

8.4.2 Konfigurace

Po instalaci se najde v Server Manageru role AD DS a spustí se *průvodce nastavení AD DS* (program *dcpromo.exe*). Hned na úvodní stránce průvodce se nebude zatrhávat volba rozšířeného nastavení a zobrazí se, jaká vylepšení v doménovém kontroléru Microsoft udělal. Následně se založí nová doména v novém lese a zadá se jméno naší nové domény *prsten.local*. Systém zkontroluje, zda již není toto jméno domény použito. Jelikož se tvoří nový nezávislý les, použije se jeho nejvyšší verze Windows Server 2008 R2. Dále není na výběr a musí se odsouhlasit volba doménového kontroléru v podobě DNS Serveru i globálního katalogu. Systémové složky se uloží na disk „*C:*“. Pokračuje se nastavením hesla pro administrátora domény. Pak se potvrdí přehled nastavení doménového kontroléru. Konfigurace se dokončí restartem celého serveru.

8.4.3 Konfigurace DNS Serveru

Restartováním se spustí doménový kontrolér, a tudíž celá služby AD DS. Upraví se ještě nastavení obou DNS zón, opět v Server Manageru. V něm se rozklikne *DNS Server -> DNS -> windows_server*. Zde se vybere dopředná zóna a pravým se klikne na doménu, kterou chceme nechat zpravovat AD DS (*prsten.local*). Zobrazí se vlastnosti dané domény, v záložce *obecné* se klikne na tlačítko *změnit* pro položku *typ*. Zvolí se možnost ukládání zóny v active directory. Jelikož je služba AD DS aktivní, je toto ukládání povoleno. Po přijetí ukládání v active directory se zvolí dynamické aktualizace na *pouze zabezpečené* a

potvrdí se volba těchto vlastností tlačítkem *ok*. To samé se opakuje u nastavení reverzní zóny.

8.4.4 Přidání uživatele do Active Directory

Takto nastavený AD DS je skoro připraven na svůj provoz. Stačí pouze přidat aspoň jednoho uživatele. Počítač do domény se přihlašuje administrátorským účtem. Bez uživatelů by se neměl, kdo na stanici přihlásit. Musí se brát na zřetel, že se používají defaultní *Group Policy*. Tyto položky se velice pohodlně mění i za chodu systému, takže není důvod procházet obsáhlé nastavení, navíc defaultní nastavení se jeví jako dostačující.

Přidání uživatele přes Server Manager

Možná více profesionální se tváří přístup přes Server Manager, kde se prokliká přes položky *AD DS -> Active Directory Users and Computers -> prsten.local*. Zde se zobrazí kontejnery AD DS, týkající se právě uživatelů a počítačů. Rozklikne se tedy kontejner *Users* a uvidí se jak všechny skupiny, tak všechny uživatele (defaultně jsou dva uživatelé, administrátor a guest - který je ale zakázán). Kliknutím pravým tlačítkem buď na jakýkoliv kontejner, nebo do prostoru výpisu uživatelů, se nabídne vytvořit nového uživatele, počítače, tiskárny atd. Vybere se tedy uživatel, vyplní se postupně základní údaje a heslo. Potvrzením souhrnných informací se vytvoří nový uživatel.

Přidání uživatele přes Active Directory Administrative Center

Vybere se v hlavním *panelu Start -> možnosti správy* (*administrative tools*) *-> Active Directory Administrative Center*. Úvodní obrazovka tohoto správce nabízí zrychlené volby, a to resetování hesla uživatele a globální vyhledávání v *Active Directory*. Klikne se na název domény *prsten.local*, v levém sloupci nabídky, zobrazí se všechny kontejnery z AD DS. Vybere kontejner *Users* a zobrazí se všichni uživatelé domény i všechny skupiny. Tento výpis se může filtrovat, což se ocení při větších počtech skupin a uživatelů. Při kliknutí na jakoukoliv položku se zobrazí ve spodní části souhrnné informace o objektu, vpravo pak nabídka pro práci s objektem. Neustále je zobrazeno v pravé části nabídka pro úpravy uživatele.

Vybere se tedy volba *nový -> uživatel*. Již na první pohled se zobrazí mnohem detailnější nastavení nového uživatele. Povinné údaje jsou přitom pouze uživatelské celé jméno a přihlašovací jméno. V praxi se vyplňovalo jméno, příjmení, povinné údaje, heslo, popis uživatele. V části *Člen* (Member of) se doplňovalo *domain user*. V následující části *profil*

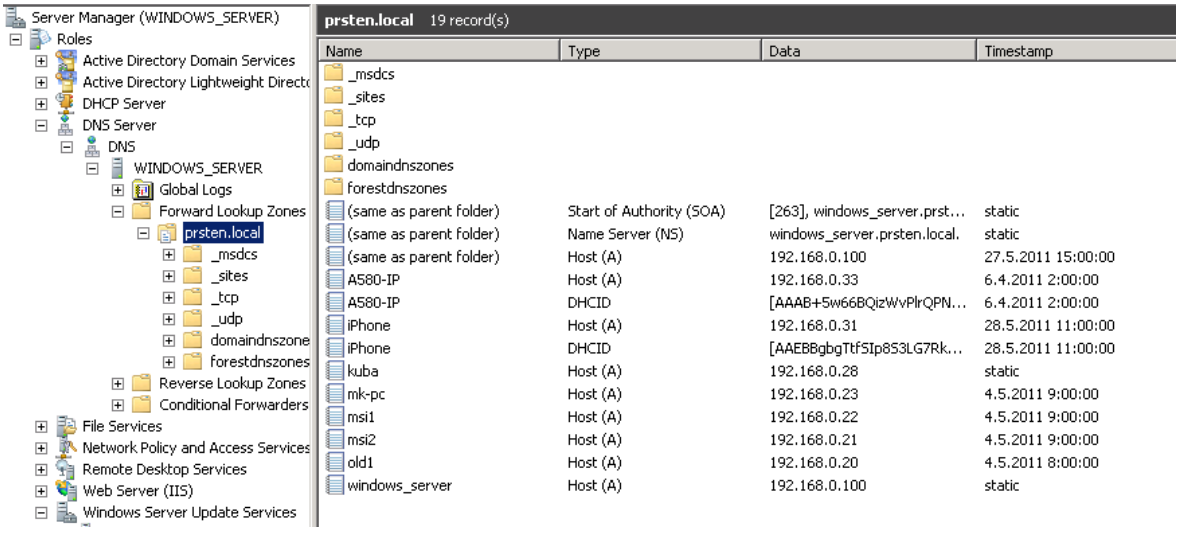
(*Profile*) lze nastavit síťovou cestu k profilu i domácí složce. Toto nastavení se používá jen pro cestovní profily. Jelikož není služba síťového uložiště (*File Server*), nelze ani cestovní profil v tuto chvíli nastavit. Tlačítkem *Ok* se vytvoří nový uživatel. Tento způsob vytvoření či upravení uživatele se tváří mnohem přehledněji.

8.4.5 Otestování role AD DS

Na stanici se otevře *ovládací panely -> Systém*, kde v oblasti *Název počítače, domény a nastavení pracovní skupiny* se klikne na *Změnit nastavení*. V záložce *Název počítače* se klikne na tlačítko *změnit*. V sektoru *Je členem* označíme *Domény* a doplní se název domény *prsten.local*. Potvrdí se dvakrát tlačítkem *Ok*. Pro přihlášení je nutné počítač restartovat. Po naběhnutí se nabízí přihlášení do domény *prsten.local* a platí tedy přihlašovací jména i hesla z *Active Directory*. Veškerá nastavení fungovala.

8.4.6 Otestování role DNS Server

Na stanici se otevře *Tento počítač* a do adresového řádku se vepíše *\\MSI1* (název jiné stanice). Dokud se objeví obsah sdílených složek i tiskáren, znamená to, že DNS Server dobře přeložil název na IP adresu. Všechny dosavadní DNS záznamy se prohlédnou v Server Manageru -> *DNS Server* -> *DNS* -> *windows_server* -> dopředná zóna -> *prsten.local*.



Obrázek 4: Výpis záznamů DNS Serveru

8.5 Role Windows Server Update Services

8.5.1 Instalace WSUS a návazných služeb

Při instalaci této role přes Server Manager se zobrazí upozornění, že WSUS potřebuje role *Web Server (IIS)* a *File Server*. Z toho plynou dvě informativní okna o možnostech *Web Serveru* a *File Serveru* resp. jejich seznam součástí, které se musí nainstalovat (tyto součásti nelze modifikovat). Informace o roli WSUS a souhrnný seznam instalovaných součástí se potvrdí tlačítkem *install*.

8.5.2 Konfigurace WSUS Serveru

Ihned po dokončení instalace se objeví průvodce nastavení role WSUS. Po akceptování licenčních podmínek se zobrazí průvodce instalace nezbytné funkce Microsoft Report Viewer, takže se volba potvrdí. Dále je možnost ukládat aktualizace lokálně na serveru, což významně uspoří počet stahovaných dat z internetu. Zvolí se tedy umístění „ *D:*“ i pro interní databázi aktualizací. Na obě umístění by mělo být dostatek místa (dohromady minimálně 10GB). Zvolí se doporučený port 80. Souhrnné informace se potvrdí a počká se na dokončení průvodce.

Dokončením prvního průvodce se objeví druhý průvodce, který je zaměřený na nastavení spojení lokálního WSUS na zdroj aktualizací. Microsoft Update Improvement Program není pro naše účely důležitý, proto se nastaví *neúčastnit*. Existuje hierarchického nastavení WSUS serverů, aby stahovali data od sebe. Vybere se tedy volba synchronizace přímo z Microsoft Web Update. Proxy server se v našem spojení nenachází. Vyzkouší se konektivita s Microsoft serverem tlačítkem *Otestovat spojení*. Po zvolení jazyků pro aktualizace se vyberou produkty, které se budou aktualizovat. V hledáčku tedy bude Microsoft Security Essentials a Windows 7. V dalším kroku se určí druh aktualizací, proto se zaškrtne kritické, definiční, bezpečnostní, service pack a update. Synchronizace se nastaví na automatickou ve 3:00, tedy v čase, kdy nebude vadit omezení síťového provozu a vytížení serveru. Potvrdí se počáteční synchronizace a počká se na její dokončení. Zobrazí se odkazy na více informací ohledně problematiky WSUS a celého průvodce ukončíme tlačítkem dokončit.

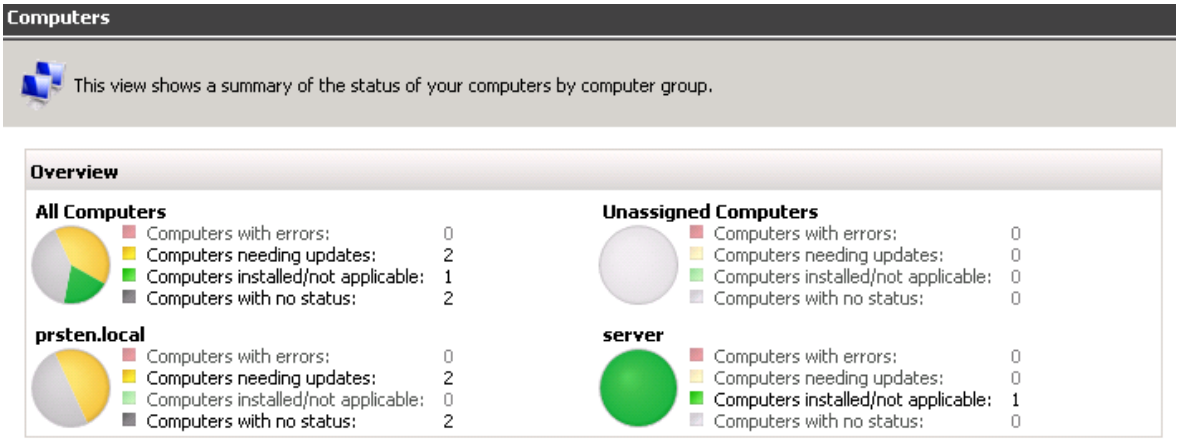
8.5.3 Konfigurace Group Policy

K takto nastavenému WSUS se nepřihlásí pro aktualizace žádné PC, musí se totiž nastavit v *Group Policy* připojení stanic na náš WSUS (a ne přímo na Microsoft Web Update, jak je to defaultně). Otevře se *Group Policy Management* (*nabídka Start -> možnosti správy*), kde se rozklikne *Forest prsten.local* -> Domains -> tady se najde naše doména *prsten.local*. V kontejneru *Group Policy Objects* se pravým tlačítkem myši klikne na *Default Domain Policy* a dá se jeho editace. Tím se dostane na nastavení *Group Policy Management Editor (GPME*) pro všechny objekty v naší doméně:

- **Nastavení stanic, aby instalovaly aktualizace pravidelně** - Ve *GPME* se proklikne přes *Konfigurace počítače* (*Computer Configuration*), *Politika* (*Policies*), *Šablony pro správu* (*Administrative Templates*), *Součásti systému Windows* (*Windows Components*), *Windows Update*. Dvojklikem se otevře *Konfigurace automatických aktualizací* (*Configure Automatic Updates*) a zde se nastaví *povolit* (*enable*), zvolí se volba *4 - Automaticky stahovat a plánovat instalaci* (*Auto download and schedule the install*), nastaví se každý den v 9:00.
- **Nastavení stahování aktualizací z našeho serveru** - Ve stejné složce GPME se upraví položka *Určení umístění intranetového serveru služby Microsoft Update* (*Specifies intranet server Microsoft update service location*). Zde se zaškrkne *povolit* a zadá se adresu našeho WSUS serveru (*http://windows_server*), a to do obou kolonek (aktualizační a statistický server).

8.5.4 Závěrečné konfigurace

Jednotlivé stanice přihlášené do domény se budou postupně objevovat ve správě služby a to v Server Manageru -> *WSUS -> Update Services -> Computers -> All Computers* ve skupině *Unassigned Computers*. V kontejneru se vytvoří nová skupina (pravým tlačítkem na *All Computers*, *přidat novou skupinu*, zadá se název *prsten.local*). Postupně se přesunou ručně všechny stanice do nové skupiny (klik pravým tlačítkem na stanici ve výpisu a dá se přesunout do skupiny *prsten.local*). Stejným postupem se vytvoří skupina *servers* a přidá se do něj náš server (*windows_server*), aby se oddělil server od stanic. Po tomto kroku je hierarchie hotová a můžou se vytvořit pravidla.



Obrázek 5: Statistika jednotlivých skupin WSUS

Nastavení pravidel pro povolování aktualizací se konfiguruje v Server Manageru -> *WSUS -> Update Services -> Options -> Automatic Approvals*. Zde je pouze defaultní filtr pro aktualizace, ale není povolen. Smaže se. Vytvoří se nové pravidlo kliknutím na *nové pravidlo*. Zde máme 4 možnosti nastavení:

- specifické kategorie (kritická, definiční, atd.)
- produkty (MS Office, MS Security Essentials, Windows 7, Windows Vista atd.)
- skupiny, pro které platí pravidlo
- deadline (čas po který bude aktualizace dostupná na našem serveru)

Nastavení pravidla č. 1 následně:

- kategorie (kritická, definiční, bezpečnostní a aktualizace)
- produkt (Microsoft Security Essentials)
- skupiny (*servers*, *prsten.local*)
- deadline (14 dní po povolení ve 3:00)

Takto zvolené pravidlo zabezpečuje aktualizaci všech našich antivirových programů.

Nastavení pravidla č. 2 následně:

- kategorie (kritická, bezpečnostní a aktualizace)
- produkt (Windows 7)
- skupiny (prsten.local)
- deadline (10 dní po povolení ve 3:00)

Takto zvolené pravidlo zabezpečuje aktualizaci windows 7 na všech stanicích.

8.6 Role File Services

Jelikož se role File Server nainstalovala při instalaci role WSUS serveru, není potřeba ji instalovat. Přidání role se ale nijak neliší od instalace jiné role v Server Manageru.

8.6.1 Nastavení sdíleného prostoru

Před samotným sdílením se musí vymyslet struktura sdílení. Na disku „*D:*“ se vytvoří složka *share*. Pro přehlednost se nebude jinde než v této složce sdílet. Vytvoří se další složka, která je podsložkou „*D:\share“*, s názvem *verejna*. V Server Manageru se najde role File Services a v ní se zvolí *Share and Storage Management* (ten se najde také v *nabídce Start -> možnosti správy*). Zobrazí kompletní přehled sdílených složek. Některé jsou defaultní, některé nastavené rolí WSUS. Klikne se na *nastavení sdílení* (*provision share*), a tím se spustí průvodce sdílení. Nejprve se najde složka, která se bude sdílet (*d:\share\verejna*). Poté bude potřeba změnit *NTFS permission,* a to že *System* a *Administrators* budou mít *plný přístup*. *Users* budou mít *práva čtení*, *spuštění* a *zápisu*. *Authenticated Users* budou mít všechna práva kromě *plné kontroly* a *speciálních přístupů*. Název a síťová cesta se ponechá. Omezení na maximum uživatelů není potřeba. Následuje okno se síťovým přístupem, tedy přístupy pro *SMB*. Zvolí se vlastní nastavení a kliknutím na tlačítko *povolení* (*permission*) se otevře nastavení složky. Skupina *Everyone* se smaže a klikne se na tlačítko *přidat*. V další nabídce se vepíše *Users* a potvrdí se. Tím se nastaví na složku povolení skupiny *Users* z domény *prsten.local*. Ještě se skupině přidá právo *zápisu* a potvrdí se. Tím se zobrazí další nastavení složky a to *DFS Namespace Publishing*, které se nebude nastavovat. Zbývá jen potvrdit celkové nastavení. Po dokončení průvodce se složka ihned objeví ve výpisu.

8.6.2 Kontrola funkčnosti

Pro ověření se na stanici otevře prohlížeč souborů a napíše se adresu *\\windows_server\verejna* (název serveru a složky, takto funguje na všech stanicích domény). Vše se chovalo naprosto v pořádku.

Pro vylepšení přístupu na toto sdílené místo, se při prohlížení sdílených složek klikne na složku *verejna* pravým tlačítkem. V nabídce se zvolí *připojit jako síťový disk* a vybere se označení disku *„X:“*. Zakřížkuje se také opětovné připojení. To se udělá u každé stanice.

8.7 Zálohování serveru

Microsoft zálohování neřadí mezi role serveru, ale mezi *Funkce* (*Features*). Bude se tedy jednat o jednu z nejdůležitějších funkcí serveru. Přidání této funkce probíhá velice podobně jako přidání role. V server manageru se klikne pravým tlačítkem myši na *Features* a vybere se *přidat*. Zakřížkuje se *Windows Server Backup Features* a potvrdí se volbu tlačítkem *ok* a *install*. Daná funkce se nalezne v Server Manageru pod položkou *Storage*, nebo v nabídce start -> *možnosti správy*. V nabídce záloh se nachází tři volby záloh *plán záloh* (*backup schedule*), *zálohovat jednou* (*backup once*) a *obnova* (*recover*).

8.7.1 Nastavení plánované zálohy

Klikne se na nabídku *plán záloh*. Zvolí se vlastní nastavení zálohy. Dále se vybere pro zálohu disk „*C:*“, stav systému a sdílená složku *D:\share\verejna*. Zakřížkuje se denní záloha v čase 1:00. Zálohovat se bude na přidaný disk „*E:“* a celkové nastavení zálohy se potvrdí. Takto nastavená záloha samozřejmě potřebuje zapnutý server v tuto dobu.

9 SÍŤOVÁ BEZPEČNOST

Pro firmy jsou informace velice důležité a je nutné je dobře chránit. Nejen rychlý přístup i záloha, ale také bezpečnost dat je velice důležitá. Nebezpečí není nejen v samotné ztrátě informace, ale i třeba zkopírování těchto informací (např. konkurenci, na internet atd.). Hrozby se rozdělují podle přístupu, a to na vnější i vnitřní, přičemž pomyslná čára je v bodě připojení k Internetu. V našem případě je to wifi router, který funguje jako vstupní brána.

9.1 Vnější útoky

DoS (Denial of Service) a DDoS (Distributed Denial of Service) útoky jsou dva typičtí zástupci nebezpečí z vnějšku. Tento způsob napadání je poslední dobou velice oblíbený. Tyto útoky mají za úkol ochromit či zničit jednotlivé služby.

Jako filtr těchto útoků funguje vstupní wifi router, který má aktivní NAT. NAT z vnějšku propouští pouze na jediném portu, a to na portu pro vzdálenou plochu, která je potřeba. Samotná služba vzdálené plochy je chráněna přístupovým jménem, heslem i šifrováním samotné aplikace. Také omezení v počtu možných pokusů se bere jako dostatečné zabezpečení.

Odchytávání informací je veliký problém. Ten může nastat prakticky kdekoliv, jak uvnitř sítě tak mimo ni. Z pohledu odchytávání informací přímo u poskytovatele Internetu, nebo někde na „cestě“ mezi zdrojem a cílem, se jeví jako velice nepravděpodobné přes množství dat, které tudy proteče. I přesto používání zabezpečené komunikace je dnes nezbytné.

9.2 Vnitřní útoky

Mezi nejčastější útoky vůbec patří viry, malware a spyware. Tyto škodlivé programy jsou velice nebezpečné a vedou k přímému ohrožení citlivých dat, hesel apod. Největším problémem virů je, že běží s uživatelskými právy a bez jeho vědomí. Ochrana proti takovému útoku není vždy lehká, lpí na dodržování přísných pravidel, čili nastavení. Začne se pravidelným aktualizováním stanic (WSUS), které „zalepí“ díry v systému. Další velice důležitá je aktualizace antivirového programu (také WSUS), nejen jeho databáze, ale i jeho programové části. Pak je ještě lidský faktor, který je omezen uživatelskými právy. Ty tento faktor velice omezují, ale nedokážou ho zcela eliminovat. Tudíž jsou naplánovány antivirové kontroly jak na stanicích, tak i na serverech.

Sdílený prostor je omezený přístupovými právy, ale také nutností se přihlásit do domény. Právě ono integrování systému Active Directory považuji za velmi bezpečné. Jednak správa a přidělování práv je velmi přehledné i rychlé, což přispívá také k bezpečnosti sítě.

Nebezpečí prolomení sítě přes wifi síť, je jednak zabezpečeno WPA šifrováním a jednak systémem Active Directory. Čili samotné prolomení šifry neznamená přímé nebezpečí, kromě sdílení internetového připojení.

Možné zneužití bývalého zaměstnance je značně omezen nejen samotného přístupu do budovy (alarm, dvoje zamčené dveře), tak existencí Active Directory. Jednotlivý uživatelé nemají přístup do terminálové služby, takže útok z vnějšku hrozí jedině viz odstavec Vnější útoky.

V jednání je také použití softwarového firewallu na vstupním routeru, vylepšení heslové strategie, zakázaní usb zařízení. Tyto omezení by měli přispět ještě k lepšímu zabezpečení celé sítě.

ZÁVĚR

Cílem práce bylo nastavit nový standard pro firmu *Elegante online s.r.o.,* a to vypracováním síťové struktury se serverem, který je jejím důležitým prvkem. Stanice byly vylepšeny, aby na nich mohly „běžet“ *Windows 7 32bit*, tím se sjednotil používaný operační systém. Na server byl nainstalován nejnovější *Windows Server 2008 R2 v edici Foundation*.

Již před prvním spuštěním serveru bylo rozvrhnuto, jak bude celá síť vypadat. Jako první se instalovala role *DHCP Server* a následně role *DNS Server*. Tyto dvě role jsou velice jednoduché a v úvodních konfiguracích se nevyskytl žádný problém.

Jako další se instalovala stěžejní služba celého serveru, respektive celé sítě, *Active Directory Domain Services*, tudíž jádro služby – *doménového kontroléru*. Doménová struktura je nejjednodušší možný model a tomu odpovídala i konfigurace. Zvolena byla kořenová doména *prsten.local*. DNS Server byl nastaven na zabezpečené dynamické aktualizace záznamů. To nám zajišťuje vždy aktuální dns záznamy obou zón.

Po přidání několika uživatelů a přeinstalování počítačů na jednotný operační systém se přikročilo k přihlášení do domény. Po restartu byly již aktivní *Group Policy*, jednotliví uživatelé se již mohli přihlásit.

Následovala instalace role pro aktualizace jednotlivých operačních systémů i jejich součástí, a to služba *WSUS*. Konfigurace této služby je velice podrobná, ale přehledná. Zprvu se neobjevovaly žádné počítače ve správě *WSUS*, ale po nastavení *Group Policy* se počítače začaly postupně objevovat.

S předchozí rolí WSUS se nainstalovala také role *File Server*. Po vytvoření jednoduché adresářové struktury, se nastavily jednotlivá sdílení a jejich práva.

Pravidelné denní zálohy byly nastaveny pomocí *Plánovače úloh* a probíhají v naprostém pořádku.

Po 100 dnech provozu celé sítě nenastal žádný zásadní problém.

ZÁVĚR V ANGLIČTINĚ

The aim of this work was to setup a new standard for Elegante online s.r.o. company. It was focused on implementing network structure with server, which was the key element. Computers have been upgraded to be able to run Windows 7 32bit, which also unified operating system. The latest Windows Server 2008 R2 Foundation was installed on the server.

The site was designed even before the first start of server, to know how the entire network will look like. Then the DHCP role was installed on the server followed by DNS role. These two roles ware very simple and there was no problem at the initial configuration.

Further, the most important role of the server, or the entire network, was installed. It means Active Directory Domain Services, the core service for the domain controller. The domain structure is the simplest possible model, and it corresponded to the configuration. Prsten.local was chosen as root domain. DNS server was set up to secure dynamic update records.

After adding a few users and reinstalling computers on a single operating system, it was possible to log into the domain. Group Policy has been active after the restart and individual users are already able to login.

The next step was the installation of WSUS service for the updates of operating systems and their components. The configuration of this service was very detailed, but clear. At first, there were no computers in the WSUS administration, but after the Group Policy settings the computers started to appear.

The File Server role was automatically installed together with the WSUS role. A simple directory structure was created and the individual access and sharing rights were set.

Regular daily backups were configured by the Task Scheduler and run in perfect order.

There was no major problem after 100 days in operation.

CITOVANÁ LITERATURA

1. **© 2011 Microsoft.** Windows Server 2008 R2 | Přehled edic. *Windows Server 2008 R2* . [Online] Microsoft, 2011. [Citace: 25. 2 2011.] http://www.microsoft.com/cze/windowsserver2008/r2-editions-overview.mspx.

2. **© 2011 Microsoft.** Windows Server 2008 R2 | Porovnání edic podle rolí serveru. *Windows Server 2008 R2.* [Online] Microsoft, 2011. [Citace: 11. 3 2011.] http://www.microsoft.com/cze/windowsserver2008/r2-compare-roles.mspx.

3. **© 2011 Microsoft.** Windows Server 2008 R2 | Požadavky na systém Windows Server 2008 R2. *Windows Server 2008 R2.* [Online] Microsoft, 2011. [Citace: 26. 2 2011.] http://www.microsoft.com/cze/windowsserver2008/system-requirements.mspx.

4. **Jaroslav Horák, Milan Keršláger.** *Počítačové sítě pro začínající správce.* Brno : Computer Press, a.s., 2008.

5. **© 2011 Microsoft.** Role služby AD DS . *Tech Net.* [Online] Microsoft, 2011. [Citace: 2. 4 2011.] http://technet.microsoft.com/cs-cz/library/cc753516(WS.10).aspx.

6. **© 2011 Microsoft.** Role globálního katalogu. *Microsoft | TechNet.* [Online] Microsoft, 2011. [Citace: 12. 4 2011.] http://technet.microsoft.com/cs-cz/library/cc736934(WS.10).aspx.

7. **© 2011 Microsoft.** Služba AD DS : řadiče domény jen pro čtení. *Microsoft | TechNet.* [Online] Microsoft, 2011. [Citace: 12. 4 2011.] http://207.46.16.252/cs-cz/library/cc732801(WS.10).aspx.

8. **© 2011 Microsoft.** Integrace zásad skupin. *Microsoft | TechNet.* [Online] Microsoft, 2011. [Citace: 12. 4 2011.] http://technet.microsoft.com/cs-cz/library/cc738526(WS.10).aspx.

9. **© 2011 Microsoft.** Nastavení zásad skupin - přehled. *Microsoft | TechNet.* [Online] Microsoft, 2011. [Citace: 12. 4 2011.] http://technet.microsoft.com/cs-cz/library/cc736676(WS.10).aspx.

10. **© 2011 Microsoft.** Windows Server 2008 R2 | Nejčastější dotazy. *Windows Server 2008 R2.* [Online] Microsoft, 2011. [Citace: 24. únor 2011.] http://www.microsoft.com/cze/windowsserver2008/faq.mspx.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AD DS	Active Directory Domain Services
atd.	a tak dále
DC	Řadič domény (domain controller)
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
IP	Internet Protokol
IPv4	Internet Protokol verze 4
IPv6	Internet Protokol verze 6
resp.	respektive
NTP	Network Time Protocol
MS	Microsoft
MSRC	Microsoft Security Response Center
WINS	Windows Internet Naming Service
WS	Windows Server

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH