Konfigurace serveru jako řadiče domény pro malou podnikovou síť

Configuration of a Server as a Domain Controller for Small Business Network

Jan Plzák

Bakalářská práce
2012

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2011/2012

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

Jméno a příjmení:	**Jan PLZÁK**
Osobní číslo:	**A08081**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Informační a řídicí technologie**
Téma práce:	**Konfigurace serveru jako řadiče domény pro malou podnikovou síť**

Zásady pro vypracování:

1. **Popište možnosti síťových služeb systému Windows 2003 Server.**
2. **Nakonfigurujte a zprovozněte server v roli řadiče domény.**
3. **Popište a nainstalujte další role – DNS, File server, terminálový server.**
4. **Analyzujte potenciální možnosti útoku na síť a možnosti obrany.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **STANEK, William R. Microsoft Windows Server 2003 : kapesní rádce administrátora. 2., aktualiz. vyd. Brno : Computer Press, 2007. 575 s. ISBN 978-80-251-1654-8.**
2. **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.**
3. **PRICE, Brad. Active Directory : optimální postupy a řešení problémů. Vyd. 1. Brno : CP Books, 2005. 381 s. ISBN 80-251-0602-0.**
4. **RUSSEL, Charlie; CRAWFORD, Sharon; GEREND, Jason. Microsoft Windows Server 2003 : velký průvodce administrátora. Vyd. 1. Brno : CP Books, 2005. 1374 s. ISBN 8025105792.**
5. **LUDVÍK, Miroslav; ŠTĚDROŇ, Bohumír. Teorie bezpečnosti počítačových sítí. 1. vyd. Kralice na Hané : Computer Media, 2008. 98 s. ISBN 978-80-86686-35-6.**
6. **ŠETKA, Petr. Mistrovství v MS Windows server 2003. 1. vyd. Brno : Computer Press, 2008. 680 s. ISBN 80-251-0036-7.**

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

Datum zadání bakalářské práce: **24. února 2012**

Termín odevzdání bakalářské práce: **8. června 2012**

Ve Zlíně dne 24. února 2012

prof. Ing. Vladimír Vašek, CSc.
děkan

L.S.

prof. Ing. Vladimír Vašek, CSc.
ředitel ústavu

ABSTRAKT

Cílem této bakalářské práce je implementace Microsoft Windows Server 2003 R2 Standart Edition Active Directory Domain Services do prostředí malé podnikové sítě.

Teoretická část objasňuje všeobecné poznatky o Active Directory Domain Services, dále pak charakterizuje základní role a služby operačního systému Windows Server 2003 R2 a na závěr analyzuje bezpečnostní hrozby.

Praktická část, popisující stav před implementací, navazuje na design Active Directory Domain Services, skupinových politik, vlastní konfiguraci a testy. V závěru zhodnotím celkový přínos firmě po realizaci daného řešení.

Klíčová slova: Active Directory Domain Services, Doména, Lokalita, Doménový řadič,

Globální katalog, Zásady skupin, DNS, DHCP, Terminálový server, Windows Server, bezpečnostní hrozby.

ABSTRACT

The point of this bachelor work is the implementation of Microsoft Windows Server 2003 R2 Standard Edition Active Directory Domain Services to small business network environment.

The theoretical part explains the general knowledge of Active Directory Domain Services, and also describes the basic roles and services of Windows Server 2003 R2, and finally analyze security threats.

The practical part describes the state before the implementation, follow-up to design an Active Directory Domain Services Group Policy, proper configuration and testing. At the end I evaluate the overall benefit for company after implementation of this solutions.

Keywords: Active Directory Domain Services, Domain, Site, Domain Controller,

Global catalog, Group Policy, DNS, DHCP, Terminal server, Windows Server, security threats.

Poděkování

Rád bych poděkoval následujícím osobám:

Ing. Jiřímu Korbelovi, Ph.D., vedoucímu mé bakalářské práce, za podnětné připomínky, jež mi umožnily úspěšné zpracování této práce.
A především správci počítačové sítě firmy Vydos servis a.s. Ing. Rudolfu Staňkovi, za příležitost tento úkol realizovat.

Motto

„Jediné, co podléhá změně je změna sama“

Herakleitos

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

Již ve starověku věděli, že změny jsou nevyhnutelné, konstantní a neodvratné. Lze o tom přemítat, či zaujmout optimistický pohled a tvrdit, že alespoň některé změny jsou přínosné. I když inovace serverů a klientů může pro správce představovat významnou výzvu, je také příležitostí, jak vylepšit fungování sítí a tím si ušetřit práci. Můžete si být jisti, že systém Microsoft Windows Server 2003 R2 obsahuje celou řadu nástrojů, které vás povedou směrem změny k lepšímu.

Motivací této bakalářské práce je prohloubení již nabitých teoretických i praktických znalostí funkcionalit serverových operačních systémů a Active Directory Domain Services (AD DS) a cílem práce je aplikovat získané vědomosti pro implementaci AD DS do prostředí firmy, kde nahradí dosavadní stav na bázi pracovní skupiny.

V úvodu teoretické části je popsán ve firmě nainstalovaný operační systém Microsoft Windows server 2003 R2 , jeho edice a licenční politika nadále je vysvětlena terminologie AD DS, její běžné funkce a jsou přiblíženy role systému, které jsou ve firmě použité. Teoretickou část uzavírá kapitola o analýze bezpečnostních hrozeb pro tyto jednotlivé role.

Praktická část v úvodu analyzuje stav sítě firmy Vydos servis a.s. Pokračuje návrhem struktury AD DS a skupinových politik a končí samotnou instalací a konfiguraci jednotlivých síťových rolí s ohledem na zdůrazněné bezpečnostní hrozby.

Závěr je věnován celkovému přínosu firmě po implementaci daného řešení.

I. TEORETICKÁ ČÁST

1 MICROSOFT WINDOWS SERVER 2003 R2

1.1 Základní popis systému

Operační systém Microsoft Windows Server 2003 R2 sice již není nejaktuálnější serverovou platformou společnosti Microsoft. Jedná se však o léty prověřený, síťový a uživatelsky příjemně navrhnutý operační systém. Operační systém v základní podobě obsahuje servery nejpoužívanějších síťových služeb (DNS, DHCP, VPN, NBNS/WINS atd.), souborových a tiskových služeb a také robustní řešení pro centralizovanou správu a zajištění síťových politik pomocí technologie Active Directory druhé generace.

Z pohledu administrace je operační systém primárně administrovatelný v grafickém prostředí pomocí MMC konzol. Existují však i nástroje pro správu v podobě konzolových, řádkových, aplikací. Jsou zde k dispozici sady Support Tools, Recource Kit Tools. Volitelně lze operační systém doplnit o technologii Microsoft Power Shell, nástupce příkazového řádku, který je plně implementován v serverovém operačním systému Microsoft Windows Server 2008, a umožňuje plnou administraci serveru pomocí řádkových příkazů a skriptů.

1.2 Přehled jednotlivých edic rodiny Windows server 2003

Skupinu operačních systémů Windows Server 2003 tvoří systémy Windows Server 2003 Standard Edition, Windows Server 2003 Enterprise Edition, Windows Server 2003 Data-center Edition a Windows Server 2003 Web Edition. V pozdějších letech ještě přibyla hodně specifická verze Small Bussiness Edition. Každá verze je určena ke konkrétnímu účelu:

- **Edice Windows Server 2003 Standard** Tato verze je určena k poskytování služeb a prostředku dalším systémům v síti. Jedná se o přímou náhradu systémů Windows NT 4.0 Server a Windows 2000 Server. Operační systém zahrnuje širokou škálu funkcí a možností konfigurace. V rámci systému Windows Server 2003 Standard Edition je možné využívat dvousměrný a čtyřsměrný symetrický multiprocessing (SMP) a až 4 GB paměti na 32bitových systémech a 32 GB paměti na 64bitových systémech.
- **Edice Windows Server 2003 Enterprise** Kromě funkcí, které jsou k dispozici v systému Windows Server 2003 Standard Edition, obsahuje tato verze navíc podpo-

ru Služby clusterů (Cluster Service), metaadresářové služby a služeb pro systém Macintosh. Tato verze také podporuje 64bitové systémy, paměť RAM typu hot swap a přístup do paměti typu NUMA (Nonuniform Memory Access). Servery s verzí Enterprise mohou využívat až 32 GB paměti RAM s procesorem x86, 1 TB paměti RAM na 64bitových systémech a 8 procesorů.

- **Edice Windows Server 2003 Datacenter** jedná se o nejrobustnější server systému Windows. Zahrnuje rozšířené funkce pro řízení clusterů a podporuje \velmi rozsáhlé konfigurace paměti - až 64 GB paměti RAM s procesorem x86 a 1 TB paměti RAM na 64bitových systémech. Minimální požadavek na počet procesorů je 8, přičemž celkem jich může podporovat až 64.
- **Edice Windows Server 2003 Web** Tato verze je určena k poskytování webových služeb při implementaci webových serverů a aplikací. Součástí je rozhraní Microsoft .NET Framework, Internetová informační služba (IIS, Microsoft Internet Information Services), technologie ASP.NET a funkce pro vyrovnávání zatížení sítě. Řadu dalších funkcí, jako například službu Active Directory, však tato verze systému neobsahuje. Dalšími klíčovými funkcemi systému Windows, které jsou součástí této verze. Je pouze systém DFS (Distributed File System), EFS (Encrypting File System) a funkce Vzdálená plocha pro správu (Remote Desktop for Administration). Systém Windows Server 2003 Web Edition podporuje až 2 GB paměti RAM a 2 procesory.
- **Edice Windows Small Business Server 2003** Je to speciální úprava operačního systému Microsoft Windows Server 2003 určená pro použití v malých společnostech. Obsahuje různé doplňky (Microsoft Exchange Server, Microsoft ISA Server), které jsou jinak prodávány jako samostatné produkty společnosti Microsoft a pro operační systém Microsoft Windows Small Business Server 2003 byly upraveny (zjednodušeny). Upravení operačního systému je negativně ovlivněno ztrátou některých funkcí jako replikace domén, omezení počtu uživatelů a nutnost provozovat veškerý software na jednom hardware.

Funkce	Standard Edition	Enterprise Edition	Datacenter Edition
Maximum paměti RAM	4GB	32 GB pro 32 bitovou verzi, 64 GB pro 64bitovou verzi	32 GB pro 32 bitovou verzi, 64 GB pro 64bitovou verzi
Maximální velikost procesoru CPU	4	8	64
Clusterová služba	Ne	Ano	Ano
Sdílení připojení k Internetu	Ano	Ano	Ne
Terminálový server	Ano	Ano	Ano
Adresář relace terminálového serveru	Ne	Ano, pouze 32bitová verze	Ano, pouze 32bitová verze
Přidávání paměti za chodu	Ne	Ano, pouze 32bitová verze	Ano, pouze 32bitová verze
64bitová podpora procesorů Intel Itanium	Ne	Ano	Ano
Nejednotný přístup k paměti	Ne	Ano	Ano
Program Datacenter	Ne	Ne	Ano

Tabulka 1. Přehled rozdílů mezi jednotlivými edicemi

1.2.1 Hardwarové požadavky

Pro používání systému *Windows Server 2003 R2* je nutné následující vybavení:

Požadavky	Standard Edition	Enterprise Edition	Datacenter Edition
Minimální rychlost procesoru	133 MHz	133 MHz pro architekturu x86	400 MHz pro architekturu x86
		733 MHz pro architekturu Itanium	733 MHz pro architekturu Itanium
Doporučená rychlost procesoru	550 MHz	733 MHz	733 MHz
Minimální velikost operační paměti	128 MB	128 MB	512 MB
Doporučená velikost operační paměti	256 MB	256 MB	1 GB
Minimální požadované místo na pevném disku	1.5 GB	1.5 GB pro architekturu x86	1.5 GB pro architekturu x86
		2.0 GB pro architekturu Itanium	2.0 GB pro architekturu Itanium

Tabulka 2. Minimální hardwarové požadavky

[1,2]

1.3 Licenční politika

K používání systému Microsoft Windows server 2003 R2 (vyjma edice web) musí mít každý uživatel, nebo zařízení licenci klientského přístupu CAL, (pro službu terminálového serveru jsou ještě navíc licence TS CAL) server rozlišuje dva licenční režimy:

- **Licence CAL vázané na zařízení** V případě licencí CAL vázaných na zařízení je nutné získat licenci CAL pro každé zařízení, například přenosný počítač, stolní počítač, počítač Pocket PC či smartphone, které potřebuje mít přístup k vašemu serveru. V případě této možnosti bude mít k serveru přístup libovolný uživatel na licencovaném zařízení. Licence CAL vázané na zařízení mohou být nejekonomičtější a administrativně nejpohodlnější pro organizace s mnoha uživateli používajícími stejná zařízení, například zaměstnanci ve směnách. Pokud zvolíte licence CAL vázané na zařízení, využije jednu licenci CAL každé zařízení, které bude získávat přístup k serveru, přičemž lze po vyřazení zařízení z provozu danou licenci CAL znovu přidělit jinému zařízení.
- **Licence CAL vázané na uživatele** V případě licencí CAL vázaných na uživatele můžete získat licence CAL pro konkrétní uživatele, kterým je jmenovitě udílen přístup k vašemu serveru. Licencovaní uživatelé mohou k serveru získat přístup z libovolného zařízení. Licence CAL vázané na uživatele budou mít pravděpodobně největší smysl pro organizace s mnoha mobilními zaměstnanci, kteří potřebují přístup do firemní sítě z mobilních zařízení, nebo zaměstnanci, kteří používají pro přístup k síti více zařízení. Licenci CAL vázanou na zařízení lze přiřadit jinému uživateli, pokud je toto přiřazení trvalého charakteru. Licence vázané na uživatele lze také přiřadit jinému uživateli dočasně, pokud má původní uživatel dovolenou nebo pokud je dané zařízení zakázáno.

2 ROLE MICROSOFT WINDOWS SERVER 2003 R2

Server je počítačem, který v síti nabízí služby. Které konkrétní služby jsou potřeba, záleží na konkrétní síti a na požadavcích společnosti. Server může mít například následující role:

- Souborový server
- Databázový server
- Aplikační server
- Terminálový server
- Tiskový server
- Řadič domény
- Server DNS
- Server WINS
- Server DHCP
- Poštovní server
- Webový server
- Server FTP
- Server NNTP
- Server POP3 či IMAP4
- Server se službou vzdálené instalace (RIS)
- Server WINS
- Server pro vzdálené připojení
- Server POP3
- Server s certifikačním úřadem

a další.

Lze říci, že některé role jsou zastoupené ve všech sítích, zatímco ostatní jsou k dispozici pouze v některých.

V naší síti budou provozovány následující role:

- Řadič domény (popsán v kapitole 3)
- Souborový server
- Terminálový server
- Server DNS
- Server Windows Update Services (WSUS)
- Server DHCP
- Databázový server

2.1 Popis provozovaných služeb

2.1.1 Souborový server

Souborovým serverem označujeme spolehlivé a dostupné úložiště dat. Souborový server poskytuje centrální umístění dat v síti, ve kterém lze ukládat a sdílet soubory s ostatními uživateli v síti. Pokud uživatelé požadují důležitý soubor, například rozpracovaný projekt, nemusí si jej předávat mezi jednotlivými počítači, ale mohou k němu získat přístup na souborovém serveru. Windows server 2003 R2 tyto základní funkce zajišťuje s nejvyšší mírou spolehlivost při současném zajištění maximální možné bezpečnosti uložených dat.

Pro zajištění spolehlivých funkcí souborového serveru jsou k dispozici nástroje pro snadné:

- zabezpečení dat uložených na serveru (přístupová oprávnění NTFS, šifrování)
- indexování obsahu úložiště dat pro snadné a rychlé vyhledávání
- sdílení dat uložených na souborovém serveru (sdílení složek)
- možnost omezení dostupného místa pro data uživatelů (diskové kvóty)
- zálohování dat

[7]

2.1.2 Terminálový server

Jedná se o mechanizmus vzdáleného řízení, správy a využívání serverů. Je to tedy jak služba umožňující vzdálenou údržbu operačního systému, tak služba umožňující použití aplikačního serveru pro velký počet uživatelů. Terminálová služba přináší do operačních systémů společnosti Microsoft možnost souběžné práce více uživatelů.

Každý uživatel, který je k serverovému operačnímu systému připojen pomocí Terminálové služby, z pohledu klientských stanic pomocí nástroje Vzdálená plocha (Remote Desktop), využívá systémové a hardwarové prostředky samotného serveru a ne klientské stanice, ze které se připojuje. Uživatel sdílí procesor, paměť RAM a pevné disky serveru. Po připojení k Terminálové službě se klientská stanice stává pouze konzolí pro připojení k Terminálové službě. Každý uživatel má svou vlastní relaci Terminálové služby a každá relace funguje samostatně a nezávisle na ostatních relacích.

Terminálová služba je velmi vhodným řešením pro mobilní uživatele, kteří potřebují pracovat s náročnými aplikacemi a přitom využívají pomalé připojení k síti a nedisponují dostatečně výkonným přenosným hardwarem.

Hardwarové nároky

Terminálovou službu lze nainstalovat na všechny operační systémy Microsoft Windows Server 2003 R2, před instalací je ovšem nutné počítat s licenční politikou společnosti Microsoft. Terminálový server pro více, jak 2 současně přihlášené uživatele, vyžaduje zakoupení doplňkové licence. Dalším kritériem při instalaci Terminálové služby je její použití jako aplikačního serveru, kdy je nutné počítat s vysokými nároky na uložení dat aplikací.

Každá relace serveru Terminálové služby využívá minimálně 20 MB RAM paměti pouze k přihlášení. K této velikosti je potřeba přidat hardwarové nároky jednotlivých spouštěných programů. Minimální velikost RAM paměti pro jednu relaci Terminálové služby je 40 MB RAM.

U procesoru je složité určit minimální kapacitu vzhledem k náročnosti jednotlivých uživatelů, podle oficiálních údajů procesor Intel Xeon pracující na frekvenci 2 GHz postačuje při dostačující velikosti paměti RAM k provozu 50 relací. Toto číslo je pouze relativní a slouží k obecné představě hardwarové náročnosti jednotlivých relací.

Velmi důležitým údajem je i rychlost připojení serveru, podle které se odvíjí maximální datový tok a tedy i množství informací, které je schopna si Terminálová služba vyměnit s klientskou stanicí. Podle toho se odvíjí nastavení rozlišení Vzdálené plochy, barevná hloubka Vzdálené plochy a jiné nastavení.

[1]

Server licencí terminálového serveru

Na serveru licencí terminálového serveru jsou uloženy všechny klientské licence. Terminálový server musí být schopen připojit se k aktivovanému licenčnímu serveru, aby bylo možné klientům vydávat trvalé licence klientského přístupu (CAL). Po aktivaci licenčního serveru poskytne služba Microsoft serveru digitální certifikát, který ověřuje vlastnictví a identitu serveru. Pomocí tohoto certifikátu může server licencí provádět další transakce se společností Microsoft a získat klientské licence pro terminálové servery. Pokud licenční server nainstalujete, ale neaktivujete, vydává pouze dočasné licence (Lhůta končí poté, co zavedete server licencí a tento server udělí první trvalou licenci CAL, nebo po 120 dnech (podle toho, co nastane dříve)).

Před instalací licenčního je třeba si ujasnit, která z obou rolí licenčního serveru bude použita – doménový licenční server nebo licenční server rozlehlé sítě. Při instalaci nástroje Správa licencí Terminálového serveru můžete vybrat jednu z těchto rolí. Ve výchozím nastavení je vybrána role Licenční server rozlehlé sítě.

- **Licenční server rozlehlé sítě** je vhodné zvolit v případě, že síť obsahuje několik domén a chcete udržovat jeden licenční server, který by mohl vydávat licence terminálovým serverům v rámci různých domén. Licenční server rozlehlé sítě může obsluhovat terminálové servery z jakékoli domény, ale ve výchozím nastavení obsluhuje pouze terminálové servery ve stejné síti.
- **Doménový licenční server** je vhodné zvolit v případě, že chcete v každé doméně spravovat samostatný licenční server. Terminálové servery mohou získat přístup k doménovým licenčním serverům pouze v případě, že se nacházejí ve stejné doméně jako licenční server.

[7]

2.1.3 Domain Name Systém (DNS)

Jedná se o internetový standard zahrnutý v TCP/IP. Slouží k překladu jmen objektů na IP adresy či jiné zdrojové záznamy. Jména objektů se označují jako doménová jména a nejčastěji se jedná o jména hostitelů, jsou to alfanumerické řetězce, které jsou lépe zapamatovatelné než IP adresy. Příkladem doménového jména je www.seznam.cz a k němu náleží IP adresa 77.75.72.3. Výhoda je zřejmá a to lepší zapamatovatelnost a také možnost změnit fyzické umístění PC a jeho IP adresu při zachování stejného jména. Funkci internetu bychom si asi nedokázali bez DNS představit. DNS je rovněž vyžadována pro provoz Microsoft Active Directory Domain Services; není podmínkou používat verzi přímo od Microsoftu, ale je to doporučené z hlediska lepší provázanosti těchto rolí.

[1, 5, 6]

Princip činnosti

Prostor doménových jmen tvoří strom. Každý uzel tohoto stromu obsahuje informace o části jména (doméně), které je mu přiděleno a odkazy na své podřízené domény. Kořenem stromu je tzv. kořenová doména, která se zapisuje jako samotná tečka. Pod ní se v hierarchii nacházejí tzv. domény nejvyšší úrovně (Top-Level Domain, TLD). Ty jsou buď tematické (com pro komerci, edu pro vzdělávací instituce atd.) nebo státní (cz pro Českou republiku, sk pro Slovensko atd.).

Strom lze administrativně rozdělit do zón, které spravují jednotliví správci (organizace nebo i soukromé osoby), přičemž taková zóna obsahuje autoritativní informace o spravovaných doménách. Tyto informace jsou poskytovány autoritativním DNS serverem.

Výhoda tohoto uspořádání spočívá v možnosti zónu rozdělit a správu její části svěřit někomu dalšímu. Nově vzniklá zóna se tak stane autoritativní pro přidělený jmenný prostor. Ve vyšších patrech doménové hierarchie platí, že zóna typicky obsahuje jednu doménu. Koncové zóny přidělené organizacím připojeným k Internetu pak někdy obsahují několik domén – například doména kdesi.cz a její poddomény bazar.seznam.cz a zbozi.seznam.cz mohou být obsaženy v jedné zóně a obhospodařovány stejným serverem.

Typy záznamů

DNS podporuje řadu různých typů záznamů, podle typu záznamu uchovává různé parametry. Obecné parametry pro všechny typy záznamů jsou jméno, třída (pouze IN jako

internet), TTL (čas jak dlouho může být záznam uložen v keši), typ záznamu, data záznamu. Zde uvádím několik nejdůležitějších typů.

- host – address (A) – běžný záznam, obsahuje adresu počítače
- alias – canonical name (CNAME) – další jméno (alias) pro existující záznam v doméně
- mail exchanger (MX) – adresa poštovního serveru
- service location (SRV) – adresa některé služby, jako ldap, kerberos, ftp, a další
- name server (NS) – seznam serverů, které zajišťují DNS služby pro doménu, záznam se nachází v nadřízené doméně a v aktuální doméně
- pointer (PTR) – užívají se pro reverzní překlad
- start of authority (SOA) – odkazuje na server, kde jsou primární údaje (primární NS), a obsahuje údaje pro zone transfer

Zónové soubory

Strom doménových jmen se dělí na zóny, tedy oblasti spravované jedním správcem (organizací). Zóna obsahuje jednu (nejčastěji) nebo více domén. V zóně jsou také uvedeny autoritativní informace o spravovaných doménách. Tyto informace poskytuje autoritativní DNS server, tedy server, který je považovaný za důvěryhodný pro zónu.

Obsah zóny, jednotlivé zdrojové záznamy, je uložen v zónovém souboru (zone file). To je většinou textový soubor. Mezi některými DNS servery může docházet k replikaci záznamů (například mezi primárním a sekundárním NS), tomuto procesu se říká zone transfer.

Systém Windows Server 2003 R2 podporuje čtyři typy zón:

- Standardní primární (Standard Primary) – všechny změny zóny se provádějí v primární zóně a její změny lze replikovat do sekundárních zón.
- Standardní sekundární (Standard Secondary) – zajišťuje redundanci pro primární zónu a vyrovnává zatížení – replikace z primární zóny pomocí přesunů zón.

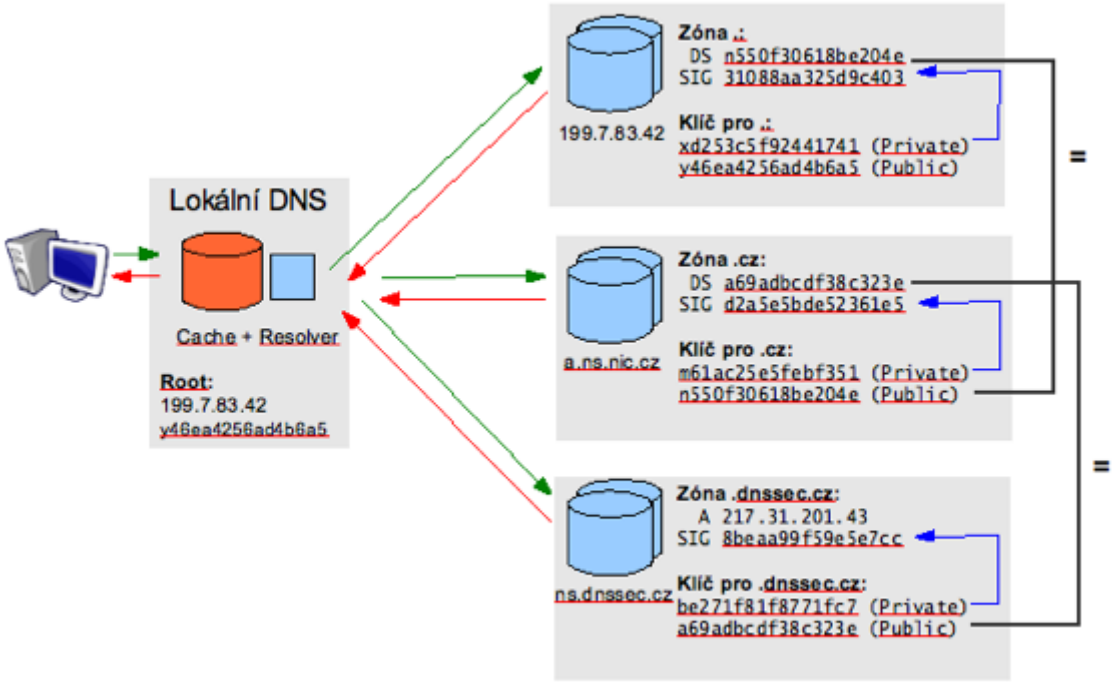
- Integrovaná se službou Active Directory (Active Directory-Integrated) – integruje informace zóny ve službě AD DS a pomocí této služby replikuje data zóny – pouze pokud je implementována služba AD DS.
- Zóna se zakázaným inzerováním (Stub) – ukládá oprávněné servery DNS pro danou zónu, neobsahuje žádné informace o hostitelích v zóně. Dotazy přímo oprávněným serverům.

[1]

DNSSEC

Běžný DNS systém slouží k překladu doménových jmen na IP adresy (a zpět), ale nemá žádnou ochranu proti napadení. Pokud je do webového prohlížeče zadána adresa www.seznam.cz, může být přeložena na podvrženou IP adresu, přičemž v adresním řádku prohlížeče bude stále www.seznam.cz, takže uživatel nepostřehne, že prohlížeč ve skutečnosti zobrazil podvrženou stránku (viz Phishing). Tomuto útoku se lze bránit tak, že www.seznam.cz použije pro komunikaci zabezpečený protokol HTTPS, avšak ne každý uživatel může tento rozdíl postřehnout.

DNSSEC zavádí DNS asymetrickou kryptografii – tedy používání jednoho klíče na zašifrování a jiného klíče na dešifrování obsahu. Obdobný princip je základem známějšího šifrování zpráv pomocí PGP či podepisování e-mailů elektronickým podpisem. V případě DNSSEC si držitel domény vygeneruje dvojici soukromého a veřejného klíče. Svým soukromým klíčem pak elektronicky podepíše technické údaje, které o své doméně do DNS vkládá. Pomocí veřejného klíče je pak možné ověřit pravost tohoto podpisu. Aby byl tento klíč dostupný všem, publikuje jej držitel ke své doméně u nadřazené autority, kterou je pro všechny domény .cz registr domén .cz. I na úrovni registru domén .cz jsou technická data v DNS podepsána a veřejný klíč k tomuto podpisu je opět správcem registru předán nadřazené autoritě. Vytváří se tak řetěz, který zajistí důvěryhodnost údajů, pokud není v žádném svém článku porušen, a všechny elektronické podpisy souhlasí, viz následující schéma.



Obrázek 1. Princip fungování DNSsec

[8]

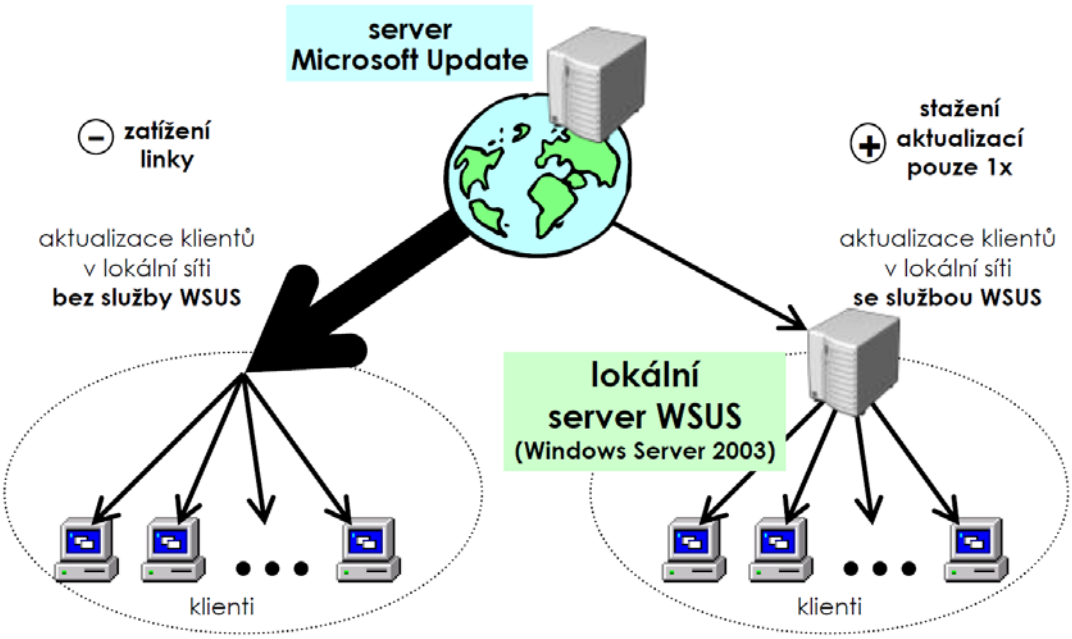
2.1.4 Windows Server Update Services (WSUS)

Windows Server Update Services (WSUS) je služba zajišťující aktualizaci softwaru pro operační systémy Microsoft Windows. WSUS je lokálně spravovaná alternativa ke službě Microsoft Update, která umožňuje správcům informačních technologií nasazovat nejnovější aktualizace produktů společnosti Microsoft do počítačů, ve kterých běží podporované operační systémy této společnosti. Infrastruktura WSUS umožňuje jednotlivým klientů v síti stahovat automaticky patche a aktualizace z centrálního serveru společnosti. To šetří vytíženost linky připojení k Internetu, čas i místo na disku, jelikož jednotlivé počítače v síti nepotřebují přistupovat k serveru Windows Update a ani nemusí mít aktualizace na svém disku, ale stačí jim pouze se připojit k centrálnímu serveru. Infrastruktura správy se skládá z následujících částí:

- **Microsoft Update:** Web společnosti Microsoft, který distribuuje aktualizace produktů této společnosti.
- **Server Windows Server Update Services:** Tato součást je nainstalována na serveru uvnitř podnikové brány firewall. Server WSUS umožňuje správcům

spravovat a distribuovat aktualizace prostřednictvím konzoly pro správu služby WSUS, kterou je možné nainstalovat do každého počítače se systémem Windows v doméně. Kromě toho může být server WSUS zdrojem aktualizací pro další servery WSUS v organizaci. Nejméně jeden server WSUS v síti musí být připojen k serveru Microsoft Update, aby získával informace o dostupných aktualizacích. Správce může určit na základě konfigurace a zabezpečení sítě, zda se budou ostatní servery připojovat přímo k serveru Microsoft Update.

- **Automatické aktualizace:** Tato součást je součástí podporovaných operačních systémů. Automatické aktualizace umožňují, aby serverové i klientské počítače získávaly aktualizace ze serveru Microsoft Update nebo ze serveru WSUS.



Obrázek 2. Základní princip a výhody fungování služby WSUS v lokální počítačové síti

[7]

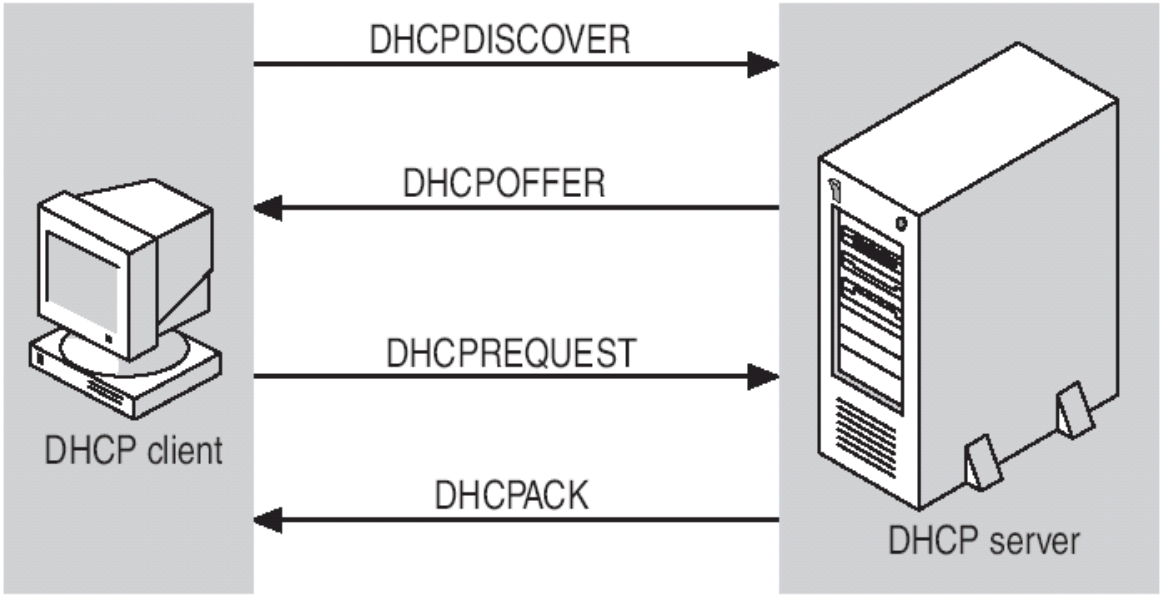
2.1.5 Dynamic Host Configuration Protocol (DHCP)

Úkolem serverů DHCP je v síti automaticky poskytovat klientským počítačům a jiným síťovým zařízením používajícím protokol TCP/IP platné adresy IP. Lze také poskytnout další konfigurační parametry, které umožní klientům se připojit k dalším síťovým prostředkům, jako jsou servery DNS, servery WINS a směrovače.

Princip činnosti

Klienti žádají server o IP adresu, ten u každého klienta eviduje půjčenou IP adresu a čas, do kdy ji klient smí používat (doba zapůjčení, anglicky lease time). Poté co vyprší, smí server adresu přidělovat jiným klientům. Po připojení do sítě klient vyšle broadcastem paket. Na ten odpoví DHCP server paketem s nabídkou IP adresy. Klient si vybere jednu IP adresu a o tu požádá paketem. Server mu ji vzápětí potvrdí odpovědí. Klient musí před uplynutím doby zapůjčení obnovit svou IP adresu. Pokud lhůta uplyne aniž by dostal nové potvrzení, klient musí IP adresu přestat používat.

Protokol definuje roli i tzv. DHCP relay agenta. Používá se v situaci, kdy existují dvě nebo více sítí oddělené směrovačem a jen jedna síť obsahuje DHCP server. V takovém případě správce na směrovači zapne relay agenta a nastaví jej tak, aby všesměrové (broadcast) DHCP dotazy ze sítí bez DHCP serveru přeposílal DHCP serveru. Agent k přeposílanému dotazu přidá číslo sítě a masku sítě, na které klienta zaslechl, aby DHCP server poznal, ze kterého adresního rozsahu má klientovi adresu přiřadit.



Obrázek 3. Komunikace mezi DHCP klientem a serverem

[2]

Možnosti přidělení IP adresy

- **Statická alokace** - DHCP server obsahuje seznam MAC adres a k nim příslušným IP adres. Pokud je žádající stanice v seznamu, dostane vždy přidělenu stejnou pevně definovanou IP adresu.

- **Dynamická alokace** - Správce sítě na DHCP serveru vymezí rozsah adres, které budou přidělovány stanicím, které nejsou registrovány. Časové omezení pronájmu IP adresy dovoluje DHCP serveru již nepoužívané adresy přidělovat jiným stanicím. Registrace dříve pronajatých IP adres umožňuje DHCP serveru při příštím pronájmu přidělit stejnou IP adresu.

2.1.6 Databázový server

Pod tímto pojmem chápeme počítač, na kterém je uložen databázový soubor a zároveň je zde spuštěn databázový stroj, to je aplikace, která pro klienty (pracovní stanice) zpracovává veškeré manipulace s daty. Součástí databázového stroje jsou také některé základní procesy řešící například správu vyrovnávací paměti, archivaci transakčních žurnálů apod. Nad databázovým strojem jsou nadstavby jádra zajišťující komunikaci s okolím, tedy především podpora síťových protokolů a služeb. Výše uvedené komponenty jsou tím, co je označováno jako databázový server. Účelem databázového serveru je tedy zpracovávat databáze prostřednictvím klientů, kteří mají k tomuto serveru přístup. Zpracováním je myšlena samotná tvorba databází, jejich transformace, vkládání dat, jejich modifikace, případně výmaz, apod.

Jediná serverová edice z rodiny Microsoft Windows Server 2003 R2 integrující v sobě databázový server je Windows Small Business Server 2003 Premium Edition jež zahrnuje produkt Microsoft SQL Server 2005 Workgroup Edition, u všech ostatních je nutno tuto funkci doinstalovat zvlášť ať už se jedná o databázové servery od Microsoftu, Oraclu či jiné. V naší síti bude provozován Microsoft SQL Server 2008 ve verzi express (bezplatná verze), toto řešení má omezení na velikost databáze 4 GB, což pro provoz v naší síti a malý počet záznamů bude stačit. Dalšího popisu funkčnosti a popisu databázového serveru se pozdržím, mnohonásobně by to překročilo rozsah této práce.

3 ACTIVE DIRECTORY DOMAIN SERVICES

Adresářová služba AD DS je rozšiřitelná a škálovatelná adresářová služba, která umožňuje efektivně uspořádat síťové prostředky, integruje internetové pojetí oboru názvů s adresářovými službami operačního systému. Tato kombinace umožňuje sjednocení více oboru názvů například ve smíšených prostředích softwaru a hardwaru v podnikových sítích, a to dokonce mezi hranicemi operačního systému. Schopnost zahrnout jednotlivé podnikové adresáře do adresáře pro obecné účely znamená, že služba AD může do značné míry snížit náklady na správu více oborů názvů.

AD není adresář X.500 (Mezinárodní standard, vyvinutý spolkem International Consultative Commitee of Telephony and Telegraphy, pro formátování elektronických zpráv přenášených přes sítě nebo mezi počítačovými sítěmi). Místo toho používá jako protokol pro přístup LDAP a podporuje informační model X.500, aniž by vyžadoval, aby byl systém hostitelem celého standardu X.500. Protokol LDAP je založen na protokolu TCP/IP a je mnohem jednodušší než X.500 DAP. Stejně jako u adresaře X.500 je adresářový model založen na záznamech, kde k odkazům na položky slouží rozlišovací název Ale Spíše než využití vysoce strukturovaného kódování dat X.500 používá LDAP k představování záznamu v adresáři jednoduchý přistup založený na řetězcích. LDAP využívá mnoho technik adresářového přístupu specifikovaných ve standardu X.500 DAP, ale vyžaduje méně klientských prostředků a usnadňuje hlavní vyžiti přes propojeni TCP/IP.

[6,9]

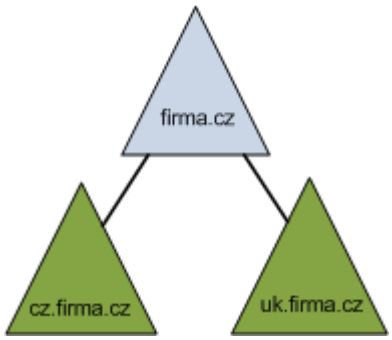
3.1 Základní terminologie a doporučení v AD

3.1.1 Doména (Domain)

Doména je základním prvkem logické struktury AD, jsou v ní přímo uloženy objekty, které do dané domény patří, jednoduše řečeno skupina počítačů sdílejících společnou adresářovou databázi. AD je tvořena jednou nebo více doménami (neomezených na fyzickou lokaci), kde každá má své vlastní zásady zabezpečení a vytvořený vztah důvěryhodností s ostatními. Doména je bezpečnostní hranicí, přístup k doménovým objektům je řízen pomocí ACL, které má nastaveno oprávnění (permissions). Bezpečnostní nastavení a oprávnění nemohou přecházet mezi doménami. [2, 6, 10]

3.1.2 Strom (Tree)

Strom je seskupení nebo hierarchická organizace jedné nebo více domén, které spolu sdílí souvislý jmenný prostor, schéma a hierarchické spojení doménových jmen Strom vznikne tak, že ke kořenové doméně přidáme podřízenou doménu (používá se standard DNS, takže jméno podřízené domény vznikne použitím jejího relativního jména doplněného za tečkou jménem jeho kořenové domény)



Obrázek 4. Ukázka doménového stromu

[6, 9]

3.1.3 Les (Forest)

Les je seskupení jednoho nebo více oddělených nezávislých stromů. Všechny domény v lese sdílí stejné schéma, globální katalog a jsou propojeny implicitním dvoucestným vztahem důvěry (trust).

3.1.4 Lokalita (Site)

Site je kombinace jedné, či více podsítí protokolu IP, které prezentují fyzickou strukturu sítě. Nikde nefigurují v logické struktuře AD, v jejich určení figurují pouze DC a spoje a používají se k replikaci mezi nimi.

3.1.5 Doménový řadič (Domain Controller - DC)

DC je počítač (server), na kterém běží operační systém Windows Server a obsahuje repliku doménového adresáře (lokální doménovou databázi). V doméně může existovat řadičů více, kde každý obsahuje úplnou repliku adresáře pro danou doménu.(replikace se provádí periodicky, případně okamžitě v případě důležitých údajů) Na jednom řadiči může být pouze jedna doména. Doménový řadič také slouží k autentizaci uživatelů.

3.1.6 Atribut

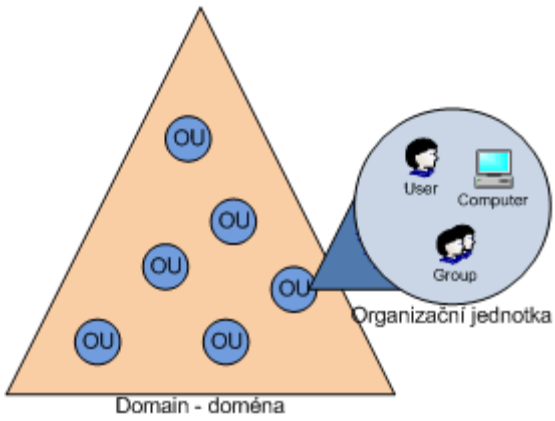
Je v podstatě jakákoliv dílčí informace, popisující nějaký aspekt zápisu. Sestává se z typu atributu a jedné nebo více hodnot atributu (příkladem: telefoní číslo a jeho hodnota atributu je: 733164428)

3.1.7 Objekt

Definuje jej určitá sada atributů, které představují něco konkrétního, kupříkladu: uživatel, tiskárna atd. Atributy obsahují data popisující, co adresářový objekt identifikuje. Atribut může v závislosti na typu obsahovat jednu nebo více hodnot. Každý objekt v AD má jedinečnou identitu, lze je přejmenovávat, nebo přesouvat, ale indentita se nikdy nemění. Danou identitu udává GUID (Globaly Unigue Identifier), který je přidělován každému nově vytvořenému objektu agentem adresářového systému.

3.1.8 Organizační jednotka (Organizational Unit - OU)

OU je kontejner, který se uvnitř domény používá k seskupování/organizování objektů do logických administračních skupin. OU je nejmenší jednotka, na kterou můžeme delegovat administrační oprávnění. OU můžeme zanořovat do sebe a vytvářet libovolnou hierarchickou strukturu. Hierarchie OU je lokální uvnitř domény a neovlivňuje jiné domény. OU se většinou vytváří tak, že odráží strukturu organizace (tedy třeba podle divizí a oddělení). Podle potřeby můžeme uživatelské a počítačové účty umísťovat do stejných OU či vytvářet oddělenou strukturu.



Obrázek 5. Ukázka organizační jednotky ve vztahu k doméně

[10]

3.1.9 Úložiště dat (adresář)

Úložiště dat je kontejnerem pro objekty, obsahující informace o účtech, sdílené prostředky, organizační jednotky, zásady skupin Řadiče domény ukládají tento adresář v souboru Ntds.dit (umístění tohoto souboru se řeší při instalaci domény Active Directory a musí být na jednotce zformátované souborovým systémem NTFS. Adresářová data je také možné uložit odděleně od hlavního úložiště dat. To platí pro zásady skupiny, skripty a další typy veřejných informací, které jsou uložené ve sdílené systémové složce SYSVOL, která musí sdílet společný přístup a replikace v celé doméně.

Replikují se:

- doménová data - obsahují informace o objektech v rámci domény (objekty pro účty, sdílené prostředky, OU a zásady skupin)
- konfigurační data – popisují topologii adresářové služby. Zahrnují seznam všech domén, stromů a lesů a také umístění řadičů domény a serverů globálního katalogu
- data schématu - popisují všechny objekty a typy dat, které mohou být v adresářové službě uloženy (účty, sdílené prostředky apod.)

3.1.10 Globální katalog (Global Catalog - GC)

GC již neurčuje ani logickou ani fyzickou strukturu AD, ale má velmi důležitou roli, pokud hledáme nějaký objekt v AD a tento objekt se nachází ve stejné doméně, tak se ptáme některého DC. Pokud však hledáme objekt z jiné domény (ale uvnitř stejného adresáře - stejné AD), tak potřebujeme nějakou službu, která nám pomůže. V AD je touto službou Globální katalog. To je centrální repozitář, který obsahuje vybrané informace o objektech z celého stromu či lesa. DC, který obsahuje kopii globálního katalogu, se nazývá Global Catalog Server (GC může být provozován pouze na DC). Globálních katalogů můžeme mít více a mezi nimi se provádí multimaster replikace. GC se často umisťují do různých site, pak ale musíme pamatovat na provoz způsobený replikací (který může být značný). Jeho další funkcí je, že poskytuje informace o členství v univerzálních skupinách (universal group membership).

Poznámka: Pokud GC není k dispozici, tak se uživatel může přihlásit pouze na lokální PC, lze obejít zapnutí funkce universal group membership caching (UGMC) na danou site. V tomto případě si DC ukládá informace lokálně.

3.1.11 Uživatel (User)

V systému Windows server 2003 R2 jsou dva typy účtů a to účty místních uživatelů a účty uživatelů domény. Na řadiči domény jsou místní uživatelé a skupiny zakázány (při odebrání role DC jsou automaticky povoleny a vytvořen účet administrátora). Ve službě AD účet uživatele obsahuje jeho jméno, heslo, skupiny, jejichž je členem a další informace (telefon, adresa a astributy typu konfigurace zabezpečení a vzdáleného přístupu).

3.1.12 Počítač (Computer)

Kromě objektů pro kontejnery, skupiny a uživatele poskytuje služba AD také objekty reprezentující počítače. Pro přihlášení do domény musí existovat pojmenovaný objekt počítač, který se buď vytvoří automaticky, nebo manuálně (tato možnost je užitečná například tehdy, pokud chcete bezobslužně instalovat. [1]

3.1.13 Tiskárna (Printer)

Prostřednictví objektů tiskárny je umožněno vytvářet nebo spravovat místní či sdílené tiskárny a tiskárny TCP/IP.

3.1.14 Skupina (Group)

Skupiny se využívají v procesu přidělování oprávnění podobným typům uživatelů a s tím související zjednodušení správy účtů. Pokud je uživatel členem skupiny, která má přístup k prostředku, může tento uživatel k prostředku také přistupovat. Je daleko efektivnější přiřazovat uživatele do skupin než samotná oprávnění přidávat uživatelům.

Typy skupin

V doméně Active Directory se lze setkat s následujícími typy skupin:

- **Skupiny se zabezpečením** Tomuto typu skupiny se udělují práva a oprávnění. Práva určují, co může člen takové skupiny (uživatel nebo počítač) provádět v doméně za činnosti, zatímco oprávnění určují, ke kterým prostředkům v místním počítači či v síti mají uživatelé přístup.
- **Distribuční skupiny** Ve spolupráci s produktem Exchange Server 2003 jsou ty to skupiny určeny pouze k odesílání emailových zpráv uživatelům. Nemohou získávat oprávnění přístupu, ani na to nejsou přizpůsobeny.

Poznámka: Skupiny se zabezpečením mají schopnosti distribučních skupin, opačně to však neplatí, tyto skupiny existují proto, neboť některé aplikace umí pracovat pouze s nimi.

Rozsah Skupin

- **Globální skupiny** můžou obsahovat uživatelské účty, účty počítačů či skupiny vytvořené ve stejné doméně, ve které byla vytvořena i ona. Globální skupině je možné, ačkoli to není ve většině případů doporučeno, udělovat oprávnění a práva k prostředkům v jakékoli doméně lesa AD (odtud v názvu slovo „globální"). Vzhledem k tomu, že globální skupiny jsou viditelné v jakékoli doméně lesa AD nepoužívají se primárně pro udělování přístupu k prostředkům ve své doméně. Jejich hlavním účelem je seskupení uživatelů s podobnými zájmy v síti (tisk na stejné tiskárny, přístup do stejných složek apod.).
- **Místní doménové skupiny** Místní doménová skupina může obsahovat globální skupiny, univerzální skupiny, uživatelské účty či účty počítačů z jakékoli domény lesa AD a jiné místní doménové skupiny z vlastní domény. Primárním účelem doménových skupin je udělování oprávnění není a práv k prostředkům pouze v rámci vlastní domény. Místní doménové skupiny jsou určené k udělování oprávnění přístupu k prostředkům, které se nacházejí ve stejné doméně.
- **Univerzální skupiny** mohou obsahovat uživatelské účty, účty počítačů nebo skupiny z jakékoli domény lesa AD. Univerzálním skupinám se zabezpečením je možné udělovat oprávnění přístupu k prostředkům v jakékoli doméně lesa. Univerzální skupiny slouží ke sloučení globálních skupin pro zjednodušení přístupu k prostředkům ve větších prostředích s více doménami v rámci lesa AD. Vzhledem k jednoduchosti našeho prostředí není nutné univerzální skupiny používat.

Strategie pro používání skupin

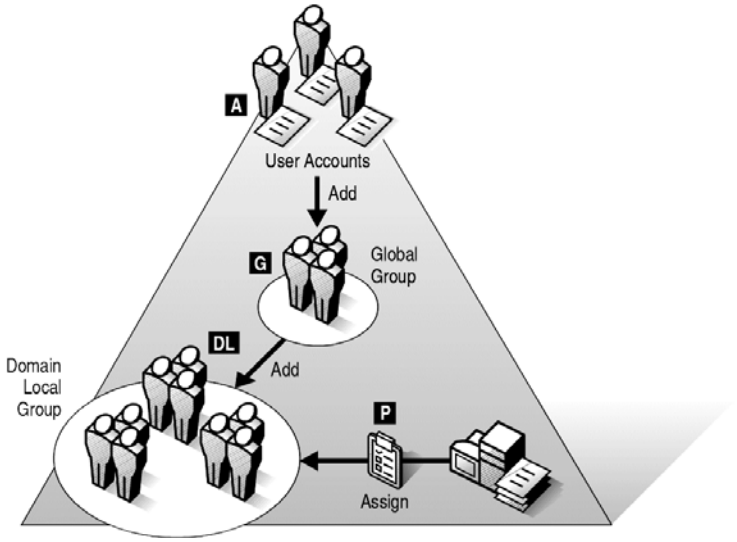
Typů a rozsahů skupin je opravdu celá řada, což by mohlo svádět k bezhlavému nasazování různých typů skupin a k následnému většímu a většímu chaosu v doméně. Proto je dobré nechat se vést doporučenými strategiemi pro používání skupin. Tyto strategie jsou navržené tak, aby co nejvíce usnadňovaly práci správcům, a aby přitom celá konfigurace zůstala přehledná a co možná nejjednodušší.

Pro účely vysvětlení strategií je nutné označit si dotčené objekty konkrétními písmeny. Objekty označíme následovně:

- A uživatelské účty (user Accounts)
- G globální skupiny (Global groups)
- DL místní doménové skupiny (Domain Local groups)
- U univerzální skupiny (Universal groups)
- P oprávnění přístupu k prostředku (Permissions)

Doporučená strategie (nejčastější)

Tuto strategii lze jednoduše označit jako A G DL P. Znamená to, že účty uživatelů se stanou členy globální skupiny a místní doménové skupině se udělí oprávnění přístupu k danému prostředku (např. složka souborů). Aby tedy měli uživatelé k tomuto prostředku přístup, zbývá jediný krok - globální skupinu vložit do místní doménové skupiny. Celý proces lze jednoduše zobrazit takto: **A -> G -> DL <- P**



Obrázek 6. Doporučená strategie pro používání skupin A G DL P

[7]

Pro příklad uvedu aplikaci této strategie v prostředí naší domény vydos.local.

Uživatelé vnitrostátní dopravy potřebují přístup do složky vozový park. Budeme-li se držet zásady, že oprávnění by se neměla udělovat jednotlivým uživatelským účtům, ale skupinám, vypadala by situace následovně:

- Vytvoření globální skupiny se zabezpečením.

- Vložení účtů obchodníků do této skupiny (seskupení uživatelů s podobnými zájmy).
- Vytvoření místní doménové skupiny se zabezpečením.
- U dělení oprávnění (například Změnit) místní doménové skupině.
- Vložení globální skupiny do místní doménové skupiny.

Poznámka: Mohlo by se zdát, že doménová skupina je v celém procesu zbytečná, toto však lze použít pouze u velmi malých sítí, kde je jasné, že v lese AD nevznikne další doména. V případě přidání další domény, v této musí existovat účty uživatelů, kteří by rádi získali přístup do existující složky používané v první doméně. Pro ně by tedy bylo vhodné vytvořit v doméně globální skupinu, které by se poté udělila oprávnění přístupu k dané složce. Na kartě zabezpečení ve vlastnostech této složky bude více položek, než v případě použití místní doménové skupiny. Což znepřehledňuje správu.

Ostatní strategie

- **Strategie A G P** Tato strategie odpovídá tomu, co bylo uvedeno v poznámce ke strategii A G DL P. Strategii A -> G <- P je tedy vhodné použít pouze ve velmi malých prostředích a pouze za předpokladu, že nikdy nebude v lese Active Directory více než jedna doména. V opačném případě se správce, který tuto strategii nasadil, žene do záhuby.
- **Strategie A G U DL P** V této strategii je použita univerzální skupina. Univerzální skupiny mají výhody a nemají nevýhody místních doménových i globálních skupin. Obecně přispívají ke zjednodušení prostředí, tedy k větší přehlednosti. Prostředí s jedinou doménou Active Directory však nikdy není tak nepřehledné (při dodržení strategie A G DL P), aby bylo nutné univerzální skupiny nasadit. Univerzální skupiny se tedy nasazují v prostředích, která sestávají z více domén Active Directory.

Poznámka: Oproti místním doménovým i globálním skupinám liší v tom, ukládá informace o tom, kdo je v dané skupině členem nikoliv na všechny řadiče domény, ve kterých jsou skupiny vytvořené, ale na servery globálního katalogu v celém lese AD, při změně v této skupině dojde k replikaci mezi těmito a to může v negativním směru ovlivňovat zatížení sítě.

- **Strategie A C L P (L = místní skupina)** Tato strategie byla doporučena v doménách se systémem Windows NT 4.0 Server, kde neexistovaly místní doménové skupiny. Nevýhody jsou zřejmé místní skupny nelze spravovat centrálně, což může způsobit značné potíže v případě, kdy jich bude zapotřebí věřší množství. Další nevýhodou je nemožnost použít místní skupinu pro přístup k prostředkům v jiném počítači, respektive by se musela vytvořit další místní skupina.

3.2 Zásady skupin (Group Policy)

Jedná o sadu pravidel aplikovatelnou v prostředí celého podniku, a to s pomocí:

- **Nastavení Zásad skupin** - umožňuje řídit konfiguraci operačního systému a jeho komponent. Slouží také ke konfiguraci počítače, uživatelských skriptů, přesměrování adresářů, bezpečnosti počítače, instalaci software a k mnohým dalším účelům. Rozeznáváme tři hlavní třídy:
    - **Nastavení Softwaru** – automatická instalace a upgrade.
    - **Nastavení systému Windows** – nastavení a ovládání klíčových nastavení systému Windows jak uživatelů, tak počítačů včetně zabezpečení a skriptování.
    - **Šablony pro správu** – slouží ke změnám konfigurací operačního systému, komponent Windows a aplikací (např. Ovládací panely, Plocha, Síť, Sdílené složky, Tiskárny, Nabídka, Start a Hlavní panel, Systém, Součásti systému Windows).
- **Předvolby Zásad skupin** se uplatní při konfiguraci, nasazení a správě nastavení operačního systému a aplikací. Patří sem zdroje dat, mapované disky, proměnné prostředí, síťové disky, možnosti složky, zástupci a další. Předvolby mají dvě zásadní třídy voleb:
    - **Nastavení systému Windows** – konfigurace klíčových nastavení, pro uživatele i počítače, systému Windows – zástupců, hodnot registrů, souborů a složek. Dále pak mapování jednotek pro uživatele a sdílení síťových složek pro počítače.

- **Nastavení Ovládacích panelů** - konfigurace utilita a voleb v Ovládacích panelech.

Rozdílem mezi předvolbami a nastavením zásad je ve vynutitelnosti, zásady skupin přísně vynucují nastavení zásad, naopak předvolby nikoliv.

V zásadách skupin jsou dvě oddělené sady:

- **Zásady počítače** - vztahují se na počítače a ukládají se v rámci GPO do uzlu Konfigurace počítače, aplikuje se při spuštění PC
- **Zásady uživatele** - vztahují se na uživatele a ukládají se v rámci GPO do uzlu Konfigurace uživatele, aplikuje se jako reakce na přihlášení uživatele k PC

4 ANALÝZA BEZPEČNOSTNÍCH HROZEB

Slova „zabezpečení" nebo „bezpečnost" se dnes v oblasti IT opakují kolem dokola. Není se co divit. S tím, jak postupně různé oblasti využívají možnosti informačních technologií více a více, mají data vyšší a vyšší cenu. Každý, kdo vlastní citlivá data, by si pak měl dvakrát rozmyslet, jak bude nakládat s jejich uložením v počítačích nebo při přenášení v síti. Ačkoli se v mnoha organizacích zapomíná na oficiální svěření oblasti zabezpečení dat a sítě konkrétní osobě, tak nějak se automaticky očekává (zejména v těch menších organizacích), že to budou správci sítě, kdo tuto oblast budou zajišťovat. Pro účely co nejlepšího zabezpečení popíšu možné hrozby, které je při tvorbě komplexního zabezpečení třeba mít vždy namysli a proti kterým je důležité systémy chránit.

4.1 Obecná rizika

Jeden z nejčastějších problémů se kterým se uživatelé často setkávají, je malware. Výraz malware vznikl složením anglických slov „malicious“ (zákeřný) a „software“ a popisuje záměr autora takového programu spíše než jeho specifické vlastnosti. Pod souhrnné označení malware se zahrnují počítačové viry, trojské koně, spyware a adware.

Tyto škodlivé programy mohou způsobit nemalé škody v provozu jakéhokoliv počítače, ať už se jedná o klientskou stanici, či dokonce serveru. Pro lepší ochranu před těmito škodlivými programy je dobré vědět, jak fungují.

Za virus se označuje program, který se dokáže sám šířit bez vědomí uživatele, replikuje se tak, že se sám připojí k nějakému jinému objektu. Dá se říci, že se chová jako virus biologický, který se šíří vkládáním svého kódu do živých buněk. V souladu s touto analogií se někdy procesu šíření viru říká nakažení či infekce a napadenému souboru hostitel. Zatímco některé viry mohou být cíleně ničivé (např. mazat soubory na disku), mnoho jiných virů je relativně neškodných popřípadě pouze obtěžujících. U některých virů se ničivý kód spouští až se zpožděním (např. v určité datum či po nakažení určitého počtu jiných hostitelů), což se někdy označuje jako (logická) bomba. Nejdůležitějším negativním důsledkem šíření virů je však samotný fakt jejich reprodukce, která zatěžuje počítačové systémy a plýtvá jejich zdroji. Některé viry mohou být takzvaně polymorfní (každý jeho „potomek“ se odlišuje od svého „rodiče“). Viry se na rozdíl od červů samy šířit nemohou.

Červ je nezávislý program, který se replikuje tak, že se sám kopíruje z jednoho počítače na druhý, obvykle přes síť nebo prostřednictvím příloh elektronické pošty. Mnoho

červů navíc obsahuje i virový kód, který dokáže poškodit data nebo spotřebovává tolik systémových zdrojů, že se operační systém stane nepoužitelným. Případně zašifruje soubory uživatele kryptovirálním útokem jako nátlak k zaplacení poplatku.

Trojský kůň je program, který má podobu skrytého serveru, umožňující vetřelci převzít kontrolu nad vzdáleným počítačem, aniž by o tom jeho uživatel věděl, většinou má podobu užitečného programu např. hry. Počítače, které byly napadeny programem v podobě trojského koně, se někdy označují jako zombie. Zástupy takto ovládnutých počítačů mohou vyvolat drastické útoky proti webovým serverům.

Nejčastěji se tyto nebezpečné programy šíří prostřednictvím příloh elektronické pošty a návštěvy webových stránek poskytujících warez. Temnou stránkou elektronické pošty je tzv. nevyžádaná pošta v dnešní době označována jako spam. Spam představuje pro většinu lidí pouhou nepříjemnost může sebou však nést viry a jiný nepřátelský software. Možnou obranou proti těmto rizikům je neustálé instalování aktualizací systému, konfigurace brány firewall a samozřejmě instalace antivirového programu. A hlavně zdraví rozum uživatele.[3, 4]

4.1.1 Sociální inženýrství

Sociální inženýrství je běžně používaný termín pro metodu, jež vede legitimní počítačové uživatele za účelem provedení určité akce, nebo k poskytnutí užitečných informací, které pomáhají útočníkovi získat neautorizovaný přístup do jejich počítačového systému. Sociální inženýrství je tedy způsob získávání důležitých informací od uživatelů bez vědomí, že tak činí. Obranou proti sociálnímu inženýrství je vzdělání uživatelů, nedůvěra, ověřování zdroje a odmítnutí. [3]

4.2 Specifická rizika služeb Windows Server 2003 R2

Každému počítači, zastávajícímu funkci serveru, hrozí specifická rizika spojená s poskytováním služeb klientům. Množství těchto rizik se zvětšuje s každou nově instalovanou službou. Níže budou popsány nejčastější útoky na nejpoužívanější služby systému Windows Server 2003 R2.

4.2.1 Bezpečnostní hrozby řadiče domény

DC je počítač, na kterém je uložen adresář služby AD. Řadič domény Windows musí být správně zabezpečený, jelikož je pravděpodobným cílem útoku, při němž může dojít k

ohrožení databáze AD a objektů v ní uložených. Řadič domény se systémem Windows Server 2003 R2 může čelit následujícím hrozbám:

- Modifikace nebo přidávání objektů služby AD
- Útoky na heslo
- Útoky s odepřením služeb (DoS)
- Útoky s vyřazením replikací
- Zneužití známých zranitelných míst

[5]

Modifikace nebo přidávání objektů služby AD

V případě napadení řadiče domény (DC) získá útočník možnost provádět jakékoliv změny stávajících objektů ve službě Active Directory (AD).

Útoky na heslo

Má-li útočník přístup k DC, má možnost replikovat databázi a protokoly služby AD na jiní PC, na tomto již je možno vést útok na heslo v off-line stavu databáze.

Útoky s odepřením služeb (DoS)

Za pomoci útoku, zvanému DoS (Denial of Service) spočívajícího vesměs ve vygenerování co největšího toku (v případě DoS Flood), dokáže útočník zahltit linku oběti tak, aby bylo zabráněno provádění ověřování uživatelů, nebo vést útoky proti službě DNS, což způsobí, že klienti nebudou moci v síti vyhledat řadiče domény. Existují i jiné typy DoS útoků: typy využívající chyb a vyčerpání systémových prostředků, které využívají zranitelnosti v softwaru nebo hardwaru oběti (bývají velmi rychle opraveny), nebo DoS využívající Mitm (Man in the middle), případně reflektivní DoS útoky. Jejich přehled a popis však není povahou této práce.

Útoky s vyřazením replikací

V případě, že se útočníkovi podaří přerušit chod replikací databáze napříč řadiči domény, může tím zabránit i v aplikaci objektů Group Policy (Zásad skupiny), které by mohly řadiče domény chránit před vyřazením z činnosti.

Zneužití známých zranitelných míst

Není-li řadič domény udržován v aktuálním stavu, může se stát snadným cílem útočníků.

4.2.2 Bezpečnostní hrozby DNS (Domain Name System)

Služba DNS (popsána v kapitole 2.1.3) může čelit následujícím hrozbám:

- Změny v záznamech služby DNS
- Přenosy zón s daty DNS do neoprávněného serveru
- Útoky s odepřením služeb (DoS) proti službám DNS
- Vyřazení přístupu k záznamům prostředků DNS v kořeni doménové struktury

[5]

Změny v záznamech služby DNS

V případě úspěšné modifikace záznamů prostředků DNS, lze přesměrovat klienty na jiný DNS server. A tímto moci podvrhnout například falešné stránky za účelem získání osobních údajů. Lze také „znečistit" mezipaměť cache serveru DNS falešnými informacemi, v tomto případě bude server DNS odesílat klientům pozměněné odpovědi a nespojí s autoritativním serverem DNS.

Poznámka: Lze zabezpečit pomocí DNSSEC což je rozšíření, která klientům DNS (resolvery) umožňuje ověření původu dat a jejich integrity.

Přenosy zón s daty DNS do neoprávněného serveru

Zóna DNS obsahuje záznamy prostředků SRV a IP adresy, z nichž se dá snadno sestavit topologický diagram sítě v případě získání dat zóny DNS útočníkem.

[4]

Útoky s odepřením služeb (DoS) proti službám DNS

Vše co bylo o útocích typu DoS popsáno v kapitole 4.2.1.3, platí též pro služby DNS. Kdy při nefunkčnosti této služby přestane v síti fungovat ověřování a vyhodnocování hostitelských názvů v síti.

Vyřazení přístupu k záznamům prostředků DNS

Zóna DNS kořenové domény struktury obsahuje záznamy prostředků DNS včetně záznamů prostředků SRV s globálně jedinečnými identifikátory GUID. Pokud k těmto záznamům nelze přistupovat, nastane situace, kdy DC nenalezne záznamy svých partnerů pro replikaci a tím selže replikace databáze napříč jednotlivými DC.

4.2.3 Bezpečnostní hrozby DHCP (Dynamic Host Configuration Protocol)

Protokol DHCP (popsán v kapitole 2.1.5) je v síťovém prostředí vystaven následujícím hrozbám:

- Neoprávněné servery DHCP
- Server DHCP přepíše platné záznamy prostředků ve službě DNS
- Neoprávněný klient DHCP

[5]

Neoprávněné servery DHCP

Útočník, který získal přístup do vnitřní sítě, může uvést do provozu falešný server DHCP, ten následně klientům podává nesprávné IP adresy a další informace.

Poznámka: V případě provozování služby AD je riziko zavlečení neoprávněného serveru DHCP sníženo neboť servery DHCP se musí autorizovat (ověřovat) v adresářové službě AD.

Server DHCP přepíše platné záznamy prostředků ve službě DNS

Proces registrace záznamů prostředků DNS na serveru DNS je ve výchozím nastavení rozdělen mezi server a klient DHCP. Server DHCP zaregistruje záznamy prostředků PTR (Pointer), zapisované do zóny zpětného vyhledávání, a je také jejich vlastníkem, zatímco klient DHCP registruje svůj záznam prostředku A v zóně dopředného vyhledávání.[3]

Při úspěšné změně konfigurace serveru DHCP, může server zaregistrovat oba záznamy prostředků (PTR, A) a následně se stát jejich vlastníkem. V takovém případě může server DHCP přepsat informace o klientu, který již nebude moci aktualizovat svoji IP adresu ve službě DNS neboť není již jeho vlastníkem.

Poznámka: Systémy podporující dynamické aktualizace DNS zajišťují, že modifikaci záznamů prostředků DNS může vykonat výhradně jeho vlastník.

Neoprávněný klient serveru DHCP

Protokol DHCP není ověřovaný protokol, neumožňuje ve své nativní podobě nijak omezit nebo odfiltrovat klienty a přiřazuje IP adresu libovolnému klientovi, který si jí vyžádá. (pokud je ve fondu pronajímaných adres volná adresa) Z toho je zřejmé, že neoprávněný klient může získat informace o konfiguraci TCP/IP a případně komunikovat s veškerými službami TCP/IP v síti a s dalšími službami AD.

Poznámka: Částečným řešením je aplikovat filtr umožňující tvorbu white nebo black listů MAC adres. Není to sice ideální ochrana, podvrhnout MAC adresu není zase tak velký problém, nicméně to již představuje poměrně sofistikovanou činnost.

4.3 Fyzické útoky

Toto nejelementárnější narušení bezpečnosti počítače nevyžaduje od útočníka žádné technické znalosti. V případě, že je počítač zanechán, bez dohledu může dojít k jeho odcizení. I když se toto týká převážně notebooků, ale ani u stolních počítačů to není ničím neobvyklým. Jestliže je útočník technicky zdatný, dokáže váš počítač odnést, pak na něm může pracovat celé dny, či týdny; s takovým dostatkem času se dokážou zloději dostat do každého počítače, bez ohledu na to, jak dobře je ochráněn. Útočník však nemusí počítač odnést, stačí jen, když nedbalí uživatelé nechají přihlášený počítač bez dozoru. V tomto případě je cesta ke zkopírování, či znehodnocení dat volná. Další možností je nahrání backdoor, keyloggeru, či jiného škodlivého kódu. Tyto útoky lze minimalizovat například, tak že počítače s citlivými informacemi budou za zamčenými dveřmi, v případě, že jde o velice citlivé informace šifrovat soubory a složky systému nebo použití bezpečnostních zámků k upevnění počítače. U serverů jsou jistá opatření přímo nutnost.

[3]

II. PRAKTICKÁ ČÁST

5 POPIS STAVU PŘED IMPLEMENTACÍ ACTIVE DIRECTORY DOMAIN SERVICES

V následujících kapitolách je popsán stávající stav IT infrastruktury Vydos servis a.s.

5.1 Síťová architektura

Většina subjektů firmy Vydos servis a.s. je soustředěna v hlavním komplexu firmy a jednotlivé budovy v rámci tohoto komplexu jsou propojeny technologií optických tras, které přímo spadají pod správu firmy. Dalším subjektem je budova autobusového nádraží spojená přes technologii wi-fi.

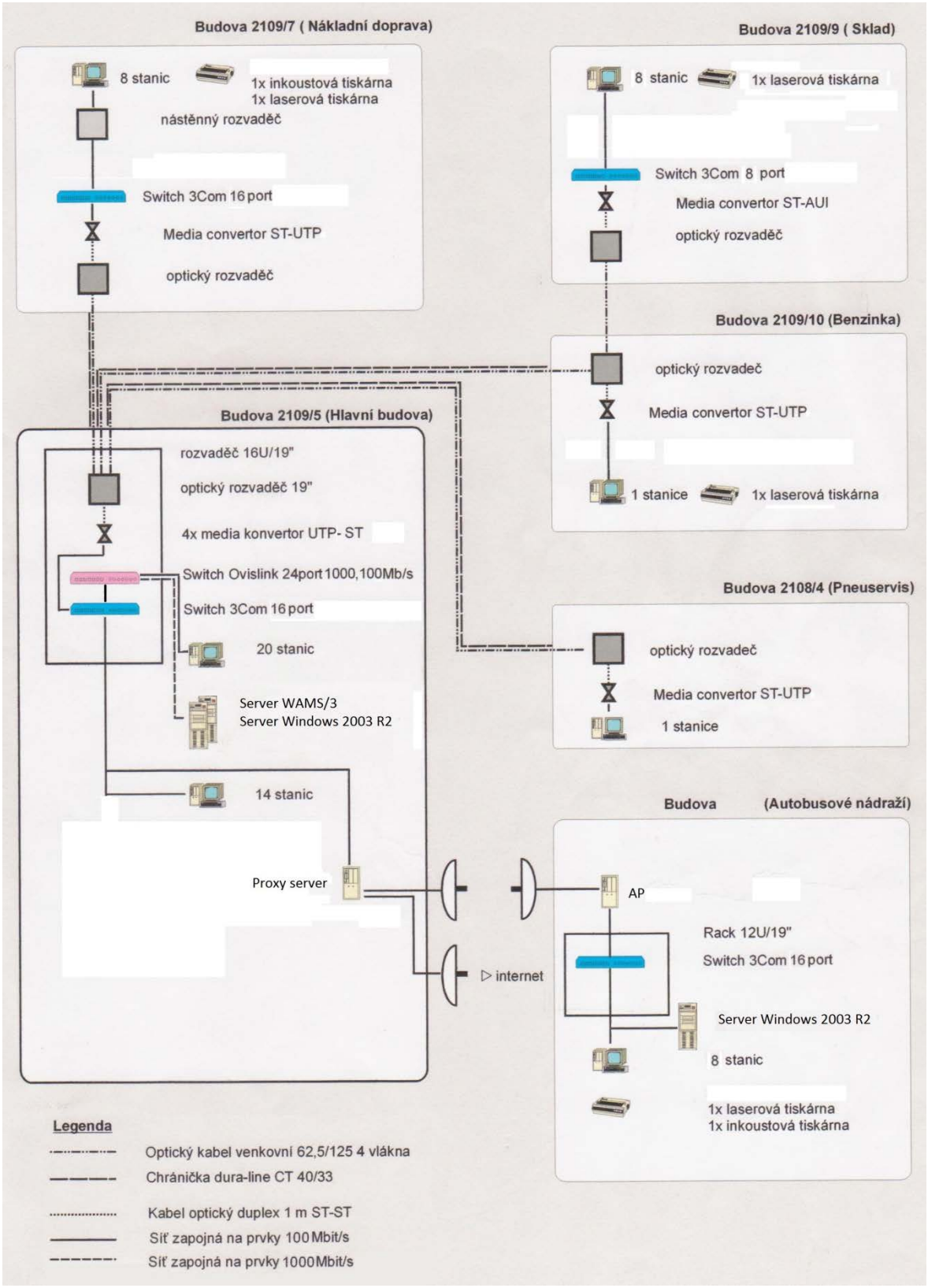
Propojení aktivních prvků v síti zprostředkovává strukturovaná kabeláž (FastEthernet 10/100Base TX, případně u serverů 1000Base-T). Vzájemná konektivita je tedy považována za propojení v rámci sítě LAN (Local Area Network).

5.2 Servery

Ve firmě jsou provozovány 4 servery, 2 na platformě SUSE Linux Enterprise Server a 2 na Microsoft Windows server 2003 R2. Na linuxových serverech běží informační systém WAMS/3 s databází Oracle a druhý má funkci proxy serveru a emailového serveru. Server na platformě Microsoft měl roli databázového a souborového serveru, druhý sloužil jako záložní. Podrobněji toto popíšu v popisu jednotlivých síťových služeb.

Server	Operační systém	Funkce	Hardware
HP ML 150 G3	Microsoft Windows Server 2003 R2 standart	Databázový a souborový server	Intel Xeon E5310, 4 jádra 1.6Ghz, 4GB ECC fully buffered DDR2, 4*500GB RAID 10 SATA
HP ML 150 G3	Microsoft Windows Server 2003 R2 standart	Databázový a souborový server (záložní)	Intel Xeon E5150, 2 jádra 2.66Ghz, 2GB ECC fully buffered DDR2, 2*250GB RAID 1 SATA
IBM x236	SUSE Linux Enterprise Server 9	Informační systém WAMS/3 na databázi Oracle	Intel Xeon 3.0GHz ,4GB DDR2 ECC, 4*73,4GB RAID 10 SCSI
IBM x206	SUSE Linux Enterprise Server 9	Proxy a emailový server	P4-3.2GHz, 2GB DDR, 3*36,4GB IBM RAID 5 SCSI

Tabulka 3. Přehled firemních serverů



Obrázek 7. Schéma počítačové sítě firmy Vydos servis a.s.

5.2.1 IP adresní plán

Adresní plán sítě vychází z rozdělení na podsítě daným prostorovým řešením. Všechny subjekty v síti (vyjma proxy serveru, který má adresu veřejnou) používají interní IP adresy z rozsahu 192.168.x.x.

IP adresace

- síť (hlavní komplex budov): 192.168.1.0/24
  - DNS server: 192.168.1.10
  - brána: 192.168.1.1
- síť (autobusové nádraží): 192.168.2.0/24
  - DNS server: 192.168.2.10
  - brána: 192.168.2.1

5.2.2 Rozdělení aktivních prvků

Hlavní budova firmy je v rámci celého komplexu propojena optickou trasou, vzdálená budova autobusového nádraží pomocí technologie wi-fi. Vně budov je rozvedena strukturovaná kabeláž k aktivním prvkům umístěných v jednotlivých předem vybraných lokalitách, ke kterým jsou připojena jednotlivá koncová zařízení (PC, tiskárny aj.). Přehled zařízení je uveden v následující tabulce:

Aktivní prvek	IP adresa	Umístění
Switch OvisLink AirLive FSH2422W, 24x 10/100 Mbps, 2x 1000 Mbps, management	192.168.1.2	2109/5 (Hlavní budova)
Switch 3Com 2016 16x 10/100 Mbps	Nemá	2109/5 (Hlavní budova)
Switch 3Com Office Connect 16x 10/100 Mbps	Nemá	2109/7 (Nákladní doprava)
Switch 3Com Office Connect 16x 10/100 Mbps	Nemá	2109/9 (Sklad)
Switch 3Com Office Connect 8x 10/100 Mbps	Nemá	2109/10 (Benzínka)
Switch 3Com Office Connect 8x 10/100 Mbps	Nemá	2109/8 (Pneuservis)

Switch 3Com Office Connect 16x 10/100 Mbps	Nemá	Budova autobusového nádraží
Edimax ET-912MST média konvertor, 10/100BaseTX na 100BaseFX multi-mode Fiber Optic ST, 2km	Nemá	2109/5 (Hlavní budova)
Edimax ET-912MST média konvertor, 10/100BaseTX na 100BaseFX multi-mode Fiber Optic ST, 2km	Nemá	2109/5 (Hlavní budova)
Edimax ET-912MST média konvertor, 10/100BaseTX na 100BaseFX multi-mode Fiber Optic ST, 2km	Nemá	2109/5 (Hlavní budova)
Edimax ET-912MST média konvertor, 10/100BaseTX na 100BaseFX multi-mode Fiber Optic ST, 2km	Nemá	2109/5 (Hlavní budova)
Edimax ET-912MST média konvertor, 10/100BaseTX na 100BaseFX multi-mode Fiber Optic ST, 2km	Nemá	2109/7 (Nákladní doprava)
Edimax ET-912MST média konvertor, 10/100BaseTX na 100BaseFX multi-mode Fiber Optic ST, 2km	Nemá	2109/9 (Sklad)
Edimax ET-912MST média konvertor, 10/100BaseTX na 100BaseFX multi-mode Fiber Optic ST, 2km	Nemá	2109/10 (Benzínka)
Edimax ET-912MST média konvertor, 10/100BaseTX na 100BaseFX multi-mode Fiber Optic ST, 2km	Nemá	2109/8 (Pneuservis)
Acces-Point UBNT NanoStation M5	192.168.2.2	Budova autobusového nádraží

Tabulka 4. Přehled aktivních prvků

5.2.3 Rozdělení LAN na VLANy

Pro logické seskupení uživatelů, zvýšení bezpečnosti a snížení broadcastů byly na Switchi OvisLink nastaveny pro jednotlivá oddělení virtuální LAN sítě. Pomocí Port VLAN, kde je port switche ručně a napevno zařazen (nakonfigurován) do určité VLANy. Veškerá komunikace, která přichází přes tento port, spadá do zadané VLANy. Přehled jednotlivých VLAN uvání následující tabulka:

Vlan č:	Popis
1	Nákladní doprava
2	Sklad
3	Benzinka
4	Pneuservis
5	Celní správa
6	Vedení
7	Fakturace
8	Účetní
9	Docházka

Tabulka 5. Přehled VLAN

5.3 Síťové služby

Před realizací této práce. Sice na firmě běžely dva servery s Microsoft Windows 2003 R2, role serveru AD však nebyla využívána. V následující části popíšu stav základních síťových služeb před realizací projektu.

5.3.1 AD DS

Tato služba nebyla využívána.

5.3.2 Souborový server

Microsoft Windows server 2003 R2 ve firmě zastával tuto roli, za účelem sdílení společných dat pro jednotlivé skupiny uživatelů a pro zálohování klientských stanic. Bez služby AD DS však byla jakákoliv změna zaměstnance, či jeho oprávnění poměrně časově náročnou činností.

5.3.3 Terminálový server

Terminálový server sice byl ve firmě využíván, nic méně pouze v režimu vzdálené plochy, tj. bez jeho aktivace a spuštění licenční služby, to znemožňovalo vzdálený přístup více než dvěma uživatelům zároveň. Toto řešení přestalo býti dostačující a vyžádalo si plnohodnotné zprovoznění této služby.

5.3.4 DNS

Původně ve firmě neběžel žádný DNS server, ale byly použity DNS servery poskytovatele připojení k internetu.

5.3.5 WSUS

Tato služba nebyla využívána.

5.3.6 DHCP

Tato služba nebyla ve firmě nikdy využita, používalo se statické adresy.

5.3.7 Databázový server

Na platformě Microsoft Windows server 2003 R2 běží ve firmě dva databázové servery Microsoft SQL server 2008 Express s databázemi pro programy ESET NOD32 (centrální správa), aplikaci Echotrack od firmy Auris a.s. pro aktuální přehled vozového parku a SW Mobilchange pro hromadné rozesílání SMS. Druhý server slouží jako záložní pro replikaci databází. Na tomto stavu se nebude nic měnit.

5.4 Ostatní služby

5.4.1 Centrální správa antiviru

V současné době se ve firmě využívá řešení od firmy ESET a to antivirový program s centrální správou NOD32. Pro ukládání dat využívá toto řešení databázový server Microsoft SQL server 2008 express.

5.4.2 Elektronická pošta

Správu e-mailů zajišťuje firemní proxy server, který má také roli e-mailového serveru (Postfix), který veškerou příchozí poštu kontroluje na přítomnost virů (NOD32) a spamu (SpamAssassin) a jsou na něm uloženy e-mailové schránky uživatelů. Stejný server zajišťuje odesílání veškeré pošty z firmy. Využívá protokolů POP3, pro použití protokolu IMAP nemá server dostatečnou diskovou kapacitu. Pro přístup k e-mailu je možné použít libovolného klienta podporujícího tento protokol nebo lze použít webového klienta SquirrelMail.

5.4.3 Docházkový systém

Docházkový, turniketový a stravovací systém je řešen produktem od firmy Cominfo a.s. a využívá Microsoft SQL serveru 2008. Toto řešení v instalované verzi s AD DS nespolupracuje, v případě nového zaměstnance je tedy třeba zadat do tohoto systému jeho údaje zvlášť.

5.4.4 Informační systém

Je využíván informační systém WAMS/3 od firmy Micros a.s., tento běží na samostatném linuxovém serveru a implementací AD DS na něj nebude mít žádný vliv.

5.4.5 Centrální správa záložních zdrojů

Na serveru je nainstalován SW APC PowerChute Business Edition, který monitoruje stav všech záložních zdrojů ve firmě.

5.5 Licenční politika

Firma vlastní 60 licencí klientského přístupu na zařízení a 15 licencí klientského přístupu pro terminálový server.

5.6 Operační systém klientských stanic

Firma vlastní 48 stanic s operačním systémem Windows XP Professional a 12 stanic se systémem Windows 7 Professional. Stanice jsou průběžně měněny za nové se systémem Windows 7 Professional vzhledem ke konci podpory Windows XP, která má být ukončena 8.dubna 2014. Nákup licencí systému Windows 7 formou upgrade se neplánuje.

6 NÁVRH ACTIVE DIRECTORY DOMAIN SERVICES

Návrh je vytvořen pro prostředí firmy Vydos servis a.s. na základě dosud nabitých poznatků autora a technickými možnostmi firmy. Základní myšlenkou je vytvoření takové struktury, která efektivně zpřístupňuje adresářové informační zdroje, aplikace a služby koncovým uživatelům prostřednictvím jednoho přihlášení.

6.1 Doménové jméno

Jedním ze základních předpokladů úspěšné implementace AD DS je stanovení si pravidel pro pojmenování objektů, je to dobré pro snadné dohledávání lokalit, serverů, počítačů nebo uživatelů, tak struktury celého doménového prostoru firmy. V případě jejich nedodržení nastane ve větších sítích chaos.

Při výběru doménového jména se nabízí u nás asi nejpoužívanější možnost a to **názevsubjektu.cz**, toto pojmenování za sebou však skýtá jistá úskalí pří konfiguraci DNS, proto je záměrně oddělena interní doména od externí s použitím přípony **.local**. Název domény je tedy ***vydos.local***. V praxi toto pojmenování zamezí kolizi s externí subdoménou.

Jistá pravidla je též nutné dodržovat i u pojmenování DC, Lokalit, klientských PC, skupin, organizačních jednotek, uživatelů atd. Zde je seznam mnou stanovených pravidel:

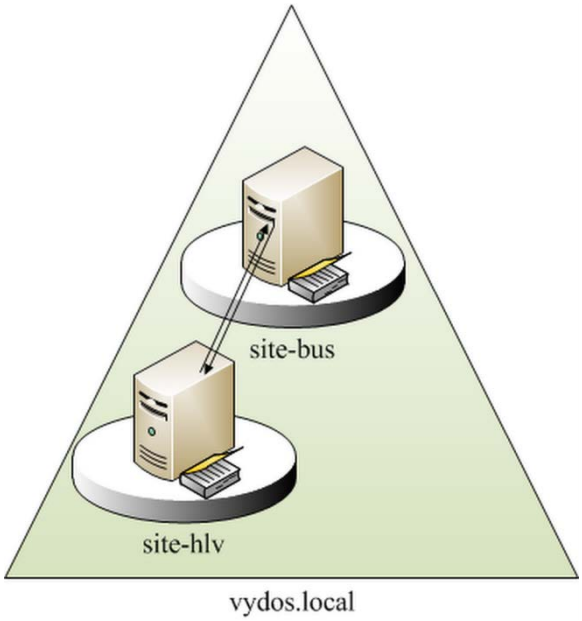
- Lokalita: site-lokace(3 znaky) např. site-bus
- Lokální skupina: druh_skupiny_název_oprávnění např. l_smlouvy_rw = přístup do adresáře smlouvy
- Skupinová politika: funkce objektu_popis objektu např. Povoleno příkazový řádek
- Počítače: příjmení uživatele + číslo kanceláře
- Uživatelé: první písmeno křestního jména_příjmení(v případě kolize doplnění čísla)

V případě organizačních jednotek a globálních skupin je pojmenování dáno organizační strukturou. U serverů a DC je pojmenování vcelku nepodstatné vzhledem k velikosti sítě s celkovým počtem tří serverů.

6.2 Doménová struktura

V rámci návrhu doménové struktury je upuštěno od více doménové struktury

i doménového lesa a je zvolena jedna doménová architektura s předpokladem stejné základní bezpečnostní a přístupové politiky pro celou firmu.



Obrázek 8. Návrh doménové struktury a lokalit

Jediná doména s názvem **vydos.local** zajišťuje doménové prostředí firmy, která je spravována dvěma DC z toho jsou každý v jiné lokalitě. Replikací všech lokalit docílíme totožné informace na všech DC. Doména je dále rozvržena do Organizačních jednotek a ty jsou pak použity k nastavování jednotlivých Zásad skupin (Group Policy, GPO).

6.3 Rozdělení síťové infrastruktury do lokalit

Podle doporučení společnosti Microsoft by pro 20-2000 uživatelů měl být DC umístěn právě do objektu Lokality, v každé této lokalitě pak musí být minimálně jeden DC. Mezi DC lokalitami musí probíhat replikace v našem případě pomocí služby Knowledge Consistency Checker (KCC), tato je ponechána ve výchozím nastavení (replikace probíhá v 15min intervalech) a pro přihlédnutí k efektivitě a uvolnění síťových prostředků komprimovaně pro omezení datového toku.

6.3.1 Globální katalog

Funkce GC je vzhledem k jednodoménové struktuře aktivní na

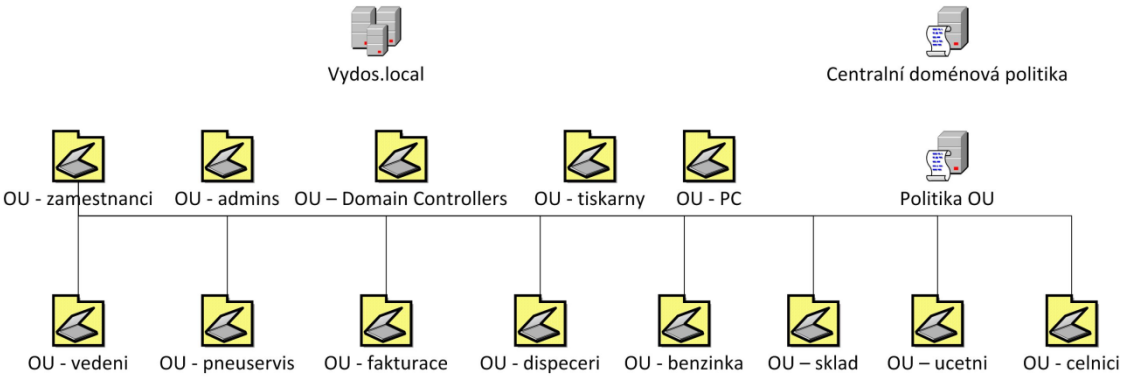
všech DC v doménovém prostoru firmy.

7 NÁVRH SKUPINOVÝCH POLITIK

7.1 Členění organizačních jednotek firmy

Pro základní rozložení Organizačních jednotek (OU) ve firmě se jevilo jako nejvhodnější centralizované řízení definované podle hlediska sdružování činností. Tento návrh zajišťuje autonomii nad objekty, transparentní řízení objektů, efektivní využití Zásad skupin a měl by odolat případné reorganizaci firmy.

.



Obrázek 9. Členění organizačních jednotek ve firmě

7.2 Strategie Skupin

Cílem návrhu Skupin je zjednodušení správy. Vzhledem k použití jediné domény **vydos.local**, není zapotřebí aplikovat univerzální skupinu, z tohoto důvodu byla použita strategie návrhu A G DL P (viz. Kapitola 3.1.14.3).

Názvy skupin musejí jasně říkat, za jakým účelem byly vytvořeny, a to i s ohledem pro konfiguraci v budoucnosti. Dále by pak měli názvy splňovat podobnou jmennou konvenci, jež by měla zajistit nesporné určení uživatelů do konkrétních skupin.

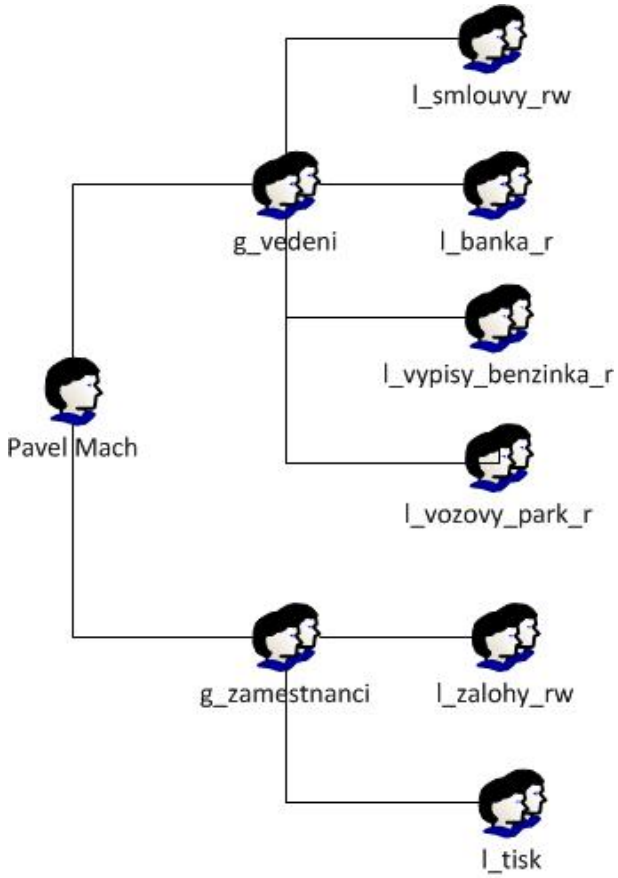
Jednotliví uživatelé s podobnými zájmy, či zařazením jsou seskupeni v globálních skupinách. Místní doménové skupiny jsou zase určené k udělování oprávnění přístupu k prostředkům, které se nacházejí ve stejné doméně.

Název globální skupiny	Popis
g_zamestnanci	skupina obsahující účty všech zaměstnanců
g_dispeceri	skupina obsahující účty dispečerů
g_vedeni	skupina obsahující účty vedení firmy
g_fakturace	skupina obsahující účty fakturace
g_ucetni	skupina obsahující účty účetních
g_admins	skupina obsahující účty správců
g_celnici	skupina obsahující účty zaměstnanců celní správy
g_skladnici	skupina obsahující účty skladníků
g_pneuservis	skupina obsahující účty skladníků
g_benzinka	skupina obsahující účty zaměstnanců benzínky

Tabulka 6. Přehled globálních skupin

Místní doménová skupina	Popis
l_smlouvy_rw	složka smlouvy – oprávnění pro čtení/zápis
l_smlouvy_r	složka smlouvy – oprávnění pro čtení
l_vozovy_park_rw	složka vozový park – oprávnění pro čtení/zápis
l_vozovy_park_r	složka vozový park – oprávnění pro čtení/zápis
l_banka_r	složka smlouvy – oprávnění pro čtení
l_banka_rw	složka výpisů z banky – oprávnění pro čtení
l_zalohy_rw	složka zálohy – oprávnění pro čtení/zápis
l_vypisy_benzinka_rw	složka výpisů z benzínky – oprávnění pro čtení/zápis
l_vypisy_benzinka_r	složka výpisů z benzínky – oprávnění pro čtení/zápis
l_tisk	oprávnění k přístupu k tiskárnám

Tabulka 7. Přehled místních doménových skupin



Obrázek 10. Příklad strategie skupin

Uživatel Pavel Mach je členem Globální skupiny g_vedeni, která mu umožňuje číst nebo psát do složky smlouvy, číst výpisy se složky vypisy_benzinka, banka a vozovy_park. Jako zaměstnanec má oprávnění číst a zapisovat do složky zálohy a může tisknout z firemních tiskáren.

7.3 Zásady skupin (Group Policy)

V této kapitole jsou definovány systémové politiky pro úroveň domény **vydos.local**

Zásady, jsou vymezené v rovině domény, ostatní OU podléhají vynucené dědičnosti těchto zásad. Vzhledem ke skutečnosti, že systém Windows Server 2003 R2 obsahuje obrovské

množství nastavení systémových politik nejen pro pracovní stanice, ale i uživatele, nelze je zde vyjmenovat všechny. Budou zde prezentovány pouze nejdůležitější nastavení, ostatní jsou vesměs ve výchozím nastavení. Drobné úpravy v zásadách pro další organizační jednotky, které jsou v hierarchické struktuře o stupeň níže budou rovněž vynechány.

7.3.1 Konfigurace počítače

Zásady hesla

Zásady	Nastavení zásady
Heslo musí splňovat požadavky na složitost	Povoleno
Maximální stáří hesla	120 dnů
Minimální délka hesla	7 znaků
Minimální stáří hesla	30 dnů
Ukládat hesla pomocí reverzibilního šifrování	Zakázáno
Vynutit použití historie hesel	5 hesel zapamatováno

Obrázek 11. Nastavení zásad hesel

Tato část slouží k nastavení zásad hesel doménových účtů. Jako kompromis mezi bezpečností a schopností uživatelů si zvolené heslo zapamatovat byla nastavena minimální délka hesla 7 znaků a použita restrikce na složitost daného hesla, které musí obsahovat malý, velký znak, číslici a jiný než alfanumerický znak. Pro nemožnost nastavit stejné heslo je posledních 5 použitých hesel zapamatováno. Platnost hesla je stanovena na 120 dní.

Zásady uzamčení účtů

Zásady	Nastavení zásady
Doba uzamčení účtu	30 minut
Prahová hodnota pro uzamčení účtu	5 chybných pokusů o přihlášení
Vynulovat čítač pro uzamčení účtu po	30 minutách

Obrázek 12. Nastavení zásad uzamčení účtů

Tyto zásady zlepšují míru zabezpečení, zadá-li uživatel 5x špatně heslo ke svému účtu, bude jeho účet na 30 minut zablokován.

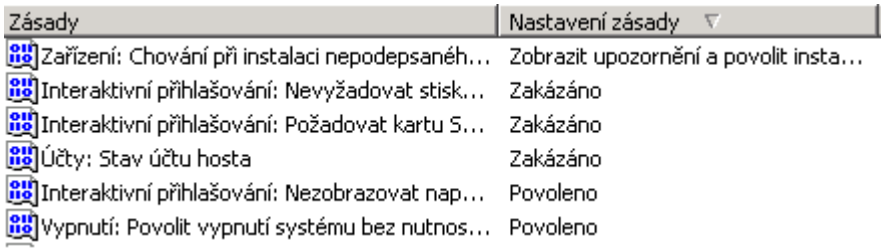
Zásady auditu

Zásady	Nastavení zásady
Auditovat správu účtů	Úspěšné pokusy, Neúspěšné pokusy
Auditovat systémové události	Úspěšné pokusy, Neúspěšné pokusy
Auditovat události přihlášení	Úspěšné pokusy, Neúspěšné pokusy
Auditovat změny zásad	Úspěšné pokusy, Neúspěšné pokusy

Obrázek 13. Nastavení zásad auditu

Ve výchozím stavu nejsou zásady auditu definovány, v rámci zvýšení zabezpečení se auditují změny zásad, jakákoliv změna na účtech uživatelů, či skupin a systémové události.

Možnosti zabezpečení

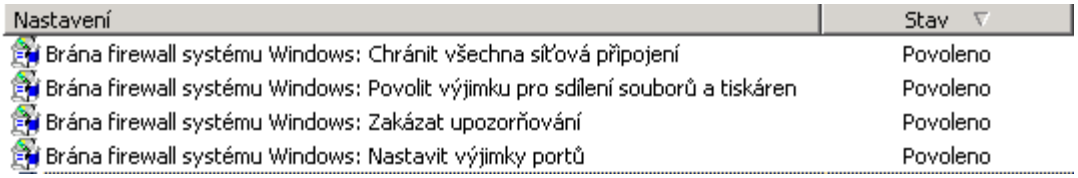


Zásady	Nastavení zásady
Zařízení: Chování při instalaci nepodepsaného...	Zobrazit upozornění a povolit insta...
Interaktivní přihlašování: Nevyžadovat stisk...	Zakázáno
Interaktivní přihlašování: Požadovat kartu S...	Zakázáno
Účty: Stav účtu hosta	Zakázáno
Interaktivní přihlašování: Nezobrazovat nap...	Povoleno
Vypnutí: Povolit vypnutí systému bez nutnos...	Povoleno

Obrázek 14. Nastavení zásad zabezpečení

V rámci bezpečnosti se nezobrazuje naposledy použité uživatelské jméno a jako opatření proti podvrhnutí přihlašovací nabídky je vyžadováno stisknutí kláves Ctrl+Alt+Del, nadále je vypnut účet hosta a použití karet čipových karet k přihlášení. Uživateli je umožněno vypnout počítač bez nutnosti se přihlásit.

Brána Windows Firewall

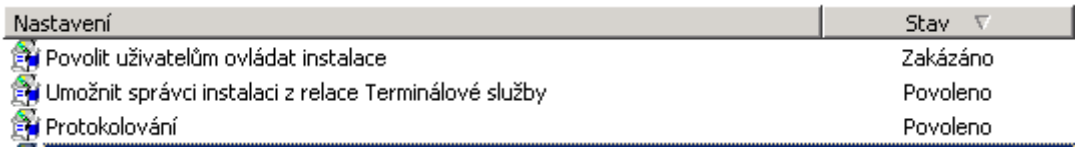


Nastavení	Stav
Brána firewall systému Windows: Chránit všechna síťová připojení	Povoleno
Brána firewall systému Windows: Povolit výjimku pro sdílení souborů a tiskáren	Povoleno
Brána firewall systému Windows: Zakázat upozorňování	Povoleno
Brána firewall systému Windows: Nastavit výjimky portů	Povoleno

Obrázek 15. Nastavení zásad brány Windows firewall

V nastavení zásad brány firewall jsou povoleny porty, které využívají firemní aplikace, nastavena ochrana všech síťových připojení a povolena výjimka pro sdílení tiskáren.

Instalační služba systému Windows



Nastavení	Stav
Povolit uživatelům ovládat instalace	Zakázáno
Umožnit správci instalaci z relace Terminálové služby	Povoleno
Protokolování	Povoleno

Obrázek 16. Nastavení zásad instalační služby systému Windows

Je zakázáno uživatelům ovládat instalace a je umožněno správcům instalovat programy z relace Terminálové služby, toto je ve výchozím nastavení umožněno pouze z místního přihlášení.

Windows update

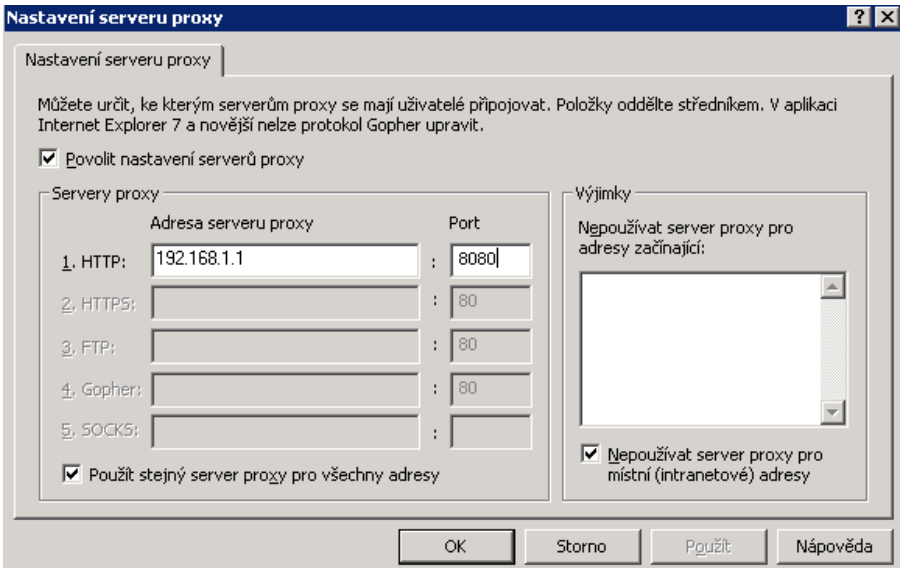
Nastavení	Stav
Opakovat dotaz na restartování pro naplánované instalace	Zakázáno
Konfigurace automatických aktualizací	Povoleno
Určení umístění intranetové služby Microsoft Update	Povoleno

Obrázek 17. Nastavení zásad Windows update

Pro využití služby WSUS je nutné nastavit zásady, ve kterých je nastaveno umístění této služby v lokální síti (http://vydsv001), dále byly nastaveny zásady pro určení času instalací na stanice a je vypnuto dotazování na restart.

7.3.2 Konfigurace uživatele

Internet Explorer



Obrázek 18. Nastavení proxy serveru pomocí zásad Internet Exploreru

V rámci centrální doménové politiky je nastavena pouze zásada nastavení proxy serveru, podrobnější nastavení už jsou v rámci jednotlivých OU.

Plocha

Nastavení	Stav
Odebrat příkaz Vlastnosti z místní nabídky Tento počítač	Povoleno
Zabránit uživatelům změnit cestu ke složce Dokumenty	Povoleno
Odebrat průvodce vyčištěním plochy	Povoleno

Obrázek 19. Nastavení zásad Plochy

V rámci zásad plochy je zakázán průvodce vyčištěním plochy a vzhledem k možnému narušení zálohování zabráněno změnit cestu ke složce Dokumenty.

Přidat nebo odebrat programy

Nastavení	Stav
Odebrat položku Přidat nebo odebrat programy	Povoleno
Skrýt stránku Přidat nebo odebrat součásti systému Windows	Povoleno
Skrýt možnost Přidat program z disku CD-ROM nebo z diskety	Povoleno
Skrýt možnost Přidat programy získané od společnosti Microsoft	Povoleno
Skrýt možnost Přidat programy získané ze sítě	Povoleno
Přejít přímo na Průvodce součástmi systému Windows	Povoleno

Obrázek 20. Nastavení zásad přidat nebo odebrat programy

Uživatelům je odebrána jakákoliv možnost přidat nebo odebrat programy, součásti systému (tato nastavení neplatí pro správce).

Instalační služba systému Windows

Nastavení	Stav
Zakázat všechny instalace z vyměnitelných médií	Povoleno

Obrázek 21. Nastavení zásad instalační služby systému Windows

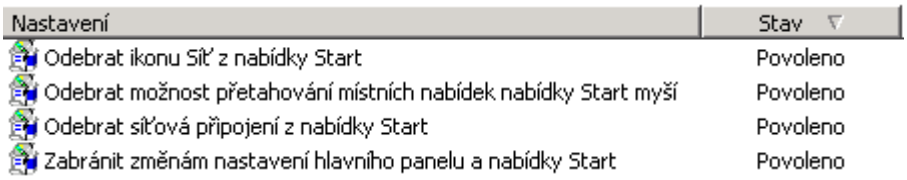
Průzkumník

Nastavení	Stav
Zakázat položku Okolní počítače ve složce Místa v síti	Povoleno
Zakázat ikonu Celá síť ve složce Místa v síti	Povoleno
Skrýt příkaz Spravovat v místní nabídce Průzkumníka Windows	Povoleno
Odebrat příkazy Připojit síťovou jednotku a Odpojit síťovou jedno...	Povoleno
Odebrat kartu Zabezpečení	Povoleno
Odebrat kartu Hardware	Povoleno
Odebrat funkci zápisu na disk CD	Povoleno

Obrázek 22. Nastavení zásad průzkumníka

V rámci průzkumníka jsou pro zvýšení bezpečnosti odebrány položky pro přístup k místní síti a správě počítače, je odebrána i možnost zápisu na disk CD.

Nabídka start a hlavní panel



Obrázek 23. Nastavení zásad nabídky start a hlavního panelu

Uživatelům jsou v rámci zachování jednotného firemního prostředí odebrány možnosti nastavení nabídky start a hlavního panelu a odebrány ikony sítě a síťových připojení

8 INSTALACE A KONFIGURACE SÍŤOVÝCH SLUŽEB WINDOWS SERVER 2003 R2

Cílem této části je definovat skupinu postupů a nastavení Windows Server 2003 R2 a klientských systémů Windows XP Professional, tak aby společně vytvářely celek, který bude nejen odpovídat současným standardům bezpečnosti, ale také poskytne dostatečné prostředky pro snadnou a efektivní administraci, která začínala být v bývalém prostředí pracovní skupiny časově neúnosná. Tato část práce tedy nabídne řadu postupů, které provedou instalací, konfigurací, zabezpečením jednotlivých služeb a klientských stanic. Bude zde popsána instalace a konfigurace služeb:

- Active Directory Domain Services včetně DNS Serveru
- Souborový server
- Terminálový server
- Server Windows Update Services (WSUS)
- Server DHCP

8.1 Active Directory Domain Services a DNS

8.1.1 Předpoklady pro instalaci

- V síťovém prostředí by měla být dostupná služba překladu jmen DNS. Tato je v našem případě instalována a konfigurována společně s Active Directory Domain services.
- Server, na němž bude provozován řadič domény, musí být připojen k síti a mít přiřazenou statickou síťovou IP adresu.
- Souborový systém na discích serveru musí být typu NTFS.

8.1.2 Instalace

Nejjednodušší způsob instalace Active Directory je pomocí grafického rozhraní. Tento způsob není automatizovaný, tudíž skoro všechny volby musí administrátor provádět ručně. Instalační průvodce lze spustit buď přes správce serveru, nebo přímo pomocí příkazu dcpromo.exe. Tento příkaz slouží jak k zavedení role řadiče domény, tak ke zrušení role řadiče domény. V této práci je popsán postup pomocí správce serveru:

1. Správce serveru – tlačítko Přidat nebo odebrat roli
2. Vybrat role serveru – řadič domény (služba Active Directory)
3. Typ řadiče domény – Řadič domény pro novou doménu (v případě serveru vydsv002 zde bude zvoleno Další řadič pro již existující doménu)
4. Doména v nové doménové struktuře
5. Úplný název DNS – vydos.local
6. Název domény pro rozhraní NETBIOS – VYDOS
7. Umístění databáze a souboru protokolu – D:\NTDS
8. Umístění složky SYSVOL – D:\SYSVOL (nelze změnit)
9. Instalátor rozpozná chybějící službu DNS a nabídne její instalaci a konfiguraci
10. Oprávnění domény – kompatibilní pouze s operačními systémy Windows server 2000 nebo Windows server 2003
11. Heslo správce režimu obnovení adresářových služeb

    Poznámka: Tento účet administrátora je odlišný od účtu doménového administrátora a je dostupný jen tehdy, když spustíme doménový řadič v režimu obnovení adresářových služeb. V takovém případě lze na doménovém řadiči požít lokální a nikoliv doménový uživatelský účet.

12. Instalátor nabídne změnu DNS serveru v konfiguraci protokolu TCP/IP a doporučí jeho nastavení na adresu serveru – 192.168.1.10
13. Restart

8.1.3 Konfigurace

V případě konfigurace AD DS a jejích objektů nelze vytvořit ucelený návod pro každý jednotlivý objekt (mnohonásobně by to přesáhlo rozsah této práce), jednotlivé postupy tedy byly popsány obecně, nebo použit konkrétní příklad.

DNS

Pokud je DNS instalováno zároveň se službou AD DS, není do její konfigurace třeba radikálně zasahovat, většina bezpečnostních nastavení je už přednastavena a zóna dopředného vyhledávání vytvořena. Jediné úpravy jsou:

- povolené jen zabezpečené dynamické aktualizace
- DNS Server je nastaven tak, aby se ve své IP konfiguraci odkazoval sám na sebe.

- Servery pro předávání byly nastaveny na servery poskytovatele připojení k Internetu

Zabezpečení:

Pro použití DNSSec je nutná úprava registrů, do klíče:

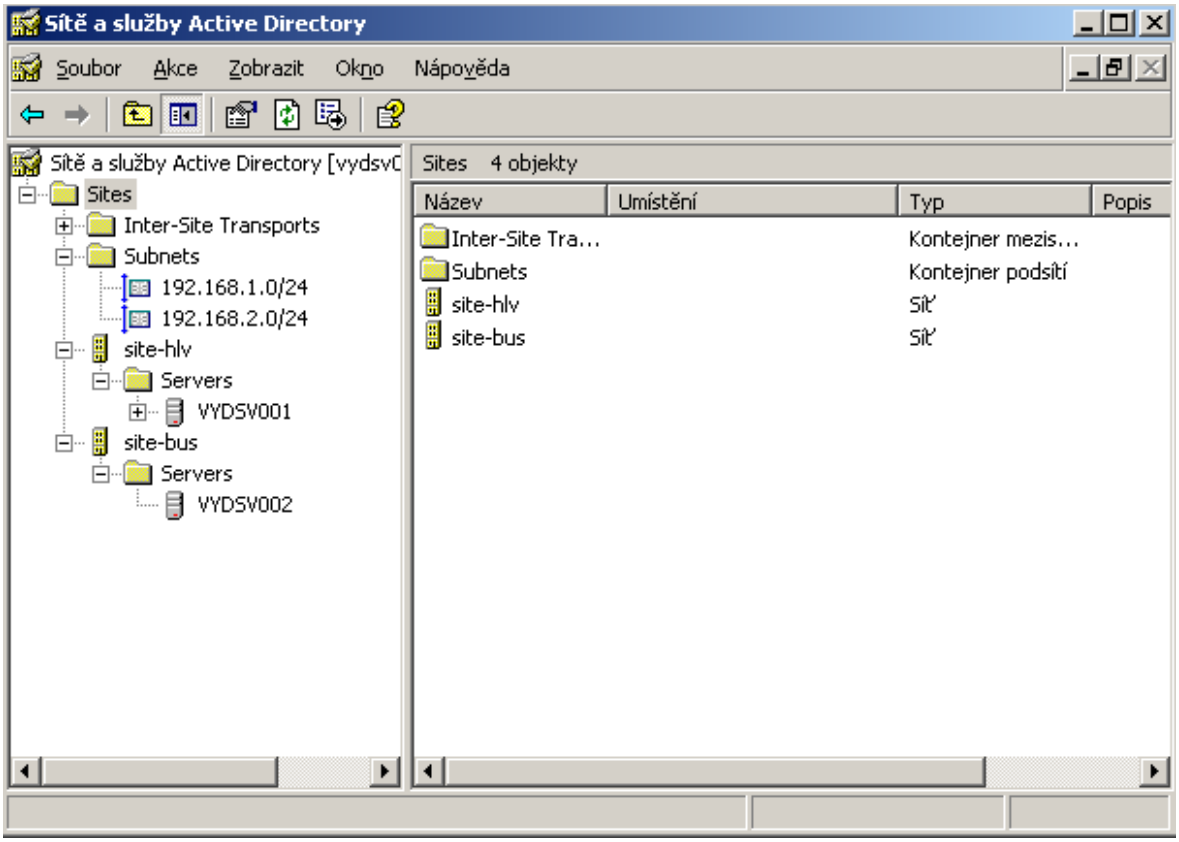
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters

Je přidána následující položky typu DWORD: EnableDnsSec

Lokality (Site)

V tomto modulu byly nakonfigurovány:

- jednotlivé lokality
- umístění DC v lokalitách
- subnety
- replikace mezi lokalitami.



Obrázek 24. Modul MMC konzole Sítě a služby Active Directory

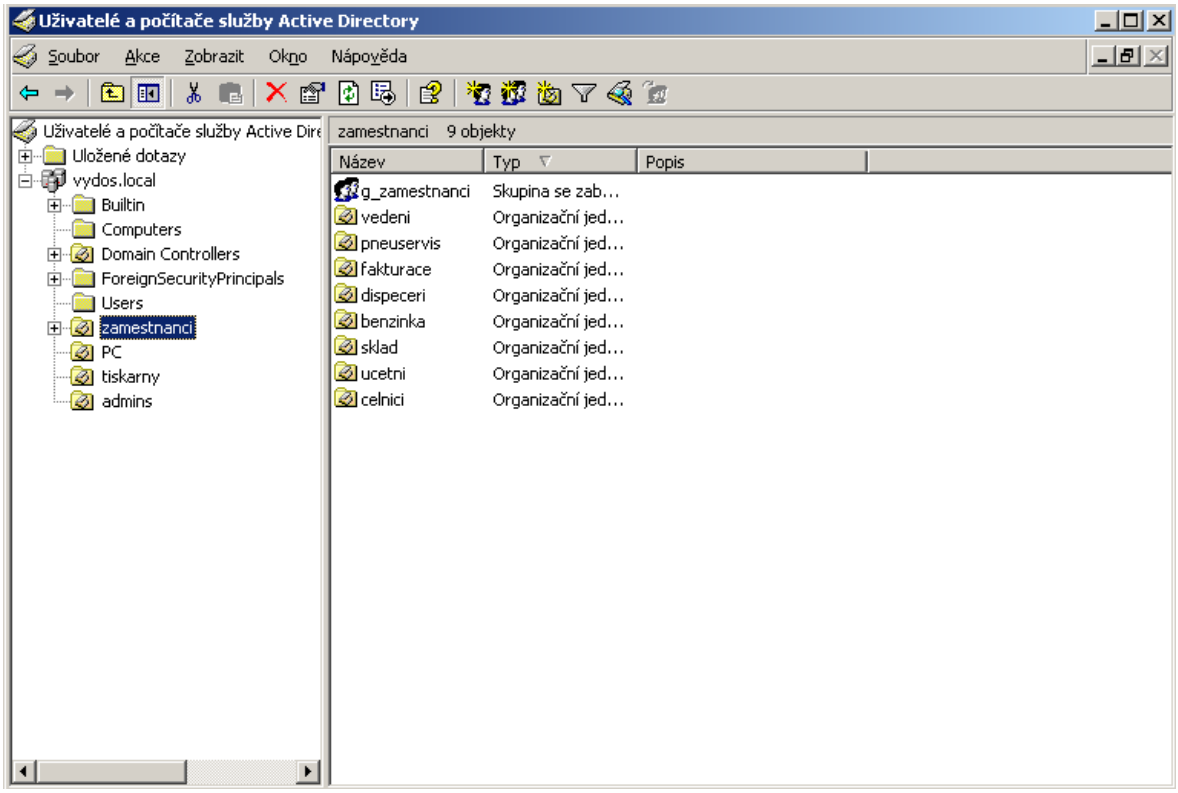
Uživatelé a počítače služby Active Directory

1. Správce serveru – tlačítko Spravovat uživatele a počítače Active Directory
   Zde se tvoří jednotliví objekty adresářové služby:
   Vytvoření organizačních jednotek
   1. Levý panel – pravé tlačítko myši na doménu – Nová položka – organizační jednotka – Název

   Vytvoření uživatelských účtů
   1. V levém panelu v struktuře domény byla označena organizační jednotka users – pravé tlačítko – nový objekt – Uživatel
   2. V dialogovém okně Nový objekt-Uživatel bylo vyplněno přihlašovací uživatelské jméno a Jméno

   Vytvoření globálních skupin
   1. V levém panelu v struktuře domény byla označena organizační jednotka zamestnanci – jednotka zamestnanci – pravé tlačítko – nový objekt – Skupina
   2. V dialogovém okně Nový objekt-Skupina byl vyplněn název podle konvence g_název a nastavena jako globální se zabezpečením
   3. Přidání uživatelů – karta členové – přidat

   Vytvoření místních doménových skupin
   1. V levém panelu v struktuře domény byla označena organizační jednotka zamestnanci – jednotka zamestnanci – pravé tlačítko – nový objekt – Skupina
   2. V dialogovém okně Nový objekt-Skupina byl vyplněn název podle konvence l_složka_prava a nastavena jako místní doménová se zabezpečením
   3. Přidání globálních skupin – karta členové – přidat

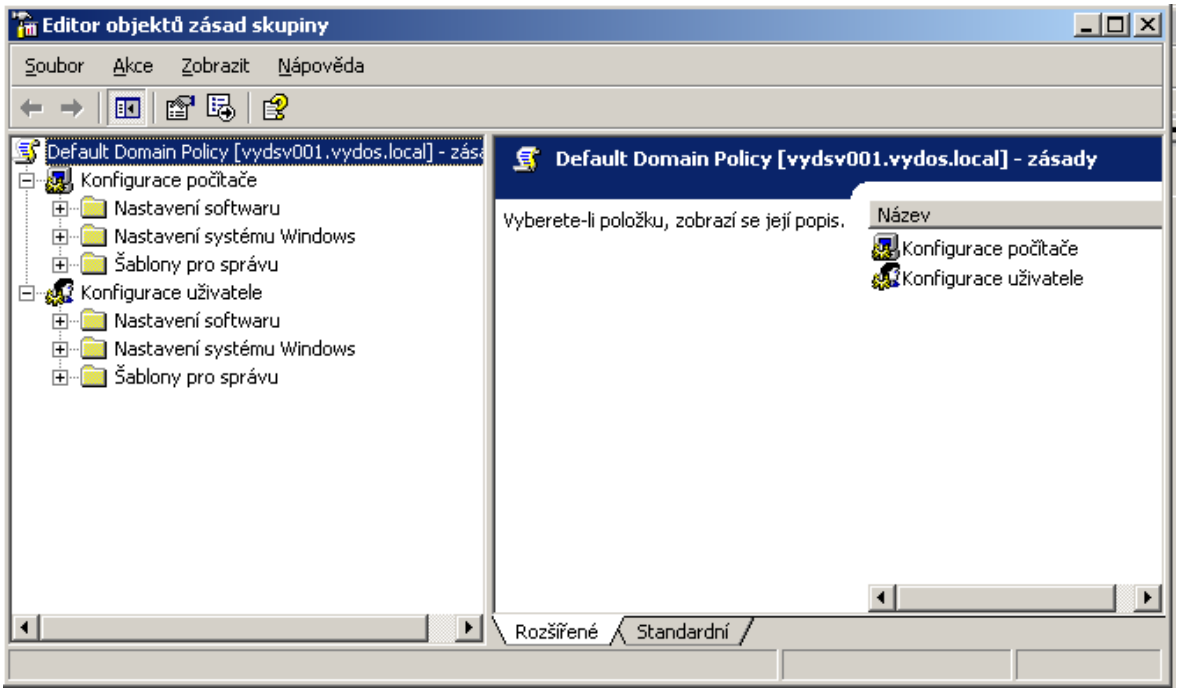


Obrázek 25. Modul MMC konzole Uživatelé a počítače služby Active Directory

Zásady skupiny

Příklad nastavení zásad hesla na úrovni domény:

1. Start - Nástroje pro správu - Správa zásad skupiny
2. Objekt zásad skupiny – pravé tlačítko myši – Default Domain Policy - Upravit
3. V Editoru správy zásad skupiny – Konfigurace počítače – Nastavení systému Windows – Nastavení zabezpečení – Zásady účtů – Zásady hesla



Obrázek 26. Modul MMC konzole Editor objektů zásad skupiny

Přidání klientské stanice do domény

1. Start – Tento počítač – Vlastnosti – Název počítače – změnit – vydos.local

8.2 Souborový server

8.2.1 Instalace

1. Správce serveru – tlačítko Přidat nebo odebrat roli
2. Vybrat role serveru – souborový server
3. Nastavení diskové kvóty souborového serveru
4. Zapnout službu indexování

8.2.2 Konfigurace

1. Správce serveru – tlačítko Průvodce sdílením složky
2. Cesta ke složce – D:\Sdilene\smlouvy
3. Název sdílené položky – smlouvy
4. Oprávnění – vlastní –> přiřadit místní doménové skupině l_smlouvy_rw a nastavit práva číst a změnit.

Toto je jen ukázka vytvoření složky smlouvy a přiřazení práv ke čtení a zápisu místní doménové skupině l_smlouvy_rw, obdobně se postupuje při nastavení ostatních sdílených složek.

8.2.3 Zálohování

1. Správce serveru – tlačítko správa Souborového serveru – server pro zálohování souborů – zálohovat soubory a nastavení – všechny informace v tomto počítači (zazálohuje i stav systému tj. registry, bootovací soubory, službu Active Directory, složku SYSVOL atd.) – umístění vydsv002.domov.local

8.3 Terminálový server

8.3.1 Instalace

1. Správce serveru – tlačítko Přidat nebo odebrat roli
2. Vybrat role serveru – Terminálový server

8.3.2 Konfigurace

Nejprve je nutno přidat licenční server, který není ve výchozí instalaci serveru nainstalován a terminálový server by po lhůtě 120 dní přestal fungovat.

1. Start – Ovládací panely – Přidat nebo odebrat programy – Přidat nebo odebrat součásti systému – správa licencí Terminálového serveru
    1. Zpřístupnit licenční server – pro tuto doménu
    2. Umístění databáze licenčního serveru – D:\TERMIS

1. Licenční server je nutné aktivovat
   Start – nástroje pro správu – správa licencí Terminálového serveru – aktivovat
2. Spustí se průvodce aktivací:
    1. Metoda aktivace – automatické připojení
    2. Vyplnění informací o společnosti
        1. Průvodce klientskými licencemi – Licenční program – Open licence
        2. zadat číslo smlouvy

3. vybrat verzi produktu – Windows server 2003
4. Typ produktu – klientská licence Terminálového serveru vázaná na zařízení
5. Množství – 15

8.3.3 Zabezpečení

Ve výchozím nastavení používá terminálový server a pro připojení klientů port TCP 3389. Společnost Microsoft nedoporučuje tuto hodnotu měnit, avšak pro zvýšení bezpečnosti bylo rozhodnuto toto nastavení změnit na hodnotu 5159.

Toto nastavení se provádí změnou podklíče PortNumber v registru HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp

8.4 Server Windows Update Services (WSUS)

Tato služba není standardně obsažena v systému, instaluje se pomocí samostatného balíčku, který je nejprve nutno stáhnout ze stránek Microsoftu.

8.4.1 Předpoklady pro instalaci

Pro instalaci služby WSUS je nutné mít nainstalovány následující role a doplňky:

- Internetová informační služba
- Rozhraní .NET Framefork 2.0
- Služba inteligentního přenosu na pozadí (BITS) 2.0

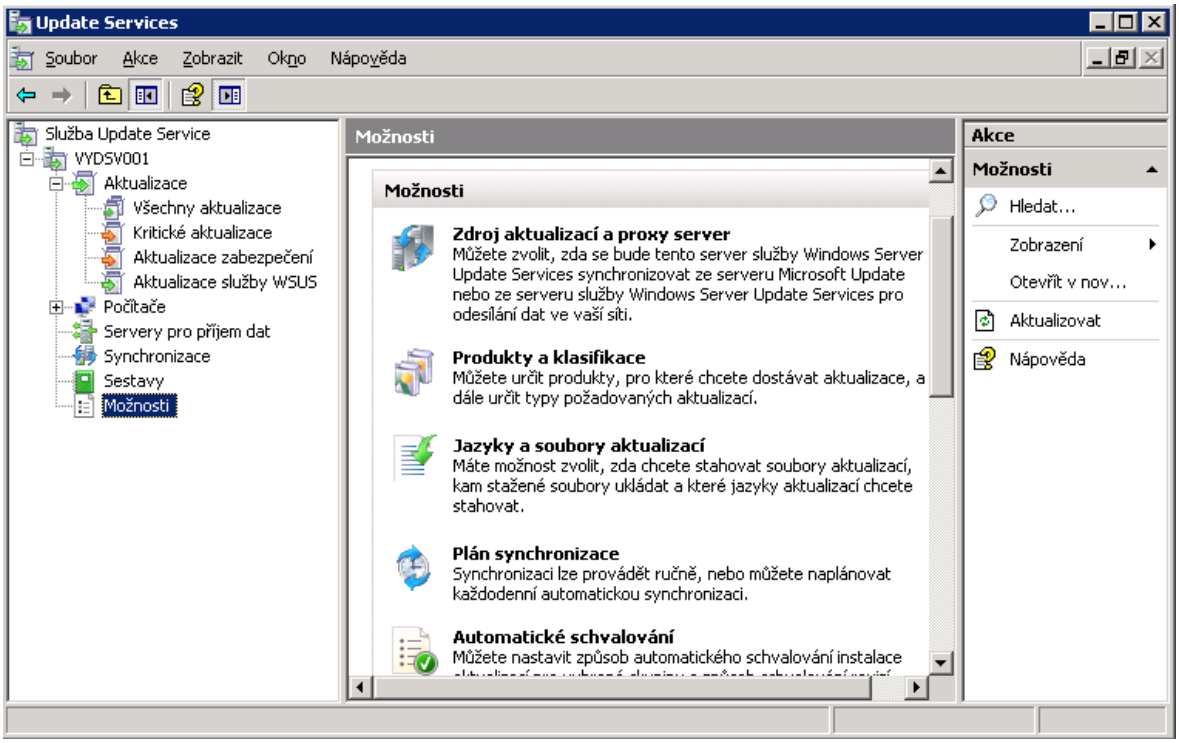
8.4.2 Instalace

1. Spuštění staženého instalátoru
2. Výběr režimu instalace – úplná instalace na serveru včetně konzole pro správu
3. Výběr zdroje aktualizace – ukládat aktualizace místně D:\WSUS
4. Možnosti databáze – použít existující databázový server v počítači
5. Výběr webového serveru – použít aktuální výchozí webový server
6. Zrcadlení nastavení aktualizací – bude použit jediný server v síti nastavení vynecháno

8.4.3 Konfigurace

1. Uložení a stažení informací o serveru pro odesílání dat a proxy serveru – Microsoft Update, proxy server – 192.168.1.1 port: 8080
2. Výběr jazyků aktualizací - čeština
3. Výběr produktů aktualizací – Office 2003-2010, Windows XP Professional, Windows 7 Professional, Windows Server 2003 standard
4. Výběr klasifikací aktualizací - všechny
5. Konfigurace plánu synchronizace – automaticky

Pro nastavení klientských stanic byl vytvořen objekt zásad skupiny viz. kapitola 7.3.1.7



Obrázek 27. Modul MMC konzole Update Services

8.5 Server DHCP

8.5.1 Instalace

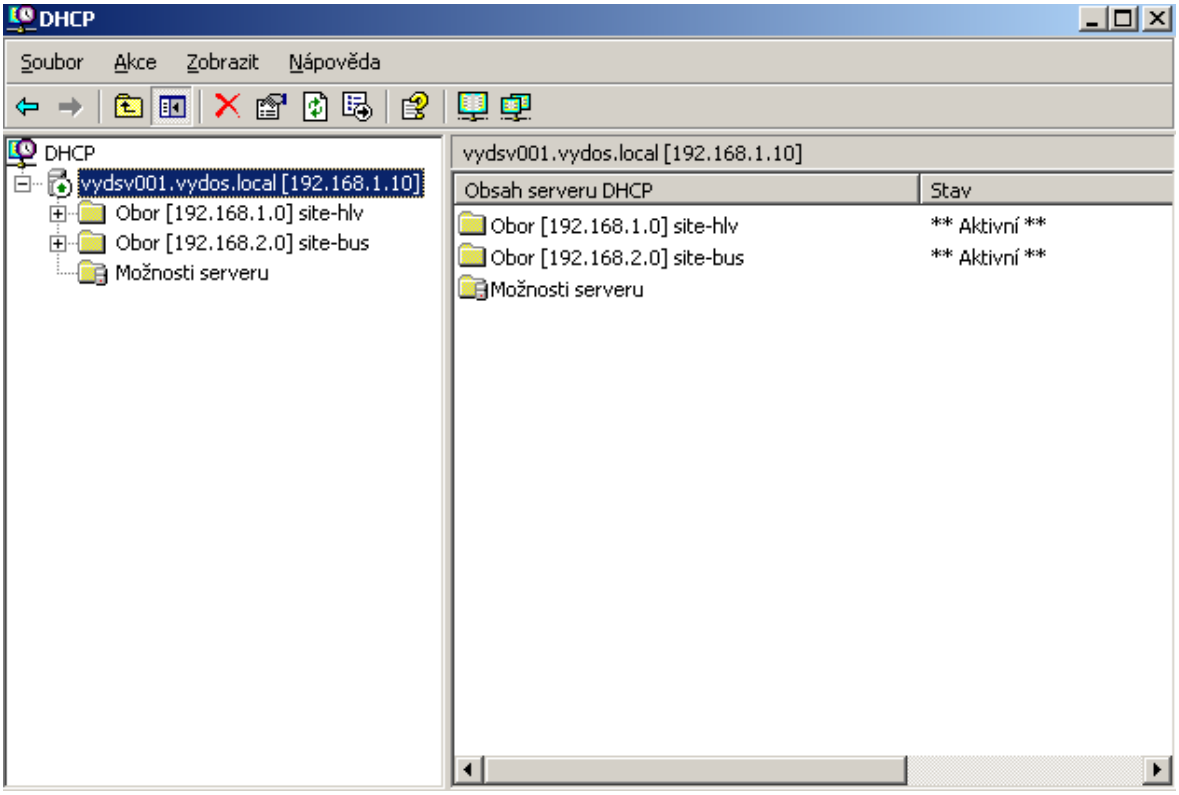
1. Správce serveru – tlačítko Přidat nebo odebrat roli
2. Vybrat role serveru – server DHCP
3. Průvodce vytvořením oboru
    1. Název oboru – site_hlv
    2. Rozsah distribuovaných adres – 192.168.1.11 – 192.168.1.100

3. Rozsah vyloučených adres – není definováno
4. Doba trvání zápůjčky – 7 dní
5. Konfigurace možností DHCP
    1. Adresa směrovače: 192.168.1.1
    2. Název domény a servery DNS
        1. Nadřazená doména – vydos.local
        2. Název DNS serveru – vydsv001, vydsv002
        3. IP adresa – 192.168.1.10, 192.168.2.10

8.5.2 Konfigurace

1. Správce serveru – tlačítko spravovat server DHCP
2. Akce – nový obor
3. Průvodce vytvořením oboru
    1. Název oboru – site_bus
    2. Rozsah distribuovaných adres – 192.168.2.11 – 192.168.2.100
    3. Rozsah vyloučených adres – není definováno
    4. Doba trvání zápůjčky – 7 dní
    5. Konfigurace možností DHCP
        1. Adresa směrovače: 192.168.2.1
        2. Název domény a servery DNS
            1. Nadřazená doména – vydos.local
            2. Název DNS serveru – vydsv001, vydsv002
            3. IP adresa – 192.168.1.10, 192.168.2.10

Na závěr je nutné ověření službou AD DS – Akce – ověřit



Obrázek 28. Modul MMC konzole DHCP

8.5.3 Zálohování

1. Správce serveru – tlačítko spravovat server DHCP
2. Akce – Zálohování
3. Výběr adresáře pro zálohu – D:\DHCP\backup

8.5.4 Zabezpečení

Jak už bylo popsáno v teoretické části DHCP není ověřovaný protokol. A neumožňuje ve výchozím nastavení žádnou ochranu, proto je nutné další funkcionalitu doinstalovat. V tomto případě je to možnost použití white a black listu na MAC adresy počítačů.

Instalace bezpečnostního doplňku

1. Tvorba adresáře D:\DHCP a do něj byla umístěna knihovna MacFilterCallout.dll a vytvořen soubor MACList.txt
2. V registru HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\DHCPServer\Parameters byly vytvořeny následující klíče:

CalloutErrorLogFile	REG_MULTI_SZ	D:\DHCP\LOGS\MacFilterLogError.txt
CalloutInfoLogFile	REG_MULTI_SZ	D:\DHCP\LOGS\MacFilterLogInfo.txt
CalloutMACAddressListFile	REG_MULTI_SZ	D:\DHCP\MacFilterList.txt
CalloutDlls	REG_MULTI_SZ	D:\DHCP\MacFilterCallout.dll
CalloutEnabled	DWORD	1

Tabulka 8. Přehled vytvořených záznamů v registru pro úpravu zabezpečení služby DHCP

Konfigurační soubor MACList.txt je v tomto tvaru:

#MACList.txt

MAC_ACTION = {ALLOW / DENY}

#List of MAC Addresses:

000a0c0d1254 #stanice1

000d0c4a6723 #stanice2

Poznámka: Po jakékoliv editaci v souboru MACList.txt je třeba restartovat službu DHCP

ZÁVĚR

Cílem této práce bylo implementovat Microsoft Windows Server 2003 R2 Standard Edition Active Directory Domain Services do prostředí firmy Vydos servis a.s. a tím umožnit administrátorům nastavovat politiku, instalovat programy na mnoho počítačů nebo aplikovat kritické aktualizace v celé organizační struktuře. Avšak ve chvíli kdy jsou počítače součástí domény, bývají spravovány přes síťové rozhraní prostřednictvím serveru. Je tedy velice důležité server co možná nejlépe zabezpečit a minimalizovat tak možné hrozby jak ze strany vnější, ale i vnitřní sítě. V práci jsem se proto věnoval popisu obecných a fyzických rizik a hlavně rizik specifických pro serverový operační systém a jeho nejčastěji používané služby. Dále se má práce zabývala obecným popisem operačního systému Microsoft Windows Server 2003 R2 a jeho síťových služeb.

Samotné implementaci předcházel návrh AD DS, skupinových politik a analýza původního stavu veškeré IT infrastruktury firmy. Ve finále byly instalovány a konfigurovány služby AD DS, DNS, Souborový server, Terminálový server, Windows Server Update Services a server DHCP s ohledem na předchozí analýzu bezpečnostních hrozeb a organizačního členění firmy.

Firma tímto získá bezpečnější, flexibilní a škálovatelné prostředí s centralizovanou správou a sníží náklady zkrácením času, který by byl potřeba k nakonfigurování nastavení na každou stanici zvlášť.

ZÁVĚR V ANGLIČTINĚ

The point of this bachelor work was the implementation of Microsoft Windows Server 2003 R2 Standard Edition Active Directory Domain Services in the environment of Vydos servis a.s. company, thereby allowing administrators to set policies, installing programs on many computers and apply critical updates throughout the organizational structure. But at the moment when the computers are part of the domain, they are managed through a network interface through the server. It is very important to secure the server to provide the best possible way to minimize potential threats from both external and internal network. In my work I therefore gave a description of general and physical hazards and major risks specific to the server operating system and most frequently used network services. Further work has dealt with a general description of Microsoft Windows Server 2003 R2 and its network services.

The actual implementation preceded by a proposal AD DS and Group Policy analysis of the original status of all IT infrastructure company. In the finals have been installed and configured the AD DS, DNS, File Server, Terminal Server, Windows Server Update Services and DHCP server with respect to previous analysis of security threats and the organizational structure of the company.

The company that gets more secure, flexible and scalable environment with centralized management and reduce costs by shortening the time that would be needed to configure the settings on each station.

SEZNAM POUŽITÉ LITERATURY

[1] RUSSEL, Charlie, CRAWFORD, Sharon, GEREND, Jason. Microsoft Windows Server 2003 : Velký průvodce administrátora. Brno : C.P. Books, a.s., 2005. 1374 s. ISBN 80-251-0579-2

[2] STANEK, William R. Microsoft Windows Server 2003 : kapesní rádce administrátora. 2., aktualiz. vyd. Brno : Computer Press, 2007. 575 s. ISBN 978-80-251-1654-8.

[3] BOTT, Ed, SIECHERT, Carl. Mistrovství v zabezpečení Microsoft Windows 2000 a XP. Brno: Computer Press, 2004. 696 s. ISBN 80-7226-878-3.

[4] HATCH, Brian; LEE, James; KURTZ, George. *Linux Hackerské Útoky: Bezpečnost Linuxu - tajemství a řešení*. Praha : SoftPress, 2002. 576 s. ISBN 80-86497-17-8.

[5] SMITH, Ben, KOMAR, Brian. Zabezpečení systému a sítě: Microsoft Windows. Brno: Computer Press, a.s., 2006. 700 s. ISBN 80-251-1260-8.

[6] PRICE, Brad. Active Directory : optimální postupy a řešení problémů. Vyd. 1. Brno : CP Books, 2005. 381 s. ISBN 80-251-0602-0.

[7] Microsoft.com/cs/cz/ [online]. 2012 [cit. 2012-05-13]. Microsoft. Dostupné z WWW: <http://www.microsoft.com/cs/cz/>.

[8] Jak funguje DNSSEC [online]. 2012 [cit. 2012-05-13]. nic.cz Dostupné z WWW: <http://www.nic.cz/page/444/jak-funguje-dnssec>.

[9] ŠETKA, Petr. Mistrovství v MS Windows server 2003. 1. vyd. Brno : Computer Press, 2008. 680 s. ISBN 80-251-0036-7.

[10] Active Directory komponenty [online]. 2012 [cit. 2012-05-13]. Petr Bouška. Dostupné z <http://www.samuraj-cz.com/clanek/active-directory-komponenty-domain-tree-forest-site/>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AD	Active Directory
AD DS	Active Directory Domain Services.
CAL	Client Access License
DC	Domain Controller
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DNSsec	Domain Name System Security Extensions
GC	Global Catalog
GPO	Group Policy
GUID	Globally Unique Identifier
HP	Hewlett-Packard
HW	Hardware
IBM	International Business Machines Corporation
IP	Internet Protocol
IT	Information Technology
KCC	Knowledge Consistency Checker
LDAP	Lightweight Directory Access Protocol
MMC	Microsoft Management Console
OU	Organizational Unit
PC	Personal Computer
RAM	Random-Access Memory
SW	Software
VLAN	Virtual Local Area Network
WSUS	Windows Server Update Services

SEZNAM OBRÁZKŮ

SEZNAM TABULEK