

Windows deployment

Windows deployment

Tomáš Mošovský

Bakalářská práce
2010



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2009/2010

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Tomáš MOŠOVSKÝ**
Osobní číslo: **A07258**
Studijní program: **B 3902 Inženýrská informatika**
Studijní obor: **Informační a řídicí technologie**

Téma práce: **Windows deployment**

Zásady pro vypracování:

1. Popište přechod typizovaných PC se starším operačním systémem Microsoft Windows na systém Microsoft Windows 7.
2. Lokální stanice nastavte pomocí Group Policy z doménové sítě s Active Directory.
3. Využijte následující technologie firmy Microsoft:
 - Windows Automated Installation Kit (Windows AIK).
 - Windows Setup a formát WIM,VHD.
 - Sysprep.
 - SIM (System Image Manager / Správce bitových kopií disků)
 - Odpovědní soubor
 - Group Policy

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. WILLIAM, R. Staněk. **Mistrovství v Microsoft Windows Server 2008 : Kompletní informační zdroj pro profesionály**. 1. vyd. [s.l.] : Computer Press, a.s., 2009. 1364 s. ISBN 978-80-251-2158-0.
2. CHARLIE, Russel, SHARON, Crawford. **Microsoft Windows Server 2008 : Velký průvodce administrátora**. 1. vyd. [s.l.] : Computer Press, a.s., 2009. 1271 s. ISBN 978-80-251-2115-3.
3. CHARLIE, Russel, SHARON, Crawford, JASON, Gerend. **Microsoft Windows Server 2003 : Velký průvodce administrátora**. 1. vyd. [s.l.] : CP Books, a.s., 2005. 1374 s. ISBN 80-251-0579-2.
4. [Http://technet.microsoft.com](http://technet.microsoft.com) [online]. Microsoft Corporation, c2010 , 2010 [cit. 2010-02-02]. Dostupný z WWW: <http://http://technet.microsoft.com>.
5. [Http://www.mstv.cz/](http://www.mstv.cz/) [online]. Microsoft, s.r.o., c2008 [cit. 2010-02-01]. Dostupný z WWW: <http://www.mstv.cz/>.

Vedoucí bakalářské práce:

doc. Ing. Martin Sysel, Ph.D.

Ústav počítačových a komunikačních systémů

Datum zadání bakalářské práce:

5. března 2010

Termín odevzdání bakalářské práce:

1. června 2010

Ve Zlíně dne 5. března 2010



prof. Ing. Vladimír Vašek, CSc.
děkan



doc. Ing. Ivan Zelinka, Ph.D.
ředitel ústavu

ABSTRAKT

Téma bakalářské práce Windows Deployment, volně v češtině přeložitelné jako Nasazení Windows, bude vycházet z reálného požadavku uskutečnění přechodu typizovaných počítačů se starším operačním systémem na nový operační systém Microsoft Windows 7. Cílem je pokusit se tento přechod co nejvíce optimalizovat a využít možností dané existujícími prostředky v síti LAN (Group Policy z Active Directory) a dále prozkoumat a zvolit účinný nástroj pro nasazení za využití technologie z Microsoft Windows Automated Installation Kit for Windows 7.

Klíčová slova:

Microsoft Windows 7, Group Policy, Active Directory, Windows Automated Installation Kit, Windows Setup a formát WIM,VHD, Sysprep, System Image Manager, Odpovědní soubor

ABSTRACT

Topic of the thesis Windows Deployment, loosely translatable to Czech as "Nasazení Windows", will be based on the real requirement of making the transition of typified computers with older operating systems to the new operating system Microsoft Windows 7. The aim is as great optimization of this transition as possible and the use of the possibilities given by the existing resources on the LAN (Group Policy from Active Directory) and further to explore and to select an effective tool for setting by using technologies from Microsoft Windows Automated Installation Kit for Windows 7.

Keywords:

Microsoft Windows 7, Group Policy, Active Directory, Windows Automated Installation Kit, Windows Setup and format WIM,VHD, Sysprep, System Image Manager, Response file

Poděkování

Rád bych poděkoval panu Doc. Ing. Martinu Syslovi, Ph.D. za možnost pracovat na tématu této bakalářské práce a za cenné konzultace a rady, které mi poskytl.

Motto

„I když inovace serverů a klientů může pro správce představovat významnou výzvu, je také příležitostí, jak vylepšit fungování sítí.“ [3].

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	10
I TEORETICKÁ ČÁST	12
1 INFRASTRUKTURA SÍŤOVÉHO PROSTŘEDÍ	13
1.1 FINET WAN	13
1.2 LAN FÚ	14
2 MICROSOT WINDOWS 2003 SERVER.....	16
2.1 HW SERVERŮ.....	16
2.2 SW RODINA PRODUKTŮ	16
2.3 SEZNÁMENÍ S MS WINDOWS SERVER 2003.....	16
2.4 NATIVNÍ SOUHRA	17
2.5 ACTIVE DIRECTORY	17
2.5.1 Globální katalog.....	18
2.6 MMC	18
2.7 GROUP POLICY.....	18
2.7.1 Group Policy Object.....	18
2.7.1.1 Group policy template.....	18
2.7.1.2 Group policy container.....	19
2.7.2 Součástí zásad skupiny.....	19
2.7.3 Správa zásad skupiny	19
2.7.4 Pořadí implementace	19
2.7.5 Tvorba objektu zásad skupiny	20
2.7.5.1 Výchozí zásady	20
2.7.5.2 Tvorba vlastních zásad GPO	20
2.7.5.3 Editor zásad skupiny	22
2.7.6 Aktualizace zásad skupiny.....	22
2.7.6.1 Vynucení požadavku zásad skupiny.....	22
2.7.6.2 Vynucení požadavku zásady „update systému“	23
2.7.7 Průvodce výslednou sadou zásad skupiny	23
2.8 INSTALACE A SPRÁVA VZDÁLENÉHO SOFTWARE POD WINDOWS SERVER 2003	23
2.8.1 Publikování aplikací	23
2.8.2 Přiřazení aplikací.....	24
2.8.3 Formát instalačního balíčku	24
2.8.3.1 .MSI balíčky	24
2.8.3.2 .ZAP balíčky	25
2.8.3.3 Nástroje pro opětovné vytvoření balíčků instalací a repackage.....	25
2.8.4 Distribuční místo software.....	25
2.8.5 Vytvoření balíčku instalace softwaru a nastavení možností	26

2.9	SPRÁVA BITOVÝCH KOPIÍ SERVERU RIS S WINDOWS SERVER 2003	27
2.10	SPRÁVA BITOVÝCH KOPIÍ SERVERU WDS S WINDOWS SERVER 2008.....	27
2.11	SERVEROVÁ SLUŽBA DHCP	27
2.12	ALTERNATIVNÍ ŘEŠENÍ I. – VIRTUÁLNÍ POČÍTAČ V SOUBORU .VHD.....	28
2.12.1	VHD soubor	29
2.13	ALTERNATIVNÍ ŘEŠENÍ II. – MINIROUTER SE SÍŤOVÝMI SLUŽBAMI	29
3	WINDOWS AUTOMATED INSTALLATION KIT WINDOWS 7	31
II	PRAKTICKÁ ČÁST.....	32
1	STRATEGIE - REFERENČNÍ PC PRO „KLONOVÁNÍ“.....	33
2	SCÉNÁŘE PRÁCE S WINDOWS AIK.....	34
2.1	FILOZOFIE PRÁCE S WAIK.....	34
2.2	WIM SOUBORY	34
2.2.1	Struktura souboru WIM.....	34
2.3	NĚKOLIK UŽITEČNÝCH POSTŘEHŮ K NÁPOVĚDĚ NÁSTROJŮ WAIK.....	35
2.4	PŘÍPRAVA PRO PRÁCI S WAIK.....	35
2.5	INSTALACE WAIK NA PC TECHNIKA.....	36
2.6	VYTVOŘENÍ SOUBORU ODPOVĚDÍ V NÁSTROJI SIM	37
2.6.1	Vytvoření souboru odpovědí.....	38
2.6.2	Přidání a nastavení konfigurace Windows.....	39
2.6.3	Ověření a uložení nastavení	42
2.7	VYTVOŘENÍ REFERENČNÍ INSTALACE - SYSPREP.....	42
2.8	VYTVOŘENÍ SPUSTITELNÉHO CD S PROSTŘEDÍM WINDOWSPE + IMAGEX.....	43
2.8.1	Vytvoření struktury CD	43
2.8.1.1	Chyba Windows Setup	44
2.8.2	Vytvoření bootovacího CD WindowsPE z .ISO obrazu	44
2.9	ZACHYCENÍ REFERENČNÍ INSTALACE DO BITOVÉ KOPIE A JEJÍ SDÍLENÍ V SÍTI	45
2.9.1	Zachycení bitové kopie referenčního počítače.....	45
2.9.2	Zkopírování bitové kopie do síťového umístění	45
2.9.2.1	Nastavení kontextu sítě referenčního PC bez služby DHCP	46
2.10	NASAZENÍ BITOVÉ KOPIE DO NOVÉHO PC	46
2.11	SCÉNÁŘ ZE SÍŤE.....	47
3	PERSONIFIKACE PC VYTVOŘENÉHO Z BITOVÉ KOPIE	49
4	SHRnutí NASAZENÍ WINDOWS.....	51
	ZÁVĚR	52
	CONCLUSION.....	53
	SEZNAM POUŽITÉ LITERATURY.....	54
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK.....	56
	SEZNAM OBRÁZKŮ.....	60

SEZNAM TABULEK 61

ÚVOD

Výpočetní technika se v průběhu posledních 15 let velmi změnila. Rychleji dosahuje změn a pokroku, a to ruku v ruce se vzrůstajícím hardwarovým (dále i jen HW- hardware) výkonem osobních počítačů (PC – Personal Computer) a softwarovými (SW – software) možnostmi moderních sofistikovaných operačních systémů, které nabízejí živnou platformu pro veliké množství aplikací a software utilit, bez kterých bychom si již dnešní svět nedokázali představit.

Tyto vzrůstající možnosti jsou ale dvoječná zbraň, neb člověk je tvor od přírody zvědavý a není nic lepšího, než vynalézt, sestavit, navrhnout, sestavit, naprogramovat a zprovoznit opět něco nového, hezčího, sofistikovanějšího. Dostáváme v jeden okamžik do stavu, že máme krásný software se spoustou možností, ale nějak nám to na tom starém PC tuhne. Pořídíme tedy lepší hardware (a že ho máme nyní dostatek a za příhodné ceny) a vida, jak to pěkně chodí. Nebylo by na škodu opět zlepšit aplikaci, ať má konkurence radost, když to tak svižně a pěkně funguje?

Jestli by bylo nebo nebylo, je spíše otázka akademického rázu. Bezpochyby totiž zlepšení bude. A na tomto principu to celé je, což nyní mohu srovnat zpětně do r.1997, kdy jsem nastoupil pracovat na Finanční úřad v Zábřehu na pozici správce počítačové sítě a informačního systému, kdy uživatelé za operační systém tehdy považovali nastavbu Microsoft Windows for Workgroups 3.11, hitem byl nepřekonatelný textový editor T602 a vrcholem spokojenosti správce daně byl přístup přes terminálový emulátor Arctel do ADISu - tímto se v prostředí ÚFO – územního finančního orgánu myslí ADIS – Automatizovaný Daňový Informační Systém. Tento jediný přežil z uživatelského pohledu a „své přívětivosti“ černé terminálové obrazovky dodnes (byť hardwarový unixový stroj se systémem IBM AIX držící při životě databázový Informix se samozřejmě díky nikdy nevyužité volbě „Export dat“ poměnil několikrát a s rostoucím objemem dat bude měnit i nadále). Volbu „Export dat“ mají k dispozici pouze administrátoři a ti ji stejně nevyužijí (resp. nedostanou tento pokyn), neboť kdo by se zbavoval největší referenční databáze, která poskytuje tolik přesných informací?

Od zmíněného roku 1997 se množství instalací a výměn hardwaru, které jsem prováděl osobně, dá nějak specifikovat, ale pro účely tématu této bakalářské práce bude stačit, když uvedeme, že jich bylo opravdu hodně, což se při cca 55 aktivních klientských stanicích + 6 –

ti notebooků, jejich obměnách, kaskádách a upgradech vedle serverů je v průběhu let do dneška pěkné číslo. To nebudeme mluvit o perifériích a zařízeních jako kamerový systém (CCTV), elektronický zabezpečovací systém (EVS), elektronický požární systém (EPS) a pobočková telefonní ústředna (PbTÚ), na jejichž provoz si musí správce sítě najít čas.

Instalace, reinstalace a upgrady PC, patří časově mezi nejnáročnější a přitom musí zůstat prostor i na helpdesk uživatelům a řešení servisu techniky a objednávek materiálů, prostor na revize, porady a další provozní záležitosti.

S touto myšlenkou „zrychleného světa“ se v této bakalářské práci pokusím seznámit čtenáře s řešeními, které je možné využít pro úsporu času při instalacích. V současné době jsme obdrželi dodávky nových identických PC, kde byl dodatečně zakoupen upgrade na nový operační systém Windows 7. Pokusím se blíže seznámit s nástrojem Windows Automated Installation Kit for Windows 7, popsat možnosti instalací které poskytuje a pokusím se nasadit vhodné užití pro časové zrychlení instalačního procesu a ke konci zkusíme zhodnotit, jak se to povedlo či nikoli.

Celá práce bude zasazena do existujícího rámce naší organizace a jejího vybavení, které popíši v teoretické části bakalářské práce. Zde také popíši technologie Microsoft Windows Serveru 2003 týkající se instalací software aplikované i v naší organizaci, a dále teoretické seznámení s nástroji sady WAIK.

V praktické části bych rád uvedl reálné užití instalací řad počítačů nástroji WAIK za pomoci vytvoření image z referenčního počítače.

I. TEORETICKÁ ČÁST

1 INFRASTRUKTURA SÍŤOVÉHO PROSTŘEDÍ

1.1 FINet WAN

FINet je název pro WAN (Wide Area Network) síť daňového resortu MF - Ministerstva financí podle projektu FINet-ADIS společností MF, IBM a DATASys , která propojuje celorepublikově Ministerstvo financí, ÚFDŘ – Ústřední finanční a daňově ředitelství, 8 Finančních ředitelství vč. Finančního ředitelství pro Hlavní město Prahu a cca 190 ÚFO - Územních finančních orgánů, které provádějí výběr a správu financí České republiky.

Síť je postavená na bázi TCP/IP protokolů a poskytuje svým uživatelům všechny základní síťové služby (datové, hlasové a internetové služby). Zároveň jsou v ní dodržována bezpečnostní opatření, vyplývající z její základní funkce, kterou je přenos citlivých dat.

Páteř sítě je postavena na vysokorychlostních ATM spojích společnosti NEXTRA, jednotlivé územní finanční orgány – Finanční úřady jsou propojeny do forestu – doménového stromu, přes jim nadřazená jednotlivá Finanční ředitelství pomocí technologie MPLS nepřepojovanými okruhy společnosti Telefónica O2 Czech Republic a. s., kopírují hierarchickou strukturu působnosti jednotlivých organizací a tím navíc umožňují efektivní názvosloví jednotlivých destinací úřadů a jejich doménových jmen.

Pro Finanční úřad v Zábřehu, celé skutečné jméno právnického subjektu zní:

Česká republika – Finanční úřad v Zábřehu je doménové jméno zab.os.ds.mfcr.cz.

Tato zdánlivě podivné spojení vysvětluje:

- .cz – doména prvního stupně – Česká republika.
- .mfcr – doména druhého stupně – doménový název organizace Ministerstva Financí České republiky.
- .ds – daňová správa.
- .os – FŘ Ostrava.
- zab – FÚ v Zábřehu.

Tímto způsobem je umožněno definovat jakoukoli destinaci úřadu a v ní příslušný objekt v Active Directory serverů Windows 2008 a serverů Windows 2003 síť FINet v rámci celé sítě WAN daňového resortu.

1.2 LAN FÚ

Popis základní informace o fyzické vrstvě sítě v modelu OSI pro LAN (Local Area Network) FÚ v Zábřehu by mohl být následující:

Konektivita s forestem FINet pro Finanční úřad v Zábřehu je zajištěna pronajatým připojeným okruhem Ostrava - Zábřeh od společnosti Telefónica O2 o rychlosti 1024 Kbit/s vyvedeném do zařízení router CISCO 1841 s technologií MPLS (Multiprotocol Label Switching) v služebním segmentu sítě LAN. Tento segment přepojuje router CISCO 2801 do aplikačního segmentu LAN FÚ.

Obě tato zařízení se nacházejí v 19“ síťovém racku zálohovány napájením přes UPS Best Fortress LI1450VA. Veškeré propojení v serverovně FÚ je realizováno metalickými obvody „kroucené dvojlinky“ UTP kategorie 5e a kategorie 6 osmi žilového kabelu zakončeného konektory RJ-45 na rychlosti (s dvěma výjimkami) 100 Mbit/s.

Ve větvi aplikačního segmentu jsou na vstupu z routeru připojena dvě zařízení vzájemně propojené Cisco WS-C3750-48PS-S Catalyst 10/100 PoE ve funkci switche, rozvádějící síť LAN po FÚ v topologii hvězda. Fyzicky jsou umístěna v ranžirovacím 19“ racku a jsou opět zálohována UPS Best Fortress LI1450VA.

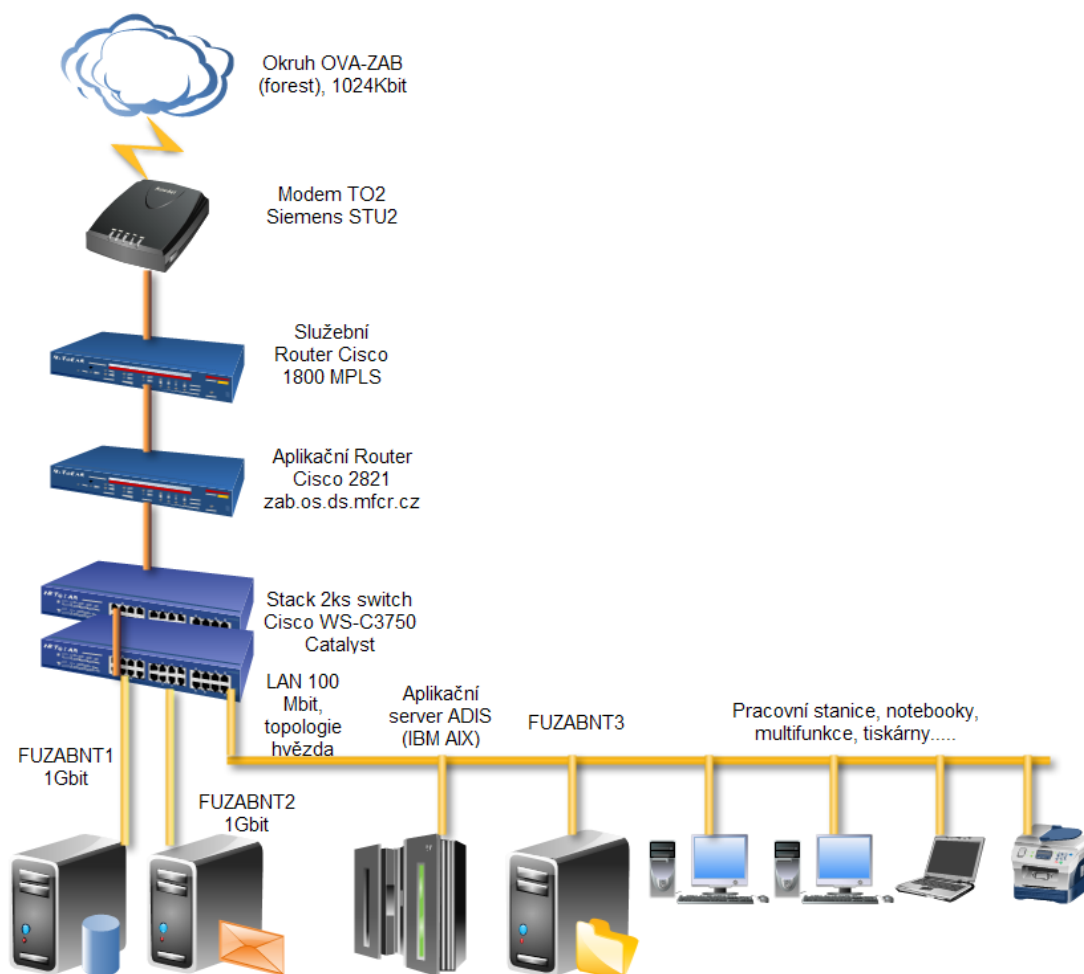
V aplikačním segmentu na rychlosti 100Mbit/s je připojen aplikační server ADIS. Tento server je realizován hardwarově RISC serverem IBM 7028-6E4 s externím diskovým polem FASTT600 připojením disků FC (fiber chanel) přes optické kabely. Záloha dat je v současnosti na externí páskovou jednotku IBM Systém Storage Ultrium LTO 3. Záloha napájení je přes UPS Powerware PW5125 2200VA. Na tomto stroji běží operační unixový systém AIX ve verzi 5.3.0.0 a v něm databázový stroj Informix verze 10.00.FC10

V aplikačním segmentu sítě LAN se dále nacházejí 3 servery Microsoft Windows Server 2003 Service Pack 2: fuzabnt1, fuzabnt2, fuzabnt3 (pozn. jejich jmenné názvy opět korespondují se projektem FINet-ADIS). První dva z nich jsou ale především controllery sítě Active Directory a zároveň DNS servery (domin name servery) a jsou nositeli Group Policy – neboli GPO politik. Jím se budeme věnovat podrobněji dále, již k tématu této bakalářské práce. Tyto dva servery jsou připojeny do zmíněných switchů Cisco WS-C3750 přes transceiver GLC-T 1000 Base-T SFP, čili na rychlosti 1Gbit každý. Zálohování dat je provedeno do kříže, a pak na externí páskovou jednotku HP StorageWorks LTO Ultrium 232 external. Záloha napájení je svěřena pro každý server své UPS APC Smart-UPS

1500VA. Třetí server FUZABNT3 je připojen na standardních 100Mbit a je zálohován identickou UPS s předchozími stroji a není na něm replikace Active Directory – neslouží jako controller domény ZAB (doména ZAB je opět výsledkem názvosloví projektu FINet-ADIS).

Všechna tato výše uvedená zařízení (včetně dalších jako EZS, PbTÚ, CCTV) zařízení se nacházejí v zabezpečené místnosti klimatizované serverovny pod dohledem CCTV, pásky s daty v antimagnetickém a požárně odolném trezoru, kopie dat pásek jsou navíc uschovávány i v safesové schránce trezoru bankovního domu.

Uživatelské pracovní stanice, notebooky a jejich připojení do sítě LAN FÚ v Zábřehu – tyto jsou připojeny do sítě přes rozvody strukturované kabeláže realizované kabeláží kategorie UTP 5e ukončené v kancelářích zásuvkami pod omítku, a v serverovně vyvedeny v ranžirovacím racku a propojeny patch cordy do zmíněných switchů na rychlosti 100 Mbit.



Obrázek 1. LAN FÚ.

2 MICROSOT WINDOWS 2003 SERVER

Informace v této velké kapitole jsou hlavně čerpány z knihy Microsoft Windows 2003 Server – Velký průvodce administrátora [3].

2.1 HW serverů

Servery MS Windows 2003 jsou na FÚ v Zábřehu hardwarově realizovány jako výkonnější PC s CPU IntelCore2 Duo 6420 (takt 2.13GHz), RAM 4 096 MB v dual chanel, a dvěma disky SATA II o kapacitě cca 250 GB v RAID 1 (mirroring), 2x 1Gbit ethernet LAN, výkonný zdroj FORTRON Blue storm II 500W, perforovaná skříň ThermalTake pro výkonné chlazení dodatečně osazena účinnými ventilátory.

2.2 SW rodina produktů

Rodina produktů Windows 2003 Sever zahrnuje 4 produkty [3]:

- Standard Edition
- Enterprice Edition
- Datacenter Edition
- Web Edition

Samostatnou kapitolu představuje Windows Small Busines.

Na FÚ v Zábřehu jsou instalovány servery v první uvedené verzi Standart Edition.

2.3 Seznámení s MS Windows Server 2003

Microsoft Windows Server 2003 je určen pro potřeby malých až středních podniků a poskytuje veškeré nezbytné sdílení souborů a tiskáren, bezpečné připojení k Internetu a možnosti spolupráce.

Jedná se o stabilní a výkonnou platformu pro technologii .NET, která je předem vytvořenou infrastrukturou pro vytváření aplikací založených na využívání Internetu.

Díky vylepšenému zabezpečení, možnostem sítě a službě Active Directory je určen jako centrum veškerého komunikačního dění v organizaci, může sloužit jako router, server Exchange nebo webový server.

Značné rozdíly ve struktuře a rolích existují v porovnání 32-bitové a 64-bitové verzi.

Funkce Instalace Software může uživateli nebo skupině přiřadit aplikaci, případně pomocí funkce publikování ji přidat na panelu Přidat nebo odebrat programy.

2.4 Nativní souhra

I když pro Windows Server 2003 je nejvhodnějším klientem Microsoft Windows XP Professional, a jejichž komunikace a fungování ve využitelnosti nabízených možností je považováno za nativní, umí připojit i jiné klienty.

Nicméně v současné době je pro Windows 7 nativním serverovým systémem nástupce Microsoft Windows 2008 [1], [2], díky technologii DirectAccess, která vytváří tunel mezi koncovým počítačem a podnikovou sítí (jedná se přibližně o něco na způsob VPN (Virtual Private Network)).

Ale organizace nemají kupříkladu prostředky pro přechod a nákup CAL (klientských) licencí a tak často dochází k přetrvávání užitečných Windows Serveru 2003 ve svých síťových pozicích.

2.5 Active Directory

Microsoft Windows Server 2003 Standart Edition obsahuje službu Active Directory, jako adresářovou službu, která propojuje adresáře uvnitř sítě a slouží jako jeden velký seznam [3].

Active Directory kombinuje pojmenovací standardy X.500, systém pojmenování domén Internetu (DNS) jako zařízení pro vyhledávání a protokol LDAP jako základní protokol.

Tento adresář poskytuje jeden centrální bod správy pro všechny zdroje, uživatele, soubory, periferní zařízení, hostitelské připojení, databáze, přístupy na web, služby a síťové prostředky.

Podporuje hierarchický obor názvů pro informace o účtech uživatele, skupiny a počítače a může zahrnovat a spravovat ostatní adresáře.

Active Directory umožňuje třídám WMI (Windows Management Instrumentation) sledovat, zda řadiče domény úspěšně replikují informace mezi sebou a také sleduje fungování důvěryhodnosti.

2.5.1 Globální katalog

Obsahuje částečnou repliku všech názvosloví kontextů v adresáři, kontexty schématu konfigurace, ale pouze s nízkým počtem atributů.

2.6 MMC

Microsoft Management Console (MMC) je hostitelem pro širokou paletu nástrojů pro správu zobrazených jako konzoly. Tyto nástroje, složené z jedné nebo více aplikací, jsou tvořeny tzv. snap-in moduly.

2.7 Group Policy

Zásady skupiny je technologie správy používaná k určení možností konfigurace sítě pro skupiny počítačů a uživatelů. Zásady skupiny jsou uloženy jako Objekty zásad skupiny (GPO), které jsou naopak spojeny s objekty adresáře Active Directory, jako jsou weby, domény nebo organizační jednotky (OU). Zásady skupiny mohou zahrnovat možnosti zabezpečení, možnosti instalace a údržby softwaru, nastavení WSUS (Windows systém update serveru) a možnosti pro skripty ovládající spouštění a vypínání. Umožňují přiřazení více úkolů, umožňují přizpůsobit a řídit nastavení v Ovládacích panelech, Terminálové služby, Vzdálené pomoci, sítí, zaslání zpráv o chybách a cestovních profilů [1], [2], [3].

2.7.1 Group Policy Object

Objekt zásady skupiny (GPO) obsahuje výsledná nastavení zásad skupiny, nástrojem pro editaci je Editor objektů zásady skupiny.

Objekty GPO uloženy na úrovni domény jsou přiřazeny k objektu služby Active Directory – serveru, doméně, řadiči domény nebo organizační jednotce. Objektů GPO může být více, stejně jako jeden GPO objekt lze aplikovat na více objektů v Active Directory.

Objekty GPO uchovávají informaci na dvou místech: GTP a GPC.

2.7.1.1 Group policy template

Struktura složek Šablon zásad skupiny (GPT) je automaticky vytvořena po vytvoření objektu GPO. Její skutečný název je globálním jedinečným identifikátorem (GUID) objektu

– číslo. Cesta ke složce zásad je %Kořenová_složka_systému%\SYSVOL\název_domény\policies [3].

2.7.1.2 *Group policy container*

Kontejner zásad skupiny (GPC) jsou objekty zásad skupiny, které nejsou místní, zahrnují vnořené kontejnery s údaji o verzi, informaci o stavu a seznamu přípon skupiny v objektu GPO.

2.7.2 **Součástí zásad skupiny**

Zásady skupiny zahrnují několik konfigurovatelných součástí [3]:

- Šablony pro správu – nastavují zásady týkající se registru.
- Nastavení zabezpečení – konfigurace u uživatelů, počítačů, domén.
- Skripty – spouštěné při spouštění a vypínání počítačů, při přihlášení a odhlášení uživatele.
- Přesměrování složky – např. umístuje v síti složku Dokumenty či složky aplikací.
- Software – přiřazuje uživatelům aplikace.

2.7.3 **Správa zásad skupiny**

Zásady skupiny jsou děděny na podřízené objekty a jsou kumulativní.

Explicitní nastavení mají přednost před zděděnými oprávněními.

Nejsou však aplikovatelné na složky Users s Computers v modulu Uživatelé a počítače služby Active Directory, protože nejsou organizačními jednotkami a nelze na nich tedy zásady skupiny uplatňovat.

Umístění skupiny zabezpečení není při konfiguraci důležité. Podstatné je přiřazení uživatelů a počítačů do členů skupiny Zabezpečení.

2.7.4 **Pořadí implementace**

Zásady skupiny se uplatňují v následujícím pořadí, které ukazuje, že nejdříve jsou použity místní zásady, jako poslední zásady organizační jednotky, do níž uživatel či počítač patří [3]:

1. Místní objekty zásad skupiny.
2. Objekty GPO připojené k serveru v administrativně stanoveném pořadí.
3. Objekty GPO domény v administrativně stanoveném pořadí.
4. Objekty GPO organizační jednotky, od největší po nejmenší organizační jednotku (od nadřazené po podřízené).

2.7.5 Tvorba objektu zásad skupiny

2.7.5.1 Výchozí zásady

Výchozí zásada domény a výchozí zásada řadičů domény jsou vytvořeny automaticky ve chvíli vytvoření – vzniku domény služby Active directory.

2.7.5.2 Tvorba vlastních zásad GPO

Chceme-li vytvořit vlastní nebo editovat již vytvořený objekt GPO pro domény, řadiče domény, nebo organizační jednotky, klikneme na modul Uživatelé a počítače služby Active Directory. Chceme-li to samé, ale pro objekty GPO serverů, spustíme modul Sítě a služby Active Directory.

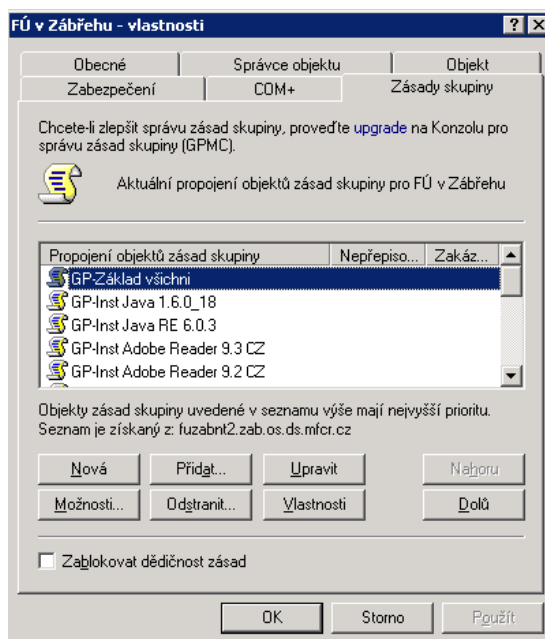
Vybereme objekt, pro který chceme vytvořit nebo editovat GPO, klikneme na něj pravým tlačítkem a dáme Vlastnosti.

Podle toho, jestli máme defaultní stav MMC konzole zvolíme záložku Zásady skupiny, viz. Obrázek 2.

Nabízené možnosti přes následující tlačítka jsou:

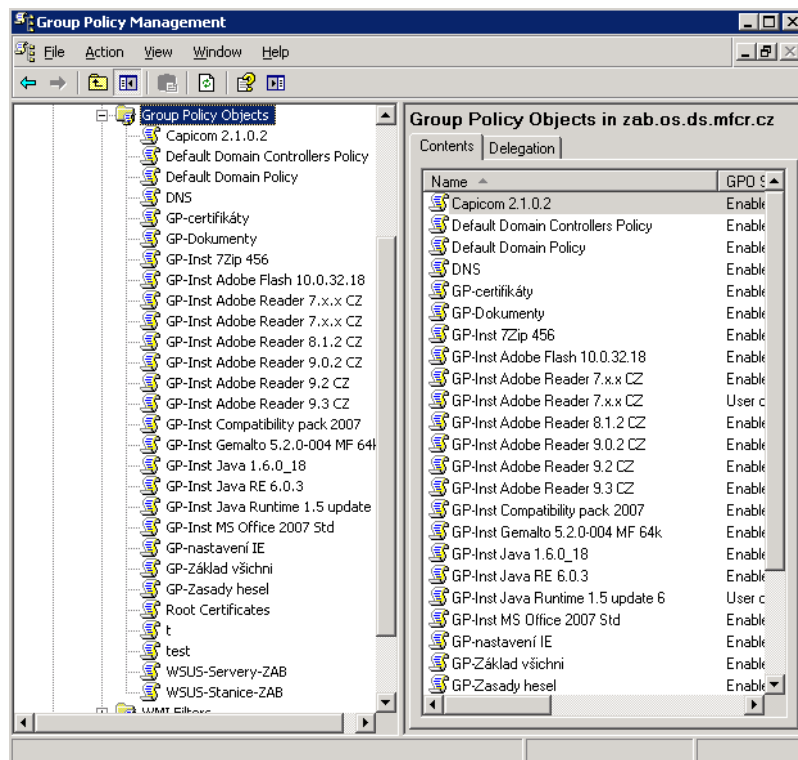
- Nová – vytvoří novou zásadu.
- Přidat – přidá propojení na novou zásadu.
- Upravit – otevře objekt GPO v editoru zásad skupiny.
- Možnosti – umožňuje nastavení „nepřepisovat“, nebo „zakázat“ objekt GPO.
- Odstranit – nabídne možnost „Odebrat propojení ze seznamu“, čímž zůstane objekt GPO ve službě Active Directory, ale nebude uplatňován na konkrétní kontejner služby Active Directory, nebo odstraní objekt GPO natrvalo.

- Vlastnosti – slouží k nastavení filtrace prostřednictvím skupin zabezpečení, je-li to na objektu GPO vyžadováno (toto je vhodné např. při testování).



Obrázek 2. MMC konsole.

V případě, že jsme na základě upozornění provedli upgrade na Konzolu pro správu zásad skupiny (GPMC), bude vypadat obrazovka takto s mírně rozdílným ovládáním:



Obrázek 3. GPMC konsole.

2.7.5.3 Editor zásad skupiny

Vytvoříme-li nový objekt GPO v jednom typu z uvedených konzolí, každopádně by měla zásada něco dělat a toto zajistíme její úpravou – editací, čímž se spustí Editor zásad skupiny, který zobrazí dva uzly: Konfigurace počítače (tento aplikuje nastavení zásad na všechny počítače při jejich zapnutí) a Konfigurace uživatele (zásady jsou uplatňovány při přihlášení konkrétního uživatele do sítě). Po jejich rozkliknutí se pod každým z nich zobrazí tyto položky a to [3]:

- Nastavení software – slouží pro efektivní vzdálenou instalaci a správu software.
- Nastavení systému Windows – umožňuje měnit nastavení v registrech systémů, skriptů při spouštění a vypínání, nastavení připojení v Internet Exploreru, zabezpečení.
- Šablony pro správu – pro existující a pro doinstalované umí ovlivňovat chování částí systémů, či aplikací.

2.7.6 Aktualizace zásad skupiny

Změny nastavení zásad skupiny jsou v podstatě okamžité, nejsou však ihned přeneseny do klientských počítačů. Tyto vysílají požadavek na aplikaci zásad v těchto případech [3]:

- Spouštění počítače.
- Přihlášení uživatele.
- Požadavek aplikace na obnovení.
- Požadavek uživatele na obnovení.
- Je povolen interval aktualizace zásad skupiny a došlo k jeho vypršení.

2.7.6.1 Vynucení požadavku zásad skupiny

Požadavek uživatele na obnovení může mít podobu příkazu cmd (command line) v řádce:

gpupdate /force – zajistí aplikaci nastavení zásad po restartu.

gpupdate /sync – vynutí proběhnutí aktualizace počítače i uživatele a způsobí po souhlasu restart.

gpresult /H GPREport.html – na Windows 7 můžeme získat i report zásad skupiny.

2.7.6.2 Vynucení požadavku zásady „update systému“

Pokud využíváme vlastností serveru MS SUS (Microsoft Software Update Services), který poskytuje bezpečnostní updaty, kritické aktualizace a opravy zabezpečení systémů řady Windows 2000, Windows XP a Windows Server 2003, nebo ještě lépe serveru MS WSUS (Microsoft Windows Server Update Services), který umožňuje rychlé a spolehlivé nasazení veškerých aktualizací softwaru společnosti Microsoft a ovladačů do počítačů v síti a tyto máme aplikované pomocí klienta automatické aktualizace, který je od Windows 2000 SP3 a Windows XP SP1 v systému již obsažen (klient využívá technologie BITS – Background Intelligent Transfer Service) [3], pak pomocí MMC konzoly zásad skupiny GPEDIT.MSC po dohrání šablony wuau.adm je možné spravovat zásadami i tyto aktualizace.

Po instalaci a přidání PC do domény se tyto aktualizace nainstalují zpravidla po druhém restartu PC.

Jejich vynucení na stanici ale můžeme provést příkazem v command line řádce:

wuauclt /detectnow

2.7.7 Průvodce výslednou sadou zásad skupiny

Umožňuje v režimu plánování analyzovat a určit, co je skutečným výsledkem sady zásad. V režimu přihlašování naopak zjistí, co se děje v daném okamžiku.

2.8 Instalace a správa vzdáleného software pod Windows Server 2003

Je součástí služby IntelliMirror, která je sadou technologií umožňujících přenesení uživatelských dat, nastavení a aplikací do jiných počítačů se systémy Windows 2000 a vyšší.

Instalace a údržba software pomocí Active Directory může být dvojitá a to instalace Přiřazené a Publikované.

2.8.1 Publikování aplikací

Jestliže zavedeme aplikaci pomocí Publikování a Active Directory, stane se tato aplikace dostupná z panelu Přidat nebo odebrat programy pro ty uživatele, pro které byla vytvořena zásada GPO. Aplikace nasazované tímto způsobem nelze publikovat pro počítač.

Toto řešení má ale jeden zásadní nedostatek, a to ten, že aplikaci nemůže nainstalovat v systému standardní běžný uživatel ze skupiny User, případně Power User.

2.8.2 Přiřazení aplikací

Tento způsob zavede aplikaci na základě zásady GPO automaticky buď na počítač nebo na uživatele, přičemž přiřazené aplikace se zobrazí v nabídce Start a nainstalují se při prvním použití anebo, a tento způsob preferuji, je umožněno vynutit nasazení automaticky ihned při dalším přihlášení.

2.8.3 Formát instalačního balíčku

Můžeme si zvolit, jakým způsobem budeme aplikace instalovat, jestli pomocí .MSI souborů, nebo pomocí .ZAP souborů.

Pro zvolení optimální formy balíčku bude naše rozhodnutí vycházet ze zjištění, v jakém instalátoru, který řídí celou instalaci aplikace, je daný software distribuován. Mezi známé instalátory např. patří:

- Windows Installer (př. aplikace společnosti Microsoft)
- InstallShield
- Inno setup (př. PDFcreator)

Tímto je skoro rozhodnuto, jakým formátem, jestli .MSI či .ZAP, budeme aplikaci nasazovat.

2.8.3.1 .MSI balíčky

Instalační služba systému Windows Installer a její .MSI balíčky jsou považovány za nejlepší volbu pro zavádění (můžeme zavést, změnit, odebrat) SW přes Group Policy [3].

Samotné aplikace zavádíme pomocí .MSI balíčků, její nastavení můžeme provést pomocí ADM/ADMX šablon (ADMX ve formátu .XML od Windows Vista; a s jazykovými popisky ADML) [4], existují-li k dané aplikaci, nebo vytvořit tzv. Transformační soubory (.MST), které budou upravovat nastavení instalované aplikace. Transformační soubory je možné vytvořit buďto nástrojem od dodavatele nebo pomocí nástrojů pro tvorbu a repackaging .MSI balíčků a .MST souborů.

2.8.3.2 .ZAP balíčky

Představují poslední možnost jak instalovat vzdáleně aplikace, které nejsou dodány ve formě .MSI balíčku Windows Installeru.

Vytvořením .ZAP souboru vytvoříme zvláštní instalační soubor odkazující se na instalační program dané aplikace, kterým lze volitelně spouštět automatizované instalační skripty.

2.8.3.3 Nástroje pro opětovné vytvoření balíčků instalací a repackage

Je málo pravděpodobné, že se nám podaří vytvořit lepší instalační program, než je dodaný výrobcem aplikace, navíc bez podrobných informací o programu, nicméně využitelné za různým účelem mohou být tyto aplikace, které se svým pojetím k našemu tématu váží:

- msixec.exe – samotný Windows Installer s parametrem /a přepne instalátor do administrátorského módu a rozbalí obsah instalace.
- Custom Installation Wizardy – existující v rámci resource kitů k aplikacím (př. MS Office), nebo jako aplikace (př. Adobe Customization Wizard 9).
- AdminStudio – výkonná komerční aplikace.
- WinstLE – vytváří .MSI balíček otiskem.
- Orca – součást Windows SDK Components for Windows Installer Developers.
- Exe to Msi Converter – jednoúčelová aplikace.
- MaSaI Editor.

2.8.4 Distribuční místo software

Na serverovém úložišti pod účtem síťového administrátora vytvoříme sdílenou složku s těmito oprávněními [3]:

- Everyone, Authenticated Users = Číst.
- Domain Computers = Číst.
- Administrators = Úplné řízení, Změnit, Číst.

Vytvořené podsložky se zděděnými oprávněními mohou obsahovat jednotlivé distribuční body.

Při velkém zatížení distribučního místa jej může být vhodné spravovat pomocí systému DFS (Distributed File System), který umožňuje vyrovnávání zatížení, replikaci a zajišťuje odolnost proti chybám.

2.8.5 Vytvoření balíčku instalace softwaru a nastavení možností

Samotnou instalaci provedeme vytvořením zásady GPO na třídě objektu Organizační jednotka v existující nebo nově vytvořené GPO zásadě a její editací v Editoru zásady skupiny, vybráním Konfigurace uzlu instalace, jestli na Počítač nebo Uživatele a zvolením položky Instalace software [3].

1. V pravém okně přes volbu NEW- Balíček otevřeme vytváření nové instalace SW, kde pomocí průvodce postupně projdeme možnostmi na všech nabídnutých záložkách. Pomocí okna výběru Otevřít nalezneme .MSI balíček ve sdíleném úložišti a vybereme jej.
2. Při dotazu Zavedení aplikace můžeme zvolit:
 - a. Přiřazené – chceme-li přiřadit aplikaci bez úprav.
 - b. Upřesnit – chceme-li konfigurovat možnost publikace nebo přiřazení a použít úpravy - transformační soubory (.MST) pro tento balíček.
3. Na záložce Obecné zvolíme Název a vyplníme jej.
4. Na záložce Zavedení můžeme zvolit Možnost – Oinstalovat tuto aplikaci, je-li mimo obor správy.
5. Na záložce Inovace můžeme přidat balíček z objektu současných skupinových zásad nebo z určitého GPO objektu, které mají být inovované naším instalačním bodem.
6. Na záložce změny můžeme (zvolili jsme-li na začátku při Zavedení aplikace Upřesnit) přidat transformační balíček, který upraví výslednou podobu instalace aplikace.
7. Na záložce Zabezpečení zkontrolujeme, kdo může vytvořenou GPO instalační zásadu použít. Zde je nanejvýš výhodné omezit čtení instalačního bodu jen třeba na specifický počítač, který vybereme z Active Directory, a vyzkoušet chování instalace. Je-li vše v pořádku, můžeme opět povolit čtení pro Authenticated Users, a umožnit nasazení balíčku všem.

Tímto je instalace aplikace vytvořena.

2.9 Správa bitových kopií Serveru RIS s Windows Server 2003

Windows Server 2003 s nainstalovanou Službou vzdálené instalace (RIS) umožňuje spravovat bitové kopie systémů Windows 2000, Windows XP a Windows 2003 a tyto systémy uživatelům automaticky nainstalovat, přičemž funkčnost služby je podobná funkčnosti poskytované při používání bezobslužných souborů odpovědí a nástroje Sysprep, je však pružnější a bezpečnější [3].

2.10 Správa bitových kopií Serveru WDS s Windows Server 2008

Od příchodu Windows Vista se změnil instalační proces a právě na toto reaguje nová služba WDS (Windows Deployment Services) obsažená ve Windows Server 2008. Tato služba umí nasazovat OS Windows Vista, Windows 2008 i Windows 7 [1], [2].

WDS by podle dokumentace měla být možná samostatně nebo v rámci druhého opravného balíčku nainstalovat i na systémy Windows 2003.

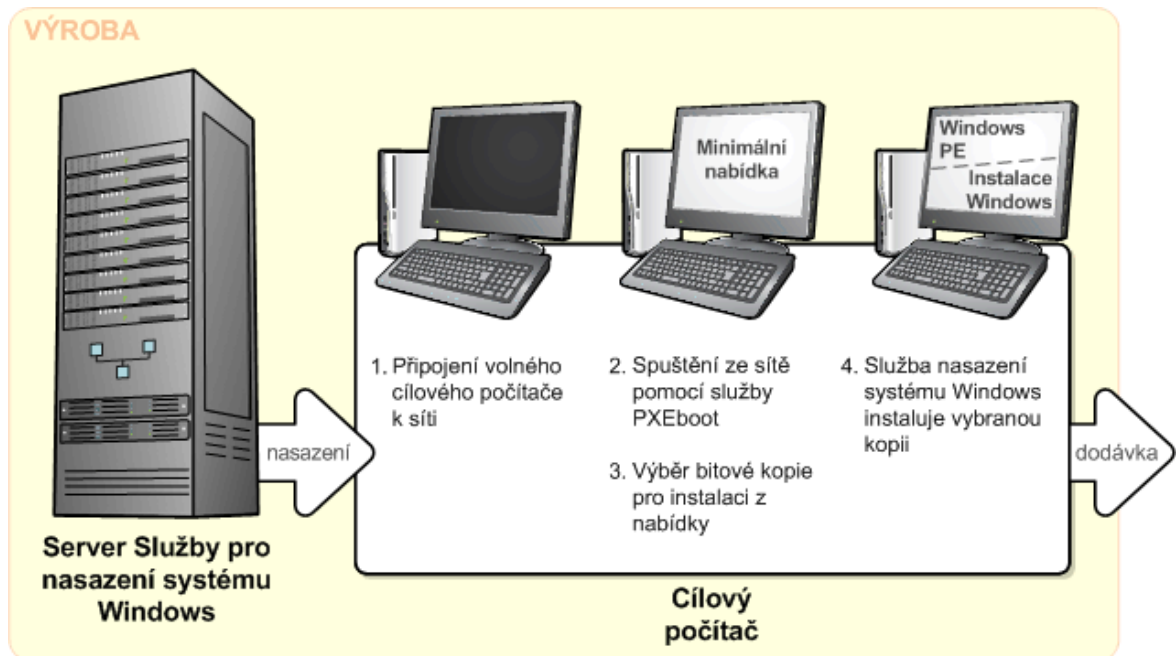
WDS kromě rychlejších bezdotazových instalací, automatického zařazování do domény, automatického pojmenování PC, automatického zařazení do Organizačních jednotek místo kontejneru Computers nabízí i vícesměrové přenosy (instalace pro více počítačů je přenášena broadcastem), čímž šetří přenosové pásmo.

2.11 Serverová služba DHCP

DHCP, neboli Dynamic Host Configuration Protocol, je serverová služba, která umí v prostředí sítě přidělovat IP adresy namísto ručního statického adresování jednotlivých síťových adaptérů každého síťového HW zařízení.

V síti FINet je podle projektu FINet-ADIS tato služba z bezpečnostních důvodů zakázána. Byť jsem schopen službu na server přidat, nakonfigurovat potřebný rozsah adres, nemám bohužel oprávnění ze skupiny Enterprise Admins, které potřebuji k ověření důvěryhodnosti pro serverovou službu DHCP z Active Directory, aby mohla služba DHCP IP adresy ze stanoveného rozsahu přidělovat.

A právě doménovou službu DHCP potřebují pro svoji funkčnost Servery instalací RIS nebo WDS, když jednotlivé PC bootují přes síťové rozhraní přes prostředí PXE a spoléhají při adresování na protokol IP [4]. Princip viz. Obrázek 4:



Obrázek 4. Instalace s DHCP.

Z tohoto důvodu jsou v tomto okamžiku Služby RIS a WDS nedostupné a řešíme bootování pomocí bootovacího CD média s prostředím WindowsPE, kdy nastavíme IP, masku a bránu posléze ručně.

2.12 Alternativní řešení I. – virtuální počítač v souboru .VHD

Jako student Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně bych mohl za účelem testování problematiku (nejen) s DHCP serverem vyřešit ještě jedním elegantním způsobem:

Instalací Microsoft Windows Serveru 2008 [5] z e-akademie studentského výukového programu software centra MSDN Academic Alliance do virtuálního prostředí SW Virtual PC 2007, kde celý souborový systém a obraz virtuálního disku by byl uložen ve formátu souboru .VHD .

Pro samotnou instalaci MS Windows Serveru 2008 by šlo efektivně využít funkčnosti MS Virtual PC 2007 [2], [8] a to načítání přímo z .ISO souboru uloženého na hostitelském PC

místo instalace z disku DVD, čím lze u některých typů SW i několikanásobně zkrátit čas pro instalaci. ISO soubor načítaný z disku výkon virtuálního stroje maximálně urychlí.

Po nastavení virtuálního počítače a jeho virtuálních síťových adaptérů by bylo umožněno po zadání vlastní IP adresy komunikovat a poskytovat síťové služby včetně naší potřebné DHCP.

2.12.1 VHD soubor

Microsoft využívá formát VHD nejen k vizualizaci hardware, ale i ke kompletním zálohám OS Windows Vista, Windows7 (nastaví-li se) a Windows 2008, přičemž je umožněno provést i samotné instalace fyzických operačních systémů do .VHD na servery, notebooky a klasické počítače. Výrazné rozdíly ve výkonu fyzického disku a disku .VHD nejsou [6], ale .VHD vyžaduje mírně vyšší zátěž CPU a naopak nabízí v některých případech mírně vyšší rychlost díky pevné alokaci diskového prostoru jediným souborem, kde je dosaženo lepších výsledků díky interní struktuře .VHD.

Formátem .VHD se zabýval i Mark Russinovich s kolegy ze Sysinternals, když vytvořili utilitu Disk2VHD [7], která umožňuje udělat snapshot aktuálního disku či jeho oddílu a vytvořit regulérní .VHD, které pak lze virtualizovat ve Virtual PC 2007 či Hyper-V (virtualizace v roli Windows Server 2008 na bázi Hypervisoru – tenké vrstvy mezi HW a virtualizačním SW o velikosti kódu Microsoftu jen 700 KB, kdy vlastní virtualizaci provádí procesor s podporou instrukcí), což považuji za skvělou věc, protože některé staré aplikace nemusí umožnit běh pod novými OS, a díky virtualizaci je bude možno opět využívat.

V samotných Windows 7 je možné .VHD připojit ve Správě disků volbou Akce - Připojit virtuální disk za podmínky, že byl systém na .VHD souboru vypnut, nikoli uspán a pak je možnost i vytvořit .VHD přes volbu Akce - Vytvořit virtuální pevný disk [4].

2.13 Alternativní řešení II. – minirouter se síťovými službami

Minirouter se síťovými službami by nám také umožnil získat IP adresu ze služby DHCP. Bohužel takové zařízení zde k dispozici též není.

Také management zařízení switch Cisco WS-C3750 Catalyst umí službu DHCP, nicméně je plně využitý a rezerva je pouze ve skupině portů serverů, které mají speciální nastavení pro servery a jejich servisní účely a nelze je pro zamýšlený účel DHCP použít.

3 WINDOWS AUTOMATED INSTALLATION KIT WINDOWS 7

Informace k sadě WAIK, uvedené v této bakalářské práci vycházejí z dokumentace - vnitřního helpu sady WAIK – „Uživatelské příručky“ [9], která je jeho součástí a jejího dalšího dokumentu „Krok za krokem: Základní nasazení systému Windows pro profesionály IT“ [10].

Sada Windows Automated Installation Kit (Windows AIK) pro Windows 7 je sada nástrojů a dokumentace určené k podpoře konfigurace a automatizovanému nasazování řad operačních systémů Windows 7 a Windows Server 2008 [4].

Umožňuje instalace systému Windows s využitím těchto nástrojů [9]:

- ImageX – nástroj pro zachytávání bitové kopie systému Windows.
- DSIM – nástroj Obsluha a správa bitových kopií umožňuje konfigurovat a upravovat bitové kopie.
- Příkazový řádek nástrojů pro nasazení.
- WindowsPE – prostředí pro vytváření bitových kopií.
- USMT – nástroj Migrace profilu uživatele vytváří bitové kopie prostředí a přenáší profily a data uživatelů.
- VAMT - nástroj Volume Activation Management Tool umožňuje odborníkům z oblasti IT automatizovat a centrálně spravovat proces aktivace svazku pomocí aktivačního kódu MAK (Multiple Activation Key).

Sadu Windows AIK je možné instalovat na následující systémy [9]:

- Windows Server 2003 Service Pack 2
- Windows Vista SP1
- Řada Windows Server 2008
- Řada Windows 7
- Řada Windows Server 2008 R2

Obraz v ISO souboru pro vytvoření instalačního DVD je dostupný po ověření pravosti Windows z adresy <http://www.microsoft.com/downloads> o velikosti 1260,8MB.

II. PRAKTICKÁ ČÁST

1 STRATEGIE - REFERENČNÍ PC PRO „KLONOVÁNÍ“

Jak udělat referenční počítač?

Otázka není o tom, jak jej fyzicky instalovat, ale spíše o tom se rozhodnout, v které fázi se rozhodnout použít instalovaný počítač jako vzor pro vytvoření image.

Vycházím-li z reálných potřeb, mám v podstatě na výběr dvě možnosti:

- zvolit počítač se základní čistou instalací systému Windows 7.
- zvolit počítač co nejvíce nainstalovaný s nainstalovanými aplikacemi a již přihlášený do Active Directory s využitím instalací spravovaného SW a updatů systému přes GroupPolicy, tedy co nejvíce se blíží již konečné personifikaci a předání koncovému uživateli.

Po důkladném zvážení jsem se rozhodl použít pro referenční počítač druhou možnost s tím, že i pro vytvoření základní instalace čistého systému vyzkouším Sestavení souboru odpovědí a s ním spojenou práci s nástroji WAIK.

K tomu rozhodnutí mě vedla čistě pragmatická věc, zjistit, jak moc je možné instalaci urychlit a usnadnit. Instalace samotného PC do stavu před personifikací pro uživatele představuje v našich podmínkách několikahodinnou práci, neb i instalace spravovaného SW a aktualizací vyžaduje svojí režii a několik restartů.

Referenční počítač je ale určitě nutné mít bez instalovaného SW, který je vázán přímo na počítač, na kterém je instalován, pokud se odkazuje na informace typu jméno PC apod., protože tyto Sysprep odebere. Takový počítač by pro image nebyl vhodný, protože na cílovém počítači by byly nefunkční aplikace. Také by to nebylo vhodné u aplikací z instalací GPO, které by se dostali mimo obor své správy, tzn. nešlo by je ani znovu zavést, potažmo odebrat. Tím by byly aplikace mimo kontrolu hromadné správy SW přes Group Policy.

2 SCÉNÁŘE PRÁCE S WINDOWS AIK

V této části si ukážeme práci s prostředky, které nabízí Windows AIK [9], [10] s cílem vhodným způsobem ukázat základy práce s jednotlivými komponentami, které mohou být v našem případě pro potřeby této bakalářské práce užitečné, jinak totiž WAIK nabízí několik scénářů typových použití, které zde pro úplnost uvedu [9]:

- Nasazení z média
- Nasazení ze sítě
- Nasazení ze serveru
- Údržba offline bitové kopie
- Údržba online bitové kopie
- Údržba bitové kopie pomocí instalačního programu systému Windows

2.1 Filozofie práce s WAIK

Naším cílem bude vytvořit referenční počítač, z něhož referenční instalaci zachytíme do bitové kopie (.wim soubor) a uložíme ji do sdílené složky v síti. Poté tuto sdílenou referenční bitovou kopii nasadíme do cílového počítače, resp. řady cílových počítačů [10].

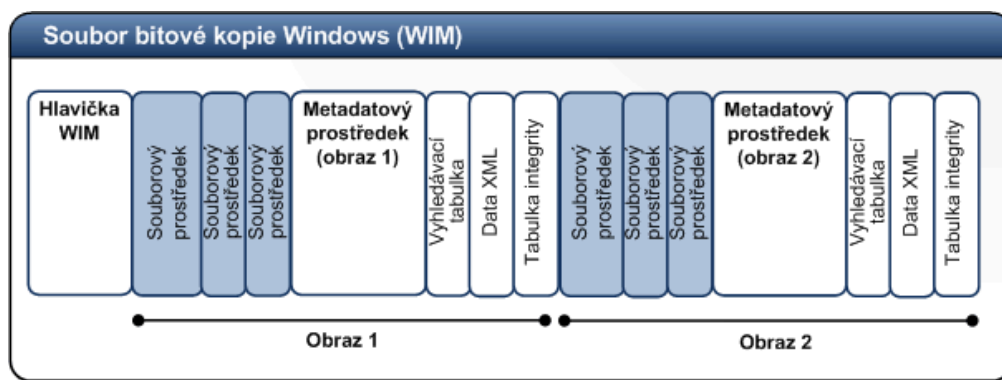
2.2 WIM soubory

Samotné bitové kopie neboli image (obrazy), představují fyzicky tzv. WIM soubory (soubory s příponou WIM). WIM je nový moderní formát (od operačního systému Microsoft Vista) bitových kopií (balíčků) založených na kompresi dat, kdy sám o sobě umí odstranění duplicitních dat.

Formát souborů WIM je optimalizován pro maximální kompresi pomocí algoritmu LZEX, pro rychlou kompresi pomocí algoritmu XPRESS nebo nemusí být komprimován [4].

2.2.1 Struktura souboru WIM

WIM obsahuje až šest typů prostředků: hlavičku, prostředek souboru, prostředek metadat, vyhledávací tabulku, data XML a tabulku integrity. Obecné rozvržení souboru s dvěma bitovými kopiemi vypadá takto [4], [9]:



Obrázek 5. Soubor bitové kopie WIM.

2.3 Několik užitečných postřehů k nápovědě nástrojů WAIK

Práce v command line prostředí podle „scénářů“ uváděných v anglické dokumentaci, i „scénářích“ v helpu české dokumentace WAIKu je celkem čitelná, ale obsahuje různé nuance a drobné odchylky (většinou od našeho zamýšleného účelu). Přesto si dovoluji z osobní zkušenosti získané při tvoření této bakalářské práce tvrdit, že se s těmito nástroji dá dobře pracovat a pokud člověk využívá nápovědy jak v grafickém prostředí SIM, tak i u command line příkazů pomocí syntaxe „HELP příkaz“ či „příkaz /?“ je mu umožněno vytvářet cíleně práci výkonným způsobem a práce je rozhodně použitelná. Je ale nutné mít určité povědomí, co v ten daný moment - přesněji jaký krok se dělá, protože již zmíněná dokumentace a třeba její značení jednotek (tedy, kde se zrovna na jakém fyzickém disku, RAMdisku, síťovém úložišti nacházíme) může být zavádějící a nesouhlasí s reálným stavem skutečného PC.

Například u vytváření odpovědního souboru v prostředí SIM ve chvíli zadávání parametrů disku je možné provést rozdělení na více logických partitions, ovlivnit velikosti, label jednotky, nastavit aktivní oblast a podobné věci. To samé umožňuje nástroj Diskpart ve chvíli konfigurace disku nového PC před nasazením bitové kopie ze síťového úložiště. Zde platí, více než kdy jindy, si projít nápovědné informace. Tyto nás bezpečně dovedou k cíli toho, co si přejeme udělat.

2.4 Příprava pro práci s WAIK

K dispozici musíme mít [10]:

- DVD disk s produktem Microsoft Windows 7.

- DVD disk s produktem Microsoft Windows Automated Installation Kit pro Windows7.
- Plně funkční síťové prostředí, nejlépe s DHCP serverem.
- Počítač technika s podporovaným operačním systémem pro instalaci WAI, DVD RW mechanikou a vypalovacím SW pro tvorbu bootovacích DVD z .ISO image, USB portem.
- Referenční počítač se síťovým rozhraním, DVD mechanikou a USB portem, instalovaný do stavu, který si budeme přát zkopírovat do jednoho nebo více cílových počítačů pomocí bitové kopie.
- Cílový počítač je HW stroj, na který budeme chtít nasadit existující bitovou kopii referenčního počítače. Měl by mít CD ROM mechaniku a síťové rozhraní.

2.5 Instalace WAIK na PC technika

Samotná instalace sady WAIK je jednoduchá instalace z vytvořeného spustitelného DVD a na počítač technika s podporovaným operačním systémem.

V rámci instalace z DVD je možné ještě provést stažení sad ACT (Application Compatibility Toolkit), která obsahuje nástroje a dokumentaci pro vyhodnocení a vyřešení potíží s kompatibilitou aplikací před nasazením systému Windows, sady MAP (Microsoft Assessment and Planning Toolkit) – výkonný nástroj pro vytváření soupisů, hodnocení a vytváření sestav bez nutnosti instalace agenta do počítače či zařízení při plánování migrace, a sady MDT (Microsoft Deployment Toolkit) – sady procesů a nástrojů pro automatizaci nasazení pro stolní počítače a servery. Těmto sadám se ale v této bakalářské práci věnovat nebudu. Případně lze doinstalovat potřebné rozhraní .NET Framework a službu MSXML 6 SP1 (pouze pro MS Windows Server 2003 SP1) .

Po instalaci nalezneme pod nabídkou Start – Všechny programy programovou skupinu Microsoft Windows AIK a v ní mimo jiné dva důležité nástroje, které použijeme:

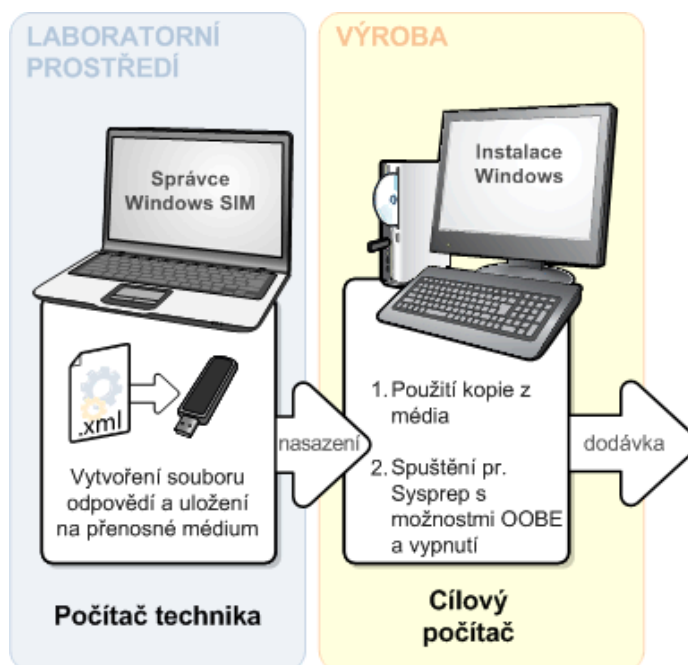
- Příkazový řádek nástrojů pro nasazení.
- Správce bitových kopií systému Windows.

2.6 Vytvoření souboru odpovědí v nástroji SIM

Následující kapitola bude úzce vycházet z elektronické Dokumentace – Názorný postup – Základní nasazení seznamu Windows pro profesionály IT z instalované sady WAIK [10], přičemž číslované postupy (návody) v kapitolách 2.6.1, 2.6.2 a 2.6.3 jsou přímo citacemi jednotlivých kroků z tohoto materiálu.

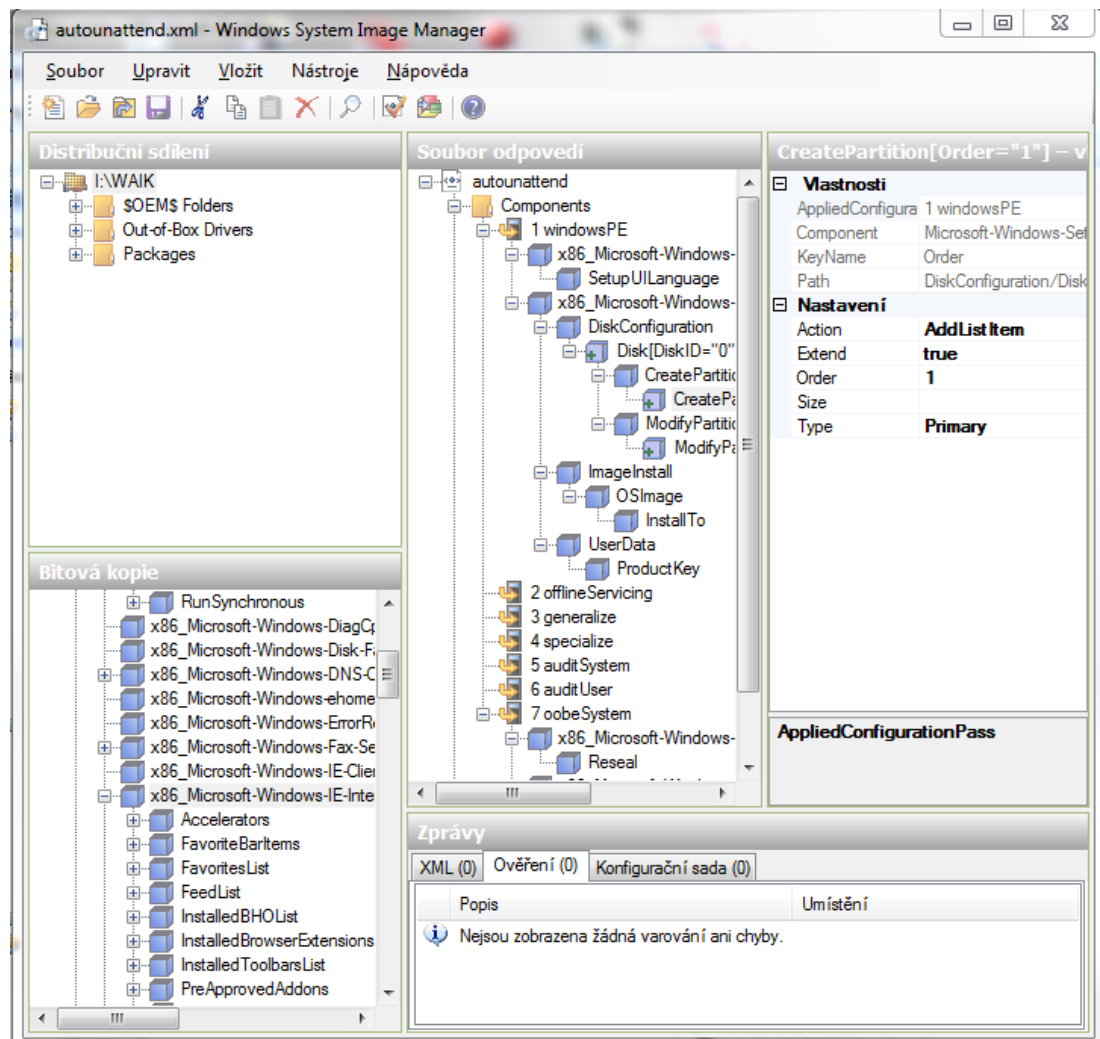
Budeme-li instalovat operační systém Microsoft Windows 7, budeme v rámci instalace z instalačního DVD média v průběhu instalačního procesu dotazováni na některé důležité údaje jako: volba jazyka instalace, volba prostředí (včetně rozhraní klávesnice), přijetí licenčního ujednání EULA, volba rozdělení diskového prostoru a dalších. U jednoho počítače toto lze samozřejmě pohodlně projít, ale v případě nasazení systému na řadu PC je vhodné si instalaci usnadnit pomocí tzv. souboru odpovědí.

Vytvoření souboru odpovědí provedeme v nástroji Správce bitových kopií (Windows SIM), který spustíme ze složky Microsoft Windows AIK. Soubor odpovědí je fyzicky .XML soubor, který uložíme na přenosné médium (př. flash disk) s jehož pomocí můžeme upravit parametry instalačního programu a využijeme jej při instalaci spolu s instalačním DVD médiem systému do referenčního/cílového počítače.



Obrázek 6. Soubor odpovědí.

Prostředí Správce bitových kopií se souborem odpovědí má několik oken: Distribuční prostředí, Bitová kopie, Soubor odpovědí, Okno vlastností a Okno zpráv a vypadá takto:



Obrázek 7. Nástroj SIM.

Po instalaci sady Windows AIK do počítače technika bude v adresáři C:\Program Files\Windows AIK\Samples k dispozici ukázkový soubor odpovědí Corp_autounattended_sample.xml.

2.6.1 Vytvoření souboru odpovědí

V tomto kroku zkopírujete soubor bitové kopie systému Windows (WIM) do počítače technika a vytvoříte soubor odpovědí [10].

1. Do počítače technika vložte disk DVD s produktem Windows 7.
2. Přejděte do adresáře \Sources v jednotce DVD-ROM a zkopírujte soubor Install.wim z disku DVD s produktem Windows na libovolné místo v počítači.

3. Otevřete sadu Windows SIM kliknutím na tlačítko **Start**, na položky **Všechny programy** a **Microsoft Windows AIK** a nakonec na příkaz **Správce bitových kopií systému Windows**.
4. V nabídce **Soubor** sady Windows SIM klikněte na příkaz **Vybrat bitovou kopii**.
5. V dialogovém okně **Vybrat bitovou kopii** přejděte do umístění, do kterého jste v prvním kroku uložili soubor Install.wim, a klikněte na tlačítko **Otevřít**. Zobrazí se výzva k výběru bitové kopie. Vyberte bitovou kopii systému Windows, kterou chcete nainstalovat, a potom klikněte na tlačítko **OK**. Zobrazí se výzva k vytvoření katalogového souboru. Kliknutím na tlačítko **Ano** vygenerujete soubor.
Pokud se zobrazí okno **Řízení uživatelských účtů** s výzvou ke schválení programu, můžete program povolit.
6. V nabídce **Soubor** klikněte na příkaz **Nový soubor odpovědí**. V podokně **Soubor odpovědí** se zobrazí prázdný soubor odpovědí.

2.6.2 Přidání a nastavení konfigurace Windows

Zde definujeme základní konfiguraci disku a nastavíme uvítání Windows [10].

1. V podokně **Bitová kopie** programu Správce bitových kopií zobrazte dostupné položky nastavení rozbalením uzlu **Součásti**.
2. V rozbaleném seznamu součástí v podokně Bitová kopie, který rozklikávejte tak dlouho, dokud nevidíte nejnižší podřízený uzel v následující tabulce, přidejte součásti uvedené v tabulce do souboru odpovědí tak, že kliknete pravým tlačítkem myši na součást a vyberete vhodný konfigurační průchod. Tím součást přidáte do konkrétního konfiguračního průchodu neboli fáze instalace systému Windows v souboru odpovědí. Všechna přidaná nastavení musí být zobrazena v podokně **Soubor odpovědí** sady Windows SIM. V části **Nastavení** vyberte požadované nastavení a ve sloupci vpravo, pak zadejte odpovídající hodnotu podle následující tabulky.

Tabulka 1. Konfigurační průchody.

Konfigurační průchod	Součást	Hodnota
1 WindowsPE	Microsoft-Windows-International-Core-WinPE	InputLocale = <i><národní prostředí></i> , například cs-CZ SystemLocale = <i><národní prostředí systému></i> , například cs-CZ UILanguage = <i><jazyk uživatelského rozhraní></i> , například cs-CZ UserLocale = <i><národní prostředí uživatele></i> , například cs-CZ
1 WindowsPE	Microsoft-Windows-International-Core-WinPE\SetupUILanguage	UILanguage = <i><jazyk uživatelského rozhraní></i> , například cs-CZ
1 WindowsPE	Microsoft-Windows-Setup\DiskConfiguration	WillShowUI = OnError
1 WindowsPE	Microsoft-Windows-Setup\DiskConfiguration\Disk	DiskID = 0 WillWipeDisk = true
1 WindowsPE	Microsoft-Windows-Setup\DiskConfiguration\Disk\CreatePartitions\CreatePartition	Order = 1 Type = Primary

1 WindowsPE	Microsoft-Windows-Setup\DiskConfiguration\Disk\ModifyPartitions\ModifyPartition	Active = true Format = NTFS Label = System Order = 1 PartitionID = 1
1 WindowsPE	Microsoft-Windows-Setup\ImageInstall\OSImage	InstallToAvailablePartition = false WillShowUI = OnError
1 WindowsPE	Microsoft-Windows-Setup\ImageInstall\OSImage\InstallTo	DiskID = 0 PartitionID = 1
1 WindowsPE	Microsoft-Windows-Setup\UserData	AcceptEula = true
1 WindowsPE	Microsoft-Windows-Setup\UserData\ProductKey	Key = < <i>kód Product Key</i> > WillShowUI = OnError
7 oobeSystem	Microsoft-Windows-Deployment\Reseal	ForceShutdownNow = false Mode = Audit
7 oobeSystem	Microsoft-Windows-Shell-Setup\OOBE	HideEULAPage = true ProtectYourPC = 3

Uvedené nastavení je modifikované oproti dokumentaci a je funkční, musíte si pouze vložit Váš kód Product Key do hodnoty Key v součásti Microsoft-Windows-Setup\UserData\ProductKey.

2.6.3 Ověření a uložení nastavení

V tomto kroku ověříte nastavení v souboru odpovědí a pak soubor uložíte (bez validního tvaru se soubor uložit nedá!) [10].

1. V programu Správce bitových kopií systému Windows klikněte v nabídce **Nástroje** na příkaz **Potvrdit soubor odpovědí**.
Hodnoty nastavené v souboru odpovědí budou porovnány s dostupnými hodnotami v bitové kopii systému Windows.
2. Pokud je soubor odpovědí úspěšně ověřen, zobrazí se v podokně **Zprávy** okna **Správce bitových kopií systému Windows** zpráva "Nejsou zobrazena žádná varování ani chyby". V opačném případě se v podokně **Zprávy** zobrazí chybové zprávy.
3. Dojde-li k chybě, přejděte na nesprávné nastavení dvojitým kliknutím na chybovou zprávu zobrazenou v podokně **Zprávy**. Opravte chybu změnou nastavení a proveďte nové ověření kliknutím na možnost **Potvrdit soubor odpovědí**. Tento krok opakujte, dokud se vám soubor odpovědí nepodaří úspěšně ověřit.
4. V nabídce **Soubor** klikněte na příkaz **Uložit soubor odpovědí**. Uložte soubor odpovědí pod názvem **Autounattend.xml**.
5. Zkopírujte soubor Autounattend.xml do kořenového adresáře jednotky USB flash.

Nyní máme základní soubor odpovědí, který automatizuje instalaci systému Windows. Tento soubor odpovědí nicméně díky zvolené strategii nasazení nevyužijeme, protože prvotní instalaci referenčního PC jsme již provedli a referenční PC je připravené.

2.7 Vytvoření referenční instalace - Sysprep

Pokud bychom využili souboru odpovědí při instalaci referenčního PC z bootovacího média DVD s operačním systémem Windows 7, měli bychom tento Soubor odpovědí na flash disku připojeného do USB portu a pomocí něho bychom provedli bezdotazovou instalaci systému referenčního PC.

Naši referenční instalaci vytvoříme na nainstalovaném počítači pomocí nástroje Sysprep [4].

Nástroj pro přípravu systému Sysprep.exe připravuje instalaci systému Windows na vytváření bitových kopií disků, testování systému nebo dodání zákazníkovi. Pomocí nástroje Sysprep lze z nainstalované bitové kopie systému Windows odstranit všechny systémové informace včetně identifikátoru zabezpečení (SID) počítače. Po odstranění jedinečných systémových informací z bitové kopie je možné zaznamenat bitovou kopii systému Windows pomocí samostatného nástroje jako je nástroj ImageX a potom ji použít k nasazení do více počítačů. Pomocí nástroje Sysprep lze navíc konfigurovat bitovou kopii systému Windows tak, aby se spustila v režimu auditování, případně aby bylo spuštěno uvítání systémem Windows. Režim auditování umožňuje testování integrity operačního systému a instalaci dalších aplikací a ovladačů zařízení. Uvítání systémem Windows vytváří první dojem koncového uživatele a umožňuje uživatelské nastavení systému Windows.

Sysprep spustíme s následujícími parametry z příkazové řádky:

```
c:\windows\system32\sysprep\>sysprep.exe /oobe /generalize /shutdown
```

Parametr /oobe spustí po restartu Uvítání systémem Windows, parametr /generalize odebere specifické informace o HW a /shutdown provede samotný restart.

2.8 Vytvoření spustitelného CD s prostředím WindowsPE + ImageX

V tomto kroku vytvoříte spustitelný disk RAM prostředí WindowsPE na disku CD-ROM pomocí skriptu Copype.cmd. Disk RAM prostředí WindowsPE umožňuje spustit počítač za účelem nasazení nebo zotavení. Spouštění disku RAM prostředí WindowsPE probíhá přímo do paměti, což umožňuje po spuštění počítače odebrat médium prostředí WindowsPE. Po spuštění prostředí WindowsPE můžete pomocí nástroje ImageX zachytávat, upravovat a používat diskové bitové kopie založené na souborech.

2.8.1 Vytvoření struktury CD

V Příkazovém řádku nástrojů pro nasazení z WAIK skriptem v CMD vytvoříme základní strukturu pro danou architekturu, kam skript nutné soubory překopíruje [9]:

```
C:\Program Files\Windows AIK\Tools\PETools>copype.cmd x86 c:\winpe_x86
```

Zkopírování nástroje ImageX do adresáře ISO:

```
c:\winpe_x86>copy "c:\Program Files\Windows AIK\Tools\x86\imagex.exe"  
c:\winpe_x86\iso
```

Nyní je potřeba ještě ručně (viz. popis možné chyby níže) překopírovat soubor winpe.wim do matrice bootovacího CD do podadresáře \source a přejmenovat na boot.wim. Pokud toto neprovedeme, nahlásí po bootování Windows Boot Manager chybu:

2.8.1.1 Chyba Windows Setup

Chyba návodu nebo skriptu ?

Při bootu z CD s WindowsPE nahlásí Windows Setup následující chybu Windows Boot Manageru:

WINDOWS BOOT MANAGER:

Windows failed to start. A recent hardware or software change might be the cause. To fix the problem:

- 1.Insert your Windows installation disc and restart the computer.
- 2.Choose your language settings, and then click "Next".
- 3.Click "Repair your computer."

If you do not have this disc, contact your system administrator or computer manufacturer for assistance.

Status: 0xc000000f

Info: The boot selection failed because a required device is inaccessible.

Po několikahodinovém prohledávání relevantních informací jsem zjistil na blogu v Technetu [11], jak situaci výše uvedeným způsobem řešit. U dokumentace - helpu Microsoft chybí buďto 2 řádky postupu nebo může být chyba ve skriptu, který tvoří strukturu CD.

2.8.2 Vytvoření bootovacího CD WindowsPE z .ISO obrazu

Po zdárné přípravě matrice CD vytvoříme bitovou kopii prostředí WindowsPE (.ISO) pomocí nástroje Oscdimg [9]:

```
c:\winpe_x86>oscdimg -n -bc:\winpe_x86\etfsboot.com c:\winpe_x86\ISO  
c:\winpe_x86\winpe_x86.iso
```

Náš image winpe_x86.iso bude mít velikost přibližně 143 MB. Pomocí SW pro vytváření bootovacích CD z .ISO souborů vytvoříme z image bootovací CD ROM médium s prostředím RAM WindowsPE a nástrojem ImageX.

Také je možná vhodné si uvědomit, že toto byl přípravný krok, který již příště nemusíme dělat – bootovací médium s prostředím WindowsPE pro systém Windows 7 již příště tvořit nemusíme. Může nám dobře sloužit i nadále.

2.9 Zachycení referenční instalace do bitové kopie a její sdílení v síti

2.9.1 Zachycení bitové kopie referenčního počítače

Referenční počítač spustíme z bootovacího média CD s prostředím WindowsPE. Po najetí se nám objeví příkazový řádek, kde zadáme tento příkaz, kterým zachytíme bitovou kopii referenční instalace [10]:

```
x:\imagex.exe /capture c: c:\imagew7.wim „Windows7“ /compress fast /verify
```

Jednorázové vytvoření image referenčního PC trvalo 11 minut 14 sekund. V jeho průběhu ještě dochází k vyjmutí některých složek a souborů, které se systémově váží k danému PC a na novém se automaticky vytvoří, např. \pagefile.sys, \hyberfil.sys, \Recycle.

2.9.2 Zkopírování bitové kopie do síťového umístění

Máme-li funkční síťové prostředí, tedy, běží-li služba DHCP, tak můžeme přímo přimapovat sdílený disk, který jsme si na serveru vytvořili a nastavili tam patřičná oprávnění, protože WindowsPE má zabudovanou síťovou podporu.

Síťový disk namapujeme příkazem:

```
net use y: \\fuzabnt3\img
```

A kopírování do síťového úložiště provedeme takto:

```
copy c:\imagew7.wim y:
```

Kopírování image o velikosti 3,1GB trvalo na 100 Mbit síti zhruba 2-3 minuty.

2.9.2.1 Nastavení kontextu sítě referenčního PC bez služby DHCP

Nemáme-li k dispozici funkční serverovou službu DHCP, musíme nastavit síťové prostředí v PC ručně změnou kontextu – zadáním postupně následujících příkazů:

netsh

interface

ipv4

set address „Připojení k místní síti“ static 172.31.xxx.yyy 255.255.255.0 172.31.xxx.zzz

Zadání IP je ve tvaru IP_adresa mezera maska mezera brána. Třetí a čtvrtý oktet (xxx, yyy a zzz) zadáte podle Vašich podmínek.

Poté je možné provést mapování sdílené složky a kopírování image do ní.

2.10 Nasazení bitové kopie do nového PC

Máme-li image referenční instalace nachystán v síťovém prostředí, můžeme provést jeho nasazení na cílový počítač, případně řadu cílových počítačů. Nejlepší výsledky práce dostaneme na hardwarově identických strojích s referenčním PC, minimální podmínkou je velikost disku, aby se tam obraz vlezl, jinak může hrát ještě roli, jaké parametry jsme použili (nebo nepoužili) u nástroje Sysprep.

V cílovém PC nastavíme bootování v BIOSu na CD mechaniku (opět krom jiných), uložíme nastavení, vložíme bootovací CD s prostředím WindowsPE a provedeme restart. Nabootujeme do WindowsPE, kde nejdříve pomocí nástroje DiskPart nakonfigurujeme disk – provádíme postupně tyto příkazy [10]:

diskpart

select disk 0

clean

create partition primary

select partition 1

format fs=ntfs label=“Win7“

assign letter=c

active

exit

Tato posloupnost příkazů by mohla být „univerzální“, neb clean smaže původní nastavení disku a následné příkazy vybudují vše znovu. Tady formátujeme klasickým formátem, tedy podle fyzické velikosti disku to může trvat.

Uložíme-li tyto příkazy do skriptu, který bude uložen spolu s bitovou kopií, můžeme volat DiskPart podle dokumentace následujícím způsobem:

```
diskpart /s <scriptname>.txt
```

Máme-li nachystaný disk cílového PC a funkční síťové prostředí, provedeme mapování a přikopírujeme na disk referenční image:

```
net use y: \\fuzabnt3\img
```

```
copy y:\imagew7.wim c:
```

Pomocí nástroje ImageX nasadíme bitovou kopii na pevný disk cílového PC:

```
d:\imagex.exe /apply c:\imagew7.wim 1 c:
```

Číslo 1 značí číslo image. Čas nasazení trval 5 minut 37 sekund.

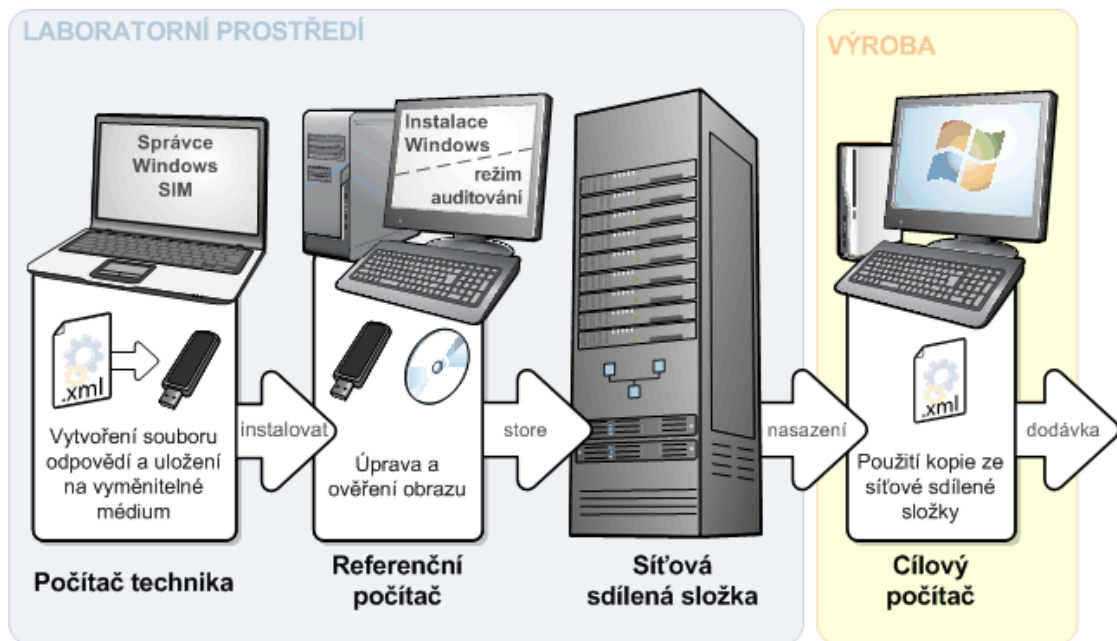
V poslední fázi nasazení použijeme nástroj BCDboot.exe – nástroj pro vytvoření a opravu spouštěcích konfiguračních souborů a jejich dat. Pomocí tohoto nástroje inicializujeme úložiště spouštěcích konfiguračních souborů a jejich dat a zkopírujeme do systémového oddílu soubory spouštěcího prostředí pomocí tohoto příkazu, kde preferujeme češtinu:

```
x:\windows\system32>bcdboot c:\windows /l cs-cz
```

Výstupem hlášky na příkazovém řádku: „Spouštěcí soubory byly úspěšně vytvořeny“ nasazení referenční bitové kopie na cílový počítač končí. Po restartu, vyjmutí bootovacího média s WindowsPE, najede počítač v identické podobě instalovaného operačního systému a aplikací referenčního počítače.

2.11 Scénář ze sítě

V rámci této bakalářské práce se dá říct, že kdyby bylo využito i Odpovědního souboru pro vytvoření referenční instalace, jednalo by se o typový Scénář se sítě ze sady WAIK, jehož implementaci popisuje graficky následující obrázek [9]:



Obrázek 8. Scénář WAIK ze sítě.

3 PERSONIFIKACE PC VYTVOŘENÉHO Z BITOVÉ KOPIE

Po nasazení bitové kopie z obrazu funkčního a nainstalovaného referenčního PC do nového počítače je nutné aplikovat bezpečnostní opatření, přihlásit se pod účtem lokálního administrátora a provést personifikaci počítače v síťovém prostředí. V prostředí naší organizace to znamená:

- Po spuštění PC změnit nastavení v BIOSu (krom jiných):
 - Nastavit bootování pouze z lokálního harddisku.
 - Aplikovat systémové heslo pro vstup do BIOSu.
 - Aplikovat uživatelské heslo pro spuštění a restart PC.
- Po přihlášení pod účtem lokálního administrátora:
 - Přiřadit pevnou IP adresu, zadat síťovou masku a bránu.
 - Při ručním zadání Proxy serveru je možné provést přegenerování Product Key a provést aktivaci systému pro legalizaci Microsoft Windows 7 Professional (jinak až ve chvíli aplikace GPO, kdy je PC pod správou GroupPolicy v Active Directory).
 - Provést změnu doménového jména PC (vyžaduje restart).
- Přihlášení pod účtem doménového administrátora:
 - Připojit PC do domény ZAB.
 - Přidat účet uživatele s právy Lokálního administrátora.
- V Active Directory přesunout PC z kontejneru Computers do Organizační jednotky zab.os.ds.mfcr.cz/FÚ v Zábřehu/Stanice pod správu GroupPolicy.
- V Symantec System Center Console přiřadit nové PC pod skupinovou správu Symantec Antivirus Serveru.
- Generování PCInfo ID identifikátoru a provedení SW auditu.
- Scan HW a SW PC pro Evidenci počítačů + naplnění sériových čísel komponent.
- Restart PC.

- Login jako uživatel s právy lokálního administrátora a skutečná personifikace pod jeho účtem v jeho profilu: tiskárny, chipové karty, ověření dostupnosti aplikací přes Internet Explorer (doinstalování ActiveX component), atd. Přikopírování jeho pracovních dat, oblíbených položek, nastavení poštovního klienta, apod. Po ukončení změna z lokálního administrátora na Standardního uživatele skupiny Users. Logout.
- Předání uživateli.

4 SHRUTÍ NASAZENÍ WINDOWS

Nákupy techniky v podmínkách naší organizace probíhají plánovaně a jsou v posledních letech dělány ve vlnách dodávek větších počtů kusů. Zaneprázdnění pracovníků IT řešící denní problémy je vytěžující a instalaci desítky, či několik desítek PC v jedné dodávce může narušit rutinní provoz a vyústit v problémy.

Čas věnovaný vytvoření nástroje bootovacího CD prostředí WindowsPE s nástrojem ImageX, instalace jednoho kusu referenčního PC, vytvoření image Sysprepem, kopie image do síťového úložiště a jeho následné instalace na jednotlivá PC může výrazným způsobem zrychlit nasazení Windows ve spolupráci se službami instalací SW a různých dalších nastavení z Active Directory pro všechny, tedy nové i již existující počítače.

Podle výsledku času instalace ze síťového úložiště, nezabere instalace včetně vybalení jednoho PC ani hodinu času. Při hromadném nasazení při instalaci nových PC připojených do sítě přes switch, lze jistě efektivitu výrazně zvýšit připojením a instalací více PC najednou.

Také je určitě rezerva v seskupení jednotlivých příkazů do „batáků“ – neboli dávkových command line souborů .cmd a také v DHCP (Dynamic Host Configuration Protocol serveru), který naše organizace z bezpečnostních důvodů nepoužívá, čím nemáme možnost získat IP ze sítě, ale nutno nastavit v PC. Tímto nemůžeme využívat bootování přímo ze síťových karet přes prostředí PXE ze sítě z RIS (na Windows Sever 2003), případně novějšího WDS (na Windows Server 2008) a vybrat nabízené bitové kopie systémů, ale musíme bootovat ze spustitelného média.

K sadě Windows AIK se dá říct, že se jedná o mocný nástroj pro lidi, kteří vědí proč a na co těchto utilit využít při administraci řad počítačů. Celkově se jedná o řešení, které Microsoft nabízí zdarma, a třeba pro státní organizace, které jsou pod bedlivým dohledem ohledně používaného SW a podléhají pravidelnému softwarovému auditu jako ta naše, to je velká výhoda.

Ohledně instalací obecně lze očekávat okamžik přechodu na platformu Microsoft Windows server 2008, kde je výkonný nástroj WDS.

ZÁVĚR

Svoji bakalářskou práci jsem pojal s cílem využití v naší organizaci a pro zlepšení své práce. Její téma mi umožnilo nahlédnout do další komnaty skutečné síťové administrace a nelituji úsilí a času, které jsem tomu věnoval. Práce ukazuje postupy s využitím Group Policy z Active Directory a ukazuje práci s nástroji ze sady WAIK.

Pevně věřím tomu, že současný trend ve vývoji IT bude pokračovat a bude nutné se umět přizpůsobit požadavkům na lepší funkčnost softwaru a jeho správy v počítačové síti. Urychlení nasazení systému Windows a moderní vzdálená správa instalací jednotlivých softwarových produktů tomu mohou pomoci.

Hlavním přínosem bude spokojený uživatel, který bude mít dostupné a funkční všechny potřebné utility a nástroje, a při dobrém zálohování jej ani závada v počítači, ani plánovaný upgrade PC a systému neomezí v práci mimo nezbytně krátkou dobu.

Celkovým výsledkem by mělo být uspoření času pro jeho další vhodné využití, protože technika by měla lidem především sloužit.

CONCLUSION

I conceive my thesis with the aim of usage in our organization and my work improvement. Its topic allowed me to have a look into another brunch of the real network administration and I do not regret the effort and the time I spent on it. Work shows how to use Group Policy from Active Directory and shows work from a set WAIK tools.

I firmly believe that the current trend in IT development will continue and it will be necessary to adapt oneself to demands for better functionality of the software and its management in a computer network. Faster setting of Windows system and advanced remote management of installings of single software products could help this.

The main benefit should be a satisfied user to whom all the necessary utilities and tools would be accessible and functional and on a good backup neither the fault of the computer nor the planned upgrade of the PC and the system should confine his work except for a very short urgent time.

The overall result points to the saving of time and its further suitable usage as the technics should be of service to the people, preferably of a really good service to them.

SEZNAM POUŽITÉ LITERATURY

- [1] WILLIAM, R. Staněk. Mistrovství v Microsoft Windows Server 2008 : Kompletní informační zdroj pro profesionály. 1. vyd. [s.l.] : Computer Press, a.s., 2009. 1364 s. Mistrovství v. Dostupný z WWW: <knihy.cpress.cz>. ISBN 978-80-251-2158-0.
- [2] CHARLIE, Russel, SHARON, Crawford. Microsoft Windows Server 2008 : Velký průvodce administrátora. 1. vyd. [s.l.] : Computer Press, a.s., 2009. 1271 s. Administrace. Dostupný z WWW: <knihy.cpress.cz>. ISBN 978-80-251-2115-3.
- [3] CHARLIE, Russel, SHARON, Crawford, JASNON, Gerend. Microsoft Windows Server 2003 : Velký průvodce administrátora. 1. vyd. [s.l.] : CP Books, a.s., 2005. 1374 s. Dostupný z WWW: <www.cpbooks.cz>. ISBN 80-251-0579-2.
- [4] [Http://technet.microsoft.com](http://technet.microsoft.com) [online]. Microsoft Corporation, c2010 , 2010 [cit. 2010-02-02]. Dostupný z WWW: <<http://http://technet.microsoft.com>>.
- [5] [Http://www.mstv.cz/](http://www.mstv.cz/) [online]. Microsoft, s.r.o., c2008 [cit. 2010-02-01]. Dostupný z WWW: <<http://www.mstv.cz/>>.
- [6] VÝŠEK, Onřej. Microsoft TechNet Blog CZ/SK [online]. 2009 [cit. 2010-05-06]. Windows 7: VHD boot a rychlost VHD. Dostupné z WWW: <<http://blogs.technet.com/technetczsk/archive/2009/03/19/windows-7-vhd-boot-rychlost-vhd-test-speed.aspx>>.
- [7] FLORIAN, Karel. Microsoft TechNet Blog CZ/SK [online]. 2009 [cit. 2010-05-06]. Užitka Disk2Vhd 1.3. Dostupné z WWW: <<http://blogs.technet.com/technetczsk/archive/2009/11/05/uzitka-disk2vhd-1-3.aspx>>.
- [8] POLZER, Jan Virtual PC 2007: kompletní návod. In . EXTRA Windows.cz : Extra Publishing s. r. o., 20. 10. 2008 [cit. 2010-05-06]. Dostupné z WWW: <<http://extrawindows.cnews.cz/virtual-pc-2007-kompletni-navod>>.
- [9] Microsoft Corporation. Uživatelská příručka sady Windows Automated Installation Kit (WAIK) pro Windows 7 [online]. [s.l.] : Microsoft Corporation, 2009 [cit. 2010-05-06]. Dostupné z WWW:

<<http://www.microsoft.com/downloads/details.aspx?familyID=f1bae135-4190-4d7c-b193-19123141edaa&displaylang=en>>.

- [10] Microsoft Corporation. Krok za krokem: Základní nasazení systému Windows pro profesionály IT [online]. [s.l.] : Microsoft Corporation, leden 2009 [cit. 2010-05-06]. Dostupné z WWW: <<http://www.microsoft.com/downloads/details.aspx?familyID=f1bae135-4190-4d7c-b193-19123141edaa&displaylang=en>>.
- [11] BERG, Richard, et al Booting to WinPE disc = 0xc000000f required device is inaccessible. In Booting to WinPE disc = 0xc000000f required device is inaccessible. Microsoft TechNet Windows Client TechCenter : Microsoft Corporation, 2009 [cit. 2010-05-06]. Dostupné z WWW: <<http://social.technet.microsoft.com/Forums/en/w7itproinstall/thread/89a1c2b3-db0d-48f6-84fb-88b201051233>>

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AC	Active directory.
ACT	Application Compatibility Toolkit.
ADIS	Automatizovaný daňový informační systém.
ADM	Administrativní šablona GPO.
ADML	Jazykový popis ADMX souborů.
ADMX	ADM soubory založené na XML.
AIX	Operační systém serveru společnosti IBM.
ATM	Asynchronous Transfer Mode.
BIOS	Basic Input-Output System.
BITS	Background Intelligent Transfer Service.
CAL	Client license.
CCTV	Closed-circuit television.
CD	Compact Disc.
CMD	Command line.
CPU	Central Processing Unit.
DFS	Distributed File System.
DHCP	Dynamic Host Configuration Protocol.
DNS	Domain Name System.
DSIM	Deployment Image Servicing and Management.
DVD	Digital Versatile Disc.
EPS	Elektronický požární/poplachový systém.
EULA	End-User License Agreement.
EZS	Elektronický zabezpečovací systém.
FC	Fibre channel.

GB	Giga byte.
Gbit	Giga bit.
GP	Group Policy.
GPC	Group policy container.
GPMC	Group policy management console.
GPO	Group Policy Object.
GTP	Group policy template.
HW	Hardware.
IP	Internet Protocol.
ISO	International Organization for Standardization.
IT	Information technology.
KB	Kilo byte.
LAN	Local Area Network.
LDAP	Lightweight Directory Access Protocol.
MAK	Multiple Activation Key.
MAP	Microsoft Assessment and Planning Toolkit.
MAP	Assessment and Planning Toolkit.
MB	Mega byte.
Mbit	Mega bit.
MDT	Microsoft Deployment Toolkit.
MF	Ministerstvo financí.
MMC	Microsoft Management Console.
MPLS	Multiprotocol Label Switching.
MS	Microsoft.
MSDN	Microsoft Development.

MSXML	Microsoft XML Core Services.
OU	Organizational unit.
PbTÚ	Pobočková telefonní ústředna.
PC	Personal Computer.
PXE	Preboot Execution Environment.
RAID	Redundant Array of Independent Disks.
RAM	Random Access Memory.
RIS	Remote Installation Services.
ROM	Read only.
RW	ReWritable.
SATA	Serial ATA.
SID	System identification.
SIM	System Image Manager.
SP	Service pack.
SUS	Software update services.
SW	Software.
T602	Text602.
TCP	Transmission Control Protocol.
ÚFO	Územní finanční orgán.
UPS	Uninterruptable Power Supply.
USB	Universal serial bus.
USMT	User State Migration Tool.
UTP	Unshielded Twisted Pair.
VA	Volt amper.
VAMT	Volume Activation Management Tool.

VPN	Virtual Private Network.
W	Watt.
WAIK	Windows Automated Installation Kit.
WAN	Wide area network.
WDS	Windows Deployment Services.
WHD	Virtual hard disk.
WIM	Windows imaging format.
WMI	Windows Management Instrumentation.
WSUS	Windows system update server.
XML	Extensible markup language.

SEZNAM OBRÁZKŮ

<i>Obrázek 1. LAN FÚ.</i>	15
<i>Obrázek 2. MMC konsole.</i>	21
<i>Obrázek 3. GPMC konsole.</i>	21
<i>Obrázek 4. Instalace s DHCP.</i>	28
<i>Obrázek 5. Soubor bitové kopie WIM.</i>	35
<i>Obrázek 6. Soubor odpovědí.</i>	37
<i>Obrázek 7. Nástroj SIM.</i>	38
<i>Obrázek 8. Scénář WAIK ze sítě.</i>	48

SEZNAM TABULEK

<i>Tabulka 1. Konfigurační průchody.</i>	<i>40</i>
---	-----------