

Migrace operačních systémů a jejich služeb malé podnikové sítě

Bc. Jan Plzák

Diplomová práce
2014



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

akademický rok: 2013/2014

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Bc. Jan Plzák**

Osobní číslo: **A12424**

Studijní program: **N3902 Inženýrská informatika**

Studijní obor: **Počítačové a komunikační systémy**

Forma studia: **prezenční**

Téma práce: **Migrace operačních systémů a jejich služeb malé podnikové sítě**

Téma anglicky: **The Migration of an Operating System and its Services in a Small Business Network**

Zásady pro vypracování:

1. Srovnejte stávající a nové operační systémy a popište výhody upgradu.
2. Analyzujte dané síťové prostředí a provedte SW audit.
3. Vypracujte harmonogram nasazení.
4. Popište jednotlivé služby serverového operačního systému.
5. Popište jednotlivé kroky migrace serverových a klientských stanic.
6. Analyzujte výsledné prostředí z hlediska bezpečnosti a přínosu firmě.

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **NORTHRUP, Anthony.** Mistrovství v Microsoft Windows 8. 1. vyd. Brno: Computer Press, 2013, 615 s. ISBN 978-80-251-4111-3.
2. **KRÁL, Mojmir a Petr SLAVÍK.** Windows 8: kompletní příručka. 1. vyd. Praha: Grada, 2013, 368 s. ISBN 978-80-247-4340-0.
3. **LYNN, Samara.** Windows server 2012: up and running. 1st ed. Sebastopol, CA: OReilly Media, 2012, xi, 243 pages. ISBN 14-493-2075-9.
4. **ZACKER, Craig.** Exam ref 70-410: installing and configuring Windows server 2012. Redmont, Washington: Microsoft Press, 2012, xiii, 384 pages. ISBN 978-073-5673-113.
5. **SOSINSKY, Barrie A.** Mistrovství - počítačové sítě: I vše, co potřebujete vědět o správě sítí. Vyd. 1. Brno: Computer Press, 2010, 840 s. ISBN 978-80-251-3363-7.

Vedoucí diplomové práce:

Ing. Jiří Korběl, Ph.D.

Ústav počítačových a komunikačních systémů

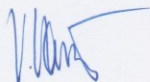
Datum zadání diplomové práce:

7. února 2014


Termín odevzdání diplomové práce:

27. května 2014

Ve Zlíně dne 7. února 2014



prof. Ing. Vladimír Vašek, CSc.
děkan



prof. Ing. Karel Vlček, CSc.
ředitel ústavu

ABSTRAKT

Cílem této diplomové práce je migrace serverového operačního systému Microsoft Windows Server 2003 R2 Standard Edition na Microsoft Windows Server 2012 R2 Standard Edition za použití virtualizace.

Teoretická část porovnává nové serverové a klientské operační systémy s těmi starými. Dále pak charakterizuje základní role a služby operačního systému Windows Server 2012 R2 a popisuje výhody softwarového auditu. Na závěr probírá jednotlivé migrační scénáře.

Praktická část sestavuje projektovou dokumentaci od swot analýzy po časový harmonogram nasazení nových systémů, analyzuje stávající síťové prostředí a provádí sw audit. Dále pak popisuje veškeré kroky od instalace nového serveru až po úplné odstavení toho starého. V závěru je hodnocen celkový přínos firmě po realizaci daného řešení.

Klíčová slova: Active Directory Domain Services, ESXi, File and Storage Services, DNS, DHCP, Migrace, SQL, SW audit, SWOT analýza, VMware, Windows Server.

ABSTRACT

The point of this thesis is the migration server operating system Microsoft Windows Server 2003 R2 Standard Edition to Microsoft Windows Server 2012 R2 Standard Edition with use of virtualization technologies.

The theoretical part compares the new server and client operating systems with the old ones. Follow-up to characterize the fundamental role and service operating system Windows Server 2012 R2 and describes the benefits of software audit. The conclusion discusses different migration scenarios.

The practical part consists of project documentation from swot analysis to a timetable for the deployment of new systems, analyzes the current network environment and performs sw audit. It describes all the steps of installing a new server to a complete shutdown of the old. In conclusion the overall benefit for company is evaluated after implementation of this solutions.

Keywords: Active Directory Domain Services, ESXi, File and Storage Services, DNS, DHCP, Migration, SQL, SW audit, SWOT analysis, VMware, Windows Server.

Rád bych poděkoval následujícím osobám:

Ing. Jiřímu Korbelovi, Ph.D., vedoucímu mé diplomové 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 diplomové/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 diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/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 diplomovou/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 - diplomovou/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 diplomové/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 diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/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 diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně

.....
podpis diplomanta

OBSAH

ÚVOD.....	12
I TEORETICKÁ ČÁST	13
1 WINDOWS 8.1	14
1.1 ZÁKLADNÍ POPIS SYSTÉMU	14
1.2 SROVNÁNÍ PODPORY PRO RODINU OPERAČNÍCH SYSTÉMŮ WINDOWS	14
1.3 SROVNÁNÍ BEZPEČNOSTI SE STARŠÍMI OPERAČNÍMI SYSTÉMY	15
1.4 VÝHODY UPGRADE	16
2 MICROSOFT WINDOWS SERVER 2012 R2.....	17
2.1 ZÁKLADNÍ POPIS SYSTÉMU	17
2.2 SROVNÁNÍ PODPORY PRO RODINU OPERAČNÍCH SYSTÉMŮ WINDOWS SERVER	17
2.3 PŘEHLED JEDNOTLIVÝCH EDIC RODINY WINDOWS SERVER 2012 R2	17
2.3.1 Srovnání funkcionalit jednotlivých síťových rolí mezi edicemi	19
2.3.2 Srovnání funkcionalit jednotlivých služeb mezi edicemi	20
2.4 SROVNÁNÍ WINDOWS 2012 R2 SE STARŠÍMI VERZEMI WINDOWS SERVER	21
2.5 LICENČNÍ POLITIKA.....	23
3 ROLE MICROSOFT WINDOWS SERVER 2012 R2	24
3.1 ACTIVE DIRECTORY CERTIFICATE SERVICES (AD CS)	24
3.1.1 Popis role.....	24
3.1.2 Praktické aplikace	24
3.2 ACTIVE DIRECTORY DOMAIN SERVICES (AD DS).....	25
3.2.1 Popis role.....	25
3.3 ACTIVE DIRECTORY FEDERATION SERVICES (AD FS).....	26
3.3.1 Popis role.....	26
3.3.2 Praktické aplikace	27
3.4 ACTIVE DIRECTORY LIGHTWEIGHT DIRECTORY SERVICES (AD LDS)	27
3.4.1 Popis role.....	27
3.4.2 Srovnání s AD DS	27
3.4.3 Aplikace pro práci s adresáři	28
3.5 ACTIVE DIRECTORY RIGHTS MANAGEMENT SERVICES (AD RMS).....	29
3.5.1 Popis role.....	29
3.5.2 Praktické aplikace	29
3.6 DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP).....	30
3.6.1 Popis	30
3.6.2 Praktické aplikace	31
3.7 DOMAIN NAME SYSTEM (DNS).....	31
3.7.1 Popis	31
3.7.2 Praktické aplikace	32

3.8	FAILOVER CLUSTERING	32
3.8.1	Popis role.....	32
3.8.2	Praktické aplikace	32
3.9	FILE AND STORAGE SERVICES	33
3.9.1	Popis role.....	33
3.9.2	Praktické aplikace	33
3.10	HYPER-V.....	33
3.10.1	Popis role.....	33
3.10.2	Praktické aplikace	34
3.11	PRINT AND DOCUMENT SERVICES	34
3.11.1	Popis role.....	34
3.11.2	Praktické aplikace	34
3.12	REMOTE DESKTOP SERVICES (RDS)	35
3.12.1	Popis role.....	35
3.12.2	Praktické aplikace	35
3.13	WEB SERVER (IIS 8)	35
3.13.1	Popis role.....	35
3.13.2	Praktické aplikace	36
3.14	WINDOWS DEPLOYMENT SERVICES (WDS)	36
3.14.1	Popis role.....	36
3.14.2	Praktické aplikace	36
3.15	WINDOWS SERVER UPDATE SERVICES (WSUS).....	37
3.15.1	Popis role.....	37
3.15.2	Praktické aplikace	37
4	SOFTWAREVÝ AUDIT	38
4.1	PRINCIP	38
4.2	PRŮBĚH.....	38
4.3	PŘÍNOSY PRO ORGANIZACI.....	39
4.4	PŘÍNOSY SW AUDITU PRO SPRÁVCE SÍŤE:	40
4.5	PŘÍNOSY SW AUDITU PRO ZAMĚSTNANCE	41
5	MIGRAČNÍ SCÉNÁŘE	42
5.1	WINDOWS SERVER 2012 R2.....	42
5.2	WINDOWS 8.1 PRO	43
5.3	INSTALACE Z MÉDIA	44
5.4	INSTALACE ZE SÍŤE	45
II	PRAKTICKÁ ČÁST	46
6	REALIZACE PROJEKTU.....	47

6.1	CÍL PROJEKTU.....	47
6.2	PROVEDITELNOST PROJEKTU	47
6.3	SWOT ANALÝZA.....	47
6.4	CENOVÁ KALKULACE PROJEKTU.....	49
6.5	ČASOVÝ HARMONOGRAM PROJEKTU	50
6.6	SHRnutí.....	52
7	ANALÝZA STÁVAJÍCÍHO SÍŤOVÉHO PROSTŘEDÍ.....	53
7.1	SÍŤOVÁ ARCHITEKTURA.....	53
7.2	SERVERY	53
7.2.1	IP adresní plán.....	55
7.2.2	Rozdělení aktivních prvků	55
7.2.3	Rozdělení LAN na VLANy.....	56
7.3	SÍŤOVÉ SLUŽBY	57
7.3.1	AD DS.....	57
7.3.2	Souborový server.....	58
7.3.3	Terminálový server.....	58
7.3.4	DNS.....	58
7.3.5	WSUS.....	58
7.3.6	DHCP.....	58
7.3.7	Databázový server	58
7.4	OSTATNÍ SLUŽBY	59
7.4.1	Centrální správa antiviru	59
7.4.2	Elektronická pošta	59
7.4.3	Docházkový systém.....	59
7.4.4	Informační systém	59
7.4.5	Centrální správa záložních zdrojů.....	59
7.4.6	Asset management.....	60
7.5	LICENČNÍ POLITIKA.....	60
7.6	OPERAČNÍ SYSTÉM KLIENŤSKÝCH STANIC	60
8	SW AUDIT.....	61
8.1	VÝSLEDKY	61
8.2	SHRnutí.....	62
9	INSTALACE A MIGRACE SERVERŮ	63
9.1	VMWARE ESXI.....	63
9.1.1	Předpoklady pro instalaci	63
9.1.2	Instalace.....	63
9.2	INSTALACE VMWARE VSPHERE KLIENTA	64
9.3	INSTALACE WINDOWS SERVER 2012 R2	65
9.3.1	Konfigurace virtuálního stroje	65
9.3.2	Instalace.....	66
9.3.3	Základní konfigurace.....	66

9.4	MIGRACE AD DS	67
9.4.1	Nastavení role řadiče domény	67
9.4.2	Přenos role Flexible Single Master Operations (FSMO)	68
9.4.3	Změna Master schématu.....	69
9.4.4	Odebrání serveru Windows 2003 R2 z Globálního katalogu.....	71
9.5	MIGRACE DHCP	71
9.5.1	Export DHCP databáze z Windows server 2003 R2.....	71
9.5.2	Import DHCP databáze na Windows Server 2012 R2	72
9.6	MIGRACE FILE SERVERU	73
9.6.1	Instalace Windows Server Migration Tools na Windows Server 2012 R2	73
9.6.2	Příprava balíčku nasazení pro zdrojový server.....	73
9.6.3	Migrace.....	73
9.7	MIGRACE SQL	74
9.7.1	Instalace SQL serveru.....	74
9.7.2	Migrace SQL serveru	75
9.8	INSTALACE OSTATNÍCH SLUŽEB A APLIKACÍ	75
9.8.1	ESET	75
9.8.2	Firemní aplikace.....	77
9.8.3	PowerChute Network Shutdown.....	77
9.8.4	RDS a WSUS	80
9.8.5	SysAid	80
9.9	FINÁLNÍ KONFIGURACE.....	81
9.9.1	Zálohování.....	81
10	MIGRACE KLIENSKÝCH STANIC	83
	ZÁVĚR	84
	SEZNAM POUŽITÉ LITERATURY.....	86
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK	89
	SEZNAM OBRÁZKŮ	92
	SEZNAM TABULEK.....	93

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.

Motivací této diplomové práce je prohloubení již nabytých teoretických i praktických znalostí funkcionalit serverových operačních systémů a Active Directory Domain Services (AD DS) a cílem práce je aplikovat získané vědomosti pro inovaci operačních systémů formou migrace s využitím virtualizace, zvýšení bezpečnosti a eliminace slabého článku ve formě nepodporovaných operačních systémů.

V úvodu teoretické části jsou popsány operační systémy Microsoft Windows 8.1 a Microsoft Windows server 2012 R2, v případě serverového systému jeho edice, licenční politika a serverové role a služby. Nadále je prezentována teorie o softwarovém auditu. Teoretickou část uzavírá kapitola, kde jsou nastíněny jednotlivé migrační scénáře pro klientský i serverový operační systém.

Praktická část v úvodu prezentuje projektovou část nasazení nových operačních systémů, včetně SWOT analýzy a kalkulaci investiční ceny projektu, analyzuje stav sítě firmy Vydos servis a.s. a provádí SW audit. Pokračuje instalací nového serveru, včetně řešení virtualizace a končí samotnou migrací jednotlivých rolí a služeb serverového operačního systému.

Závěr je věnován celkovému přínosu firmě po implementaci daného řešení.

I. TEORETICKÁ ČÁST

1 WINDOWS 8.1

1.1 Základní popis systému

Windows 8 přinesla velké změny na platformě operačního systému a uživatelského rozhraní, zejména pro zlepšení práce na dotykových zařízeních, kde Windows teď soutěží s mobilními operačními systémy jako Android a IOS. Nová platforma klade důraz na integraci se službami cloudu a dotykové ovládání. Přibylo i mnoho nových bezpečnostních prvků a snadné obnovení systému. Mezi nejdůležitější novinky patří: dlaždicové rozhraní nabídky start, podpora USB.3.0, vestavěný antivirus, Windows Store a podpora UEFI Secure Boot.

1.2 Srovnání podpory pro rodinu operačních systémů Windows

Každý produkt Windows má svůj životní cyklus. Ten začíná vydáním produktu a končí, když se produkt už nepodporuje. Znalost klíčových dat v tomto životním cyklu vám pomůže se kvalifikovaně rozhodnout, kdy upgradovat nebo provést jiné změny softwaru. Ukončení podpory označuje datum, kdy Microsoft přestane poskytovat automatické opravy, aktualizace nebo online technickou podporu. Bez podpory Microsoftu už nebudete dostávat aktualizace zabezpečení, které váš počítač chrání před nebezpečnými viry, spywarem a jiným škodlivým softwarem, který může odcizit vaše osobní údaje. Na následující tabulce je vidět, že oblíbený Windows XP končí a je nutné jej nahradit, pokud se nechcete vystavit potenciálnímu riziku ohrožení firemních dat:

Klientské operační systémy	Poslední aktualizace, nebo Service Pack	Ukončení hlavní fáze technické podpory	Ukončení rozšířené podpory
Windows XP	Service Pack 3	14. dubna 2009	8. dubna 2014
Windows Vista	Service Pack 2	10. dubna 2012	11. dubna 2017
Windows 7	Service Pack 1	13. ledna 2015	14. ledna 2020
Windows 8	Windows 8.1	9. ledna 2018	10. ledna 2023

Tabulka 1. Srovnání podpory operačních systémů Windows

1.3 Srovnání bezpečnosti se staršími operačními systémy

V následující tabulce je uveden výčet přidanych služeb zvyšujících bezpečnost operačního systému od Windows XP až po Windows 8:

Windows XP	Windows XP SP2	Windows Vista	Windows 7	Windows 8
Přihlášení (Ctrl+Alt+Del)	Address Space Layout Randomization (ASLR)	BitLocker	Vylepšený ASLR a DEP	UEFI (Secure Boot)
Kontrola přístupu	Data Execution Prevention (DEP)	Patchguard	Vylepšený IPsec stack	Firmware Based TPM
Uživatelské profily	Automatická aktualizace jako výchozí nastavení	Vylepšený ASLR a DEP	Managed Service Accounts	Trusted Boot (s ELAM)
Bezpečnostní zásady	Zapnutý firewall ve výchozím nastavení	Security Development Lifecycle (SDL)	Vylepšení UAC	Measured Boot a podpora Remote Attestation
Systém souborů Encrypting File System (EFS)	Windows Security Center	User Account Control (UAC)	Vylepšené auditování	Výrazná vylepšení ASLR a DEP
Podpora Smartcard a PKI	Podpora WPA	Digital Right Management	AppLocker	AppContainer
Windows Update		Internet Explorer Smart Screen Filter	BitLocker to Go	BitLocker: šifrování pouze použitého místa
		Vylepšení firewallu	Windows Biometric Service	Windows Store
		Požadavek na podepsané ovladače	Windows Action Center	Internet Explorer 10 (bez pluginů, vylepšení ochranných módů)
		Bezpečnostní funkce zapnuté ve výchozím nastavení	Windows Defender	Reputace aplikací součástí jádra systému
		Podpora TPM		Virtuální smartcard
		Windows Integrity Levels		Obrázkové heslo, PIN
				Dynamic Access Control
				Vestavěný antivirus

Tabulka 2. Srovnání bezpečnostních funkcí operačních systémů Windows

1.4 Výhody upgrade

- **Vylepšení v jádře** Novější verze Windows mají mnoho bezpečnostních vylepšení v jádře Windows. Díky tomu je pro útočníky těžší používat tradiční techniky hackingu, jako je buffer overflow nebo odhadnutí umístění kódu v paměti.
- **Ochrana před malwarem v reálném čase** Ve Windows 8 poskytuje Windows Defender ochranu v reálném čase před malwarem a potenciálně nevyžádaným softwarem.
- **Šifrování pomocí nástroje BitLocker** Tento nástroj, představený poprvé ve Windows Vista, umožňuje uživatelům a administrátorům šifrovat celé pevné disky a chránit tak data před neoprávněným přístupem v případě krádeže nebo ztráty počítače. Windows 7 poprvé přinesl nástroj BitLocker To Go, který umožňuje šifrovat přenosná média. Ve Windows 8 lze BitLocker snadněji nasadit a spravovat.
- **Řízení uživatelských účtů (User Account Control, UAC)** Bylo poprvé představeno ve Windows Vista, pomáhá zabraňovat neoprávněným změnám v počítači tím, že uživatelským účtům je uděleno oprávnění administrátora jen v nezbytně nutných situacích. UAC bylo dále vylepšeno ve Windows 7 a novějších systémech a přináší uživatelům vyšší komfort.
- **AppLocker** Nástroj poprvé představený ve Windows 7, mohou IT oddělení využít k zabránění spuštění programů podle flexibilních a propracovaných pravidel. Ve Windows 8 mohou navíc administrátoři kromě klasických desktopových aplikací omezit i aplikace z Windows Store.
- **UEFI Secure Boot** je funkce využívající hardware, která je dostupná na všech certifikovaných Windows 8 zařízeních. Zabraňuje spuštění neoprávněných operačních systémů nebo firmwaru a pomáhá tak chránit počítač před napadením škodlivým malwarem.
- **Trusted Boot** Tato funkce ve Windows 8 ověřuje integritu spouštěcích souborů Windows a zahrnuje funkci Early Launch AntiMalware (ELAM), která umožňuje spuštění antivirového programu před spuštěním ostatních programů. Tímto lze snížit riziko napadení rootkity.

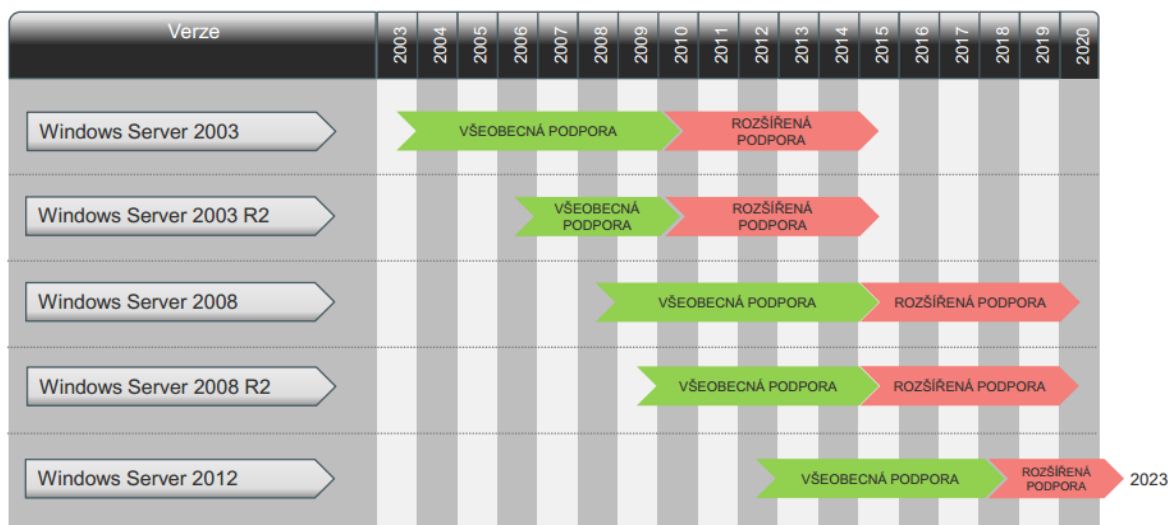
2 MICROSOFT WINDOWS SERVER 2012 R2

2.1 Základní popis systému

Windows Server 2012 R2 je pravděpodobně nejvýznamnější verze systému z rodiny Windows Server. Díky novému uživatelskému rozhraní, lepší podporou Windows PowerShell, možností instalace jako „Core“ verze bez GUI, dlouho očekávanou funkcí NIC Teaming, Storage Spaces v kombinaci s novým na chybu o mnoho odolnějším systémem souborů ReFS a stovky nových funkcí v oblasti sítí, práce s daty a virtualizace. Na rozdíl od svých předchůdců je systém od základu navržen pro budování veřejných i soukromých cloudových řešení.

2.2 Srovnání podpory pro rodinu operačních systémů Windows Server

Podobně jako Windows XP i Windows Server 2003 R2 má své datum „životnosti“, konec podpory byl stanoven na datum: 14.7.2015.



Obrázek 1. Srovnání podpory operačních systémů Windows Server

2.3 Přehled jednotlivých edic rodiny Windows server 2012 R2

Skupinu operačních systémů Windows Server 2012 R2 tvoří následující systémy, kde každá verze je určena ke konkrétnímu účelu:

- **Edice Windows Server 2012 R2 Datacenter** pro vysoce virtualizovaná privátní cloudová prostředí.

- **Edice Windows Server 2012 R2 Standard** lehce nebo pro zcela nevirtualizovaná prostředí.
- **Edice Windows Server 2012 R2 Essentials** malé firmy s maximálně 25 uživateli na serverech až se dvěma procesory.
- **Edice Windows Server 2012 R2 Foundation** malé firmy s maximálně 15 uživateli na serverech s jedním procesorem.

[4]

Základní rozdíly v možnostech připojení, licencování a maximálních HW parametrů jsou uvedeny v následující tabulce:

Specifikace	Datacenter	Standard	Essentials	Foundation
Distribuce	Volume licensing, OEM	Retail, volume licensing, OEM	Retail, volume licensing, OEM	Pouze OEM
Maximální počet uživatelů	Na základě počtu zakoupených licencí	Na základě počtu zakoupených licencí	25	15
Maximum SMB připojení	16,777,216	16,777,216	16777216	30
Maximum RRAS připojení	Neomezeně	Neomezeně	50	50
Maximum IAS připojení	2,147,483,647	2,147,483,647	50	10
Maximum procesorů	64	64	2	1
Maximum RAM	4 TB	4 TB	64 GB	32 GB
Server se může připojit do domény	Ano	Ano	Pouze k migraci	Pouze k migraci
DirectAccess	Ano	Ano	Omezeně	Ano
Možnost provozu VM	Neomezeně	2VMs	1 VM nebo 1 fyzický stroj, ne oba zároveň	Ne

Tabulka 3. Přehled rozdílů mezi jednotlivými edicemi

[5]

2.3.1 Srovnání funkcionalit jednotlivých síťových rolí mezi edicemi

Základní rozdíly ve srovnání jednotlivých síťových rolí mezi edicemi je uvedeno v následující tabulce:

Specifikace	Datacenter	Standard	Essentials	Foundation
Active Directory Certificate Services	Ano	Ano	Omezené	Omezené
Active Directory Domain Services	Ano	Ano	Musí být kořenový řadič domény	Musí být kořenový řadič domény
Active Directory Federation Services	Ano	Ano	Ano	Ano
AD Lightweight Directory Services	Ano	Ano	Ne	Ano
AD Rights Management Services	Ano	Ano	Ano	Ano
Application Server	Ano	Ano	Ano	Ano
DHCP Server	Ano	Ano	Ano	Ano
DNS Server	Ano	Ano	Ano	Ano
Fax Server	Ano	Ano	Ano	Ano
File Services	Ano	Ano	Ano	Ano
Hyper-V	Ano	Ano	Ne	Ne
Network Policy and Access Services	Ano	Ano	Ano	Ano
Print and Document Services	Ano	Ano	Ano	Ano
Remote Access	Ano	Ano	Ano	Ano
Terminal Services Application Sharing	Ano	Ano	Ne	Ano
Terminal Services Gateway	Ano	Ano	Ne	Ano
Web Services (IIS)	Ano	Ano	Ano	Ano
Windows Deployment Services	Ano	Ano	Ano	Ano
Windows Essentials	Ano	Ano	Default	Ne
Windows Media Services	Ano	Ano	Ano	Ano
WINS Server	Ano	Ano	Ano	Ano

Tabulka 4. Srovnání funkcionalit jednotlivých síťových rolí mezi edicemi

2.3.2 Srovnání funkcionalit jednotlivých služeb mezi edicemi

Základní rozdíly v jednotlivých službách mezi edicemi jsou uvedeny v následující tabulce:

Specifikace	Datacenter	Standard	Essentials	Foundation
RODC - read only domain controller	Ano	Ano	Ne	Ne
Automatic Virtual Machine Activation	Obojí jak hostitel, tak host	Pouze host	Pouze host	Ne
Best Practices Analyzer	Ano	Ano	Ano	Ano
BranchCache Hosted Server	Ano	Ano	Ano	Ano
BranchCache P2P Cache	Ano	Ano	Ano	Ano
Windows Control Panel	Ano	Ano	Ano	Ano
Distributed File System Replication	Ano	Ano	Ano	Ano
Data Deduplication	Ano	Ano	Ne	Ne
ISCSI target support	Ano	Ano	Ano	Ano
DirectAccess	Ano	Ano	Ano	Ano
Dynamic Memory (in virtualization)	Ano	Ano	Ano	Ne
Failover Clustering	Ano	Ano	Ne	Ne
"Hot" add/replace RAM	Ano	Ano	Ano	Ne
IPAM (IP Address Management)	Ano	Ano	Ano	Ano
Microsoft Management Console	Ano	Ano	Ano	Ano
Minimal Server Interface	Ano	Ano	Ne	Ne
Network Load Balancing	Ano	Ano	Ano	Ano
Support for Non-volatile Memory Express	Ano	Ano	Ano	Ano
Windows PowerShell	Ano	Ano	Ano	Ano
Server Core mode	Ano	Ano	Ne	Ne
Server license logging	Ano	Ano	Ano	Ano
Server Manager	Ano	Ano	Ano	Ano
SMB Direct and SMB over RDMA	Ano	Ano	Ano	Ano
Storage Management Service	Ano	Ano	Ano	Ano
Storage Spaces	Ano	Ano	Ano	Ano
Volume Activation Services	Ano	Ano	Ne	Ne
VSS (Volume Shadow Copy Service) integration	Ano	Ano	Ano	Ano
Windows Server Update Services	Ano	Ano	Ano	Ne

Tabulka 5. Srovnání funkcionalit jednotlivých služeb mezi edicemi

2.4 Srovnání Windows 2012 R2 se staršími verzemi Windows Server

V rámci rozsahu diplomové práce, nelze popsat všechny změny, vylepšení a změnu funkcionalit mezi staršími a novějšími verzemi operačního systému Windows Server, v následující tabulce jsou uvedeny ty podle Microsoftu nejzásadnější:

Specifikace	Windows Server 2003 R2 SP2	Windows 2008 R2 SP2	Windows 2012
Enterprise-class scale and performance	Podpora 64 logických procesorů (LP) a 1TB operační paměti (RAM)	Podpora to 256 LPs a 2 TB RAM Podporuje 64 LPs, 1 TB RAM, a 512 aktivních VM na Hyper-V hostu, hostovaná VM má přístup k 4 virtuálním procesorům 64GB RAM a 2TB virtuálním diskům. Cluster podporuje 16 nodů a 1000 VM.	Podpora to 640 LPs a 4 TB RAM Podporuje 320 LPs, 4 TB RAM, a 1024 aktivních VM na Hyper-V hostu, hostovaná VM má přístup k 64 virtuálním procesorům 1TB RAM a 64TB virtuálním diskům. Cluster podporuje 64 nodů a 4000 VM.
Shared-nothing live migration	Ne	Ne	Schopnost migrace virtuálních strojů mezi servery Hyper-V na jiné clusteru pouze pomocí připojení k síti Ethernet prakticky bez prostojů.
Hyper-V Network Virtualization	Ne	Ne	Schopnost izolovat síťový provoz z různých poboček, či zákazníků na sdílené infrastruktuře, se sníženou potřebou virtuálních lokálních sítí (VLAN) Schopnost přesouvat virtuální stroje podle potřeby v rámci virtuální infrastruktury, při současném zachování přiřazení k virtuální síti.
Hyper-V Replica	Ne	Ne	Virtuální disky jsou po síti replikovány na jiný Hyper-v server. V případě výpadku první instance je možné repliku nastartovat a pokračovat v chodu. Pomocí této technologie je možné také replikovat i řadiče domény

Úložiště souborů	SMB 1.0	SMB 2.0 pomocí řetězení dotazů rychlejší, odstranění velikosti omezení bloku.	Nový SMB 3.0 protokol s pomocí technologií SMB Direct a SMB Multichannel přinesl značné vylepšení výkonu a snížení pravděpodobnosti výpadku, zejména pro SQL a Hyper-V serverové služby.
Windows PowerShell 3.0	Podporuje více než 100 cmdletů	Podporuje více než 200 cmdletů	Podporuje více než 2300 cmdletů
Hybridní aplikace	Je zapotřebí virtuální privátní síť (VPN)	Je zapotřebí virtuální privátní síť (VPN)	Jednotná správa aplikací. Flexibilita sestavit a nasadit hybridní aplikace jak u uživatele, tak v cloudu.
Velké webové portály	Postrádá izolaci a správu systémových prostředků	Základní možnosti izolace a správy systémových prostředků.	Rozsáhlá podpora webových aplikací a "cloud-based" strategií, sandboxing, lepší využití HW zdrojů.
Simplified, feature-rich Virtual Desktop Infrastructure (VDI)	Ne	Ano	Vylepšené způsoby zjednodušení a urychlení úlohy nasazení a správy pro správce IT. Jednotná konzole pro virtuální plochy a aplikace RemoteApp. Zjednodušená tvorba, přiřazení a oprava virtuálních ploch.
Dynamic Access Control	Ne	Ne	Nové způsoby pro kontrolu přístupu datům a lepší dodržování předpisů Nová generace autorizace a auditování. Možnosti klasifikace pro použití správy informací k nestrukturalizovaných dat na souborových serverech.

Tabulka 6. Srovnání zásadních změn mezi generacemi systému Windows Server

2.5 Licenční politika

K používání systému Microsoft Windows server 2012 R2 (vyjma edic Essentials a Foundation) 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 neekonomičtější 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.

3 ROLE MICROSOFT WINDOWS SERVER 2012 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:

3.1 Active Directory Certificate Services (AD CS)

3.1.1 Popis role

AD CS poskytuje přizpůsobitelné služby pro vystavování a správu digitálních certifikátů v systémech softwarového zabezpečení založených na technologii veřejných klíčů.

Digitální certifikáty, které poskytuje služba AD CS slouží k šifrování a digitálnímu podpisu elektronických dokumentů a zpráv. Tyto digitální certifikáty lze použít k ověření počítače, uživatele nebo zařízení účty v síti. Digitální certifikáty se používají k zajištění:

- Důvěrnosti prostřednictvím šifrování
- Integrity prostřednictvím digitálních podpisů
- Ověření sdružením klíče certifikátu s účty počítače, uživatele nebo zařízení v počítačové síti

3.1.2 Praktické aplikace

Službu AD CS můžete použít ke zvýšení zabezpečení tak, že identitu osoby, zařízení nebo služby spojí s odpovídajícím privátním klíčem. Služba AD CS rovněž zahrnuje funkce, které umožňují spravovat zápis a odvolání certifikátu v různých škálovatelných prostředích.

Mezi aplikace podporované službou AD CS patří Secure/Multipurpose Internet Mail Extensions (S/MIME), zabezpečené bezdrátové sítě, virtuální privátní sítě (VPN), Internet protokol IPsec (IPsec), systém souborů EFS (ENCRYPTING File System), přihlašování pomocí čipové karty, Secure Socket Layer/Transport Layer Security (SSL/TLS) a digitální podpisy.

3.2 Active Directory Domain Services (AD DS)

3.2.1 Popis role

Pomocí role serveru služby AD DS, můžete vytvářet škálovatelné, zabezpečenou a spravovatelnou infrastrukturu pro správu uživatelů a prostředků a poskytovat podporu pro práci s adresáři aplikace, například Microsoft Exchange Server.

AD DS poskytuje distribuovanou databázi, která ukládá a spravuje informace o síťových prostředcích a specifická data z aplikací pracujících s adresářem. Server se službou AD DS se nazývá řadič domény. Správci mohou pomocí služby AD DS uspořádat prvky sítě, například uživatele, počítače a další zařízení, do hierarchické kontejnerové struktury. Hierarchická Kontejnerová struktura zahrnuje doménovou strukturu služby Active Directory, domény v doménové struktuře a organizační jednotky (OU) v každé doméně.

Uspořádání prvků sítě do hierarchické kontejnerové struktury přináší následující výhody:

- Les jako bezpečnostní hranice organizace a definuje rozsah oprávnění pro správce. Ve výchozím nastavení obsahuje doménová struktura jedinou doménu, která se nazývá kořenová doména doménové struktury.
- Lze vytvořit další domény v doménové struktuře na oddíly údaje služby AD DS, která umožňuje organizacím k replikaci dat pouze kde je to potřeba. Díky tomu je možné pro službu AD DS škálovat globálně v síti, která má omezené dostupné šířky pásma. Domény služby Active Directory také podporuje řadu dalších základních funkcí, které se týkají správy, včetně identity uživatele celé sítě, ověřování a vztahy důvěryhodnosti.
- Organizační jednotky zjednoduší delegováním pravomocí usnadňuje správu velkého počtu objektů. Prostřednictvím delegování majitelé mohou přenášet úplné nebo omezené oprávnění objektů jiným uživatelům nebo skupinám. Delegování je důležité, protože pomáhá distribuovat správu velkého počtu objektů k počtu lidí, kteří získali důvěru k provádění úkolů správy.

Bezpečnost je integrována se službou AD DS prostřednictvím přihlašovací ověřování a řízení přístupu k prostředkům v adresáři.

S jediného přihlášení správci mohou spravovat data adresáře a organizace jejich sítě. Oprávnění uživatelé sítě lze také použít jediného přihlášení k síti přistupovat k prostředkům kdekoli v síti. Správa na základě zásad usnadňuje řízení i té nejsložitější sítě.

Mezi další služby AD DS patří následující:

- Soubor pravidel, schématu, který definuje třídy objektů a atributů, které jsou obsaženy v adresáři, omezení a limitů na instance těchto objektů a formát jejich jména.
- Globální katalog, který obsahuje informace o všech objektů v adresáři. Uživatelé a správci mohou pomocí globálního katalogu k nalezení informací adresáře, bez ohledu na které domény v adresáři skutečně obsahuje data.
- Dotaz a indexu mechanismus, takže to objekty a jejich vlastnosti lze publikovat a vyhledávat uživatele sítě nebo aplikacemi.
- Služba replikace, která distribuuje data adresáře v síti. Všechny nenasazuje řadiče domény v doméně účastnit replikace a obsahovat úplnou kopii všech informací adresáře pro svou doménu. Všechny změny dat adresáře je replikována do všech řadičů domény v doméně.
- Role hlavního operačního serveru (označované také jako flexible single master operations, neboli FSMO). Řadiče domény, které obsahují operace role hlavního operačního serveru, jsou určeny k provádění konkrétních úkolů k zajištění konzistence a odstranění konfliktních položek v adresáři.

3.3 Active Directory Federation Services (AD FS)

3.3.1 Popis role

Služba AD FS pomáhá používat jednotné přihlášení (SSO) k ověřování uživatelů pro více souvisejících webových aplikací v průběhu životnosti jedné online relace. Služba AD FS toho dosahuje zabezpečeným sdílením digitální identity a oprávnění přes hranice zabezpečení a rozlehlé sítě.

3.3.2 Praktické aplikace

AD FS zjednodušuje přístup koncových uživatelů systémů a aplikací pomocí mechanismu autorizace přístupu založeného na nárocích pro zachování bezpečnosti aplikací. Nasazením služby AD FS lze:

- Poskytnout zaměstnancům nebo zákazníkům okamžitý přístup k webovým prostředkům v jakékoliv organizaci partnera federace na internetu bez nutnosti vícenásobného přihlášení.
- Zachovat úplnou kontrolu identity nad vašimi zaměstnanci nebo zákazníky bez použití jiných přihlášení zprostředkovatele (Windows Live ID, Liberty Alliance a další).
- Poskytnout zaměstnancům nebo zákazníkům zkušenosti SSO založeného na webu, když potřebují vzdálený přístup k vnitřně hostovaným webovým stránkám, nebo službám.

3.4 Active Directory Lightweight Directory Services (AD LDS)

3.4.1 Popis role

Službu AD LDS vyvinula společnost Microsoft pro organizace, jež vyžadují flexibilní podporu pro aplikace pro práci s adresáři. Služba AD LDS je adresářová služba využívající protokol LDAP (Lightweight Directory Access Protocol).

Služba AD LDS zajišťuje ukládání a načítání dat pro aplikace pro práci s adresáři, a to bez závislostí, jež jsou vyžadovány pro službu AD DS. Služba AD LDS zajišťuje v podstatě podobné funkce jako služba AD DS, nevyžaduje však nasazení domén ani řadičů domén. V jednom počítači lze současně spustit několik instancí služby AD LDS s nezávisle spravovaným schématem pro každou instanci služby AD LDS.

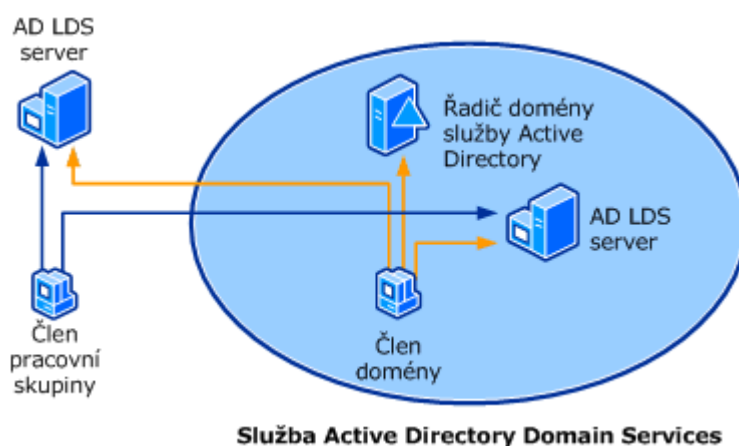
3.4.2 Srovnání s AD DS

Díky službě AD LDS nabízí společnost Microsoft možnost výběru adresářové služby. Služby AD LDS a AD DS jsou založeny na stejných základních technologiích adresářových služeb společnosti Microsoft, jsou však určeny pro různé potřeby v rámci organizace.

Služba AD DS zajišťuje adresářové služby pro operační systém Windows Server i pro aplikace pro práci s adresáři. Pro operační systém serveru ukládá služba AD DS důležité informace o síťové infrastruktuře, uživateli a skupinách, síťových službách atd. V této roli musí služba AD DS v celé doménové struktuře používat jediné schéma.

Služba AD LDS zajišťuje adresářové služby speciálně pro aplikace pro práci s adresáři. Služba AD LDS nevyžaduje ani nevyužívá domény nebo doménové struktury služby AD DS. V prostředích, ve kterých existuje služba AD DS, však může služba AD LDS využívat službu AD DS k ověřování objektů zabezpečení systému Windows.

Služby AD LDS a AD DS mohou být spuštěny souběžně ve stejné síti. Služba AD LDS navíc podporuje současně uživatele domény i pracovní skupiny, jak je vidět na následujícím obrázku.



Obrázek 2. Ukázka kombinace ADDS a AD LDS

3.4.3 Aplikace pro práci s adresáři

Aplikace pro práci s adresáři využívá místo (nebo kromě) databáze, souboru s prostým textem či jiné struktury úložiště k ukládání svých dat adresář. Řada dodávaných aplikací i řada uživatelsky vytvořených aplikací využívá k ukládání dat adresáře. Jako příklady typů aplikací, které často využívají k ukládání dat adresáře, lze uvést aplikace pro řízení vztahů se zákazníky (CRM - Customer Relationship Management), aplikace pro správu lidských zdrojů (HR - Human Resources) a aplikace globálního adresáře.

Adresářové služby (například služba AD LDS) i relační databáze zajišťují ukládání a načítání dat, liší se však optimalizací. Adresářové služby jsou optimalizovány pro zpracování čtení, zatímco relační databáze jsou optimalizovány pro zpracování transakcí. Obecně platí, že byste měli zvážit implementaci adresářové služby,

pokud příslušná aplikace čte data častěji, než je zapisuje. Implementaci relační databáze zvažte v případě, že příslušná aplikace zapisuje nebo upravuje data častěji, než je čte.

Kromě toho adresářové služby poskytují rovněž takové výhody, jako jsou distribuovaná architektura (návrh více hlavních serverů, replikace a geografická škálovatelnost), úložiště dat identit, jež je společné pro aplikace a platformy v celé organizaci, flexibilní schéma dat a přesně definované zásady přístupu.

3.5 Active Directory Rights Management Services (AD RMS)

3.5.1 Popis role

AD RMS umožňuje rozšířit bezpečnostní strategie dokumentů pro vaši organizaci pomocí Správy informačních práv (IRM).

Též umožňuje jednotlivcům a správci prostřednictvím IRM politik určit přístupová oprávnění pro dokumenty, sešity a prezentace. To pomáhá zabránit úniku citlivých informací - tisku, předávání nebo přeposíláním neoprávněnými uživateli.

Omezení přístupu a využití jsou vynuceny bez ohledu na to, kde je informace, protože oprávnění k souboru je uloženo v samotném souboru dokumentu.

AD RMS a IRM pomáhají jednotlivcům uplatňovat osobní požadavky týkající se přenosu osobních nebo soukromých informací. Také pomáhají organizacím uplatňovat podnikové zásady a rozšiřování důvěrných nebo chráněných informací.

3.5.2 Praktické aplikace

Řešení technologie IRM, které AD RMS umožňuje, se používají k pomoci zajistit následující:

- Trvalých zásad použití, které zůstávají spojeny s informacemi bez ohledu na to, kde se pohybují, odesílají, nebo předávají.
- Další úroveň soukromí k ochraně citlivých informací - například finanční výkazy, specifikace produktů, zákaznická data a důvěrné e-mailové zprávy, které se mohou úmyslně, nebo náhodou dostat do nepovolaných rukou.

- Zabránit oprávněnému příjemci obsahu s omezeným přístupem k předávání, kopírování, úpravě, tisku, faxování nebo vložení obsahu.
- Obsahu s omezeným přístupem zabránit kopírování v Microsoft Windows pomocí funkce Print Screen.
- Podporovat vypršení platnosti souboru, aby obsah dokumentů nebylo možné zobrazit po určeném časové období.
- Uplatňovat podnikové zásady, které řídí používání a distribuci obsahu uvnitř podniku.

Řešení založená na technologii IRM, které AD RMS podporuje, nemůže zabránit všem typům hrozeb pro bezpečnost citlivých dokumentů. Zde jsou uvedeny příklady bezpečnostních hrozeb pro dokumenty, které AD RMS nemůže řešit, či zmírnit:

- Vymazání obsahu, krádeži, zachycení škodlivými programy, jako jsou trojské koně, zaznamenávající úhozy kláves, nebo některé druhy spywaru.
- Ztrátě nebo poškození způsobenému počítačovými viry
- Obsah s omezeným přístupem, který je ručně zkopírován, nebo přepsán z obrazovky.
- Pořízení digitální fotografie obsahu.
- Zkopírování obsahu pomocí programů pro zachycení obrazovky třetích stran.

3.6 Dynamic Host Configuration Protocol (DHCP)

3.6.1 Popis

Protokol DHCP je standard protokolu IP, jehož cílem je zjednodušit správu konfigurace adres pomocí serveru, který centrálně spravuje adresy IP a související konfigurační data. Máte-li v úmyslu provádět přidělování adres vícesměrového vysílání a dynamicky získávat adresy IP klientů a související parametry konfigurace, nastavte tento server jako server DHCP.

3.6.2 Praktické aplikace

Po nakonfigurování role serveru DHCP lze provádět následující činnosti:

- Můžete centrálně spravovat adresy IP a související informace.
- Protokol DHCP zabraňuje vzniku konfliktů adres způsobených tím, že dříve přiřazená adresa IP je znovu použita při konfiguraci nového počítače v síti.
- Server DHCP lze nakonfigurovat tak, aby během přiřazování zapůjčení adres poskytoval úplný rozsah dalších konfigurační hodnot. Tímto způsobem se výrazně sníží čas potřebný ke konfiguraci či změně konfigurace počítačů v síti.
- Proces obnovení zapůjčení adresy DHCP rovněž zajišťuje, aby v případě potřeby častých aktualizací konfigurace klienta (například uživatelů s mobilními, nebo přenosnými počítači, jejichž umístění se často mění) byly tyto aktualizace prováděny efektivně a automaticky klienty, kteří komunikují přímo se serverem DHCP.

3.7 Domain Name System (DNS)

3.7.1 Popis

Server DNS zajišťuje překlad adres IP pro síť na základě protokolu TCP/IP. Umožňuje tedy uživatelům klientských počítačů používat k identifikaci vzdálených hostitelů názvy místo číselných adres IP. Klientský počítač odešle název vzdáleného hostitele na server DNS, který odpoví poskytnutím odpovídající adresy IP. Klientský počítač může poté odeslat zprávy přímo na adresu IP vzdáleného hostitele. Pokud nemá server DNS pro vzdáleného hostitele položku ve své databázi, může odpovědět klientovi adresou serveru DNS, který bude pravděpodobně mít informaci o daném vzdáleném hostiteli, nebo může sám zadat dotaz na daný jiný server DNS. Tento proces může probíhat rekurzivně, dokud klientský počítač neobdrží adresu IP nebo dokud se nestanoví, že dotazovaný název nepatří k hostiteli v rámci konkrétního oboru názvů DNS.

3.7.2 Praktické aplikace

Po nakonfigurování role serveru DNS lze provádět následující činnosti:

- Server může plnit funkci hostitele záznamů distribuované databáze DNS a používat tyto záznamy k odpovídání na dotazy DNS odeslané klientskými počítači služby DNS, například dotazy na názvy webových serverů nebo počítačů v síti nebo v Internetu.
- Lze pojmenovávat a vyhledávat síťové prostředky pomocí popisných názvů.
- Můžete řídit překládání názvů v každém segmentu sítě a replikovat změny do celé sítě nebo globálně v Internetu.
- Dynamickou aktualizací informací systému DNS lze omezit správu služby DNS.

3.8 Failover Clustering

3.8.1 Popis role

Failover cluster je skupina nezávislých počítačů, které pracují společně na zvýšení dostupnosti a škálovatelnosti clusterovaných rolí. Clustery serverů (nazývané nody) jsou připojeny kabely a softwarově. Pokud jeden nebo více nodů clusteru selžou, ostatní nody začínají poskytovat službu (proces je známý jako převzetí služeb při selhání). Jednotlivé role clusteru jsou navíc aktivně monitorovány a ověřovány, zdali správně pracují. Pokud nefungují, jsou restartovány nebo přesunuty do jiného nodu. Failover clustery poskytují také funkci Cluster Shared Volume (CSV), která poskytuje konzistentní a distribuovaný obor názvů, který jednotlivým rolím clusteru slouží k přístupu k sdílenému úložišti ze všech uzlů. Díky funkci Failover Clustering se uživatelé zažívají nejméně závad v provozu.

3.8.2 Praktické aplikace

- Vysoce dostupné nebo nepřetržitě k dispozici sdílené úložiště pro aplikace, například Microsoft SQL Server a technologie Hyper-V virtuálních strojů.
- Vysoce dostupné role clusteru spuštěné na fyzických serverech nebo na virtuálních strojích, které jsou nainstalovány na serverech se spuštěnou službou Hyper-V.

3.9 File and Storage Services

3.9.1 Popis role

File and Storage Services zahrnuje technologie, které vám pomohou nastavit a spravovat jeden nebo více souborových serverů, jenž jsou servery, které poskytují centrální umístění v síti, kde můžete ukládat soubory a sdílet je s uživateli a případně je centrálně spravovat a zálohovat.

3.9.2 Praktické aplikace

Správci mohou pomocí role File and Storage Services nastavit a spravovat více souborových serverů a jejich ukládání pomocí Správce serveru nebo Windows PowerShell. Některé z konkrétních aplikací jsou následující:

- Použití deduplikace dat za účelem snížení nákladů na výslednou kapacitu.
- Použití iSCSI serveru k vytvoření centralizované, softwarově a hardwarově nezávislý iSCSI diskový subsystém v Storage Area Network (SAN).
- Použití Storage Spaces, jenž umožňuje rozšíření pomocí cenově dostupných standardních disků.
- Pomocí Správce serveru vzdáleně spravovat více souborových serverů z jediného okna.
- Použití Windows PowerShell k automatizaci správy většiny úloh správy pro souborové servery.

3.10 Hyper-V

3.10.1 Popis role

Technologie Hyper-V virtualizuje hardware za účelem poskytovat prostředí, ve kterém lze provozovat více operačních systémů současně na jednom fyzickém počítači. Hyper-V umožňuje vytvářet a spravovat virtuální stroje a jejich zdroje. Každý virtuální stroj je izolovaný, virtualizovaný počítačový systém, který může spustit svůj vlastní operační systém. Operační systém, který běží ve virtuálním stroji se nazývá hostovaný operační systém.

3.10.2 Praktické aplikace

Hyper-V poskytuje infrastrukturu, takže si můžete virtualizovat aplikace a pracovní vytížení na podporu různých obchodních cílů zaměřených na zvyšování efektivity a snížení nákladů, jako jsou například:

- Zvýšení využití hardwaru. Konsolidací serverů na méně výkonnějších fyzických počítačů můžete snížit spotřebu zdrojů.
- Zlepšení obchodní kontinuity. Hyper-V může pomoci minimalizovat dopad i plánované a neplánované prostoje zatížení.
- Zvýšení efektivity v oblasti vývoje a testovacích aktivit. Můžete použít virtuální stroje na reprodukci různých výpočetních prostředí bez nutnosti nabytí hardware, který by byl jinak potřeba

3.11 Print and Document Services

3.11.1 Popis role

Print and Document Services umožňuje sdílení tiskáren v síti a centralizaci správy tiskových serverů a síťových tiskáren. S touto rolí můžete také získávat naskenované dokumenty ze síťových skenerů a dokumenty směřovat do sdíleného síťového adresáře, webové služby Windows SharePoint Services nebo e-mailové adresy.

Faxový Server odesílá a přijímá faxové zprávy a umožňuje spravovat faxové úlohy, nastavení, zprávy a faxová zařízení na faxovém serveru.

3.11.2 Praktické aplikace

Tiskový Server umožňuje sledovat tiskové fronty a dostávat upozornění na zpracování tiskové úlohy. Také umožňuje migraci tiskových serverů a připojení tiskáren pomocí zásad skupiny.

Distribuovaný skenovací server poskytuje službu, která přijímá naskenované dokumenty ze síťových skenerů a směřuje je na správné cíle. Zahrnuje také modul snap-in Správa skenování, který slouží ke správě síťových skenerů a nastavení procesů skenování.

Pomocí Správce služby Fax můžete automaticky zpřístupnit faxové spojení na uživatele a počítače v organizaci.

3.12 Remote Desktop Services (RDS)

3.12.1 Popis role

Role Vzdálená plocha v systému Windows Server 2012 R2 poskytuje technologie, které umožňují uživatelům připojit se k relaci vzdálené plochy, případně aplikaci RemoteApp a to za pomoci podnikové sítě, nebo Internetu.

3.12.2 Praktické aplikace

Služba Vzdálená plocha umožňuje pracovníkům pracovat kdekoliv. Některé z hlavních výhod služby Vzdálená plocha v systému Windows Server 2012 R2 jsou:

- **Sjednocená správa** - lze spravovat relace a virtuální plochy, konfigurovat aplikace RemoteApp z jedné centrální konzole.
- **Uživatelské přizpůsobení** - lze zachovat jednotné uživatelské rozhraní.
- **Levnější úložiště** - v rámci relace vzdálené plochy lze kombinovat lokální i vzdálené úložiště a tím ušetřit místo na disku.

3.13 Web server (IIS 8)

3.13.1 Popis role

Role webového serveru (IIS) v systému Windows Server 2012 poskytuje bezpečnou, snadno spravovatelnou, modulární a rozšiřitelnou platformu pro spolehlivé hostování webů, služeb a aplikací. Služba IIS 8 umožňuje sdílet informace s uživateli přes Internet, intranet a extranet. Služba IIS 8 je jednotná webová platforma, do které jsou integrovány technologie IIS a ASP.NET, služby FTP, jazyk PHP a technologie Windows Communication Foundation (WCF).

3.13.2 Praktické aplikace

Správci mohou používat roli webového serveru (IIS) k nastavení a správě většího množství webů, webových aplikací a serverů FTP. Mezi charakteristické funkce patří:

- Pomocí modulu Správce služby IIS lze konfigurovat funkce služby IIS a spravovat weby.
- Pomocí protokolu FTP (File Transfer Protocol) lze povolit vlastníkům webů odesílání a stahování souborů.
- Pomocí izolace webů lze zamezit vzájemnému rušení mezi weby na serveru.
- Je možné konfigurovat webové aplikace napsané různými technologiemi, například klasickou technologií ASP, technologií ASP.NET nebo v jazyce PHP.
- Pomocí prostředí Windows PowerShell lze automatizovat provádění většiny úloh správy webového serveru.
- Můžete nakonfigurovat více webových serverů do jedné serverové farmy, kterou lze spravovat pomocí služby IIS.
- Můžete využít všechny výhody hardwaru NUMA a získat optimální výkon serveru podporujícího platformu NUMA.

3.14 Windows Deployment Services (WDS)

3.14.1 Popis role

WDS umožňuje nasazení operačních systémů Windows prostřednictvím sítě, což znamená, že není třeba instalovat každý operační systém přímo z disku CD nebo DVD.

3.14.2 Praktické aplikace

- Umožňuje síťové instalace operačních systémů Windows, která snižuje složitost a náklady ve srovnání s ručními instalacemi.
- Podporuje smíšená prostředí systémů Windows XP a Windows Server 2003 až po Windows 8.1 a Windows Server 2012 R2.

- Používá standardní technologie instalace systému Windows, včetně prostředí Windows Preinstallation Environment (Windows PE), souborů WIM a instalace pomocí bitových kopií.
- Přenáší data a obrázky pomocí funkce vícesměrového vysílání.
- Umožňuje vytvářet bitové kopie referenčních počítačů pomocí Průvodce vytvořením bitové kopie, což je alternativa k nástroji ImageX.
- Můžete na server přidat balíčky ovladačů, konfigurovat je a nasadit do klientských počítačů s pomocí instalační bitové kopie.

3.15 Windows Server Update Services (WSUS)

3.15.1 Popis role

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 klientům 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.

3.15.2 Praktické aplikace

Základní scénáře kde nasazení WSUS jsou:

- Centralizovaný update management
- Automatizace správy aktualizací

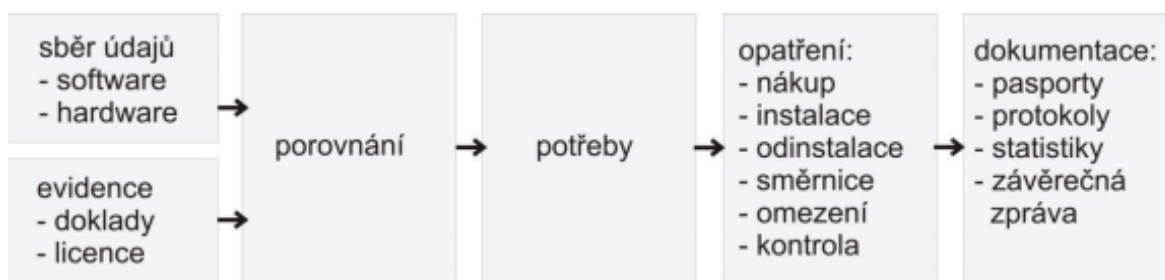
4 SOFTWAREVÝ AUDIT

Audit (z latiny *auditus*, slyšení) znamená úřední přezkoumání a zhodnocení dokumentů, nezávislou osobou. Účelem je zjistit, zda doklady podávají platné a spolehlivé informace o skutečnosti a obvykle také zhodnotit kvalitu vnitřní kontroly firmy. V případě softwarového auditu je cílem vyrovnaní a legalizace veškerého software ve společnosti. Jeho hlavní náplní je úplná inventarizace firemního SW a HW, tu je následně možné využít pro správu tzv. software asset management.

4.1 Princip

Princip softwarového auditu spočívá v řádné inventarizaci nainstalovaného softwaru, zakoupených licencí a hardwarových prostředků. Ty jsou vzápětí podrobně analyzovány. Výsledky nálezu se pak standardně porovnávají s účetními doklady a dalšími doklady, které prokazují legální nabytí software. V případě zjištění nedostatku dochází k nápravě navržením nejvhodnějšího způsobu zajištění potřebných softwarových licencí, případně upgradu hw a tím eliminovat případné budoucí problémy s porušováním autorského zákona, či neschopnost provozu daného softwaru na konkrétní hardwarové konfiguraci PC.

4.2 Průběh



Obrázek 3. Cyklus softwarového auditu.

[10]

Existuje zásadní rozdíl mezi tím, co uživatelé chtějí na svých počítačích mít nainstalované, a co skutečně ke své práci potřebují. Sjednocením software, který budou jednotlivá pracoviště používat, lze další nákupy licencí centralizovat a dosáhnout výrazných finančních úspor. Typicky se tento problém řeší definováním tzv. softwarových profilů, typizovaných instalací pro jednotlivá pracoviště. Z těch se pak složí celkový obraz software pro firmu tzv. koncepční software. Nevyhovující produkty nalezené na počítačích, ale v rozporu s koncepcí, je pak třeba urychleně odinstalovat a nahradit vyhovujícími.

Pokud má firma přehled o svém softwaru, je třeba se zaměřit na účetní stránku věci. Nejdůležitějším dokladem pro evidenci software je doklad o jeho nabytí, které se musí dohledat, zkontrolovat a zadat do evidence. Kromě nabývacího dokladu by v případě produktů dodávaných s tištěnou smlouvou měli správci uchovávat licenční smlouvy a certifikát autentičnosti (Certificate of Authenticity), což může být důkaz o legálnosti nabytí software. Hlavní důvod, proč tyto dokumenty schraňovat, je však specifikace práva užívání produktu, ke kterému se vztahuje. Je třeba mít na paměti, že se smlouvy u jednotlivých verzí produktů mění, proto nestačí archivovat jednu smlouvu k jednomu typu programu (například MS Windows). Typicky se pak jedná o faktury, převodní či darovací smlouvy, prohlášení prodejce nebo dodací list. Za nabývací doklad je považován doklad splňující následující náležitosti: jasná identifikace dodavatele a odběratele, datum nabytí, specifikaci produktu - název produktu, verze produktu, jazyková mutace, počet nabytých licencí, podpis, nebo podpis a razítko. Pokud je SW audit dokončen, posledním krokem je přenesení zodpovědnosti do maximálně možné míry až na koncové uživatele.

[11]

4.3 Přínosy pro organizaci

SW, jak komerční, tak zakázkový, je nedílnou součástí drtivé většiny firem a měl by být adekvátně spravován. Softwarový audit jako součást kompletní správy SW poskytuje velmi konkrétní přínosy:

1. **Úspora finančních prostředků.** SW firmy většinou poskytují slevy při hromadných objednávkách, při správě SW bude možné tyto výhody využít
2. **Snížení celkových nákladů na software a jeho využívání.** Mezi tyto náklady patří školení uživatelů, úpravy a údržba software, technická podpora a samotná evidence software.
3. **Snížení ztrát vzniklých odcizením.** Jednoduché postupy pro správu softwarových prostředků mohou tyto ztráty výrazně omezit a dále tak přispět ke zvýšení zisku.
4. **Snížení rizika a odpovědnosti.** Informovanost a předání osobní odpovědnosti jednotlivým uživatelům odstraňuje riziko obžalování představitelů firmy za porušování autorských práv.

5. **Snížení problémů v komunikaci a v přenosu dat.** Nesjednocenost systémů a dat může vést k problémům v komunikaci. Správa software může pomoci se standardizací technologií a aplikováním zvolených standardů v rámci celé organizace.
6. **Podpora investic do nových technologií.** Správa software umožňuje organizacím lépe poznat hodnoty, které získávají z využívání určitých technologií, a směřovat technologické prostředky do oblastí, které zajistí jejich maximální návratnost.

4.4 Přínosy SW auditu pro správce sítě:

Přes všechny uvedené přínosy, které může mít správa SW pro celou organizaci, nejvýraznější přínosy přináší pro IT pracovníky, kde může pomoci následujícím způsobem:

1. **Snížení požadavků na technickou podporu.** Správa SW pomůže standardizovat technologie. To uvolní odborně vyškolené pracovníky podpory pro jiné úkoly.
2. **Redukce počítačových virů.** Účinná správa SW pomůže snížit kontakt s neautorizovaným softwarem a tím sníží možnost napadení počítačovými viry.
3. **Lepší využívání nového software.** Většina počítačových systémů a sítí je zaplněna nepoužívaným softwarem. Správa software ho pomáhá identifikovat a odstraňovat, důsledkem je snížení potřeby technické podpory.
4. **Zlepšení atmosféry v organizaci.** Pomocí správy software si může IT oddělení vytvořit lepší představu o rozsahu a využívání stávajícího SW a tudíž efektivněji reagovat, což vyvolá pozitivní ohlasy u ostatních zaměstnanců firmy.
5. **Větší důležitost oddělení IT.** Kompletní správa SW pomáhá zviditelnit jeho důležitost a zdůraznit potřebu požadovaných finančních prostředků.

4.5 Přínosy SW auditu pro zaměstnance

Vytvoření jednoznačných a zásadních pravidel užívání výpočetní techniky a technologických standardů je pro organizaci velkým přínosem. Softwarový audit jako součást správy SW může zaměstnancům pomoci následujícím způsobem:

1. **Rozpozná se potřeba lepších nástrojů.** Odborníci na IT jsou obecně schopnější zjistit potřebu nových a lepších softwarových nástrojů než ostatní zaměstnanci a komplexní správa SW jim k tomu poskytuje prostředky.
2. **Sníží se závislost na pracovnících technické podpory.** Komplexní správa SW pomáhá zaměstnancům rychleji řešit jejich problémové stavy.
3. **Vyjasní se legální podmínky užívání technologií.** Určité množství softwarových programů umožňuje zaměstnancům legální užití druhé kopie programu na jejich přenosném, případně domácím počítači pro práci související s jejich zaměstnáním. Přesným seznámením se s těmito podmínkami se sníží rizika postihů za jejich porušování pro jednotlivé pracovníky i celou organizaci.
4. **Lepší zdůvodnění nových nákupů.** V případě nedobře dokumentovaného nákupu SW, jeho stavu a využívání jsou IT oddělení nucena dělat subjektivní rozhodnutí. Správa SW pomáhá zprehlednit systém pořizování SW

[12,13]

5 MIGRAČNÍ SCÉNÁŘE

5.1 Windows Server 2012 R2

Migrace je preferovaná metoda nahrazení stávajícího serveru novým serverem se systémem Windows Server 2012 R2. Na rozdíl od in-place upgradu, migrace kopíruje zásadní informace z existujícího serverového systému do čisté instalace Windows Server 2012 R2.

Server 2012 R2, můžete migrovat data mezi servery v rámci některé z následujících podmínek:

- **Mezi verzemi** Můžete přenést data z libovolné verze systému Windows Server od Windows Server 2003 SP2 do systému Windows Server 2012 R2.
- **Mezi platformami** Můžete přenést data z x86, nebo x64 platformy Windows Server 2012 na x64 platformu serveru se systémem Windows Server 2012.
- **Mezi edicemi** Můžete přenést data mezi servery s jinou edicí systému Windows Server 2012 R2
- **Mezi fyzickými a virtuálními instancemi** můžete přenést data z fyzického serveru na virtuální, či naopak.

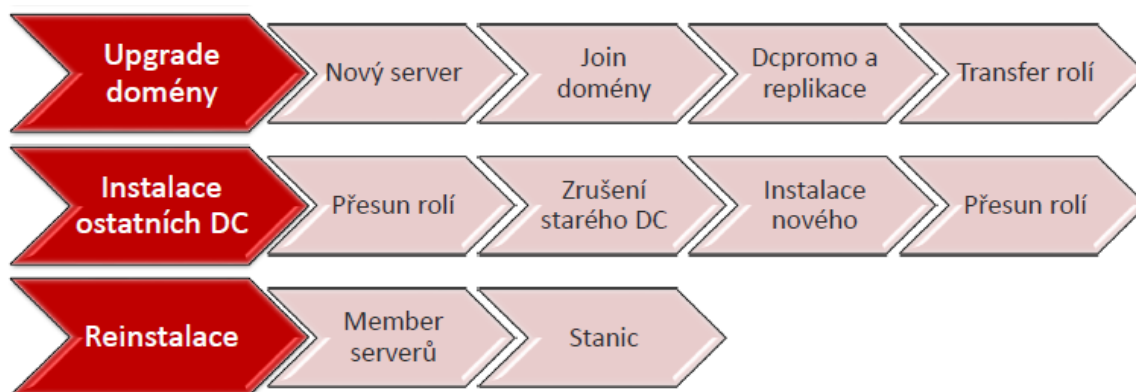
Přímá migrace některých služeb lze provést přímo pomocí nástroje Windows Server 2012 Migration Tools (WSMT), z operačního systému Windows Server 2003 R2 lze migrovat tyto role:

- Directory Federation Services
- File and Storage Services
- IP Configuration
- Network Policy Server
- Print and Document Services
- Remote Access
- Windows Server Update Services

Další služby bohužel nelze migrovat přes WSMT, ale je nutné použít jiné postupy, případně je nelze zmigrovat vůbec:

- **Active Directory Domain Services**

Pro migraci AD DS neexistuje žádná přímá metoda, či nástroj, pouze doporučený postup znázorněn na následujícím obrázku:



Obrázek 4. Postup migrace AD DS

- **Dynamic Host Configuration Protocol**

Z Windows Server 2003 R2 neexistuje migrační scénář, lze však ručně exportovat a importovat databázi.

- **Domain Name Services**

Z Windows Server 2003 R2 neexistuje migrační scénář, nutno přenesením zón ze stávajícího serveru DNS na nový ručně, nebo replikací.

- **Remote Desktop Services**

Migrace RDS není z Windows Server 2003 R2 na Windows server 2012 R2 možná, je nutná nová instalace včetně zakoupení nových licencí terminálového přístupu.

[15, 16, 17]

5.2 Windows 8.1 Pro

Podle následujícího obrázku lze migraci z operačního systému Windows XP na Windows 8 provést pouze se zachováním osobních dat, vzhledem k tomu, že veškerá neosobní data uživatelů jsou ukládána na serveru, je tato funkcionální nepodstatná.

Instalace na Windows 8	Přenos nastavení			
	Přenos nastavení Windows, osobní soubory, a aplikace	Windows a osobních souborů (data a systémové nastavení)	Přenos osobních souborů (pouze data)	Nic není přeneseno
Windows XP (Service Pack 3 a vyšší)	✗	✗	✓	✓
Windows Vista	✗	✗	✓	✓
Windows Vista se SP1	✗	✓	✓	✓
Přechod mezi architekturou (32-bit na 64-bit) Windows Vista se SP1 a vyšší	✗	✗	✗	✗
Přechod mezi jazyky Windows Vista se SP1 a vyšší	✗	✗	✓	✓
Windows 7	✓	✗	✓	✓
Přechod mezi architekturou (32-bit na 64-bit) Windows 7	✗	✗	✗	✗
Přechod mezi jazyky Windows 7	✗	✗	✓	✓
Windows 8	✓	✗	✓	✓
Přechod mezi architekturou (32-bit na 64-bit) Windows 8	✗	✗	✗	✗
Přechod mezi jazyky Windows 8	✗	✗	✓	✓

Obrázek 5. Možnosti migrace Windows 8

[18]

5.3 Instalace z média

Instalace z média je způsob instalace zpravidla s použitím instalačního CD nebo DVD, případně flash disku (metoda označována jako High Touch deployment with Retail media).

Instalace z média je výhodná tím, že nevyžaduje žádnou infrastrukturu v daném prostředí, naopak její nevýhodou je nutnost interakce uživatele s počítačem během instalace. Obecně platí, že instalace z média přichází v úvahu, pokud chceme provést instalaci řádově na jednotlivé stroje, ve větších prostředích ji nemá cenu uvažovat, protože by byla neúnosně časově náročná.

Malé organizace mohou vytvořit efektivnější proces nasazení pomocí instalačního programu systému Windows přizpůsobit a nainstalovat standardní obraz, který je obrazem počítače, který je konfigurován s aplikacemi a nastaveními. Organizace mohou vytvořit standardní obrazy, které obsahují nastavení počítače, ovladače zařízení, aplikace, a tak dále. Tento proces pomáhá automatizovat instalaci, což umožňuje administrátorovi,

aby se vyhnul interakci s instalací systému Windows během instalace (metoda označována jako High Touch deployment with Standard Image).

5.4 Instalace ze sítě

Instalační soubory operačního systému lze rovněž umístit do sdílené složky na síti a provést instalaci z tohoto umístění. Aby se počítač bez operačního systému dokázal připojit k sdílené složce, je nutné do něj zavést Windows Preinstallation Environment (zkráceně Windows PE), což je vlastně operační systém Windows, který však obsahuje pouze základní ovladače a programy.

V sofistikovanějších prostředích, využívajících AD DS a Windows Server přichází v úvahu instalace pomocí nástroje Windows Deployment Services (metoda označována jako Light Touch deployment), případně System Center Configuration Manager (metoda označována jako Zero Touch deployment) v případě opravdu velkých prostředí a mnoha strojů.

Použitím nástrojů WDS odpadá nutnost složitější interakce s počítačem na který je systém instalován, jelikož zavedení systému je zajištěno přímo ze sítě. Narůstají ovšem nároky na infrastrukturu prostředí a v případě System Center i nároky na finanční stránku věci.

Oba dva výše nastíněné postupy jsou na rozdíl od instalace z média vhodné pro provedení instalací ve větším rozsahu, kdy se může jednat o desítky až stovky strojů.

II. PRAKTICKÁ ČÁST

6 REALIZACE PROJEKTU

6.1 Cíl projektu

- Inovace starého HW a SW klientských stanic.
- Eliminace bezpečnostního rizika při používání nepodporovaných operačních systémů.

6.2 Proveditelnost projektu

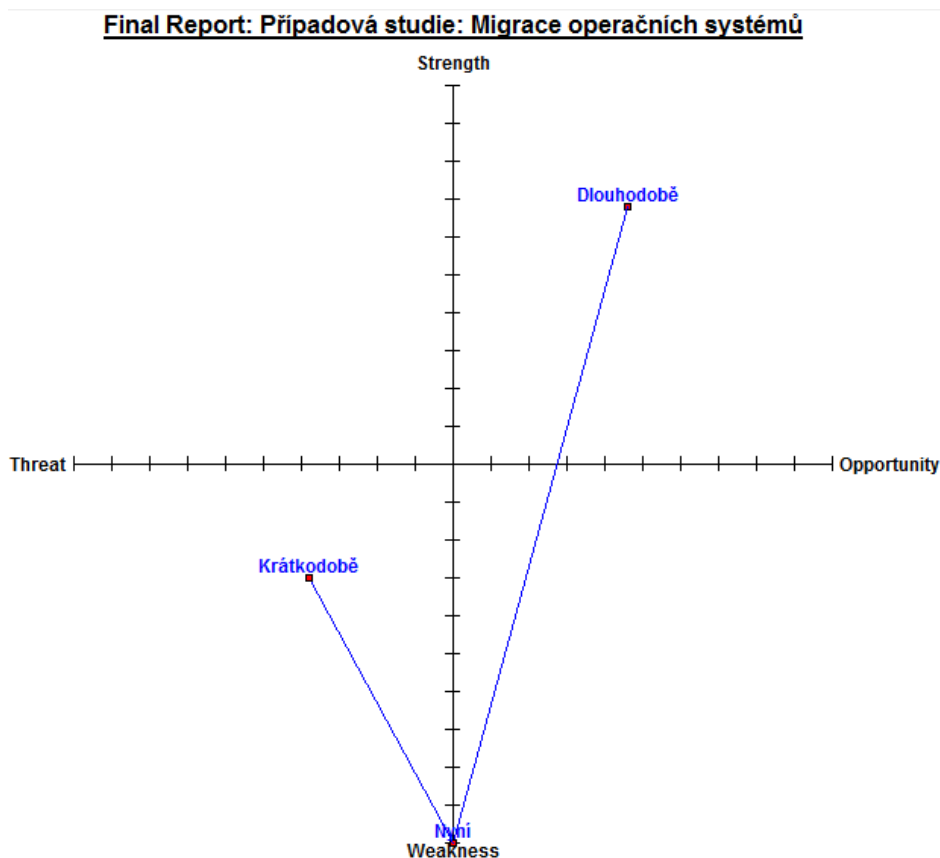
Na základě analýzy stávajícího síťového prostředí, sw auditu, migračních scénářů, a testování migrace ve virtuálním prostředí ještě před implementací a danému rozpočtu byl projekt shledán proveditelným, s relativně malým rizikem.

6.3 SWOT analýza

Pro rychlejší schválení projektu ze strany vedení byla vypracována swot analýza

- **Silné stránky**
 - *Dlouhodobě*
 - Bezpečnost
 - Zvýšení Bezpečnosti klientských i operačních systémů
 - Dopad=100 :: Pravděpodobnost =100 :: Bilance=100
 - Zjednodušení správy
 - Zjednodušení a urychlení správy operačních systémů
 - Dopad=60 :: Pravděpodobnost =90 :: Bilance=54
 - Virtualizace
 - Snížení spotřeby elektrické energie
 - Snížení nákladů na hardwarovou obnovu a údržbu serverů
 - Dopad=60 :: Pravděpodobnost =100 :: Bilance=60
 - Výkon
 - Zvýšení výkonu serveru, nová PC zrychlí práci uživatelů
 - Dopad=60 :: Pravděpodobnost =100 :: Bilance=60

- **Slabé stránky**
 - *Nyní*
 - Cena
 - Cena pořízení nového serveru a zejména CAL licencí a RDS licencí
 - Dopad=100 :: Pravděpodobnost =100 :: Bilance=100
 - *Krátkodobě*
 - Školení
 - Nutnost proškolení administrátora i koncové uživatele na nové funkce a změny v ovládání
 - Dopad=30 :: Pravděpodobnost =100 :: Bilance=30
- **Příležitosti**
 - *Dlouhodobě*
 - Cloud
 - Možné využití cloudových služeb do budoucna
 - Dopad=60 :: Pravděpodobnost =30 :: Bilance=18
 - Nároky do budoucnosti
 - Implementace platformy, která by vyhovovala i nárokům kladeným v budoucnosti
 - Dopad=80 :: Pravděpodobnost =80 :: Bilance=64
- **Hrozby**
 - *Krátkodobě*
 - Problémy s nasazením
 - Problémy v průběhu migrace, delší nefunkčnost některého ze systémů
 - Dopad=100 :: Pravděpodobnost =30 :: Bilance=30
 - Nekompatibilita firemních aplikací
 - Možné problémy provozu některých firemních aplikací na nové platformě
 - Dopad=100 :: Pravděpodobnost =15 :: Bilance=15



Obrázek 6. Graf SWOT analýzy projektu migrace operačních systémů

6.4 Cenová kalkulace projektu

Zboží	Cena/ks	Ks	Celková cena	Cena s DPH
Win Svr CAL OLP C Device CAL	390	60	23 400	28 314
Software MS Windows Remote Desktop Svcs CAL 2012 SNGL OLP NL Device CAL	2 650	7	18 550	22 446
Microsoft Windows Server 2012 R2 Standard Sngl OLP	12 146	1	12 146	14 697
Triline Profi I80, Pentium G2030, 4GB DDR3, 250GB, 3roky záruka on-site, W8.1Pro OEM	8 150	28	228 200	276 122
HP ProLiant ML310eG8v2 E3-1220v3, 16GB, 4x1TB, 3NBD	26 949	1	26 949	32 608
Lenovo Iomega ix2 NAS 2-bay 2TB (2HD x 1TB)	4 109	1	4 109	4 972
Office Home and Business 2013 DOEM CZ, lic.	3 916	12	46 992	56 860
HP 8GB microSD Enterprise Mainstream Flash Media Kit	1 580	1	1 580	1 912
			361 926	437 930

Tabulka 7. Cenová kalkulace projektu

6.5 Časový harmonogram projektu

Etapa	Co je cílem etapy	Odhad doby realizace etapy	Skutečná doba realizace dané etapy	Odhad dopadu na provoz firmy	Skutečný dopad na provoz firmy
Příprava projektu	Zahájení projektu - způsob realizace a organizační zajištění projektu, kontrola kompatibility aplikací, testování ve virtuálním prostředí, úvodní jednání s vedením	20h	48h, v rámci testovacího prostředí se narazilo na nečekané překážky v průběhu migrace	Žádný	Žádný
Analýza stávajícího síťového prostředí	Zjištění jaké serverové služby, na jakých serverech a na jakém HW běží	2h	4h, drobné rozdíly mezi dokumentací a skutečností	Žádný	Žádný
SW audit	Zjištění možnosti upgrade, revize nakoupených licencí, kontrola sw na stanicích.	8h	12h, dohledání dokladů trvalo déle	Žádný	Žádný
Vyhodnocení potřeb	Vyhodnocení potřeb z předcházejících analýz, cenová kalkulace, swot analýza	2h	2h	Žádný	Žádný
Schválení projektu	Schválení rozpočtu a časového plánu	1h	1h	Žádný	Žádný
Nákup HW a SW		1h	1h	Žádný	Žádný
Instalace serveru a ESXi	Základní konfigurace serveru, update firmware, konfigurace ILO, instalace hypervisoru ESXi	2h	2h	Žádný	Žádný
Instalace Windows Server 2012 R2 Standard jako 1VM	Instalace jako řadič domény, DNS, DHCP, File and Storage server.	2h	3h, zapomnělo se na délku tvorby Eager Zeroed storage pro VM	Žádný	Žádný
Kopírování dat na nový server		5h	4h	Žádný	Žádný

Migrace ADDS, DNS, DHCP, File Services na 1VM		3h	3h	4h odstávka, celé infrastruktury	3h nefunkční celá infrastruktura
Instalace Windows Server 2012 R2 Standard jako 2VM	Instalace aplikačního serveru (SQL, aplikace, ESET, Echotrack, docházkový a obědový systém)	2h	2h, oproti předchozí instalaci urychlení již přesunutému instalačnímu mediu na datastoru ESXi	Žádný	Žádný
Migrace SQL a instalace jednotlivých aplikací	Restore databází programů Echotrack, NOD32, Raal a docházkového a obědového systému z SQL 2008 a import do SQL 2012.	4h	5h, rebuild databází na verzi 2012 a instalace a konfigurace aplikací trvalo déle, než se čekalo	6h odstávka	Nefunkční jednotlivé aplikace 7h
Instalace RDS, Licenčního serveru a aktivace licencí		2h	1.5h	Žádný	Žádný
Výměna a instalace klientských stanic		14h	20h, zdržení v nutnosti instalace lokálních tiskáren	Omezení zaměstnance 0.5h při výměně stanice	Minimální
Školení uživatelů na novinky a ovládání Windows 8, jednotlivě v rámci výměny stanic		14h	20h, u některých uživatelů nutná další podpora	Omezení zaměstnance 0.5h školení na nový systém	Minimální

Tabulka 8. Časový harmonogram a popis jednotlivých etap a dopadů na provoz firmy

6.6 Shrnutí

Na projekt byl původně schválen rozpočet 350 000Kč, jedná se o projekt s větší počáteční rizikovostí, dlouhodobě však přináší více přínosu viz. Obrázek 6. Graf SWOT analýzy, rozpočet projektu byl v průběhu lehce navýšen z důvodu rozhodnutí provést výměnu všech klientských stanic s operačním systémem Windows XP.

Celková doba realizace projektu do plné funkčnosti trvala 14dní, prvních pět dní se jednalo o přípravnou část, schvalování, nákup HW a SW a testování průběhu migrace ve virtuálním prostředí, nejkrizovější část a to migraci serverů byla zvládnuta za tři dny, dva dny se jednalo o víkend s minimálním omezením provozu a jeden den pracovní z důvodu nutnosti kooperace s tvůrci některých programů používaných ve firmě. Rozdíly mezi odhadovanými časy jednotlivých úkonů a reálné doby provádění včetně odůvodnění popisuje Tabulka 8. Časový harmonogram a popis jednotlivých etap a dopadů na provoz firmy. Dalších pět dní trvala výměna a konfigurace klientských stanic a školení uživatelů na nový systém.

7 ANALÝZA STÁVAJÍCÍHO SÍŤOVÉHO PROSTŘEDÍ

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

7.1 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.

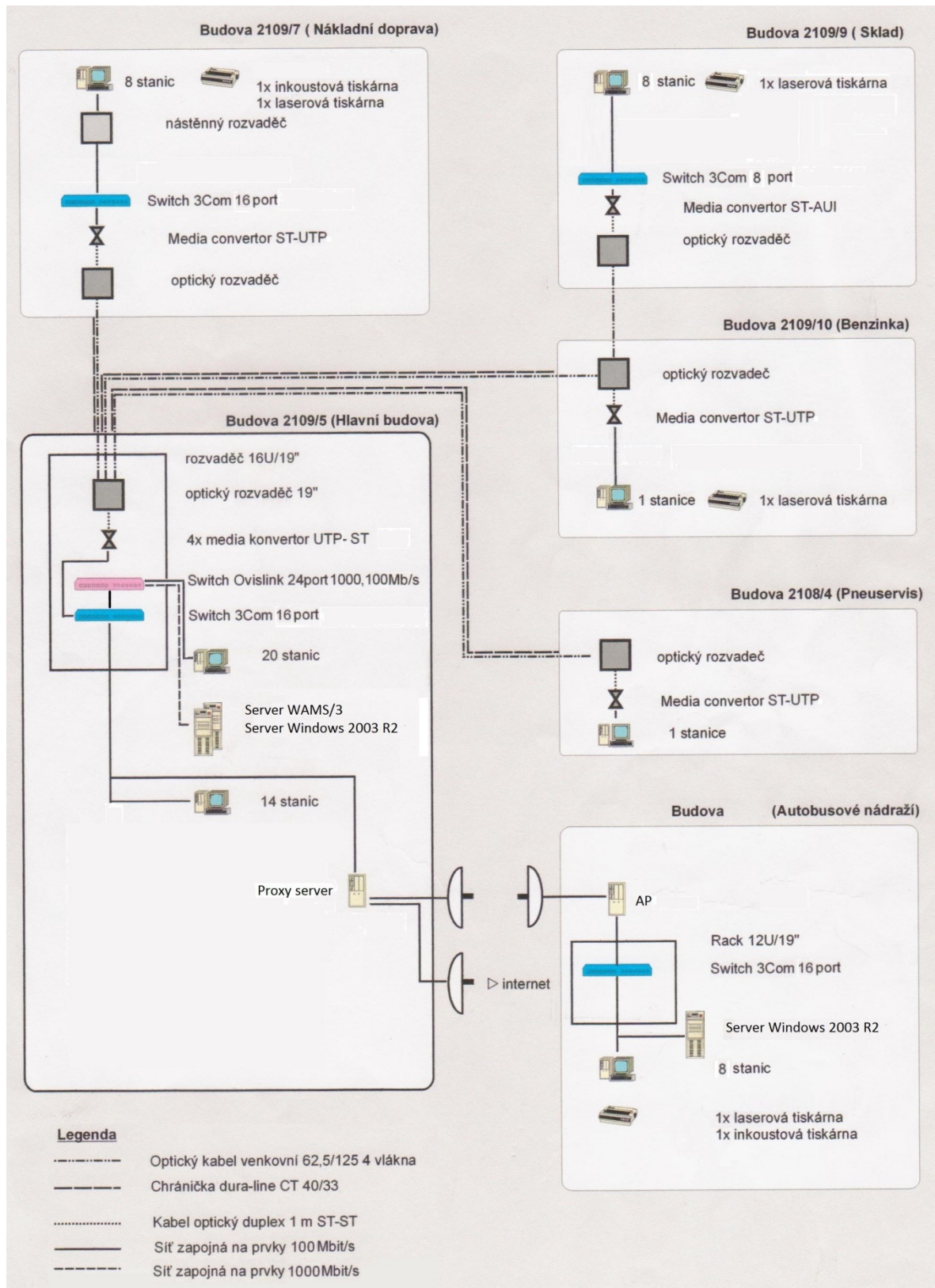
Propojení aktivních prvků v síti zprostředkovává strukturovaná kabeláž (FastEthernet 10/100Base TX, případně u serverů 1000Base-T). Vzájemná konektivita je tedy považována za propojení v rámci sítě LAN (Local Area Network).

7.2 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. Servery na platformě Microsoft mají roli řadiče domény, dns serveru, dhcp serveru, wsus serveru a databázového a souborového serveru, druhý server slouží pro replikaci AD a jako záložní server.

Server	Operační systém	Funkce	Hardware
HP ML 150 G3	Microsoft Windows Server 2003 R2 standard	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 standard	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 9. Přehled firemních serverů



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

7.2.1 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

7.2.2 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)
Access-Point UBNT NanoStation M5	192.168.2.2	Budova autobusového nádraží

Tabulka 10. Přehled aktivních prvků

7.2.3 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 uvádí následující tabulka:

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

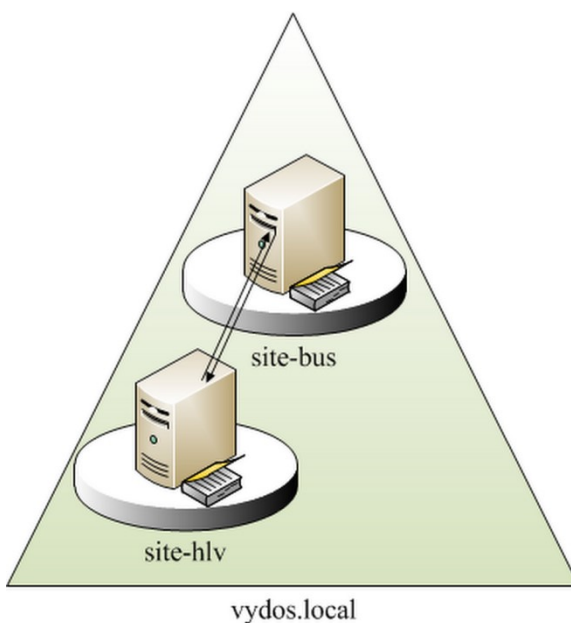
Tabulka 11. Přehled VLAN

7.3 Síťové služby

V následující části je popsán stav základních síťových služeb před realizací projektu.

7.3.1 AD DS

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



Obrázek 8. Doménová struktura a lokality

7.3.2 Souborový server

Ve firmě běží souborový server na hlavním řadiči domény se zálohováním na sekundární.

7.3.3 Terminálový server

Ve firmě běží jeden terminálový server a to na sekundárním řadiči domény.

7.3.4 DNS

Ve firmě běží dva DNS servery a to na každém ze dvou řadičů domény.

7.3.5 WSUS

Ve firmě běží služba WSUS 3.0 SP2 na sekundárním řadiči domény.

7.3.6 DHCP

Služba DHCP běží na hlavním řadiči domény a je nakonfigurována s následujícími obory a rozsahem přidělovaných adres podle lokality:

1. Název oboru - site_hlv

Rozsah distribuovaných adres - 192.168.1.21 - 192.168.1.100

2. Název oboru - site_bus

Rozsah distribuovaných adres - 192.168.2.21 - 192.168.2.100

7.3.7 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, GPS sledování vozidel a mapové podklady. Dále spediční databanka RaalTrans. Druhý server slouží jako záložní pro replikaci databází. V rámci migrace bude přeinstalován na verzi 2012.

7.4 Ostatní služby

7.4.1 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, jeho databáze bude přesunuta v rámci migrace databázového serveru.

7.4.2 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.

7.4.3 Docházkový systém

Docházkový, turniketový a stravovací systém je řešen produktem od firmy Cominfo a.s. a využívá Microsoft SQL serveru 2008, jeho databáze bude přesunuta v rámci migrace databázového serveru.

7.4.4 Informační systém

Je využíván informační systém WAMS/3 od firmy Micros a.s., tento běží na samostatném linuxovém serveru a migrace operačního systému Windows Server na něj nebude mít žádný vliv.

7.4.5 Centrální správa záložních zdrojů

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

7.4.6 Asset management

Ve firmě je nainstalována sw SysAid ve verzi Free starající se o evidenci licencí, help desk a monitoring sítě.

7.5 Licenční politika

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

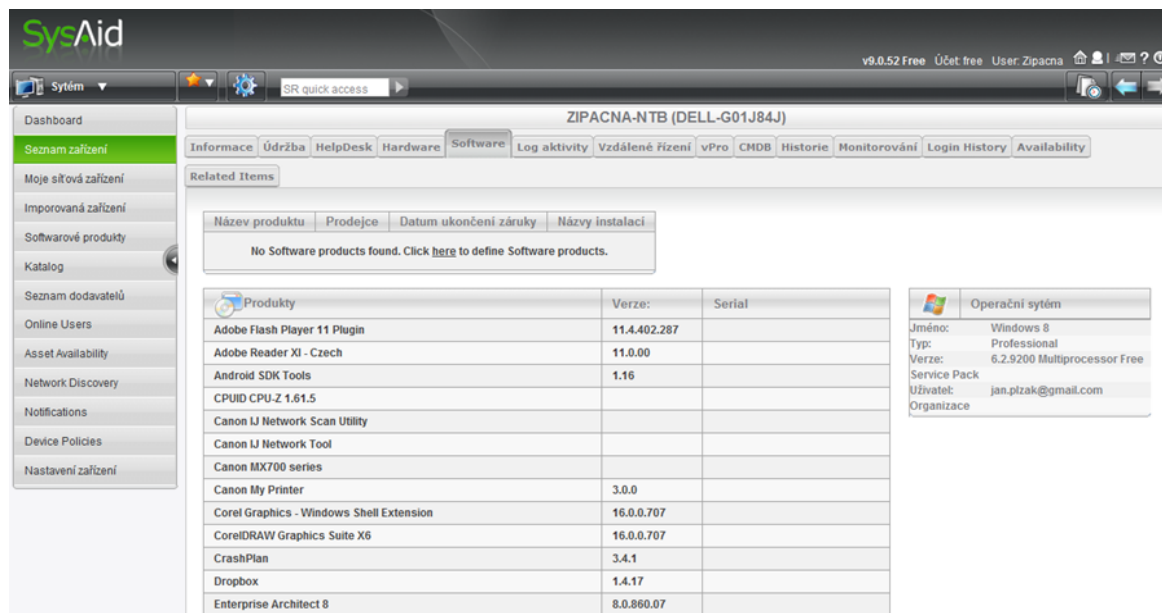
7.6 Operační systém klientských stanic

Firma vlastní 32 stanic s operačním systémem Windows XP Professional a 28 stanic se systémem Windows 7 Professional.

[20]

8 SW AUDIT

Byl proveden zejména kvůli zjištění stavu HW a SW jednotlivých stanic, do budoucna se však počítá s plným nasazením asset managementu, i když pouze s Free verzí programu SysAid. Free verze má omezení nově na využití pouze MSSQL, dříve Firebird a podporuje pouze maximálně 2 administrátory, dále postrádá přímou integraci s technologiemi Microsoft Active Directory. Je určena pro maximální počet 100 uživatelů helpdesku i 100 spravovaných PC v rámci SAM a není k němu podpora ze strany výrobce, pouze komunity. Přes všechna tato omezení je však je tento sw ve firmě využíván a i když nedosahuje komfortu a funkcionality placených nástrojů a zejména kvůli absenci integrace s AD vyžaduje práci administrátora navíc, management firmy neuvolnil na jiné řešení dostatek finančních prostředků.



Obrázek 9. Ukázka prostředí programu SysAid

8.1 Výsledky

Program umožňuje exportovat výsledky s aplikováním filtrů, pro přehlednost a využití v této práci a dopomoc v případě migrace na novější systém však musely být výsledky dále upraveny a některé parametry dohledány u výrobců daného HW, nejvíce stěžejní jsou hodnoty v následujících tabulkách:

Doporučený Upgrade Hardware	Stanic nutných vylepšit ke splnění minimálních požadavků	Stanic nutných vylepšit ke splnění optimálních požadavků
Navýšení paměti RAM	13	20
Navýšení kapacity pevného disku	3	3
Výměna grafické karty	20	20
Nová verze BIOSu	2	2
Upgrade CPU	13	13

Tabulka 12. Přehled vylepšení jednotlivých stanic pro nasazení Windows 8.1

Stanice	počet	HW	Cena upgrade jedné stanice včetně licence systému	Možnost instalace Windows 8.1
1. Generace stanic	13	CPU: Intel Celeron, RAM: 512MB DDRI		Ne
2. Generace stanic	7	CPU: Intel Pentium IV, RAM: 1GB DDRII	5000Kč bez DPH	Krajně nedoporučeno
3. Generace stanic	2	CPU: Intel Pentium E2140, RAM: 2GB DDRII	3500kč bez DPH	Ano, po update BIOSu
3. Generace stanic - novější série	6	CPU: Intel Pentium E2160, RAM: 2GB DDRII	3500kč bez DPH	Ano

Tabulka 13. Přehled generací koncových stanic, možnosti a ceny upgrade

8.2 Shrnutí

Z auditu je vidět, že na úplně nejstarší sérii PC ve firmě, čítající 13 klientských stanic, se z hlediska upgrade může zcela zapomenout. Stanice mají jednojádrové procesory a 512MB dnes již buď obtížně, nebo vůbec nesehnatelné paměti ram typu DDRI. Další série PC činí 7 klientských stanic, kde by bylo nutné vyměnit grafickou kartu a pro optimální běh navýšit operační paměť na 2GB v tomto případě typu DDRII,

Co se týče posledních 8 stanic, všechny byly zakoupeny s operačním systémem Windows Vista, který se však ukázal jako problémový, a tak byl proveden downgrade na Windows XP kvůli zachování konzistence prostředí, u 6 stanic není žádný problém s přechodem na novější verzi systému, 2 stanice nejsou ze stejné série a podle stránek výrobce základní desky je nutné nahrát novější verzi BIOSu.

9 INSTALACE A MIGRACE SERVERŮ

9.1 VMWARE ESXI

9.1.1 Předpoklady pro instalaci

Než se začne s instalací ESXi, doporučuje se ověřit, zda HW, na který se vybere pro instalaci, je kompatibilní pro tento systém. Tyto informace jsou k dispozici na webu VMware Hardware Compability List, nebo v tomto konkrétním případě je již server certifikován pro užití s daným produktem.

9.1.2 Instalace

1. Instalace microSD karty do serveru HP ProLiant ML 310e Gen8 v2
2. Update firmware, po připojení serveru na stávající síť stisknutím klávesy F9 při startu se spustí HP Intelligent Provisioning - volba update firmware, po updatu proběhne restart.
3. Tvorba RAID pole, po spuštění serveru stiskem klávesy F5 nastavení smart array - Create Array - select all disk - typ pole RAID 10 - velikost bloku - doporučená pro daný řadič 256KB.
4. Zvolit možnost Create Logical volume.
5. Stažení instalačního CD VMware HP custom image z webových stránek firmy HP, jenž obsahuje všechny potřebné ovladače k instalovanému serveru a vypálí na CD
6. Vloží se do mechaniky instalační CD, poté se zobrazí boot obrazovka s možností zahájit instalaci ESXi. Zvolí se ESX(i) Installer
7. Potvrzení Hardware Compability Listu stiskem klávesy Enter
8. Potvrzení licenčních podmínek stiskem klávesy F11
9. Nastaví se disk (SD Karta), kde bude provedena instalace ESXi, poté se dál pokračuje stiskem klávesy Enter
10. Nastaví se jazykové nastavení klávesnice - doporučuje se možnost U. S. English a pokračuje se stiskem Enter
11. Následně se zobrazí výzva k nastavení hesla a pokračuje se v instalaci kliknutím tlačítka Enter

12. Poté se zobrazí výzva k potvrzení instalace. Potvrdí se stiskem klávesnice F11
13. Po krátké chvíli je provedena instalace a poté se provede restart serveru
14. Po restartu probíhá stahování jednotlivých modulů ESXi. Zobrazí se obrazovka s možnostmi dalšího nastavení serveru klávesou F2 „Customize system“ nebo je možnost provést restart/vypnutí PC stisknutím klávesy F12
15. Pro konfiguraci je potřeba zadat heslo.
16. Následně je nastavena komunikace po síti. Defaultně je nastaven DHCP server, ale je nastavena statická adresa, nastavení DNS a vypnutí protokolu IPv6.
17. Následuje restart.

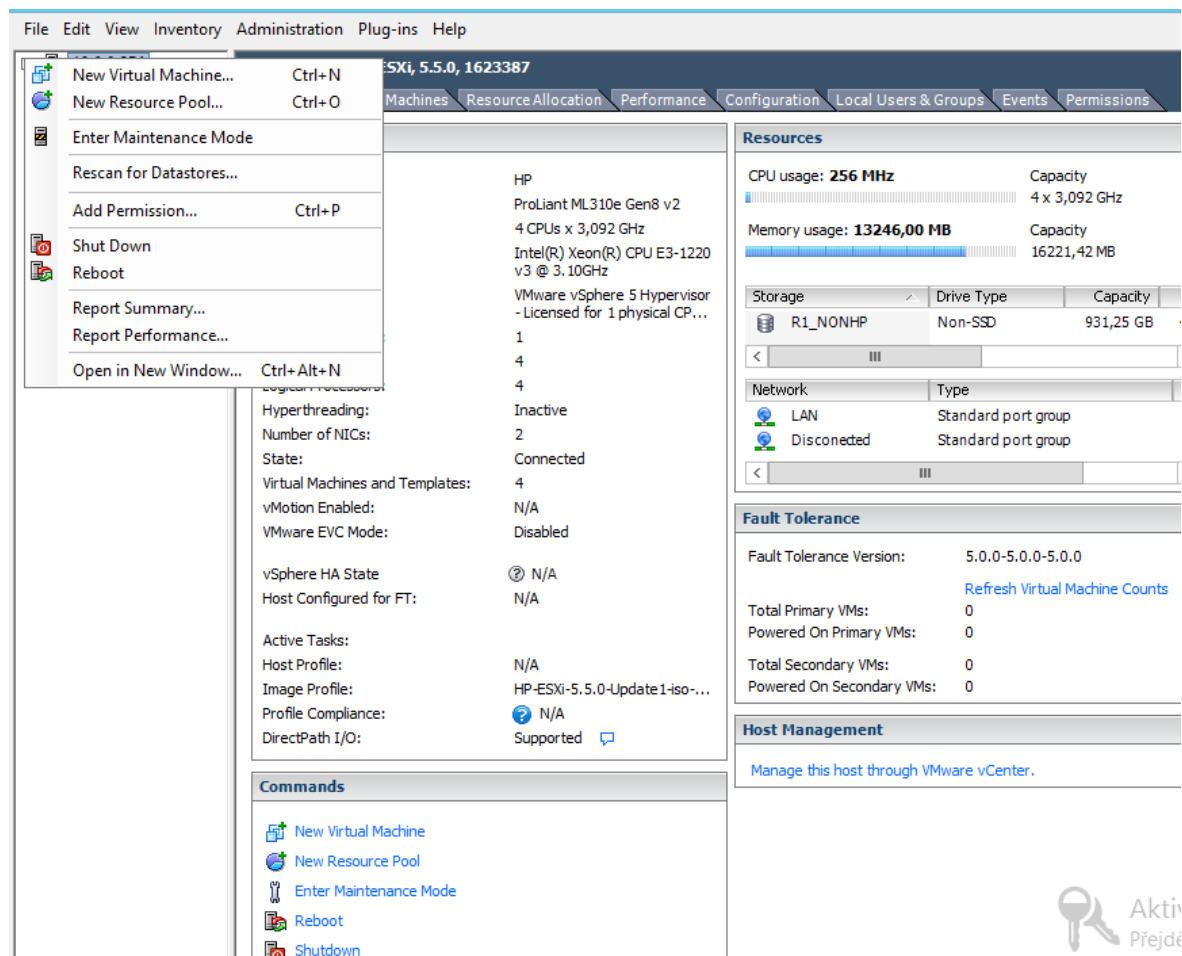
Poznámka: Nepoužívat HP Intelligent Provisioning, při jeho použití nelze nainstalovat ESXi na microSD kartu, ale rovnou se nainstaluje na pevné disky, což je vzhledem ke snížení výkonu diskového pole v tomto případě nežádoucí.

9.2 Instalace VMware vSphere Klienta

Instalace je k dispozici na webu VMware. Samotná instalace je jednoduchá. Odklikne se několikrát za sebou **Next** a odsouhlasí se licenční podmínky. Nic se zde nenastavuje.

Po instalaci se pokračuje spuštěním VMware Klienta, automaticky se přednastaví IP adresa, která byla nastavena během instalace ESXi. Doplní se již jen „User name“ v tomto případě je to „root“ a heslo.

Po otevření je možnost instalovat a konfigurovat nové virtuální stroje.



Obrázek 10. Ukázka prostředí ESXi přes klienta vSphere

9.3 Instalace Windows Server 2012 R2

9.3.1 Konfigurace virtuálního stroje

1. V úvodní nabídce se zvolí nový virtuální stroj - typické nastavení
2. Nastaví se název virtuálního stroje - W2012R2_ADDS
3. Zvolí se datastore
4. Zvolí se typ hostovaného systému - Windows 2012 R2
5. Nastaví se emulace síťové karty - doporučeno VMXNET3 (Windows neuvidí síťový adaptér do instalace VMWare Tools - nainstalují se sami při prvním korektním spuštění, ale je značně rychlejší než kompatibilní E1000)
6. Nastavení se virtuální disk - 50GB - Thick Eager Zeroed

7. Zaškrtnutí Edit nového virtuálního stroje před dokončením - nastavení přidělení 6GB operační paměti, přidání nového disku - přidat nový virtuální disk - velikost 300GB - Thick Eager Zeroed - SCSI - Finish

9.3.2 Instalace

1. Instalace započne automaticky po vložení instalačního média a spuštění VM
2. Nastaví se volba jazyka a klávesnice - Český - Další
3. Stiskne se „Instalovat teď“
4. Vyberte se verze systému. Standard with a GUI“
5. Odsouhlasení licenčních podmínek „Další“
6. U čisté instalace se vybere volba „Custom“
7. Vyberte disk, na který chcete systém instalovat a stiskněte „Další“
8. Nyní se systém instaluje. Doba instalace závisí na výkonu počítače
9. Zadá se heslo administrátora, Pokračuje se stisknutím tlačítka „Finish“
10. Po skončení instalace se můžete přihlásit. Stiskněte tedy klávesovou zkratku Ctrl+Alt+Delete a přihlaste se pomocí vámi zadaného hesla
11. Obdobě se postupuje i při instalaci druhé instance serverového operačního systému

9.3.3 Základní konfigurace

- **Doménový server vydsrv003**

1. Spustí se powershell - start - powershell a zadají se následující příkazy:
2. Rename-Computer vydsrv003 -LocalCredential administrator heslo
3. New-NetIPAddress -InterfaceAlias “Síť Ethernet” -IPv4Address “192.168.1.11”
-PrefixLength 24 -DefaultGateway 192.168.1.1
4. Set-DnsClientServerAddress -InterfaceAlias “Síť Ethernet” -ServerAddresses
192.168.1.10

- **Aplikační server vydsrv004**

1. Spustí se powershell - start - powershell a zadají se následující příkazy:
2. Rename-Computer vydsrv003 -LocalCredential administrator heslo
3. New-NetIPAddress -InterfaceAlias "Síť Ethernet" -IPv4Address "192.168.1.12"
-PrefixLength 24 -DefaultGateway 192.168.1.1
4. Set-DnsClientServerAddress -InterfaceAlias "Síť Ethernet" -ServerAddresses
192.168.1.10

9.4 Migrace AD DS

9.4.1 Nastavení role řadiče domény

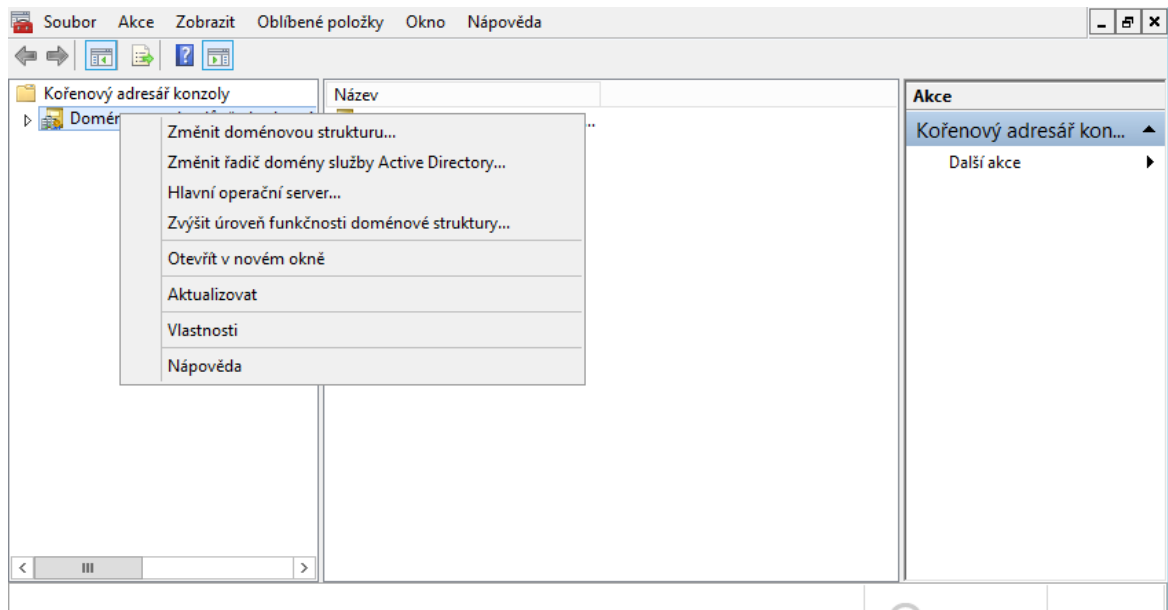
1. Otevře se konzole správce serveru a klikne se Přidat role a funkce
2. Vybere se instalace na základě rolí nebo funkcí a klikne se na Další
3. Vybere se server z fondu serverů
4. Vybere se role Active Directory Services.
5. Zvolí se přidat výchozí funkce, které služba vyžaduje - nechá se ve výchozím stavu
- Další
6. Ve výsledném potvrzení se klikne na Instalovat
7. Jakmile je instalace dokončena v konzoli server manageru se objeví možnost
Povýšit server na doménový řadič
8. Vybere se přidat doménový řadič do existující domény vydos.local
9. Klikne se - Změnit, zadá se jméno a heslo administrátora domény - Další
10. Definuje se, zdali server má být serverem DNS a Globálního katalogu (GC), zvolí
se Site, do které DC patří a nadefinuje Directory Services Restoration Mode
(DSRM) heslo pro danou doménu
11. Nastavení umístění databáze AD, Sysvol a logů D:\ - Další
12. Pokud instalační program prošel úspěšně všemi prekvizitami klikne se na tlačítko
Instalovat, po dokončení je nutné restartovat server

9.4.2 Přenos role Flexible Single Master Operations (FSMO)

1. Otevře se Uživatelé a Počítače Active Directory konzole na serveru s Windows Server 2012 R2
2. Klikne se pravým tlačítkem myši na doménu vydos.local a vybere se Hlavní operační servery
3. V otevřeném okně, vybereme záložku RID
4. Klikne se na tlačítko Změnit a potvrdíme tlačítkem OK
5. Opakujeme postup na záložkách Primární řadič domény a Infrastruktura

Changing the Active Directory Domain Controller

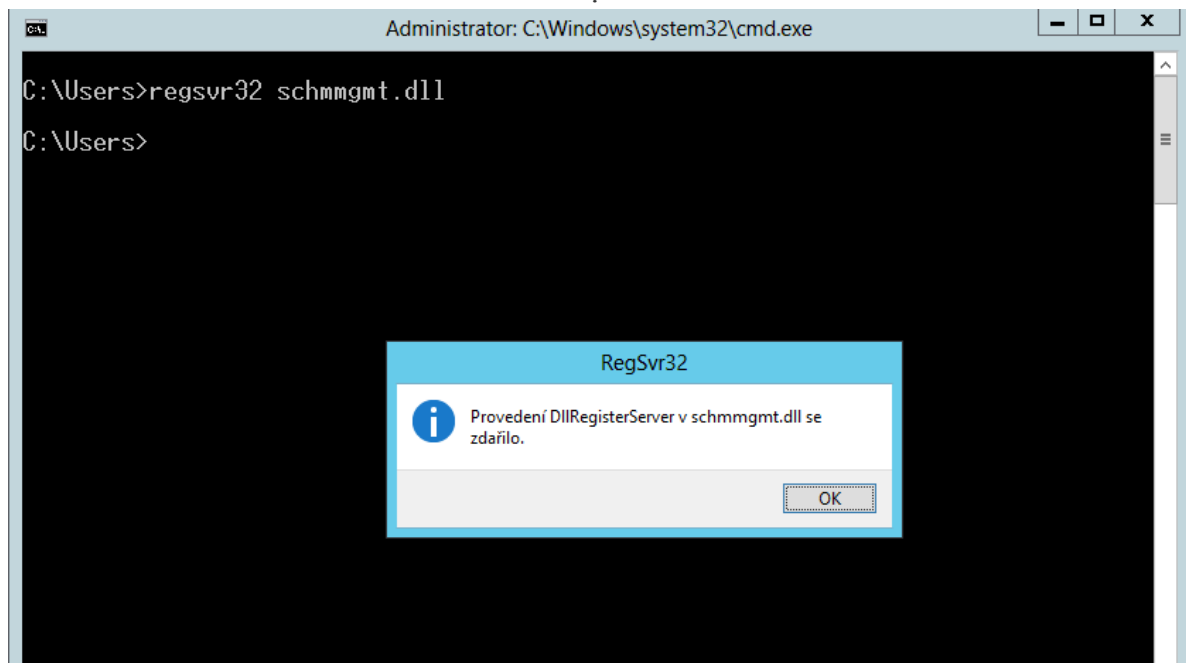
1. Otevře se MMC konzole Domény a vztahy důvěryhodnosti na serveru s Windows Server 2012 R2
2. Klikne se pravým tlačítkem myši na doménu vydos.local a zvolí se možnost - Změnit řadič domény
3. Zvolí se možnost Tento řadič domény nebo instance služby AD LDS
4. Vybereme server s 2012 R2 Windows Server
5. Klikne se Ano pro pokračování
6. Vráti se zpět v konzole Domény a vztahy důvěryhodnosti
7. Klikne se pravým tlačítkem myši na strom Domény a vztahy důvěryhodnosti a zvolí se možnost - Hlavní operační server
8. V okně Hlavní operační server se potvrdí změna tlačítkem Změnit
9. Potvrdí se dialogové okno, chceme-li skutečně přenést roli hlavního operačního serveru na jiný počítač, klikne se Ano.



Obrázek 11. Snap-in modul Domény a vztahy důvěryhodnosti

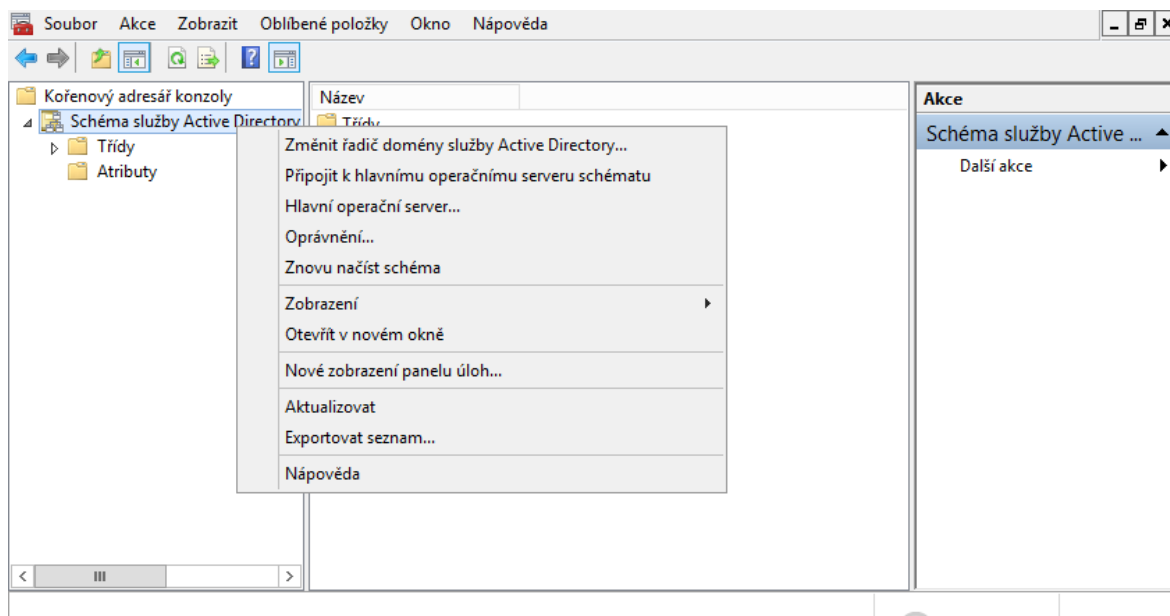
9.4.3 Změna Master schématu

1. Spustí se příkazový řádek - pravé tlačítko myši v levém dolním okně - spustit příkazový řádek (správce)
2. Zadá se příkaz: `regsvr32 schmmgmt.dll` a potvrdí Enterem
3. Jakmile je hotovo potvrdí se následující dialog:



Obrázek 12. Registrace DLL pro použití snap-in modulu Schéma Active Directory

4. Otevře se MMC konzole, snap-in modul Schéma Active Directory
5. Klikne se pravým tlačítkem myši na doménu strom Schéma služby Active Directory a zvolí se možnost - Změnit řadič domény služby Active Directory
6. Zvolí se možnost Tento řadič domény nebo instance služby AD LDS
7. Vybere se server s 2012 R2 Windows Server.
8. Klikne se Ano pro pokračování
9. Zobrazí se varování, že snap-in modul Schéma Active Directory není připojen, Klikne se Ano pro pokračování
10. Nyní je v snap-in modulu Schéma Active Directory vidět server s Windows Server 2012 R2.
11. Klikne se pravým tlačítkem myši na doménu strom Schéma služby Active Directory a zvolí se možnost - Hlavní operační server
12. V dialogovém okně Změnit hlavní server schémat se Klikne se Změnit
13. Potvrdí se dialogové okno, chceme-li skutečně přenést roli hlavního operačního serveru na jiný počítač, klikne se Ano

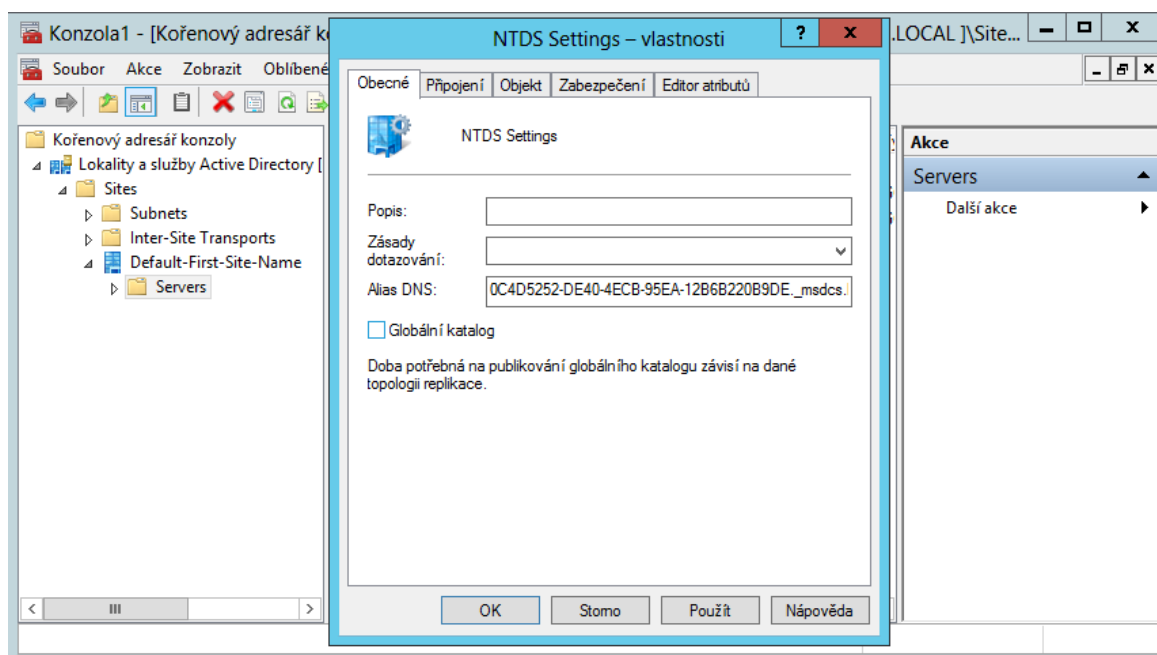


Obrázek 13. Snap-in modul Schéma služby Active Directory

Poznámka: Jakmile je proces dokončen otevře se MMC konzole Uživatelé a počítače služby Active Directory ke kontrole, proces replikace trvá nějaký čas, záleží na počtu objektů.

9.4.4 Odebrání serveru Windows 2003 R2 z Globálního katalogu

1. Otevře se MMC konzole, snap-in modul Lokality a služby Active Directory
2. Klikne se pravým tlačítkem myši na doménu strom Schéma služby Active Directory a zvolí se možnost - Změnit řadič domény služby Active Directory
3. Rozbalí se složka Sites - Default-First-Site-Name - Servers
4. Vybere se server se systémem Windows Server 2003, Rozbalí se složka.
5. Klikne se pravým tlačítkem myši na NTDS Settings
6. V menu se vybere Vlastnosti
7. Pod záložkou Obecné, odvybrat Globální katalog
8. Klikne se na OK pro potvrzení.
9. Ověření zdali role FSMO běží na novém serveru v pořádku se provede příkazem: Netdom query fsmo.



Obrázek 14. Odebrání Globálního katalogu ze starého serveru

9.5 Migrace DHCP

9.5.1 Export DHCP databáze z Windows server 2003 R2

1. Spustí se příkazový řádek - Win+R - cmd - Enter
2. Zadá se příkaz: netsh

3. Zadá se příkaz: DHCP
4. Zadá se příkaz: server \\vydsrv001.vydos.local
5. Zadá se příkaz: export c:\w2k3DHCPdb

9.5.2 Import DHCP databáze na Windows Server 2012 R2

1. Zkopíruje se databáze na disk s Windows Server 2012.
2. Otevře se konzole správce serveru a klikne se Přidat role a funkce
3. Vybere se instalace na základě rolí nebo funkcí a klikne se na Další.
4. Vybere se server vydsrv001 z fondu serverů
5. Vybere se role DHCP.
6. Zvolí se přidat výchozí funkce, které služba vyžaduje- nechá se ve výchozím stavu - Další
7. Ve výsledném potvrzení se klikne na Instalovat, po skončení se v konzoli správce serveru objeví položka DHCP
8. Spustí se příkazový řádek - pravé tlačítko myši v levém dolním okně - spustit příkazový řádek (správce)
9. Vypne se server zadáním příkazu net stop dhcpserver
10. Smaže se DHCP.mdb zadáním příkazu del c:\windows\system32\DHCP.
11. Zapne se server zadáním příkazu net start dhcpserver
12. Zadá se příkaz: netsh
13. Zadá se příkaz: DHCP
14. Zadá se příkaz: server \\vydsrv003
15. Zadá se příkaz: import c:\w2k3DHCPdb
16. Restartuje se DHCP server zadáním příkazů net stop dhcpserver a potom net start dhcpserver
17. Vypnutí a odebrání role DHCP ze serveru Windows 2003 R2.
18. Autorizace DHCP serveru s doménou.

9.6 Migrace File Serveru

9.6.1 Instalace Windows Server Migration Tools na Windows Server 2012 R2

1. Otevře se konzole správce serveru a klikne se Přidat role a funkce
2. Vybere se instalace na základě rolí nebo funkcí a klikne se na Další
3. Vybere se server z fondu serverů vydsrv003
4. Vybere se funkce Windows Server Migration Tools
5. Ve výsledném potvrzení se klikne na Instalovat

9.6.2 Příprava balíčku nasazení pro zdrojový server

1. Spustí se powershell - start - spustit powershell
2. Zadá se příkaz `C:\Windows\System32\ServerMigrationTools\SmigDeploy.exe /package /architecture X86 /os WS03 /path "C:\Migration"`
3. Nastaví se sdílení pro danou složku a zkopíruje se na server s Windows 2003 R2
4. V příkazovém řádku se nastaví cesta ke zkopírované složce a zadá se příkaz `smigdeploy.exe`
5. V nabídce start přibyl zástupce Migration Tools v něm se provedou následující příkazy na obou serverech:

9.6.3 Migrace

- Na straně serveru s Windows 2003 R2
 1. `Add-PSSnapin Microsoft.Windows.ServerManager.Migration`
 2. `Get-Command -Module Microsoft.Windows.ServerManager.Migration`
- Na straně serveru s Windows 2012 R2
 1. `Add-PSSnapin Microsoft.Windows.ServerManager.Migration`
 2. `Get-Command -Module Microsoft.Windows.ServerManager.Migration`
 3. `Receive-SmigServerData`
 4. `ues as password` zadá se heslo

- Na straně serveru s Windows 2003 R2
 1. Send-SmigServerData -ComputerName "vydsrv003" -DestinationPath "D:\Users" -Include All -SourcePath "D:\users" -Recurse
 2. Export klíče - regedit najít následující klíč - export
HKEY_LOCAL_MACHINE>SYSTEM>CurrentControlSet>Services>Lanman Server>Shares
- Na straně serveru s Windows 2012 R2
 1. Import klíče - překopírovat exportovaný klíč na server - regedit - import (pouze pokud je stejné písmeno jednotky jako na starém serveru, v opačném případě nutno editovat)

Poznámka: Na serveru s Windows 2003 R2 musí být nainstalován Microsoft .NET Framework 2.0 a Windows PowerShell minimálně ve verzi 1.0.

9.7 Migrace SQL

Sql server bude provozován na druhé instanci operačního serveru Windows Server 2012 R2 instalovaného jako druhá VM.

9.7.1 Instalace SQL serveru

1. Z webu Microsoftu se stáhne instalační soubor SQLEXPRT_x64_ENU.exe
2. V SQL Server installation center se zvolí New SQL Server stand-alone installation
3. Potvrdí se licenční podmínky - Next
4. Potvrdí se zahrnutí updatu - Next
5. Vyberou se instalované služby - select all - Next
6. Zadá se jméno instance VydosSQLEXPRESS
7. Zadá se umístění instalace serveru D:\Microsoft SQL Server\
8. Zadá se heslo a druh spouštění pro Servisní účty Database Engine a Browser
9. Zvolí se forma Authentizace - Windows

9.7.2 Migrace SQL serveru

Spustí se PowerShell a zadají následující příkazy na straně serveru s Windows 2003 R2:

1. Set-ExecutionPolicy RemoteSigned
2. Import-Module SQLPS
3. Backup-SqlDatabase -ServerInstance vydsrv001\VydosSQL2005 -Database echotrack -BackupAction Database

Spustí se PowerShell a zadají následující příkazy na straně serveru s Windows 2012 R2:

1. Set-ExecutionPolicy RemoteSigned
2. Import-Module SQLPS
3. Restore-SqlDatabase -ServerInstance vydsrv004\VydosSQL2012 -Database echotrack
4. -BackupFile "\\vydosrv001\Backup\echotrack.bak" -ReplaceDatabase
5. Opakování postupu pro ostatní databáze

Poznámka: Při tomto postupu je databáze automaticky povýšena na funkčnost SQL serveru verze 2012 dobré ověřit u autorů jednotlivých databází funkčnost, v opačném případě by se muselo postupovat jiným způsobem.

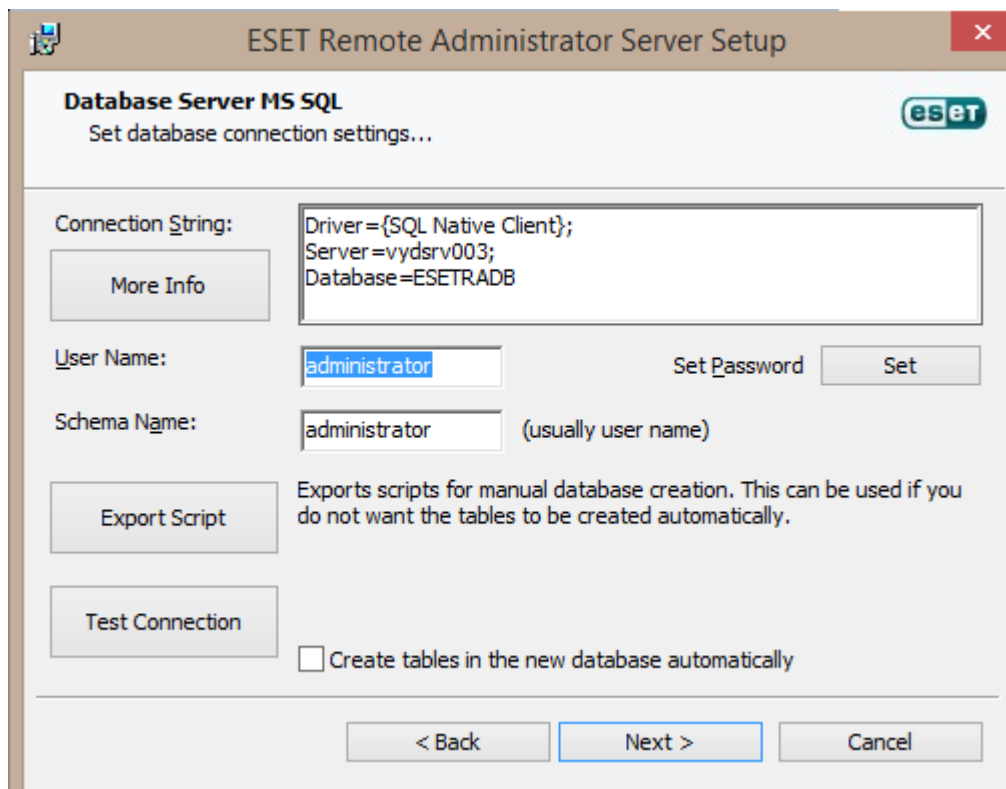
9.8 Instalace ostatních služeb a aplikací

9.8.1 ESET

- **ESET Remote Administrator Server**

1. Na webu firmy Eset se stáhne instalátor ESET Remote Administrator Server
2. Spustí se instalátor ESET Remote Administrator Serveru
3. Odsouhlasí se licenční podmínky a klikne se na tlačítko Next
4. Zvolí se typ instalace - Advanced - Next
5. Vloží se licenční soubor .lic, který byl obdrženo při nákupu.

6. Zvolí se výchozí složka instalace programu C:\Program Files\ESET\ESET Remote Administrator\Server\ - Next
7. Zvolí se pod jakým účtem bude služba startovat - zvolí se Local System Account
8. Zvolí se typ databáze - MS SQL server - Next
9. Nastavení se provede dle následujícího obrázku:



Obrázek 15. Nastavení přístupu programu k SQL databázi

10. Nastaví se porty, na kterých přistupuje k serveru konzole, klienti a replikace - ponechá se výchozí
11. Nastaví se heslo pro konzoli, vzdálenou instalaci, klienty a replikaci
12. Nastaví se server, ze kterého jsou brány aktualizace a jméno a heslo k serveru
13. Nastaví se smtp server - smtp mail.vydos.cz
14. Nastaví se emailová adresa eset@vydos.cz a přihlašovací údaje
15. Nastaví se umístění logů - log to OS Application Log
16. Klikne se na tlačítko Install

- **ESET Remote Administrator Console**

1. Spustí se instalátor ESET Remote Administrator Serveru
2. Odsouhlasí se licenční podmínky a klikne se na tlačítko Next
3. Zvolí se typ instalace - Advanced - Next
4. Zvolí se výchozí složka instalace programu C:\Program Files\ESET\ESET Remote Administrator\Console\ - Next
5. Zadá se název serveru - vydosrv004 a komunikační port 2223 - Next

9.8.2 Firemní aplikace

Databáze jednotlivých firemních aplikací byly migrovány v rámci migrace SQL serveru, o finální instalaci programů se postaraly vzdáleně firmy poskytující jednotlivé programy v rámci servisní smlouvy.

9.8.3 PowerChute Network Shutdown

V případě nasazení vizualizačního řešení of firmy VMware, je nutné docílit korektního vypínání serveru v případě poruchy elektrické sítě. Z tohoto důvodu bude program PowerChute obsluhující UPS zálohující server instalován jako samostatná VM. Pomocí VMware vSphere Management Assistant 5.5 (vMA).

- **Instalace**

1. Připojí se k ESXi pomocí vSphere klienta
2. V menu File - Deploy OVF Template
3. Se zadá adresa OVF Template pro VMA. (dostupná na webu VMware po přihlášení)
4. Pokračovat dále jako při vytváření normální virtual machine - nazvat virtual machine, vybrat datastore, network apod.
5. OVF template se stáhne a vytvoří se virtual machine.
6. Spustí se VMA.
7. Nastavit VMA je možno provést na konzoli po naboťování. První se nastavuje síť, potom heslo pro uživatele vi-admin.


8. Po nastavení je možno se přihlásit přes SSH (jako uživatel vi-admin) a provedou se následující příkazy:
9. Mkdir powerchute
10. Cd powerchute
11. Wget <https://www1.osu.cz/software/pcns201ESXi.tar.gz>
12. tar xvzf pcns301ESXi.tar.gz
13. cd ESXi/
14. sudo /install_en.sh
15. Následuje odsouhlasení licenčních podmínek - Enter
16. Nastaví se umístění instalace javy - Stiskněte klávesu Enter pro ponechání výchozí hodnoty
17. Nastaví se umístění instalace PowerChute – Stiskne se klávesa Enter pro ponechání výchozí hodnoty
18. Zobrazí se dialog pro potvrzení, zadá se yes a stiskne se klávesa Enter
19. Zadá IP VMware hostitele a stiskne se klávesa Enter
20. Zadá login na VMware ESXi a stiskne se klávesa Enter
21. Zadá se heslo pro příslušného uživatele a stiskne se klávesa Enter

Poznámka: Pokud bu se objevilo chybové hlášení Failed to add ESXi host. tak je třeba přidat hostitele příkazem: sudo vifp addserver IP_HOSTITEL -username root

- **Konfigurace**

1. Konfigurace se provádí přes web - adresa je https://IP_VMA:6547
2. Uvítací dialog se odklikne tlačítkem - Next.
3. Nastaví se jméno a heslo pro přihlášení do web rozhraní
4. Zadá se Authentication Phrase pro připojení klienta k SNMP management kartě - Next

5. Vybere se první položka (Using power from a single UPS.) - Next
6. NMC Protocol - nechá se http.
7. NMC Port - nechá se 80.
8. NMC IP address - zadá se adresa UPS v našem případě 192.168.1.8 - Next
9. PowerChute uloží nastavení a spojí se s SNMP management kartou. - Finish
10. Na obrazovce web rozhraní PowerChute se klikne na Configure Events
11. U položky UPS: On Battery se klikne na čtvereček ve sloupci Shut Down System
12. Zaškrtně se Yes, I want to shut down the PCNS operating system
13. Nastaví se čas na 600 sekund. - Apply



PowerChute
— NETWORK SHUTDOWN

Configure Events ?

The table below identifies how PowerChute Network Shutdown will respond to UPS events. Select an icon to see the details of the event.

Events	Log Event	Notify Users	Run Command File	Shut Down System
UPS: On Battery	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Input Power: Restored	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Runtime: Exceeded	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Runtime: Normal Again	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Battery: Discharged	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Battery: Recharged	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Bypass: Due to a Fault	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Bypass: For Maintenance	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Bypass: Manual	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Bypass: Ended	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Bypass Switch: Failed	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Obrázek 16. Konfigurační prostředí PowerChute

9.8.4 RDS a WSUS

Dané služby běží ještě na starém serveru vydsrv002 a to z důvodu problémů s nasazením plánovaných RemoteApp ve zkušebním virtuálním prostředí, další odlazování a testování by zpomalilo celkový, jednou už schválený proces migrace na nové operační systémy, doinstalace, testování a následná konfigurace těchto služeb a odstavení druhého serveru vydsrv002 bude probíhat až po odevzdání této práce.

9.8.5 SysAid

1. Na webu firmy SysAid se stáhne instalátor SysAid Server Free
2. Spustí se instalátor SysAid Server Free
3. Odsouhlasí se licenční podmínky a klikne se na tlačítko Next
4. Zvolí se typ instalace - Customized - Next
5. Zvolí se výchozí složka instalace programu D:\SysAidServer - Next
6. Zvolí se výchozí složka instalace programu D:\SysAidServer\Repository - Next
7. Pokud najde instalaci MSSQL serveru umístí databázi do ní po zadání hesla, pokud ne nainstaluje Express verzi
8. Další konfigurace se může přeskočit, bude načtena později se zálohované databáze
9. Nastaví se porty, na kterých přistupuje k serveru konzole, klienti a replikace - ponechá se výchozí
10. Nastaví se jazyk - Angličtina
11. Nastaví jméno a heslo administrátora systému
12. Změna jazykové verze
13. Settings-Customize-Account Defaults - klikne se na přidání jazyku a zatrhne čeština
14. Settings-Customize-Translation - klikne se na přidání jazyku a zatrhne čeština
15. Obnova databáze - popsáno v kapitole o migraci SQL

9.9 Finální konfigurace

- **Odstavení starého doménového řadiče**

1. Klepne se na tlačítko Start, klepne se na příkaz Spustit, zadá se příkaz dcpromo do pole Otevřít a poté klepnutím na tlačítko OK se spustí Průvodce instalací služby Active Directory.
2. Klepne se na tlačítko Další
3. Nezaškrtnout tlačítko - tento server je posledním řadičem domény klepne se na tlačítko Další
4. Zadá se uživatelské jméno a heslo s oprávněními správce rozlehlé sítě pro tuto doménu a poté klepněte na tlačítko Další
5. Zadá se a potvrdí heslo účtu Administrator na serveru a poté klepněte na tlačítko Další
6. Klepne na tlačítko Další v dialogu Shrnutí
7. Klepnutím na tlačítko Dokončit se odebere služba Active Directory z počítače.

- **Změna IP adresy a názvu nového doménového serveru**

1. Spustí se powershell - start - powershell a zadají se následující příkazy:
2. Rename-Computer vydsrv001 -DomainCredential administrator heslo
3. New-NetIPAddress -InterfaceAlias "Sít' Ethernet" -IPv4Address "192.168.1.10" -PrefixLength 24 -DefaultGateway 192.168.1.1
4. Aktivace Windows slmgr - ipk product key. (Aktivace se provede i na druhé instanci Windows Serveru)

9.9.1 Zálohování

Vzhledem k omezenému rozpočtu nezbyly prostředky pro efektivní zálohování VM v podobě sofistikovaných nástrojů typu Veeam Backup & Replication, případně jiných, nemluvě o nezbytnosti zakoupení placené verze VMware ESXi, free verze je limitována nemožností zapisovat do vSphere Command-Line Interface (vSphere CLI),

což znemožňuje nasazení zálohovacích řešení třetích stran, z tohoto důvodu bylo přistoupeno na zálohování pomocí Windows Server Backup na Network Attached Storage (NAS) pomocí protokolu iSCSI. Konfigurace probíhala následujícím způsobem:

1. Přihlášení k NAS serveru přes webové rozhraní a zadání loginu a hesla a klikne se na tlačítko manage
2. V záložce storage - iSCSI - Add ani SCSI drive
3. Posuvník aktivace funkce se přepne na ON
4. Zadá se jméno jednotky - BackupVydsrv001 a kapacita 900GB
5. Pro obě jednotky se vytvoří uživatel Backup a zadá se mu heslo.
6. V rámci obou instancí se připojí disky pomocí iSCSI Software Initiator
7. Start - powershell - iscsicp - Enter
8. V záložce cíle se zadá iqn.2014-04.com.lenovoemc:storage.ix2.backupvydosrv001
9. Zobrazí se dialog connect to target zde se zvolí tlačítko Advanced a zaškrtně se enable CHAP log on
10. Zadá se jméno a heslo vytvořené při tvorbě LUNu - OK
11. Start - powershell - diskmgmt.msc - Enter
12. V konzoli je vidět připojený nový svazek, pravé tlačítko myši vytvořit nový svazek
- Další - kapacitu ponechat na maximu - nepřirázovat písmeno jednotky ani cestu (Server Backup jednotku uvidí) - formát NTFS - velikost alokační jednotky - výchozí - název Backup - zaškrtnout rychlý formát a kompresi - Další - Dokončit.
13. Install-WindowsFeature Windows-Server-Backup -IncludeAllSubFeature
14. Start - powershell - wbadmin.msc - Enter
15. Plán zálohování - Celý server - Další
16. Více než jednou denně - 0:00 a 12:00
17. Zálohovat na pevný disk vyhrazený pro zálohy - vybrat připojený iSCSI disk - Další
18. Zobrazí se přehled, co bude zálohováno - Dokončit.
19. Obdobě se nastaví i druhá instance Windows Server 2012 R2

10 MIGRACE KLIENTSKÝCH STANIC

Vzhledem k výsledku SW auditu, kdy pouze 6 z 28 stanic s Windows XP splňovalo HW požadavky pro upgrade na operační systém Windows 8.1 a další dvě stanice by vyžadovaly upgrade BIOSu, byl vedením lehce navýšen rozpočet a bylo koupeno 28 nových klientských stanic, namísto plánovaných 20. Z tohoto důvodu nebude zapotřebí nástrojů jako Microsoft Deployment Tools, zakoupené stanice mají již od výroby instalován operační systém se všemi aktualizacemi a základními programy (toto se dá považovat za způsob „High Touch deployment with Standard Image“, časová náročnost na vytížení administrátora vzhledem k faktu, že bude muset uživatele proškolit na nový operační systém a PC zapojit a tím stejně trávit nějaký čas u uživatele, by v tomto konkrétním případě byla spíše navýšena. Výsledná migrace klientských stanic tedy probíhala podle bodů:

1. Rozbalení PC.
2. Roztřídění podle uživatelů, kteří budou používat balík Microsoft Office 2013, druhé skupině bude nainstalován editor Libre Office.
3. Výměna PC.
4. Přidání PC do domény.
5. Konfigurace emailových klientů.
6. Instalace firemních aplikací.
7. Instalace lokálních tiskáren, které nejsou v adresáři AD.
8. Školení uživatele ohledně nového operačního systému.
9. Finální test funkčnosti a přizpůsobení potřebám konkrétního uživatele.

ZÁVĚR

Pokud je hardware srdcem počítače, je operační systém jeho duší. V zásadě platí, že teprve operační systém představuje charakteristiku počítače, a proto je důležité, aby byl vždy v bezvadném stavu. Protože dne 8. dubna 2014 přestává společnost Microsoft oficiálně podporovat operační systém Windows XP a vzápětí 14. července 2015 serverový operační systém Windows Server 2003 R2 a není možno po tomto datu nadále provozovat nepodporované operační systémy, bylo proto nutné provést na 28 klientských počítačích ve firmě Vydos servis a.s. migraci stávajícího provozovaného operačního systému Microsoft Windows XP na nový operační systém. V rámci migrace se též migroval serverový operační systém na verzi Windows Server 2012 R2.

Jako nový operační systém klientských stanic byl vybrán Microsoft Windows 8.1, i když zbytek stávající infrastruktury využívá operačního systému Windows 7. Tento systém byl vybrán z důvodu nutného pokroku, Windows 7 tu nebudou věčně a uživatele je nutné připravit na nové operační systémy a možnosti, které skýtají. V případě klientského operačního systému byl nakonec zvolen ne úplně ideální migrační scénář High Touch deployment with Standard Image, kdy je operační systém se základními programy, případně dalšími produkty od firmy Microsoft již předinstalován na rozdíl od Light Touch deployment s využitím nástroje Microsoft Deployment Toolkit a to z důvodu zhodnocení větší zátěže na administrátora v přípravě migrace, zejména pokud téměř hotový systém již byl dodán dodavatelem.

Důsledně zpracovaná analýza současného stavu síťové infrastruktury firmy a provedení SW auditu bylo důležitým krokem pro správnou volbu počtu nákupu nových stanic, zhodnocení výhodnosti upgrade koncových stanic oproti nákupu nových a časového harmonogramu migrace. Nejdůležitější částí bylo ověření funkčnosti a stanovení doby migrace jednotlivých síťových služeb poskytovaných serveru firmy, zejména pro dosažení minimální odstávky IT infrastruktury a minimálního dopadu na chod firmy. Nadále byla zpracována SWOT analýza, která hrála hlavní úlohu při přesvědčování vedení firmy o důležitosti upgrade na novější verze operačních systémů a schválení rozpočtu.

Samotná doba realizace projektu do plné funkčnosti trvala 14dní, prvních pět dní se jednalo o přípravnou část, schvalování, nákup HW a SW a testování průběhu migrace ve virtuálním prostředí, nejkritičtější část a to migrace serverů byla zvládnuta za tři dny, 2 dny s minimálním omezením chodu firmy a jednodenní odstávkou infrastruktury.

Firma realizací projektu a nasazením moderních technologií získala zejména zvýšení bezpečnosti klientských i operačních systémů, zjednodušení a urychlení správy operačních systémů a vzhledem i k implementaci virtualizace též snížení spotřeby elektrické energie a nákladů na HW obnovu a údržbu serverů.

Postupy použité v rámci této Diplomové práce kombinují klasickou konfiguraci pomocí GUI, příkazů v příkazovém řádku a v powershellu a v některých případech je lze zaměnit, postupy popsané v práci byly voleny s ohledem na co nejjednodušší konfiguraci a s menšími odchylkami je lze aplikovat i v jiných organizacích.

SEZNAM POUŽITÉ LITERATURY

- [1] Microsoft Corporation, *Přehled informací o životním cyklu Windows* [cit. 2012-11-28]. Dostupné online. <http://windows.microsoft.com/cs-cz/windows/lifecycle>
- [2] QTD spol s.r.o., *Proč přejít z Windows XP na vyšší verzi z hlediska bezpečnosti* [cit. 2012-11-28]. Dostupné online. http://www.qtd.cz/dokumenty/prechod_z_xp_bezpecnost.pdf
- [3] NORTHROP, Anthony. *Mistrovství v Microsoft Windows 8: kompletní průvodce do posledního detailu*. 1. vyd. Brno: Computer Press, 2013, 615 s. ISBN 978-80-251-4111-3.
- [4] Microsoft Corporation, *Windows Server 2012 Licencing Data Sheet* [cit. 2012-11-28]. Dostupné online. http://download.microsoft.com/download/0/4/B/04BD0EB1-42FE-488B-919F-3981EF9B2101/WS2012_Licensing-Pricing_Datasheet.pdf
- [5] Microsoft Corporation, *Windows Server 2012 R2 Products and Editions Comparison* [cit. 2012-11-28]. Dostupné online. <http://download.microsoft.com/download/D/4/6/D464EB09-9999-48DC-82F0-C82DB6A4A091/Windows%20Server%202012%20R2%20Products%20and%20Editions%20Comparison.pdf>
- [6] Microsoft Corporation, *Feature Comparison Windows Server 2003 R2, Windows Server 2008 R2, and Windows Server 2012* [cit. 2012-11-28]. Dostupné online. http://download.microsoft.com/download/3/F/2/3F24A601-D7B1-4F68-91C3-CFADB2CD419D/WS%202012%20Feature%20Comparison_Windows%20Server%200Versions.pdf
- [7] Microsoft Corporation, *Server Roles and Technologies in Windows Server 2012* [cit. 2012-11-28]. Dostupné online. <http://technet.microsoft.com/cs-cz/library/hh831669.aspx>
- [8] LYNN, Samara. *Windows server 2012: up and running*. 1st ed. Sebastopol, CA: O'Reilly Media, 2012c2013, xi, 243 pages. ISBN 14-493-2075-9.
- [9] ZACKER, Craig. *Exam ref 70-410: installing and configuring Windows server 2012*. xiii, 384 pages. ISBN 978-073-5673-113.

- [10] AUDITPRO. *Příručka administrátora systému* [cit. 2012-11-30]. Dostupné online: <http://www.auditpro.cz/data/files/auditpro70cz-96.pdf>
- [11] HYNDRÁKOVÁ Martina, *Softwarový audit v praxi* [cit. 2012-11-29]. Dostupné online. <http://www.systemonline.cz/clanky/softwarovy-audit-v-praxi.htm>
- [12] FREML Martin, *Detailní přínosy softwarového auditu* [cit. 2012-11-28]. Dostupné online. <http://www.freml.cz/index.pdf>
- [13] MAREŠ Martin, *přínos auditu SW*, [cit. 2012-11-28]. Dostupné online. http://www.matcom.cz/audit_software_3.htmmatcom.cz
- [14] Microsoft Corporation, *Migrate Roles and Features to Windows Server 2012 R2 or Windows Server 2012* [cit. 2012-11-28]. Dostupné online http://download.microsoft.com/download/0/F/B/0FBFAA46-2BFD-478F-8E56-7BF3C672DF9D/Migrate_Roles_and_Features_to_Windows_Server_2012_R2_or_Windows_Server_2012.pdf
- [15] Microsoft Corporation, *Upgrade Domain Controllers to Windows Server 2012* [cit. 2012-11-28]. Dostupné online. <http://technet.microsoft.com/en-us/library/hh994618.aspx>
- [16] BARTOLO, Anthony, *Step-By-Step: Active Directory Migration from Windows Server 2003 to Windows Server 2012 R2* [cit. 2012-11-28]. Dostupné online. <http://blogs.technet.com/b/canitpro/archive/2014/04/02/step-by-step-active-directory-migration-from-windows-server-2003-to-windows-server-2012.aspx>
- [17] BARTOLO, Anthony, *Step-By-Step: Migration of DHCP from Windows Server 2003 to Windows Server 2012* [cit. 2012-11-28]. Dostupné online. <http://blogs.technet.com/b/canitpro/archive/2013/04/29/step-by-step-migration-of-dhcp-from-windows-server-2003-to-windows-server-2012.aspx>
- [18] VÝŠEK, Ondřej, *Edice Windows 8, porovnání, jak migrovat* [cit. 2012-11-28]. Dostupné online. <http://www.optimalizovane-it.cz/windows-8/edice-windows-8-porovnani-jak-migrovat.html>
- [19] Microsoft Corporation, *Deploy Windows 8.1* [cit. 2012-11-28]. Dostupné online. <http://technet.microsoft.com/cs-cz/windows/hh974336.aspx>

[20] PLZÁK, Jan. *Konfigurace serveru jako řadiče domény pro malou podnikovou síť* Zlín, 2012. bakalářská práce (Bc.). Univerzita Tomáše Bati ve Zlíně. Fakulta aplikované informatiky

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AD	Active Directory
AD CS	Active Directory Certificate Services
AD DS	Active Directory Domain Services.
AD FS	Active Directory Federation Services
AD LDS	Active Directory Lightweight Directory Services
AD RMS	Active Directory Rights Management Services
ASLR	Address Space Layout Randomization
BIOS	Binary Input Output System
CAL	Client Access License
CD	Compact Disc
CSV	Cluster Shared Volume
DC	Domain Controller
DDR	Double Data Rate
DEP	Data Execution Prevention
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DSRM	Directory Services Restoration Mode
DVD	Digital Versatile Disc
ELAM	Early Laung AntiMalware
EFS	Encrypting File System
FSMO	Flexible Single Master Operation
FTP	File Transfer Protocol
GC	Global Catalog
GPO	Group Policy

GUI	Graphical User Interface
HP	Hewlett-Packard
HW	Hardware
CHAP	Challenge-Handshake Authentication Protocol
IAS	Internet Authentication Service
IBM	International Business Machines Corporation
IIS	Internet Information Services
IP	Internet Protocol
IRM	Information Rights Management
ISCSI	Internet Small Computer System Interface
IT	Information Technology
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LP	Logical Procesor
LUN	Logical Unit Number
MMC	Microsoft Management Console
NAS	Network Atached Storage
NUMA	Non-Uniform Memory Access
NTFS	New Technology File System
OEM	Original Equipment Manufacturer
OLP	Open License Program
OU	Organizational Unit
PC	Personal Computer
PE	Preinstallation Environment
POP3	Post Office Protocol

RAM	Random-Access Memory
RDS	Remote Desktop Services
RRAS	Routing and Remote Access Service
SAM	System Asset Management
SAN	Storage Area Network
SMB	Server Message Block
SNMP	Simple Network Management Protocol
SSL	Secure Socket Layer
SSO	Single Sign-On
SQL	Structured Query Language
SW	Software
TLS	Transport Layer Security
UAC	User Account Control
UEFI	Unified Extensible Firmware Interface
UPS	Uninterruptible Power Supply
VDI	Virtual Desktop Infrastructure
VLAN	Virtual Local Area Network
VM	Virtual Machine
VMA	vSphere Management Assistant
VPN	Virtual Private Network
VSS	Volume Shadow Copy Service
WDS	Windows Deployment Services
WSMT	Windows Server Migration Tools
WSUS	Windows Server Update Services

SEZNAM OBRÁZKŮ

Obrázek 1. Srovnání podpory operačních systémů Windows Server	17
Obrázek 2. Ukázka kombinace ADDS a AD LDS	28
Obrázek 3. Cyklus softwarového auditu.	38
Obrázek 4. Postup migrace AD DS	43
Obrázek 5. Možnosti migrace Windows 8.....	44
Obrázek 6. Graf SWOT analýzy projektu migrace operačních systémů	49
Obrázek 7. Schéma počítačové sítě firmy Vydos servis a.s.....	54
Obrázek 8. Doménová struktura a lokality	57
Obrázek 9. Ukázka prostředí programu SysAid	61
Obrázek 10. Ukázka prostředí ESXi přes klienta vSphere	65
Obrázek 11. Snap-in modul Domény a vztahy důvěryhodnosti.....	69
Obrázek 12. Registrace DLL pro použití snap-in modulu Schéma Active Directory.....	69
Obrázek 13. Snap-in modul Schéma služby Active Directory	70
Obrázek 14. Odebrání Globálního katalogu ze starého serveru.....	71
Obrázek 15. Nastavení přístupu programu k SQL databázi.....	76
Obrázek 16. Konfigurační prostředí PowerChute.....	79

SEZNAM TABULEK

Tabulka 1. Srovnání podpory operačních systémů Windows.....	14
Tabulka 2. Srovnání bezpečnostních funkcí operačních systémů Windows	15
Tabulka 3. Přehled rozdílů mezi jednotlivými edicemi	18
Tabulka 4. Srovnání funkcionalit jednotlivých síťových rolí mezi edicemi.....	19
Tabulka 5. Srovnání funkcionalit jednotlivých služeb mezi edicemi	20
Tabulka 6. Srovnání zásadních změn mezi generacemi systému Windows Server.....	22
Tabulka 7. Cenová kalkulace projektu.....	49
Tabulka 8. Časový harmonogram a popis jednotlivých etap a dopadů na provoz firmy	51
Tabulka 9. Přehled firemních serverů	53
Tabulka 10. Přehled aktivních prvků	56
Tabulka 11. Přehled VLAN	57
Tabulka 12. Přehled vylepšení jednotlivých stanic pro nasazení Windows 8.1	62
Tabulka 13. Přehled generací koncových stanic, možnosti a ceny upgrade	62