Hromadné nasazení OS Windows a jeho zabezpečení v prostředí velké organizace

Deployment and Security of Windows in Large Organizations

Bc. Jan Křivák

Diplomová práce
2013

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2012/2013

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

Jméno a příjmení:	**Bc. Jan Křivák**
Osobní číslo:	**A11349**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Hromadné nasazení MS Windows a jeho zabezpečení v prostředí velké organizace**

Zásady pro vypracování:

1. **Popište přípravy na nasazení nové verze OS Windows v prostředí velké organizace.**
2. **Vyhodnoťte kompatibilitu provozovaného SW s novou verzí OS.**
3. **Objasněte způsoby nasazení pomocí nástrojů Windows AIK, WDS, LTI a ZTI.**
4. **Navrhněte referenční image s novým OS Windows.**
5. **Nasaďte OS Windows pomocí Lite-Touch nebo Zero-Touch technologie.**
6. **Doporučte způsob řešení migrace uživatelských dat.**
7. **Zabezpečte uživatelské prostředí a naplánujte způsob instalace aplikací a aktualizací.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **TULLOCH, Mitch. Windows 7 resource kit. Redmond, WA: Microsoft Press, c2010, xlviii, 1709 p. ISBN 978-073-5693-852.**
2. **SMITH, Ben a Brian KOMAR. Zabezpečení systému a sítě Microsoft Windows. 1. vyd. Překlad David Krásenský, Anna Rychetská. Brno: Computer Press, 2006, 700 s. ISBN 80-251-1260-8.**
3. **MICROSOFT CORPORATION. 6294A Planning and Managing Windows 7 Desktop Deployments and Environments: Microsoft Official Course. Microsoft Corporation, 2009, 623 s. X17-40182.**
4. **MICROSOFT CORPORATION. 6292A Installing and Configuring Windows 7 Client: Microsoft Official Course. Microsoft Corporation, 2009, 459 s. X17-37160.**
5. **BOTT, Ed, Carl SIECHERT a Craig STINSON. Mistrovství v Microsoft Windows 7. Vyd. 1. Brno: Computer Press, 2010, 936 s. ISBN 978-80-251-2817-6.**
6. **VÝŠEK, Ondřej. Optimalizovane IT: Nové myšlenky pro vaše it [online]. [cit. 2013]. Dostupné z: http://optimalizovane-it.cz/**
7. **MICROSOFT CORPORATION. Microsoft TechNet: Materiály pro IT odborníky [online]. [cit. 2013]. Dostupné z: http://technet.microsoft.com/cs-cz/**

Vedoucí diplomové práce: **doc. Ing. Martin Sysel, Ph.D.**
Ústav počítačových a komunikačních systémů

Datum zadání diplomové práce: **8. února 2013**

Termín odevzdání diplomové práce: **3. června 2013**

Ve Zlíně dne 8. února 2013

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Cílem této Diplomové práce je úspěšné provedení migrace stávajícího, v dnešní době již technologicky zastaralého operačního systému Microsoft Windows XP na operační systém Windows 7 na více jak 4400 počítačích ve Všeobecné zdravotní pojišťovně České Republiky. Teoretická část objasňuje všeobecné poznatky různých metod nasazení operačních systémů a charakterizuje nejčastěji používané nástroje pro Windows Deployment. Zároveň představuje možnosti zabezpečení uživatelských prostředí v prostředí velkých organizací. Praktická část popisuje současný stav ve Všeobecné zdravotní pojišťovně České Republiky, plánuje a realizuje nejvhodnější způsob nasazení nového operačního systému, zabezpečuje uživatelské prostředí z pohledu klientských počítačů a navrhuje způsob vzdálené instalace aplikací a aktualizací.

Klíčová slova: Microsoft Windows XP, Microsoft Windows 7, Windows Deployment, Microsoft Deployment Toolkit, Lite-Touch High-Volume Deployment, Nasazení, Referenční Image, Obraz, Zásady skupiny

ABSTRACT

The target of this Thesis is represented by successful migration of the existing and technologically already obsolete operating system Windows XP to the operating system Windows 7 on more than 4,400 computers in the General Health Insurance Company of the Czech Republic. The theoretical part clarifies general knowledge about various implementation methods of operating systems and characterizes the most often used tools for Windows Deployment. At the same time, theoretical part represents options how to protect the user environment in large organization. The practical part describes the existing situation in the General Health Insurance Company of the Czech Republic, plans and implements the most suitable implementation method of the new operating system, protects the user environment from the aspect of client computers and proposes the method of remote installation of applications and updates.

Keywords: Microsoft Windows XP, Microsoft Windows 7, Windows Deployment, Microsoft Deployment Toolkit, Lite-Touch High-Volume Deployment, Implementation, Reference Image, Image, Group Policy

PODĚKOVÁNÍ

Děkuji svému vedoucímu Diplomové práce doc. Ing. Martinu Syslovi, Ph.D. za profesionální a vstřícný přístup, cenné rady a připomínky, které mi poskytl k vypracování mé práce.

Dále pak děkuji paní Marku Škopovi za užitečné rady a Všeobecné zdravotní pojišťovně ČR za poskytnuté informace.

MOTTO

„Mnohem větší tragédie než je nedosáhnout cíle, je nemít žádný cíl.“

Benjamin Mays

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

Změna operačního systému na počítači může být pro uživatele noční můrou a není těžké pochopit proč. Uživatel si zpravidla myslí, že nenajde své původní soubory na místech, kde s nimi naposledy pracoval, že se zásadně změní ovládání systému nebo aplikace, se kterými byl zvyklý pracovat, nebude je mít k dispozici, nebo místo nich budou aplikace jiné. V neposlední míře to může být obecně strach z nových technologií nebo jejich záměrné odmítání.

Cílem Diplomové práce je provedení migrace stávajícího provozovaného operačního systému Microsoft Windows XP na nový moderní operační systém ve Všeobecné zdravotní pojišťovně České Republiky. Hlavním důvodem pro přechod na nový operační systém je ukončení podpory produktu Windows XP ze strany společnosti Microsoft k 8. dubnu 2014.

Diplomová práce je rozdělena na dvě části - teoretickou a praktickou.

V teoretické části bude provedena literární rešerše, týkající se nasazení nového operačního systému v organizacích pomocí různých technologií, počínaje obecnou instalací z DVD disku, konče plně automatizovaným nasazením pomocí technologie Lite-Touch High Volume Dynamic Deployment nebo Zero-Touch Deployment s využitím migračních scénářů In-Place Deployment, Wipe-and-Load Deployment nebo Side-by-Side Deployment. Součástí této části je objasnění problematiky řešení migrace uživatelských dat a obecné nahlédnutí na oblast zabezpečení uživatelského prostředí.

Praktická část bude rozdělena na část přípravnou a realizační. V první přípravné části bude představena Všeobecná zdravotní pojišťovna ČR. Následná analýza zjistí softwarové a hardwarové vybavení na počítačích uživatelů a stanoví předpoklady pro nasazení konkrétního operačního systému. Tyto skutečnosti spolu s možnostmi síťových prostředků a serverových technologií poslouží pro zvolení správného migračního scénáře, časového harmonogramu migrace a strategie pro referenční obraz. Poté bude následovat důkladná příprava migračních nástrojů s následným provedením migrace operačního systému na všech uživatelských počítačích v rámci celé pojišťovny.

Na závěr bude navržen centrální způsob instalace aktualizací operačního systému a aplikací a konkrétní zabezpečení uživatelského prostředí nejmodernějšími technologiemi z pohledu nově nasazeného operačního systému.

I. TEORETICKÁ ČÁST

1 PŘÍPRAVA NA NASAZENÍ SYSTÉMU WINDOWS VE FIREMNÍM PROSTŘEDÍ

Provoz nového operačního systému má mnoho výhod, nicméně mnoho organizací nasazení operačního systému považuje za komplikované a ekonomicky náročné. Právě složitost a cenu nasazení nového operačního systému (OS) rychle vyváží jeho výhody.

Mezi další úskalí nasazení patří:

- Nekompatibilita aplikací;
- Přenos uživatelských dat a nastavení;
- Nedostatek nástrojů pro provedení migrace;
- Nedostatek znalostí a zkušeností pro provedení migrace;
- Nedostatek podpory a školení pro koncové uživatele.

Nasazení nové verze operačního systému Microsoft Windows 7 se v organizaci zpravidla neobejde bez kvalitního projektu řešícího kompletní analýzu, návrh, implementaci a instalaci.

1.1 Důvody nasazení nového operačního systému

Než se začne uvažovat o nasazení nového operačního systému, je třeba si uvědomit, proč vlastně migraci provádět. Je mnoho důvodů proč nový OS zavést. Pro někoho jsou tyto důvody opodstatněné, pro druhého nikoliv. Je ale nesporné, že nový systém Windows obsahuje celou řadu novinek a zefektivnění práce pro koncové uživatele či administrátory IT.

Z pohledu koncového uživatele můžou rozhodování ovlivnit tyto funkce:

- Nové uživatelské rozhraní;
    - Hlavní panel a náhledy na celou obrazovku;
    - Seznamy odkazů;
    - Vylepšená práce s okny;
- Služba Windows Search;
- Lepší správa zařízení;
- Domácí skupina;
- Vyšší výkon;
- Podpora dotykových obrazovek;

- Vylepšené řízení spotřeby;
- Nové možnosti zabezpečení;
    - BitLocker ToGo;
    - Přepracovaný User Account Control [30].

Pro administrátora IT mohou být zajímavé například tyto funkce:

- Kompatibilita aplikací a zařízení;
- Stejné jádro operačního systému společné se serverovým systémem;
- Kontrola nad problémy a jednodušší řešení problémů;
- Spolupráce Windows 7 s Windows Serverem 2008;
    - DirectAccess;
    - BranchCache;
    - Nové možnosti nasazení operačního systému;
    - Rozšířená správa pomocí skupinových politik [30];

Kompletní porovnání jednotlivých verzí Windows 7 jsou součástí přílohy č. 1.

Zásadním důvodem přechodu na novější verzi operačního systému je v mnoha případech ukončení podpory aktuálně provozovaného operačního systému ze strany společnosti Microsoft. Absence vydávání aktualizací představuje pro organizaci značně velký bezpečnostní problém.

Nové vlastnosti operačního systému nemusí být ovšem jediným důvodem přechodu na jeho novější verzi. Dalším z důvodů je unifikace provozovaného prostředí a s tím související jeho jednoduchá údržba a podpora. Tyto výhody vedou k levnějšímu a efektivnějšímu provozu IT technologií a to je managementem v podnikové nebo státní sféře pozitivně vnímáno.

Zřejmě není možné vždy najít platné důvody, které by dokázaly odpovědět na otázku, z jakého důvodu přejít na nový operační systém. Každé IT prostředí je odlišné, má různé problémy a specifické požadavky, které je třeba znát ještě před přípravou projektu a to je klíčem k úspěchu.

Z některých studií uváděných na internetu [30] je možné vysledovat problematické oblasti s provozem a správou moderních IT prostředí – pro příklad, 68% společností bojuje s problémy při nemožnosti správy počítačů, které nejsou fyzicky připojené do firemní sítě;

10% volání na helpdesk je spojeno s VPN konektivitou; 14% volání na helpdesk je způsobeno instalací neautorizovaného software uživatelem.

Tato čísla se však mohou změnit v případě nasazení technologií, které Windows 7 a Windows Server 2008 R2 nabízejí – např. DirectAccess umožňuje správu počítačů i v případě, že se připojují pomocí internetu do firemní sítě a navíc není nutné, aby uživatel musel ručně vytvářet VPN připojení – vše je předkonfigurováno správou IT. AppLocker umožňuje efektivní správu možností instalace a provozu software uživatelem. Ve spojení s vhodnou kombinací UAC je tedy možné i u mobilních uživatelů dosáhnout použitelné a funkční konfigurace operačního systému v kombinaci se zajištěním zabezpečeného prostředí [30].

1.2 Nástroje na podporu plánovací fáze

Plánovací fáze projektu vyžaduje shromažďování informací sloužících k analýze stávajícího prostředí a jejího upravení pro potřeby úspěšného nasazení OS. V případě, že nebude projekt dobře připraven, je možné, že se v průběhu nasazení vyskytne nějaký problém, který může vlastní proces zpomalit či úplně zastavit. Technické a finanční otázky projektu je třeba zvážit v jeho přípravné části.

- Kolik stolních a přenosných počítačů organizace vlastní?
- Jaký je poměr počítačů na uživatele? Je více počítačů než uživatelů nebo je více uživatelů než počítačů?
- Existuje v tomto projektu racionalizace nebo snížení zdrojů (počítačů, aplikací a software)?
- Kolik počítačů je možné migrovat bez nutnosti nákupu dalšího hardware?
- Jak rychle může být migrace dokončena na existující infrastruktuře?
- Jak dlouhá je návratnost investice?
- Jaká jsou případná rizika implementace?
- Je třeba řešit vzdělání administrátorů a uživatelů?

1.2.1 Windows 7 Upgrade Advisor

Windows 7 Upgrade Advisor (W7 UA) aktuálně ve verzi 2.0.4 je nástroj, který zdarma poskytuje společnost Microsoft a jehož úlohou je ověřit kompatibilitu konkrétního PC a instalace Windows.

Prověřují se čtyři aspekty: splnění minimálních HW požadavků, možnost přímého upgrade Windows, kompatibilita dalšího HW a dostupnost ovládačů a kompatibilita instalovaného software. V případě problémů s kompatibilitou rovněž navrhne řešení.

1.2.2 Assessment and Planning Toolkit

Microsoft Assessment and Planning (MAP) Toolkit je nástroj pro neinvazivní provedení inventarizace, kalkulace nasazení a reportingu v prostředích, ve kterých se uvažuje o migracích či konsolidacích. MAP Toolkit po nasazení do firemní sítě nejprve provede inventarizaci stávajících prostředků a sběr dat, na základě těchto dat pak navrhne optimální cestu migrace. Blíže se tomuto nástroji věnuje kapitola 1.3.3.

1.2.3 Application Compatibility Toolkit

Microsoft Application Compatibility Toolkit (ACT) verze 5.6 obsahuje nezbytné nástroje a dokumentaci pro posouzení a zmírnění problémů s kompatibilitou aplikací před nasazením systému Windows 7, Windows Vista, Windows Update, nebo nové verze aplikace Internet Explorer. Více se této problematice věnuje kapitola 1.4.3.

1.2.4 System Center Configuration Manager

Microsoft System Center Configuration Manager 2007 (SCCM) poskytuje komplexní serverové řešení pro správy změn a konfigurací na platformě Microsoft. Configuration Manager umožňuje provádět např. tyto úlohy: nasazení operačního systému, nasazení softwarové aplikace, nasazení aktualizací software, měření využití software, zhodnocení odchylky od požadované konfigurace, HW a SW inventarizaci, vzdálenou správu PC.

Configuration Manager shromažďuje informace v databázi Microsoft SQL Server. Může řídit širokou škálu operačních systémů společnosti Microsoft, včetně klientských a serverových platforem a mobilních zařízení.

1.2.5 System Center Essentials

Microsoft System Center Essentials 2010 (SCE) je řešení v rodině produktů System Center pro správu systémů informačních technologií. Je určen pro středně velké firmy do 50 serverů a 500 klientů. Essentials 2010 představuje ucelené řešení pro správu, umožňující IT specialistům v organizacích střední velikosti proaktivně a efektivněji spravovat jejich IT prostředí. Využívá jednoduchého průvodce instalací pro všechny součásti a požadované komponenty, což napomáhá jeho rychlému uvedení do provozu [27].

1.2.6 Asset Inventory Service

Asset Inventory Service 2.0 je aplikace, která je součástí Microsoft Desktop Optimization Packu (MDOP). AIS pomocí klientské části, instalované na firemních počítačích, sbírá potřebná data a následně je zpracovává v rámci online služby. Přístup k této službě je zajištěn pomocí webové konzole.

Na základě údajů posbíraných z klientských počítačů zpracovává detailní přehledy o hardware a software [1]. K provozu není třeba serverová architektura.

1.3 Posouzení aktuálního prostředí pro nasazení nové verze systému Windows

Před nasazením Windows 7 je třeba prověřit, že počítače splňují minimální hardwarové požadavky potřebné pro provoz systému. Dále je třeba učinit rozhodnutí, která edice systému Windows bude nejlépe vyhovovat potřebám organizace a jaké platformy bude, zdali 32-bit nebo 64-bit.

Po ověření hardwarových požadavků a zvolení správné edice existuje několik možností, jak nainstalovat a nasadit Windows. V závislosti na konkrétních faktorech, jako je například IT infrastruktura v organizaci nebo politiky, bude vybrán jeden nebo více způsobů instalace [13].

1.3.1 Edice systému Windows 7

K dispozici je šest druhů edic Windows 7. Pro běžné spotřebitele i profesionální uživatele, specializované edice pro podnikové zákazníky, technické nadšence, pro rozvíjející se trhy a pro začátečníky. Vlastnosti každého vydání odpovídají požadavkům jednotlivých typů uživatelů [12].

Obr. 1. Edice systému Windows 7 [12]

Z obrázku č. 1 je patrné, že pro firemní využití slouží edice Professional, Enterprise a Ultimate. Všechny edice mimo Starter jsou jak ve verzi 32-bit tak i 64-bit.

Přehled klíčových vlastností základních edicí systému Windows 7 je znázorněno na obrázku č. 2, detailní porovnání všech edicí je pak součástí přílohy č. II.

Přehled hlavních funkcí jednotlivých edicí systému	Windows 7 Starter	Windows 7 Home Premium	Windows 7 Professional	Windows 7 Ultimate
Vylepšený hlavní panel a seznamy odkazů (Jump lists)	✓	✓	✓	✓
Rychlé vyhledávání pomocí služby Windows Search	✓	✓	✓	✓
Připojení k domácí skupině (HomeGroup)	✓	✓	✓	✓
Centrum akcí (Action Center)	✓	✓	✓	✓
Nástroj Device Stage™	✓	✓	✓	✓
Vysílání datových proudů médií v domácí síti, včetně funkce Přehrát v zařízení (Play To)	✓	✓	✓	✓
Nástroj Fax a skener	✓	✓	✓	✓
Živé náhledy oken		✓	✓	✓
Přepínání mezi uživateli bez nutnosti odhlášení		✓	✓	✓
Připojení k počítačům v okolí bez potřeby speciálního síťového hardware		✓	✓	✓
Podpora více monitorů		✓	✓	✓
Centrum nastavení mobilních zařízení		✓	✓	✓
Pozadí Aero®, Aero Glass a pokročilá práce s okny		✓	✓	✓
Dotykové ovládání Windows® Touch a rozpoznávání českého rukopisu Tablet PC		✓	✓	✓
Vytvoření domácí skupiny (Home Group)		✓	✓	✓
Windows® Media Center a Windows DVD Maker		✓	✓	✓
Vypalování a přehrávání DVD		✓	✓	✓
Vzdálené vysílání datových proudů médií (Remote Media Streaming)		✓	✓	✓
Windows XP Mode: provozování mnoha starších aplikací v systému Windows 7			✓	✓
Tisk podle umístění (Location Aware Printing)			✓	✓
Připojení k doméně a zásady skupiny			✓	✓
Pokročilé zálohování a obnovení (síť a zásady skupiny), šifrování souborů EFS			✓	✓
Offline soubory (Offline Folders)			✓	✓
BitLocker™ a BitLocker To Go™				✓
AppLocker™				✓
DirectAccess				✓
BranchCache™				✓
Vícejazyčné uživatelské rozhraní pomocí jazykových balíčků				✓
Podnikové vyhledávání (Enterprise Search Scopes)				✓

Obr. 2. Porovnání jednotlivých edicí systému Windows 7 [36]

1.3.2 Hardwarové požadavky pro Windows 7

Pro správný běh systému je důležité, aby splňoval minimální HW požadavky pro edici, která se bude instalovat. Pokud počítač nesplňuje minimální požadavky na hardware, nemusí

některé funkce systému fungovat správně, nebo se může snížit úroveň výkonu systému na nepřijatelnou hranici.

Tab. 1. Minimální HW požadavky pro provoz systému Windows 7

Hardware	Minimální požadavky
Procesor	1 GHz
Paměť RAM	1 GB paměti RAM (32bitový systém) nebo 2 GB paměti RAM (64bitový systém)
Grafická karta	Grafické zařízení DirectX 9 s ovladačem WDDM 1.0 nebo vyšším
Harddisk	16 GB volného místa na disku (32bitový systém) nebo 20 GB (64bitový systém)
Optická mechanika	DVD mechanika v případě instalace z DVD média

Pokud se plánuje zabezpečení PC pomocí implementace BitLockeru, musí být na systémovém disku vytvořeny dvě partitions, obě formátované souborovým systémem NTFS. Podrobně se této technologii věnuje samostatná kapitola 4.1.3 zabezpečení uživatelského rozhraní.

1.3.3 Inventarizace hardware

První oblastí, kterou bude pravděpodobně nutné připravit a získat o ní informace při přípravě migrace, je hardware. Zde se nabízí volně dostupný nástroj Microsoft Assessment and Planning Toolkit (MAP), který je velice jednoduchý v instalaci a použití.

Výsledkem práce s tímto nástrojem jsou reporty, které pomohou identifikovat provozovaný hardware, verze operačních systémů, kontroly ovladačů a aplikací. Všechny tyto informace jsou sumarizovány do reportů (Excel a Word dokument), kde jsou uvedeny všechny důležité informace o současném stavu a návrhy akcí, které umožní hromadné nasazení Windows 7 [30].

Verze 8.0 umožňuje zhodnotit, zda je u daného prostředí možné zpracovat a nasadit jeden či více následujících produktů či služeb: Windows 8, Windows 7, Office 2010, Office 2013, Office 365, Windows Server 2012, Windows 2008 R2, SQL Server 2012, Hyper-V, Microsoft Private Cloud Fast Track a Windows Azure [11].

Report „Not Windows 7 Ready“ znamená, že po úpravě (uvolnění místa na disku či doplnění paměti) je možné Windows 7 provozovat. V tom okamžiku se počítač stává

„Windows 7 Ready“. „Cannot RunWindows 7“ zůstanou označena ta PC, u kterých není možný běh Windows 7 ani po provedení úprav.

Nástroj MAP může být nainstalovaný na jakýkoliv počítač v síti, součástí instalace je SQL Server 2008 Express Edition. Instalací MAP je vytvořena vlastní instance SQL.

Před spuštěním skenování počítačů je zapotřebí na koncových počítačích splnit některé předpoklady, především povolení výjimek z lokálních firewallů (porty TCP 135 a 445, UDP 137 a 138). Pokud jsou počítače provozovány v rámci pracovní skupiny (nepřipojené do domény), je nutné vytvořit na všech počítačích identický účet se stejným heslem, aby mohla být použita tzv. pass through authentication. Pokud mají být skenovány i operační systémy Windows Server 2003 x64, je nutné doinstalovat Windows Installer Provider (MSI Provider) pro WMI – tento provider není součástí instalace 64bitové edice Windows Server 2003. Pro Windows NT 4.0 je pak zapotřebí instalovat celý WMI core [30].

1.4 Kompatibilita aplikací

Před vlastním upgradem aktuální verze Windows na jakoukoli vyšší verzi musí organizace otestovat své provozované aplikace, aby bylo zjištěno, že jsou kompatibilní s novou verzí Windows. Pokud má organizace několik stovek aplikací v celé své síti, mohou problémy s kompatibilitou jedné nebo více aplikací zabránit uživatelům plnění jejich úloh. To může mít zásadní dopad na běh a fungování firmy.

Za úspěšné nasazení nového operačního systému se dá označit takové nasazení, kde v organizacích nedochází k výpadkům z důvodů nefunkčních aplikací či problémům s uživatelskými profily, které byly migrovány z předchozí verze operačního systému [11].

1.4.1 Nejčastější problémy s kompatibilitou

Většina programů vytvořených pro systém Windows XP je funkční i ve Windows 7, ale některé starší programy nemusí fungovat správně nebo se nedají spustit vůbec. Pokud nelze program vytvořený pro starší verzi systému Windows správně spustit, lze to řešit následujícími způsoby.

1.4.1.1 User Account Control

V případě, že je uživatel členem skupiny lokálních administrátorů tak tato technologie zajišťuje to, že desktop a aplikace běží jako u uživatele standardního. Potřebuje-li aplikace administrátorská práva, tak uživateli zobrazí dialogové okno, kde musí odsouhlasit povýšení

oprávnění. Uživatel, který nevlastní administrátorská práva, nemůže měnit součásti operačního systému. Při případném vniknutí škodlivého SW na PC nejsou způsobeny tak veliké škody.

UAC tedy zajišťuje větší úroveň zabezpečení informací na koncových počítačích zejména v podnikových prostředích a na počítačích, kde pracuje více uživatelů. Problematice UAC se věnuje kapitola 4.1.5.

1.4.1.2 Provoz interaktivních služeb a ovladačů

U Windows XP bylo možno provozovat služby a aplikace, které zasílaly informace do prostředí přihlášeného uživatele - služby a ovladače běžely ve stejné session. U Windows 7 jsou provozovány služby a aplikace v naprosto oddělené relaci a není tedy možné přímo zasílat informace na uživatelský desktop. Tuto funkcionalitu využívají například některé služby sledující hardware a v případě problémů uživatele informují. Podobných aplikací se vyskytuje celá řada a jedná se především o aplikace vyvinuté uvnitř firem vlastními vývojáři [31].

1.4.1.3 Změna verze operačního systému

Windows 7 má verzi operačního systému 6.1. Kupodivu toto vede k lepší spolupráci především s aplikacemi, které kontrolují přítomnost Windows XP (verze 5.1). Aplikace kontrolují „MajorVersion“ a „MinorVersion“, kde u Windows Vista byly způsobeny problémy s verzí (6.0) [31].

1.4.1.4 Windows Resource Protecion

Windows Resource Protecion (WRP) zabraňuje nahrazení základních systémových souborů, složek a klíčů registru, které jsou nainstalovány jako součást operačního systému. Byl k dispozici již ve Windows Server 2008 a Windows Vista. Plná práva pro přístup k modifikaci WRP chráněného zdroje má pouze TrustedInstaller. Pokud tedy nějaká aplikace modifikuje soubory chráněné WRP, akce skončí chybou a systém obnoví původní soubor.

1.4.1.5 Chráněný mód Internet Exploreru

Když je UAC zapnutý, může být IE provozován v protected módu. Pak může Internet Explorer zapisovat pouze do souboru s mezipaměti. Jestliže se IE snaží provést zápis do jiných adresářů, aktivuje se UAC s potvrzením případné akce.

1.4.1.6 Uživatelský profil na jiném místě

Počínaje Windows Vista výše jsou uživatelské profily místo adresáře *„Documents and Settings“* umístněny v adresáři *„Users“*. To může některým aplikacím, které nevyužívají systémové proměnné pro přístup k vlastním souborům působit problém – soubor nemohou najít.

1.4.1.7 Platforma x64

Při volbě operačního systému, který se bude nasazovat, je nutné také zvážit, jakou bitovou architekturu zvolit. Platforma x64 bezesporu přináší velké množství výhod, ale je nutné mít na zřeteli, že není možné provozovat 32bit ovladače a není možné provozovat 16bit aplikace [31]. Všechen moderní HW za posledních pět let již obsahuje ovladače pro 64bit platformu a u 16bit aplikací je provoz možno zajistit Windows XP módem.

1.4.2 Testování aplikací

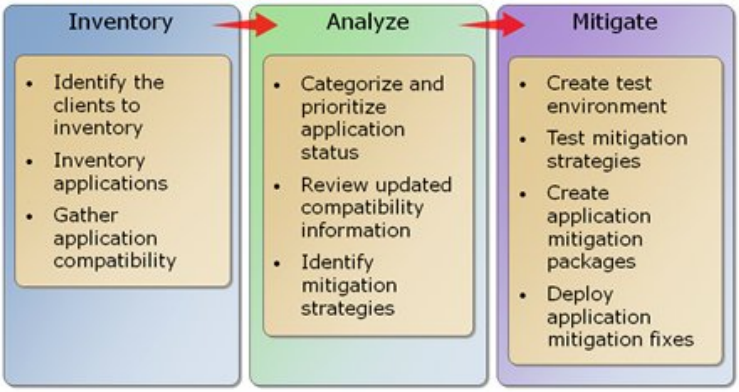
Většina komerčních aplikací běží na Windows 7 bez problémů. Doporučuje se ale všechny Business Critical aplikace otestovat na aplikační kompatibilitu, aby jejich funkčnost splňovala očekávání. Společný test musí obsahovat minimálně:

- Nainstalovat aplikaci při přihlášení jako standardní uživatel a znovu jako správce;
- Přihlásit se jako standardní uživatel a otestovat funkce důležité pro koncového uživatele;
- Vyzkoušet všechny možnosti instalace, které jsou použity v organizaci;
- Aplikovat Zásady skupiny pro uživatele a počítače a zjistit, zdali nastavení skupinových politik nemá negativní vliv na aplikace;
- Spuštění kombinace více aplikací na standardním nastavení desktopu;
- Vyzkoušet manipulaci s velkými soubory;
- Otestovat HW (tiskárny, skenery apod.) připojené jako Plug and Play zařízení.

Proces testování aplikační kompatibility je patrný z obrázku č. 3. a skládá se z těchto tří fází:

- ***Fáze inventarizace*** určuje klientské počítače a aplikace, které budou do procesu testování kompatibility zahrnuty;
- ***Fáze analýzy*** kategorizuje aplikace dle priorit, které nejsou kompatibilní s novou verzí OS;

- ***Fáze zmírnění*** navrhuje vytvoření testovacího prostředí pro minimalizaci negativních dopadů ze zavedení nové verze OS.



Obr. 3. Proces testování aplikační kompatibility [13]

Mezi metody na zmírnění dopadu nekompatibility aplikací patří:

- Upgrade aplikace na kompatibilní verzi;
- Úprava konfigurace aplikace;
- Změna nastavení zabezpečení;
- Spuštění aplikace ve virtualizovaném prostředí;
- Použití funkcí kompatibilitu aplikací;
- Výběr jiné aplikace, která splňuje stejné funkce.

1.4.3 Posuzování a řešení problémů s kompatibilitou aplikací pomocí ACT

Ve firmením prostředí se využívají nástroje, řešící problematiku kompatibility aplikací centrálně. Zde se přímo nabízí centrální řešení od společnosti Microsoft pod názvem Application Compatibility Toolkit (ACT). ACT obsahuje komponenty zajišťující sběr informací na uživatelských PC a jejich předání na server, zpracování do databáze a rozhraní pro práci s daty.

- Sběr na koncových počítačích zajišťuje tzv. Data Collection Provider (DCP), který je připravený jako .msi balíček a je možné jej instalovat mnoha různými metodami na počítače. DCP je na počítači automaticky spuštěn a monitoruje běh aplikací na původním operačním systému před migrací (např. Windows XP). Dle konfigurace DCP předává informace na síťové sdílení ve formátu XML v pravidelných intervalech. Informace, které jsou na počítačích, se týkají především problémů s provozem aplikací jako standardní uživatel - tedy následně UAC problémy. Také

mohou být například zpracovány informace, týkající se kompatibility Internet Exploreru atd. [31].

- Zpracování informací a zařazení do databáze zajišťuje na straně serveru Log Processing Service (LPS), která detekuje přítomnost nových XML souborů na síťovém sdílení, soubory zpracuje a zařadí do databáze. V případě, kdy prostředí neobsahuje tisíce počítačů a stovky aplikací, je možné využít pro ukládání SQL 2008 Express, který je zdarma, případně je možné využít stávající instalaci SQL v organizaci [31].
- Následné zpracování informací administrátory probíhá pomocí Application Compatibility Manager (ACM). Jedná se o běžnou aplikaci, která se připojuje k databázi, kde jsou uloženy informace z koncových počítačů. V rámci ACM je možné provést různé klasifikace podle druhu aplikace, její důležitosti pro provoz organizace atd. Také je možné provést synchronizaci informací s databází kompatibility Microsoftu, kde uživatelé z celého světa umisťují informace o tom, která aplikace je či není kompatibilní a jakým způsobem je možné aplikaci zprovoznit [31].

ACT stačí nasadit na určitý reprezentativní vzorek uživatelů, je zbytečné monitorovat všechny PC v organizaci. Časový úsek sledování je vhodné zvolit delší, protože ne všechny aplikace jsou spouštěny pravidelně a je nutné zajistit, aby běžely v době, kdy je monitorování pomocí DCP aktivní. Proto se délka toho intervalu volí asi 1 měsíc.

Pokud ACT vyhodnotí nějakou aplikaci jako problematickou s ohledem na UAC, provede se její opětovné testování pomocí Standard User Analyzeru (SUA), který je součástí ACT. SUA běží na původním operačním systému a v tomto nástroji je rovněž spuštěna problematická aplikace. Po ukončení činnosti aplikace SUA vyhodnotí volání API a identifikuje problematická místa. Následně dokáže připravit DLL knihovnu, která uzpůsobí funkčnost aplikace tak, aby nevyžadovala administrátorské oprávnění.

ACT podporuje operační systémy Windows XP SP2 a novější, Windows Server 2003 SP a novější. Již nejsou podporovány Windows 2000 a starší a Windows NT Server 4.0. Jako databázi využívá MS SQL Server minimálně ve verzi 2005 včetně varianty Express.

2 WINDOWS DEPLOYMENT

Instalační proces Windows Vista, Windows 7 i Windows 8 je založený na Image-base instalační architektuře. Tato architektura se sestává z nástrojů a technologií pro nasazení, které pomáhají s přizpůsobením a nasazením Windows v rámci celé organizace. Pomocí těchto nástrojů mohou organizace nakonfigurovat efektivní počítačové obrazy a metodiku nasazení pro bezpečný a standardizovaný systém Windows v desktopovém prostředí.

2.1 Scénáře nasazení

Volba správného scénáře nasazení je z převážné části závislá na rozpočtu a IT infrastruktuře organizace. Každá z metod se dá do jisté míry automatizovat pro zmenšení operativy IT oddělení.

2.1.1 In-Place Deployment

Pod pojmem In-place (upgrade) rozumíme přeinstalování stávajících Windows na novou verzi. Výhodou je zachování instalace aplikací a nastavení, nevýhodou možné problémy s kompatibilitou ovladačů i aplikací. Stará Windows a další složky jsou uložena do adresáře *„Windows.old“* kvůli záloze [15].

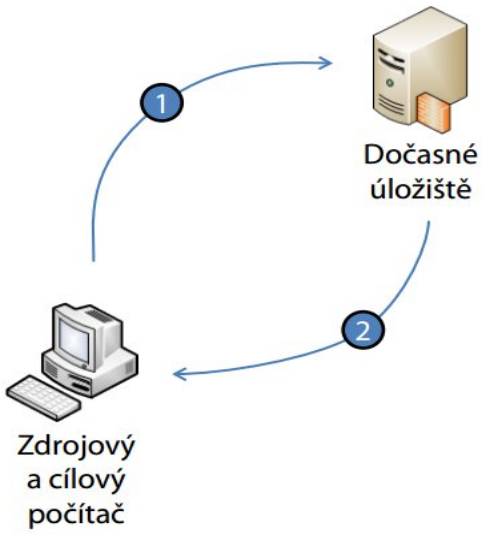
Vlastní proces upgrade se spouští souborem *„setup.exe“* volbou upgrade z instalačního média. Ještě před provedením je vhodné provést full backup systémového disku nebo systémové partition. Na konci upgrade se doinstalují potřebné ovladače. Aplikace, které nejsou funkční, se aktualizují.

2.1.2 Wipe-and-Load Deployment

Scénář Wipe-and-Load (refresh) nahrazuje stávající provozovaný operační systém operačním systémem novým v rámci jedné pracovní stanice. Následně se importují uživatelská data a nastavení z předchozích Windows, jak je znázorněno na obrázku č. 4. Typický postup pro provedení refresh migrace je následující:

- Záloha systémového disku nebo systémové partition;
- Export uživatelských dat a nastavení pomocí WET nebo USMT. Data, která nebudou exportována, budou ztracena;
- Spuštění *„setup.exe“* z instalačního média, volbou vlastní instalace se vybere partition pro instalaci;

- Instalace požadovaných uživatelských aplikací;
- Provedení importu uživatelských dat a nastavení.

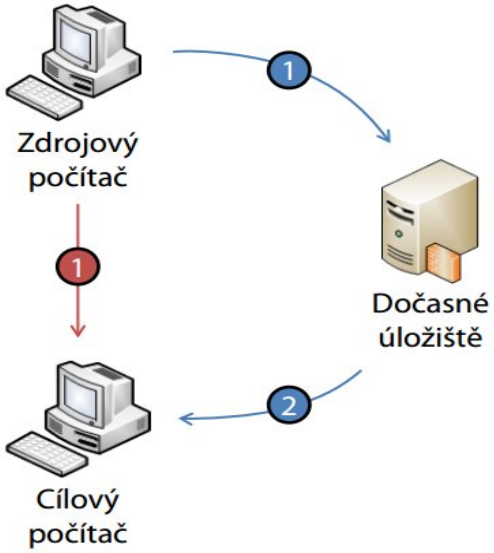


Obr. 4. Wipe-and-Load migrace [9]

2.1.3 Side-by-Side Deployment

Side-by-Side (replace) migrace se v organizacích používá nejčastěji v okamžiku nahrazování starých PC novými. Tento scénář se tedy aplikuje v případě migrace dat mezi dvěma počítači s možností využití dočasného úložiště dle obrázku č. 5. Data pořád zůstávají na zdrojovém počítači.

Postup pro povedení migrace formou replace je následující: na stávajícím PC se programem WET nebo USMT vyexportují uživatelské data a nastavení, na cílovém PC se provede čistá instalace nového operačního systému. Následně se doinstalují požadované uživatelské aplikace a provede import uživatelských dat a nastavení. Po ověření správné funkčnosti nového PC je možno data ze zdrojového (původního) PC odstranit. Při této variantě migrace není třeba původní PC zálohovat.



Obr. 5. Side-by-Side migrace [9]

2.2 Návrh standardního image Windows

Převážná většina středních a velkých organizací používají pro OS Deployment model Image-base instalace pro desktopové operační systémy [13]. Po instalaci a konfiguraci referenčního počítače se zachytí jeho bitová kopie, která slouží jako instalační zdroj.

Image-base architektura se sestává a nástrojů a technologií, které pomáhají s přizpůsobením a nasazením Windows v rámci celé organizace. Tato sbírka nástrojů včetně dokumentace je součástí Windows Automated Installation Kitu (Windows AIK). Pomocí těchto nástrojů lze nakonfigurovat image PC a metodiku nasazení, která bude poskytovat standardizovaný systém Windows v rámci celé organizace.

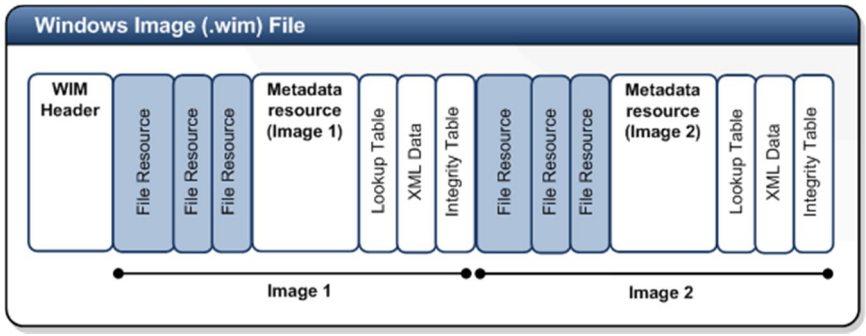
2.2.1 Windows Imaging File Format

Windows Imaging File Format (WIM) je soubor založený na obrazu disku představený již v systému Windows Vista. WIM soubory jsou komprimované balíčky obsahující několik souvisejících souborů. Formát souboru WIM je optimalizován pro dosažení maximální komprese pomocí LZX, rychlé komprese pomocí Xpress, nebo je nekomprimovaný.

2.2.1.1 Struktura WIM souboru

Struktura souboru WIM obsahuje šest typů zdrojů: header, file resource, metadata resource, lookup table, XML data a integrity table [37]. Na obrázku č. 6 je znázorněno obecné uspořádání souboru WIM, který obsahuje dva image.

- WIM Header – hlavička WIM definuje obsah souboru WIM včetně paměti klíčových zdrojů (metadat, lookup tabulky, XML dat) a další atributy WIM souborů (verze, velikost, typ komprese);
- File Resources – řada balíčků, které obsahují zachycená data, jako jsou například zdrojové soubory;
- Metadata Resource – obsahují informace o zachycených souborech včetně adresářové struktury a atributů souborů;
- Lookup Table – zahrnuje paměťovou lokaci zdrojových souborů v souboru WIM;
- XML Data – soubor obsahující další údaje o image;
- Integrity Table – obsahuje bezpečnostní hash informace používané pro ověření integrity image.



Obr. 6. Struktura souboru WIM [37]

Mezi hlavní výhody formátu WIM patří:

- Jeden WIM soubor může řešit více hardwarových konfigurací. WIM nevyžaduje, aby cílový hardware odpovídal hardware vstupnímu. Jedním obrazem je možno řešit vícero hardwarových konfigurací;
- Do jednoho souboru WIM lze uložit více obrazů;
- WIM umožňuje kompresi a Single Instancing. Tím se významně snižuje velikost obrazu. Single Instancing je technika, která umožňuje v případě více obrazů sdílet jednu kopii souborů, které jsou společné mezi instancemi;
- WIM umožňuje obsluhovat obraz v offline režimu. Je možno přidávat nebo odebírat některé prvky operačního systému, soubory, aktualizace a ovladače bez vytvoření nového obrazu;

- WIM umožňuje nainstalovat obraz na oddíl disku, který je menší, rovný nebo větší než oddíl původní, který byl zachycen a pokud má cílový diskový oddíl dostatečný prostor pro uložení obsahu image;
- Windows 7 poskytuje API pro formát obrazu WIM s názvem WIMGAPI, které mohou vývojáři používat pro práci se soubory WIM;
- WIM umožňuje spuštění systému Windows PE ze souboru WIM. Instalační proces Windows 7 používá systém Windows PE. Soubor WIM je načten do paměti RAM, ze které se přímo spouští [13].

2.2.2 Konfigurační fáze instalace

Konfigurační fáze jsou děleny do sedmi částí a jejich správné použití je důležité pro přípravu a automatizaci instalace pomocí Windows System Image Manageru (Windows SIM, WSIM) nebo Windows AIK.

Jednotlivé konfigurační fáze jsou následující (pořadí zvoleno tak, aby odpovídalo WSIM):

- ***WindowsPE*** – jsou náhradou za bootloader známý z Windows XP. WindowsPE jsou víceméně plnohodnotná Windows, která podporují vícejazyčnost, sktiptování, WMI, ADO atd. V této fázi je možné nastavit např.: rozlišení obrazovky při instalaci, umístění ukládání *log* souborů, rozdělení a formátování disků, volbu instalačního image pro instalaci na počítač, volba cílové partition pro instalaci, spouštění různých konfiguračních skriptů.
- ***offlineServicing*** – tato fáze se používá pro integraci ovladačů, aktualizací apod. před započetím instalace operačního systému. OfflineServicing může být použitý kompletně mimo setup proces, kde se využívá také pro integrace aktualizací ovladačů, aktualizací OS a dalších balíčků ve spolupráci s nástrojem DISM. V této fázi je také aplikován odpovědní soubor do instalačního obrazu při spuštění instalace.
- ***generalize*** – fáze generalize je použita při přípravě počítače, před sejmutím image do wim souboru. Tato fáze je iniciována spuštěním nástroje *„sysprep /generalize“* a je možné automatizovat chod sysprep.
- ***specialize*** – fáze je spouštěna po rozbalení instalačního image a je pravým opakem fáze generalize. V této fázi jsou prováděna nastavení, která jsou specifická pro instalovaný počítač - nastavení sítě, mezinárodní nastavení, připojení do domény. Pokud je počítač nastartovaný do audit módu, pak setup pokračuje na auditSystem a auditUser. Pokud jde o standardní instalaci, pak setup pokračuje na oobeSystem.

- ***auditSystem*** – je fáze, která umožňuje OEM výrobcům a administrátorům přidávat další ovladače, aplikace do referenčního obrazu, stejně tak provést testování obrazu před jeho produktivním využitím. Při jeho tvorbě je možné vytvořit čistý obraz a teprve v audit módu přidávat ovladače, aplikace apod. Tato fáze je spuštěna pouze v případě, kdy je spuštěný sysprep s parametry *generalize* a *audit*.
- ***auditUser*** – tato fáze je automaticky spouštěna po fázi auditSystem, kde jsou aplikována nastavení pro audit, která se týkají uživatele.
- ***oobeSystem*** – jedná se o poslední fázi instalačního procesu a je spouštěna při prvním nastartování počítače po instalaci. V této fázi se provádí konfigurace prvního uživatele, název počítače, zpracovávají se uvítací obrazovky, ale také spouští různé skripty, které mohou provést další konfiguraci počítače [32].

2.2.3 Strategie sestavení image

Cílem většiny organizací je mít standardní konfiguraci pro PC, která je založena na společném obrazu pro každou verzi operačního systému. V ideálním případě je nejlepší použít univerzální image, aplikovat jej na libovolný počítač a následně jej přizpůsobit specifickým potřebám uživatele.

2.2.3.1 Thick images

„Tlustý“ obraz je monolitický celek obsahující klíčové aplikace, language packy, případně další data a nastavení. Vzniká instalací Windows na referenční počítač spolu s instalací dalších komponent před zachycením obrazu pomocí ImageX nebo MDT. Většina společností jde právě touto cestou. Výhodou je konzistence obrazu, každý dostane stejný základ, bez nutnosti spoléhat se na dodatečné instalace aplikací pomocí jiných metod. Nevýhodu bývá velká velikost obrazu a nutnost větší (častější) údržby obrazu pro udržení aktuálního stavu a s tím spojené celkové náklady [17].

2.2.3.2 Thin image

„Tenký“ obraz obsahuje minimální změny z originální distribuce Windows. Pouze několik dodatečných aplikací, či komponent, pokud vůbec nějaké. Nasazení takového obrazu na koncové stanice trvá krátkou dobu, aplikace, language packy apod. se instalují až ve spuštěných nainstalovaných Windows. Výhodou je variabilita přizpůsobení koncového počítače – nainstalují se pouze aplikace, které požaduje uživatel. Nevýhodou může být delší čas dokončení celkové instalace poté, co již uživatel mohl zjevně pracovat [17].

2.2.3.3 Hybrid image

Hybridní image kombinuje obě zmíněné metody. Lépe řečeno kompromis, mající pozitivní dopad na redukci nákladů a úsilí věnované údržbě a nasazení obrazů. Vychází z předpokladu určení základní konfigurace referenčního obrazu (ovladače kritické pro boot, aplikace, ovladače apod.) a redukce na minimální počet obrazů. Pokud je shoda pouze v jediném, jedná se o ideální stav. Zbytek aplikací, komponent a nastavení se aplikuje pomocí centrální správy, například zásad skupinových politik [17].

2.2.4 Faktory ovlivňující strategii nasazení

Objemné obrazy je třeba častěji aktualizovat, jsou náročnější na distribuci a testování. I když se aktualizuje pouze malá část obrazu, musí se poté distribuovat celý soubor [13]. Mezi hlavní faktory, které mohou ovlivnit strategii nasazení, patří:

- Geografické rozložení klientů nebo poboček – vysoké požadavky na distribuci, uvažovat o technologiích typu DFS pro replikaci obrazu mezi lokalitami;
- Specifické požadavky uživatelů – pokud například obchodní oddělení vyžaduje vlastní aplikace a ekonomické oddělení větší bezpečnostní opatření, většinou se skončí s několika obrazy, které jsou jinak nakonfigurované;
- Možnost duálního bootu – může existovat potřeba pro některé uživatele, aby měli více operačních systémů na jednom počítači;
- Síťová infrastruktura – někteří uživatelé se připojují vzdáleně na pomalých linkách, někteří nemají síťové připojení k dispozici vůbec;
- Administrace – například nastavení operačního systému bude realizováno pomocí zásad skupiny nebo bude zapracované již v základním image.

2.2.5 Údržba image

Uložené snímky je potřeba udržovat v aktualizované podobě. Servis obrazu představuje implementaci aktualizací a hotfixů, přidávání nebo odebírání balíčků ovladačů hardware, změnu jazykového nastavení, povolovaní nebo zakazovaní vestavěných funkcí Windows či změnu na vyšší edici Windows [13].

Offline údržba

Pokud je třeba do existujícího obrazu přidat aktualizaci, ovladač, odebrat či přidat Windows komponenty, language pack či nakopírovat do namapovaného obrazu soubory a adresáře,

nemusí se existující obraz instalovat na počítač kvůli provedení požadovaných změn[17]. Údržba se provádí příkazem DISM.

Online údržba

Tento typ údržby se prakticky rovná aplikaci Windows z obrazu, provedení změn a opětovné zachycení obrazu pro distribuci.

2.3 Nasazení pomocí Windows AIK

Instalační proces Windows lze zjednodušit tím, že využívá Image-base instalační architekturu, která je součástí Windows Automated Installation Kitu (Windows AIK, WAIK). Tato architektura obsahuje distribuční nástroje a technologie, které pomáhají s přizpůsobením instalace Windows 7 a jeho nasazením. Tím zajišťuje bezpečné a standardizované Windows 7 prostředí v rámci celé organizace.

2.3.1 Windows AIK

Windows Automated Installation Kit je sada nástrojů a dokumentace na podporu konfigurace a nasazení operačních systémů Windows. Sada Windows AIK automatizuje instalace systémů Windows 7, zaznamenává bitové kopie systému Windows 7 pomocí nástroje ImageX, konfiguruje a mění bitové kopie pomocí nástroje (DISM), vytváří bitové kopie systému Windows PE a migruje uživatelské profily a data pomocí nástroje Migrace profilu uživatele (USMT). Sada Windows AIK obsahuje také nástroj VAMT (Volume Activation Management Tool), který umožňuje automatizaci a centrální správu procesu aktivace více licencí pomocí aktivačního kódu MAK (Multiple Activation Key) [22]. Ve výchozím nastavení se Windows AIK instaluje do adresáře *„C:\Program Files\Windows AIK“*.

Windows AIK verze 3.0 podporuje konfiguraci a nasazení těchto operačních systémů:

- Windows Server 2003 with Service Pack 2;
- Windows Vista SP1;
- Windows Server 2008 family;
- Windows 7 family;
- Windows Server 2008 R2 family.

Metody nasazení Windows 7 pomocí nástrojů Windows AIK:

- Využití Windows PE a ImageX pro nasazení vlastního instalačního obrazu Windows ze sdílené síťové položky;
- Využití Windows Deployment Services (WDS) pro nasazení vlastního instalačního obrazu Windows ze serveru;
- Instalace operačního systému Windows i instalačního média přímo na nová PC.

Komponenty využívané ve výše uvedených metodách nasazení:

- ***Referenční počítač:*** na počítači je nainstalován systém Windows, z něhož je vytvořen instalační obraz. Obraz bude později zkopírován do cílových počítačů;
- ***Administrátorský počítač:*** počítač s instalovanou sadou Windows AIK, na kterém se bude vytvářet odpovědní soubor;
- ***Cílový počítač:*** počítač, kde bude nový OS Windows nainstalován;
- ***Odpovědní soubor:*** XML soubor, který obsahuje nastavení a konfiguraci vztahující se na image Windows během instalace;
- ***Konfigurační set:*** sada souborů a složek obsahující soubory řídící pre-instalační proces
- ***Katalog systému Windows:*** katalogový soubor obsahující seznam všech nastavení a balíčků v rámci Windows image.
- ***Audit Mode:*** fáze instalace systému Windows, která umožňuje dodatečné úpravy a testování před nasazením.
- ***ImageX:*** nástroj sloužící k zachycení a nasazení operačního systému Windows.
- ***Windows PE:*** jedná se o Windows 32-bit instalační prostředí s omezenými službami, postavené na jádře Windows. Windows PE poskytují prostředí pro přípravu počítače na instalaci systému Windows, kopíruje diskové obrazy ze síťového souborového serveru a startuje instalaci.
- ***Windows Deployment Services:*** serverové služby, které umožňují správci nastavit nové klientské počítače vzdáleně, aniž by museli navštívit každého klienta. Cíloví klienti musí podporovat vzdálené spuštění. Windows Deployment Services jsou náhradou za službu vzdálené instalace (RIS).

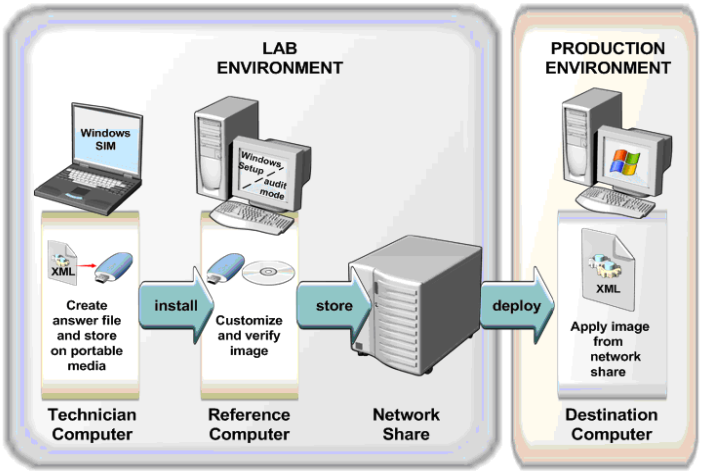
2.3.1.1 Nasazení ze sítě

Nasazení vlastního obrazu Windows pomocí sítě je ideální pro podniky s velkým počtem klientských počítačů, kde je hlavní prioritou rychlost nasazení. Tato metoda vytváří

a distribuuje obraz kombinací nástrojů ImageX a Windows PE. ImageX poskytuje technologie pro zachycení a vlastní instalaci Windows 7, Windows PE zabezpečuje stand-alone předinstalační prostředí včetně připojení k síti a konfiguraci disku.

Ve firemním prostředí umožňuje Image-base instalace rychlejší a konzistentní instalaci všech systémů. Jakmile je obraz vytvořen, může být instalován současně na více počítačích. Základní image může být přizpůsoben požadavkům konkrétního uživatele nebo skupiny uživatelů.

Proces vytváření obrazu začíná vytvořením odpovědního souboru pomocí Windows SIM a uložením konfigurace na vyměnitelné paměťové zařízení, například USB flash disk. Do referenčního počítače se vloží vyměnitelné médium, obsahující odpovědní soubor a produkt Windows 7. Počítač se spustí a instalační program systému Windows 7 používá nastavení uložené v odpovědním konfiguračním souboru.



Obr. 7. Struktura Image-base procesu nasazení [13]

Po dokončení instalace systému Windows 7 se systém restartuje do režimu auditu pro dodělání případných úprav a ověření, že konkrétní úpravy a nastavení byly aplikovány. Jakmile bude instalace odzkoušená, vytvoří se duplikát instalace systému nástrojem Sysprep, Imagex a Windows PE a uloží na sdílenou síťovou složku, viz obrázek č. 7.

Proces nasazení image začíná spuštěním cílového PC do prostředí Windows PE a připojením počítače do sítě. Následně se pomocí nástroje ImageX aplikuje vlastní image ze sdílené síťové složky.

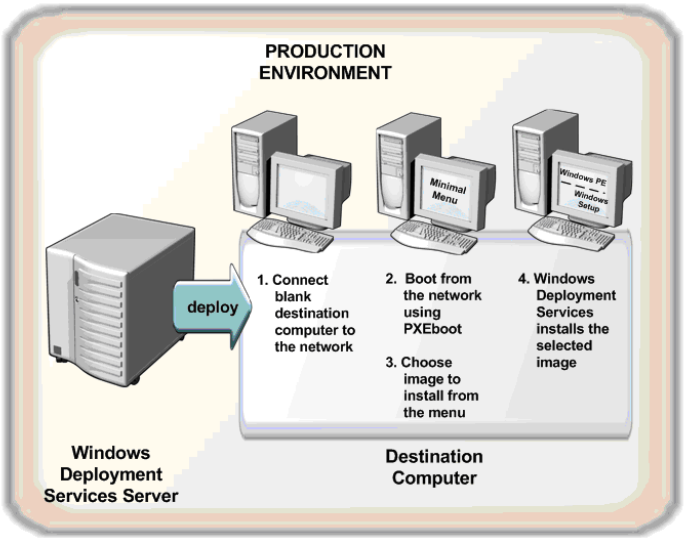
2.3.1.2 Nasazení ze serveru WDS

Tato metodika vytváří a využívá obraz vlastní instalace systému Windows 7 pomocí Windows Deployment Services (WDS). WDS je aktualizovaná verze Služby vzdálené instalace (RIS) a nachází se na systému Windows Server 2008, který má nainstalovaná Windows Directory Services. Tato metoda se používá pro instalaci nových počítačů založené na network-base instalaci [13].

V dnešní době již většina podporuje bootovaní přímo ze sítě stisknutím funkční klávesy při startu. To znamená, že při spuštění počítače není potřeba přítomnost instalačního média. Po připojení k serveru je možno vybrat ze seznamu image k instalaci.

Výhody instalace pomocí WDS:

- Umožňuje network-base instalace operačních systémů Windows 7, což snižuje složitost a náklady ve srovnání s ruční instalací;
- Nasazení obrazu systému Windows 7 do počítačů bez operačních systémů;
- Používá standardní Windows 7 instalační technologie včetně Windows PE, *wim* souboru a Image-base setupu.



Obr. 8. Instalace pomocí WDS [13]

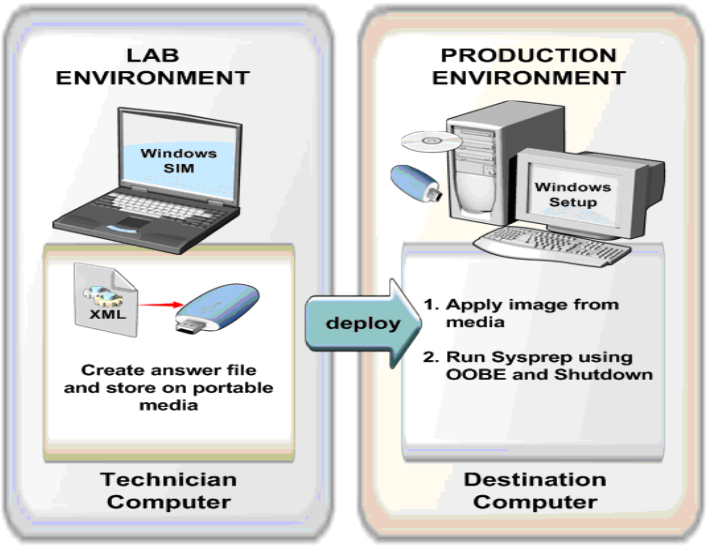
Stejně jako u nasazení ze sítě začíná proces vytváření obrazu vytvořením odpovědního souboru pomocí Windows SIM a uložením konfigurace například na USB flash disk. Následně se vloží vyměnitelné médium, obsahující odpovědní soubor a produkt Windows do referenčního počítače.

Proces nasazení začíná bootováním cílového počítače ze sítě. Windows Deployment Services poskytuje seznam obrazů k instalaci. Výběrem konkrétního image ze seznamu spustí Windows Deployment Services instalaci obrazu na cílovém počítači pomocí Windows PE a instalace systému Windows 7. Proces instalace je schematicky znázorněn na obrázku č. 8.

2.3.1.3 Nasazení z instalačního média

Pro malé podniky, které nepoužívají pro instalaci vlastní nakonfigurované Windows 7 obrazy nebo mají jen málo počítačů, je vhodné použití instalace přímo z instalačního DVD média systému Windows 7. Tento proces nevyžaduje síťovou infrastrukturu.

Tato manuální metoda je ve srovnání s ostatními pomalejší a většinou vyžaduje po instalační konfiguraci počítače. Instalace z DVD média se používá pro vytvoření referenční instalace a je znázorněna na obrázku č. 9.



Obr. 9. Instalace z instalačního média [13]

Proces nasazení začíná vytvořením konfiguračního setu pomocí Windows SIM. Konfigurační sada obsahuje odpovědní soubor a další zdrojové soubory, jako jsou vlastní ovladače a aplikace, potřebné k dokončení instalace.

2.3.2 Vytvoření referenčního obrazu Windows

Jako první krok v nasazení Windows 7 je vytvoření referenčního počítače a následné zachycení jeho konfigurace. Na přípravu systému slouží nástroj Sysprep spouštěný

z příkazové řádky a nástroj Windows SIM, který je součástí Windows AIK a pomáhá s budováním a zachycením počítačového obrazu.

2.3.2.1 Windows System Image Manager

Windows SIM je nástroj používaný pro přizpůsobení a automatizaci instalace Windows 7. Umožňuje vytvářet a spravovat bezobslužné odpovědní soubory systému Windows 7. Tyto odpovědní soubory jsou používány v průběhu instalačních fází Windows 7 pro konfiguraci a úpravy výchozí instalace. Lze například změnit výchozí stránku v Internet Exploreru, upravit nastavení sítě, povolit nebo zakázat bránu firewall systému Windows nebo přerozdělit disk.

Windows SIM se využívá v těchto případech pro:

- Vytvoření nového odpovědního souboru: odpovědní soubory vytvořené v aplikaci SIM jsou spojeny s konkrétním obrazem Windows 7 a používají se pro zobrazení všech komponent, které jsou k dispozici v obrazu Windows a jejich konfiguraci, odpovídající konkrétní instalační fázi;
- Editace existujícího odpovědního souboru: SIM se používá k přidání nových komponent, balíků nebo dalších aktualizací na existující odpovědní soubor;
- Doplnění ovladačů zařízení;
- Přidání dodatečných aplikací a aktualizací;
- Import balíčků ze sdíleného adresáře: SIM importuje balíčky, které nejsou součástí obrazu Windows 7. Tyto balíčky jsou přidány do odpovědního souboru z distribuční složky;
- Vytvoření konfigurační sady: tato sada obsahuje kompletní kolekci souborů, ovladačů, aplikací, záplat a odpovědních souborů, které se používají k přizpůsobení instalace systému Windows 7. Konfigurační sada obsahuje všechny potřebné binární soubory zabalené s přidruženým odpovědním souborem [13].

2.3.2.2 Sysprep

Příprava systému nástrojem Sysprep je používána ve spojení s jinými nástroji pro nasazení systému Windows 7 na nový hardware a slouží hlavně pro zobecnění instalace. Nástroj Sysprep vykonává následující funkce:

- Odstraní unikátní název počítače. V případě, že stejné SID nejsou v některých prostředích problémem, pak název počítače nesmí být shodný;

- Odebere počítač z domény. Tato akce je velice důležitá, při následné instalaci počítače je počítač přidávaný do domény již pod novým názvem;
- Odinstaluje P'n'P (Plug and Play) ovladače, což snižuje riziko nekompatibility. Potřebné ovladače budou nainstalovány v průběhu spuštění následné instalace;
- Může odstranit event logy (parametr reseal), což je užitečné v případě řešení problémů s nově instalovaným systémem, ale také v případě, kdy se připravený systém ocitne mimo organizaci u koncových uživatelů;
- Odstraní jednotlivé body obnovy (Restore Point). Pokud by se použil bod obnovy ze vzorového počítače, mohly by nastat problémy s provedenou obnovou na jiném počítači;
- Odstraňuje účet místního administrátora, zakazuje jej a odstraňuje jeho profil. Tím je zajištěno větší zabezpečení, kdy je účet lokálního administrátora zakázán a nemůže být zneužit;
- Zajišťuje, že počítač bude restartován do tzv. „Audit módu", kde je možné instalovat ovladače a aplikace třetích stran;
- Zajišťuje, že po prvním startu počítače bude spuštěn „mini setup", kde je provedeno specifické nastavení počítače, vygenerován nový SID, nastavení jméno počítače atd.
- Umožňuje vynulovat tzv. „grace period" - časový interval, po který může být počítač použitý bez nutnosti aktivace [33]. Toto vynulování aktivace se nazývá rearm a může být spuštěno pouze třikrát.

Sysprep je umístěný v adresáři *„%WINDIR%\system32\sysprep"* a použití musí odpovídat nainstalované verzi operačního systému - týká se především bitové verze Windows [33].

Po spuštění nástroje Sysprep prochází následujícími kroky:

- Kontroluje, je-li možné sysprep spustit, je-li uživatel administrátorem a zdali je spuštěna pouze jediná Sysprep instance;
- Inicializuje logování;
- Zpracovává zadané parametry příkazové řádky, pokud nejsou zadány žádné parametry, je zobrazeno okno Sysprepu. Načítá informace z odpovědního xml souboru;
- Zpracovává jednotlivé akce, volá odpovídající dll knihovny a spustitelné soubory, zapisuje informace do log souboru;

- Kontroluje, zdali byly zpracovány všechny odpovídající dll knihovny a všechny úkoly popsané v těchto knihovnách, vypíná a restartuje operační systém [33].

2.3.3 Správa Windows PE prostředí

Předinstalační prostředí Windows PE je řešení pro instalaci, diagnostiku, řešení problémů nebo zálohování. Zjednodušený mini operační Systém Windows nahrazuje zastaralou systémovou disketu, ale nemá být brán jako plnohodnotná náhrada operačního systému. Základem je jádro systému Microsoft Windows, ale bez mnoha dodatečných modulů a funkcí [38].

Windows PE jsou navrženy tak, aby ve velkém měřítku usnadňovaly nasazení nového operačního systému tím, že řeší následující úkoly:

- ***Instalace Windows:*** instalace Windows automaticky spouští Windows PE. Grafické nástroje, které shromažďují informace o konfiguraci během instalace, běží v prostředí Windows PE. Kromě toho mohou oddělení IT přizpůsobit a rozšířit prostředí Windows PE, aby plnily své jedinečné potřeby v instalačním procesu. Windows PE také poskytují podporu pro servisní bitové kopie systému Windows.
- ***Odstraňování problémů:*** Windows PE jsou také užitečné pro automatické a manuální odstraňování potíží. Například, pokud systém Windows 7 nedokáže spustit z důvodu poškozeného systémového souboru, může systém Windows PE automaticky spustit prostředí Windows Recovery Environment.
- ***Obnova:*** OEM výrobci mohou použít Windows PE na vytváření vlastních, automatizovaných řešení pro obnovu a rekonstrukci počítačů se systémem Windows.

Vzhledem k tomu, že jsou Windows PE 3.0 založena na jádře Windows 7, překonávají omezení MS-DOS spouštěcí disketu tím, že podporují:

- Souborový systém NTFS 5.x včetně dynamických svazků;
- TCP/IP sítě a sdílení souborů;
- 32-bit (nebo 64-bit) ovladače;
- Podmnožinu Application Programming Interface (API Win32);
- Windows Management Instrumentation (WMI), Microsoft Data Access Component (MDAC), a HTML Application (HTA);
- Start z mnoha typů médií, včetně CD, DVD, USB flash disku a Služby vzdálené instalace (RIS) serveru;

- Offline údržbu obrazů Windows v prostředí Windows PE;
- Windows PE zahrnují všechny Hyper-V ovladače.

2.3.4 Zachycení, aplikování a údržba obrazu Windows

Windows AIK obsahuje nástroje potřebné k vytváření, nasazování a údržbě obrazů Windows 7. Mezi klíčové komponenty Windows AIK patří ImageX a DISM.

2.3.4.1 ImageX

ImageX je nástroj spouštěný z příkazového řádku, sloužící k vytvoření, úpravě a nasazení obrazu Windows 7 v organizaci. Obrazy jsou zachyceny do wim souboru. Mezi klíčové vlastnosti imageX patří:

- Zobrazení obsahu WIM souboru;
- Zachycení obrazu;
- Připojení obrazu pro jeho následnou off-line editaci;
- Uložení více obrazů do jednoho wim souboru;
- Komprimování wim souborů s obrazy.

Nejčastější scénáře nástroje imageX

- Zachycení a použití obrazu ze síťového úložiště pro rychlé nasazení - tento scénář vyžaduje spuštění referenčního počítače do Windows PE, zachycení obrazu pomocí ImageX, uložení obrazu na sdílené síťové úložiště a jeho následné aplikování na cílových počítačích.
- Přizpůsobení existujícího obrazu, včetně aktualizace souborů a složek - tento scénář zahrnuje přidávání, odstraňování, editaci a kopírování souborů z obrazu pomocí Windows Imaging File System Filteru (WIM FS filtr driver) a souborového nástroje, jako je například Windows Explorer [13].

2.3.4.2 DISM

Deployment Image Servicing and Management (DISM) je nástroj pro údržbu bitové kopie systému Windows. Umožňuje správcům IT na připojeném obrazu Windows přidávat nebo odebírat jednotlivé instalační balíčky, aktualizace softwaru a ovladačů. DISM může být použit v režimu offline k údržbě obrazů systému Windows před nasazením nebo přípravě Windows PE obrazu [13].

DISM nahrazuje nástroje Package Manager, PEimg a Intlcfg používané v systému Windows Vista. DISM konsoliduje funkce těchto tří nástrojů, stejně jako přináší nové funkce pro zlepšení zkušeností s offline údržbou. DISM může být použit k údržbě systému Windows Vista s aktualizací Service Pack 1 a Windows Serveru 2008. Při použití se systémem Windows 7 a Windows Server 2008 R2 je jeho funkcionalita rozšířena o:

- Přidání, odebrání prohlížení seznamu instalačních balíčků a ovladačů;
- Povoluje nebo zakazuje funkce Windows;
- Aplikuje změny na základě *„unattend.xml“* odpovědního souboru;
- Konfiguruje mezinárodní nastavení;
- Provádí upgrade obrazu Windows na jinou edici;
- Připravuje Windows PE obraz;
- Udržuje všechny platformy (32-bit, 64-bit i Itanium) [21].

2.4 Nasazení pomocí Windows Deployment Services

Windows Deployment Services (WDS) jsou nástupcem RIS (Remote Installation Services) ze starších verzí serverových Windows. Umožní bootování ze sítě pomocí PXE, čímž se na počítači spustí instalační program Windows. Služba WDS nabídne takto nabootovaným počítačům seznam obrazů, které jsou k dispozici pro nasazení.

Je zde potřeba odlišit možnosti jednotlivých nástrojů. Jinak řečeno, spolu s nasazovaným obrazem lze použít odpovědní soubor pro konfiguraci nasazovaných Windows v jednotlivých fázích, nicméně WDS slouží pouze jako transportní komponenta.

Serverová komponenta Windows Serveru 2008 či Serveru 2008 R2 Windows Deployment Services se instaluje jako jedna z rolí serveru. Poskytuje serverové prostředky pro spuštění klientského počítače (pomocí PXE) s možností aplikace obrazu Windows 7 přes síťové připojení. Je to jedna z klíčových komponent pro usnadnění celého procesu nasazení Windows. Na koncovém počítači je třeba mít síťovou kartu s podporou PXE [16]. Celý proces nasazení může běžet bez účasti nebo jenom s minimální účastí pracovníka IT.

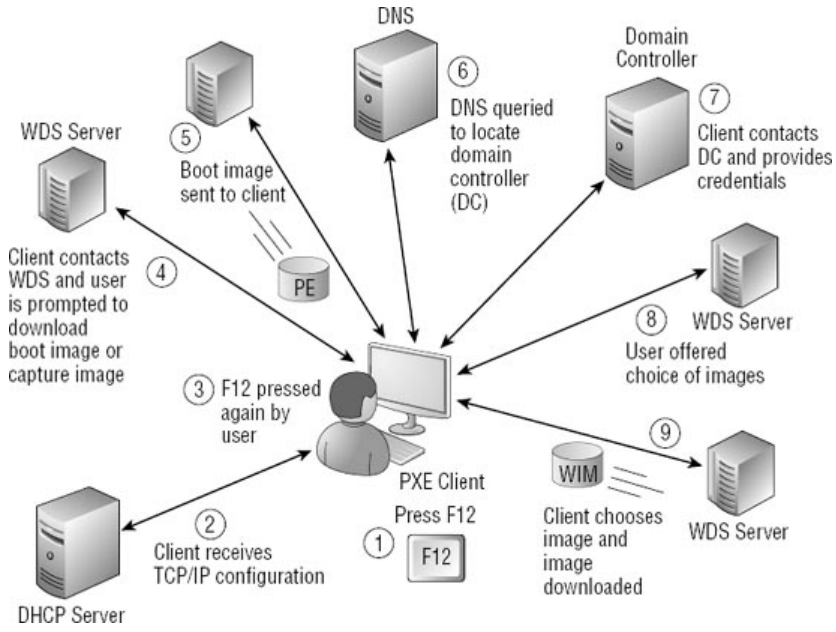
Mezi hlavní předpoklady instalace WDS je:

- WDS server musí být členem domény Active Directory;
- Funkční síťové služby DHCP a DNS;
- Úložiště s obrazy musí být formátováno systémem NTFS;

WDS podporuje různé typy obrazů pro různé typy akcí:

- Instalační – typický obraz Windows. Ať již originální z DVD, nebo upravený;
- Boot – obraz obsahující pouze WindowsPE pro boot počítače a poskytnutí síťové konektivity;
- Capture – obraz obsahující nástroje pro vytvoření referenčního obrazu;
- Discover – slouží pro umožnění funkcionality bootování ze sítě i pro počítače bez podpory PXE [16].

Princip činnosti WDS serveru je znázorněn na obrázku č. 10, z něhož je patrné, že počítač bez operačního systému se pomocí PXE připojí k serveru a stáhne obraz s instalací Windows. Jednotlivé kroky 1 až 9 jsou vysvětleny níže.



Obr. 10. Princip činnosti WDS serveru [8]

- Krok 1: administrátor spustí PXE bootování stiskem klávesy F12;
- Krok 2: klientská počítač získá z DHCP serveru konfiguraci TCP/IP - typicky IP adresu, masku, bránu a IP adresu serveru DNS;
- Krok 3: opět je administrátor vyzván ke stisknutí klávesy F12 pro start síťových služeb. Pokud F12 nebylo stisknuto znovu, bude systém spuštěn normálně. Pokud je ale klávesa F12 stisknuta znovu, bude klient kontaktovat WDS server;

- Krok 4: pokud jsou na serveru WDS dva druhy image – bootovací i zachycený, je administrátor vyzván k výběru konkrétního obrazu. Zde je třeba vybrat image zaváděcí (bootovací);
- Krok 5: boot image je odesílán na klientský počítač a následně je administrátor vyzván k nastavení regionálního prostředí, klávesnice a následně k vložení doménových přihlašovacích údajů ve tvaru doména\uživatelské jméno a heslo;
- Krok 6: DNS server je dotazován k vyhledání řadiče domény. Počítač má IP adresu serveru DNS z dřívějšího pronájmu DHCP;
- Krok 7: Řadič domény obsahuje Active Directory Domain Services, administrátorem vložené uživatelské jméno a heslo je kontrolováno proti řadiči domény;
- Krok 8: Administrátorovi je nabídnuta možnost výběru obrazů založených na oprávnění uživatelského účtu. Obrazy mohou být omezeny na určité uživatele nebo skupiny uživatelů změnou oprávnění. Pokud uživatel nemá oprávnění ke stažení obrazu, obraz se nezobrazí;
- Krok 9: poté, co administrátor vybere obraz, bude stažen a nainstalován na klientském počítači [8].

WDS podporuje nasazení pomocí ruční instalace, Lite-Touch instalace nebo Zero-Touch instalace.

2.5 Nasazení pomocí Lite-Touch instalace

Některé organizace mají proces nasazení nového operačního systému plně automatizovaný, jiné organizace zase počítají s vyšším zapojením pracovníků IT. Organizace, které udržují standardizované prostředí, ale nevlastní infrastrukturu potřebnou pro nasazení pomocí Zero-Touch instalace, využijí pravděpodobně funkce obsažené v Microsoft Deployment Toolkitu (MDT) pro podporu Lite-Touch instalace (LTI).

Microsoft Deployment Toolkit je sada nástrojů, které podstatně zjednodušují migrace operačních systémů a jejich nasazení, nejenom v síťových prostředích. Pomocí MDT je možné jednoduše automatizovat celý proces instalace pomocí uživatelského rozhraní bez nutnosti znalosti specifických nástrojů pro úpravu instalací (např.: DSIM, ImageX a dalších) [29].

Jak již bylo napsáno, LTI vyžaduje minimální interakci administrátora během procesu nasazení. Instalace je obvykle spuštěna ručně a vlastní informace pro instalační proces jsou poskytovány prostřednictvím nakonfigurovaného *ini* odpovědního souboru, nebo se zadávají ručně prostřednictvím průvodce, který se aktivuje při zahájení procesu instalace. Organizace, které implementují LTI, vlastní obvykle standardizované síťové prostředí a musí zde být předpoklady pro automatizované využití nástrojů, obsažených v MDT při nasazování Windows.

LTI podporuje tyto scénáře nasazení: nový počítač, upgrade počítače, obnovení počítače a nahrazení počítače.

Proces nasazení Windows pomocí LTI s využitím MDT se skládá z těchto částí:

- Návrh prostředí pro LTI;
- Implementace LTI infrastruktury;
- Instalace aplikace MDT;
- Vytvoření a naplnění adresáře DeploymentShare;
- Vytvoření a přizpůsobení sekvence úloh (Task Sequence);
- Vytvoření Windows PE a obrazu Windows;
- Distribuce operačního systému na klientské počítače.

Návrh prostředí pro LTI

Již v procesu plánování se navrhuje prostředí pro LTI. V tomto kroku je třeba se ujistit, že existuje infrastruktura podporující LTI nástroje. Proces plánování pomáhá v přípravě na nasazení v produkčním prostředí.

Výsledkem plánovacího procesu je sada projektových dokumentů ulehčujících vytvoření a automatické nasazení operačních systémů a aplikací v produkčním prostředí technologií LTI s využitím nástrojů MDT.

Implementace LTI infrastruktury

Serverové role, které vyžaduje LTI mohou být rozloženy v rámci celého prostředí v závislosti na požadavcích infrastruktury nebo mohou být sloučeny na jednom fyzickém serveru. Jedná se o následující role:

- Build server: zdroj pro distribuční obrazy včetně out-of-box ovladačů, aktualizací nebo jazykových balíčků. Umístění tohoto serveru je potřeba vhodně naplánovat s ohledem na možnosti síťového prostředí.
- Data server: je používán pro ukládání počítačových záloh a uživatelských dat. Datový server může být umístěn přes několik fyzických serverů, nebo může být umístěn na jiné servery, které se používají v procesu nasazení.
- Application installation server: slouží jako úložiště pro hlavní a doplňkové aplikace
- Microsoft Windows Deployment Services server: je základem pro PXE bootování. Server VDS ukládá spouštěcí a instalační obrazy a poskytuje podporu po počítače bez operačního systému. Jedná se o volitelnou roli.
- Database server: tento volitelný server může být použit jako centrální úložiště pro řízení konfigurace procesu nasazení. Databázový server běží na platformě Microsoft SQL Server a může být umístěn na stejném počítači, kde je nainstalován MDT nebo na jakémkoliv jiném SQL serveru v organizaci.

Instalace aplikace MDT

Obvykle se MDT instaluje na build server. Rovněž ale může být nainstalován na technický počítač a nakonfigurován tak, aby byl bodem pro distribuci build server nebo data server. Počítač, na kterém má být MDT nainstalován, musí splňovat tyto softwarové předpoklady:

- Microsoft Management Console (MMC) 3.0;
- Microsoft .NET Framework 2.0 a vyšší;
- Windows PowerShell 2.0;
- Windows Automated Installation Kit (Windows AIK) verze 2.0 as vyšší.

Vytvoření a naplnění adresáře Deployment Share

Adresář Deployment Share je výchozí úložiště pro všechny skripty, operační systémy, aplikace, ovladače a další soubory, které jsou potřeba pro nasazení operačního systému. Adresář obsahuje všechny informace a nastavení, které MDT používá během procesu LTI. Obvykle je umístěn na build serveru a vytváří jej přímo MDT.

Vytvoření a přizpůsobení sekvence úloh (Task Sequence)

Sekvence úloh v MDT obsahuje kroky, které mají být provedeny v daném pořadí během Lite-Touch instalace. Sekvence úloh obsahují stejné úlohy jako sekvence v System Center

Configuration Manageru (SCCM), ale SCCM není pro LTI vyžadován. Task Sequence jsou uloženy v adresáři Deployment Share.

MDT obsahuje šablony úloh (Task Sequence Templates), které se používají k provádění běžných scénářů nasazení. V mnoha případech je totiž možné provést nasazení pomocí šablon bez jakýchkoliv úprav sekvencí úloh. A opačně je možno změnit sekvence úloh vytvořených ze šablon pro splnění požadavků organizace. Tabulka č. 2. zobrazuje dostupné šablony.

Tab. 2. Přednastavené Task Sequence v MDT

Šablona	Popis
Capture Only	Připraví počítač pro sběr dat a následně zachytí jeho obraz
Standard Client Task Sequence	Vytvoření výchozího pořadí úloh pro nasazení kopií operačního systému na klientských počítačích, včetně stolních a přenosných počítačů
Standard Client Replace Task Sequence	Zálohuje celý systém, uživatelské nastavení a vymaže disk
Custom Task Sequence	Vytvoření vlastního pořadí úloh, které ale neinstalují operační systém.
Standard Server Task Sequence	Vytvoření výchozího pořadí úloh pro nasazení systému na serverech včetně konfigurace služeb serveru.
Lite-Touch OEM Task Sequence	Pro výrobce OEM, slouží pro nahrání operačního systému na distribuované počítače. Počítače nejsou doinstalovány, ale připraveny na instalaci.
Post OS Installation Task Sequence	Pomocí tohoto typu sekvence je možné provádět konfigurační změny na již nainstalovaných počítačích.

Sekvence úloh se skládají z kombinovaného sledu kroků za účelem provedení konkrétní automatické akce bez zásahu uživatele. Každý krok sekvence úloh provádí konkrétní úkol, jako je ověření, že cílový počítač je schopen přijímat obraz pro instalaci, ukládání uživatelských dat na bezpečné místo, nasazení obrazu do cílového počítače, obnovení uložených uživatelských dat apod.

Vytvoření Windows PE a obrazu Windows

V případě využití LTI pro nasazení Windows v organizaci je možno se doporučuje vytvořit a spravovat Windows PE boot obrazy a obrazy operačního systému pomocí MDT. Aktualizace adresáře Deployment Share v prostředí MDT aktualizuje všechny konfigurační soubory a vytváří vlastní verzi systému Wndows PE.

Jako obraz samotného Windows je možno použít originální instalační disk DVD nebo obraz zachytit na referenčním počítači a následně jej instalovat v rámci organizace jako standardizované prostředí.

Návrh prostředí pro LTI

Pro nasazení operačního systému na klientském počítači je důležité mít oprávnění správce, který má práva pro spuštění instalačního procesu.

Z výše uvedeného vyplývá, že LTI vyžaduje pouze malý zásah na straně instalovaného počítače (při začátku instalace), jinak je instalace předpřipravena a automatizována, z čehož plyne i jednotnost instalovaných PC. Standardně probíhá instalace ze sítě, ale je možno i z vyrobeného DVD (nebo USB disku). Není potřeba speciální infrastruktury a vystačí se se zdarma poskytovanými nástroji (ale můžeme ji použít i ve spojení s SCCM) [23].

2.6 Nasazení pomocí Zero-Touch instalace

Organizace s moderním IT vybavením mohou těžit z automatizovaných možností Zero Touch Installation (ZTI). Tato robustní technologie se nejlépe uplatní ve velkých organizacích s vyspělou síťovou technologií a zabezpečuje naprosto bezobslužnou instalaci operačních systémů na koncové počítače.

Jakmile se rozhodne, že organizace půjde cestou ZTI, je nutné navrhnout Zero Touch prostředí. Musí se zjistit, zdali organizace splňuje všechny nezbytné předpoklady včetně skladovacích kapacit a znalosti síťového prostředí včetně jeho omezení [13].

Nasazení Windows pomocí ZTI se provádí pomocí System Center Configuration Managera a Microsoft Deployment Toolkitu a skládá se z těchto kroků:

- Návrh prostředí ZTI;
- Implementace ZTI infrastruktury;
- Instalace SCCM a MDT;
- Integrace MDT do SCCM;

- Konfigurace služby PXE;
- Vytvoření a distribuce obrazů a instalačních balíčků;
- Vytvoření a přizpůsobení sekvence úloh;
- Vytvoření kolekcí dle potřeby.

Návrh prostředí ZTI

Návrh ZTI prostředí je procesem plánování který obsahuje:

- Výběr scénáře a metody nasazení;
- Ujištění, že existuje požadovaná infrastruktura;
- Nastavení vhodných procesních pravidel (pouze v případě použití MDT nebo SCCM);
- Určit plán monitoringu;
- Zaškolit pracovníky týmu [13].

Ve většině produkčních prostředí již existují služby potřebné pro nasazení. Přesto je nutné ověřit, že požadovaná infrastruktura existuje a podporuje technologie ZTI ještě před pokračováním procesu nasazení. Navíc je nutné specifikovat roli serveru WDS: plná funkčnost WDS nebo využití pouze jako Transport Server.

Výsledkem plánovacího procesu je sada projektové dokumentace sloužící k vybudování SCCM infrastruktury. Ta poslouží k provádění plně automatizovaného nasazení operačního systému a aplikací v produkčním prostředí [13].

Implementace ZTI infrastruktury

Serverové role, které vyžaduje ZTI, mohou být stejně jako u LTI rozloženy v rámci celého prostředí v závislosti na požadavcích infrastruktury nebo mohou být sloučeny na jednom fyzickém serveru. Jedná se o totožné role jako v procesu LTI.

Instalace SCCM a MDT

SCCM se instaluje jako služba serveru pomocí instalačního průvodce nebo je možno využít bezobslužnou instalaci pomocí skriptů. SCCM může být instalován na jakékoliv serverové roli v závislosti na potřebách infrastruktury. Minimální verze SCCM pro nasazení operačních systémů je verze 20007 SP2.

MDT se instaluje spuštěním souboru *„MicrosoftDeploymentToolkit_platform.msi“* a dále se postupuje dle instalačního průvodce.

Integrace MDT do SCCM

Integrací MDT do SCCM se rozšiřují možnosti SCCM o instalaci operačních systémů. Integrace se provádí spuštěním souboru *„Microsoft.BDD.WizLauncher.exe“* z adresáře, kde je nainstalován MDT.

Konfigurace služby PXE

Servisní bod PXE je rolí SCCM, která reaguje na PXE požadavky z počítačů, které jsou do SCCM importovány. Služba PXE musí být nakonfigurována tak, aby reagovala na PXE bootovací žádosti klientů SCCM za účelem komunikace ze serverem SCCM.

Poskytování služby PXE se konfiguruje jako role WDS serveru, po instalaci WDS nebude WDS na klienty reagovat, protože všechny úkoly budou prováděny v rámci SCCM konzoly.

Vytvoření a distribuce obrazů a instalačních balíčků

Přidání obrazu operačního systému a zaváděcího obrazu se provádí pomocí SCCM konzoly a tyto obrazy jsou pak používány pro nasazení operačního systému na klienta SCCM.

Zaváděcí obrazy nejsou zachyceny z referenčních počítačů, ale jsou přímo upraveny správcem v SCCM nebo získány z externích zdrojů. SCCM obsahuje dva zaváděcí obrazy: jeden pro podporu x86 platformy a jeden na podporu x64 platformy. Doporučuje se použít tyto obrazy, pokud nejsou zapotřebí jiné specifické ovladače v boot image.

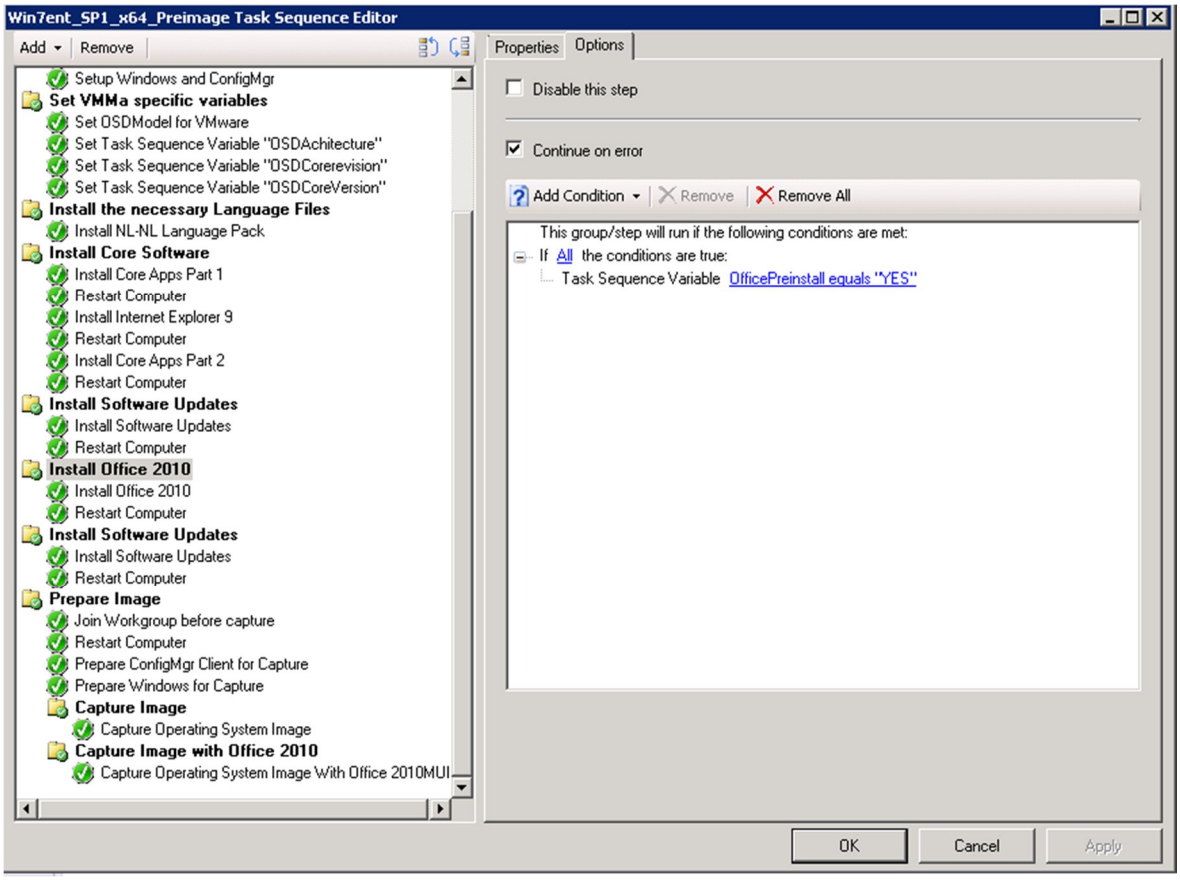
Obrazy operačních systémů jsou distribuovány z distribučních bodů. Nasazují se jako balíček na SCCM klienta, obraz je zkopírován na pevný disk cílového počítače a následně je spuštěn z připraveného prostředí PE.

Vytvoření a přizpůsobení sekvence úloh

Sekvence úloh poskytují mechanismus pro provedení více kroků nebo úkoly na počítači bez nutnosti zásahu uživatele. Sekvence úloh je možno využít pro:

- Vytvoření a zachycení snímku na referenčním počítači;
- Instalaci existujícího obraz na klientských počítačích;
- Provedení vlastních instalačních úloh pomocí proměnných.

Vlastní sekvence úloh mohou být použity k provedení specializovaného nasazení operačního systému nebo k provádění jiných specifických instalací. Na obrázku č. 11 je vidět Task Sequence v prostředí SCCM sloužící pro instalaci Microsoft Office 2010, která bude následovat ihned po instalaci operačního systému na koncovém počítači.



Obr. 11. Task Sequence v prostředí SCCM [7]

Vytvoření kolekcí dle potřeby

Kolekce představují skupiny zdrojů a obsahují nejen počítače, ale rovněž uživatele a uživatelské skupiny. Kolekce poskytují prostředky na uspořádání zdrojů do upravovatelných jednotek, což umožní vytvořit organizovanou strukturu, na kterou se budou přidělovat úlohy k provedení.

2.6.1 Požadavky na prostředí pro ZTI instalaci

Návrh funkčního ZTI prostředí je rozhodující pro úspěšné nasazení Windows. Mezi hlavní požadavky Zero-Touch instalace patří:

Požadavky na sítě a infrastrukturu

Obrazy, které obsahují od 500 megabajtů do několika gigabajtů dat, kladou velké požadavky na infrastrukturu a sítě. Jednotlivé role serveru, které jsou potřebné pro ZTI, musí zohlednit:

- Build server: kolik místa je třeba přidělit pro obrazy operačních systémů;

- Data server: správný odhad požadavku na místo v případě zálohování uživatelských dat a nastavení;
- Application installation server: jak veliké boudou instalační balíky hlavních a doplňkových aplikací;
- WDS server: vysokorychlostní připojení mezi serverem WDS a cílovým počítačem pro stažení Windows PE.

Požadavky na WDS

WDS servery musí být umístněný na stejném subnetu sítě pro zajištění vysokorychlostního připojení jako cílové počítače. Pokud organizace nemůže zajistit dostatečnou kapacitu sítě, je možné provést jednu z následujících akcí:

- Dočasně umístit příslušné servery blíže cílových počítačů (do jejich subnetu);
- Dočasně přesunout cílové počítače do pracovní oblasti, kde může být OS nasazen a po kompletní instalaci je vrátit do jejich původního umístění;
- Provedení ZTI na místě pomocí off-line instalačního média.

Požadavky na migrace uživatelských dat

Pokud se budou migrovat uživatelská data, je vhodné zjistit, kolik úložného prostoru je vyžadováno pro migraci dat. Pokud využíváme scénář nasazení „obnovení“ (refresh), je dobré zvážit migraci hard-link pomocí USMT.

Výpočet kapacity potřebné na zálohu uživatelských dat se stanoví vynásobením počtu dní potřebných pro uchování dat, průměrné velikosti uživatelských dat a počtu uživatelů pro dané migrační období. Např. v případě, že průměrný uživatel má velikost dat 3 GB a tato data musí být uložena po dobu 5 dnů je potřeba pro 100 uživatelů 1.500 GB volného místa na serveru (3 GB × 5 dní × 100 uživatelů za den) [13].

3 MIGRACE PROFILU UŽIVATELE

Migrace profilu uživatele zachytí všechny jeho data a nastavení na stávajícím počítači a poté je obnoví na nově instalovaném (cílovém) počítači. Obvykle se provádí ihned po nasazení nového operačního systému a jejím cílem je umožnit uživatelům jejich okamžitou produktivitu, aniž by ztráceli čas konfigurací uživatelského prostředí či hledáním dat. Migrace se dělí na:

- Migraci uživatelských nastavení: migrace uživatelského profilu, jako je nastavení plochy, vzhled oken, nastavení internetového prohlížeče nebo nastavení e-mailu. Patří sem rovněž migrace lokálních i doménových uživatelských účtů.
- Migraci uživatelských dat: migrace dat, která jsou uložena na lokáních discích. Je potřeba zvážit typy souborů a jejich umístnění, které se do procesu migrace zahrnou.
- Migraci aplikačních nastavení: zahrnuje migraci konfigurace konkrétní aplikací, ale nemigruje aplikaci jako takovou.

3.1 Migrační nástroje

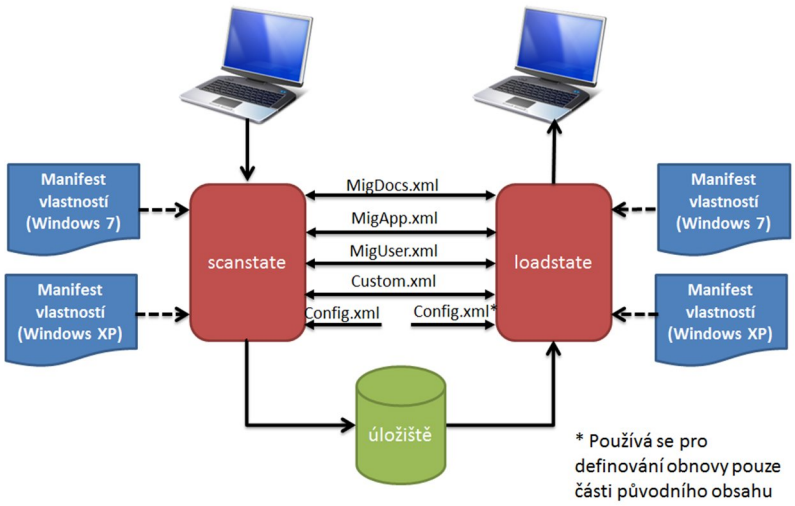
Pro provedení migrace je možno využít následující dva nástroje z produkce Microsoftu:

- Windows Easy Transfer (WET) - slouží k provedení migrace na jednom počítači nebo několika málo počítačích. WET podporuje datové přenosy pomocí Easy Transfer kabelu, přes síť, vyměnitelné médium nebo pomocí sdílené síťové složky. Protože se jedná o aplikaci spíše pro domácí použití, nebude dále zmiňována.
- User State Migration Tool (USMT) - provádí migraci na mnoha počítačích a co nejvíce proces migrace automatizuje.

3.1.1 Proces přenesení uživatelských dat pomocí USMT

USMT se skládá z několika jednotlivých nástrojů. Primárně budou využívány komponenty *„ScanState.exe“*, pomocí které je prováděna záloha uživatelského stavu a následně pak *„LoadState.exe“*, pomocí které je prováděna obnova uživatelského stavu.

USMT je součástí Microsoft Deployment Toolkitu a spolupráce jednotlivých komponent je patrná z obrázku č. 12. Výhodou USMT je dozajista to, že se jedná pouze o nástroj příkazové řádky, neexistuje žádné uživatelské rozhraní.



Obr. 12. Spolupráce jednotlivých komponent v USMT [32]

Modifikace chování nástroje USMT se provádí pomocí XML souborů. Součástí instalace USMT jsou soubory:

- *„MigApp.xml“* - předdefinovaná migrace aplikačního nastavení včetně migrace ze starších verzí Office na Office 2010/2013;
- *„MigDocs.xml“* - využíván coby „Doc finder“ v případech, kdy není možné přesně identifikovat soubory určené pro migraci;
- *„MigUser.xml“* - definice migrace uživatelských souborů a nastavení.

Velkou výhodou USMT je využití tzv. hardlink migrací při scénáři refresh. V takovém případě dochází k vytvoření propojení mezi starým souborem a adresářem určeným pro migraci a následně pak z migračního adresáře do cílového adresáře. Nejedná se o vlastnost USMT, USMT je v tomto případě pouze „konzumentem“ standardní funkcionality souborového systému NTFS. Identického výsledku je možno docílit nástrojem FSUTIL. Výhodou takové migrace je to, že s daty není fyzicky manipulováno (ani přesun) a proto je celá migrace podstatně rychlejší. Využití hardlink migrace je řízeno parametrem *„/hardlink“* [34].

Mezi další přednosti USMT patří:

- Vylepšené možnosti určení velikosti dat pro migraci - před tím, nežli je spuštěna reálná migrace uživatelských dat, je možné spustit USMT. Ten určí, kolik prostoru bude zapotřebí pro uložení dat. Ve verzi 4 USMT určuje prostor, který bude zapotřebí v komprimovaném stavu, tedy výstup je mnohem více relevantní cílovému stavu.

- Možnost uložení stavu uživatele i mimo spuštěný operační systém pomocí S*canState* - jedná se o velice užitečnou vlastnost, kde data mohou být „vytažena“ z operačního systému, který neběží. Tedy například z nastartovaných Windows PE řídících instalaci nového operačního systému. Také je možnost provedení zálohy z původní instalace Windows, která byla setupem přesunuta do adresáře *„Windows.old“*.
- Není zapotřebí přístup na doménový kontrolér při spouštění *ScanState* a *LoadState* - nyní je možná kompletní migrace nedoménových i doménových uživatelských profilů i v případě, že není dostupný řadič domény, což je užitečné v případě offline migrace (viz. předchozí bod).
- Přímá integrace s Microsoft Deployment Toolkitem a System Center Configuration Managerem - nástroj USMT přímo spolupracuje s nástroji pro řízení a správu instalací.
- Nové podpůrné funkce - *ScanState* nyní obsahuje dvě nové podpůrné funkce - *MigXmlHelper.FileProperties*, pomocí které je možné definovat, jaké soubory mají být migrovány na základě uživatelem definovaných vlastností souboru - např. datum vytvoření, datum posledního přístupu, velikost atd. Druhá funkce *MigXmlHelper.GenerateDocPatterns* umožňuje snadné nalezení dokumentů v rámci celého počítače, aniž by bylo nutné vyvářet kompletní migrační xml soubor.
- Využití Volume Shadow Copy - pomocí přepínače *„/vsv“* je možné při spouštění *ScanState* využít Volume Shadow, kdy je provedena záloha souborů, které jsou používány a uzamčeny jiným procesem.
- Migrace lokálních skupin - je možné využít sekci v souboru *„Config.xml“*, pro migraci členství uživatelů v lokálních skupinách. To umožňuje například automatizovanou změnu uživatele ze skupiny lokálních administrátorů do skupiny standardních uživatelů.
- Podpora pro šifrování pomocí AES - délka šifrovacího klíče závisí na podpoře zdrojového operačního systému [32].

Před migrací uživatelských dat a nastavení nebo nastavení aplikací je zapotřebí provést řádné plánování a testování. V tomto případě je doporučeno obrátit se na specialisty, ti jsou schopní identifikovat nastavení aplikací, definovat nastavení uživatelů atd. Při nevhodném použití nástrojů nemusí být přenesena všechna potřebná data a výsledkem může být i nefunkční uživatelský profil [32].

4 NÁVRH A KONFIGURACE ZABEZPEČENÍ UŽIVATELSKÉHO PROSTŘEDÍ

Počítače zapojené v síti jsou prakticky pořád pod neustálým útokem. V minulosti byly vynakládány nemalé náklady na opravu napadených počítačů. Windows 7 a Windows 8 se snaží tyto náklady snížit zavedením nástrojů jako je UAC, AppLocker, Windows Defender, Bitlocker apod. [28]. Na zabezpečení uživatelského prostředí v podnikové síti je vhodné využít i doménové nástroje jako je Group Policy nebo autentizaci pomocí 802.1x.

4.1 Bezpečnostní nástroje na úrovni OS Windows

Operační systém Windows 7 v edici Professional , Enterprise či Ultimate poskytuje robustní a bezpečné nástroje prostřednictvím poskytování řady programů, které pomáhají zvýšit jeho bezpečnost a použitelnost. Je třeba správně pochopit, jak jednotlivé funkce zabezpečení fungují. Teprve potom lze efektivně diagnostikovat a opravit problémy, týkající se vyřešení konkrétního bezpečnostního problému. Následující nástroje jsou zahrnuty do Centra zabezpečení, které je součástí operačního systému.

4.1.1 Windows Defender

Windows Defender je antispywarový software, který je dodáván se systémem Windows. Pokud je program aktivován, spouští se automaticky. Použitím antispywarového softwaru můžete chránit počítač proti spywaru a dalšímu potenciálně nežádoucímu softwaru. Spyware se může bez vědomí uživatele nainstalovat do počítače kdykoli je připojen k Internetu. K infikování počítače může také dojít při instalaci některých programů z disku CD, DVD nebo jiného vyměnitelného média. Spyware může být naprogramován také tak, aby se spustil v neočekávaném čase, nejen ihned po instalaci. Windows Program Defender nabízí dva způsoby ochrany před infikováním počítače spywarem:

Ochrana v reálném čase. Windows Program Defender uživatele varuje, když se spyware pokouší nainstalovat nebo spustit v počítači a upozorní, pokud se programy pokusí změnit důležitá nastavení systému Windows.

Možnosti prohledávání. Program Windows Defender lze použít k vyhledávání spywaru, který by mohl být nainstalován v počítači, k plánování prohledávání v pravidelných intervalech a k automatickému odstraňování softwaru, který je zjištěn v průběhu prohledávání.

Při používání programu Windows Defender je důležité, aby byly definice co nejaktuálnější, proto spolupracuje program Windows Defender se systémem Windows Update a automaticky instaluje nově vydané definice. Program Windows Defender lze také nastavit tak, aby před prohledáváním prověřil online existenci aktualizovaných definicí [20].

4.1.2 Windows 7 AppLocker

Ve Windows 7 je obecně možné určovat, který software lze v počítači spouštět a který nikoliv. Ve všech edicích Windows 7 je možné využít Zásady omezení softwaru. Ty mají za úkol zabránit spouštění nepovolených či nebezpečných programů. Nastavení se provádí v Zásadách skupin, kde lze definovat dvě úrovně – *„Bez omezení“* a *„Nepovoleno“*.

Omezení softwaru umožňuje řídit možnosti spouštění aplikací, určit, kdo smí do počítače přidávat důvěryhodné vydavatele software, povolit uživatelům spouštění pouze vybraných souborů a další. Omezení softwaru v počítači lze provádět na základě algoritmu hash (nezávislý na umístění souboru, ale závislý na verzi souboru), pravidla cesty (závislé na umístění souboru), pravidla certifikátu (identifikace softwaru podepsaného určitým certifikátem), a pravidla zóny (ovlivňují pouze instalační balíčky systému Windows).

Verze Windows 7 Enterprise a Ultimate umožňuje AppLocker omezovat software pro určité uživatele nebo skupiny uživatelů, podporuje automatické vytváření pravidel na základě analýzy adresářů a další.

4.1.3 Windows BitLocker

Šifrování BitLockerem chrání celý oddíl, zatímco EFS pouze vybrané soubory. BitLocker chrání před neoprávněným systémem, zatímco EFS před neoprávněným uživatelem. BitLocker (a v podstatě ani EFS) není pro běžné použití Windows 7 nutný, na disku by musely být velmi cenné informace. Nejčastěji BitLocker chrání proti tomu, když někdo vezme fyzicky disk a připojí ho do jiného počítače, na němž je administrátorem. Potom lze snadno převzít vlastnictví souborů a dostat se tak k jejich obsahu. U BitLockeru se nevybírají soubory, které chceme zašifrovat a kdo k nim bude moci přistupovat. BitLocker pracuje v reálném čase při práci s diskem a chrání systém před offline prolomením a zcizením dat ze systémového oddílu, případně i jiného oddílu. BitLocker není při standardní instalaci v systému dostupný. Nejprve se musí aktivovat v ovládacích panelech.

BitLocker souhrnně potřebuje ověření, autentifikaci, aby otevřel sekci klíčů a jimi dešifroval systémová data. Tato autentifikace nemá souvislost s autentifikací uživatelskou, je to autentifikace systémové služby. Často se použije TPM integrovaný čip, který nástroj BitLocker používá k zašifrování a ochraně klíčů. Autentifikační režimy jsou čtyři a vybrat se musí jeden z nich:

- BitLocker s podporou TPM;
- BitLocker s podporou TPM a PIN;
- BitLocker s podporou TPM a jednotky USB;
- BitLocker bez podpory TPM.

Pokud není v počítači čip TPM (zpravidla na běžných PC, nikoliv noteboocích), je pro provoz BitLockeru jediná možnost – aby se klíče ukládaly přímo v systému. Kdykoli později je možno BitLocker deaktivovat. Důležité ale je dobře uložit heslo pro obnovu, které systém u deaktivace oznámí. Toto bude zapotřebí v případě vložení disku do jiného počítače, například při poruše základní desky v PC. BitLocker nabízí možnost uložit heslo Recovery Password na disk USB, do složky nebo jej vytisknout [3].

BitlockerToGo

V OS Windows 7 je doplňková funkce BitLockerToGo pro přenosné disky, kde běžný BitLocker nelze použít. Tedy nejčastěji pro různé klíčenky. BitLockerToGo umožňuje šifrovat data na vyměnitelných médiích a zabezpečit je heslem nebo digitálním certifikátem uloženým na Smart kartě. Správci a uživatelé tak dostávají možnost, aby bylo toto rizikové místo přenosu informací zabezpečeno šifrováním.

4.1.4 Systém souborů EFS (Encrypting File System)

Systém souborů EFS (Encrypting File System) je funkcí systému Windows 7, kterou je možné použít k uložení informací na pevný disk v šifrovaném formátu. Šifrování je nejsilnějším typem ochrany, který systém Windows nabízí k zabezpečení informací. Některé klíčové vlastnosti systému souborů EFS:

- Šifrování je jednoduché. K zapnutí šifrování stačí zaškrtnout políčko ve vlastnostech souboru nebo složky;
- Kontrolu před tím, kdo může soubory číst;

- Soubory jsou při uzavření zašifrovány, ale po otevření se automaticky opět připraví k použití;
- Při rozhodnutí, že už není potřeba soubor šifrovat, stačí zrušit zaškrtnutí políčka ve vlastnostech souboru [5].

Pokud se v PC data zašifrují, je třeba mít k dispozici nějaký způsob jejich obnovy v případě, že se něco stane se šifrovacím klíčem. Pokud dojde ke ztrátě nebo poškození šifrovacího klíče a není způsob, jak data obnovit, jsou tato data ztracena. Ke ztrátě dat také dojde, pokud se šifrovací klíč uloží na čipovou kartu a tato karta bude poškozena nebo se ztratí. Šifrovací certifikáty a klíče by se měli vždy zálohovat.

4.1.5 User Account Control

Řízení uživatelských účtů (UAC) má za úkol zvýšit bezpečnost celého systému. Princip je jednoduchý - zamezit spouštění takových uživatelských procesů, které by mohly mít za následek ohrožení nebo případnou nestabilitu systému (jedná se např. o instalaci softwaru a ovladačů, manipulaci se soubory v systémových složkách atd.). UAC v definovaných chvílích částečně zatemní obrazovku a zobrazí dialogové okno, v němž čeká na potvrzení od administrátora. Až po schválení akce pokračuje a provede požadovanou operaci.

Systém je to však v základu i přes námitky uživatelů velice dobrý. Přesto se však ozývají vůči tomuto bezpečnostnímu prvku z více stran námitky - sám Microsoft dokonce později přiznal, že je třeba s UAC ještě nadále pracovat a vylepšit jej. V systému Vista totiž nešlo s UAC nijak manipulovat ani měnit úroveň jeho ochrany, šel jen úplně vypnout, což mělo za následek oslabení obranných schopností systému Vista. V operačním systému Windows 7 je tedy možnost alespoň částečně konfigurovat chování Řízení uživatelských účtů [18].

4.1.6 Windows Firewall

Brána Firewall je software nebo hardware, který kontroluje informace přicházející z Internetu nebo ze sítě a v závislosti na svém nastavení je buď zablokuje, nebo jim umožní projít do počítače.

Brána firewall pomáhá zabránit hackerům a škodlivému softwaru (například červům) v získání přístupu k počítači prostřednictvím sítě nebo Internetu. Brána firewall může rovněž zabránit tomu, aby počítač odesílal škodlivý software do jiných počítačů [2]. Popis činnosti Firewallu Windows je velmi obsáhlý a není předmětem této práce.

4.1.7 Centrum akcí

Centrum akcí je centrální místo, ve kterém se zobrazují výstrahy a ze kterého lze provádět akce, pomocí nichž lze zajistit bezproblémový běh systému Windows. Zobrazují se v něm důležité zprávy o nastavených zabezpečení a údržbě, která vyžadují pozornost. Červeně označené položky v Centru akcí mají popisek *Důležité* a označují vážné problémy, které je potřeba co nejdříve vyřešit. Žlutě označené položky jsou navrhované kroky, jejichž provedení je třeba zvážit, například doporučené úlohy údržby.

V Centru akcí lze rychle ověřit, zda jsou nějaké nové zprávy. A to umístěním ukazatele myši na ikonu Centra akcí v oznamovací oblasti zcela vpravo na hlavním panelu. Kliknutím na ikonu jsou vidět podrobnější informace a kliknutím na zprávu lze přejít k řešení problému. Je možno také otevřít Centrum akcí a zobrazit zprávu v plném znění. Jestliže jsou potíže s počítačem, nahlédnutím do Centra akcí se zjistí, zdali v něm není problém uveden. Pokud ne, jsou k dispozici užitečné odkazy na poradce při potížích a další nástroje, pomocí kterých lze potíže odstranit [4].

4.2 Zabezpečení síťového prostředí

S přechodem většiny důležitých vnitropodnikových dat na elektronickou formu může získání přístupu neautorizovanou osobou k počítačové síti znamenat pro firmu potenciální nebezpečí. Z tohoto důvodu je nutné podobnému jednání zamezit. To neznamená zabezpečit fyzický přístup k aktivním prvkům či počítačové kabeláži, ale zejména znemožnit k počítačové síti v libovolném místě připojit donesený notebook, bezdrátový přístupový bod či analyzátor sítě. Řízením přístupu k síti lze v aktivních prvcích přesně vyspecifikovat skupinu zařízení či uživatelů, kteří se mohou přes tento aktivní prvek připojit. Ostatní zařízení/uživatelé potom nebudou do sítě vpuštěni dočasným či trvalým zablokováním fyzického portu, skrz který se pokoušeli neoprávněně do sítě připojit [39].

Není předmětem této práce dopodrobna rozebrat všechny možnosti zabezpečení podnikové sítě, přesto ale budou zmíněny dva nejsilnější doménové nástroje pro zabezpečení uživatelského prostředí a to je aplikování Zásad skupiny (Group Policy) a ověřování pomocí protokolu 802.1x.

4.2.1 Hrozby plynoucí z provozu síťového prostředí

Při implementaci pevných i bezdrátových sítí se musí čelit různým hrozbám, z nich největší problém představuje:

- Nahodilé připojení do bezdrátové sítě – automatické připojení počítače do bezdrátové sítě si lidé v organizaci často ani neuvědomí. To může vést k připojování počítačů do sítě bez odpovídajících bezpečnostních opatření, např. s vypnutým Firewallem apod. Takový počítač je pak samozřejmě snadným cílem útoku.
- Odposlech dat – mezi daty odesílanými z počítače po pevné i bezdrátové síti může jakákoliv neoprávněná osoba, připojená do stejné sítě odposlouchávat například přihlašovací údaje uživatele.
- Modifikace dat – jestliže útočník získá přístup do sítě, může zde vést útok s mužem uprostřed – to znamená, že odposlechne právoplatné pakety na cestě ze zdroje do cíle, upraví je a odešle dále.
- Falešné přístupové body – před verzí Windows XP SP2 se systém ve svém výchozím nastavení automaticky připojoval do jakékoliv detekované bezdrátové sítě. To znamená, že útočník nebo zlomyslný uživatel mohl do sítě snadno napojit svůj vlastní přístupový bod a připojovat se do podnikové sítě.
- Neoprávněné připojení k pevné i bezdrátové síti:
    - V bezdrátové síti může útočník získat přístup k síti i bez nutnosti vstupu do fyzických zařízení firmy. Přenos paketů v bezdrátové síti se zkrátka „nezastaví o zeď“. Dosah vysílání je závislý na síle signálu provozovaného přístupového bodu a na tom, z jakých stavebních materiálů je budova postavena.
    - U většiny firem se v pevné síti nachází množství volných síťových konektorů – v různých zasedacích místnostech, kancelářích apod. Návštěvníci firmy mohou často do sítě zapojit notebook, získat plnohodnotnou IP adresu a přistupovat k síťovým prostředkům [26].

4.2.2 Zásady skupiny

Zásady skupiny (Group Policy) je nástroj pro hromadnou správu oprávnění a nastavení aplikovaných jak na celý počítač, tak na přihlášeného uživatele. V zásadách skupiny je možné vytvářet kolekce nastavení, kterým říkáme Group Policy Object (GPO), které dokáží měnit konkrétní parametry chování počítače nebo uživatele. Samotné nastavení Zásad skupiny se pak "linkuje" na jednotlivé organizační jednotky (OU) v AD, čímž

se zajistí aplikování nastavení jen na vybrané počítače nebo uživatele. Tímto způsobem je možno spravovat potenciálně tisíce počítačů nebo uživatelů změnou jednoho GPO.

Group Policy Management Console je nástroj pro hromadnou správu oprávnění a nastavení aplikovatelných jak na celý počítač, tak na přihlášeného uživatele a používá se pro:

- Aplikování firemních standardů (skrytí ovládacích panelů, síťové tiskárny, spuštění scriptů);
- Aplikování zabezpečení (změna oprávnění na určitých složkách, složitost hesla, skupiny s možností se lokálně přihlásit);
- Hromadné instalace aplikací (Office, Adobe Reader, apod.).

Group Policy Object je seskupení několika nastavení najednou:

- Komponenta globální politiky;
- Dělí se na nastavení pro počítač tak na nastavení pro uživatele;
- Linkují se na organizační jednotky OU v AD;
- Jeden GPO může být linkován hned na několik OU.

Skupinové politiky se dělí na:

- ***Lokální*** - každý počítač od Windows 2000 má lokální politiky (local Group Policy), které ovlivňují lokální počítač a přihlášené uživatele. Pokud počítač není připojen do domény, tak právě lokální politiky jsou jako jediné použity. Lokální politiky jsou uloženy ve skrytém adresáři *„%systemroot%\system32\GroupPolicy“*.
- ***Doménové*** - doménové politiky lze použít výhradně u počítačů a uživatelů, kteří jsou členy nějaké domény.

Group Policy obsahují něco přes 2 500 různých nastavení, které ovlivňují chování jak počítače, tak přihlášeného uživatele. Není bohužel možné použít všechna nastavení na všechny operační systémy najednou (2000, XP, Vista, 7), jelikož s každým novým operačním systémem přichází stovky nových nastavení, které lze použít pouze pro daný systém. Pokud tedy použijeme nastavení určené pro Windows 7 na Windows XP se bude jednoduše ignorovat [6].

4.2.2.1 Aplikování zásad skupiny

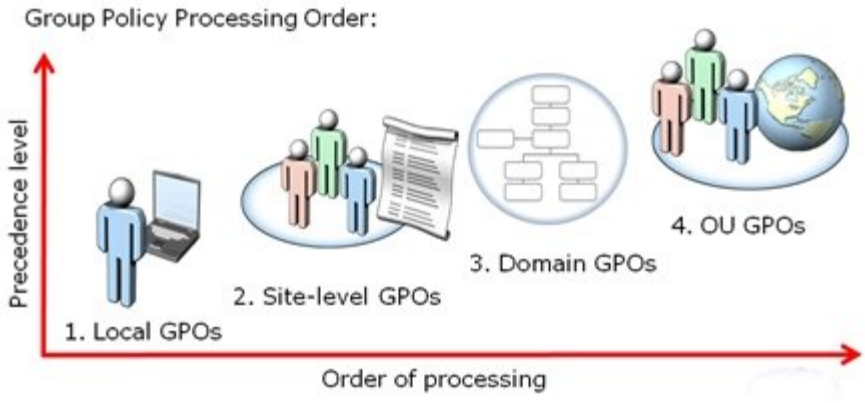
Aplikování Zásad skupiny se provádí na dvou úrovních a to zvlášť pro konfigurace počítače a zvlášť pro konfigurace uživatele. Oboje zajišťuje služba Group Policy Client. Aplikace

se provádí při startu počítače nebo přihlášení uživatele a pak každých 90 minut. Globální politiky dokáží detekovat rychlost linky a v případě pomalé linky (méně než 500 kilobits) a několika dalších faktorů nemusí být některé z politik aplikovány.

Jak již bylo napsáno, politiky dělíme na lokální a doménové. Dále je možno toto rozdělení ještě více specifikovat na:

- Lokální politiky "Local Group Policy";
- Politiky na úrovni sítí "Site Level GPOs";
- Politiky na úrovni domény "Domain level GPOs";
- Politiky na úrovni organizačních jednotek "Organizational Unit GPOs" [6].

Aplikování politik je pak z úrovně 1 na úroveň 4, jak je patrné z obrázku č. 13. Pokud je na úrovni jedna nastaveno např. PROXY Enable a na úrovni 4 je PROXY Disable, „vyhraje“ úroveň 4 a PROXY zůstane v počítači ve stavu Disable.



Obr. 13. Pořadí aplikování zásad skupiny na GPO [13]

Samotné aplikování zásad skupiny je tedy možné ovlivňovat přímo na úrovni každé z politik (GPO). Na každé politice tedy může být aplikováno nastavení dle tabulky č. 3.

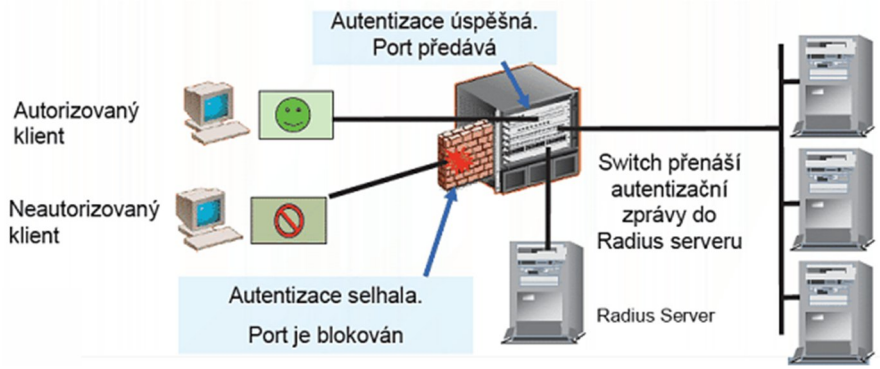
Tab. 3. Ovlivnění zásad skupiny na úrovní GPO [6]

Method	Description
Blocking inheritance	Blokování dědění doménových politik nebo politik z nadřazených OU
Enforcement of GPO links	Vynucení politiky. Využívá se, pokud chcete zajistit, že politika nebude přepsána.
Filtering using security groups	Na Každé GPO je možné nastavit oprávnění, tím můžete definovat, na jaké uživatele či skupiny bude politika aplikována
Filtering using WMI filters	Pomocí WMI filtrů je možné aplikování politik, třeba jen na PC s WIN XP, nebo na počítače s větší RAM od 3GB atd.
Disabling GPOs	Můžete zcela zablokovat použití GPO pro danou síť, doménu nebo organizační jednotku. Můžete také zcela vypnout část GPO Uživatele nebo Počítače, aby výsledná politika měla menší velikost

4.2.3 NetworkLogin 802.1x

Zabezpečení počítačové sítě pomocí funkce NetworkLogin 802.1x umožňuje aktivnímu prvku bezpečně ověřit uživatele na základě uživatelského jména a hesla a teprve po ověření jej připustit ke zdrojům sítě. Aktivním prvkem může být v tomto případě přepínač, přístupový server, bezdrátový přístupový bod (AP). Ověřovací autoritou není aktivní prvek sám, ale centrální databáze uživatelů, se kterou jako její klient komunikuje. Tato databáze se nazývá RADIUS. RADIUS server je možné provozovat jako službu integrovanou v AD. Celý proces ověření probíhá tak, že stanice (v terminologii 802.1x Suplicant) se připojí k portu zabezpečenému 802.1x. Svoji existenci dá přepínači najevo libovolným paketem, například požadavkem o přidělení IP adresy. Přepínač však přijatý DHCP požadavek nepřeposílá dál, ale obratem posílá žádost o identifikaci zpět na stanici. Stanice odpovídá svým uživatelským jménem a heslem. Přepínač přijaté informace zašifruje do paketu a pošle na ověřovací autoritu. RADIUS server provede vyhodnocení přijatých informací a zpět přepínači odešle potvrzení či odmítnutí uživatele. Přepínač na základě této informace vpustí či odmítne stanici přístup do takto zabezpečené sítě [39]. Celý proces autentizace je znázorněn na obrázku č. 14.

Ověření probíhá na základě uživatelského jména nebo hesla, eventuálně digitálního certifikátu. V případě využití ověřování pomocí digitálního certifikátu je vyžadována doménová Certifikační autorita a přítomnost digitálních certifikátů na uživatelských počítačích. Veškeré pracovní módy protokolu 802.1 jsou uvedeny v příloze III.



Obr. 14. Proces autentizace pomocí 802.1x [39]

Protokol 802.1x může zřetelně zvýšit úroveň zabezpečení sítě a zajistit ochranu před neoprávněným přístupem. Síťová zařízení mohou podle výsledku ověření řídit přístup uživatelů nebo stanic do sítě. Ověřováním získá správce lepší přehled o zařízeních a uživatelích připojených v síti. Jeho zavedení ovšem nemusí být snadné a vyžaduje pečlivou analýzu, přípravu, správný návrh a přesné provedení.

4.2.3.1 Typy ověřování v síti 802.1x

Protokol PKI v systému Windows Server zajišťuje nezbytné certifikáty pro autentizaci 802.1x v bezdrátových i pevných sítích. Při autentizaci uživatele nebo počítače podle standardu 802.1x jsou k dispozici dva typy autentizace:

- Ověřování EAP-TLS – metoda ověřování s certifikáty, která při implementaci síťového řešení s autentizací 802.1x zajišťuje vzájemné ověření mezi uživatelem nebo počítačem na jedné straně a serverem RADIUS na druhé straně.
- Ověřování PEAP – u protokolu PEAP musí uživatel zapsat jméno svého uživatelského účtu a heslo, které se odešle na server RADIUS. K prokázání totožnosti musí tedy uživatel uvést své jméno a heslo, které jsou chráněny protokolem MS-CHAPv2 . U serveru RADIUS je k prokázání totožnosti opět nezbytný certifikát s identifikátorem OID typu Server Authentication EKU, ale uživatel již žádný certifikát nepotřebuje [26].

II. PRAKTIC KÁ ČÁST

5 PŘEDSTAVENÍ VŠEOBECNÉ ZDRAVOTNÍ POJIŠŤOVNY ČESKÉ REPUBLIKY

Všeobecná zdravotní pojišťovna České republiky (dále jen VZP ČR) byla zřízena zákonem ČNR č. 551/1991 Sb., o Všeobecné zdravotní pojišťovně České republiky ze dne 6. prosince 1991 s účinností od 1. ledna 1992.

Tab. 4. Základní údaje o Všeobecné zdravotní pojišťovně České Republiky

Obchodní název:	Všeobecná zdravotní pojišťovna České republiky
Sídlo:	Orlická 2020/4 Praha 3 13000 Česká republika
IČ:	41197518
Právní forma:	391 - Zdravotní pojišťovna
Typ subjektu	právnická osoba tuzemská
Datum vzniku:	1. 1. 1992
Předmět činnosti:	provádění veřejného zdravotního pojištění
Logo:	VZP

VZP ČR provádí veřejné zdravotní pojištění, na jehož základě je poskytována pojištěncům zdravotní péče plně nebo částečně hrazená zdravotním pojištěním v rozsahu stanoveném zákonem č. 48/1997 Sb., o veřejném zdravotním pojištění, ve znění pozdějších předpisů. VZP ČR je právnickou osobou, v právních vztazích vystupuje svým jménem. Může nabývat práv a povinností a nese odpovědnost z těchto vztahů vyplývajících.

VZP ČR je s více než 6,5 miliony klientů největší zdravotní pojišťovnou v České republice, má za sebou 15 let své činnosti a dlouhodobě patří k základním pilířům systému zdravotnictví v ČR. Je partnerem renomovaných odborných sdružení a uznávaným členem Asociace mezinárodních neziskových zdravotních a nemocenských pojišťoven (Association Internationale de la Mutualité). VZP ČR je pro své klienty silným, stabilním a seriózním partnerem. Poskytuje kvalitní služby a informace související se zdravotním pojištěním. V rámci platné legislativy dbá na to, aby byla jejím klientům poskytována kvalitní zdravotní péče ve všech odbornostech v rámci rozsáhlé sítě smluvních zdravotnických pracovišť. Orientuje se na efektivitu a hospodaření. VZP ČR bez ohledu na sociální postavení svých

klientů za ně platí zdravotní péči čerpanou na území České republiky a v zemích EU – pomáhá řešit jakoukoli zdravotní situaci. Dbá na to, aby nebyla porušována lidská, pacientská a pojištěnecká práva klientů. VZP ČR je schopna hradit i ty nejnáročnější zdravotnické úkony. Zaměřuje se vedle zdravotní péče na zdravotní programy a další preventivní akce, jejichž cílem je předcházet vzniku závažných onemocnění, klade důraz na prevenci a zdravý životní styl. VZP ČR podporuje zavádění nových diagnostických, vyšetřovacích a léčebných metod a postupů. V pilotních projektech umožnila vyzkoušení a následné zavedení např. screeningového vyšetření okultního krvácení do stolice, mamografického screeningu, operace hemoroidů Longovou metodou, vyšetření C-reaktivního proteinu apod. [10].

5.1 Organizační struktura

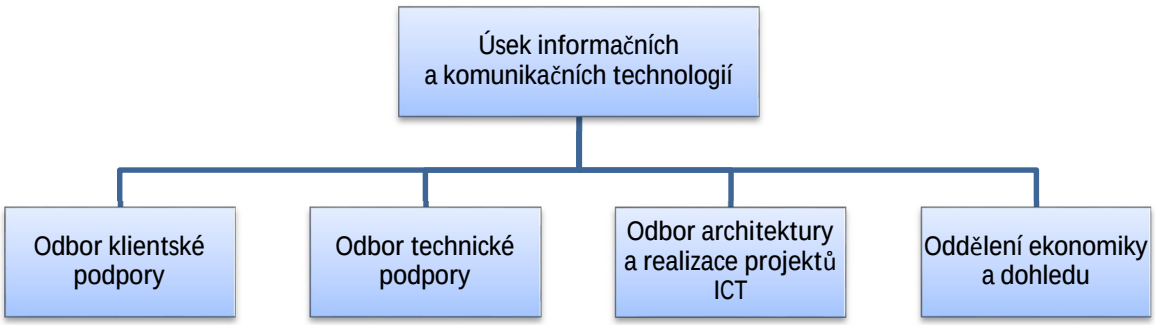
Organizační strukturu Pojišťovny tvoří Ústředí, regionální pobočky a klientská pracoviště. Regionální pobočky a klientská pracoviště jsou organizačními složkami Pojišťovny, které jednají a vykonávají činnost jménem VZP ČR.

V souladu se zákonem č. 551/1991 působí ve VZP ČR následující orgány:

- SPRÁVNÍ A DOZORČÍ RADA;
- ROZHODČÍ ORGÁN;
- VÝBOR PRO AUDIT.

Představenstvo správní a dozorčí rady tvoří předseda, místopředseda a členové, jmenovaní vládou ČR a voleni Poslaneckou sněmovnou Parlamentu ČR.

Na obrázku č. 15 je znázorněno organizační schéma Úseku informačních a komunikačních technologií, kompletní organizační schéma VZP ČR je poté součásti přílohy IV.



Obr. 15. Organizační schéma Úseku informačních a komunikačních technologií

Ústředí VZP ČR se nachází v Praze, regionální pobočky slučují převážně dva sousední kraje a jejich umístnění je následující:

- Regionální pobočka Praha, pobočka pro Hl. m. Prahu a Středočeský kraj;
- Regionální pobočka Plzeň, pobočka pro Jihočeský, Karlovarský a Plzeňský kraj;
- Regionální pobočka Ústí nad Labem, pobočka pro Liberecký a Ústecký kraj;
- Regionální pobočka Hradec Králové, pobočka pro Královéhradecký a Pardubický kraj;
- Regionální pobočka Brno, pobočka pro Jihomoravský kraj a Kraj Vysočina;
- Regionální pobočka Ostrava, pobočka pro Moravskoslezský, Olomoucký a Zlínský kraj.

Klientské pracoviště (KLIPR) VZP ČR se dělí na dvě velikosti. KLIPR I jsou současné regionální pobočky, bývalé krajské pobočky pojišťovny a uzemní pracoviště a KLIPR II jsou úřadovny podřízené bývalým územním pracovištím. Celkové počty regionálních poboček a klientských pracovišť představuje tabulka č. 5.

Tab. 5. Počty klientských pracovišť

KLIPR	Počet
KLIPR I	84
KLIPR II	105

5.2 Úsek informačních a komunikačních technologií (ÚICT)

Úsek informačních a komunikačních technologií zajišťuje podporu procesů a činností, k nimž je VZP ze zákona zmocněna nebo oprávněna. Zodpovídá za nepřetržitý provoz informačního systému a za efektivní investiční politiku v této oblasti, chrání data v informačních systémech proti zneužití.

ÚICT zajišťuje zejména:

- Nepřetržitý provoz informačního systému;
- Podporu uživatelů informačního systému;
- Vytváření strategie a plánování rozvoje informačního systému;
- Řízení a realizaci změn informačního systému;
- Plánování a řízení ekonomiky informačního systému.

Organizační strukturu Úseku informačních a komunikačních technologií tvoří:

- Odbor klientské podpory (OKP);
- Odbor technické podpory (OTP);
- Odbor architektury a realizace projektů ICT (OARP ICT);
- Oddělení ekonomiky a dohledu (OED).

Na procesu migrace na Windows 7 ve VZP se bude primárně podílet Odbor klientské podpory v součinnosti s Odborem technické podpory.

5.2.1 Odbor klientské podpory

Hlavní náplní práce odboru je podpora provozu aplikací a práce uživatelů. Další činností odboru je správa a podpora uživatelů pro koncová zařízení IT a podpora pro elektronickou komunikaci. Organizační strukturu Odboru klientské podpory tvoří:

- Oddělení podpory aplikací příjmových a ekonomických agend (PPEA);
- Oddělení podpory aplikací výdajových a personálních agend (PVPA);
- Oddělení správy a podpory koncových zařízení a elektronické komunikace (PKZ);
- Oddělení Service Desk (SD);
- Oddělení vzdálené podpory uživatelů (VPU);
- Oddělení uživatelské podpory v místě (UPM).

Migraci budou zajišťovat hlavně oddělení PKZ, VPU a UPM, které v současnosti zajišťují:

- **Oddělení PKZ** zabezpečuje v rámci celého životního cyklu provoz koncových zařízení v pojišťovně (počítače, tiskárny, skenery a další periferie) a podílí se výrazným způsobem na jeho nákupu. Dále zajištuje podporu elektronických komunikaci (Portál, B2B, Intranet) a některých lokálně provozovaných aplikací. Vyčlenění pracovníci tohoto oddělení jsou rovněž interními lektory v IT oblasti.
- **Oddělení VPU** zabezpečuje vzdálenou podporu uživatelů a místní podporu v místě sídla oddělení VPU. Toto oddělení je lokalizováno pouze na třech lokalitách v ČR. V případě problému s IT napíše uživatel prostřednictvím aplikace HP ServiceDesk servisní požadavek a Oddělení SD jej dle uvážení předá na jedno z oddělení Odboru klientské podpory v závislosti na charakteru požadavku. Pokud právě oddělení VPU obdrží tento servisní požadavek, pokusí se pomocí vzdáleného připojení problém odstranit. V případě, že se problém nedaří vyřešit vzdáleně, předá servisní požadavek na oddělení UPM.

- **Oddělení UPM** má sídlo na bývalých krajských pobočkách pojišťovny a Ústředí. Řeší veškeré problémy, které nejdou vyřešit vzdáleně. Toto oddělení se na vlastní realizaci migrace bude podílet nejvíce.

5.2.2 Odbor technické podpory

Odbor technické podpory zajišťuje správu serverů, serverových operačních systémů, databází a síťové infrastruktury. Rovněž zajišťuje dohled nad všemi výše uvedenými technologiemi. Organizační strukturu Odboru technické podpory tvoří:

- Oddělení centrálního dohledu (OCD);
- Oddělení správy aplikací (OSA);
- Oddělení správy databází (OSD);
- Oddělení správy unixových systémů (OSUS);
- Oddělení správy Microsoft systémů (OSMS);
- Oddělení správy sítí (OSS);
- Oddělení správy infrastruktury (OSI).

5.3 Uživatelské počítače

Jako jediný operační systém na stolních počítačích i noteboocích je v současnosti používán dnes již zastaralý operační systém Windows XP SP3 s kancelářským balíkem Microsoft Office 2007. Většina aplikací je centralizovaných a pro spuštění využívají Rozcestník aplikací v kombinaci se Single Sign-On[1] systémem. Dále jsou u všech zaměstnanců na počítačích nainstalovány tyto aplikace: JSignPdf na podepisování dokumentů v PDF formátu, Adobe Acrobat 9.0, souborový manažer Total Commander 7.0, klient aplikace DameWare 9.0 pro vzdálenou správu a antivirový systém Microsoft Forefront Endpoint Protection 2010.

[1] Single sign-on systémy (označované jako SSO) se zaměřují na zvýšení zabezpečení přístupů do IT systémů. Běžně si musí uživatel pamatovat mnoho přístupových uživatelských jmen a k nim příslušných hesel. V závislosti na frekvenci používání dochází často k jejich zapomenutí a s tím jsou spojené požadavky na jejich reset, což je časově náročné pro Helpdesk nebo administrátory systémů. Zároveň jsou často uživateli používána jednoduchá a snadno zapamatovatelná hesla, která mohou být snadno zneužita ke kompromitaci systému. Nejhorší možný případ je, když jsou hesla ukládána na jiná snadno zneužitelná místa, než v hlavě uživatele. SSO systémy řeší oba uvedené neduhy spojené s používáním hesel. Využívají silná automaticky generovaná hesla, která automaticky doplňují za uživatele. Ten získává komfort rychlého a bezpečného přihlášení bez nutnosti si pamatovat více hesel. [36].

Jednotlivé odborné útvary mají na počítačích nainstalovány specifické aplikace pro jejich potřebu, například vybraní zaměstnanci právního oddělení mají nainstalován právní systém ASPI, pracovníci ekonomického oddělení bankovní aplikace apod.

5.3.1 Výrobci, modely a počty PC

Celkový počet aktuálně provozovaných počítačů (slovem počítač je dále myšleno stolní počítač nebo notebook u koncového uživatele) je 4456, z čehož je 3852 stolních počítačů a 604 notebooků. Tabulka č. 6 zobrazuje počty PC dle jednotlivých typů a výrobců. Ve VZP ČR platí pravidlo, že jeden uživatel = jeden počítač a není tedy možno až na výjimky, aby měl jeden pracovník více počítačů.

Tab. 6. Počty počítačů dle výrobce a modelu

Výrobce	Model	Počet
Dell	Latitude E6400	178
Dell	OptiPlex 755	1649
Hewlett Packard	HP Compaq 6000 Pro SFF PC	26
Hewlett Packard	HP Compaq 6530b	99
Hewlett Packard	HP Compaq 6710b	30
Hewlett Packard	HP Compaq 6730b	10
Hewlett Packard	HP Compaq 6910p	84
Hewlett Packard	HP Compaq dc5800 Small Form Factor	98
Hewlett Packard	HP Compaq dc7600 Small Form Factor	10
Hewlett Packard	HP Compaq dc7700 Small Form Factor	382
Hewlett Packard	HP Compaq dc7900 Small Form Factor	1651
Hewlett Packard	HP Compaq dx2400 Microtower	12
Hewlett Packard	HP Compaq dx7300 Microtower	12
Hewlett Packard	HP Compaq dx7400 Microtower	12
Hewlett Packard	HP Compaq nx7400	16
Hewlett Packard	HP EliteBook 8440p	20
Hewlett Packard	HP EliteBook 8460p	53
Hewlett Packard	HP EliteBook 8470p	68
Hewlett Packard	HP ProBook 6450b	26
IBM Lenovo	Lenovo ThinkPad R61	20

Všechny počítače splňují minimální konfiguraci pro provoz OS Windows 7 tak,

jak je uvedeno v kapitole 1.3.2. Nejméně výkonný je model Compaq dc7700 Small Form Factor od výrobce Hewlett Packard.

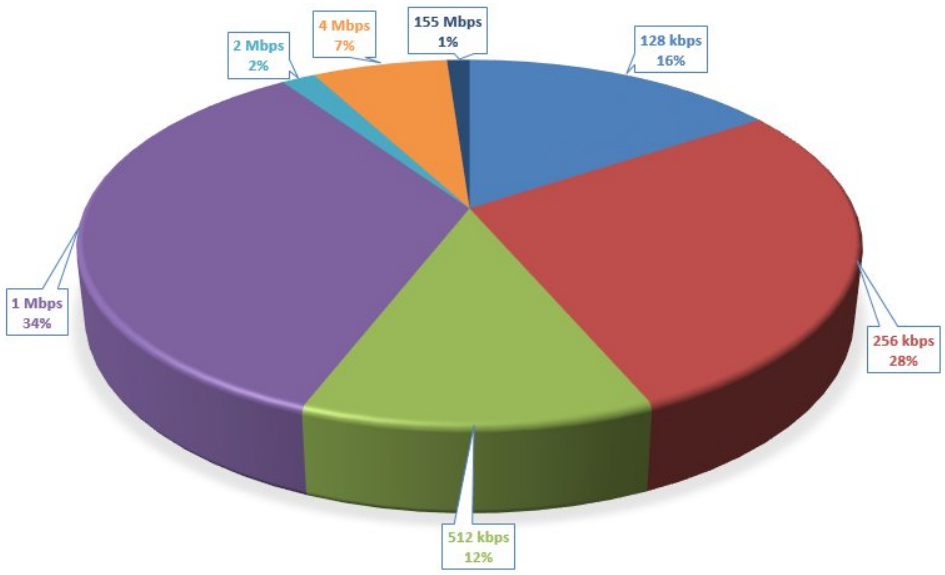
5.4 Síťová infrastruktura

V této kapitole nebude představená veškerá síťová infrastruktura, ale pouze zařízení vyžadovaná pro nasazení operačního systému metodou LTI nebo ZTI.

5.4.1 Aktivní a pasivní prvky sítě

Strukturovaná kabeláž je ve většině případů Cat. 5E, v omezené míře v Cat. 6 nebo Cat. 7. Jako aktivní prvky sítě jsou použity 100 Mbps technologie fy. CISCO.

Rychlost WAN se odvíjí od počtu uživatelů na klientském pracovišti. Z obrázku č. 16 je patrné, že nejvíce klientských pracovišť je připojeno rychlostí 1Mbps, z historického hlediska se jedná o bývalé okresní pojišťovny. Rychlostí 128 kbps, 256 kbps a 512 kbps jsou připojeny klientská pracoviště II, sídlící v menších, nikoliv okresních městech kraje. Rychlost 2 Mbps a 4 Mbps je rezervována pro klientské pracoviště v krajských městech a rovněž pro regionální pobočky. Rychlost 155 Mbps má vyčleněnou Ústředí VZP s datovými centry a regionální pobočka Praha jako záložní připojení k internetu v případě výpadku konektivity Ústředí.



Obr. 16. Průměrná rychlost WAN na klientských pracovištích ve VZP ČR

5.4.2 Servery

Na všech klientských pracovištích sídlících v krajských a okresních městech je umístěn server HP ProLiant DL360 Generation 6 (G6) v následující konfiguraci:

- **Procesor:** 2 x Quad-Core Processor Intel Xeon X5550 v režimu Hyper-Threading;
- **Paměť:** 48GB (12 x 4GB) Unbuffered Memory;
- **Disky:** 6 x 300 GB SAS HDD (RAID5)
- **LAN:** 3x (MGMT, VMs, iLO);
- **OS:** MS Windows Server 2008 R2 SE x64.

Součástí serveru je zálohovací knihovna HP StoreEver LTO-3 Ultrium 920 SCSI obsahující 2 x kabinet po 4 páskách (800 GB), 7 x zálohovací pásku a 1 x pásku čistící.

Na serveru je instalována a konfigurována role Hyper-V umožňující provoz virtuálního Domain Controlleru (vDC) a virtuálního distribučního serveru (vDS).

Konfigurace vDC:

- **Procesor:** 2 x vCPU;
- **Paměť:** 4GB vRAM;
- **Disk:** vHDD 100 GB
- **LAN:** 1x vLAN;
- **OS:** MS Windows Server 2008 R2 SE x64.

Konfigurace vDS:

- **Procesor:** 4 x vCPU;
- **Paměť:** 16GB vRAM;
- **Disk C:** vHDD SYSTEM 100 GB;
- **Disk D:** vHDD SWAP 50 GB;
- **Disk E:** vHDD DEPOT 50 GB;
- **Disk F:** vHDD DATA_UP 250 GB;
- **Disk G:** vHDD DATA_ADM 100 GB;
- **Disk W:** DVD mechanika;
- **LAN:** 1x vLAN;
- **OS:** MS Windows Server 2008 R2 SE x64.

Na vDS je instalována role SCCM 2007 R3 – Secondary Site (distribuční bod), je zde nainstalován HP Data Protector jako zálohovací software. Server dále slouží jako Print Server a File Server.

Klientská pracoviště lokalizovaná v krajských městech disponují dále Network Attached Storage (NAS) HP StorageWorks X1400 G2 4TB SATA.

5.4.2.1 SCCM server

Centrální SCCM Site server je realizován na dedikovaném virtualizovaném serveru na platformě Hyper-V R2 resp. Windows Server 2008 R2 umístěném v datovém centru.

Site databáze je umístěna také na dedikovaném virtualizovaném SQL Server na platformě Windows Server 2008 R2 x64 s Microsoft SQL 2008 R2 na odděleném fyzickém systému.

Na centrálním SCCM serveru je nainstalován operační systém Windows Server 2008 R2 Standard Edition s aktuální verzí produktu System Center Configuration Manager 2007 Service Pack 2 R3.

SCCM je nakonfigurován s jednou Primární/Centrální SCCM Site s těmito rolemi: Distribution Point, Management Point, PXE Service Point, Fallback Status Point, Out of Band Service Point. Na dedikovaném SQL Serveru jsou umístěny následující role: SCCM Site Database a Software Update Point. Protože všechny pracovní stanice a servery jsou umístěny v jediné doméně Active Directory a zároveň nejsou požadavky na různá nastavení klientských agentů, je SCCM hierarchie tvořena jediným SCCM Primary Site Code PR0. Pro zajištění požadavků, motivovaných především optimalizací datového pásma na vzdálené lokality, je na každé vzdálené lokalitě vybavené podporovanou serverovou infrastrukturou umístěna podřízená Secondary Site.

Dále je zřízen dedikovaný server pro poskytování reportů na 32-bit platformě s následujícími SCCM rolemi: Reporting Services Point, Reporting Point.

Pro lokality bez serverových OS (KLIPR II) není využívána role Branch DP především z provozních důvodů. Optimalizace datového pásma na tyto lokality je řešena vyhrazením BITS Enabled Distribučního pointu v ústředí VZP, na kterém je pomocí QoS na úrovni Windows Server 2008 R2 řízeno datové pásmo protokolu SMB (TCP 445, 139). Klienti na těchto lokalitách jsou v rámci BITS konfigurace pomocí Zásad skupiny konfigurováni tak, aby v provozních hodinách nepřetěžovali datové pásmo na vzdálená pracoviště.

6 PŘÍPRAVA NASAZENÍ NOVÉHO OS V PROSTŘEDÍ VZP

Společnost Microsoft již nebude od 8. dubna 2014 vydávat bezpečnostní aktualizace pro Windows XP a Office 2003. V případě, že se v tomto produktu objeví bezpečnostní chyba, která může být zneužita útočníky, Microsoft nebude vydávat bezpečnostní aktualizace, které by tuto chybu opravily a znemožnily její využití. Proto je nejlepší možností přejít na novější verzi operačního systému Windows a sady Microsoft Office. Kromě jistoty zabezpečení počítače i po tomto datu jsou k dispozici navíc nové funkce a možnosti, jak lépe využít počítače. Druhou možností je zakoupení podstatně dražší Custom Support prostřednictvím Premier Supportu pro setrvání na nepodporovaných verzích produktů.

6.1 Volba operačního systému

26. 10. 2012 vydal Microsoft oficiálně novou verzi svých Windows s označením Windows 8. Někomu se může zdát, že jsou tato Windows na trhu již dlouho, ale opak je pravdou. Zdaleka ne všechny softwarové firmy stačily upravit své aplikace pro provoz na Windows 8 a ne všichni výrobci hardware stačili dodat upravené ovladače pro svá zařízení. Toto jsou hlavní důvody, proč VZP v dnešní době bude přecházet z Windows XP na Windows 7 a nikoliv na Windows 8. Hlavní důvody, které vedly vedení ÚICT k rozhodnutí provést migraci na Windows 7, jsou následující:

- Pouze pro 4% (167 PC z celkového počtu 4456 PC) ze všech provozovaných počítačů ve VZP jsou k dispozici ovladače pro Windows 8. Mezi tato zařízení patří HP Compaq 6000 Pro SFF PC, HP EliteBook 8460p, HP EliteBook 8470p a IBM Lenovo ThinkPad R61;
- Použití nového uživatelského rozhraní živých dlaždič neboli METRO by znamenalo přeškolit převážnou většinu uživatelů v ovládání nového systému;
- Doména AD je vybudována na OS Windows Server 2008 R2 SP1, vycházející z jádra Windows 7 a je plně kompatibilní s Windows 7;
- Doporučení systémového implementátora společnosti Hewlett-Packard s.r.o. na základě znalostí prostředí VZP.

Je třeba uvést, že pro 38 PC nejsou k dispozici ovladače ani pro Windows 7. Jedná se o PC HP Compaq dc7600 Small Form Factor, HP Compaq dx7300 Microtower a HP Compaq nx7400. Tyto PC budou v průběhu migrace nahrazeny počítači podporující Windows 7 z vlastních interních zdrojů VZP.

Výzkumná společnost Gartner ve svých analýzách říká, že přepracovaná Windows 8 budou mít nejspíše nějakou dobu potíže s přijetím u koncových zákazníků i v byznysu. Firmy, které stále používající Windows XP by se nyní měly zaměřit na upgrade na Windows 7 a nečekat na to, až Windows 8 dospějí. Pět důvodů, proč podle společnosti Gartner není vhodná doba na přechod k Windows 8: [19]

- Podpora pro Windows XP skončí (8. dubna 2014) předtím, než budou organizace moci plně zapojit systém Windows 8. Tomu bude trvat aspoň rok (po vydání 26. října 2012), než dospěje a získá plné přijetí na trhu a potřebnou aplikační kompatibilitu. Zákazníci si mohou vybrat individuální podporu Microsoftu „XP Custom Support“, tedy rozšíření podpory po dubnu 2014, ale tento plán podpory je drahý a peníze za něj bude lépe utratit za přechod na Windows 7.
- Pokud organizace čeká na aktualizaci příliš dlouho, pak nový software dostupný na trhu nebude možno spouštět na Windows XP.
- Nezávislým dodavatelům softwaru by nějakou dobu trvalo, než budou plně kompatibilní s Windows 7. Stejně dlouho jim bude trvat zajištění kompatibility svých produktů s Windows 8.
- Správa a podpora bezpečnosti ve Windows 8 vyžaduje pro IT skupiny odlišný soubor znalostí; tyto IT skupiny budou tedy potřebovat nějaký čas, než se zdokonalí s prací ve Windows 8.
- Vista efekt. Organizace, které migrovaly na Windows Vista, měly problém. Ve výsledku jich tedy nemigrovalo mnoho a z toho důvodu někteří dodavatelé softwaru zastavili podporu tohoto systému. To samé se může stát Windows 8.

6.2 Vyčlenění hardwarového vybavení

Hardwarové vybavení nutné pro zajištění úspěšného provedení migrace, je patrné z tabulky č. 7. Veškerý HW je ve VZP k dispozici a není třeba jej pořizovat.

Tab. 7. HW vybavení pro přípravu migrace

HW	Účel
P080A99.kz.vzp.cz	Počítač HP Compaq dc7900 s OS Windows 7 vyhrazený pro instalaci nástrojů potřebných pro provedení LTI v prostředí VZP
S01VKMNT.srv.vzp.cz	Virtuální server postavený na technologii Hyper-V pro instalaci monitorovacích nástrojů a DB MS SQL Express 2012 pro rozšíření LTI o tzv. Dynamic Deployment.
SXXV0DS.srv.vzp.cz	Virtuální distribuční servery (vDS) postavené na technologii Hyper-V na klientských pracovištích (KLIPR I) určené jako úložiště instalačních souborů Windows 7 a s tím souvisejících migračních skriptů, aplikací a driverů. Jsou zde dále uloženy migrovaná uživatelská data a LOG soubory.
P080A200.kz.vzp.cz	Testovací počítač Dell Latitude E6400 bez OS
ReferPC	PC HP Compaq dc7900 Small Form Factor sloužící k vytvoření referenčního image
USB Flash Disk	14ks USB Flash disků o velikosti 32GB potřebných pro offline migraci na klientských pracovištích (KLIPR II) bez vDS.

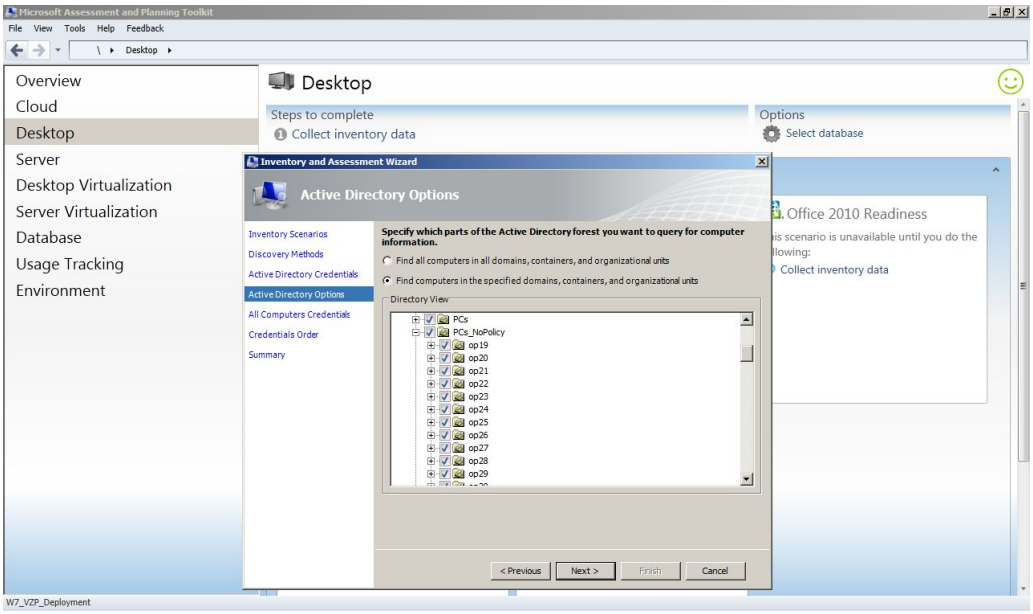
6.3 Analýza současného stavu uživatelských počítačů

Pro analýzu připravenosti počítačů na migraci Windows 7 byl zvolen profesionální nástroj od společnosti Microsoft a to Microsoft Assessment and Planning Toolkit v aktuální verzi 8.0 ze dne 8. 1. 2013. Jak již bylo zmíněno v kapitole 1.2.2, slouží tento reportovací nástroj k analýze připravenosti organizace na migraci operačního systému na vyšší verzi.

MAP 8.0 je nabízen volně ke stažení ze stránek Microsoftu *„http://technet.microsoft.com/en-us/solutionaccelerators/dd537566.aspx“* ve formě instalačního balíčku *„Microsoft_Assessment_and_Planning_Toolkit_Setup.exe“*. Instalace se provede na serveru S01VKMNT, který je určen pro monitoring a inventarizaci. Podmínkou instalace je přítomnost Microsoft .NET Frameworku verze 3.5 SP1, Microsoft .NET Frameworku verze 4.0 Full Profile včetně aktualizace 4.0.2 (KB2544514). Instalace v sobě rovněž zahrnuje instalaci Microsoft SQL Serveru 2012 ve verzi Express s lokální databází.

MAP se spouští pomocí odkazu *„Microsoft Assessment and Planning Toolkit“* z nabídky Start. Hned po spuštění se aplikace dotazuje na zadání názvu nové databáze, sloužící k uložení nasbíraných dat. Databáze se pojmenuje *„W7_VZP_Deployment“*.

Z levého menu se vybere položka *„Desktop“* pro inventarizaci desktopového prostředí, následně se zvolí *„Windows 7 Readiness“* a potvrdí *„Windows computers“*. V dalším kroku je potřeba zvolit metodu discovery *„Use ActiveDirectory Domain Services (AD DS)“* a zadat doménu, uživatelské jméno a heslo, které má oprávnění připojení do AD. Poté je možnost provést inventarizaci ve všech organizačních jednotkách (OU) AD, nebo si vybrat konkrétní OU. Protože se bude provádět migrace uživatelských počítačů, vybereme organizační jednotky *„PCs“* a *„PCs_NoPolicy“*, viz obr. č. 17. V organizační jednotce *„PCs“* jsou umístěny uživatelské počítače dle konkrétní lokality, V OU *„PCs_NoPolicy“* jsou počítače VIP uživatelů a administrátorů.



Obr. 17. Výběr organizační jednotky pro discovery systému

Jako poslední krok je potřeba zadat uživatelská oprávnění umožňující připojení k počítači, nejlépe účet ve skupině Domain Admins a vybrat technologii WMI.

Protože inventarizace 4456 počítačů trvá cca 20 hodin, je důležité zajistit spuštěné počítače u všech uživatelů přes noc, u přenosných počítačů je důležité jejich připojení prostřednictvím VPN v případě, že jej používá zaměstnanec z domova nebo z terénu. Výsledkem inventarizačního procesu jsou dva reporty:

- *„Windows7Proposal-19-03-2013-20h015m05s.docx“*
- *„Windows7Assessment-19-03-2013-20h15m55s.xlsx“*

Report *„Windows7Proposal-19-03-2013-20h15m05s.docx“* shrnuje výsledky hardwarové připravenosti přechodu na Windows 7. Doprovodný dokument *„Windows7Assessment-19-03-2013-20h15m55s.xlsx“* poskytuje podrobné informace o jednotlivých počítačích na síti VZP, což umožňuje provést detailní analýzu stávajícího počítačového hardware. Z tohoto posouzení vyplývá, které počítače, za jakých podmínek a opatření jsou připraveny k upgradu na systém Windows 7 Enterprise.

Z analýzy uživatelských počítačů (tabulka č. 8) ve VZP plyne, že 79% počítačů je ihned připraveno pro migraci na Windows 7, u 20% počítačů je potřeba provést drobné úpravy, dle reportu se jedná v převážné míře o uvolnění místa na disku. U 1% počítačů z nějakého důvodu inventarizace neproběhla, inventarizace těchto počítačů se bude řešit individuálně.

Tab. 8. Připravenost počítačů na migraci Windows 7 [report aplikace MAP]

Relative Readiness for Windows 7	Computer Count	Percentage
Ready for Windows 7	3542	79%
Not Windows 7 Ready	869	20%
Cannot Run Windows 7	0	0%
Insufficient data	45	1%
Total	4456	100%

6.4 Aplikační kompatibilita

Všechny aplikace typu Business Critical jsou ve VZP centralizované a jejich současný běh zajišťuje Oracle JInitiator 1.3.1.22 nebo jsou provozovány ve formě tenkého klienta v okně Internet Exploreru 7. Centralizované aplikace, využívající pro svůj běh Internet Explorer verze 7 jsou funkční i pod Internet Explorerem verze 9.0, který bude v rámci migrace nasazen. Jedná se o nejnovější aplikace, které již při svém vývoji a zavedení do VZP musely Internet Explorer ve verzi 9.0 podporovat. Horší situace je s centralizovanými aplikacemi využívajícími pro svůj běh Oracle JInitiator, protože tento runtime již není od Windows Vista výše podporován a proto je potřeba všechny centralizované aplikace upgradovat na podporu Java Runtime verze 7. Tady se jedná o převážnou většinu centrálních aplikací.

Tento upgrade bude řešen dodavatelsky systémovým implementátorem společností Hewlett-Packard (HP) ve spolupráci s českým zastoupením fy. Oracle. Veškeré podmínky spolupráce bude řešit projekt „Migrace aplikací na podporu Windows 7“. Dle sdělení společnosti HP by neměl celý projekt včetně pilotáže zabrat déle než 5 měsíců od podpisu smlouvy a předání referenčního Windows 7 image, které obě firmy použijí pro ladění a testování aplikací. HP musí rovněž zajistit funkčnost centralizovaných aplikací pod oběma systémy, starými Windows XP i novými Windows 7 během 2 měsíců, což je délka období potřebného na provedení migrace. Časový harmonogram migrace je uveden v kapitole 6.5.2.

Mezi další aplikace provozované na všech uživatelských PC patří pouze Microsoft Office 2007, který bude v rámci migrace migrován na verzi Microsoft Office 2010, JSignPdf, Adobe Acrobat 9.0, souborový manažer Total Commander 7.0, klient aplikace DameWare 9.0 a Microsoft Forefront Endpoint Protection 2010. Veškeré výše zmíněné aplikace Windows 7 podporují.

Všechny další provozované aplikace uvedené v tabulce č. 9 jsou dle garantů[2] plně funkční ve Windows 7. Jedná se o aplikace vyskytující se na počítačích uživatelů v omezené míře a sloužící pro specifické potřeby odborných útvarů.

Tab. 9. Přehled méně používaných aplikací ve VZP

Aplikace	Účel
TRANiS Kilometrovník	Používá Úsek zdravotní péče pro kontrolu vykazování kilometrů zdravotnickými subjekty a pacienty.
ASPI	Právní systém pro pracovníky právního oddělení
Mozilla Firefox, Portable Edition	Tento alternativní prohlížeč využívá Document Management System (DMS) od firmy YOUR SYSTEM, spol. s r.o., který nepodporuje Internet Explorer 7.0.
602XML Filler	Umožňuje vyplňovat elektronické formuláře online i offline, autentifikovat vyplněné údaje za pomoci digitálního podpisu a odesílat formuláře na web či e-mailem.

[2] Každá provozovaná aplikace má ve VZP ČR svého garanta, zpravidla pracovníka ÚICT, který odpovídá za její funkčnost a řeší případné aplikační problémy a aktualizace aplikace. Seznam garantů aplikací je uvedený na intranetových stránkách VZP.

Samozřejmě jsou ve VZP v provozu i další aplikace, které využívají spíše jednotlivci. Jedná se například o aplikaci Hirsch Velocity Security Management System Software, kterou používají převážně pracovníci úseku bezpečnosti, produkty společnosti Adobe (Adobe Photoshop, Adobe Illustrator, Adobe Acrobat), které využívá oddělení Marketingu nebo jde o různý podpůrný software pro mobilní telefony a tablety u VIP uživatelů. Analýza připravenosti těchto produktů na migraci bude řešena pracovníky Oddělení uživatelské podpory v místě individuální formou a v dostatečném předstihu. Zde ale není předpoklad s aplikační nekompatibilitou.

6.5 Volba scénáře a metody nasazení

Od hromadné migrace operačních systémů ve VZP se očekává nejenom nasazení operačního systému Windows 7 na uživatelských počítačích, ale i určitým způsobem „pročištění“ a sjednocení uživatelského prostředí.

Z výše uvedených důvodů je jako migrační scénář zvolen Wipe-and-Load Deployment, který v rámci jedné pracovní stanice nahradí současně provozovaná Windows XP systémem Windows 7 včetně upgrade Microsoft Office 2007 na Microsoft Office 2010.

V rámci migrace bude proveden i redesign AD, kde OU *„PCs“* a *„PCs_NoPolicy“* včetně všech podložek, které představují jednotlivé klientské pracoviště pojišťovny. Nahradí OU *„PCs“* s podsložkami *„L0“*, *„L1“*, *„L2“* a *„L3“* (Level 0 až Level 3) na které se budou aplikovat Zásady skupiny v závislosti na pracovním zařazení zaměstnance.

V rámci scénáře Wipe-and-Load bude navržen univerzální hybridní referenční image společný pro stolní počítače i notebooky, zároveň sloužící i pro instalaci nově dodávaných počítačů do pojišťovny. Může se také využit pro migrační scénář Side-by-Side, kdy bude potřeba nahradit zastaralý počítač novějším.

Jako metoda nasazení bude ve VZP zvolena technologie Lite-Touch High Volume Dynamic Deployment, která ve spojení s databází dokáže dynamicky měnit vlastnosti migračního procesu v závislosti na lokalitě, modelu, výrobce PC, role nebo konkrétního PC. Tato metoda je určena pro organizace do cca 1000 počítačů. Pro organizace s větším počtem počítačů se doporučuje nasazení formou Zero-Touch, High-Volume Deploymentu, která ale pouze rozšiřuje metodu LTI o vzdálené spuštění PC s možností cílení migračního procesu na předem definované kolekce počítačů. Obě metody jinak využívají společných nástrojů

a to MDT 2012 SP1, WDS, WAIK a USMT 4.0. Ani jedna z metod nevyžaduje interakci uživatele nebo správce během migračního procesu.

Hlavním důvodem, proč nebude ve VZP použita metoda ZTI, byť má pojišťovna k dispozici System Center Configuration Manager 2007 SP2 R3, který jako jediný metodu ZTI pro Windows 7 podporuje je rychlost linek WAN. Zde je dle několika zdrojů [14], školení u společnosti AutoCont CZ a.s., doporučená rychlost minimálně 2Mbps pro bezproblémový OS Deployment. Celých 90 % lokalit ve VZP však toto doporučení nesplňuje a proto tedy ani na zbývajících 10 % lokalit nebude uvažováno o metodě ZTI.

Dalším důvodem, proč nebude migrace provedena metodou ZTI je fakt, že není možno provést migraci celé pobočky najednou z důvodu nutnosti zachování provozu. V SCCM je samozřejmě možné vytvořit kolekci jednotlivých počítačů na lokalitě a deployment spustit pouze na tuto kolekci. V tomto případě se ale nevyužije hlavní výhoda ZTI a to hromadné vzdálené spuštění všech počítačů na lokalitě a následné nasazení Windows 7.

SCCM bude využit pro hromadnou instalaci aplikací po dokončení migrace a pro aktualizaci antivirového systému. Rovněž splní účely, pro které si VZP tento robustní nástroj pořídila.

Mezi hlavní důvody použití Lite-Touch High Volume Dynamic Deploymentu ve VZP patří:

- Nezávislost na rychlosti WAN prostředí;
- Nemožnost migrovat všechny počítače na lokalitě hromadně;
- Dynamicky ovlivňovat migrační procesu u „problémových PC“
- Návrh migračního procesu a vlastní provedení migrace spadá do gesce jednoho odboru (OKP);

6.5.1 Migrační plán

Nasazení operačního systému Windows 7 v pojišťovně bude realizovat Odbor klientské podpory, konkrétně Oddělení správy a podpory koncových zařízení a elektronické komunikace, Oddělení vzdálené podpory uživatelů a Oddělení uživatelské podpory v místě. Částečné se na tomto procesu budou dále podílet Oddělení podpory aplikací výdajových a personálních agend a Oddělení podpory aplikací příjmových a ekonomických agend. Poslední dvě oddělení se na procesu migrace podílí pouze ve smyslu otestování upgradovaných centralizovaných aplikací na podporu Windows 7, které tato oddělení spravují.

6.5.1.1 Příprava migrace

Celou přípravnou fázi migrace zrealizuje oddělení PKZ a jedná se hlavně o:

- Instalace a konfigurace MDT 2012 SP1 se všemi potřebnými aplikacemi na počítač P080A99.kz.vzp.cz , který bude sloužit pro přípravu realizace všech migračních částí;
- Instalace a konfigurace DB MS SQL Express 2012 na serveru S01VKMNT .srv.vzp.cz pro potřebu Dynamic Deployment a MDT 2012 SP1, který na tomto serveru zabezpečí vzdálený monitoring migrace;
- Konfigurace migračního procesu;
- Vytvoření adresáře *„DeploymenShare“* na všech vDS s potřebným oprávněním;
- Vytvoření referenčního image;
- Testování migračního procesu;
- Vytvoření off-line distribučního média a jeho uložení na bootovací USB disk;
- Distribuce USB disku na lokality pracovníkům oddělení VPU a UPM

6.5.1.2 Provedení migrace

Vlastní provedení migrace realizují oddělení VPU a UPM za podpory oddělení PKZ následujícím způsobem:

- Provedení kopie obsahu USB disku do předem připraveného adresáře *„DeploymenShare“*;
- Domluva s uživatelem na termínu migrace a oznámení konkrétního data na oddělení PKZ za účelem provedení zálohy počítače;
- Spuštění migračního skriptu a monitorování migračního procesu;
- Kontrola úspěšnosti provedení migrace, případně řešení nečekaných problémů;
- Instalace a konfigurace specifických aplikací, které image neobsahuje a které nejsou instalovány dodatečně prostřednictvím SCCM. Jedná se m málo využívané aplikace odborných útvarů.

6.5.2 Časový harmonogram migrace

Tato kapitola se nezabývá konkrétními daty zahájení a ukončení migrace ve VZP, ale vychází ze dne D, kterým je den předání upravených centralizovaných aplikací ve formě upgrade do VZP.

- Den D: předání referenčního image společnosti HP;
- Den D + 150: nejzazší termín, do kterého musí společnost HP dodat upgrade pro centralizované aplikace;
- Den D + 180: dokončení přípravy migračního procesu oddělením PKZ;
- Den D + 240: dokončení migrace na Windows 7 na 90% zařízení;
- Den D + 270: úplné dokončení migrace na Windows 7 ve VZP.

Z výše uvedeného je patrné, že VZP ČR potřebuje minimálně 270 dní na provedení migrace na všech počítačích. Nejdelší časový úsek potřebuje společnost HP na úpravu aplikací. Do toho harmonogramu není zahrnuta prvotní příprava referenčního image pro společnost HP ještě přede dnem D.

Jak již bylo řečeno, vlastní spuštění migračního procesu na počítačích uživatelů provedou oddělení VPU a UPM. Tato oddělení mají vždy po dvou pracovnících v sídlech bývalých krajských pojišťoven a na Ústředí. V sídlech bývalých okresních pojišťoven nejsou žádní pracovníci těchto oddělení a migraci zajistí pracovníci z nebližší krajské pobočky, tak jako všechny servisní požadavky na IT.

Na migraci se tedy bude podílet celkem 23 pracovníků obou oddělení, kteří musí během dvou měsíců, potřebných na provedení migrace u 90 % počítačů zajišťovat i běžný provoz IT technologií. Z toho vyplývá, že každý pracovník každý pracovní den spustí migrační skript alespoň na 5 PC.

7 REALIZACE MIGRACE

Provedení migrace se skládá z přípravné fáze a realizační fáze, které jsou publikovány v kapitole 6.5.1. IT prostředí ve VZP je dosti specifické a proto správné pochopení konfigurace migračních nástrojů je nezbytné pro správné provedení migrace na Windows 7.

7.1 Referenční image

Referenční image obsahuje vše potřebné, tedy ovladače, nastavení a aplikace, které budou distribuovány společně s operačním systémem. V zásadě lze zvolit několik způsobů, jak referenční image připravit - ruční příprava, příprava pomocí Microsoft Deployment Toolkitu či použití System Center Configuration Manager. Budou zapotřebí dva druhy referenčního image:

- Image pro hromadnou migraci na Windows 7 ve VZP;
- Image pro potřeby společnosti HP na testování a ladění centralizovaných aplikací.

Oba obrazy jsou shodné ve smyslu verze a konfigurace operačního sytému, ovladačů a aplikací. Verze pro HP navíc obsahuje lokální kopii GPO, které v referenčním image pro potřeby VZP nebudou aplikovány – tyto politiky bude nastavovat doména AD.

7.1.1 Referenční instalace Windows 7

Na vyčleněný referenční počítač HP Compaq dc7900 SFF se nainstaluje operační systém Microsoft Windows 7 32-bit verze z instalačního souboru *„SW_DVD5_SA_Win _Ent_7w_SP1_32BIT_Czech_MLF_X17-27681.ISO“*. Obsah souboru se vypálí na DVD médium nástrojem na vypalování bitových kopií, který je součástí Windows 7. Po vložení DVD média do referenčního počítače je spuštěn s požadavkem na bootování z CD\DVD mechaniky, vyvolaného klávesou F9.

Po spuštění instalačního procesu zvolíme české regionální nastavení, konfiguraci disku pro instalaci OS necháme beze změn, tj. bez vytvoření dalších logických jednotek. Výchozí uživatelské jméno je zvoleno *„VzpRef“* bez hesla. Počítač není zařazen do domény a zůstává v pracovní skupině. Ovladače zařízení se neinstalují, byly by stejně nástrojem Sysprep odstraněny.

Jakmile je systém nainstalován, provede se konfigurace uživatelského prostředí pro potřeby VZP následujícím způsobem:

- *Ovládací panely\Vzhled a přizpůsobení\Individuální nastavení\Zvuky\Zvukové schéma* výběr *„Bez zvuku“*
- *Ovládací panely\Vzhled a přizpůsobení\Individuální nastavení\Spořič obrazovky* výběr *„Žádný“*
- *Ovládací panely\Vzhled a přizpůsobení\Individuální nastavení\Změnit ikony plochy* zvolit Ikony na ploše *„Počítač“* a *„Koš“*
- *Ovládací panely\Systém a zabezpečení\Systém\Upřesnit nastavení systému\Upřesnit\ Možnosti výkonu* vybrat *„Optimalozovat pro výkon“*
- *Ovládací panely\Vzhled a přizpůsobení\Individuální nastavení\Pozadí plochy\Plné barvy\další barvy* výběr barvy *„R:0 G:118 B:163“*
- *Ovládací panely\Vzhled a přizpůsobení\Individuální nastavení* uložení motivu jako *„vzp_theme“*

Soubor *vzp_theme.theme* se přesune z adresáře *„C:\Users\VzpRef\AppData\Local\ Microsoft\Windows\Themes“* do adresáře *„C:\Windows\System32“* kam se na něj bude odkazovat nastavení Zásad skupiny v prostředí AD stejně jako další přizpůsobení a zabezpečení pracovního prostředí, které není v referenčním image řešeno. Do adresáře *„C:\Windows\System32“* se umístí spořič obrazovky *„vzp_scr.scr“*, který je využíván i ve Windows XP.

Následně se připraví budoucí adresářová struktura, což obnáší vytvoření následujících složek s oprávněním dle tabulky č. 10.

Tab. 10. Oprávnění na složky Appl, Data a TMP

Adresář	Oprávnění pro skupinu Administrators	Oprávnění pro skupinu Users
C:\Appl	Úplné řízení	*„Číst a spouštět“* a *„Zobrazovat obsah složky“*
C:\DATA	Úplné řízení	Úplné řízení mimo volby *„měnit oprávnění“* a *„přebírat vlastnictví“;*
C:\TMP	Úplné řízení	Úplné řízení mimo volby *„měnit oprávnění“* a *„přebírat vlastnictví“;*

Oprávnění na adresáře *„Windows“*, *„Program Files“* a *„Data“* je ponecháno beze změn.

7.1.2 Instalace aplikací a aktualizace systému

Po instalaci a konfiguraci Windows 7 se doinstalují aplikace, které budou součástí hybridního image. Mezi tyto aplikací patří pouze Microsoft Office 2010 Professional Plus 32-bit, klient SCCM 4.0 a klient antivirového systému Forefront Endpoint Protection 2010.

Instalace Microsoft Office 2010 Professional Plus se provádí z instalačního adresáře umístěného na vDS, tato instalace je již přizpůsobena potřebám VZP, tj. akceptace EULA, výběr kompletní instalace všech komponent, umístnění serveru KMS pro aktivaci apod.

Klient SCCM verze 4.00.6487.2000 se instaluje z instalačního adresáře umístněného na centrálním vDS. Parametr pro zahájení instalačního procesu je *„CCMSETUP.EXE SMSSITECODE=PR0 FSP=S00CMPR0.SRV.VZP.CZ“*. Parametry *„SMSSITECODE“* a *„FSP“* zajišťují jeho správnou konfiguraci.

Antivirový klient Forefront Endpoint Protection 2010 (FEP) se také instaluje z instalačního adresáře umístněného na centrálním vDS. Konfiguraci klienta provedl dodavatel tak, aby vyhovovala potřebám VZP. Instalace je spuštěna příkazem *„FEPInstall.exe /s /q /policy „VZP – FEP Policy““*. Soubor s politikami zajišťuje správné nastavení klienta FEP pro aktualizace definic nebo možnosti změny konfigurace na uživatelském PC.

Ostatní aplikace, používané na všech uživatelských PC již na rozdíl od image Windows XP v image Windos 7 nebudou, jejich instalace je zabezpečena poinstalačními Task sekvencemi v MDT nebo budou nasazeny pomocí Zásad skupiny tak, aby se dala dynamicky změnit verze aplikace.

Po instalaci výše zmíněných aplikací následuje velmi důležitý krok a to kompletní aktualizace formou Windows Update. Po provedení kontroly aplikací nabízí služba Windows Update k 28. 3. 2013 celkem 104 důležitých aktualizací v celkovém objemu 188 MB, mezi kterými je i Internet Explorer 9.0. Z volitelných aktualizací se vyberou všechny aktualizace týkající se Windows 7, aktualizace Windows 7 Language Packs instalovány nebudou.

Aktualizace Windows 7 je záměrně naplánována až po instalaci aplikace Microsoft Office 2010 Professional Plus proto, aby zahrnula aktualizaci i této aplikace.

7.1.3 Sysprep referenční instalace

V kapitole 2.3.2.2 bylo zmíněno, že nástroj Sysprep zobecní instalaci Windows 7 pro potřeby jejího zachycení a následnému deploymentu. Sysprep se spouží z adresáře *„C:\Windows*

System32\sysprep“ souborem *„sysprep.exe“*. Obsluha nástroje je jednoduchá, v dialogovém okně se zvolí *„Zobrazit prostředí při prvním zapnutí počítače“* a vybere volba *„Zobecnit“*. Aby se počítač po provedení Sysprep vypnul, zvolí se ještě možnost *„Vypnout“*. Sysprep ,lze provést také z příkazového řádku pomočí příkazu *„sysprep.exe /generalize /shutdown“*.

- *„/generalize“* - připravuje operační systém pro imaging. Zadáním tohoto parametru budou z operačního systému odebrány všechny specifické informace (SID, system restore point, eventlog,…). Při dalším spuštění instalace operačního systému bude vytvořený nový SID ve fázi specialize, kde resetuje počitadlo aktivací;
- *„/shutdown“* - po ukončení nástroje sysprep vypíná počítač a tím je počítač připravený pro zachycení image.

Pro potřeby zachycení (capture) systému je nutné spustit počítač do prostředí Windows PE a pomocí ImageX zachytit aktuální stav systému.

7.1.4 Vytvoření Windows PE bootovacího USB Flash disku

Windows PE jsou součástí instalace Microsoft Windows AIK 3.0, který je volně ke stažení ze stránek Microsoftu na adrese *„http://download.microsoft.com/download/D/6/B/D6BC8A4A-B59B-431E-8EF7-8FCE2BA72384/KB3AIK_CS.iso“* ve formě ISO souboru o velikosti 1,2 GB. Instalace se provede na počítači P080A99, na který se bude následně instalovat i MDT 2012. Následující sekvence příkazů popisuje vytvoření bootovacího ISO souboru s Windows PE z umístnění *„C:\Program Files\Windows AIK\Tools\PETools“*:

- *„copype.cmd x86 c:\WinPE“;*
- *„copy winpe.wim c:\WinPE\iso\sources\boot.wim“;*
- *„copy c:\Program Files\Windows AIK\Tools\x86\imagex.exe c:\WinPE\ISO“;*
- *„copy C:\Program Files\Windows AIK\Tools\x86\oscdimg.exe c:\WinPE\ISO“;*
- *„oscdimg -n -bc:\WinPE\etfsboot.com c:\WinPE\ISO c:\WinPE\winpex86.iso“*.

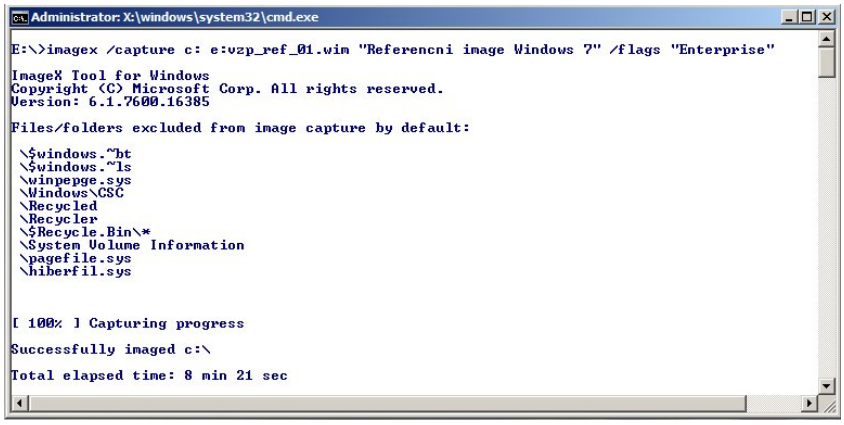
Oscdimg je nástroj příkazového řádku pro vytváření obrazového souboru, parametr *„n“* zapíná podporu long name a parametr *„b“* určuje místo pro El Torito[3] boot sector file.

[3] El Torito je specifikace napsaná firmami Phoenix Technologies a IBM pro bootovací CD-ROM. El Torito specifikace umožňuje vytvoření CD-ROM jako obraz pevného disku nebo disketové jednotky.

Výsledný soubor se extrahuje pomocí volně šiřitelného nástroje Rufus 1.3.2 na prázdný USB disk o velikosti alespoň 8GB, na kterém následně proběhne i capture systému. Nástroj Rufus umí z bootovacího ISO souboru vytvořit bootovací USB Flash disk velmi jednoduchým způsobem.

7.1.5 Capture referenční instalace

Jakmile je dokončen chod sysprepu, počítač se vypne a je nutné provést boot do Windows PE z předem připraveného USB Flash disku, ve kterých se provede capture - zachycení instalačního obrazu do *.wim souboru. Sejmutí instalačního obrazu se provádí pomocí nástroje ImageX a parametru *„/capture“*. Povinné parametry jsou zdrojová cesta k nainstalovanému operačnímu systému, název image souboru, cesta, kam má být image uložen a popis instalace. Protože bude instalační image použit nástrojem MDT 2012, je nutné přidat ještě parametr *„/flags“*. Ten bude v uvozovkách definovat edici, o kterou se jedná. Výsledný příkaz vypadá následovně: *„IMAGEX /CAPTURE C: E:vzp_ref_01.wim “Referencni image Windows 7“ /flags “Enterprise”“*, kde parametr *„C“* specifikuje disk, ze kterého se bude snímek pořizovat. Jak je vidět z obrázku č. 18, tak ImageX přeskakuje některé nepotřebné soubory a adresáře jako například soubor *„pagefile.sys“* nebo adresář *„Recycled“*.



Obr. 18. Proces zachycení referenčního image

7.2 Příprava migračních nástrojů pro Lite-Touch High Volume Dynamic Deployment

Kromě sady Windows Automated Installation Kit 3.0 se LTI instalace neobejde bez klíčového nástroje, kterým je Microsoft Deployment Toolkit (MDT) 2012 Update 1,

nástroje Windows User State Migration Tool (USMT) a pro potřeby dynamického nastavení migračního procesu ještě nástroje Microsoft SQL Server 2012 Express.

7.2.1 Microsoft SQL Server 2012 Express

Databáze MDT je v podstatě databázová verze souboru *„CustomSettings.ini“* v prostředí Microsoft SQL Serveru, kterou lze použít jako centrální úložiště pro ukládání nastavení konfigurace a slouží k migraci více počítačů pomocí MDT. Bez MDT databáze se jinak musí vytvořit samostatný soubor *„Customsettings.ini“* pro každý počítač, který je potřeba instalovat pomocí MDT. S MDT databází se používá pouze jeden *„Customsettings.ini“* soubor pro všechny počítače, plus databáze SQL, která obsahuje úpravy specifické pro každý počítač. Detailnímu popisu souboru *„CustomSettings.ini“* se věnuje kapitola 7.2.2.1.

SQL Server Express je bezplatná edice systému SQL Server, dostupná volně ke stažení ze stránek *„http://www.microsoft.com/betaexperience/pd/SQLEXPCTAV2/enus/default.aspx“*. Protože na serveru S01VKMNT vyhrazeném pro instalaci SQL Serveru běží Windows Server 2008 R2 SE x64, zvolí se i SQL server verze 64-bit.

Spuštěním souboru *„SQLEXPRWT_x64_ENU.exe“* se otevře SQL Server Installation Center a potvrzením volby *„New SQL Server stand-alone installation or add Features to an existing installation“*. Je zahájena instalace. Následuje odsouhlasení a stažení aktualizace KB2793634. Po restartu serveru instalační proces pokračuje výběrem instalačních balíčků, je potvrzen výchozí výběr a název databázové instance je *„SQLS01VKMNT“*. Posledním krokem následuje konfigurace serveru a konfigurace databázového engine:

- SQL Server Database Engine: Account Name: *„S01VKMNT \Administrators“*; Startup Type *„Automatic“*;
- SQL Server Browser: Startup Type *„Automatic“;*
- Database Engine Configuration: *„Windows authentication mode“*.

Konfigurace síťového prostředí SQL serveru je spuštěna příkazem *„SQLServerManager11.msc“* nebo prostřednictvím nabídky Start odkazem SQL Server Configuration Manager. Ve stromové struktuře složky *„SQL Server Network Configuration“* se nachází submenu *„Protocols for SQLEXPRESS“* ve kterém se musí povolit Named Pipes *„Named Pipes - Enable“*. Toto povolení je nutné, aby se MDT i klientské počítače dokázaly připojit k SQL MDT databázi.

V kořenové nabídce *„SQL Server Services“* na položce *„SQL Server Browser“* se v menu *„Vlastnosti“* na kartě *„Service“* v položce *„Start Mode“* potvrdí volba *„Automatic“*. Na závěr se provede restart služby *„SQL Server (SQLEXPRESS)“* z kořenové složky *„SQL Server Services“*.

Konfigurace Windows Firewallu obnáší přidání výjimky pro příchozí i odchozí spojení profilu *„Domain“* u souboru *„sqlbrowser.exe“*, který se nachází v adresáři *„C:\Program Files\Microsoft SQL Server\90\Shared\“* a souboru *„sqlservr.exe“* z umístění *„C:\Program Files\Microsoft SQL Server\MSSQL11.SQLEXPRESS\MSSQL\Binn“*.

7.2.2 Microsoft Deployment Toolkit 2012

Na počítači P080A99 se nainstaluje produkt Microsoft Deployment Toolkit 2012 (dále pouze MDT), který je volně ke stažení ze stránek Microsoft na adrese *„http://technet.microsoft.com/en-us/solutionaccelerators/dd407791.aspx"*. Po instalaci je důležité provést kompletní aktualizaci potřebných komponent, případně jejich instalaci. Z menu *„Components“* v nabídce *„Information Center“* se zvolí *„Check for Updates“* a potvrdí aktualizace či instalace následujících komponent:

- Microsoft Core XML Services (MSXML) 6.0;
- Windows Automated Instalation Kit (x86) 6.1.7600.16385 (tato komponenta je již instalována pro přípravu Windows PE);
- User State Migration Tool (USMT) 3.0.

Zásadním krokem v konfiguraci MDT je vytvoření adresáře *„DeploymentShare“* z menu *„Deployment Shares“*, ve kterém jsou všechna zdrojová data pro potřeby nasazení. Pravým tlačítkem myši se potvrdí volba *„New Deployment Share“* a na dotazy průvodce je potvrzeno následující nastavení:

- Deployment share path: *„C:\DeploymentShare“*
- Share name: *„DeploymentShare“*
- Deployment share description: *„MDT Deployment Share“*
- Options: potvrdit volbu *„Ask if a computer backup should be performed“*

Po vytvoření adresáře *„DeploymentShare“* je v MDT zpřístupněno submenu *„MDT Deployment Share“*, obsahující dílčí menu podle logických celků, se kterými se bude pracovat a to: *„Applications“*, *„Operating Systems“*, *„Out-of-Box Drivers“*, *„Packages“*, *„Task Sequences“*, *„Advanced Configuration“* a *„Monitoring“*.

MDT se rovněž nainstaluje na server S01VKMNT bez aktualizace a instalace dodatečných komponent. Na serveru bude spuštěna monitorovací služba *„Microsoft.BDD. MonitorService“*, která se aktivuje automaticky se spuštěním MDT.

Před vlastním importem referenčního operačního systému, ovladačů, aplikací či úpravou task sekvencí je nutno MDT správným způsobem nakonfigurovat.

7.2.2.1 Obecná konfigurace MDT DeploymentShare

Správná konfigurace MDT DeploymentShare je zásadní pro správný průběh migračního procesu. Konfigurace se provádí z menu *„Akce“*, poté *„Vlastnosti“*, kde v následujícím dialogovém okně jsou patrné čtyři záložky: *„General“*, *„Rules“*, *„Windows PE“* a *„Monitoring“*.

General

Záložka slouží pro obecné nastavení MDT DeploymentShare. Zde zůstávají všechny hodnoty výchozí, pouze v části *„Platforms Supported“* se zvolí nabídka *„x86“*, *„x64“*, zůstane neaktivní, protože s touto platformou se v současné době ve VZP nepočítá.

Rules

V této záložce je zobrazen obsah souboru *„CustomSettings.ini“*. Ten slouží pro definici úkolů, které se mají dít před spuštěním sekvence úloh a instalací operačního systému, a také to, co se má stát po úplném ukončení migračního procesu. Zjednodušeně by se dalo říci, že tento soubor automatizuje průvodce, pomocí kterého se připravuje počítač před instalací. Protože se využije databáze MDT, bude v souboru *„CustomSettings.ini“* uvedena pouze cesta k monitorovacímu serveru a parametry spojení s MDT databází na SQL serveru. Výchozí obsah souboru je nyní následující:

```
[Settings]
Priority=Default

[Default]
OSInstall=Y
SkipCapture=YES
SkipAdminPassword=YES
SkipProductKey=YES
SkipComputerBackup=NO
SkipBitLocker=YES
```

Parametry, které jsou zapsány v *„CustomSettings.ini“*, modifikují chování MDT jak při spuštění z boot media, tak i přímým spuštěním z běžícího operačního systému skriptem *„BDD_Autorun.wsf“*. Soubor se mění dynamicky po provedení *„Update Deployment Share“* nebo je možné změnu provést ručně v souboru *„C:\DeploymentShare\Control\ CustomSettings.ini“*. Veškeré konfigurační parametry jsou včetně ukázkových příkladů ke stažení ze stránek MDT Download Center page na adrese *„http://www.microsoft.com/en-us/download/details.aspx?displaylang=en&=tm&id=25175“* pod odkazem *„Optional - MDT 2012 Print-Ready Documentation.zip“*.

Na této záložce se nachází i tlačítko *„Edit Bootstrap.ini“*. To je soubor, který definuje, co se má dít, nežli se MDT připojí na distribuční sdílení. Tento ini soubor je umístěný v souboru *„boot.wim“* a je spouštěný v případě, kdy instalace startuje z WDS, CD, USB. Pokud je proces spuštěný z běžícího systému, pak se tento soubor nepoužívá. Pokud se tento soubor aktualizuje, je nutné znovu vygenerovat boot soubory pomocí *“Update Deployment Share”*.

Výchozí obsah souboru obsahuje pouze cestu k adresáři MDT Deployment Share:

[Settings]
Priority=Default

[Default]
DeployRoot=\\P080A99\DeploymentShare

Obsah tohoto souboru je potřeba změnit zásadním způsobem, protože ve VZP bude distribuční sdílení na všech vDS serverech a zároveň bude použitý adresář DeploymentShare univerzální. Proto je potřebné do souboru *„Bootstrap.ini“* doplnit informace o umístnění adresáře *„DeploymentShare“* na vDS v příslušné lokalitě tak, aby byla využitá pro distribuci lokální síť a nikoli WAN. Například pokud administrátor spustí migraci na pobočce Uherské Hradiště, tak je důležité, aby se data potřebná pro migraci stahovala z vDS serveru umístěného v Uherském Hradišti. Toto zabezpečí konfigurační položka *„DefaulGateway“*, která podle příslušné Gateway přiřadí správnou cestu k *„DeployRoot“* adresáři na vDS serveru. Dále je v souboru uvedeno přihlašovací jméno, heslo a doména sloužící k připojení na distribuční sdílení, položka *„SkipBDDWelcome“*, která odstraní dialogové okno o začátku migračního procesu z důvodu co největší míry automatizace migrace a položka *„KeyboardLocale“* pro nastavení českého prostředí

ve Windows PE. Vzor takto upraveného souboru pro pobočky ve Zlínském kraji (Uherské Hradiště, Kroměříž, Zlín a Vsetín) je následující:

[Settings]
Priority=Default, DefaultGateway

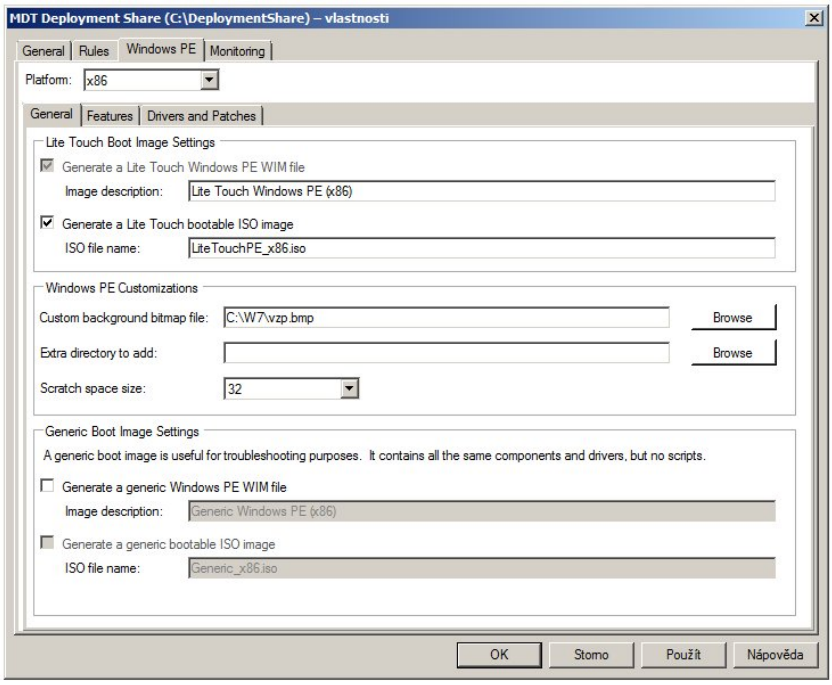
[Default]
SkipBDDWelcome=NO
KeyboardLocale=cs-CZ
*UserID=********
*UserPassword=********
UserDomain=vzp

[DefaultGateway]
10.75.22.252=s75v0vds
10.76.22.252=s76v0vds
10.77.22.252=s77v0vds
10.78.22.252=s78v0vds

[s75v0vds]
DeployRoot=\\s75v0vds.srv.vzp.cz\DeploymentShare
[s76v0vds]
DeployRoot=\\s76v0vds.srv.vzp.cz\DeploymentShare
[s77v0vds]
DeployRoot=\\s77v0vds.srv.vzp.cz\DeploymentShare
[s78v0vds]
DeployRoot=\\s78v0vds.srv.vzp.cz\DeploymentShare

Windows PE

Tato záložka konfiguruje vlastnosti zaváděcího prostředí Windows PE pro každou z platforem: x86 nebo x64, jak je zobrazeno na obrázku č. 19.



Obr. 19. Konfigurace Windows PE v MDT

V platformě x86 definuje oblast *„Lite Touch Boot Image Settings“* název pro *wim* soubor s prostředím Windows PE nebo určuje, zdali se má zároveň generovat *iso* soubor například pro jednoduché vytvoření bootovacího USB disku.

Dále je zde možnost využití vlastního pozadí instalačního procesu, kde se zvolil předem vytvořený obrázek v rozlišení 800 x 600px pod názvem *„vzp.bmp“*. Protože není třeba přidávat do Windows PE žádné další soubory či adresáře a není třeba generovat obecný obraz Windows PE, zůstanou možnosti *„Extra direktory to add“* a *„Generic Boot Image Settings“* bez výběru.

Součástí záložky Windows PE jsou mimo záložku *„General“* ještě další dvě záložky: *„Features“* a *„Drivers and Patches“*.

Záložka *„Features“* slouží k instalaci doplňkových *cab* balíčků do Windows PE. V případě migrace ve VZP se zde vybere balíček *„Microsoft Diagnostics and Recovery Tool 7 (DaRT 7)“*. Ve výchozí instalaci MDT není ovšem balíček k dispozici a musí se do MDT integrovat, tak jak je popsáno v kapitole 7.2.2.2.

Na záložce *„Drivers and Patches“* se vybírá, které ovladače hardware se mají Windows PE obsahovat. Vybere volba *„Include all network drivers“* a *„Include all mass storage drivers“*, protože není třeba z důvodu velkého množství typů PC zvětšovat objem zaváděcího *„boot.wim“* souboru o ovladače, které nejsou v prostředí Windows PE zapotřebí.

Je důležité, aby Windows PE obsahovaly ovladače síťových karet pro spojení s vDS a ovladače mass storage pro správnou funkci pevného disku, DVD nebo USB disků.

Monitoring

Poslední záložka monitoring určuje cestu k počítači, na kterém běží monitorovací služba *„Microsoft.BDD.MonitorService“* pro monitoring migračního procesu. Jako výchozí nastavení je počítač nebo server, na kterém je MDT nainstalován. Protože ve VZP je na monitoring vyhrazený server S01VKMNT s nainstalovaným a spuštěným MDT, bude nastavení této záložky následující:

Monitoring host:	*S01VKMNT.srv.vzp.cz*
Event port:	*9800*
Data port:	*9801*

V soboru *CustomSettings.ini* je pak odkaz na monitorovací server uveden následovně:

EventService=http://s01vkmnt.srv.vzp.cz:9800

7.2.2.2 Integrace DaRT 7.0

Microsoft Diagnostics and Recovery Tool 7 (DaRT 7.0) je sadou nástrojů na snadnou obnovu nefunkčních počítačů, rychlou diagnostiku, určení příčiny problému a následnou opravu nefungujícího počítače. DaRT 7.0 rovněž umožňuje vzdálenou diagnostiku a obnovu, což znamená, že IT administrátor nemusí fyzicky navštívit uživatele s nefungujícím PC. DaRT 7.0 je součástí Microsoft Desktop Optimization Pack (MDOP) 2011 R2, který je ke stažení na webu Volume Licensing Service Center společnosti Microsoft.

Integrací DaRT 7.0 do Windows PE začne služba *„Microsoft Deployment Toolkit Monitor Service*“ nainstalovaná na serveru S01VKMNT, přijímat události ze sledovaných počítačů, jak daleko jsou v procesu instalace. Zároveň umožní administrátorovi připojit se a vzdáleně ovládat pomocí Remote Connection migrační proces v prostředí Windows PE na aktuálně instalovaném počítači. V následujících bodech je popsán postup povolení podpory DaRT 7.0 v MDT 2012.

- Na počítači P080A99 se z instalačního souboru *„MSDaRT70x86.msi“* nainstaluje DaRT 7.0 jako volitelná instalace zahrnující komponenty: *„Crash Analyzer“*, *„DaRT Recovery Image“* a *„DaRT Remote Connection Viewer“* do adresáře *„C:\Program Files\Microsoft DaRT 7“;*

- Z adresáře *„C:\Program Files\Microsoft DaRT 7\v7“* se zkopíruje soubor *„tools.cab“* do adresáře *„C:\DeploymentShare\Tools\x86“;*
- Povolení komponenty *„Microsoft Diagnostics and Recovery Tool 7 (DaRT 7.0)“* v MDT ve vlastnostech *„MDT DeploymentShare“* na kartě *„Windows PE“* platformy *„x86“* a podzáložce *„Features“*.

7.2.2.3 Import operačního systému

Import operačního systému určeného k migraci se provádí v MDT z menu *„Operating Systems“*, které je umístěno v *„MDT DeploymentShare“*. Jako zdrojový soubor se použije snímek operačního systému z referenční stanice ReferPC, pojmenovaný jako *„vzp_ref_01.wim“*.

Import se provádí z kontextového menu volbou *„Import Operating System“* s následujícími předvolbami:

- OS type: *Custom image file*
- Image: *„vzp_ref_01.wim“*
- Setup: *Setup and Sysprep files are not needed*
- Destination: *VZP_REFERENCNI_IMAGE*

7.2.2.4 Import ovladačů

Pro správnou funkčnost hardware migrovaných počítačů je potřeba zajistit správné ovladače k jednotlivým typům PC. Tento krok obnáší větší množství práce, protože ve VZP je dle tabulky č. 6 celkem 20 různých modelů počítačů od výrobců Dell, Hewlett Packard a Lenovo.

Protože jsou pouze 2 modely počítačů od fy. Dell a 1 model od fy. Lenovo, stáhnou se ovladače ručně z internetových stránek výrobce. U modelů počítačů fy. Hewlett Packard se využije nástroj *„HP SoftPaq Download Manager“* pro automatické stahování.

Ovladače HW výrobce Dell

Jedná se o notebook Latitude E6400 a stolní PC OptiPlex 755 a Dell nabízí možnost stažení ovladačů z jediného místa, kde jsou ovladače umístěny v *cab* souborech. S těmi je velice jednoduchá práce, protože se jedná se o archiv, který je možné rozbalit přímo v operačním systému nebo nejlépe v MDT, ten *cab* archívy nativně podporuje. Tyto balíčky jsou k dispozici zde: *„http://en.community.dell.com/techcenter/enterprise-client/*

w/wiki/2065.dell-driver-cab-files-for-enterprise-client-os-deployment.aspx“ a po stažení se umístí do adresáře *„C:\W7\Drivers\Dell“*.

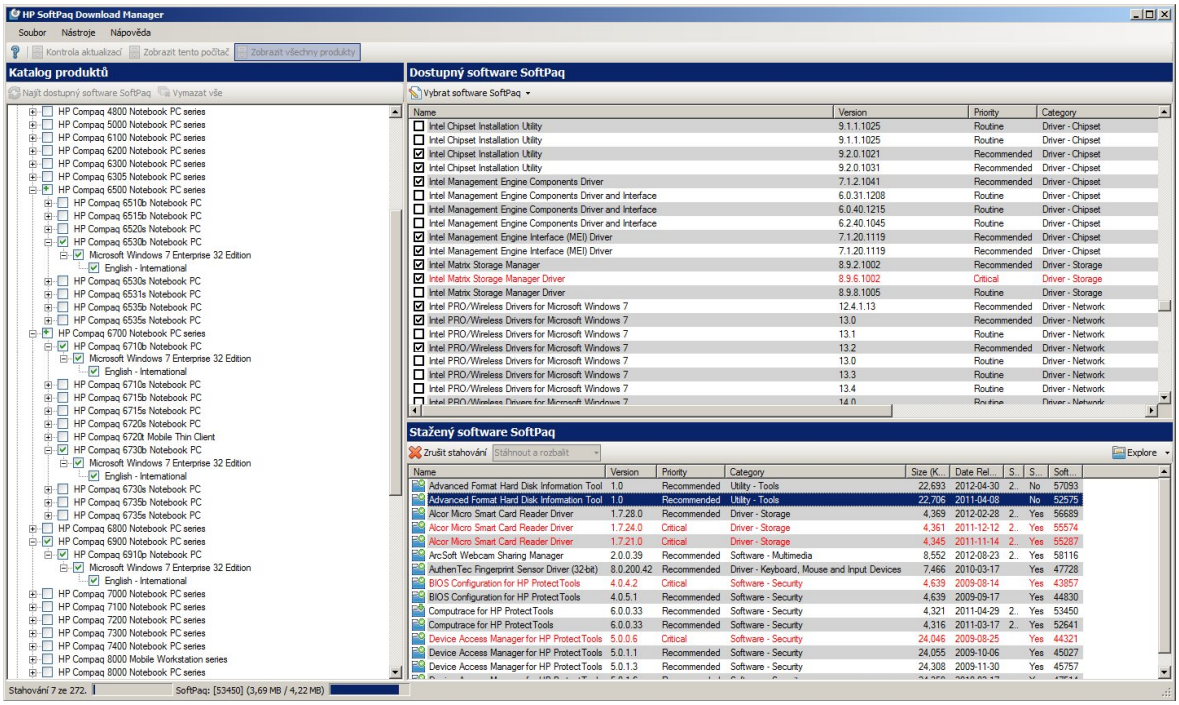
Ovladače HW výrobce Lenovo

Tady se jedná pouze o notebook ThinkPad R61 a příslušné ovladače jsou k dispozici ke stažení ze stránek Lenovo ve formě instalačních balíčku na adrese: *„http://support.lenovo.com/en_US/research/hints-or-ips/detail.page?&DocID=HT037648“*. Po stažení se musí instalační balíček spustit. Po odsouhlasení licenčních podmínek proběhne jejich rozbalení do složky *„C:\DRIVERS\“*. Následuje jejich přesun do adresáře *„C:\W7\Drivers\Lenovo“*.

Ovladače HW výrobce Hewlett Packard

Protože jednotlivých modelů od výrobce HP je ve VZP skutečně mnoho, použije se ke stažení ovladačů k těmto účelům ideální nástroj z produkce fy. HP a to HP SoftPaq Download Manager. Nástroj je ke stažení zdarma z FTP serveru HP *ftp://ftp.hp.com/pub/caps-softpaq/HP_SDM_Setup.exe.* Po instalaci tohoto nástroje a jeho spuštění je nejprve zobrazena volba aktualizace pouze pro daný model počítače (v případě spečení na počítači HP) nebo zobrazení software pro všechny modely HP. Při spuštění nástroje se stáhne aktuální katalog ze stránek HP.

Po zvolení odpovídajících modelů, jazyka a ovladačů jsou tyto balíčky (SoftPaq), jak je znázorněno na obrázku č. 20, uloženy a rozbaleny na lokální počítač do adresáře *„C:\SoftPaqDownloadDirectory“*. Odsud se přesunou do adresáře *„C:\W7\Drivers\HP“*.



Obr. 20. Prostředí HP SoftPaq Download Managera

Import ovladačů se provádí pomocí kontextového menu *„Import Drivers“* na složce *„Out-of-Box Drivers“*. Jako zdrojová cesta pro ovladače se v dialogovém okně *„Driver source direcotory“* vloží *„C:\W7\Drivers\“*, MDT již rekurzivně skenuje všechny vnořené adresáře a potřebné ovladače importuje do příslušných složek v adresáři *„C:\DeploymentShare\Out-of-Box Drivers“* podle typu ovladače, např.: do složky *„Display“* umístí ovladače od grafických karet.

7.2.2.5 Import aplikací

Pro tento krok je předpokladem zjistit, jak danou aplikaci instalovat v silent módu, resp. jak provést plně automatizovanou instalaci bez zásahu uživatele. Jednodušší varianta je u msi balíčků, ale řada výrobců podporuje tento druh instalace i u aplikací šířených jako exe soubory. U instalátoru InstallShield je parametr pro tichou instalaci *„/s“* nebo *„/silent“*, u Windows Installeru je to naopak *„/i“* nebo *„/qn“*.

Všechny aplikace kromě JSignPdf jsou již přichystány ve formě bezobslužných instalačních exe balíčků, které stačí do MDT jednoduše naimportovat. U této aplikace se musí použít pro bezobslužnou instalaci parametr *„/silent“*.

Import aplikací se provádí pomocí kontextového menu *„New Application“* na složce *„Applications“* pro každou aplikaci samostatně. Příklad importu aplikace JSignPdf je následující:

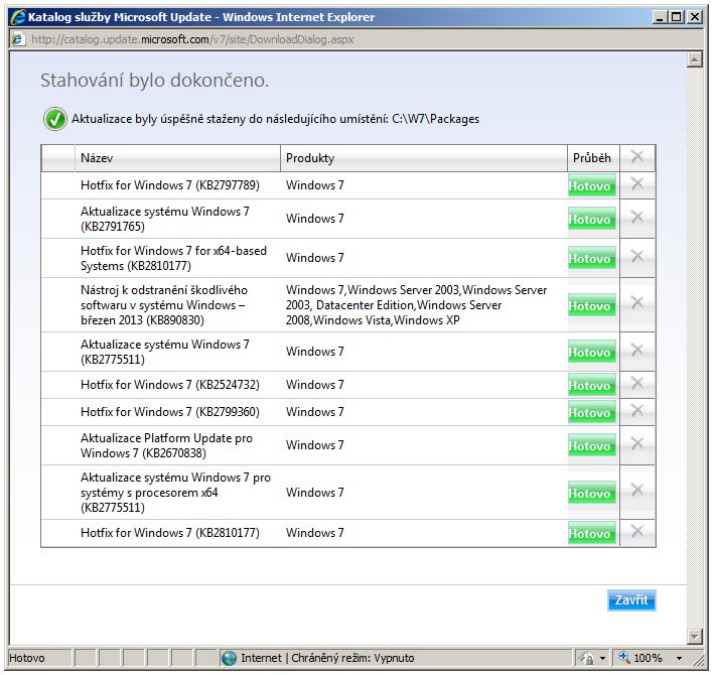
- Application Type: *Application with source files*
- Publisher: *Josef Cacek*
- Application Name: *JSingPdf*
- Version: *1.4.4*
- Language: *Czech*
- Source direktory: *„C:\W7\Appl\JSignPDF“*
- Specify the name: *Josef Cacek JSignPdf 1.4.4 (předvyplněno)*
- Command line: *JSignPdf_setup_1.4.4_wjre.exe /silent*
- Working directory: *.\Applications\Josef Cacek JSignPdf 1.4.4*

Instalace aplikací bude řídit DB MDT. Proto není třeba nastavovat podrobné vlastnosti u jednotlivých aplikací, jako je její skrytí v Deployment Wizardu či určení podporované platformy OS. Pokud ale aplikace vyžaduje po instalaci restart, je důležité tuto vlastnost pomocí instalačního parametru *„/noreboot“* vypnout a restart nastavit jako po instalační akci *„Reboot the computer after installing this application“* ve vlastnostech aplikace na kartě *„Details“*. Pokud by se restart neprovedl tímto způsobem, pak by klasický restart vyvolaný instalačním procesem způsobil přerušení migrace.

7.2.2.6 Import aktualizačních balíčků

Pro zajištění aktualizovaného image je nutné v prostředí MDT importovat aktuální záplaty operačního systému. Aktualizace pro Windows lze stáhnout ve formě *msu* balíčků (packages) ze stránek Microsoftu na adrese *„http://catalog.update.microsoft.com“*. Od doby vzniku referenčního image do 9. 4. 2013 je dostupných deset aktualizací pro Windows 7 x86 ze dne 11. 3. 2013, jak je patrné z obrázku č. 21.

Import aktualizací se provádí pomocí kontextového menu *„Import OS Packages“* na složce *„Packages“*. Jako zdrojová cesta se pro *msu* balíčky v dialogovém okně *„Package source direcotory“* vloží *„C:\W7\Packages\“*, MDT stejně jako u ovladačů rekurzivně skenuje všechny vnořené adresáře a potřebné balíčky importuje do složky *„HotFix“* nebo *„Update“* v adresáři *„C:\DeploymentShare\Packages“* podle druhu aktualizace.



Obr. 21. Stažení aktualizačních balíčků

7.2.2.7 Vytvoření a přizpůsobení Task Sequences

Jak již bylo napsáno v kapitole 2.5 Task Sequence (TS) představují jednotlivé korky, které probíhají při instalaci operačního systému. V prostředí VZP se použijí dva druhy TS:

- ***Standard Client Task Sequence*** pro počítače, které se budou migrovat, a jejich počítač nebude vyměněn za jiný. Tato TS bude použita u 99% všech stávájících počítačů a bude rovněž využívána i u nově dodaných počítačů do VZP;
- ***Standard Client Replace Task Sequence*** pro počítače, které budou vyměněny za jiný, novější model. TS extrahuje uživatelská data a provede wipe[4] disku.

Vytvoření nové TS se provádí pomocí kontextového menu *„New Task Sequence“* na složce *„Task Sequences“*. Pro Standard Client Task Sequence je postup vytvoření TS následující:

- Task Sequence ID: *VZP_REFRESH*
- Task Sequence Name: *Migrace na Windows 7 (REFRESH)*
- Select Template: *Standard Client Task Sequence*

[4] Pod pojem wipe (smazat) se označuje nenávratné odstranění dat z disku. Na rozdíl od standardního postupu, kdy je "vymazaná" oblast disku označena jako volná. S daty, které tam jsou uložena, se nic nedělá, při wipu dojde k fyzickému smazání (přepsání nulami) samotných záznamů.

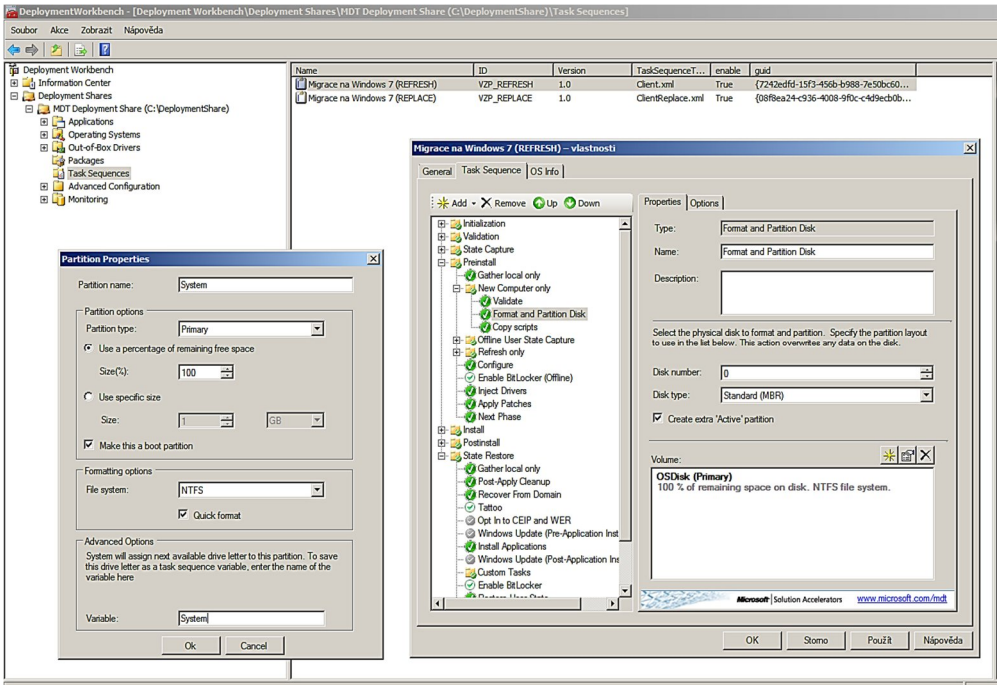
- Operating Systems: *Referencni image Windows 7 …vzp_ref_01.wim*
- Specify Product Key: *Do not specify a product key in this time*
- OS Settings Full Name: *VZP ČR*
- OS Settings Organization: *VZP ČR*
- OS Settings IE Home Page: *http://intranet.vzp.cz*
- Admin Password: *Do not specify an Administrator password at this time*

Nastavení TS pro Standard Client Replace Task Sequence je jednodušší:

- Task Sequence ID: *VZP_REPLACE*
- Task Sequence Name: *Migrace na Windows 7 (REPLACE)*
- Select Template: *Standard Client Replace Task Sequence*

Obě TS jsou uloženy v podobě XML souborů v adresáři *„C:\DeploymentShare\Control \VZP_REPLACE“* resp. *„C:\DeploymentShare\Control\VZP_REPLACE“*.

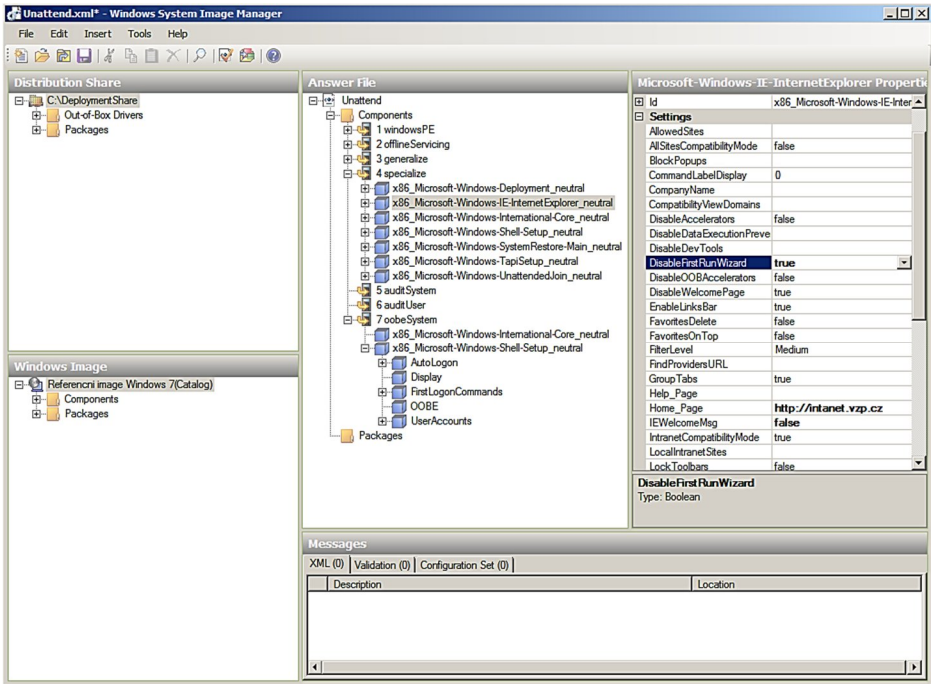
Protože má Microsoft velmi precizně zpracovaný template typu refresh, je editace této TS pro potřeby VZP jednoduchá a to obnáší pouze přejmenování disku u nových PC a minimální úpravu odpovědního souboru *„Unattend.xml“* pro nastavení Internet Exploreru a výchozího rozlišení, které se provádí právě v souvislosti s konfigurací TS.



Obr. 22. Konfigurace Task Sequence

Ve vlastnostech TS *„VZP_REFRESH“* se na záložce *„Task Sequence“* ve stromové struktuře jednotlivých kroků ve větvi *„Preinstall“* – *„New Computer Only“* – *„Format and Partition Disk“* *„Partition“* místo *„OSDisk (Primary)“* nastaví *„System (Primary)“* se 100% využitím volného místa na disku stejně jak je zobrazeno na obrázku č. 22. V této souvislosti je důležité nastavit ve větvi *„Install“* – *„Install Operating System“* jméno logické jednotky disku na *„System“*.

Na záložce *„Os Info“* je k dispozici tlačítko *„Edit Unattend.xml“*, které zpřístupní odpovědní soubor se stejným jménem pro následnou detailní úpravu vlastností instalace. Pro tento účel volá MDT aplikaci Windows System Image Manager, ve kterém je automaticky načtený odpovědní soubor referenční instalace *„vzp_ref_01.wim“*. Zde se v sekci *„Components“* – *„Specialize“* – *„x86_Microsoft-Windows-IE-IntertnetExplorer_neutral“* u položky *„DisableFirstRunWizerd“* potvrdí volba *„true“* pro zakázání wizardu při prvotním spuštění Internet Exploreru v nově vytvořeném profilu na počítači.



Obr. 23. Detailní nastavení unattend.xml

V sekci *„Components“* – *„Specialize“* – *„x86_Microsoft-Windows-Shell-Setup_neutral“* se u položky *„TimeZone“* nastaví *„Central Europe Standard Time“* a u položek *„InputLocale“*, *„SystemLocale“ a „UserLocale“* se nastaví *„cs-CZ“* pro české národní prostředí. Na závěr následuje smazání celé položky *„Display“* v sekci *„Components“* –

„oobeSystem“ – „x86_Microsoft-Windows-Shell-Setup_neutral“ pro zapnutí doporučeného rozlišení podle úhlopříčky LCD displeje. Po provedených úpravách se z menu *„File“ – „Save Answer File“* změny uloží a aplikace uzavře.

Nyní následuje update celého MDT Deployment Share pro vytvoření bootovacích souborů *„LiteTouchPE_x86.wim“* a *„LiteTouchPE_x86.iso“* v adresáři *„Boot“* s patřičnými ovladači, upraveným souborem *bootstrap.ini*, vlastním pozadím a nástrojem DaRT. Z kontextového menu vyvolaného na složce *„MDT Deployment Share“* volba *„Update Deployment Share“* zajistí kompletní regenerování adresáře *„C:\DeploymentShare“*. Ve vlastnostech generování je důležité potvrdit volbu *„Completely regenerate the boot images“*, jinak by se upravené pozadí a nástroj DaRT do bootovacího obrazu nedostal. Celá akce trvá cca. 2 hodiny.

7.2.2.8 Generování, účel a distribuce off-line instalačního média

Off-line instalační médium bude sloužit pro pracovníky UPM a VPU pro migraci Windows na pobočkách KLIPR II a pro provedení distribuce migračních souborů do připraveného adresáře *„\\sXXv0vds.srv.vzp.cz\DeploymentShare“* na vDS serverech umístěných na pobočkách typu KLIPR I a to z důvodu minimalizace zatížení WAN.

Kontextové menu *„New Media“* ze submenu *„Media“* v části *„Advanced Configuration*“ zajistí vygenerování tohoto off-line instalačního média. Do následujícího formulářového okna *„General Settings“* na dotaz *„Media Path“* se vloží cesta *„C:\W7\Offline-Media“* pro uložení výsledného souboru. Po kliknutí na *„Next“* se v adresáři *„Offline-Media“* vygeneruje potřebná adresářová struktura s příslušnými migračními skripty. Od tohoto okamžiku je v prostředí MDT v submenu *„Media“* k dispozici odkaz na médium *„Media001“*. Vlastní generování iso souboru se provede vyvoláním kontextového menu *„Update Media Content“* právě na tomto médiu001.

Vygenerovaný bootovací iso soubor *„LiteTouchMedia.iso“*, který je kopii lokálního adresáře *„C:\DeploymentShare“*, se pomocí aplikace Rufus extrahuje do podoby bootovacího USB Flash disku, který obdrží příslušní administrátoři. Po startu počítače z toho disku dojde k automatickému spuštění migračního procesu nebo se migrační proces spustí ručně z adresáře *„DeploymentShare“* na vDS, kam se obsah adresáře *„Deploy“* z USB disku nakopíruje.

7.2.2.9 Vytvoření a konfigurace MDT databáze

Jak již bylo napsáno, databáze MDT umožňuje ukládat mnoho konfiguračních nastavení, používaných pro přizpůsobení migrace. Toto nastavení je v podstatě stejné jako nastavení, které je uloženo v souboru *„CustomSettings.ini“*. Právě databáze umožní mít pouze jeden, obecný *„CustomSettings.ini“* soubor, zatímco zbývající nastavení jsou uložena v databázi.

Prostřednictvím menu *„Advanced Canfiguration“* – *„Database“* se potvrdí volba *„New Database“* a v následujícím průvodci se zadají tyto parametry:

- SQL Server name: *S01VKMNT.srv.vzp.cz*
- Instance: *SQLS01VKMNT*
- Create a new database: *MDT*
- SQL Share: *DeploymentShare*

Po vytvoření DB se v menu „Database“ zpřístupní následující sekce:

- *„Compuers“* – migrační parametry uvedené v této sekci se aplikují na konkrétní počítače podle specifické MAC adresy, Asset Tag nebo UUID;
- „Roles“ – obecné role zde vytvořené se následně využijí v sekcích *„Roles“*, *„Locations“* a *„Computers“* a tímto zjednodušují nastavení celkové konfigurace;
- *„Locations“* – tato sekce konfiguruje skupinu počítačů v rámci jedné Gateway;
- *„Make and Model“* – konfigurace skupiny počítačů podle výrobce a konkrétního modelu.

Každá z těchto sekcí obsahuje záložky:

- *„Identity“* – pro vložení jednoznačného rozlišovacího parametru (MAC adresa, Gateway, model apod.);
- *„Details“* – zde se provádí hlavní konfigurace migračního procesu dle příslušné sekce;
- *„Applications“* – určení aplikací, které se budou po migraci instalovat;
- *„ConfigMgr- Packages“* – jednoznačné určení instalačního balíčku z SCCM serveru ve tvaru *XXX00000:Program* pro následnou pomigrační instalaci;
- *„Roles“* – vložení předdefinovaných konfiguračních rolí;
- *„Administrators“* – uživatelské účty, které budou automaticky vloženy po migraci do lokální skupiny *„Administrators“* .

V následující části bude uveden příklad konfigurace MDT DB pro počítače na pobočce KLIPR I - Uherské Hradiště.

Vytvoření obecných konfiguračních rolí

Obecné konfigurační role budou aplikovány na všech migrovaných počítačích pro vytvoření určitého standardizovaného prostředí.

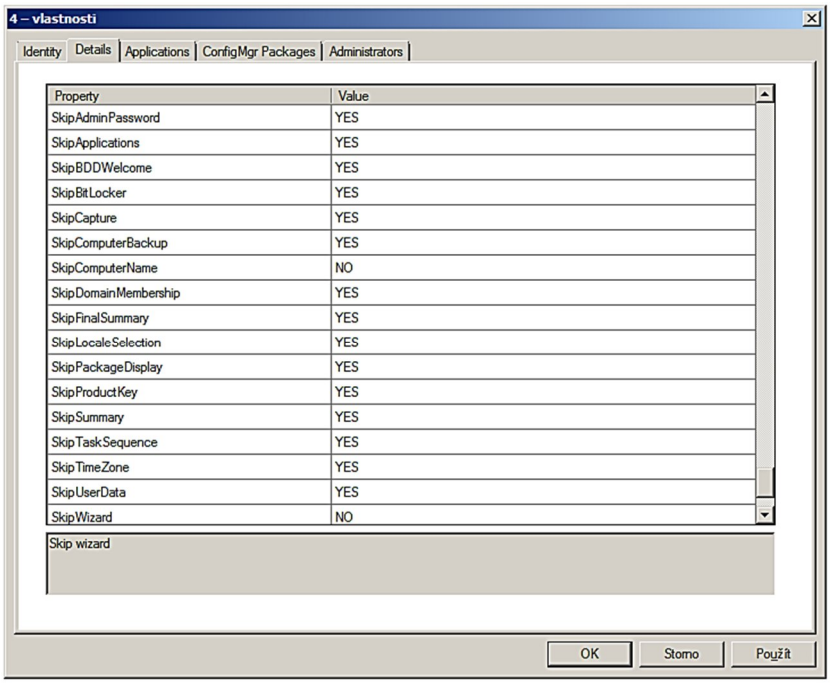
V sekci *„Roles“* se vytvoří tři konfigurační role s názvem *„01_obecna konfigurace_refresh“*, *„02_wizard_control_referesh“ a „03_aplikace“*.

Role *„01_obecna konfigurace“* nastavuje na záložce *„Details“* obecné konfigurační položky dle tabulky č. 11, jako je jméno účtu oprávněného vložit počítač do domény nebo další důležitou položku se jménem Task Sequence, která bude v rámci migrace použita.

Tab. 11. Parametry role „01_obecna konfigurace_refresh“

Property	Value	Poznámka
DomainAdmin	*mig_vzp_00*	účet umožňující vložení počítače do domény
DomainAdminDomain	*vzp.cz*	doména uživatelského účtu
DomainAdminPassword	********	heslo uživatele *„mig_vzp_00“*
_SMSTSORGNAME	*UICT / OKP / OKZaEK*	nápis uvedený v migračním okně – zkratka oddělení plánujícího migraci
FinishAction	*REBOOT*	akce provedená po úspěšné migraci
AdminPassword	********	heslo pro lokálního administrátora
TaskSequenceID	*VZP_REFRESH*	TS vyvolaná migračním procesem

Role *„02_wizard_control_refresh“* rovněž na záložce *„Details“* říká, která dialogové okna se v migračním procesu skryjí a která ne. U všech položek bude nastavena volba *„YES“* mimo položky *„SkipComputerName“* a *„SkipWizard“* tak, jak je patrné z obrázku č. 24. Povolení těchto položek zajistí administrátorovi možnost vložit doménové jméno počítače u nově instalovaných PC. U počítačů, které se migrují z prostředí Windows, bude u této položky navržen stávající název počítače, kterou buď administrátor odsouhlasí, nebo jej změní.



Obr. 24. Role „02_wizard_control_refresh“

Role *„03_aplikace“* na záložce *„Applications“* specifikuje aplikace, které budou v rámci migračního procesu nasazeny na všechny počítače. Zde se pomocí tlačítka *„Add“* – *„Lite Touch Application“* přidají aplikace: *„Josef Cacek JSignPdf 1.4.4“; „Adobe Acrobat 9.0“; „Total Commander 8.0.1“; „DameWare 9.0“* a *„Forefront Endpoint Protection 2010“*, které jsou již v prostředí MDT naimportovány.

Úprava konfigurace pro pobočku Uherské Hradiště

Specifická konfigurace migračního procesu pro pobočku Uherské Hradiště se nastavuje v sekci *„Locations“*. Zde budou využity záložky *„Identity“*, *„Details“*, *„Roles“* a *„Administrators“*.

Tab. 12. Specifické parametry pro pobočku Uherské Hradiště

Property	Value	Poznámka
UDShare	*\\s75v0vds.srv.vzp.cz\Deployment Share\MigData*	adresář pro uložení migrovaných dat
UDDir	*%OSDComputerName%*	soubor s uživatelskými daty nesoucí jméno podle názvu počítače
SLShareDynamic Logging	*\\s75v0vds.srv.vzp.cz\Deployment Share\Logs*	adresář pro uložení log souborů
MachineObjectOU	*OU=L3,OU=PCs, DC=VZP, DC=CZ*	AD LDAP cesta pro umístění počítače

Na záložce *„Identity“* se vloží do formulářového pole *„Location“* hodnota *„75_Uherske_Hradiste“* a do pole *„Default gateways“ brána „10.75.22.252“*. Na záložce *„Details“* budou nastaveny cesty podle tabulky č. 12 s údaji, kam se mají zálohovat data pomocí USMT, LDAP cesta pro umístění počítače v AD a cesta k adresáři, který slouží pro uložení logových souborů o provedené migraci.

Na záložce *„Role“* se pomocí tlačítka *„Add“* přidají připravené role *„01_obecna konfigurace_refresh“*, *„02_wizard_control_refresh“ a „03_aplikace“*.

Poslední záložka *„Administrators“* slouží pro přidání doménových účtů odpovědných administrátorů, kteří budou v lokání skupině *„Administrators“* na všech počítačích v Uherském Hradišti ve tvaru *„VZP\nazev_uctu“*.

Stejným způsobem se do sekce *„Locations“* přidá konfigurace i pro ostatní pracoviště VZP.

Nastavení pro scénář „VZP_REPLACE“

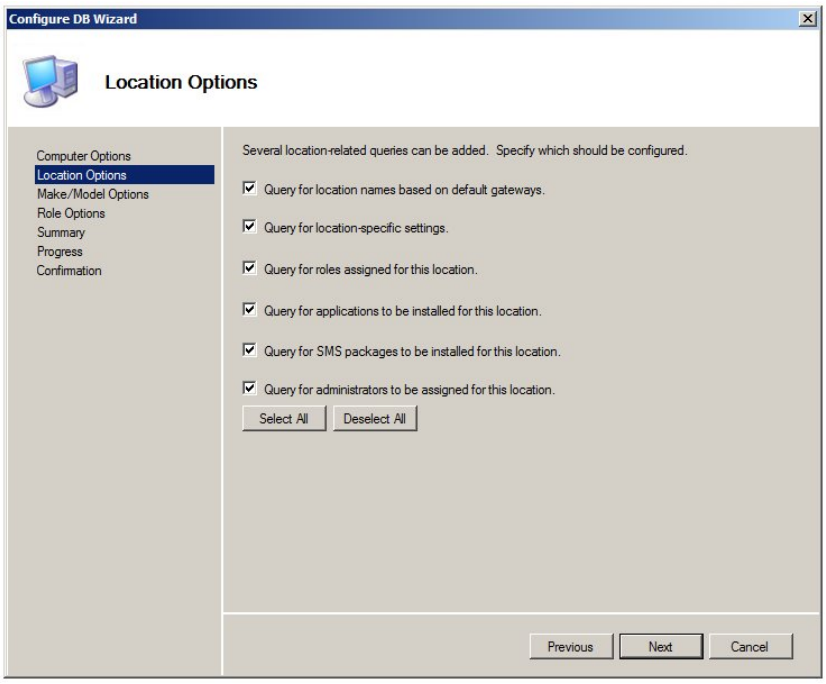
Pro případ využití scénáře replace pro TS *„VZP_REPLACE“* u počítačů, které se v průběhu migrace nahradí novým nebo jiným modernějším, bude zpřístupněna sekce *„Computers“*. Na záložce *„Indentity“* se do pole *„MAC address“* vloží MAC adresa počítače ve tvaru *„00:00:00:00:00:00“*, který bude právě tímto scénářem migrován. Následuje obdobný postup jako u TS *„VZP_REFRESH“* s tím rozdílem, že se vytvoří dvě nové role. Role *„04_wizard_control_replace“* bude kopírovat nastavení role *„02_wizard_control_refresh“*. Pouze u položky *„SkipUserData“* se nastaví *„NO“* pro to, aby měl administrátor možnost ovlivnit název souboru pro export a následný import uživatelských dat. Novou rolí je také role *„05_obecna konfigurace_replace“*, ve které je změněno pouze ID TS na *„TaskSequenceID“ = „VZP_REPLACE“*.

Na konec se na záložce *„Role“* přidají doplněné role *„04_obecna konfigurace_replace“*, *„05_wizard_control_replace“ a „03_aplikace“*. Role *„01_obecna konfigurace_refresh“*, *„02_wizard_control_refresh“* přidány nebudou.

Generování *„CustomSettings.ini“* pro databázovou podporu

Nyní přichází čas na vygenerování nového souboru *„CustomSettings.ini“*, který už bude obsahovat konfiguraci pro podporu DB MDT. Z té bude migračními skripty načítaná konfigurace sekcí *„Compuers“*, *„Roles“*, *„Locations“*, *„Make and Model“* dle předchozího nastavení.

V menu MDT *„Advanced Configuration“* probíhá generování vyvoláním kontextového menu *„Configure Database Rules“* na položce *„Database.* V následujícím průvodci zůstanou ve všech krocích *„Computer Options“*, *„Location Options“*, *„Make/Model Options“* a *„Role Options“* vybrané všechny volby proto, aby se v případě změny konfigurace některých sekcí nemuselo provádět generování a přizpůsobení souboru *„CustomSettings.ini“* znovu. Výběr možností pro sekci *„Location Options“* je znázorněno na obrázku č. 25.



Obr. 25. Generovaní souboru „CustomSetting.ini“ pro podporu MDT DB

Po dokončení generování je možné ověření nové podoby souboru *„CustomSettings.ini“* ve vlastnostech MDT Deployment Share na záložce *„Rules“*. Soubor nyní obsahuje jediný původní odkaz na monitorovací server a dále konfigurační položky pro každou sekci, definující spojení na DB MDT. Níže je uveden začátek konfigurace souboru *„Custom Settings.ini“* a konfigurace spojení pro sekce *„Locations“*, konkrétně záložky *„Identity“*, *„Datails“ a „Applications“*. Pro ostatní sekce je konfigurace obdobná.

[Settings]

Priority=Default, Locations, LSettings, LApps, LAdmins, LRoles, MMSettings, MMApps, MMAdmins, MMRoles, RSettings, RApps, RAdmins

[Default]

EventService=http://s01vkmnt.srv.vzp.cz:9800

[Locations]
SQLServer=S01VKMNT.srv.vzp.cz
Instance=SQLS01VKMNT
Database=MDT
Netlib=DBMSSOCN
SQLShare= DeploymentShare
Table=Locations
Parameters=DefaultGateway

[LSettings]
SQLServer=S01VKMNT.srv.vzp.cz
Instance=SQLS01VKMNT
Database=MDT
Netlib=DBMSSOCN
SQLShare= DeploymentShare
Table=LocationSettings
Parameters=DefaultGateway

[LApps]
SQLServer=S01VKMNT.srv.vzp.cz
Instance=SQLS01VKMNT
Database=MDT
Netlib=DBMSSOCN
SQLShare= DeploymentShare
Table=LocationApplications
Parameters=DefaultGateway
Order=Sequence

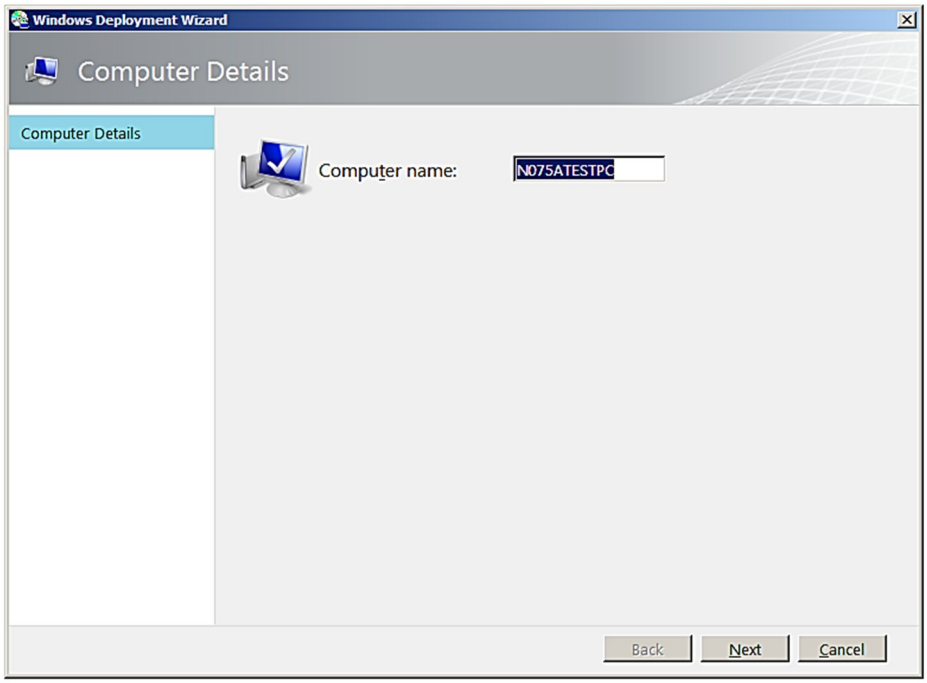
7.2.2.10 Monitoring

Monitoring, jak již bylo napsáno, probíhá ve dvou úrovních. Centrální monitoring na serveru S01VKMNT v prostředí MDT, menu *„Monitoring“*. Zde jsou zobrazeny všechny probíhající migrační procesy v celé VZP a lze se odsud prostřednictvím tlačítka *„DaRT Remote Control“* připojit do libovolné probíhající migrace, která je ve fázi instalace s použitím prostředí Windows PE. Vzdálené připojení lze realizovat pomocí tlačítka *„Remote Desktop“*, když je instalace hotová a je potřeba se z nějakého důvodu připojit do prostředí Windows 7. Druhý způsob monitoringu je prohlížení logových souborů, uložených na příslušném vDS v adresáři *„DeploymentShare\Logs“*. Tyto soubory, pojmenováné podle proměnné *„%OSDComputerName%“*, tj. podle názvu migrovaného počítače, poskytují detailní záznamy o provedených migracích.

7.3 Provedení migrace

Vlastní provedení migrace Windows XP na Windows 7 je spíše otázkou potřebného času, než náročnosti provedení. Potřebná doba na provedení se pohybuje od cca 30 do 180 minut v závislosti na výkonu počítače a množství dat, která se budou migrovat. Všechny předmigrační kroky jsou nastaveny tak, aby administrátor pouze proces migrace spustil a potvrdil jméno počítače. Všechny další konfigurace budou řízeny pomocí DB MDT. V následujících bodech jsou popsány jednotlivé kroky migračního procesu, který bude spuštěn z běžícího prostředí Windows XP.

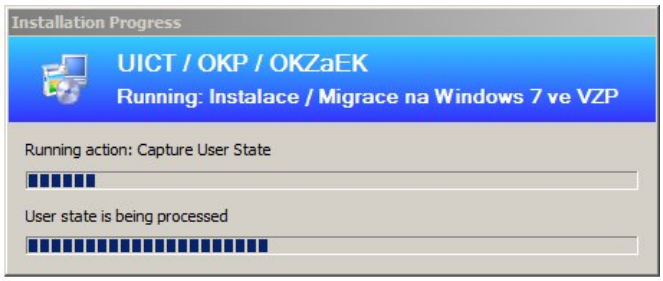
- Migrace se provádí z prostředí Windows XP, které je přihlášeno pod účtem s právy lokálního administrátora;
- Administrátor otevře adresář *„\DeploymentShare\Scripts“* z vDS na příslušné lokalitě a spuštěním souboru *„BDD_Autorun.wsf“* zahájí start migračního procestu;
- Proběhne analýza souboru *„CustomSettings.ini“* a z DB MDT se načtou odpovídající konfigurační parametry;
- Administrátor je vyzván k odsouhlasení jména počítače převzatého z Windows XP. Zde je možnost toto jméno změnit, jak je vidět na obrázku č. 26;



Obr. 26. Kontrola jména počítače v migračním procesu

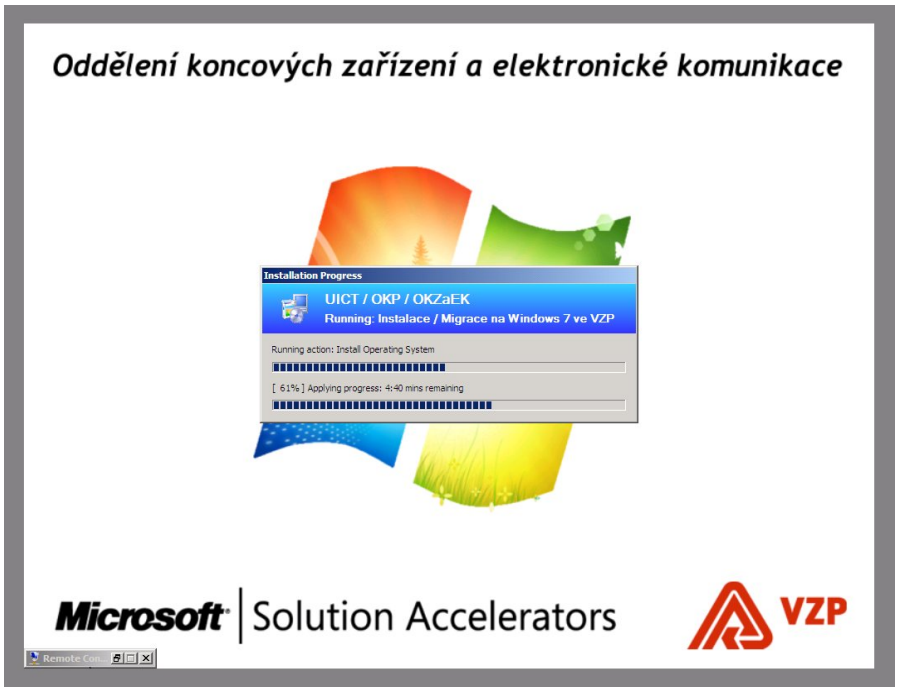
- Nyní následuje provedení *„Capture User State“*, což znamená, že migrační nástroj USMT extrahuje všechna uživatelská data a systémová nastavení pro pozdější

použití a ukládá je do adresáře na vDS „*\DeploymentShare\MigData*“ pod názvem souboru „*N075ATESTPC*“;



Obr. 27. Zálohování uživatelských dat a nastavení

- V posledním kroku před restartem probíhá aplikování upraveného prostředí Windows PE pro instalaci Windows 7 ze souboru „*DeploymentShare\Boot\ LiteTouchPE_x86.wim*“;
- Po restartu PC jsou spuštěna Windows PE včetně monitorovacích nástrojů DaRT pro vzdálený monitoring;
- Následuje bezobslužná instalace operačního systému Windows 7 na základě konfiguračních parametrů, uložených v DB MDT včetně importu ovladačů a vymazání dat na disku;



Obr. 28. Instalace Windows 7 v upraveném prostředí Windows PE

- Jakmile je OS Windows 7 nainstalován, proběhne automatický restart PC. Instalační proces dokončí instalaci a provede testování výkonu počítače;
- Ve finální fázi instalace je provedeno zařazení počítače do domény VZP, proveden import uživatelských dat a nastavení a instalace aplikací dle role *„03_aplikace“;*
- Na samotný závěr migrace je proveden restart počítače.

Nyní se může do počítače přihlásit uživatel, který by kromě nového pozadí a jiného prostředí neměl poznat, že mu na počítači něco schází nebo přebývá. V součinnosti s administrátorem zkontrolují, zdali:

- Je funkční přihlášení do počítače;
- Je počítač korektně zařazen do domény VZP;
- Obsahuje veškerá uživatelská data;
- Jsou v pořádku naimportovány certifikáty z osobního úložiště;
- Jsou namapovány sdílené složky;
- Jsou připojeny tiskárny. U tiskáren značky Hewlett-Packard není potřeba provádět žádná opatření, u tiskáren značky UTAX je potřeba provést aktualizaci ovladače z kontextového menu tiskárny *„Aktualizovat ovladač“;*
- Jsou funkční centrální aplikace.

Celá migrační akce ukládala logové soubory na server vDS do adresáře *„DeploymentShare\Logs“*, kde je možné dohledat případné problémy, které jsou společně s uživatelem odhaleny.

Protože referenční image obsahuje předkonfigurovaného SCCM klienta, proběhne do 15 minut od konce instalace na počítači instalace aktualizací systému, aktualizace antivirového programu a případná instalace aplikací, které nejsou součástí image.

V rámci Zásad skupiny je nastaveno *„Computer Certificate Autoenrollment“* a tudíž by měl počítač do 90 minut, což je doba pro periodickou obnovu Zásad skupiny, obdržet nový *„strojový certifikát“* pro potřeby ověřování 802.1x. Podmínkou je úspěšné zařazení počítače do domény VZP.

Instalace z USB Flash Disku

Instalace z USB Flash disku se bude provádět na pracovištích, kde není k dispozici vDS server nebo je spuštění z prostředí Windows XP nefunkční. Instalační proces probíhá obdobným způsobem. Do počítače stačí vložit předpřipravený bootovací USB Flash disk

a počítač spustit s podporou bootovaní právě z tohoto disku. Tentokrát proběhne i analýza souboru *„Bootstrap.ini“* pro nastavení příslušných cest k adresáři *„DeploymentShare“* podle Gateway. Cesta směřuje buď na vDS v případě, že je počítač umístěn na stejné lokalitě jako vDS, nebo směřuje na USB Flash Disk na lokalitách KLIPR II, kde vDS není. Další postup je naprosto totožný s migrací spouštěnou z prostředí Windows XP.

Instalace se současnou výměnou počítače

V ojedinělých případech se bude provádět migrace počítače s jeho současnou výměnou, nejčastěji z důvodu nedostatečného výkonu počítače. V tomto případě budou využity obě Task Sequence a to *„VZP_REPLACE“* i *„VZP_REFRESH“*. Postup provedení migrace formou Sice-by-Side je následující:

- Do DB MDT se vloží MAC adresa počítače, který bude vyměněn, jak je uvedeno v kapitole 7.2.2.9 - Nastavení pro scénář *„VZP_REPLACE“;*
- Na tomto původním PC se z adresáře *„\DeploymentShare\Scripts“* spuštěním souboru *„BDD_Autorun.wsf“* zahájí migrační proces stejně jako u TS *„VZP_REFRRESH“;*
- Protože ale předinstalační proces vyhodnotí MAC adresu počítače, budou uplatněna pravidla MDT sekce *„Compuers“*. Na základě role *„05_wizard_control_replace“* se použije scénář *„VZP_REPLACE“*, který pouze vyextrahuje uživatelská data a nastavení. Protože je dle role *„04_wizard_control_replace“* povolena volba *„SkipUserData“*, bude administrátor požádán o vložení cesty, kam se mají data zálohovat. Na závěr této TS je proveden výmaz disku formou wipe;
- Následuje fyzická výměna počítače, do kterého se vloží bootovací USB Flash disk a dále se postupuje dle odstavce Instalace z USB Flash Disku.

7.4 Shrnutí uvedeného způsobu nasazení

Tento způsob realizace migrace, uvedený v Diplomové práci je možno po menších úpravách aplikovat v obdobných organizacích, které mají větší množství poboček po celé republice či světě. Nasazení technologií LTI je sice vhodné pro organizace s celkovým počtem počítačů do 1000, ale po úpravách lze bez jakýchkoliv problémů aplikovat i na podstatně větší počty počítačů, pro které je již spíše vyhrazena technologie ZTI. Migrace touto technologií je ovšem v současné době ve VZP uskutečnitelná jen stěží, protože vyžaduje vyšší rychlost linek WAN, než má pojišťovna k dispozici. Do budoucna je ovšem možné

technologii LTI integrovat s SCCM do podoby ZTI pro naprosto bezobslužnou formu migrace.

Celý navržený způsob migrace vychází nejenom z rychlostí linek WAN, ale i z organizačního uspořádání VZP ČR, zejména úseku ÚICT, jehož pracovníci budou migraci provádět. Také z dalších limitujících faktorů jako je množství rozdílných počítačových konfigurací nebo IT infrastruktura jednotlivých poboček.

8 PLÁNOVÁNÍ A INSTALACE APLIKACÍ A AKTUALIZACÍ

Pro účely instalace aplikací je ve VZP zprovozněn System Center Configuration Manager 2007 SP R3, jak již bylo uvedeno v kapitole 5.4.2.1, který rovněž využívá Windows Server Update Services (WSUS) pro aktualizaci operačního systému na koncových zařízeních. Protože se ale plánuje ve 3 čtvrtletí roku 2013 migrace SCCM serveru na verzi 2012 SP1, budou níže uvedené postupy a doporučení vycházet právě z této nové verze SCCM, která je již v testovacím prostředí ve VZP k dispozici.

8.1 Patch management

SCCM 2012 SP1 již plně podporuje Software Update Management (SUM) s využitím Windows Server Update Services. Níže uvedené doporučení pro aktualizaci operačního systému vychází z návrhu společnosti Microsoft, uvedeného na stránkách *„http://technet.microsoft.com/en-gb/library/jj134348.aspx“*.

8.1.1 Instalace role WSUS

Instalace role WSUS verze 30.0 SP2 se provádí na SCCM serveru z instalačního balíčku *„WSUS30-KB972455-x64.exe„* staženého ze stránek Microsoft na adrese *„http://www.microsoft.com/en-us/download/details.aspx?id=5216“* nebo pomocí průvodce z prostředí SCCM. Na dotaz, zdali se má pro instalaci vytvořit Windows Internal Database nebo SQL Server, se využije druhá možnost. Jako výchozí port bude ponechán 80/443. Po instalaci se zobrazí průvodce konfigurací, který je možno uzavřít, protože se konfigurace provede až v prostředí SCCM.

Přidání role Software Update Point v SCCM se provede pomocí průvodce *„Add Site System Role Wizard“* vyvolaného z menu *„Administration“ – „Site Configuration“ – „Servers and Site Systems Roles“*. Na dotaz, zdali má být tento server aktivní software update point, bude potvrzena volba *„Use this server as the active software update point“* na výchozím portu 80/443. Jako sychnonizace se potvrdí možnost *„Microsoft update“* bez vlastního naplánování, taktéž nebude provedena klasifikace produktů a jazyků.

Následuje konfigurace Software Update Point prostřednictvím menu *„Administration“ – „Site Configuration“ – „Sites“*. V menu *„Site PR0“* se nastaví *„Clasifications“*, *„Products“* a *„Languages“* prostřednictvím menu *„Configure Site Components“ – „Software Update Point“*.

Následuje provedení ruční synchronizace *„Synchronize Software Updates“* z menu *„Software Library“* – *„Software Updates“* – *„All Software Updates“* odsouhlasením informací, že bude proveden synchronizační proces. V tomto kroku nedochází k vlastnímu stažení aktualizací, stahují se pouze informace o nich.

8.1.2 Software Update Group

V SCCM je nasazování aktualizací prováděno pomocí Software Update Group. Každá z těchto skupin může obsahovat max. 1000 aktualizací a používá se jak pro Compliance (zjištění, kde nejsou aktualizace nainstalovány), tak pro samotnou instalaci. Aktualizace je možno filtrovat dle různých podmínek, např. data vydání nebo operačního systému. Jakákoliv změna ve skupině vyvolá kontrolu shody na příslušné kolekci počítačů.

Vytvoření Compliance Group je jednoduché, pomocí menu *„Software Library“* – *„Software Updates“* – *„All Software Updates“* jsou vybrány požadované aktualizace a následně se tlačítkem *„Create Software Update Group“* vytvoří skupina *„W7_Clients_All“*. Po nasazení se z Compliance Group stává Update Group.

8.1.3 Instalace aktualizací

Nasazení aktualizací na klientech představuje aplikaci Software Update Group na konkrétní kolekci počítačů. Klient si stáhne do lokální cache software update content file z distribučního bodu, instalace pak bude provedena v přednastavené době nebo si ji může uživatel vyvolat sám dříve. Pro instalaci aktualizací je nejlepší využití průvodce *„Deploy Software Updatew Wizard“*, vyvolaného na skupině *„W7_Clients_All“* pomocí tlačítka menu *„Deploy“* s níže uvedenými předvolbami.

- Deployment name: *Aktualizace stanic s Windows 7*
- Software Update group: *W7_Clients_All*
- Collection: *Windows 7 Computers*
- Create a new deployment package: *Windows 7 Updates*
- Package source: *\\S01VKMNT\Sources\Updates\Windows7*

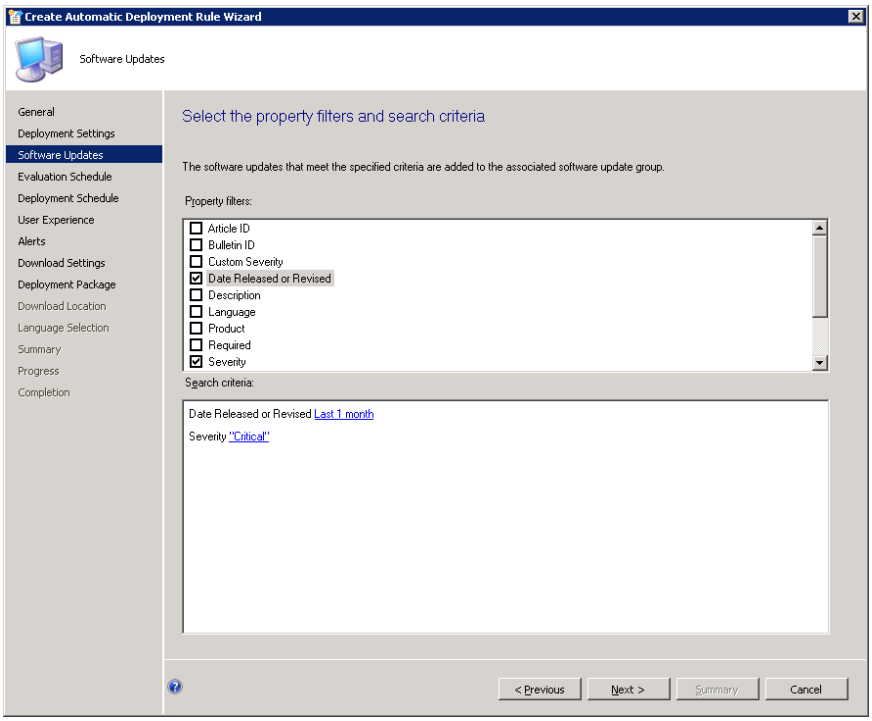
V kroku *„Summary“* se tlačítkem *„Save As Template“* nastavení uloží pod názvem *„VZP_W7_Client_Updates_Template“* pro další použití. Poslední krok *„Progress“* stahuje aktualizace do síťové složky.

8.1.4 Automatic Deployment Rules

Role Automatic Deployment Rules (ADR) zajišťuje automatické schvalování a nasazení aktualizací podle různých pravidel a za určitých podmínek. Opět se využije průvodce *„Create Automatic Deployment Wizard“* z menu *„Software Library“* – *„Software Updates“* – *„Automatic Deployment Rules“*.

- Deployment name: *Kritické aktualizace Windows 7*
- Collection: *Windows 7 Computers*
- Automatic deployment rules: *Create a new Software Update Group*
- Enable the deployment after this role is run: YES

V dalším kroku *„Software Updates“* následuje přesná definice pravidla pro výběr aktualizace dle obrázku č. 29.



Obr. 29. Definice pravidel aktualizace v prostředí SCCM

Závažnost *„Severity“* se nastaví *„Critical“* a jako *„Date released or Revised“* jeden měsíc *„Last 1 month“* – není zapotřebí instalovat při prvním spuštění všechny staré aktualizace.

Další část je obdobná jako při instalaci běžných aktualizací s výjimkou kroku *„User Experience“*, kde je vhodné vybrat volbu potlačení restartu na serverových operačních

systémech. Jako *„Deployment Package“* bude vytvořen nový balíček *„Windows 7 Critical Updates“* v místění *„\\S01VKMNT\Sources\Updates\Windows7\Critical“*. Tlačítkem *„Run Now“* je možno aktualizace na klientských počítačích spustit okamžitě.

Automatic Deployment Rules se rovněž využívá pro aktualizace antivirového systému Microsoft Forefront Endpoint Protection, který je do prostředí SCCM plně integrován a využívá všech jeho možností pro distribuci virových definic na koncové zařízení a servery.

8.2 Instalace aplikací

Pro instalací aplikací se použije stejně jako v případě aktualizací OS Microsoft System Center Configuration Manager 2012, který přináší do správy aplikací několik nových myšlenek. Hlavní je zaměření na uživatele místo na zařízení. Označuje se to termínem User-centric Application Management a jde o to, že uživatel může mít řadu zařízení nebo může užívat různé počítače. Instalace aplikace je řízena podle toho, kde se uživatel přihlásí.

Další novinkou je State-based Application Management, kdy instalace závisí na stavu aplikace. Zjišťuje se, zda již aplikace není nainstalovaná, jestli se má instalovat nebo odinstalovat a teprve při instalaci se kopírují data. Aplikace je možno instalovat za určitých předem zadaných podmínek, například pouze na počítač, který má více než 2GB RAM nebo jde o Windows 7. Může být více typů instalace, na některých zařízeních je využita standardní instalace, zatímco jinde App-V verze aplikace [24].

Protože SCCM nabízí nepřeberné možnosti pro instalaci aplikací a rozbor těchto funkcí není ani předmětem této práce, bude v následujícím postupu předvedeno nasazení aplikace Firefox Portable nejjednodušším způsobem.

8.2.1 Vytvoření instalačního balíčku

Jako zdroj pro vytvoření instalace poslouží výborný kompresní nástroj 7-Zip, stažený ze stránek *„http://downloads.sourceforge.net/sevenzip/7z920.msi“* ve formě *msi* instalačního balíčku, uloženého do adresáře *„\\S01VKMNT\Sources\Appl\“*.

Kliknutím na ikonu *„Create Application“* z menu *„Software Library“* – *„Application Management“* – *„Applications“* se zahájí proces vytvoření nové instalace:

- Installer Type: *Windows Installer (native)*
- Location: *\\S01VKMNT\Sources\Appl\7z920.msi*

- Name: *7-Zip*
- Software version: *9.20*
- Install Behavior *Install for System*
- Installation program: *msiexec /i „7z920.msi“ /q*

Nyní je aplikace připravena k distribuci na počítače a nebude využívat možnost instalace na uživatele.

8.2.2 Nasazení aplikace

Instalace aplikací se provádí nasazením aplikace na předem připravenou vhodnou kolekci počítačů. Protože je zapotřebí aplikaci 7-Zip nasadit na všechny nové počítače se systémem Microsoft Windows 7, bude vybrána kolekce *„Windows 7 Computers“*.

Pro nasazení aplikací slouží ikona *„Deploy“* z menu *„Software Library“ – „Application Management“ – „Applications“*:

- Software: *7-Zip 9.20*
- Collection: *Windows 7 Computers*
- Automatically distribute content for dependencies: *YES*
- Distribution Point: *PR0*
- Deployment Settings Action: *Install*
- Scheduling: *As soon as possible*

Kroky User Experience a Alert není třeba pro nasazení této aplikace řešit, používají se u Business Critical aplikací, kde je důležité sledovat chyby v instalaci a tyto pak neprodleně reportovat administrátorovi SCCM. Rovněž se neřeší instalace aplikací na vyžádání.

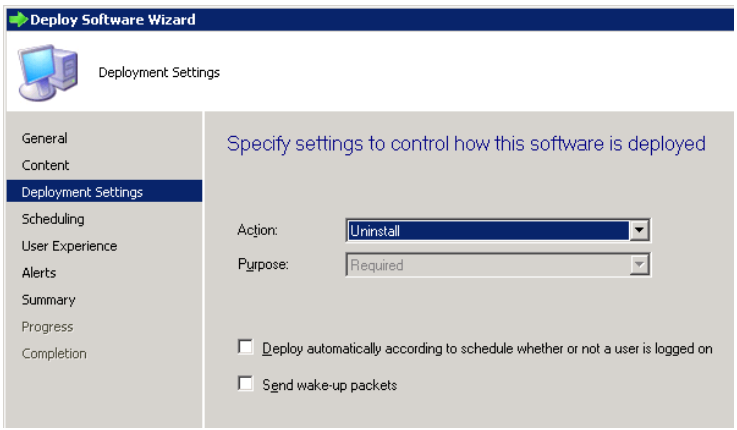
8.2.3 Monitoring instalace

SCCM umožnuje jednoduchým způsobem sledovat průběh instalace. V menu *„Monitoring“ – „Deployments“* je zobrazen seznam všech instalovaných aplikací. Na konkrétní aplikaci stačí vyvolat z kontextového menu *„View Status“*, kde je několik záložek pro sledování. V případě, že je stav nasazení *„Success“*, proběhl proces instalace úspěšně, pokud je zde

uvedeno *„In Progress“*, instalace probíhá. Stav *„Unknown“* je stav neznámý, *„Requirements Not Met“* nebyly splněny podmínky pro instalaci a *„Error“*, kdy z nějakého důvodu došlo k chybě instalace.

8.2.4 Odinstalování aplikací

Pokud je vytvořen Deployment na určitou kolekci, který aplikaci instaluje, není možno vytvořit nový, jenž aplikaci odinstaluje, protože by došlo ke konfliktu. V tomto případě se musí buď konkrétní počítač odstranit z kolekce a připraví se nová kolekce, která aplikaci odinstaluje. Nebo se smaže původní Deployment tlačítkem *„Delete“* na záložce *„Deployments“* v menu *„Software Library“* – *„Application Management“* – *„Applications“*. Poté se vytvoří nová aplikace výše uvedeným způsobem, pouze u volby *„Deployment Settings Action“* bude nastaveno *„Uninstall“*, jak je patrné z obrázku č. 30.



Obr. 30. Odinstalování aplikací pomocí SCCM

9 ZABEZPEČENÍ UŽIVATELSKÉHO PROSTŘEDÍ

Otázka zabezpečení uživatelského prostředí je velmi obsáhlá a v prostředí velkých organizací se tomuto problému věnuje nejenom oddělení IT, ale i oddělení bezpečnosti, jak je tomu i v případě VZP ČR.

V poslední kapitole bude tedy nastíněno možné zabezpečení uživatelského prostředí pomocí Zásad skupiny na straně Active Directory a aplikování protokolu 802.1x na straně operačního systému Windows 7. Ten předpokládá správně nakonfigurované síťové prostředí, zejména server Radius nebo Cisco switche. Na nově dodaných noteboocích s čipem TPM verze 1.2 a vyšším se navíc počítá s implementací funkce BitLocker pro zabezpečení dat na disku. Tato funkcionalita ale nebude zavedena dříve, než se Active Directory upraví pro ukládání klíčů. Poté bude Bitlocker aktivován pomocí Zásad skupiny. Další formy zabezpečení, kde patří třeba heslo do BIOSu nebo přihlašování pomocí certifikátu apod., již rozebírány nebudou, protože se jedná o obecné formy zabezpečení, aplikovatelné v různých operačních systémech.

9.1 Zabezpečení klientských stanic pomocí Zásad skupiny

Systémové politiky, aplikované na doménové úrovni, patří bezesporu k nejefektivnějším nástrojům zabezpečení uživatelské prostředí v rámci podnikové sítě. Protože se ale v této Diplomové práci jedná o aplikaci bezpečnostních politik v reálném prostředí velké organizace, jsou v následujícím textu záměrně některé citlivé konfigurační parametry a cesty uvedeny z důvodu bezpečnosti zkresleně, nebo nejsou uvedeny vůbec. Rovněž níže uvedené Zásady skupiny jsou pouze obecně doporučující zásady aplikovatelné v libovolném podnikovém prostředí. Klíčové bezpečnostní Zásady skupiny, použité ve VZP, zde uvedené nejsou.

Ve VZP jsou politiky aplikovány jak na pracovní stanice, tak uživatele v organizačních jednotkách pro tyto LDAP cesty:

- OU=PCs, DC=vzp, DC=cz
- OU=Users, DC=vzp, DC=cz

V OU *„PCs“* jsou z politik vyčleněny kontejnery *„Level_0“* a *“Level_1“*, na které Zásady skupiny aplikovány nejsou. Tady se jedná o počítače některých systémových administrátorů a VIP uživatelů. Na tyto počítače se ovšem vztahují politiky na úrovni domény vzp.cz.

9.1.1 Zásady skupiny - konfigurace počítače

Níže uvedené konfigurační parametry obsahují obecné doporučující parametry pro prostředí VZP, po úpravách je možné jejich použití v jakékoliv jiné organizaci. Jsou zde uvedena nejdůležitější nastavení, která se budou určitě časem měnit podle potřeb uživatelů a správců.

Tab. 13. GPO - Zásady hesla

Zásada	Nastavení
Heslo musí splňovat požadavky na složitost	Povoleno
Maximální stáří hesla	120 dní
Minimální délka hesla	10 znaků
Minimální stáří hesla	1 dní
Vynutit použití historie hesel	15 hesel zapamatováno

Tab. 14. GPO - Zásady uzamčení účtu

Zásada	Nastavení
Doba uzamčení účtu	90 min.
Prahová hodnota pro uzamčení účtu	8 neplatných pokusů o přihlášení
Vynulovat čítač pro zamknutí účtu po	30 min.

Tab. 15. GPO - Zásady auditu

Zásada	Nastavení
Auditovat používání oprávnění	Neúspěch
Auditovat přístup k objektům	Neúspěch
Auditovat správu účtů	Úspěch, selhání
Auditovat systémové události	Úspěch, selhání
Auditovat události přihlášení	Úspěch, selhání
Auditovat události přihlášení k účtu	Úspěch, selhání
Auditovat změny zásad	Úspěch, selhání

Tab. 16. GPO - Přiřazení uživatelských práv

Zásada	Nastavení
Povolit přihlášení prostřednictvím Vzdálené plochy	vzp_admins
Zakázat přihlášení prostřednictvím Vzdálené plochy	users

Tab. 17. GPO - Interaktivní přihlášení

Zásada	Nastavení
Interaktivní přihlašování: Chování při odebrání čipové karty	Uzamknout pracovní stanici
Interaktivní přihlašování: Nezobrazovat naposledy použité uživatelské jméno	Povoleno
Interaktivní přihlašování: Počet předchozích přihlášení uložených v mezipaměti pro případ, že řadič domény není k dispozici	20 přihlášení
Interaktivní přihlašování: Nevyžadovat stisknutí kláves Ctrl+Alt+Del	Zakázáno
Interaktivní přihlašování: Text zprávy pro uživatele pokoušející se přihlásit	Neautorizované použití je zakázáno! / Unauthorized use is prohibited!
Interaktivní přihlašování: Vyzvat uživatele ke změně hesla před jeho vypršením	10 dnů
Interaktivní přihlašování: Nadpis zprávy pro uživatele pokoušející se přihlásit	"Varování / Warning"

Tab. 18. GPO - Konzola obnovení

Zásada	Nastavení
Konzola pro zotavení: Povolit automatické přihlášení správce	Zakázáno
Konzola pro zotavení: Povolit kopírování na disketu a přístup ke všem jednotkám a složkám	Zakázáno

Tab. 19. GPO - Server sítě Microsoft

Zásada	Nastavení
Server sítě Microsoft: Digitálně podepsat komunikaci (pokud klient souhlasí)	Povoleno
Server sítě Microsoft: Doba nečinnosti před přechodem relace do režimu spánku	30 min.
Server sítě Microsoft: Vždy digitálně podepsat komunikaci	Zakázáno

Tab. 20. GPO - Účty

Zásada	Nastavení
Účty: Přejmenovat účet Guest	"%Host!!!"
Účty: Přejmenovat účet správce	"wadmin"

Tab. 21. GPO - Vypnout

Zásada	Nastavení
Vypnutí: Povolit vypnutí systému bez nutnosti přihlášení	Zakázáno

Tab. 22. GPO - Zařízení

Zásada	Nastavení
Zařízení: Omezit přístup k disketové jednotce pouze na místně přihlášené uživatele	Povoleno
Zařízení: Omezit přístup k jednotce CD-ROM pouze na místně přihlášené uživatele	Povoleno
Zařízení: Povoleno formátování a vysunutí vyměnitelných médií	Administrators
Zařízení: Zabránit uživatelům instalovat ovladače tiskáren	Povoleno

Tab. 23. GPO - Protokol událostí

Zásada	Nastavení
Maximální velikost aplikačního protokolu	10240 kilobajtů
Maximální velikost protokolu zabezpečení	10240 kilobajtů
Maximální velikost systémového protokolu	10240 kilobajtů
Metoda uchování aplikačního protokolu	Podle potřeby
Metoda uchování protokolu zabezpečení	Podle potřeby
Metoda uchování systémového protokolu	Podle potřeby
Zabraňuje místní skupině Guests získat přístup k aplikačnímu protokolu.	Povoleno
Zabraňuje místní skupině Guests získat přístup k protokolu zabezpečení.	Povoleno
Zabraňuje místní skupině Guests získat přístup k systémovému protokolu.	Povoleno

Tab. 24. GPO - Brána Windows Firewall

Zásada	Nastavení
Brána Windows Firewall: Chránit všechna síťová připojení	Povoleno
Brána Windows Firewall: Povolit výjimky místních programů	Povoleno
Brána Windows Firewall: Povolit výjimku protokolu ICMP	Povoleno
Brána Windows Firewall: Zakázat upozorňování	Povoleno

Tab. 25. GPO - Instalační služba systému Windows

Zásada	Nastavení
Povolit uživatelům ovládat instalace	Zakázáno
Protokolování	Povoleno
Umožnit správci instalaci z relace služby Vzdálená plocha	Povoleno

Tab. 26. GPO - Internet Explorer

Zásada	Nastavení
Zóny zabezpečení: Nepovolit uživatelům měnit zásady	Povoleno
Zóny zabezpečení: Nepovolit uživatelům přidávat či odebírat servery	Povoleno
Neumožnit uživatelům povolovat či zakazovat doplňky	Povoleno
Zakázat zobrazení úvodní obrazovky	Povoleno

Tab. 27. GPO - Služba Vzdálená plocha

Zásada	Nastavení
Nastavit časový limit aktivních, ale nečinných relací služby Vzdálená plocha	20 min.
Nepovolit přesměrování tiskárny klienta	Povoleno
Nepovolit přesměrování jednotek	Povoleno
Umožňuje nastavit pravidla vzdáleného řízení uživatelských relací služby Vzdálená plocha.	Povoleno

Tab. 28. GPO - Zásady automatického přehrávání

Zásada	Nastavení
Vypnout automatické přehrávání (Turn off Autoplay)	Povoleno

Tab. 29. GPO - Zásady skupin

Zásada	Nastavení
Interval aktualizace zásad skupiny pro počítače	90 min.
Rozpoznání pomalého připojení zásad skupiny	Povoleno

9.1.2 Zásady skupiny - konfigurace uživatele pro skupinu *„Všichni uživatelé“*

Tab. 30. GPO - Nabídka Start a Hlavní panel

Zásada	Nastavení
Nepovolovat připojování programů na hlavní panel	Povoleno
Nezobrazovat žádné vlastní panely nástrojů na hlavním panelu	Povoleno
Odebrat ikonu Síť z nabídky Start	Povoleno
Odebrat ikonu Hudba z nabídky Start	Povoleno
Odebrat odkaz Hledat počítač	Povoleno
Odebrat příkaz Hry z nabídky Start	Povoleno
Odebrat síťová připojení z nabídky Start	Povoleno
Zabránit změnám nastavení hlavního panelu a nabídky Start	Povoleno
Odebrat ikonu Centrum akcí	Povoleno
Odebrat příkaz Spustit z nabídky start	Povoleno

Tab. 31. GPO - Ovládací panely

Zásada	Nastavení
Zakázat přístup k Ovládacím panelům	Povoleno
Zobrazit pouze určené panely v Ovládacích panelech	Povoleno
Časový limit spořiče obrazovky	600 sec.
Chránit spořič obrazovky heslem	Povoleno
Povolit spořič obrazovky	Povoleno
Vynutit konkrétní spořič obrazovky	*„C:\windows\system32\vzp_scr.scr“*
Zabránit změnám pozadí plochy	Povoleno
Načíst konkrétní motiv	*„C:\windows\system32\ zp_theme.theme“*
Skrýt kartu Nastavení	Povoleno
Zabránit změnám barevného schématu	Povoleno
Zabránit změnám motivu	Povoleno
Zabránit změnám vizuálního styku oken a tlačítek	Povoleno
Zabránit změnám nastavení barvy a vzhledu okna	Povoleno

Zabránit změnám pozadí plochy	Povoleno
Zabránit změnám ukazatelů myši	Povoleno
Zabránit změnám spořiče obrazovky	Povoleno

Tab. 32. GPO - Přidat nebo odebrat programy

Zásada	Nastavení
Odebrat položku Přidat nebo odebrat programy	Povoleno
Skrýt možnost Přidat program z disku CD-ROM nebo z diskety	Povoleno
Skrýt možnost Přidat programy získané od společnosti Microsoft	Povoleno
Skrýt stránku Přidat nebo odebrat součásti systému Windows	Povoleno
Skrýt stránku Nastavit přístup a výchozí hodnoty programu	Povoleno
Přejít přímo na Průvodce součástmi systému Windows	Povoleno
Odebrat informace o podpoře	Povoleno

Tab. 33. GPO - Plocha

Zásada	Nastavení
Odebrat průvodce vyčištěním plochy	Povoleno
Odebrat příkaz Vlastnosti z místní nabídky ikony Počítač	Povoleno
Odebrat příkaz Vlastnosti z místní nabídky ikony Dokumenty	Povoleno
Zakázat úpravy panelů nástrojů na ploše	Povoleno
Zakázat změny	Povoleno
Zakázat systém Active Desktop	Povoleno

Tab. 34. GPO - Instalační služba systému Windows

Zásada	Nastavení
Zakázat všechny instalace z vyměnitelných médií	Povoleno

Tab. 35. GPO - Internet Explorer

Zásada	Nastavení
Zakázat změnu nastavení domovské stránky	Povoleno
Zakázat změnu nastavení barev	Povoleno
Zapnout automatické dokončování pro uživatelská jména a hesla ve formulářích	Zakázáno
Zakázat stránku Připojení	Povoleno
Zakázat stránku Programy	Povoleno
Zakázat stránku Rozšířené	Povoleno
Zakázat stránku Zabezpečení	Povoleno
Automaticky zjišťovat nastavení konfigurace	Povoleno
Automatická konfigurace prohlížeče	Povoleno
Adresa URL automatického serveru proxy (soubor JS, JVS nebo PAC)	http://proxy.vzp.cz:3128/vzp.pac
Adresa URL domovské stránky	http://intranet.vzp.cz/default.aspx

Tab. 36. GPO - Další součásti systému Windows

Zásada	Nastavení
Odebrat kartu DFS	Povoleno
Odebrat kartu Hardware	Povoleno
Odebrat kartu Zabezpečení	Povoleno
Odebrat příkaz možnosti složky z nabídky Nástroje	Povoleno
Maximální povolená velikost Koše	2
Odebrat možnost měnit nastavení animace nabídek pomocí uživatelského rozhraní	Povoleno
Zakázat ikonu Celá síť ve složce Místa v síti	Povoleno
Zakázat položku Okolní počítače ve složce Umístění v síti	Povoleno

Omezit přístup uživatelů pouze k výslovně povoleným modulům snap-in	Povoleno
Zabránit uživateli přejít do autorského režimu	Povoleno
Vypnout aplikaci Windows Mail	Povoleno
Nepovolit animace okna	Povoleno
Nepovolit tvorbu plochy	Povoleno
Nepovolit použití funkce Přepínání oken 3D	Povoleno
Zakázat spuštění aplikace Windows Media Center	Povoleno

Tab. 37. GPO - Systém

Zásada	Nastavení
Zakázat přístup k příkazovému řádku	Povoleno
Vypnout přístup k části pro řešení potíží s výkonem	Povoleno
Vypnout přístup k hlavní části centra sledování výkonu	Povoleno
Při obnovení činnosti z režimu spánku nebo režimu hlubokého spánku vyžadovat heslo	Povoleno
Zakázat uživateli přepsat nastavení národního prostředí	Povoleno

Instalace aplikací pomocí Zásad skupin nebude ve VZP využita, pro tyto účely je k dispozici Microsoft System Center Configuration Manager.

9.2 Aplikace ověřování 802.1x ve Windows 7

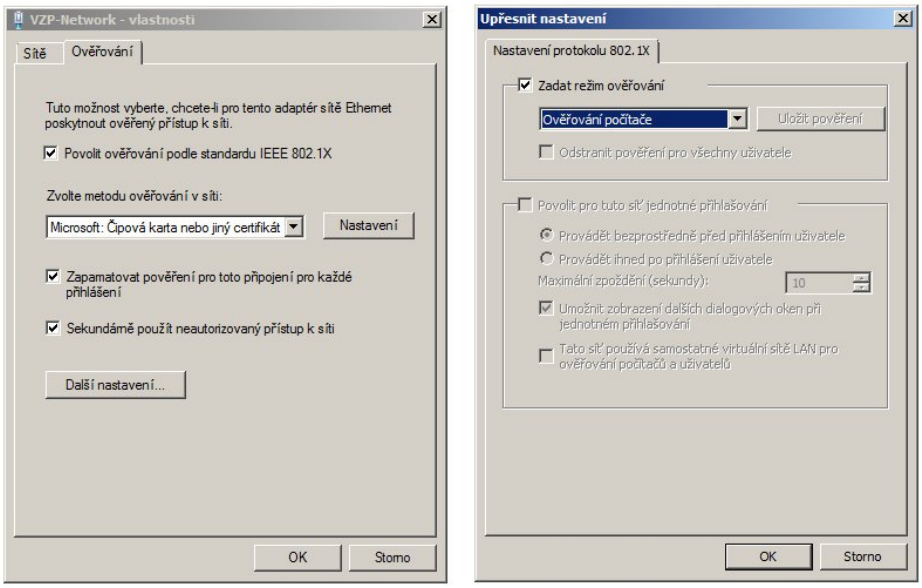
Pro správnou funkci autentizace protokolem 802.1x je důležité mít správně nakonfigurovaný server RADIUS a klienta v podobě switche Cisco. Tuto konfiguraci provedli pracovníci Oddělení správy sítí. Předmětem této kapitoly je konfigurace Windows 7 pro ověřování 802.1x na koncových stanicích.

Autentizace je nastavena na ověřování počítače pomocí strojového certifikátu. Pokud se nejedná o autorizovaný stroj, do sítě se nedostane, resp. bude zařazen do VLAN, neumožňující tento přístup. V opačném případě bude počítač zařazen do správné VLAN dle požadavku. Pro počítače uživatelů je vyčleněna VLAN 19, pro počítače administrátorů VLAN 28.

Konfigurace Windows 7 pro ověřovaní pomocí protokolu 802.1x lze ve VZP nastavit dvěma způsoby. Automatizovaným instalačním balíčkem *„802.1x.exe“*, který lze aplikovat pomocí SCCM centrálně nebo ruční konfigurací stanice. Pokud se použije automatizovaný instalační balíček, není potřeba žádná interakce administrátora či uživatele pro nastavení autentizace. Po instalaci je počítač restartován a jeho registrace do sítě VZP již proběhne pomocí certifikátu *„VZP-Root-CA-WIN“*.

Ruční aktivace ověřování spočívá v provedení následujícího postupu:

- Zobrazení služeb systému pomocí příkazu *„services.msc“;*
- Spuštění služby *„Wired AutoConfig Service“;*
- V *„Ovládacích panelech“* – *„Síť a Internet“* – *„Centrum sítí a sdílení“* se vybere odkaz *„Spravovat síťová připojení“;*
- Na síťovém připojení *„VZP-Network“* se ve vlastnostech připojení povolí ověřování 802.1X;
- Výběrem *„Povolit ověřování podle standardu IEEE 802.1X“* bude zapnuto ověřování 802.1x;
- Jako zvolený způsob ověřování je použita metoda: *„Microsoft: Čipová karta nebo jiný certifikát“* a pomocí tlačítka *„Další nastavení“* se vybere režim ověřování *„Ověřování počítače“* jak je zobrazeno na obrázku č. 31;



Obr. 31. Vlastnosti nastavení ověřování 802.1x

- *Na závěr se pomocí tlačítka „Nastavení“* na kartě *„Ověřování“* vybere certifikát pro ověření *„VZP-Root-CA-WIN“*.

Kontrolu úspěšnosti autentizace pomocí certifikátu lze jednoduše ověřit pomocí příkazu *„ipconfig.exe“*, kde by měla být zobrazena správná IP adresa. Počítač by měl mít umožněn přístup do sítě VZP. Pokud autentizace neproběhne, nebude počítači umožněn přístup do sítě VZP a počítač zůstane nadále v karanténě.

ZÁVĚR

Pokud je hardware srdcem počítače, je operační sytém 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 není možno po tomto datu nadále provozovat nepodporovaný operační systém, je proto nutné provést na 4456 počítačích ve Všeobecné zdravotní pojišťovně České Republiky migraci stávajícího provozovaného operačního systému Microsoft Windows XP na nový operační systém.

Jako nový operační systém byl vybrán Microsoft Windows 7, i když jsou již půl roku k dispozici nejnovější Windows 8. Mezi dva hlavní důvody volby operačního systému Windows 7 je dostupnost ovladačů hardware pro všechny modely počítačů provozovaných ve Všeobecné zdravotní pojišťovně a minimalizace dopadů ze změny operačního systému právě pro koncového uživatele.

Jako migrační scénář byl zvolen Wipe-and-Load Deployment, který nahrazuje stávající provozovaný operační systém operačním systémem novým v rámci jedné pracovní stanice a zároveň zajistí jednotnost všech počítačů v pojišťovně.

Důsledně zpracovaná analýza současného stavu IT byla důležitá pro správnou volbu operačního systému a časového harmonogramu migrace. Z toho vyplývá, že je potřeba 270 dní na provedení úprav centralizovaných aplikací společností Hewlett-Packard s.r.o., provedení předmigračních akcí Oddělením koncových zařízení a elektronické komunikace a vlastní realizaci migrace.

Jako metoda nasazení byla zvolena technologie společnosti Microsoft, která má opodstatnění hlavně u hromadných instalací ve velkých organizacích, a to Lite-Touch High Volume Dynamic Deployment. Výhodou této technologie je žádná nebo naprosto minimální interakce místního administrátora během migračního procesu.

Mezi nejdůležitější kroky přípravné fáze patří zajisté příprava hybridního referenčního image, který bude v prostředí VZP ČR nasazen a konfigurace klíčového nástroje Microsoft Deployment Toolkit 2012 pro zajištění migrace technologií LTI.

Na vlastní realizaci migrace potřebuje VZP ČR 2 měsíce, aby byl na 90 procentech počítačů nahrazen stávající operační systém novým. Tuto finální část migrace bude realizovat Oddělení uživatelské podpory v místě současně s Oddělením vzdálené podpory uživatelů.

O včasnou aktualizaci klientského operačního systému se bude starat robustní nástroj Microsoft System Center 2012 Configuration Manager společně se službou Microsoft Windows Server Update Services. Tyto nástroje rovněž zajistí aktualizaci antivirového systému Microsoft Forefront Endpoint Protection.

Instalace aplikací, které nejsou součástí image, bude rovněž zajištěna nástrojem Microsoft System Center 2012 Configuration Manager na vhodnou předem připravenou kolekci počítačů.

Správné zabezpečení uživatelského prostředí bude řešeno na fyzické úrovni pomocí protokolu 802.1x, který umožní přístup do sítě VZP ČR pouze autentifikovaným počítačům na základě platného certifikátu. Na doménové úrovni bude zabezpečení realizováno pomocí Zásad skupiny na příslušné organizační jednotky.

Pro tuto Diplomovou práci bylo nutno spolupracovat s pracovníky napříč všemi odbory v rámci Úseku informačních a komunikačních technologií. Velké poděkování patří zejména pracovníkům Oddělení správy Microsoft systémů, kteří byli nápomocni v oblasti konfigurace služby WSUS pro podporu Windows 7 a pracovníkům Oddělení správy sítí za přípravu switchů Cisco a serveru Radius pro ověřování pomocí protokolu 802.1x.

Věřím, že Všeobecná zdravotní pojišťovna České Republiky využije všechny informace, nebo alespoň jejich převážnou část, pro provedení migrace operačních systémů na uživatelských počítačích a ušetří tím nemalé finanční prostředky než by tomu bylo v případě zajištění migrace externím subjektem.

Na závěr je důležité podotknout, že, s menšími odchylkami, je postup uvedený v této Diplomové práci snadno aplikovatelný i v jiných organizacích.

CONCLUSION

If hardware is the heart of a computer, the operating system is its soul. In principle, it is the operating system which characterizes a computer, therefore, it is important for the operating system to be always in immaculate condition.

As the company Microsoft will officially stop the support for the operating system Windows XP on the 8th April 2014 and it is not possible after this date to run an unsupported operating system, therefore, migration of the existing operating system Microsoft Windows XP to a new operating system has to be performed on 4,456 computers in the General Health Insurance Company of the Czech Republic.

Microsoft Windows 7 has been chosen as the new operating system despite the newest system Windows 8 has been available for half a year already. Two main reasons why the operating system Windows 7 has been chosen are represented by availability of hardware drivers for all models of computers operated in the General Health Insurance Company and by minimization of effects caused by change of the operating system for end users.

The Wipe-and-Load Deployment migration method has been chosen which supersedes the existing operating system by a new operating system within one work station and which will, at the same time, ensure uniformity of all computers in the insurance company.

A consistent analysis of the existing situation in IT was important for the right choice of the operating system and the time schedule for the migration. It follows from the above mentioned that 270 days are necessary to perform modifications of centralized applications by the company Hewlett-Packard s.r.o., to perform pre-migration provisions by the Department of Terminals and Electronic Communication and to perform the migration as such.

The implementation method chosen is the Lite-Touch High Volume Dynamic Deployment, a technology of the company Microsoft which is justified mainly in case of collective installations in large organizations. Advantage of this method is represented by no or by absolutely minimum interaction of the local administrator during the migration process.

The most important steps in the preparatory phase are surely represented by preparation of a hybrid reference image which will be implemented in the environment of the General

Health Insurance Company of the Czech Republic and by configuration of Deployment Toolkit 2012, the key Microsoft tool to ensure migration of technologies LTI.

The General Health Insurance Company of the Czech Republic needs 2 months to perform the migration as such and to supersede the existing operating system by the new one on 90 % of computers. This final part of the migration will be performed locally by the Department of User Support simultaneously with the Department of Remote Support for Users.

A robust tool Microsoft System Center 2012 Configuration Manager together with Microsoft Windows Server Update Services will look after timely updating of the client operating system. These tools will also ensure updating of the antivirus system Microsoft Forefront Endpoint Protection.

Installation of applications which are not a part of the image will also be ensured by the tool Microsoft System Center 2012 Configuration Manager on a suitable collection of computers prepared in advance.

Correct protection of the user environment on physical level will be by means of the protocol 802.1x which will enable only authenticated computers to have access to the network of the General Health Insurance Company of the Czech Republic on the basis of a valid certificate. Protection on the domain level will be performed by Group Policy of the relevant organization unit.

Cooperation with workers from all branches within the Department of Information and Communication Technologies was necessary for this Thesis. Grateful acknowledgment is made mainly to workers in the Microsoft Systems Administration Department who were very helpful in configuration of WSUS services to support Windows 7 and no less grateful acknowledgment is also made to workers in the Network Administration Department for preparation of Cisco switches and Radius server for verification with the use of the protocol 802.1x.

I do believe that the General Health Insurance Company of the Czech Republic will use all information or at least the prevailing part of the information to carry out migration of operating systems on user's computers and will thus save considerably higher financial resources than if migration were ensured by an outsourced entity.

It is important to mention at the end that the procedure given in this Thesis is easily applicable also in other organizations with small changes.

SEZNAM POUŽITÉ LITERATURY

[1] Asset Inventory Service 2.0. *Microsoft Technet: Zdroje informací pro profesionály v oboru IT* [online]. 2011 [cit. 2013-01-19]. Dostupné z: http://blogs.technet.com/b/technetczsk/archive/2011/05/25/asset-inventory-service-2-0.aspx

[2] Brána firewall: nejčastější dotazy. *Microsoft* [online]. [cit. 2012-11-22]. Dostupné z: http://windows.microsoft.com/cs-CZ/windows7/What-is-a-firewall

[3] CAFOUREK, Bohdan. *Windows 7: kompletní příručka*. 1. vyd. Praha: Grada, 2010, 326 s. ISBN 978-80-247-3209-1.

[4] Co je Centrum akcí? *Microsoft* [online]. [cit. 2013-02-16]. Dostupné z: http://windows.microsoft.com/cs-CZ/windows7/What-is-Action-Center

[5] Co je systém souborů EFS (Encrypting File System)? *Microsoft* [online]. [cit. 2013-02-16]. Dostupné z: http://windows.microsoft.com/cs-CZ/windows7/What-is-Encrypting-File-System-EFS

[6] Co jsou skupiny zásad (Group Policy). SOUKUP, Ondřej. *C:\> IT Bloguje* [online]. 2009 [cit. 2013-02-17]. Dostupné z: http://www.it-bloguje.cz/windows-server/active-directory/70-co-jsou-skupiny-zasad-group-policy.html

[7] Deploying a Windows 7 MUI machine based on a "Hybrid MUI image" within Configmgr 2012. BUNTINX, Kenny. *System Center: User Group Belgium* [online]. 2013 [cit. 2013-02-16]. Dostupné z: http://scug.be/sccm/2013/01/07/deploying-a-windows-7-mui-machine-based-on-a-hybrid-mui-image-within-configmgr-2012/

[8] Deploying Images with Windows Deployment Services (part 1) - WDS Requirements & Deploying Images with WDS. *WINDOWS* [online]. 2011 [cit. 2013-02-14]. Dostupné z: http://allcomputers.us/windows_7/deploying-images-with-windows-deployment-services-(part-1)---wds-requirements---deploying-images-with-wds.aspx

[9] Desktop systémy Microsoft Windows: IW1/XMW1 2012/2013. FIEDOR, Jan. Vysoké učení technické v Brně: Fakulta informačních technologií [online]. 2012 [cit. 2013-02-02]. Dostupné z: http://www.fit.vutbr.cz/study/courses/IW1/public/info/lib/exe/fetch.php?media=iw1:iw1-lecture-01.pdf

[10] KŘIVÁK, Jan. Projekt na zavedení dopravního informačního systému v organizaci [online]. Uherské Hradiště, 2011 [cit. 2013-03-11]. Dostupné z: https://portal

.utb.cz/stag?urlid=prohlizeni-prace-detail&praceIdno=19923. Bakalářská práce. Univerzita Tomáše Bati ve Zlíně. Univerzita Tomáše Bati ve Zlíně. Fakulta logistiky a krizového řízení. Vedoucí práce Ing. Jan Strohmandl.

[11] MAP Toolkit 8.0 k dispozici. *Microsoft Technet* [online]. 2013 [cit. 2013-01-14]. Dostupné z: http://blogs.technet.com/b/technetczsk/archive/2013/01/03/map-toolkit-8-0-k-dispozici.aspx

[12] MICROSOFT CORPORATION. 6292A Installing and Configuring Windows 7 Client: Microsoft Official Course. Microsoft Corporation, 2009, 459 s. X17-37160.

[13] MICROSOFT CORPORATION. 6294A Planning and Managing Windows 7 Desktop Deployments and Environments: Microsoft Official Course. Microsoft Corporation, 2009, 623 s. X17-40182.

[14] Microsoft DeploymentToolkit 2010 Update 1: Using the Microsoft Deployment Toolkit. *Scribd: The World's Largest Online Library. Read, Publish, and Share Documents and Written Works* [online]. 2010 [cit. 2013-03-25]. Dostupné z: http://www.scribd.com/doc/50846412/Using-the-Microsoft-Deployment-Toolkit

[15] Nasazujeme Windows 7 – díl první. *Microsoft Technet: Zdroje informací pro profesionály v oboru IT* [online]. 2010 [cit. 2013-02-02]. Dostupné z: http://blogs.technet.com/b/technetczsk/archive/2010/03/15/serial-nasazujeme-windows-7-dil-prvni.aspx

[16] Nasazujeme Windows 7 - metody nasazení, WDS (díl pátý). *Microsoft Technet: Zdroje informací pro profesionály v oboru IT* [online]. 2010 [cit. 2013-02-14]. Dostupné z: http://blogs.technet.com/b/technetczsk/archive/2010/04/12/nasazujeme-windows-7-metody-nasazeni-wds-dil-paty.aspx

[17] Nasazujeme Windows 7 – strategie pro obraz, údržba referenčního obrazu (díl třetí). *Microsoft Technet: Zdroje informací pro profesionály v oboru IT* [online]. 2010 [cit. 2013-02-02]. Dostupné z: http://blogs.technet.com/b/technetczsk/archive/2010/03/29/nasazujeme-windows-7-strategie-pro-obraz-udrzba-referencniho-obrazu-dil-treti.aspx

[18] Novinky Windows 7: Řízení uživatelských účtů (UAC). *Cnews.CZ* [online]. 24.9.2009 [cit. 2013-02-16]. Dostupné z: http://extrawindows.cnews.cz/novinky-windows-7-rizeni-uzivatelskych-uctu-uac

[19] Pět důvodů, proč se zaměřit na Windows 7 a ne 8. *CIO Business World on-line* [online]. 2012 [cit. 2013-03-20]. Dostupné z: http://businessworld.cz/it-strategie/Aktualizace-podniku-Pet-duvodu-proc-se-zamerit-na-Windows-7-a-ne-8-9695

[20] Používání programu Windows Defender. *Microsoft* [online]. [cit. 2013-02-16]. Dostupné z: http://windows.microsoft.com/cs-CZ/windows7/Using-Windows-Defender

[21] Prepare and Service Windows Images Using the New DISM Tool. *Microsoft Technet Magazine* [online]. [cit. 2013-02-14]. Dostupné z: http://technet. microsoft.com/en-us/magazine/dd490958.aspx

[22] Sada Windows® Automated Installation Kit (AIK) pro systém Windows® 7. *Microsoft: Download Center* [online]. 2009 [cit. 2013-02-07]. Dostupné z: http://www.microsoft.com/cs-cz/download/details.aspx?id=5753

[23] SCCM 2012 - Operating System Deployment. *Www.SAMURAJ-cz.com* [online]. 2012 [cit. 2013-02-16]. Dostupné z: http://www.samuraj-cz.com/clanek/sccm-2012-operating-system-deployment/

[24] SCCM 2012 - správa (instalace) aplikací. *Www.SAMURAJ-cz.com* [online]. 2012 [cit. 2013-04-18]. Dostupné z: http://www.samuraj-cz.com/clanek/sccm-2012-sprava-instalace-aplikaci/

[25] Single Sign-On. TRASK SOLUTIONS A.S. *Trask* [online]. [cit. 2013-03-18]. Dostupné z: http://www.trask.cz/single-sign-on

[26] SMITH, Ben a Brian KOMAR. *Zabezpečení systému a sítě Microsoft Windows. 1*. vyd. Překlad David Krásenský, Anna Rychetská. Brno: Computer Press, 2006, 700 s. ISBN 80-251-1260-8.

[27] System Center Essentials. *Microsoft* [online]. 2009 [cit. 2013-01-19]. Dostupné z: https://www.microsoft.com/cze/systemcenter/essentials/

[28] TULLOCH, Mitch. Windows 7 resource kit. Redmond, WA: Microsoft Press, c2010, xlviii, 1709 p. ISBN 978-073-5693-852.

[29] VÝŠEK, Ondřej. Microsoft Deployment Toolkit (MDT) 2010 - finální verze. *Optimalizovane IT* [online]. 2009 [cit. 2013-02-15]. Dostupné z: http://www .optimalizovane-it.cz/deployment/microsoft-deployment-toolkit-mdt-2010-finalni-verze.html

[30] VÝŠEK, Ondřej. Projekt nasazení Windows 7 - část první: Přípravy. *Optimalizovane IT* [online]. 2009 [cit. 2013-01-13]. Dostupné z: http://www.optimalizovane-it.cz/windows-7/projekt-nasazeni-windows-7-cast-prvni-pripravy.html

[31] VÝŠEK, Ondřej. Projekt nasazení Windows 7 - díl druhý kompatibilita aplikací. *Optimalizovane IT* [online]. 2009 [cit. 2013-01-19]. Dostupné z: http://www.optimalizovane-it.cz/windows-7/projekt-nasazeni-windows-7-dil-druhy-kompatibilita-aplikaci.html

[32] VÝŠEK, Ondřej. Projekt nasazení Windows 7 díl třetí instalace operačního systému. *Optimalizovane IT* [online]. 2010 [cit. 2013-02-02]. Dostupné z: http://www.optimalizovane-it.cz/windows-7/projekt-nasazeni-windows-7-dil-treti-instalace-operacniho-systemu.html

[33] VÝŠEK, Ondřej. Sysprep - základní stavební kámen tvorby instalačního image Windows 7. *Optimalizovane IT* [online]. 2010 [cit. 2013-02-12]. Dostupné z: http://www.optimalizovane-it.cz/windows-7/sysprep-zakladni-stavebni-kamen-tvorby-instalacniho-image-windows-7.html

[34] VÝŠEK, Ondřej. User State Migration Tool (USMT) 5.0 - jak migrovat uživatelská data. *Optimalizovane IT* [online]. 2013 [cit. 2013-02-16]. Dostupné z: http://www.optimalizovane-it.cz/deployment/user-state-migration-tool-usmt-5.0-jak-migrovat-uzivatelska-data.html

[35] Windows 7 - kterou verzi zvolit? KENCKI, Adam. *PCWorld* [online]. 2009 [cit. 2013-01-19]. Dostupné z: http://pcworld.cz/software/windows-seven-6679.

[36] Windows 7: Přehled hlavních funkcí jednotlivých edicí systému. *DITCom* [online]. [cit. 2013-02-22]. Dostupné z: http://www.ditcom.cz/download/partner_datasheet_w7.pdf

[37] Windows Imaging File Format (WIM). *Microsoft Technet: Zdroje informací pro profesionály v oboru IT* [online]. 2009 [cit. 2013-02-02]. Dostupné z: http://technet.microsoft.com/en-us/library/dd799284(WS.10).aspx

[38] Windows PE 2.0 (Windows Preinstallation Environment alias WinPE). *AdminXP.cz* [online]. [cit. 2013-02-13]. Dostupné z: http://www.adminxp.cz/windowsvista/index.php?aid=223

[39] Zabezpečení podnikové sítě - NetworkLogin 802.1x. *CompuNet: Network Design & Supervision* [online]. [cit. 2013-02-17]. Dostupné z: http://www.compunet.cz/networklogin/

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ACM	Application Compatibility Manager
ACS	Access Control Systém
ACT	Application Compatibility Toolkit
AIS	Asset Inventory Service
AIS	Asset Inventory Service
API	Application Programming Interface
DCP	Data Collection Provider
DFS	Distributed File Systém
DISM	Deployment Image Servicing and Management
DLL	Dynamic-link library
FTP	File Transfer Protocol
GPMC	Group Policy Management Console
GPO	Group Policy Object
HW	Hardware
IE	Internet Explorer
IT	Informační technologie
KMS	Key Management Services
LDAP	Lightweight Directory Access Protocol
LPS	Log Processing Service
LZX	LZ77 family compression algorithm
MAP	Microsoft Assessment and Planning Toolkit
MDOP	Microsoft Desktop Optimization Pack
MDT	Microsoft Deployment Toolkit
MS-CHAPv2	Microsoft Challenge Handshake Authentication Protocol verze 2

OS	Operační systém
OU	Organizational Unit
PDF	Portable Document Format
PKI	Public Key Infrastrukture
RADIUS	Remote Authentication Dial In User Service - RFC 2865
RAM	Random Access Memory
SCCM	System Center Configuration Manager
SCE	System Center Essentials
SCE	System Center Essentials
SQL	Structured Query Language
SUA	Standard User Analyzer
SUM	Software Update Management
SW	Software
TCP	Transmission Control Protocol
VPN	Virtual Private Network
W7 UA	Windows 7 Upgrade Advisor
WAIK	Windows Automated Installation Kit
WDS	Windows Deployment Services
WIM	Windows Imaging File Format
WMI	Windows Management Instrumentation
WMI	Windows Management Instrumentation
WRP	Windows Resource Protecion
WSUS	Windows Server Update Services
XML	Extensible Markup Language

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: POROVNÁNÍ VERZÍ OS WINDOWS

Kategorie	Vlastnost	Windows XP SP3	Windows Vista SP1	Windows 7
Správa a organizace souborů	Desktop search	Ke stažení	Ano	Vylepšené
	Knihovny	Ne	Ne	Nové
	Federované vyhledávání	Ne	Ne	Nové
	Enterprise Search Scopes (Windows 7 Ultimate/Enterprise + Windows Server 2008 R2)	Ne	Ne	Nové
Vzdálený přístup	DirectAccess	Ne	Ne	Nové
	VPN Reconnect	Ne	Ne	Nové
	BrancCache	Ne	Ne	Nové
	Mobilní širokopásmový přístup	Ne	Ne	Nové
	RemoteApp & připojení desktopu	Ne	Ne	Nové
Bezpečnost	BitLocker	Ne	Ano	Vylepšené
	BitLocker ToGo	Ne	Ne	Nové
	AppLocker	Ne	Ne	Nové
	Více profilů FireWall	Ne	Ne	Nové
	Detailní audit	Ne	Ano	Vylepšené
	User Account Control	Ne	Ano	Vylepšené
	Domain Name System Security Extensions	Ne	Ne	Nové
	Podpora Smart karet	Ano	Ano	Vylepšené
	Podpora Biometriky	Ano, 3. strana	Ano, 3. strana	Nové
Správa	Windows PowerShell v2	Ke stažení	Ke stažení	Již obsaženo
	Skriptování nastavení skupinových politik	Ne	Ne	Vylepšené
	Group Policy preferences	Ke stažení	Ke stažení	Nové
	Windows Recovery Environment	Ne	Ano	Vylepšené
	Platforma pro řešení problémů	Ne	Ne	Nové
	Jednotné trasování	Ano	Ano	Vylepšené
	Záznam problému	Ne	Ne	Nové
	Vzdálený přístup k informacím o spolehlivosti	Ne	Ne	Nové
Nasazení	Deployment image servicing & správa obrazů	Ne	Ano	Vylepšené
	Dynamic Driver Provisioning	Ne	Ne	Nové

	Volume Activation	Ne	Ano	Vylepšené
	Multicast multiple stream transfer	Ne	Ne	Nové
	User State Migration Tool	Ano	Ano	Vylepšené
	Správa a nasazení pomocí VHD	Ne	Ne	Nové
	Možnosti vzdáleného přístupu (Multimedia, obousměrný zvuk, více monitorů)	Ne	Ne	Nové
	VHD boot	Ne	Ne	Nové

PŘÍLOHA P II: POROVÁNÍ EDIC OS WINDOWS 7

Možnosti uživatelského rozhraní					
	Home Basic	Starter	Home Premium	Professional	Enterprise & Ultimate
Základní rozhraní Windows					
Standardní rozhraní Windows					
Rozhraní Windows Aero ("Glass")					
Aero Peek					
Aero Snaps					
Aero Shake					
Pozadí Aero					
Windows Flip					
Windows Flip 3D					
Živý náhled (hlavní panel)					
Živý náhled (Explorer)					
Jump Lists					
Windows Search					

Bezpečnostní vlastnosti					
	Home Basic	Starter	Home Premium	Professional	Enterprise & Ultimate
Vylepšené UAC					
Centrum akcí					
Windows Defender					
Windows Firewall					
IE 8 Protected Mode					
Windows Update					
Rychlé přepínání uživatelů					
Rodičovská kontrola					

Výkon					
	Home Basic	Starter	Home Premium	Professional	Enterprise & Ultimate
Windows ReadyDrive					
Windows ReadyBoost					
SuperFetch					

Podpora 64-bit procesorů			✓	✓	✓
Maximální fyzických počet procesorů	1	1	2	2	2
Počet jader procesorů	Neomezeno	Neomezeno	Neomezeno	Neomezeno	Neomezeno
Max RAM (32-bit)	4 GB	4 GB	4 GB	4 GB	4 GB
Max RAM (64-bit)	n/a	n/a	16 GB	192 GB	192 GB
Dostupnost a spolehlivost					
	Home Basic	Starter	Home Premium	Professional	Enterprise & Ultimate
Windows Backup	✓	✓	✓	✓	✓
Instalace obrazem disku	✓	✓	✓	✓	✓
Záloha na síť				✓	✓
Encrypted File System (EFS)				✓	✓
BitLocker					✓
BitLocker To Go					✓
Automatická defragmentace	✓	✓	✓	✓	✓
Předchozí verze souborů	✓	✓	✓	✓	✓
Vytvořit a připojit VHD	✓	✓	✓	✓	✓
Přiložené aplikace					
	Home Basic	Starter	Home Premium	Professional	Enterprise & Ultimate
Internet Explorer 8	✓	✓	✓	✓	✓
Miniaplikace Windows a galerie	✓	✓	✓	✓	✓
Základní hry (FreeCell, Hearts, Minesweeper, Purble Palace, Solitaire, Spider Solitaire)	✓	✓	✓	✓	✓
Prémiové hry (Internet Backgammon, Internet Checkers, Internet Spades, Mahjong Titans)			✓	✓	✓
Kalkulačka	✓	✓	✓	✓	✓
Paint	✓	✓	✓	✓	✓
Výstřižky			✓	✓	✓
Poznámky			✓	✓	✓
Windows Journal			✓	✓	✓
Faxování a skenování	✓	✓	✓	✓	✓
Windows PowerShell a ISE	✓	✓	✓	✓	✓
WordPad	✓	✓	✓	✓	✓
Prohlížeč XPS	✓	✓	✓	✓	✓

Digitální média a zařízení					
	Home Basic	Starter	Home Premium	Professional	Enterprise & Ultimate
Prohlížeč fotografií					
Foto slide-show					
Windows MediaPlayer 12 s technologií Play To					
Windows MediaPlayer vzdálené přehrávání					
Dekódování MPEG-2					
Kompatibilita s DolbyDigital					
Dekódování AAC a H.264					
DVD playback					
Je možné doinstalovat MPEG-2 (přehrávání DVD)			n/a	n/a	n/a
Windows Media Center					
Počet podporovaných TV tunerů			4 od každého typu (analog, digital,...)	4 od každého typu (analog, digital,...)	4 od každého typu (analog, digital,...)
Windows DVD Maker					
Device Stage					
Sync Center					

Síťové možnosti					
	Home Basic	Starter	Home Premium	Professional	Enterprise & Ultimate
Připojení pomocí SMB	20	20	20	20	20
Centrum sítí a sdílení					
HomeGroup	Pouze připojit	Pouze připojit			
Vylepšená správa napájení					
Připojení k projektoru					
Vzdálená plocha					
Připojení k počítači - vzdálená plocha					
IIS Web Server					
Podpora RSS					
Sdílení připojení k internetu					
Propojení síťových adaptérů					
Soubory Offline					

Vlastnosti pro mobilní zařízení					
	Home Basic	Starter	Home Premium	Professional	Enterprise & Ultimate
Windows Mobility Center	Ano (Bez prezentačního módu)		Ano (Bez prezentačního módu)		
Windows Sideshow (Další monitory)					
Sync Center					
Tablet PC					
Podpora Multi-Touch					
Podnikové možnosti					
	Home Basic	Starter	Home Premium	Professional	Enterprise & Ultimate
Připojení do domény (Windows Server)					
Licencovaný XP Mode					
AppLocker					
Boot z VHD					
BranchCache					
DirectAccess					
Federované vyhledávání (Enterprise Search Scopes)					
Vícejazyčná podpora (MUI)					
Tisk Location-aware					
Subsystém pro UNIX-based Aplikace					

PŘÍLOHA P III: PRACOVNÍ MÓDY PROTOKOLU 802.1X

Network Login blokován
- Klienti bez bezpečnostního mechanismu budou mít přístup do sítě

Standardní Network Login
- Bude vyžadována autentizace neautorizovaných klientských portů
- Port přepínače, který byl již autentizován, bude otevřen - Tento pracovní mód umožňuje přístup neautorizovaných stanic do sítě například použitím opakovače nebo přepínače, za nímž bude jediná ověřená stanice. Z hlediska úrovně poskytované bezpečnosti je nutné se tomuto módu pokud možno vyhnout.

Zabezpečený mód
- MAC adresa je zaznamenána oproti portu autorizace bude platná pouze proti MAC adrese, která ověření provedla.
- Bude předáván pouze provoz do a z této MAC
- Druhá a případné další MAC adresy viděné na portu budou blokovány
- Tento mód je vhodný pro omezení množství připojených stanic na koncových přepínačích na jednu per port.

Upozornění: tento mód nelze použít souběžně s hardware IP telefonie (VoIP telefony s integrovaným dvouportovým bridge) či virtualizací systému nástroji typu VMWare či Virtual PC v bridge modu. Virtualizační nástroje mohou pracovat v NAT režimu na ověřované stanici bez omezení.

Vícenásobně zabezpečený mód
- " MAC adresa stanice je zaznamenána oproti portu, na kterém provedla úspěšné 802.1x ověření a dále bude předáván pouze provoz do a z této MAC adresy
- Na tom samém portu se mohou autentizovat další uživatelé pro získání přístupu
- Stanice, jejíž MAC adresa neprovedla úspěšné ověření, bude vyřazena z provozu, aniž to ovlivní činnost na portu již ověřených stanic

RADA

Radius Authenticated Device Access - modifikace technologie Network Login, která umožní přihlášení do sítě na všechna zařízení, bez ohledu na klienta, tedy například i síťové tiskárny, IP telefony, bezdrátové přístupové body, terminály a podobně. Toto rozšíření umožní namísto ověření 802.1x použití MAC adresy konzového zařízení pro potřeby ověření v centrální databázi RADIUS serveru. RADA navíc umožňuje definovat řízený přístup k síti pro dočasné uživatele, které začlení do definované hostitelské oblasti, například s přístupem pouze do Internetu. RADA tak používá k ověření fyzickou adresu stanice, ale lze ji kombinovat i s ověřením přes 802.1x. Síť potom rozlišuje, zda je připojeno povolené zařízení nebo neznámý počítač, případně v kombinaci s přihlášením rozlišuje i práva uživatele. Tyto způsoby ověření podporují i automatické zařazení uživatele ke skupině (AutoVLAN) nebo automatické nastavení kvality služby (AutoQoS). V této souvislosti je třeba zmínit, že existují postupy, jak měnit fyzickou MAC adresu síťových rozhraní, nicméně tato procedura není obecně známá běžným uživatelům výpočetní techniky. Doporučeno je omezit použití RADA technologie pro ověřování pouze a právě jen zařízení, v nichž není podpora 802.1x implementována a takto ověřená zařízení zařazovat do virtuálních sítí určených pro specifický provoz (například VLAN pro síťové tiskárny a scannery či VLAN pro VoIP).

AutoVLAN

Funkce, která doplňuje ověřování uživatele a umožňuje automatizovat nastavení virtuální sítě. Uživatel/stanice má na ověřovacím serveru uveden rovněž příznak skupiny (vedle jména a hesla). Po úspěšném ověření uživatele je port přístupového přepínače nastaven do příslušné virtuální sítě. Uživatelé a stanice jsou potom nezávislí na místě připojení, vždy dostanou stejné prostředí.

GuestVLAN

Funkce umožňují automatické zařazení neautorizovaných uživatelů do zvláštní VLAN, která má nastavená přístupová pravidla třeba jen pro přístup k Internetu.

AutoQoS

Funkce, která doplňuje ověřování uživatele a umožňuje automatizovat nastavení QoS parametrů. Uživatel/stanice má na ověřovacím serveru uveden příznak QoS, vedle jména a hesla. Po úspěšném ověření uživatele je na port přístupového přepínače nastavena příslušná kvalita služby. Uživatelé a stanice jsou potom nezávislí na místě připojení, vždy dostanou stejné prostředí.

Voice VLAN

Funkce, která usnadní konfiguraci uživatelům IP telefonie. Podporuje IP telefony hlavních dodavatelů a automaticky umístí telefon do definované hlasové VLAN.

DHCP Tracker

Zajímavá funkce přepínačů, které směrují IP provoz. L3 přepínač sleduje, zda stanice používá adresu, kterou získala korektní DHCP žádostí. Funkce umožní komunikovat mimo svoji VLAN pouze klientům, kteří přijali svoji IP adresu z DHCP serveru. Pokud uživatel manuálně nastaví jiné parametry, přepínač komunikaci zablokuje.

PVLAN

Privátní virtuální síť sice není přímo součástí NetworkLogin, ale je výborným rozšířením zabezpečení sítě. PVLAN zajistí, že stanice/uživatelé v jedné VLAN nemohou vzájemně sdílet prostředky. Mohou komunikovat pouze směrem na L3 interface. Zde mohou být aplikována další přístupová pravidla.

PŘÍLOHA P IV: ORGANIZAČNÍ SCHÉMA VZP ČR