Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačního inženýrství

Diplomová práce

Infrastruktura tenkých klientů

Zdeněk Kukla

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Katedra informačního inženýrství

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Zdeněk Kukla

Informatika

Název práce

Infrastruktura tenkých klientů

Název anglicky

Thin clients infrastructure

Cíle práce

Diplomová práce je zaměřena na problematiku provozu aplikací podnikových informačních systémů prostřednictvím infrastruktury tenkých klientů. Hlavním cílem je ve vybrané organizaci navrhnout konkrétní řešení, zrealizovat jej za pomoci dostupných technologií a vlastního software a následně úspěšně uvést do rutinního provozu. Programové vybavení bude poskytováno terminálovými servery s operačním systémem Windows a prostřednictvím služby Vzdálená plocha doručováno do koncových zařízení, která budou pracovat se síťově zaváděným operačním systémem Debian a prostředím zhotoveným podle potřeb organizace.

Metodika

Teoretická část práce je zaměřena na analýzu problematiky a rešerši dostupných technologických řešení. Praktická část práce navazuje analýzou prostředí vybrané organizace, návrhem řešení, jeho realizací a uvedením do reálného provozu. Závěr práce zhodnocuje dosažených výsledků.

Doporučený rozsah práce

50 60 stran

Klíčová slova

Tenký klient, terminálový server, vzdálená plocha, RDP protokol, print server, PXE server

---

Doporučené zdroje informací

ANDERSON, Christa a Kristin L. GRIFFIN, Windows Server 2008 R2 Remote Desktop Services: Resource Kit. Redmond: Microsoft Press, 2010, s. 720 ISBN 978-07-356-2737-6.

DEBIAN.ORG. Debian Univerzální operační systém [online]. Dostupné z: http://www.debian.org/

HERTZOG, Raphaël a Roland MAS. The Debian Administrator's Handbook. Freexian, 2013, s. 464 ISBN 979-10-91414-02-9.

MICROSOFT.COM. Microsoft TechNet [online]. Dostupné z: http://technet.microsoft.com/

REIMER, Stan, Conan KEZEMA, Mike MULCARE, Byron WRIGHT. Windows server 2008 Active Directory: Resource Kit. Redmond: Microsoft Press, 2008, s. 827 ISBN 978-07-356-2515-0.

Předběžný termín obhajoby

2015/06 (červen)

Vedoucí práce

Ing. Marek Pícka, Ph.D.

Elektronicky schváleno dne 10. 11. 2014

Ing. Martin Pelikán, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 10. 11. 2014

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 24. 03. 2015

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Infrastruktura tenkých klientů" jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 24.3.2015 _____

Poděkování

Rád bych touto cestou poděkoval vedoucímu diplomové práce Ing. Marku Píckovi, Ph.D. za pomoc při zpracování práce, podněty a připomínky. Dále Mgr. Nataše Petsini, ředitelce Rehabilitační nemocnice Beroun, za svěřenou důvěru pro reálnou implementaci řešení.

Infrastruktura tenkých klientů

Thin clients infrastructure

Souhrn

Diplomová práce se zabývá problematikou praktické realizace infrastruktury tenkých klientů pro provozování informačních systémů a aplikačního software v prostředí moderní nemocnice. Teoretická část práce je přehledem typických možností řešení. Obsahem praktické části je analýza současného stavu ICT v organizaci, předložení vyhovujících inovativních řešení a vlastní realizace, která spočívá ve výběru hardwaru, zhotovení softwaru pro řízení a správu infrastruktury a uvedení celého projektu do reálného provozu.

Summary

The thesis is concerned with the problems of practical implementation of the thin clients infrastructure for the operation of information systems and application software in the setting of a modern hospital. The theoretical part gives an overview of the typical options of solution. The practical part describes the ICT contemporary state in the organisation, gives proposal of compliant inovative solutions and solves the main realization, which consists of the choice of hardware, of the software development for the infrastructure running and maintenance, and launches the project into real operation.

Klíčová slova

Tenký klient, terminálový server, vzdálená plocha, RDP protokol, print server, PXE server

Keywords

Thin client, terminal server, remote desktop, RDP protocol, print server, PXE server

Obsah

Seznam obrázků

Seznam tabulek

Seznam použitých zkratek

AD – Active Directory

CAL - Client Access License

GP – Group Policy

GUI - Graphical User Interface

ICA - Independent Computing Architecture

ICT - Information and Communication Technologies

LAN – Local Area Network

OEM – Original Equipment Manufacture

PCoIP – PC over IP Protocol

PXE - Preboot Execution Environment

RDP – Remote Desktop Protocol

ROI - Return on Investment

SA – Software Assurance

TCO - Total Cost of Ownership

TCP - Transmission Control Protocol

UDP - User Datagram Protocol

VDA – Virtual Desktop Access

VDI – Virtual Desktop Infrastructure

VLAN - Virtual Local Area Network

VNC - Virtual Network Computing

WAN – Wide Area Network

WMI - Windows Management Instrumentation

XPS - XML Paper Specification

1 Úvod

Ve své diplomové práci se budu zabývat problematikou praktické realizace infrastruktury tenkých klientů, primárně určené pro provoz klientské části informačních systémů a dalšího aplikačního software. V současné době jde o aktuální téma, často skloňované v souvislosti s infrastrukturou virtuálních desktopů (VDI, Virtual Desktop Infrastructure). Jeho význam posílil díky ukončení oficiální podpory operačního systému Windows XP v měsíci dubnu 2014, který byl nebo stále je v mnoha organizacích četně využíván, obvykle na standardních desktopech. Přestože tato událost neznamená ukončení provozu systému, představuje zejména potenciální bezpečnostní riziko, neboť společnost Microsoft nebude nadále vydávat opravné balíky odstraňující chyby v operačním systému, což může v důsledku vést k nežádoucím bezpečnostním incidentům, které mohou mít zejména ve firemním prostředí fatální následky. Díky absenci rozšiřujících aktualizací nelze ani očekávat, že bude možné v tomto systému nadále provozovat některá moderní softwarová řešení. Provozovatelé informačních systémů a technologií tak stojí před rozhodnutím, zda zastaralou infrastrukturu, často tvořenou standardními desktopy právě se systémem Windows XP, konzervativně nahradit zakoupením nových strojů s aktuální verzí Windows, nebo zvolit alternativu v podobě VDI či jiné technologie odpovídající jejich požadavkům.

V teoretické části práce budou stručně charakterizována vybraná infrastrukturní řešení, se kterými se lze ve firemním prostředí běžně setkat. Půjde o standardní desktopovou infrastrukturu tvořenou osobními počítači, infrastrukturu pro prezentační virtualizaci, známou například jako terminálové služby, a VDI. Uveden bude také přehled souvisejících využívaných komunikačních protokolů. Aby bylo možné provést srovnání z hlediska finančních nákladů, budou vysvětleny hodnotící ukazatele TCO (Total Cost of Ownership) a ROI (Return on Investment), vyjadřující celkové finanční náklady, resp. návratnost investice.

Klíčová bude především praktická část, která se bude zabývat reálnou implementací infrastruktury tenkých klientů v moderním zdravotnickém zařízení, Rehabilitační nemocnici Beroun. Výběr technologie bude učiněn na základě šetření současného stavu

ICT prostředí v organizaci, dle potřeb a požadavků managementu na jeho inovace a nákladových kalkulací pro stanovený životní cyklus.

Výstupem a přínosem práce bude ekonomicky atraktivní a funkční řešení uvedené do reálného provozu. K jeho realizaci budou uplatněny nové poznatky získané při studiu na ČZU, dlouhodobé zkušenosti s provozem terminálových služeb pod operačními systémy Windows Server a preference efektivních a nízkonákladových řešení na bázi opensource operačních systémů Linux. Bude také vhodně využito výsledků mé předchozí bakalářské práce na téma „Řízení vzdálených aplikací v doméně MS Windows“, která se zabývala vývojem softwarových nástrojů pro zvýšení komfortu a zajištění bezproblémového rutinního provozu vzdálených aplikací RemoteApp v doménovém prostředí Microsoft Windows s výrazným pohybem uživatelů.[1]

Pro zhotovení software budou použity moderní programovací platformy Java, PHP nebo C#. Jako úložiště dat databáze MS SQL 2008 Express.

[1] KUKLA, Zdeněk. Řízení vzdálených aplikací v doméně MS Windows [online]. 2013 [cit. 2014-11-13]. Bakalářská práce. Vysoká škola finanční a správní. Vedoucí práce Jan Lánský.
Dostupné z: http://is.vsfs.cz/th/22360/vsfs_b

2 Cíl práce a metodika

Hlavním cílem této diplomové práce je navrhnout dle požadavků, zrealizovat a uvést do provozu v Rehabilitační nemocnici Beroun infrastrukturu tenkých klientů. Tím se rozumí vybrat a nainstalovat terminálové servery, tenké klienty, PXE server a vytvořit další nezbytný software pro vlastní provoz a správu infrastruktury.

Metodika pro dosažení cíle spočívá nejprve ve studiu dostupných odborných informačních zdrojů, často v cizím jazyce, které jsou podkladem nejen pro teoretický přehled problematiky. Praktická část bude zahájena analýzou současného stavu ICT prostředí v organizaci, zpracováním požadavků managementu, na jejichž základě bude navrženo konkrétní řešení k realizaci, včetně orientačních srovnávacích finančních kalkulací několika dalších variant.

Vlastní realizace proběhne ve třech etapách:

1) Rapidní vývoj prvních verzí klíčových softwarových součástí, zajištění testovacích tenkých klientů, jejich instalace a nasazení do pilotního provozu na vybraném pracovišti nemocnice.

2) Průběžné ladění a odstraňování identifikovaných chyb v software, konfiguraci operačních systémů a přizpůsobení řešení na základě reakcí a podnětů od uživatelů. V okamžiku dosažení rutinní použitelnosti dokončení zbývajících softwarových komponent.

3) Zprovoznění infrastruktury v požadovaném rozsahu.

Dosažené výsledky budou vyhodnoceny v závěru práce v kapitole 6 – Zhodnocení výsledků a doporučení.

3 Přehled řešené problematiky

Infrastrukturu lze pro potřeby této diplomové práce definovat jako soubor hardwarových a softwarových prostředků pro zpřístupnění informačních systémů a dalšího software jejich uživatelům. Teoreticky jednotlivá vybraná infrastrukturní řešení vychází z podstaty výpočetního modelu, který je ucelenou představou o tom, kde jsou aplikace uchovávány jako programy a kde skutečně běží, zda (a jak) jsou aplikace rozděleny na části, jak tyto části vzájemně spolupracují, kde a jak se uchovávají a zpracovávají data, kde se nachází uživatel, kdy, jak a jakým způsobem komunikuje se svými aplikacemi.[2] Řeší se tak především otázka úplné centralizace, úplné decentralizace a hledání toho správného kompromisu mezi nimi.

Pozornost bude podrobněji věnována následujícím řešením:

- standardní desktopová infrastruktura,
- infrastruktura pro prezentační virtualizaci,
- infrastruktura virtuálních desktopů (VDI).

3.1 Standardní desktopová infrastruktura

Představuje jednotlivé fyzické osobní počítače, které mohou fungovat samostatně nebo být součástí podnikové sítě. Na každém z nich běží operační systém, v jehož prostředí uživatel přímo pracuje s často lokálně nainstalovanými aplikacemi a kde může mít uložena svá data. Z tohoto pohledu se jedná o jednoduchý decentralizovaný přístup, kdy instalace, aktualizace či správa operačního systému a aplikací probíhá na každém jednotlivém stroji zvlášť, a to i s přihlédnutím k faktu, že existují nástroje pro usnadnění těchto servisních činností. Z hlediska výkonu a jeho využití v čase jsou tyto stanice mnohdy předimenzované vzhledem k reálné potřebě.

Vybrané potenciální výhody řešení:

- výpočetní výkon hardwaru vyhrazený většinou jedinému uživateli,

[2] PETERKA, Jiří. Počítačové sítě, verze 3.0. [online]. [cit. 2014-11-13].
Dostupné z: http://www.earchiv.cz/l212/slide.php3?&l=12&me=2

- bezproblémová práce s nejrůznějšími lokálními periferiemi, které jsou aplikacím přímo přístupné,
- obvykle výhodnější podmínky pro nákup licence operačního systému Windows společně s novým počítačem (OEM licence).

Vybrané potenciální nevýhody řešení:

- instalace, aktualizace či správa operačního systému a aplikací na každém jednotlivém stroji zvlášť,
- bezpečnostní riziko spočívající v možném úniku či ztrátě dat při zcizení zařízení,
- vyšší spotřeba elektrické energie (desítky wattů),
- větší rozměry, častá přítomnost pohyblivých součástí (pevné disky, ventilátory procesoru a zdroje) vyžadující náročnější údržbu a vedoucí k častějším servisním zásahům.

3.2 Infrastruktura pro prezentační virtualizaci

Prezentační virtualizace představuje návrat ke klasickému výpočetnímu modelu host/terminal, kde oproti prvotnímu konceptu došlo k odstranění uživatelsky nepříjemného textového prostředí zavedením grafického režimu při rozumných nárocích na přenosovou kapacitu. Pojem virtualizace je zde užíván v souvislosti s představou, kdy „virtualizací označujeme techniky a postupy vedoucí ke skrytí skutečných HW prostředků před uživateli.“[3]

Například v pojetí Microsoftu jde o terminálové služby, nově nazývané službou Vzdálená plocha (Remote Desktop Services). Hostitelem je zde Terminálový server, což je server hostující programy, založené na systému Windows, nebo úplnou plochu systému Windows pro klienty služby Vzdálená plocha. Uživatelé se mohou připojit k terminálovému serveru a spustit programy, pracovat se soubory nebo používat další prostředky daného serveru.[4]

---

[3] FRIČ, Michal. Virtualizační technologie. [online]. [cit. 2014-11-13].
Dostupné z: http://hippo.feld.cvut.cz/vrbata/gopas/virtualizace-uvod.pdf

[4] MICROSOFT. Hostitel relací vzdálené plochy (hostitel relací VP). [online]. [cit. 2014-11-13].
Dostupné z: http://technet.microsoft.com/cs-cz/library/cc742822

V roli terminálu se objevují zařízení různého typu - osobní počítače, notebooky, smartphony, často však tenký klient, jehož jediným úkolem je komunikace s hostitelským serverem a lokální interpretace vzdáleného grafického prostředí. Výkonnostní nároky na hardware tenkého klienta jsou minimální, neboť prakticky veškerou práci vykonává terminálový server. Díky tomu bývá tenký klient vybaven naprosto minimalisticky a musí být schopen pouze provozovat operační systém s aplikací pro vzdálené připojení.

Infrastrukturou pro prezentační virtualizaci se rozumí spojení jednoho či více hostitelů (terminálových serverů) a terminálů (např. tenkých klientů), které zpřístupní uživatelům vzdálené pracovní prostředí, ať už v rámci lokální sítě LAN, nebo rozlehlé sítě WAN. Z hlediska výkonu celého řešení lze oproti standardním desktopům při vhodně dimenzované konfiguraci serverů a provozování nepříliš výpočetně náročných aplikací dosáhnout jejich rychlejší odezvy, díky možnému přístupu k vysokému výpočetnímu výkonu hostitelských serverů, který je sdílením mezi více uživateli v čase zároveň efektivněji využit.

Vybrané potenciální výhody řešení:

- velmi nízká spotřeba elektrické energie tenkých klientů (jednotky wattů),
- výrazně efektivnější instalace, aktualizace či správa operačního systému a aplikací na jednom, či maximálně několika serverech,
- zvýšení zabezpečení důležitých dat díky jejich přesunu na servery, obvykle umístěné v zabezpečeném datacentru, s ideálními provozními podmínkami,
- nízká cena tenkého klienta, malé rozměry, atraktivní design, obvykle bez přítomnosti pohyblivých součástí (pevné disky, ventilátory procesoru a zdroje).

Vybrané potenciální nevýhody řešení:

- počáteční investice do serverové infrastruktury,
- možné problémy s přesměrováním některých lokálních periferií do vzdáleného prostředí,
- možné problémy s víceinstančním provozem některých aplikací, zejména z důvodu vyžadované exkluzivity použití některých prostředků na serveru.

3.3 Infrastruktura virtuálních desktopů (VDI)

Popularita modelu VDI, zejména v poslední době, značně roste. Za hlavní důvody se marketingově často zdůrazňují redukce nákladů na správu a provoz takové infrastruktury, zvýšené zabezpečení, zpřístupnění standardního pracovního prostředí uživateli rychle, prakticky kdekoli a na zařízeních různého typu - osobních počítačích, noteboocích, tenkých klientech či smartphonech. Problematika VDI je značně rozsáhlým tématem, přičemž pro potřeby této diplomové práce budou vysvětleny jen základní principy.

V případě Virtual Desktop Infrastructure jde o centralizovaný model, kdy jsou jednotlivé virtuální desktopy (operační systém + aplikace + uživatelská data) provozovány na serverové infrastruktuře v datacentru a klientovi jsou doručována opět především obrazová data, podobně jako u prezentační virtualizace. Z pohledu běžného uživatele tak není mezi těmito technologiemi zcela zřetelný rozdíl, který je však zásadní. Zatímco u terminálových služeb sdílí uživatelé, byť prakticky izolovaně, jediný operační systém serveru, u VDI mají pro sebe k dispozici vlastní separovaný operační systém, stejně jako na fyzických desktopech. Podle požadavků organizace se volí z následujících modelů přidělování:[5]

- ***trvalý desktop*** - je vázán na jednoho uživatele, přičemž stejný desktop je uživateli k dispozici pokaždé, když se přihlásí. Model vyžaduje vysokou kapacitu centrálního datového úložiště a je vhodný pouze pro organizace s několika uživateli,
- ***dočasný desktop*** - uživateli je po přihlášení k dispozici nový desktop výchozí konfigurace, vygenerovaný ze standardního obrazu, který je následně pokaždé přizpůsoben o specifická nastavení, aplikace a data uložená v uživatelském profilu. To nevyžaduje tak velkou kapacitu úložiště jako v předchozím případě,
- ***trvalý klon desktopu*** – je personalizovaný klon, vytvořený při prvním přihlášení uživatele, který jej následně používá při každém dalším přihlášení.

[5] RUEST, Danielle a Nelson RUEST. Virtualization, A Beginner´s Guide. The McGraw-Hill Companies, 2009, s. 248-249. ISBN 978-0-07-161402-3.

Vybrané potenciální výhody řešení:

- velmi nízká spotřeba elektrické energie tenkých klientů (jednotky wattů),
- výrazně efektivnější instalace, aktualizace či správa operačního systému a aplikací udržováním jednoho či více standardních obrazů výchozích virtuálních desktopů,
- zvýšení zabezpečení důležitých dat díky jejich přesunu na servery, obvykle umístěné v zabezpečeném datacentru s ideálními provozními podmínkami,
- nízká cena tenkého klienta, malé rozměry, atraktivní design, obvykle bez přítomnosti pohyblivých součástí (pevné disky, ventilátory procesoru a zdroje).

Vybrané potenciální nevýhody řešení:

- počáteční investice do serverové infrastruktury,
- vyšší licenční poplatky (licencování infrastruktury + Microsoft VDA nebo SA).

3.4 Přehled komunikačních protokolů

Terminálové služby nebo VDI využívají pro komunikaci mezi serverem a klientem různých komunikačních protokolů, které jsou obvykle dané výrobcem použité technologie. Nejčastěji jde o **RDP** (Remote Desktop Protocol) firmy Microsoft, **PCoIP** (PC over IP) firmy Teradici a **ICA** (Independent Computing Architecture) firmy Citrix.

3.4.1 RDP (Remote Desktop Protocol)

Microsoft Remote Desktop Protocol (RDP) poskytuje vzdálený displej a vstupní funkce pro aplikace, běžící na serveru se systémem Windows, přes síťové připojení. RDP je navržen tak, aby podporoval různé typy síťových topologií a LAN protokolů.[6] Klient komunikuje se serverem obvykle na TCP portu 3389. Základní vlastnosti protokolu verze 6.1 a vyšší jsou:

- barevná hloubka zobrazení 8, 15, 16, 24 a 32 bitů,
- 128 bitové šifrování komunikace algoritmem RC4 nebo TLS 1.0,
- možnost přesměrování tiskáren, zvuku, diskových jednotek, I/O portů a schránky,
- podpora vícemonitorového zobrazení,

[6] MICROSOFT. Remote Desktop Protocol [online]. [cit. 2014-11-13].
Dostupné z: https://msdn.microsoft.com/en-us/library/aa383015

- podpora vzdálených aplikací RemoteApp,
- podpora Windows Aero a technologie ClearType,
- dokonalejší adaptace klientů na aktuální šíři přenosového pásma.

3.4.2 PCoIP (PC over IP)

Protokol Teradici PCoIP je inovativní technologie pro vzdálené displeje, která umožňuje umístit desktop uživatele, aplikace a data do datového centra, čímž eliminuje potřebu použití tradičních pracovních stanic. PCoIP komunikuje přes transportní protokol UDP, poskytuje vysoké rozlišení, výkonnou 3D grafiku a bezproblémovou interoperabilitu USB periferií přes lokální LAN nebo WAN síť s vysokou latencí. V závislosti na dostupné šířce pásma adaptivně přizpůsobuje kódování a kompresi obrazových snímků.
Protokol PCoIP je také integrován přímo v hardwarových čipech firmy Teradici, což přináší vysoký výkon i bezpečnost řešení v takto vybavených zařízeních jakou jsou PCoIP Zero Client nebo hardwarový akcelerátor APEX 2800, určený pro servery. Softwarovou implementací je například řešení VMware Horizon View.[7]

3.4.3 ICA (Independent Computing Architecture)

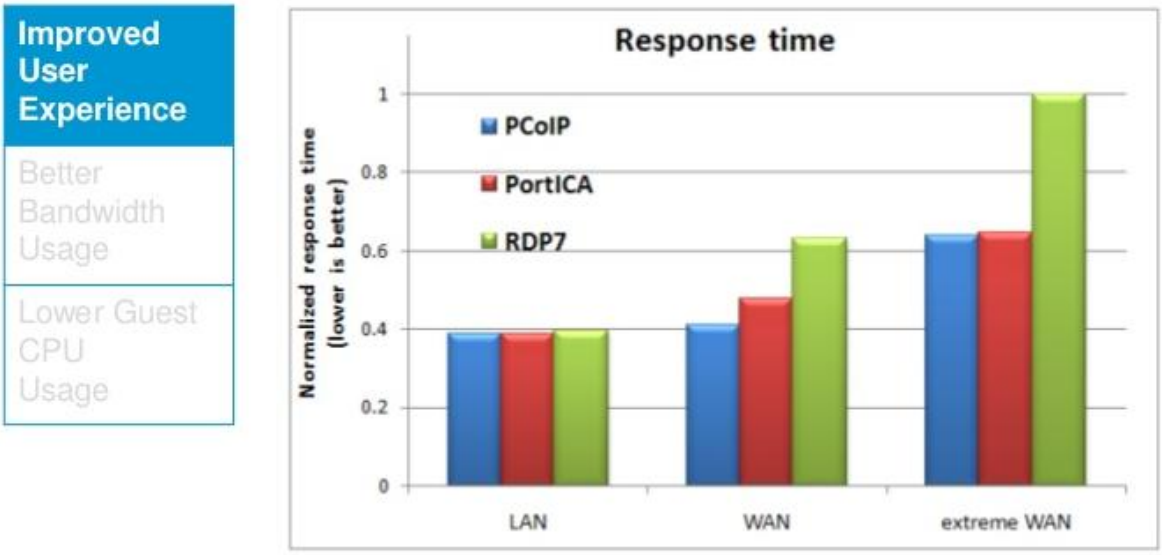
ICA je proprietární protokol navržený firmou Citrix Systems. Je nezávislý na konkrétní platformě nebo transportním protokolu. Může tedy běžet pod operačními systémy jako jsou Windows, Linux nebo iOS a je schopen komunikace přes standardní síťové protokoly jako jsou TCP/IP, NetBEUI, IPX/SPX, nebo PPP. Protokol ICA pracuje na prezentační vrstvě OSI modelu. Koncepčně je podobný protokolu X-Windows známém ze systémů UNIX. Klient komunikuje se serverem obvykle na TCP portu 1494. Každá relace poté používá další porty pro zpětnou komunikaci mezi serverem a klientem. V rámci protokolu ICA se využívají virtuální kanály pro zapouzdření dalších funkcí jako jsou například přesměrování zvuku, USB periferií, schránky, diskových jednotek nebo tiskáren.[8]

---

[7] TERADICI.COM. Teradici PCoIP Solutions: About PCoIP technology. [online]. [cit. 2014-11-13]. Dostupné z: http://www.teradici.com/docs/default-source/resources/brochures/teradici-brochure-120817-web-2.pdf

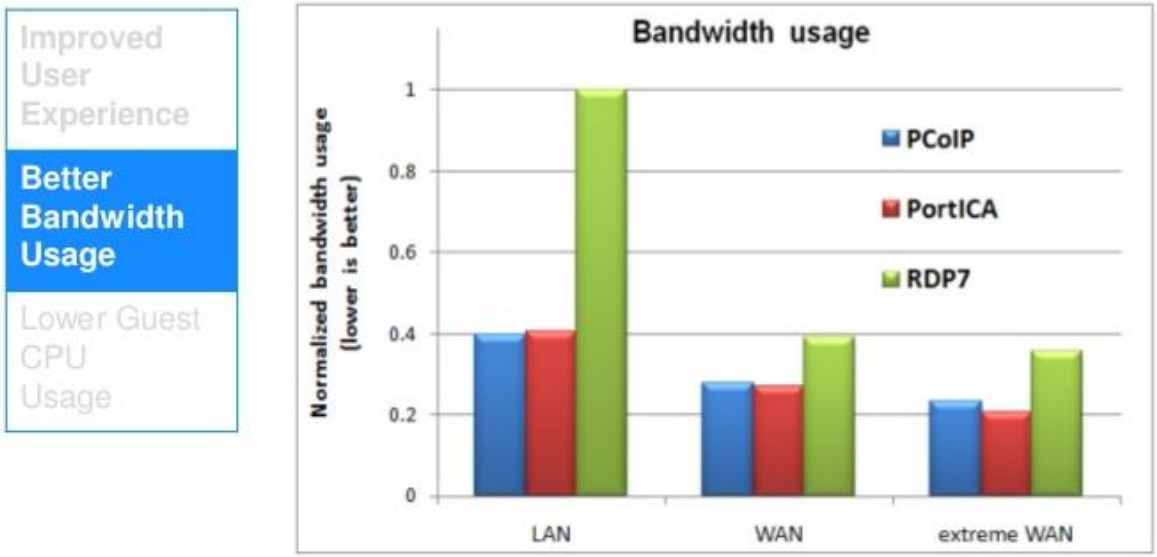
[8] SERWAN, Pawel. Dive into Citrix ICA protocol – Part1 [online]. [cit. 2014-11-13]. Dostupné z: https://pawelserwan.wordpress.com/2014/09/24/dive-into-citrix-ica-protocol-part1

3.4.4 Benchmark komunikačních protokolů



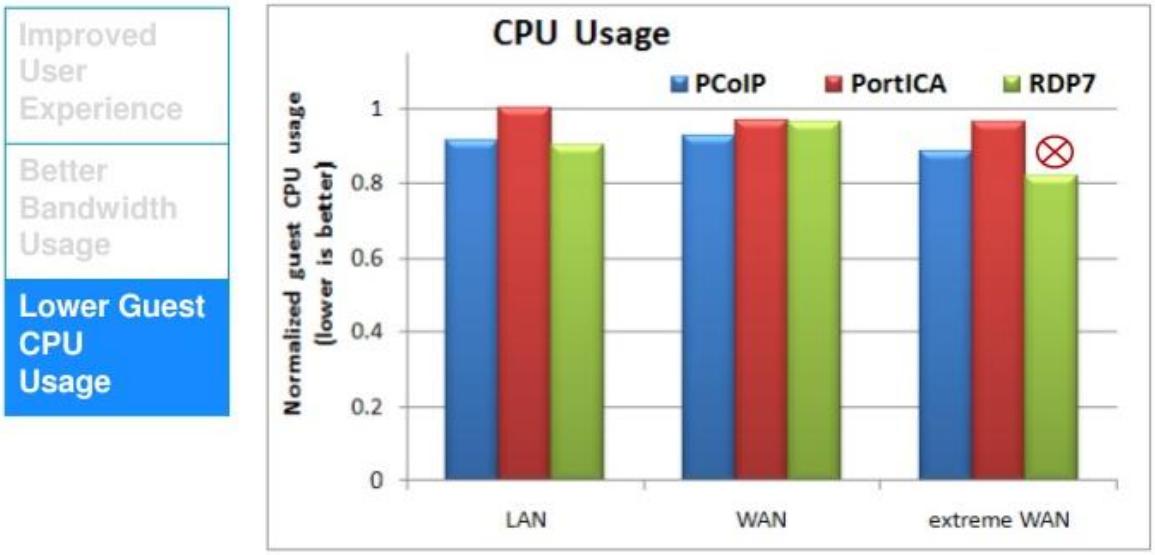
Obrázek 1: Normalizovaná doba odezvy

Zdroj: http://image.slidesharecdn.com/euc1987-pcoip-improvements-110911145716-phpapp02/95/vmware-view-pcoip-performance-best-practices-33-728.jpg



Obrázek 2: Normalizované využití šířky pásma

Zdroj: http://image.slidesharecdn.com/euc1987-pcoip-improvements-110911145716-phpapp02/95/vmware-view-pcoip-performance-best-practices-34-728.jpg



Obrázek 3: Normalizované využití hostitelského procesoru
Zdroj: http://image.slidesharecdn.com/euc1987-pcoip-improvements-110911145716-phpapp02/95/vmware-view-pcoip-performance-best-practices-35-728.jpg

Parametry experimentu[9]:

- **LAN**: propustnost 100 Mbps, doba odezvy 1 ms,
- **WAN**: propustnost 2 Mbps, doba odezvy 100 ms,
- **extreme WAN**: propustnost 300 kbps, doba odezvy 100 ms

- **klient**: 32-bit WinXP SP3, 1 CPU, 768 MB RAM, rozlišení 1152x864
- **server**: 32-bit Win7, 1 CPU, 1 GB RAM, rozlišení 1152x864

- **protokoly**: PCoIP (VMware View 5.0), ICA (XenDesktop 5.0), RDP 7.0

Z výsledku uvedených testů je zřejmé, že výkon protokolů PCoIP a ICA je téměř srovnatelný, zatímco protokol RDP dosahuje nejhorších výsledků na extrémní síti WAN. Z praktické osobní zkušenosti lze potvrdit také výsledek využití šířky pásma na síti LAN, kdy je protokol RDP schopen například při přenosu videa přenosové pásmo až paralyzovat.

[9] VMWARE. VMware View PC-over-IP Performance and Best Practices [online]. [cit. 2014-11-13]. Dostupné z: http://image.slidesharecdn.com/euc1987-pcoip-improvements-110911145716-phpapp02/95/vmware-view-pcoip-performance-best-practices-26-728.jpg

3.6 Kalkulace finančních nákladů

Pro vyjádření finančních nákladů, které bude potřeba na určitý projekt alokovat, se obvykle využívá ukazatele **TCO** (Total Cost of Ownership) – celkové náklady vlastnictví. Jeho výsledná hodnota zahrnuje veškeré náklady, které musí provozovatel za určité období (v průběhu životního cyklu) vynaložit. Jedná se nejen o pořizovací, ale také o provozní náklady. Při sestavování TCO pro delší časový horizont je třeba zohlednit časovou hodnotu peněz započtením diskontního faktoru.

Mezi pořizovací náklady patří:

- nákup hardware,
- nákup software, případně rozšiřujících licencí,
- instalace a konfigurace.

Mezi provozní náklady patří:

- údržba a servis,
- výdaje na energie,
- technická podpora a aktualizace.

Dalším z ukazatelů je **ROI** (Return on Investment) – návratnost investice. „Jedná se o hodnotu, na základě které je možné zjistit, jak rychle se prostředky vynaložené na projekt vrátí společnosti zpět. Pokud je hodnota ROI větší než 1 nebo 100 procent, pak to znamená, že za měřené období (typicky v IT se ROI počítá pro období jednoho roku či tří let) se investice do projektu nejen vrátila, ale již generuje nové prostředky, popřípadě šetří prostředky oproti původnímu stavu (tj. kdyby k realizaci projektu nedošlo).“[10]

[10] ŠVÍK, Martin. ROI, TCO a NPV: Svatá trojice. [online]. [cit. 2014-11-13].
Dostupné z: http://businessworld.cz/it-strategie/roi-tco-a-npv-svata-trojice-5303

4 Analytická část

Praktická část této práce je cílena do prostředí moderní Rehabilitační nemocnice Beroun, která změnila během privatizace středočeských nemocnic v roce 2007 společně s Nemocnicí Hořovice vlastníka. Od té doby zde postupně dochází k realizaci naplánovaného modelu, spočívajícího ve funkčním propojení obou zdravotnických zařízení do smysluplného celku, kde Nemocnice Hořovice poskytuje především multioborovou akutní péči a Rehabilitační nemocnice Beroun jednodenní výkony a léčebnou rehabilitaci s podporou oddělení vnitřního lékařství. O pacienty nejen v regionu je tímto komplexně postaráno jak během akutního stavu, tak později, po jeho zvládnutí.

Je nezbytné, aby pro poskytování služeb vysoké úrovně, byl provoz těchto zdravotnických zařízení vhodně podporován také moderními a smysluplně nasazenými informačními systémy a technologiemi.

4.1 Cíle a aktuální požadavky managementu v ICT

Cílem managementu nemocnice v oblasti ICT je zefektivnit, ztransparentnit a zvýšit spolehlivost rutinního provozu, dbát na adekvátní zabezpečení dat a používat moderní technologie a software. Vzhledem k aktuálnímu stáří některých technologií, ukončené podpoře operačního systému Windows XP s četným výskytem, ale také výskytu nepříliš flexibilní desktopové infrastruktury jsou definovány tyto požadavky:

- nahradit operační systém Windows XP u uživatelů a zajistit, aby jejich pracovní prostředí bylo provozováno na podporovaných verzích operačních systémů společnosti Microsoft,
- obměnit zastaralé pracovní stanice (100x),
- obměnit zastaralé terminálové servery (2x) a zajistit jeden redundantní,
- usnadnit provoz a správu infrastruktury (=>snížit výdaje na správu infrastruktury),
- snížit spotřebu elektrické energie,
- sbírat statistické údaje z provozu jednotlivých pracovních stanic a zvýšit tak přehled o využití ICT,
- snížit riziko potenciálního úniku a zneužití dat zcizením zařízení,

- vyřešit úplnou blokaci použití periferií – např. flash disky, externí pevné disky a další zařízení připojitelná typicky jako USB Mass Storage,
- zefektivnit podporu uživatelů.

To vše s minimálními dalšími investicemi a bez omezení provozu.

4.2 Současný stav ICT prostředí

Pro minimalizaci rizik neúspěchu, spojeného s inovací nebo zaváděním informačních systémů či technologií, je zapotřebí vždy nejprve popsat a analyzovat jejich současný stav. Posuzují se zejména tyto oblasti:

- vybavení pracovními stanicemi, tiskárnami, servery...,
- dostupnost a stav počítačové sítě a ostatní telekomunikační infrastruktury,
- používané operační, informační systémy a aplikační software,
- klíčové vlastnosti infrastruktury jako celku,
- skupiny uživatelů, charakteristika jejich práce s ICT, bezpečnostní politika,
- interní zajištění správy ICT a podpory uživatelů,
- rozsah servisní podpory u externích dodavatelů, stavy záručních lhůt na klíčový hardware apod.

Popis ICT Rehabilitační nemocnice Beroun bude proveden ve zjednodušeném rozsahu odpovídajícímu zaměření této práce.

Informační systémy používané společně v obou organizacích jsou provozovány na serverech, které jsou fyzicky umístěny v Nemocnici Hořovice (NH). Mezi oběma subjekty je k dispozici zálohované datové propojení o fullduplexní kapacitě 50 Mbps, což však nestačí k tomu, aby bylo možné v Rehabilitační nemocnici Beroun (RNB) lokálně provozovat aplikace informačních systémů s přijatelnou odezvou. Z toho důvodu jsou poskytovány prostřednictvím terminálové služby, kde terminálové servery na lokální straně sítě (NH) hostují programy informačních systémů pro klienty na vzdálené straně sítě (RNB). Toto řešení představuje pro síť WAN výrazně nižší zátěž, a naopak umožňuje dosáhnout vysokého výkonu díky vysokorychlostnímu propojení serverů v rámci lokální sítě LAN na straně NH. Stav hardwaru terminálových serverů již vyžaduje upgrade. Dva

ze strojů výkonnostně zaostávají a jsou v nepřetržitém provozu přes pět let, tedy na konci svého životního cyklu. Tyto servery nejsou virtualizovány.

Uživatelé pracují s běžnými osobními počítači s operačním systémem Windows, kde pro přístup k programům využívají většinou vzdálené plochy nebo vzdálené aplikace RemoteApp. Celkový počet pracovních stanic je 180, přičemž zastoupení verzí operačních systémů je v poměru Windows XP - 52% (93x), Windows Vista - 12% (22x), Windows 7 – 36% (65x). Výkon stanic je pro dané využití vyhovují a nevyžaduje nutně změnu, avšak záruční lhůta a servisní podpora typu NBD (Next Business Day) je zejména u strojů s Windows XP již u konce. Tam, kde se využívá terminálových služeb, je zakoupena licence VP CAL vázaná na zařízení. Problémem je ukončená podpora systému Windows XP v dubnu 2014.

Pro tiskové služby je určen centrální tiskový server, provozovaný na virtuálním serveru, s operačním systémem Windows Server 2008 R2. Software zajišťující tisk byl vytvořen pro organizaci na míru. Všechna pracoviště jsou vybavena moderními tiskárnami s připojením na ethernet, ať už prostřednictvím pevné sítě LAN nebo pomocí bezdrátové Wi-Fi sítě, která je v celém areálu nemocnice k dispozici.

Klíčový nemocniční informační systém je zhotoven ve vývojovém prostředí Delphi a je možné jej provozovat pouze pod operačním systémem Windows. Jedná se o sadu výpočetně nenáročných programů kancelářského typu, které však vyžadují rychlé a stabilní spojení s databázovým serverem. Dále se využívá většinou webových aplikací nebo programů zhotovených v jazyce JAVA. Správa uživatelů probíhá pomocí služby Active Directory, což umožňuje zejména jejich bezpečné ověřování v lokální doméně, centrální správu, jednotné přihlašování do aplikací pomocí SSO (Single-Sign-On), řízení přístupu k datům na bázi skupin uživatelů, nebo konfiguraci prostředí pracovních stanic pomocí zásad skupiny (Group policy).

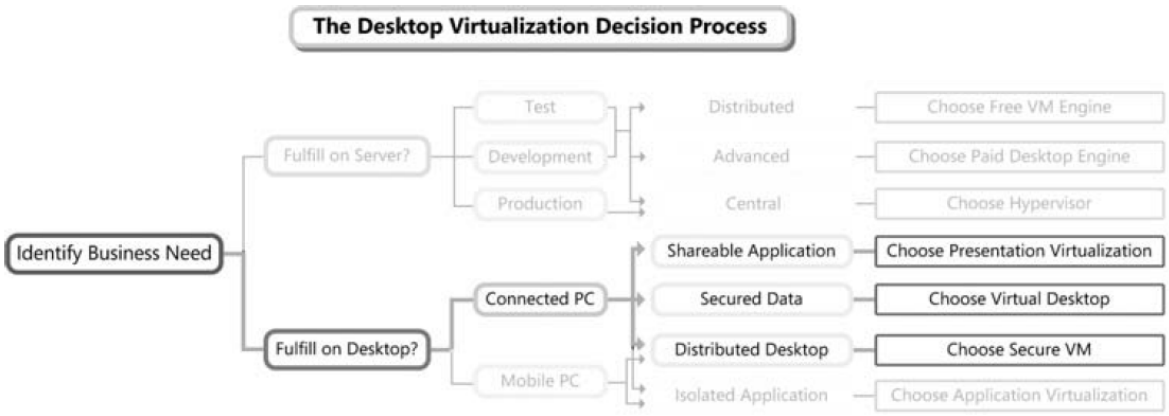
4.3 Možnosti řešení

Primárním úkolem, který vyplývá z požadavků managementu organizace, je obměna části klientských stanic. K tomu se nabízí tyto možné varianty řešení:

- konzervativní náhrada osobních počítačů novými stroji s podporovanou verzí operačního systému Windows,
- nasazení tenkých klientů v režimu VDI, jako plnohodnotných virtuálních desktopů s operačním systémem Windows,
- využití místních zkušeností s provozem terminálových služeb a experimentální nasazení operačního systému Linux na tenkých klientech, s pracovním prostředím Windows na serverech.

Konzervativní nahrazení zastaralé techniky novou bez dalších změn sice nepředstavuje prakticky žádné riziko, zároveň však nedokáže naplnit požadavky organizace, zejména ve vztahu k usnadnění provozu a správy infrastruktury, či snížení provozních nákladů, kdy téměř jistě nedojde k poklesu výdajů na správu či spotřebu elektrické energie.

Toho lze dosáhnout v dalších dvou případech – u virtuálních desktopů a prezentační virtualizace, kde zjednodušení a zlevnění správy infrastruktury vychází z centralizovaného přístupu, nižší spotřeba energie pak především z technologických vlastností tenkých klientů. K rozhodnutí, kterým směrem se vydat, vede především správná identifikace potřeb konkrétní organizace. Napovědět může následující rozhodovací diagram:



Obrázek 4: Rozhodovací proces volby desktopové virtualizace

Zdroj: RUEST, Danielle a Nelson RUEST. Virtualization, A Beginner´s Guide. The McGraw-Hill Companies, 2009, s. 264. ISBN 978-0-07-161402-3

V organizaci se již prezentační virtualizace dlouhodobě využívá, především z uvedených infrastrukturních důvodů. Uživatelé pracují s jednoduchými sdílenými aplikacemi pro operační systém Windows, které bez problémů fungují v terminálovém režimu. Zavedení VDI by v tomto směru zjevně nebylo přínosem. Rozhodnutím bude zřejmě snaha vytěžit maximum z dosavadního řešení a obohatit jej o moderní přístup, s jehož pomocí bude možné splnit požadavky. Pro dokreslení celé situace z ekonomického hlediska následuje orientační vyjádření investičních a provozních nákladů v pětiletém životním cyklu.

4.4 Orientační výpočet TCO v pětiletém životním cyklu

Pro ocenění jednotlivých variant řešení bude vyjádřena hodnota TCO (Total Cost of Ownership) – celkové náklady na vlastnictví, jejíž význam byl podrobněji vysvětlen v teoretické části práce. Vyčísleny budou především náklady na:

- pořízení hardware a software,
- spotřebu elektrické energie (níže uvedené údaje o spotřebě koncových zařízení jsou zaokrouhleným průměrem z hodinového reálného měření při typickém použití),
- servisní činnosti - fyzická profylaxe, softwarové práce (revize a úkony vedoucí k udržení bezproblémového stavu).

Organizace má zjištěno, že na místech, kde předpokládá obnovu techniky, jsou zařízení v provozu denně průměrně 12 hodin, a to včetně dní pracovního volna. Za elektrickou energii přitom vydá orientačně 3,50 Kč bez DPH za jednu kWh. Mzdové náklady na technika informačních technologií zde činí přibližně 250 Kč za hodinu práce. Předpokládá se, že servisním činnostem na jedné pracovní stanici dosud věnuje asi 2 hodiny ročně. V případě použití tenkých klientů organizace odhaduje snížení této dotace na maximálně 30 minut ročně, když očekává pouze provádění zjednodušené fyzické profylaxe.

Další vstupní údaje pro kalkulaci jsou:

- 100 pracovních stanic určených k výměně,
- pětiletý životní cyklus,
- zachování modelu prezentační virtualizace (mimo ukázky řešení VDI),
- výměna dvou terminálových serverů a pořízení jednoho záložního pro zajištění vysoké dostupnosti.

Kalkulace nezahrnuje:

- cenu licencí VP CAL vázané na zařízení, které má organizace zakoupeny a může je dále použít pro VDI i terminálové služby,
- ostatní použitelné části infrastruktury (datové úložiště, tiskový server...),
- cenu instalačních prací terminálových, resp. VDI serverů (předpokládá se přibližně stejná cena),
- cenu dokončovacích instalačních prací na desktopech,
- cenu za zhotovení software pro tenké klienty, který je předmětem další části této práce.

Ceny uvedené v Kč, bez daně z přidané hodnoty, k datu 15.1.2014 poskytla Rehabilitační nemocnice Beroun a vychází z tehdy předložených nabídek dodavatelů. Je třeba zdůraznit, že výslednou cenu nelze vzhledem k nezapočtení veškerých potenciálních vstupních nákladů považovat za úplnou. Smyslem je ukázat, kde u jednotlivých řešení dochází k podstatným rozdílům v nákladech.

	2014			2015	2016	2017	2018
Pořizovací náklady	Počet	Cena	Celkem				
Osobní počítač*	100	11850	1185000				
Terminal server pro 50 stanic**	2	105000	210000				
Redundantní terminal server pro 50 stanic**	1	105000	105000				
Provozní náklady							
Spotřeba elektrické energie - klienti***	100	765	76500	76500	76500	76500	76500
Spotřeba elektrické energie - server****	3	6130	18390	18390	18390	18390	18390
Servisní činnosti	100	500	50000	50000	50000	50000	50000
Náklady celkem v letech			**1644890**	**144890**	**144890**	**144890**	**144890**
Celkem náklady za 5 let = 2 224 450,- Kč							

Tabulka 1: TCO - Osobní počítače

Zdroj: Vlastní zpracování

* Dell OptiPlex 3020 SFF (CPU Intel Pentium G3220, 4 GB RAM, 500GB SATA HDD, 8X DVD+/-RW, klávesnice, myš), předinstalovaný Windows 7 Professional, záruka 5 let ProSupport a Next Business Day On-Site;

** Dell PowerEdge R320, 1U (CPU Intel Xeon E5-2430, 32 GB RAM, 3x HDD 600 GB SAS 15k - RAID 1 & hotspare), Windows 2008 R2, záruka 5 let ProSupport a 4hr Mission Critical;

*** 50W, 12 hodin denně, 365 dní v roce; **** 200W, 24 hodin denně, 365 dní v roce.

	2014			2015	2016	2017	2018
Pořizovací náklady	Počet	Cena	Celkem				
Tenký klient*	100	3750	375000				
Server pro 50 stanic**	2	127000	254000				
Redundantní server pro 50 stanic**	1	127000	127000				
Provozní náklady							
Licence Microsoft VDA	100	2250	225000	225000	225000	225000	225000
Spotřeba elektrické energie - klienti***	100	150	15000	15000	15000	15000	15000
Spotřeba elektrické energie - server****	3	6130	18390	18390	18390	18390	18390
Servisní činnosti	100	125	12500	12500	12500	12500	12500
Náklady celkem v letech			**1026890**	**270890**	**270890**	**270890**	**270890**
Celkem náklady za 5 let = 2 110 450,- Kč							

Tabulka 2: TCO – Tenký klient + VDI

Zdroj: Vlastní zpracování

* ZOTAC ZBOX SD-ID18 (CPU Intel Celeron 1007U, 2 GB RAM, klávesnice, myš), bez OS, záruka 5 let;

** Dell PowerEdge R320, 1U (CPU Intel Xeon E5-2430, 96 GB RAM, 3x HDD 600 GB SAS 15k - RAID 1 & hotspare), Windows 2012 R2, záruka 5 let ProSupport a 4hr Mission Critical;

*** 10W, 12 hodin denně, 365 dní v roce; **** 200W, 24 hodin denně, 365 dní v roce.

	2014			2015	2016	2017	2018
Pořizovací náklady	Počet	Cena	Celkem				
Tenký klient*	100	3750	375000				
Terminal server pro 50 stanic**	2	105000	210000				
Redundantní terminal server pro 50 stanic**	1	105000	105000				
Provozní náklady							
Spotřeba elektrické energie - klienti***	100	150	15000	15000	15000	15000	15000
Spotřeba elektrické energie - server****	3	6130	18390	18390	18390	18390	18390
Servisní činnosti	100	125	12500	12500	12500	12500	12500
Náklady celkem v letech			**735890**	**45890**	**45890**	**45890**	**45890**
Celkem náklady za 5 let = 919 450,- Kč							

Tabulka 3: TCO – Tenký klient + prezentační virtualizace

Zdroj: Vlastní zpracování

* ZOTAC ZBOX SD-ID18 (CPU Intel Celeron 1007U, 2 GB RAM, klávesnice, myš), bez OS, záruka 5 let;

** Dell PowerEdge R320, 1U (CPU Intel Xeon E5-2430, 32 GB RAM, 3x HDD 600 GB SAS 15k - RAID 1 & hotspare), Windows 2008 R2, záruka 5 let ProSupport a 4hr Mission Critical;

*** 10W, 12 hodin denně, 365 dní v roce; **** 200W, 24 hodin denně, 365 dní v roce.

Výše uvedené kalkulace se zabývají výhradně řešeními s produkty společnosti Microsoft. Pro dokreslení je vhodné uvést modelový příklad konkurenčního produktu společnosti Citrix, VDI-in-a-Box. Zde pochopitelně není možné využít již zakoupených licencí VP CAL, s čímž se počítá v předchozích případech.

	2014			2015	2016	2017	2018
Pořizovací náklady	Počet	Cena	Celkem				
Tenký klient*	100	3750	375000				
Server pro 50 stanic**	2	127000	254000				
Redundantní server pro 50 stanic**	1	127000	127000				
Licence Citrix VDI-in-a-box permanent	100	2460	246000				
Provozní náklady							
Licence Microsoft VDA	100	2250	225000	225000	225000	225000	225000
Citrix 1 year maintenance	100	640	64000	64000	64000	64000	64000
Spotřeba elektrické energie - klienti***	100	150	15000	15000	15000	15000	15000
Spotřeba elektrické energie - server****	3	6130	18390	18390	18390	18390	18390
Servisní činnosti	100	125	12500	12500	12500	12500	12500
Náklady celkem v letech			**1336890**	**334890**	**334890**	**334890**	**334890**
Celkem náklady za 5 let = 2 676 450,- Kč							

Tabulka 4: TCO – Tenký klient + Citrix VDI-in-a-Box

Zdroj: Vlastní zpracování

* ZOTAC ZBOX SD-ID18 (CPU Intel Celeron 1007U, 2 GB RAM, klávesnice, myš), bez OS, záruka 5 let;

** Dell PowerEdge R320, 1U (CPU Intel Xeon E5-2430, 96 GB RAM, 3x HDD 600 GB SAS 15k - RAID 1 & hotspare), bez OS, záruka 5 let ProSupport a 4hr Mission Critical;

*** 10W, 12 hodin denně, 365 dní v roce; **** 200W, 24 hodin denně, 365 dní v roce.

Za daných vstupních podmínek je pro organizaci jednoznačně nejvýhodnější nasadit tenké klienty společně s prezentační virtualizací, kde dosáhne nejnižších výdajů jak na pořízení, tak na provoz.

Při srovnání VDI (Microsoft) a standardní infrastruktury osobních počítačů hovoří pořizovací výdaje pro virtuální desktopy, naopak provozní výdaje, i přes výrazně vyšší spotřebu elektrické energie, pro běžná PC, kde je rozdíl způsoben poplatkem za licence Windows VDA. Výsledně však vychází výhodněji virtuální desktopy, které by organizace při výběru z těchto dvou řešení pravděpodobně implementovala, z důvodu principu centralizace i aktuálního trendu green computingu.

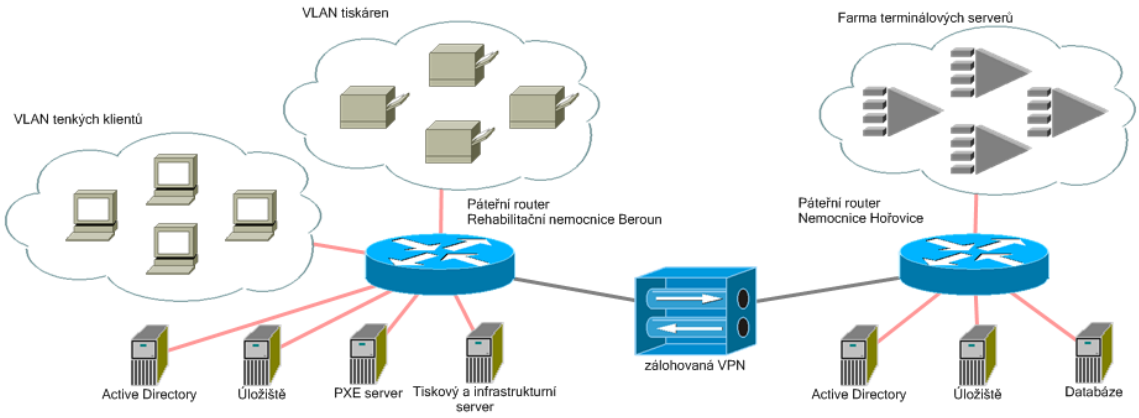
5 Vlastní řešení

Vlastním řešením bude vytvoření infrastruktury tenkých klientů k provozování modelu prezentační virtualizace s následujícími předpokládanými součástmi:

- 3x terminálový server (2x primární, 1x záloha, OS Windows 2008 R2),
- 100x tenký klient (OS Linux Debian),
- 1x infrastrukturní server (databáze, služba infrastrukturního serveru, služba tiskového serveru, webový server, OS Windows 2008 R2),
- 1x PXE server (OS Linux Debian).

Navrhovaný software pro provoz:

- klientská aplikace pro tenkého klienta,
- infrastrukturní server,
- tiskový server (využití stávajícího řešení),
- modul pro správu PXE serveru,
- webové rozhraní pro správu infrastruktury.



Obrázek 5: Zjednodušené schéma infrastruktury

Zdroj: Vlastní zpracování

Realizace bude spočívat v instalaci nových terminálových serverů do Nemocnice Hořovice. V Rehabilitační nemocnici Beroun bude nainstalován nový virtuální PXE server. Beze změn bude využito stávajícího tiskového serveru, přičemž na stejném virtuálním stroji bude spuštěn nový infrastrukturní server a webový management. V počítačové síti bude vytvořena další virtuální síť VLAN, kam budou připojování tencí klienti.

5.1 Nástroje použité pro vývoj softwaru

K vývoji jednotlivých softwarových modulů budou použity bezplatné nástroje nebo softwarová díla. Především to bude Java, jedno z nejpopulárnějších aplikačních prostředí na světě. Javu využívají firmy ve všech hlavních odvětvích průmyslu. Ať už v mobilních telefonech, herních konzolích, noteboocích nebo datacentrech. Java nabízí bohaté uživatelské prostředí, výkon, univerzálnost, přenosnost a bezpečnost, kterou dnešní síťové aplikace vyžadují.[11]

Java byla zvolena především z těchto důvodů:

- kombinace operačních systémů Windows a Linux v řešení infrastruktury, přičemž programy zhotovené v Javě lze z principu spustit na obou z nich,
- subjektivně jednodušší verze syntaxe jazyka C a C++,
- snadná implementace vícevláknových aplikací,
- vývojové prostředí pro komerční využití k dispozici zdarma,
- snadno dostupné informace a konkrétní příklady zdrojových kódů na Internetu.

Webový management bude zhotoven v PHP, což je široce používaný opensource skriptovací jazyk, který se hodí zejména pro vývoj webu. Kód PHP je vykonáván na serveru a generuje zdrojový kód HTML stránky, který je následně poslán klientovi. Ten tedy obdrží pouze výsledek skriptu, jehož zdrojový kód je pro něj neznámý. Za největší výhodu PHP lze považovat fakt, že je extrémně jednoduché pro začátečníka, ale nabízí i mnoho pokročilých funkcí pro profesionální programátory.[12] Součástí webového managementu jsou i přehledy v podobě grafů. Ty jsou generovány pomocí knihovny JpGraph, což je objektově orientovaná knihovna pro vytváření grafů určená pro PHP od verze 5.1 do 5.5. Knihovna je kompletně napsaná v PHP a je tak připravena pro použití v jakýchkoli PHP skriptech.[13]

---

[11] ORACLE. Java: The Best Environment for Network-Based Applications [online]. [cit. 2014-11-13]. Dostupné z: http://www.oracle.com/us/technologies/java/10045230-br-java-c17307-187867.pdf

[12] PHP.NET. What is PHP? [online]. [cit. 2014-11-13]. Dostupné z: http://php.net/manual/en/intro-whatis.php

[13] JPGRAPH.NET. JpGraph: Most powerful PHP-driven charts. [online]. [cit. 2014-11-13]. Dostupné z: http://jpgraph.net

Data budou ukládána do databáze MS SQL. Pro účely tohoto projektu je použito vydání Microsoft SQL Server Express 2008 R2. Jde o bezplatnou edici určenou pro vývoj méně náročných aplikací pro klientské počítače, web a malé servery. Omezení ve srovnání s plnohodnotnou placenou verzí se týkají výkonu nebo výbavy doplňky. Databáze využije maximálně 1 GB operační paměti a 1 procesor, velikost databázového souboru nebude větší jak 10 GB, k dispozici zde není SQL agent vhodný například pro plánování úloh. Tato omezení nejsou překážkou pro nasazení.

5.2 Terminálový server

Jako terminálové servery byly zakoupeny 1U rackmount stroje DELL PowerEdge R320 s následujícími technickými parametry:

- 1x Intel Xeon E5-2430 v2 2.50 GHz, 15 MB Cache, 7.2GT/s QPI, Turbo, 6C, 80W,
- 2x 16 GB RDIMM, 1600 MHz, Low Voltage, Dual Rank, x4,
- 3x 600 GB Hot-plug HDD, SAS 6 Gbps, 3.5“, 15k RPM,
- řadič RAID PERC H710, 512 MB NV Cache,
- SATA DVD mechanika,
- 2x integrovaná síťová karta Broadcom NetXtreme Gigabit Ethernet,
- 2x Hot-plug napájecí zdroj (max. 350W),

- OEM operační systém Windows Server 2008 R2 Standard CZ,
- záruka 5 let (ProSupport) a do 4 hodin expresní servis (Mission Critical).

5.2.1 Konfigurace hardwaru

Výchozí nastavení serveru od výrobce obvykle nevyžaduje mnoho zásadních úprav. Vzhledem k předpokládanému nepřetržitému provozu systému je vhodné modifikovat následující nastavení BIOSu:

- povolit „AC Recovery“ (spuštění serveru po selhání napájení) a nastavit náhodnou prodlevu v rozmezí desítek sekund od okamžiku obnovení dodávky elektrické energie,
- zakázat „Wait For 'F1' If Error“ (čekání na klávesu F1 v případě, že je detekována během POSTu některá z chyb).

Je třeba zdůraznit, že v serverech DELL PowerEdge je standardně instalována management karta iDRAC (Integrated Dell Remote Access Controller), která slouží k jednoduché vzdálené správě stroje, podporuje SNMP apod. Z toho důvodu je nutné provést přenastavení výchozí IP adresy a přihlašovacích údajů, jinak by mohlo dojít k jejich zneužití. Při této příležitosti je výhodné nastavit identifikační údaje serveru, které se zobrazují na displeji hlavního panelu a umožňují správci snažší orientaci v datacentru.

Dalším krokem je vytvoření diskového pole, přičemž v uvedeném serveru jsou k dispozici tři fyzické pevné disky. Pro vyšší zabezpečení dat je zvolen RAID 1 (zrcadlení), který je doplněn o hotspare disk. Ten si lze představit jako „pojistku“, která umožňuje snížit riziko ztráty dat tím, že v případě selhání některého z disků pole je tímto okamžitě nahrazen. Správci tak dává delší časový prostor na výměnu vadného komponentu.

5.2.2 Instalace operačního systému Windows Server 2008 R2

Základní instalace probíhá standardně z DVD média a je natolik intuitivní, že není třeba provádět její podrobnější popis. Před jejím zahájením je však často nutné připravit ovladače pro řadič RAID, které během instalačního procesu zpřístupní diskové pole, pokud jimi operační systém nedisponuje (jako v tomto případě). Podstatné kroky celého instalačního procesu jsou následující:

- rozdělení diskového pole na systémový a datový oddíl, volba vhodné velikosti alokačních jednotek souborového systému,
- instalace posledních verzí ovladačů hardwaru,
- nastavení síťového rozhraní, názvu serveru a revize nastavení pravidel brány firewall,
- instalace role Vzdálená plocha a povolení vzdálené správy serveru,
- prvotní aktualizace operačního systému z Internetu,
- odebrání tiskárny Microsoft XPS Document writer, instalace a konfigurace virtuálních tiskáren založených na ovladači Passthrough XPS Printer driver,
- konfigurace automatických aktualizací:
    - u terminálového serveru je vhodné ponechat aktualizace systému výhradně v režii administrátora, který určí vhodný okamžik, odpojí klienty apod.,
    - zvolit „Stahovat aktualizace, ale dotázat se zda mají být nainstalovány“,
    - zakázat instalace aktualizací všem standardním uživatelům,
- instalace antivirového software, optimalizace pro terminálový provoz:
    - použití programů určených pro serverovou instalaci s podporou provozu v terminálovém režimu,
    - zvýšení počtu skenovacích jader dle doporučení výrobce programu,
    - vypnutí GUI v uživatelských relacích,
    - revize nastavení kontroly aplikačních protokolů a přístupů na web,

- instalace Dell OpenManage Systems Management Software (správa hardwaru serveru), nastavení emailových upozornění na kritické události,
- instalace aplikací pro uživatele,
- aktivace operačního systému po Internetu,
- připojení do lokální domény služby Active Directory.

5.2.3 Konfigurace role Vzdálená plocha

Role Vzdálená plocha je klíčová pro funkci terminálového serveru. Přímo na serveru lze nastavit zejména následující parametry:

- zabezpečení komunikačního protokolu,
- volbu síťového rozhraní a omezení počtu připojení,
- parametry klienta (barevnou hloubku, počet monitorů, přesměrování periferií...),
- uživatele, nebo skupiny uživatelů, kteří se mohou k serveru připojovat,
- parametry relací (časové limity, akce při připojení...),
- způsob licencování (vázaný na zařízení nebo uživatele).

Pokud je server součástí domény se službou Active Directory (jako v tomto případě), je možné část těchto parametrů nakonfigurovat prostřednictvím Zásad skupiny, což umožňuje různým uživatelům nebo skupinám nastavit rozdílné parametry. Navigace v objektu GP je následující:

Konfigurace uživatele -> Zásady -> Šablony pro správu -> Součásti systému Windows -> **Služba Vzdálená plocha**

Zvláštní pozornost je třeba věnovat licencování. Při provozování více terminálových serverů se doporučuje nainstalovat jediný společný licenční server na doménovém řadiči, nikoli na každém z terminálových serverů. Pro volbu způsobu licencování klientského přístupu ke službě Vzdálená plocha obvykle platí, že tam, kde převažuje počet uživatelů nad počtem zařízení, je zpravidla výhodné použít licencování per device a naopak. Za zmínku stojí, že licence VP CAL vázané na uživatele nejsou vynucovány službou Licencování VP a k připojení klientů proto může docházet bez ohledu na počet nainstalovaných licencí. To však správce nezbavuje povinnosti dodržovat licenční

podmínky pro software společnosti Microsoft, které vyžadují, aby pro každého uživatele byla k dispozici platná licence VP CAL vázaná na uživatele.[14]

V případě této práce byla ponechána většina nastavení na výchozích hodnotách. Došlo k úpravě vlastností parametrů klienta (byla snížena barevná hloubka zobrazení na **16 bitů**). Dále byly zkráceny časové limity relací (ukončení odpojených relací – **1 hodina**, ukončení aktivních ale nečinných relací – **3 hodiny**). Licencování je vázané na zařízení.

5.2.4 Přizpůsobení uživatelského prostředí pomocí Zásad skupiny

U terminálových serverů je narozdíl od běžných počítačů kladen větší důraz na úpravu pracovního prostředí uživatelů, spočívajícího často v softwarových restrikcích nebo omezení přístupu ke konfiguraci systému.

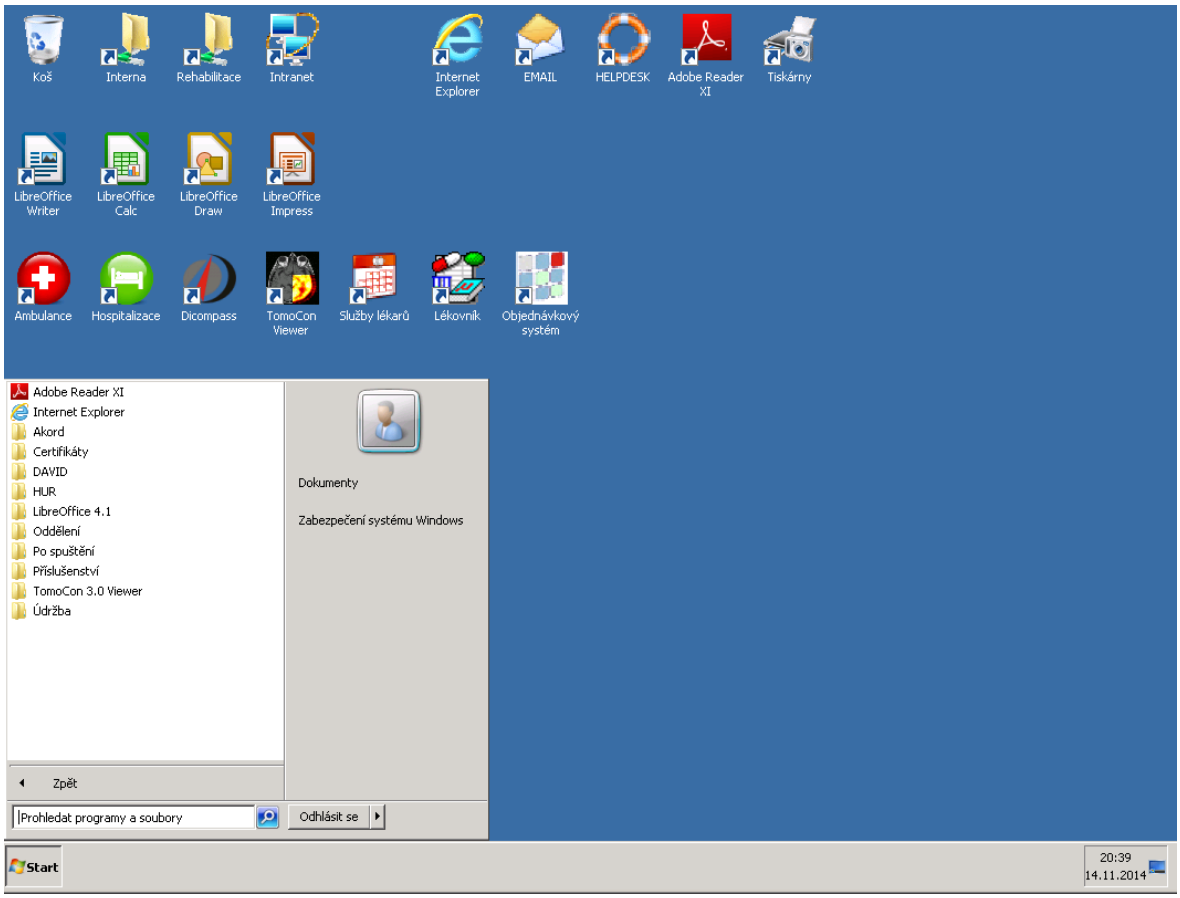
K tomuto účelu se používají Zásady skupiny, které v systému Windows Server 2008 poskytují funkce pro správu konfigurace v prostředí se službou Active Directory, kde umožňují ovlivnit celou řadu oblastí:

- instalace softwaru,
- skripty,
- nastavení zabezpečení,
- přesměrování složek,
- kvalitu služeb (QoS),
- nastavení prohlížeče Internet Explorer,
- šablony pro správu,
- předvolby,
- restrikce instalace zařízení,
- nastavení napájení.

Každá z výše uvedených sekcí v sobě skrývá velké množství nastavení zásad, které mohou ovlivnit konfiguraci počítače nebo uživatele. Ta je uložena v objektu zásad skupiny (GPO), který je podle potřeby napojen v určité úrovni struktury Active Directory, jako je například

[14] MICROSOFT. Licence pro klientský přístup k Vzdálené ploše (VP CAL). [online]. [cit. 2014-11-13]. Dostupné z: http://technet.microsoft.com/cs-cz/library/cc753650

síť, doména nebo organizační jednotka. Struktura AD je hierarchická a umožňuje dědit vlastnosti z vyšší úrovně do nižší, čímž poskytuje účinnou metodu pro použití nastavení zásad skupiny v širokém rozsahu.[15]



Obrázek 6: Přizpůsobené uživatelské prostředí pomocí Zásad skupiny

Zdroj: Vlastní zpracování

V některých situacích však statická struktura Active Directory nestačí ke správnému zamýšlenému uplatnění konkrétního objektu zásad skupiny. V takovém případě je možné použít filtr WMI, kde lze definovat pravidla pomocí dotazovacího jazyku WQL (WMI query language). Díky tomu dochází k dynamizaci tím, že lze do vyhodnocování zahrnout proměnné parametry a danou politiku podle toho buď přijmout nebo zamítnout.

[15] REIMER, Stan, Conan KEZEMA, Mike MULCARE, Byron WRIGHT. Windows server 2008 Active Directory: Resource Kit. Redmond: Microsoft Press, 2008, s. 400-401 ISBN 978-07-356-2515-0

V případě této práce došlo k výraznému přizpůsobení zásad skupiny v sekcích **Nastavení systému Windows** (Skripty, Nastavení zabezpečení, Přesměrování složek); **Šablony pro správu** (Nabídka Start a Hlavní panel, Ovládací panely, Plocha, Internet Explorer) a **Předvolby** (Nabídka Start). Takto upravená politika byla pomocí WMI filtru aplikována pouze na vybraných terminálových serverech podle jejich názvu.

5.2.5 Generátor signálních UDP paketů

Z pilotního provozu řešení vyšla najevo potřeba ošetřit detekci rozpadu WAN sítě. Ukázalo se, že pokud dojde k výpadku delšímu jak přibližně deset sekund, přestane klient RDP protokolu (freerdp-x11) reagovat a je nutné jeho proces ukončit a znovu spustit. Byl tedy vytvořen extrémně jednoduchý generátor signálních UDP paketů s jejichž pomocí aplikace na klientu detekuje stav a stabilitu WAN sítě a činí potřebná opatření. Generátor je automaticky spuštěn při startu terminálového serveru a odesílá každou sekundu UDP paket, který v sobě nese jeho název.

```
package cz.nember.udpsender;
import java.io.IOException;
import java.net.*;

public class UDPSenderServer {
    public static void main(String[] args){

        DatagramSocket socket = null;
        DatagramPacket outPacket = null;
        byte[] outBuf;

        if (args.length==2){
            String msg = System.getenv("COMPUTERNAME"); // paket bude obsahovat nazev serveru
            String host = args[0];                      // cilova IP adresa
            final int port = Integer.valueOf(args[1]);  // cilovy port

            try {
                InetAddress address = InetAddress.getByName(host);
                socket = new DatagramSocket();
                outBuf = msg.getBytes();
                outPacket = new DatagramPacket(outBuf, 0, outBuf.length, address, port);

                for (;;){
                    socket.send(outPacket);
                    try {
                        Thread.sleep(1000);
                    } catch (InterruptedException e) {break;}
                }
            } catch (IOException ioe) {System.out.println(ioe);}
        }
    }
}
```

Obrázek 7: Generátor UDP paketů v Javě

Zdroj: Vlastní zpracování

5.3 Tenký klient

Pracovní stanice budou realizované jako tenký klient:

- umožní připojení k terminálovým serverům s operačním systémem Windows,
- nebudou obsahovat žádné paměťové médium,
- operační systém bude zaváděn pomocí technologie PXE přímo z počítačové sítě,
- bude použit bezplatný operační systém Linux Debian,
- prostředí bude realizováno klientskou aplikací.

5.3.1 Instalace operačního systému Debian Wheezy 7.5

Jako operační systém pro síťově zaváděného tenkého klienta je zvolena distribuce Linuxu Debian Wheezy v aktuální verzi 7.5. Instalace je v první fázi provedena na modelovém tenkém klientu osazeném pevným diskem, ze které je poté vytvořena síťová image. ISO obrazy instalačních CD jsou poskytovány na webu https://www.debian.org/distrib/netinst zdarma ve verzích podle velikosti média a architektury procesoru (i386 – 32 bit, amd64 – 64 bit...). Po vypálení disku je možné zahájit vlastní instalaci, během které je při použití tzv. malého CD zapotřebí funkční připojení k Internetu. Podstatné kroky instalačního procesu jsou následující:

- volba lokalizace (jazyk, oblast, klávesnice),
- konfigurace root a non-root uživatele,
- nastavení diskových oddílů („všechny soubory v jedné partition“ a swap),
- výběr sestavení systému (základní systém, standardní systémové utility a SSH).

Po dokončení instalačního procesu jsou v režimu superuživatele (root) nainstalovány pomocí apt (Advanced Packaging Tool) další standardní balíky:

- mc (souborový manažer Midnight Commander),
- ntpdate (utilita pro synchronizaci systémového času),
- x-window-system (software umožňující provozovat grafické uživatelské prostředí),
- numlockx (utilita pro zapnutí numerické klávesnice),
- alsa-utils (podpora zvukových zařízení),
- default-jre (Java Runtime Environment),
- initramfs-tools (nástroje pro vytvoření a zavedení initramfs pro balíčkovaná jádra Linuxu řady 2.6).

Za normálních okolností by byl stejným způsobem instalován také klíčový balík freerdp-x11 představující RDP klienta. V distribuci Debian Wheezy 7.5 jsou však k dispozici starší verze (1.0.1 - 1.1) obsahující celou řadu identifikovaných chyb. Z toho důvodu jsou staženy aktuální zdrojové kódy verze 1.2 z repositáře webové služby GitHub, která podporuje vývoj softwaru používáním verzovacího nástroje Git a nabízí bezplatný hosting pro open-source projekty. Stažené kódy jsou zkompilovány dle instrukcí ve specifikaci dostupné z https://github.com/FreeRDP/FreeRDP/wiki/Compilation.

Pro účely vzdálené podpory uživatelů je nainstalován také balík x11vnc. Software umožňuje sledovat a pracovat na dálku v systémech Linux/Unix s reálnými X displeji pomocí jakéhokoliv prohlížeče VNC.[16]

Poté je potřeba systém připravit na start s automatickým přihlášením root uživatele a okamžitým spuštěním GUI klientské aplikace. K tomuto účelu je nutné změnit nastavení v konfiguračním souboru **`/etc/inittab`** takto:

```
#1:2345:respawn:/sbin/getty 38400 tty1
1:2345:respawn:/bin/login -f root tty1 </dev/tty1 >/dev/tty1 2>&1
```

Po přihlášení dojde ke spuštění skriptu uvedeného v souboru **`/root/.bash_profile`**. Tento skript bude v případě lokálního přihlášení startovat grafické prostředí, naopak v případě vzdáleného přihlášení například pomocí ssh umožní vstup do konzole. Typ přihlášení lze zjistit podle použitého terminálu:

tty (Terminal Type) – lokální konzole klienta,

pts (Pseudo Terminal Slave) – vzdálená konzole (xterm, ssh).

```
#!/bin/bash
if tty | fgrep tty ; then
      cd /appd
      while true
      do
            startx ./client
      done
shutdown
fi
```

[16] RUNGE, Karl. x11vnc: a VNC server for real X displays. [online]. [cit. 2014-11-13]. Dostupné z: http://www.karlrunge.com/x11vnc

Pokud dojde k lokálnímu přihlášení (tty), bude v nekonečné smyčce spouštěn příkaz startující grafické prostředí **`startx ./client`**. Cyklus zabraňuje možnému přístupu uživatele k lokální konzoli v případě selhání programu. Argumentem příkazu je další skript, který již nastavuje dílčí parametry GUI (zde konkrétně vypíná screensaver), zapíná numerickou klávesnici a spouští vlastní klientskou aplikaci v Javě.

```
#!/bin/bash
xset -dpms &
xset s noblank &
xset s off &
numlockx
java -jar client.jar
```

Na závěr je vhodné deaktivovat defaultně nainstalovanou službu exim4 (Mail transfer agent), která se nebude na klientu používat. K tomu slouží skript **`update-rc.d`**, který přidá nebo odebere zvolenou službu ze startovacích skriptů. Je také možné smazat non-root uživatele pomocí **`deluser`**, protože terminál bude pracovat výhradně pod uživatelem root. Po dodání klientské aplikace je v tomto okamžiku zařízení schopno fungovat jako požadovaný tenký klient z pevného disku.

5.3.2 Vytvoření síťově bootovatelného diskového obrazu

Před úpravami na síťově bootovatelný diskový obraz je vhodné provést kompletní zálohu aktuální instalace například pomocí nástroje Clonezilla. Další zásahy totiž znemožní budoucí spuštění tohoto systému z pevného disku. Úpravy jsou následující:

- nastavení připojení diskových oddílů při startu, obsah konfiguračního souboru **`/etc/fstab`** bude nahrazen takto:

```
# /etc/fstab: static file system information.
/dev/nfs  /        nfs     defaults 0 0
none      /tmp     tmpfs   defaults 0 0
none      /run     tmpfs   defaults 0 0
none      /var/tmp tmpfs   defaults 0 0
none      /media   tmpfs   defaults 0 0
```

- nastavení initramfs v konfiguračním souboru **`/etc/initramfs-tools/initramfs.conf`**, kde bude změněno:

```
BOOT=nfs
MODULES=netboot
```

- vytvoření nové initrd image pomocí příkazu

  `mkinitramfs -o initrd.img.netboot` spuštěného ve složce **`/boot`**

- změna chování shutdown skriptu uloženého v **`/etc/init.d/halt`**, kde bude změněno:

  `NETDOWN=no`
  Zakáže deaktivaci sítě během vypínání zařízení (vzhledem k závislosti na NFS).

- nastavení síťového rozhraní v konfiguračním souboru **`/etc/network/interfaces`**, který bude v případě existence jednoho fyzického rozhraní obsahovat:

```
# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
iface eth0 inet manual
```

  Použije se nastavení sítě z DHCP tak, jak klient nabootoval z PXE.

Následuje připojení NFS úložiště a zkopírování obsahu disku 1:1 do určené složky:

```
mount -tnfs -onolock xx.xx.xx.xx:/nfs/tc /mnt
cp -axv /. /mnt/.
```

Po zkopírování se smaže obsah složky **`/mnt/dev`**.

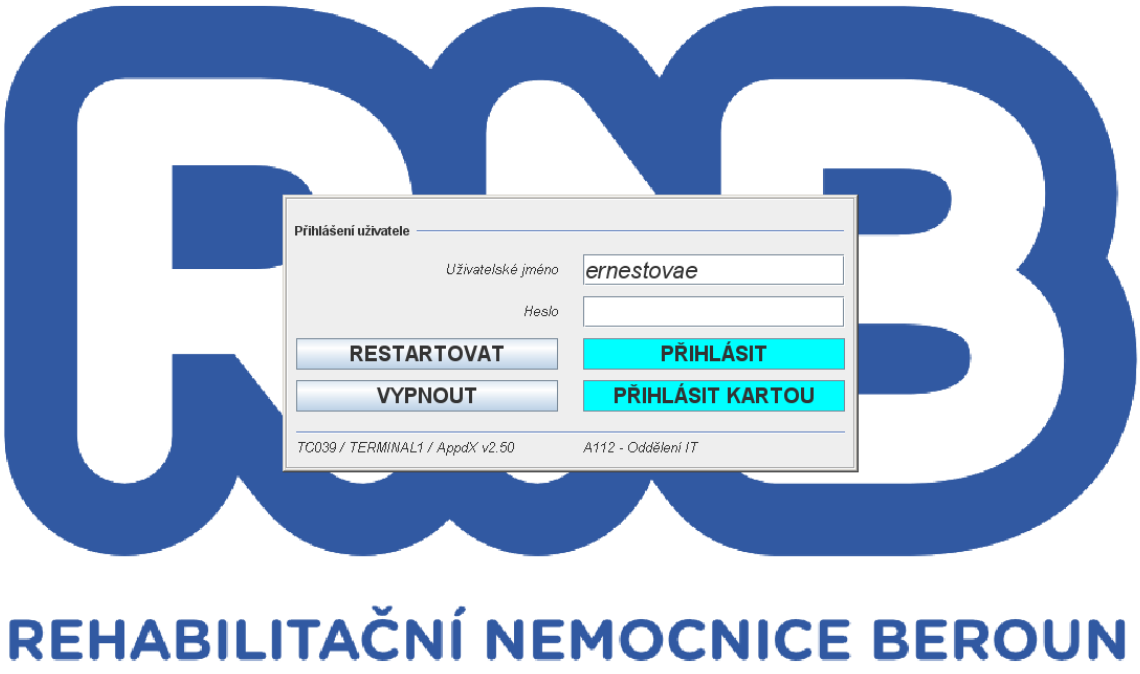
Poté se na NFS serveru pomocí programu **`tar`** vytvoří ze složky nekomprimovaný archiv, který slouží jako výchozí disková image. Ostatní dílčí úpravy konfigurace jsou automaticky prováděny při generování diskových obrazů z tohoto archivu PXE serverem.

5.3.3 Klientská aplikace

Úkolem klientské aplikace bude vytvořit prvotní kontaktní prostředí pro uživatele, zajistit obsluhu zařízení a komunikaci s infrastrukturním serverem. Program bude řešit:

- nastavení prostředí terminálu podle konfigurace v centrální databázi (rozlišení obrazovky, výhledově aktivace periferií – USB přesměrování apod.),
- spuštění VNC serveru a vytvoření jednorázového náhodného přihlašovacího hesla pro pracovníky technické podpory,
- přihlášení uživatele pomocí uživatelského jména a hesla ověřovaným v AD,

- zobrazení disponibilních vzdálených ploch, kam se může uživatel připojit, nebo automatické připojení (pokud je pouze jedna),
- provedení všech úkonů nezbytných pro sestavení relace vzdálené plochy (nastavení výskytu uživatele, kontrolu zámků apod.),
- obsluhu XFreeRDP klienta, jeho spuštění s odpovídajícími parametry a zpracování návratových kódů,
- kontrolu stavu síťového spojení pomocí UDP signálních paketů a akce v případě rozpadu spojení,
- průběžné odesílání provozních informací infrastrukturnímu serveru, manipulaci se zařízením – vypnutí a restart.



Obrázek 8: Tenký klient - přihlašovací obrazovka
Zdroj: Vlastní zpracování

Z pohledu uživatele dojde za normálních okolností po přihlášení k automatickému spuštění RDP klienta a připojení příslušné vzdálené plochy. Po odhlášení pak dojde k návratu na výše uvedenou přihlašovací obrazovku. Pokud je na stanici umožněno připojení k více vzdáleným plochám, je po přihlášení uživateli zobrazen nejdříve jejich seznam.

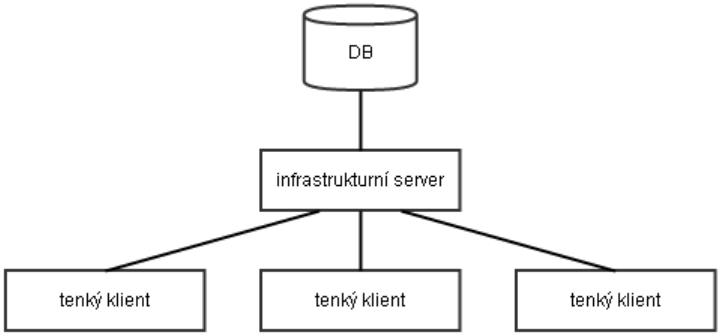
Zdrojový kód programu je zapsán v jazyce Java a je rozdělen do následujících balíčků:

- „client“ obsahuje třídy zajišťující běh programu, zpracování konfigurace, volání externích aplikací, obsluhu programu xfreerdp, UDP listener a generátor náhodných hesel,
- třídy balíčku „client.commands“ představují jednotlivé příkazy, kterými klientská aplikace komunikuje s infrastrukturním serverem,
- „client.gui“ zajišťuje pomocí několika tříd realizaci grafického prostředí aplikace.

Detailnější popis struktury programu klientské aplikace je uveden v příloze A.

5.4 Infrastrukturní server

Je aplikace představující klíčovou součást celého řešení. Jeho úlohou je především role zprostředkovatele, kde na straně jedné komunikuje s databází provozních údajů, na straně druhé pak s aplikací na tenkých klientech. Je zde implementována podstatná logika celého systému.



Obrázek 9: Schéma komunikace základních prvků infrastruktury
Zdroj: Vlastní zpracování

Výhodou tohoto návrhu je praktická izolace klientů od databáze a také to, že dílčí změnu chování celé infrastruktury lze provést přímo na serveru, často bez nutnosti úprav na klientech. Zdrojový kód programu je zapsán v jazyce Java a je rozdělen do následujících balíčků:

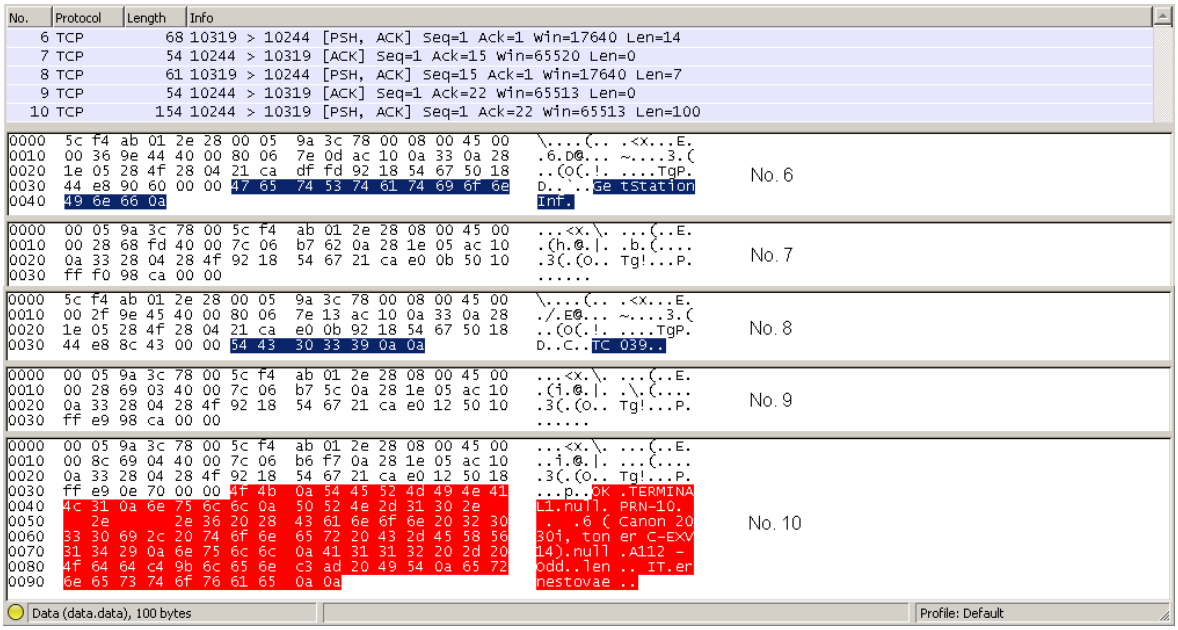
- „srv“ obsahuje třídy zajišťující provoz serveru, UDP/TCP listener, UDP forwarder, správu podřízených vláken, zpracování konfigurace, napojení na databázi, logování a volání externích aplikací,
- třídy balíčku „srv.handler“ zajišťují zpracování požadavků od klientů a vytváření instancí výkonných tříd podle přijaté textové identifikace příkazů (k realizaci bylo vhodně využito návrhového vzoru Factory),
- „srv.handler.impl“ obsahuje jednotlivé výkonné třídy příkazů s konkrétní funkční implementací, které jsou prováděny nezávisle ve vlastních vláknech.

Detailnější popis struktury programu infrastrukturního serveru je uveden v příloze B.
Schéma databáze, se kterou server komunikuje, je obsahem přílohy D.

5.4.1 Komunikace serveru s klientem

Komunikace probíhá prostřednictvím jednoduchých příkazů a zahajuje ji vždy klient paketem, který v sobě nese název příkazu (třídy na serveru). Server po jeho přijetí vytvoří

instanci příslušné třídy a příkaz následně dále zpracovává ve vlastním vlákně, kde obdrží argumenty, vykoná deklarované akce a případně odešle zpět výsledky. Na serveru je z hlediska bezpečnosti omezen maximální možný počet paralelních spojení. Nebude-li obsah zpráv vyžadovat utajení, či hrozit jeho potenciální zneužití, bude po síti přenášen pomocí protokolu TCP v prostém textu. To je možné i proto, že server bude komunikovat s klientem v rámci jednoho segmentu přepínané lokální sítě, kde může dojít k odposlechu paketů jen obtížně.



Obrázek 10: Ukázka TCP komunikace mezi serverem a klientem

Zdroj: Vlastní zpracování

Jak lze vidět na předcházejícím obrázku:

- komunikaci zahájil klient příkazem „GetStationInf“ (paket 6),
- server vrátil potvrzení (ACK, paket 7),
- klient zaslal argument – název stanice „TC039“ (paket 8),
- server vrátil potvrzení (ACK, paket 9),
- server zaslal výsledek příkazu – informace o stanici (paket 10).

Protože je však potřeba přenášet i citlivé zprávy, kde budou obsahem například přihlašovací údaje uživatele, musí být zajištěn také zvlášť zabezpečený přenos. K tomuto účelu je použita symetrická bloková šifra AES (Advanced Encryption Standard), která pro

šifrování i dešifrování využívá stejný klíč na data s pevně danou délkou bloku 128 bitů. Umožňuje volbu velikosti klíče 128, 192 nebo 256 bitů a je nástupcem dříve používané šifry DES (Data Encryption Standard).[17]

5.4.2 UDP listener a UDP forwarder

Úkolem serveru je také příjem provozních informací od klientů. Jedná se o data, která přichází periodicky a nemají přímý vliv na provoz infrastruktury. Jsou odesílána v podobě UDP paketu bez očekávané odpovědi od serveru. Použití UDP zde citelně sníží náročnost zpracování, když server nemusí s klientem navazovat TCP spojení a data pouze přijme a zpracuje. Prakticky jde o realizaci podle výpočetního modelu agent – manažer.

Další z činností klientské aplikace je kontrola stavu síťového spojení pomocí UDP signálních paketů (heartbeat paketů) od terminálových serverů. Ty jsou vysílány v pravidelných intervalech a aplikace je podle toho schopna vyhodnotit případný rozpad WAN sítě nebo nefunkčnost serveru, aniž by to musela sama zjišťovat například pomocí protokolu ICMP. Aby nebylo nutné tyto pakety cílit přímo na IP adresu každého klienta, jsou zasílány na síťový broadcast. To však nelze vzhledem ke konfiguraci WAN sítě realizovat. Z toho důvodu je do infrastrukturního serveru implementován také UDP forwarder, který přijme paket od terminálového serveru a odvysílá jej na lokální broadcast tenkým klientům.

5.4.3 Využití Active Directory

Infrastrukturní server bude pro klientskou aplikaci zajišťovat také ověřování přihlašovacích údajů uživatelů, protože tenký klient ze své VLAN nedisponuje konektivitou k řadiči Active Directory ani příslušnou funkcionalitou. V programovacím jazyce Java existuje API rozhraní JNDI (Java Naming and Directory Interface), které umožňuje přístup k adresářovým službám typu LDAP. Protože však server běží na stroji s operačním systémem Windows, který je zařazen přímo v doméně služby Active Directory, jeví se jako efektivní použít pro ověření uživatele extrémně jednoduchý kód zapsaný v C#, využívající rozhraní .NET Framework. Kód je zkompilován jako spustitelný soubor, který

[17] WIKIPEDIA. Advanced Encryption Standard. [online]. [cit. 2014-11-13].
Dostupné z: http://cs.wikipedia.org/wiki/Advanced_Encryption_Standard

si server zavolá jako subproces a zpracuje jeho návratový kód, ze kterého získá informaci, zda je uživatel autentifikován nebo nikoli.

```
using System.DirectoryServices;
using System;

namespace ADAuth
{
    class Program
    {
        public static int Main(string[] args)
        {
            bool authenticated = false;
            if (args.Length==3) {
                try
                {
                    DirectoryEntry entry = new DirectoryEntry(args[0], args[1], args[2]);
                    object nativeObject = entry.NativeObject;
                    authenticated = true;
                }
                catch (DirectoryServicesCOMException cex) {}
                catch (Exception ex) {}
            }
            else Console.WriteLine("Pouzij syntaxi: adauth.exe server user password");
            if (authenticated) return 0; else return 1;
        }
    }
}
```

Obrázek 11: Ověřování uživatelů v Active Directory pomocí C#

Zdroj: Vlastní zpracování

Aplikace na klientovi umožňuje uživateli také provést změnu jeho hesla v doméně. K tomuto účelu infrastrukturní server využívá command-line utilitu **`Net user`**, která je k dispozici v operačním systému Windows a zajišťuje přidání a modifikaci uživatelských účtů nebo o nich zobrazuje informace.[18]

Použitá syntaxe je následující:

```
net.exe user <uživatelské jméno> <nové heslo> /DOMAIN
```

V obou předchozích případech dochází k volání externích aplikací jako subprocesů, což může představovat potenciální bezpečnostní problém. Pokud je ovšem daný server adekvátně zabezpečený a není zde například možné podvrhnout jiné soubory s potenciálně škodlivým obsahem, není třeba se této implementace zvlášť obávat.

[18] MICROSOFT. Net user [online]. [cit. 2014-11-13].
Dostupné z: http://technet.microsoft.com/en-us/library/cc771865

5.4.4 Wrapper pro zapouzdření aplikace jako služby

Aby bylo možné spustit běžnou Java aplikaci jako službu, je zapotřebí použít framework označovaný jako wrapper. V tomto případě byl použit YAJSW (Yet another java service wrapper) dostupný pod licencí LGPL, který umožňuje Java aplikacím, aby byly spuštěny jako služba v operačním systému Windows nebo jako démon v systémech typu UNIX. Framework podporuje[19]:

- zapouzdření jakéhokoli nativního spustitelného Java procesu nebo groovy skriptu a jeho spuštění jako služby nebo démona,
- platformovou nezávislost v instalaci i konfiguraci,
- zachytávání výstupu do konzole, jeho logování a spouštění skriptů nebo restart procesu na základě shody výstupu s definovanými regulárními výrazy,
- monitorování a automatický restart nereagujícího nebo havarovaného procesu,
- časované spuštění nebo ukončení procesu,
- čtení ze standardního výstupu a zápis do standardního vstupu procesu,
- provoz pod jiným uživatelem (RunAs / sudo),
- přítomnost ikony v hlavním panelu (System Tray) a zobrazení zpráv, například výjimek,
- vzdálené ovládání po síti.

[19] SOURCEFORGE.NET. Welcome to YAJSW. [online]. [cit. 2014-11-13].
Dostupné z: http://yajsw.sourceforge.net

5.5 Použité tiskové řešení

V rámci nově budované infrastruktury je bez nutnosti úprav zcela využito osvědčeného tiskového řešení. Jde o vlastní tiskový server, který vznikl jako jeden ze softwarových modulů v rámci mé předchozí bakalářské práce na téma „Řízení vzdálených aplikací v doméně MS Windows“, kde jedním z dílčích cílů bylo odstranit problémy s tiskem právě při provozu terminálových aplikací. Tento server zpracovává veškeré tiskové úlohy přicházející z terminálových serverů, případně jiných destinací. Stroj, na kterém je spuštěn, disponuje síťovou konektivitou na všechny požadované tiskárny, a ty musí být v operačním systému nainstalované.

Tiskové úlohy se přenáší jako soubory formátu XPS (XML Paper Specification), vyvinutým společností Microsoft a určeným k reprezentaci dokumentů či jako formát souborů tiskové fronty (spool file). Na straně terminálových serverů generují tyto soubory bez interakce s uživatelem virtuální tiskárny založené na ovladači Passthrough XPS Printer driver, který je produktem společnosti Frogmore Computer Services Ltd. a je k dispozici zdarma. Výsledkem je poté soubor doručený tiskovému serveru do sdíleného síťového adresáře, který je v názvu opatřen unikátním sériovým číslem dokumentu, názvem terminálového serveru a uživatelským jménem. Jde o klíčové informace, ze kterých je možné lokalizovat, kam přesně se má daná úloha vytisknout. To tiskový server zjistí jednoduchým dotazem do provozní databáze na poslední výskyt uživatele.

Toto řešení odstraňuje celou řadu problémů, především však zjednodušuje infrastrukturu tím, že není potřeba fyzické tiskárny instalovat ani na klientech (a používat problematické přesměrování) ani na každém terminálovém serveru zvlášť - instalují se pouze jednou na printserveru. Uživatel má potom k dispozici jednu nebo více obecných virtuálních tiskáren a může se snadno a naprosto plynule (bez ukončování aplikací) pohybovat mezi různými pracovišti, přičemž díky exkluzivitě terminálových relací má jistotu, že úloha bude vždy vytištěna na správném místě.

Tiskový server také umožňuje zpracování jednoduchých tisků podle šablony. Prakticky jde o vestavěný generátor tiskových sestav. Šablona reprezentovaná XML souborem obsahuje informace o vlastnostech a rozložení textu či prvků. Využít lze jednoduchých grafických

útvarů nebo generátoru čárového kódu. Od aplikace poté přichází pouze textový soubor se specifikovanou šablonou, jejími prvky a přiřazenou hodnotou. Toho se četně využívá například k realizaci tisku identifikačních štítků, pořadových lístků nebo stvrzenek na specializovaných tiskárnách. Tato přímá integrace do tiskového serveru na straně jedné a do informačních systémů na straně druhé výrazně usnadňuje nasazení v terminálových aplikacích a podtrhává význam tiskového serveru. Zároveň zvyšuje uživatelský komfort tím, že uživatel vůbec nemusí řešit výběr tiskáren, o který se podle typu úlohy a určené tiskárny postará automaticky tiskový server.

Je zde také implementováno testování online stavu tiskárny před zahájením tisku pomocí protokolu ICMP. Pokud tiskárna neodpovídá, je tisková úloha stornována a uživateli je na plochu zaslána zpráva s informací. Nedochází tak k plnění tiskové fronty, k jejímuž vyprázdnění by došlo až po zapnutí nebo zprovoznění tiskárny a dokumenty by se tak mohly dostat k neoprávněné osobě.

Shrnutí vlastností tiskového serveru:

- podpora tisku souborů formátu XPS z virtuálních tiskáren,
- podpora tisku podle šablony (XML šablona + textový soubor popisující dokument),
- směrování tisku podle posledního platného výskytu uživatele v infrastruktuře,
- podpora oboustranného tisku (jednostranná a oboustranná virtuální tiskárna, použití příslušných preferencí pro tisk u fyzické tiskárny),
- testování dostupnosti tiskáren, avízo uživateli,
- reporting (sledování tiskových úloh – počet stran, uživatelé, pracoviště…)

5.6 PXE server

Preboot execution environment (PXE) je označení standardu, umožňujícího start operačního systému bezdiskových počítačů nebo zařízení přímo ze sítě. Byl zaveden firmou Intel v září roku 1999. Jeho programový kód je v dnešní době obvykle běžnou součástí BIOSu na základních deskách, které mají integrovanou síťovou kartu. Nechybí však ani u samostatných síťových karet, kde je uložen ve flash paměti.

PXE je definován na základech standardních internetových protokolů a služeb, které jsou široce nasazeny v průmyslu, a to TCP/IP, DHCP a TFTP. Tím je standardizována podoba interakce mezi klienty a servery.[20] Při vlastním bootovacím procesu se nejdříve provede automatická konfigurace síťového rozhraní klienta pomocí DHCP, následně je z TFTP serveru stažen NBP (Network Bootstrap Program), který je obdobou zavaděče jádra operačního systému. Ten poté umožní další síťovou komunikaci "vyšší úrovně", v případě Linuxu se obvykle používá NFS, kde je uložen kompletní obraz disku stanice.

PXE server bude obsahovat:

- bezplatný operační systém Linux Debian,
- datové úložiště s kapacitou minimálně 200 GB pro obrazy disků jednotlivých tenkých klientů (uvažuje se asi 1,5 GB / stanice + rezerva),
- službu DHCP serveru,
- službu TFTP serveru,
- službu NFS serveru,
- aplikaci pro správu diskových obrazů a rekonfiguraci DHCP serveru.

Operačním systémem pro PXE server je zvolen stejně jako v případě tenkých klientů Debian Wheezy 7.5. Postup základní instalace je téměř identický. Rozdílná je však konfigurace diskových oblastí. Virtuálnímu serveru, kam je PXE server umístěn, jsou přiděleny dva virtuální pevné disky (VHD). Jeden je určen pro instalaci operačního systému, druhý pak pro NFS úložiště s obrazy disků jednotlivých tenkých klientů.

[20] INTEL CORPORATION. Preboot Execution Environment (PXE) Specification [online]. [cit. 2014-11-13]. Dostupné z: ftp://download.intel.com/design/archives/wfm/downloads/pxespec.pdf

Důvodem rozdělení už na úrovni VHD je především možnost rychlejší manipulace s virtuálním diskem operačního systému, kde se na rozdíl od druhého disku očekává jeho velikost maximálně v jednotkách GB.

Po dokončení instalačního procesu jsou v režimu superuživatele (root) nainstalovány pomocí apt (Advanced Packaging Tool) další balíky:

- dhcp3-server (DHCP server),
- tftpd-hpa (TFTP server),
- nfs-kernel-server (NFS server),
- syslinux (projekt sdružující "lehké" zavaděče operačního systému Linux - SYSLINUX, PXELINUX, ISOLINUX a EXTLINUX)[21],
- mc (souborový manažer Midnight Commander),
- ntpdate (utilita pro synchronizaci systémového času).

Dále je deaktivována defaultně nainstalovaná služba exim4 (Mail transfer agent), která se nebude na serveru používat. K tomu slouží skript **`update-rc.d`**, který přidá nebo odebere zvolenou službu ze startovacích skriptů.

5.6.1 Služby PXE serveru

DHCP (Dynamic Host Configuration Protocol) je protokol, pomocí kterého může stroj při bootování automaticky získat nastavení pro síťové rozhraní. To umožňuje centralizaci konfigurace sítě. Server DHCP poskytuje řadu síťových parametrů. Nejběžnější z nich je IP adresa, rozsah sítě a výchozí brána. Poskytovat může také další údaje jako jsou například servery DNS, WINS nebo zde TFTP. Hlavním autorem DHCP serveru je ISC (Internet Software Consortium), v systému Debian jde o balíček isc-dhcp-server (resp. dhcp3-server)[22]

[21] SYSLINUX.ORG. The Syslinux Project. [online]. [cit. 2014-11-13].
Dostupné z: http://www.syslinux.org/wiki/index.php/The_Syslinux_Project

[22] HERTZOG, Raphaël a Roland MAS. The Debian Administrator's Handbook. Freexian, 2013, s. 464 ISBN 979-10-91414-02-9. s. 239.

Konfigurační soubor DHCP serveru je uložen v **`/etc/dhcp/dhcpd.conf`** a jeho obsah bude generován modulem pro správu z databáze infrastruktury.
Je vhodné, aby konfigurovaný DHCP server byl tím jediným v konkrétní síti. V případě existence více DHCP by mohlo dojít k přidělení chybné konfigurace. I z toho důvodu je infrastruktura tenkých klientů separována do vlastní uzavřené virtuální sítě VLAN.

TFTP (Trivial File Transfer Protocol) je velmi jednoduchý protokol, používaný pro přenos souborů pomocí transportního protokolu UDP. Je navržen tak, aby byl malý a snadno implementovatelný. Proto postrádá většinu možností standardního FTP protokolu a jedinou jeho funkcí je čtení a zápis souborů z nebo na vzdálený server.[23]
Konfigurační soubor TFTP serveru je uložen v **`/etc/default/tftpd-hpa.conf`**.
Zde je uvedena cesta k adresáři s daty a také rozhraní, kde server naslouchá. Ve výchozím nastavení je určeno jako "0.0.0.0:69", což znamená, že server komunikuje na všech dostupných lokálních rozhraních a portu 69. Z hlediska bezpečnosti je vhodné specifikovat pouze rozhraní do sítě tenkých klientů.

NFS (Network File System) je protokol, který umožňuje vzdálený přístup k systému souborů prostřednictvím sítě. Lze s ním pracovat ve všech unixových systémech a jde zde pravděpodobně o nejpoužívanější protokol k tomuto účelu. Pro komunikaci používá obvykle protokol UDP, od verze 3 je možné volitelně použít TCP[24], což má smysl především pokud komunikace mezi serverem a klientem probíhá po síti typu WAN.

NFS má několik historických omezení, které lze považovat za nedostatky hlavně v oblasti bezpečnosti:

- veškerá data jsou po síti přenášena nešifrovaně a může tak dojít k jejich zachycení,
- omezení přístupu je prováděno podle IP adresy, která může být zfalšována,
- neošetřeným nastavením může dojít k nežádoucímu zpřístupnění všech souborů na úložišti (je-li klientem uživatel root).

[23] IETF. RFC 1350 - The TFTP Protocol (Revision 2). [online]. [cit. 2014-11-13].
Dostupné z: http://tools.ietf.org/html/rfc1350
[24] IETF. RFC 1094 - NFS: Network File System Protocol specification. [online]. [cit. 2014-11-13].
Dostupné z: http://tools.ietf.org/html/rfc1094

V Debianu je NFS server k dispozici jako jaderný modul, který se spustí automaticky při startu, je-li nainstalován balíček nfs-kernel-server.[25]

Konfigurační soubor NFS serveru je uložen v **`/etc/exports`**.

Jedná se o seznam adresářů, které mají být k dispozici po síti a s jakými parametry:

- forma přístupu - **ro** (pouze čtení - výchozí) / **rw** (čtení i zápis),
- reakce NFS na požadavky - **sync** (odpoví po skončení diskové operace - výchozí) / **async** (odpoví ještě před skončením diskové operace – může zvýšit výkon, ale také riziko ztráty dat při pádu serveru),
- zákaz root přístupu – **root_squash** (server považuje uživatele root za uživatele nobody – výchozí) / **no_root_squash** (je umožněn root přístup k filesystému).

Pro tenké klienty startované ze sítě musí být síťový adresář přístupný pro čtení i zápis (rw) a musí umožnit root přístup k souborovému systému (no_root_squash).

Po modifikaci konfiguračního souboru je nutné zavolat příkaz **`exportfs -r`** (reexport).

5.6.2 Správa PXE serveru

Správu PXE serveru zajišťuje aplikace, která sekvenčně zpracovává jednotlivé úlohy pro PXE server vygenerované webovým managementem:

- konfigurace DHCP serveru

  Na základě údajů z databáze vytvoří konfigurační soubor pro DHCP server uložený v /etc/dhcp/dhcpd.conf, a poté restartuje službu DHCP serveru. Konfigurace jednotlivé stanice obsahuje následující nezbytné údaje:

```
host TC010 {
hardware ethernet 00:14:0B:6D:26:C8;    (MAC adresa)
next-server 10.  .  . ;                 (TFTP server)
fixed-address 10.  .  .10;              (IP adresa stanice)
filename "/tc010/pxelinux.0";           (cesta k zavaděči jádra)
option host-name "TC010";               (název stanice)
option routers 10.  .  .1;              (výchozí brána)
}
```

[25] HERTZOG, Raphaël a Roland MAS. The Debian Administrator's Handbook. Freexian, 2013, s. 464 ISBN 979-10-91414-02-9. s. 271-274.

- tvorba diskových obrazů

Úloha nejprve v úložišti TFTP serveru vytvoří adresář s názvem stanice a naplní jej soubory:

```
initrd.img.netboot                    (inicializační RAM disk)
pxelinux.0                            (lehký zavaděč pro PXE)
vmlinuz                               (jádro systému)
```

Dále vytvoří podadresář **`pxelinux.cfg`**, kam vygeneruje konfigurační soubor s názvem **`default`** obsahující specifikaci jádra, inicializačního RAM disku, způsobu získání IP konfigurace a cestu k NFS úložišti s diskovým obrazem celého systému:

```
DEFAULT vmlinuz root=/dev/nfs initrd=initrd.img.netboot ip=dhcp rw
nfsroot=10.  .  .  :/nfs/tc010
```

V úložišti NFS serveru poté vytvoří opět adresář s názvem stanice, do kterého rozbalí celý obsah tar archivu s klonem diskového obrazu stanice. Následně podle údajů z databáze přepíše obsah souborů **`/etc/hostname`** a **`/etc/hosts`** skutečnými údaji.

- odstranění diskových obrazů

Provede odstranění adresářů příslušné stanice z TFTP a NFS úložiště.

Protože ke změnám konfigurace dochází jen minimálně, neběží aplikace na serveru trvale jako služba, ale je spouštěna v pravidelných časových intervalech pomocí plánovače cron. Tím došlo ke zjednodušení, které má však nevýhodu při zpracování většího počtu úloh. Může se stát, že za běhu jedné instance aplikace by byla plánovačem spuštěna instance další, což by mohlo způsobit nežádoucí souběh (race-condition) ve zpracování rozvrhu úloh. Je nutné ošetřit, aby na serveru mohla běžet pouze jedna instance této aplikace. To je provedeno zápisem příznaku aktivity do databáze. Díky tomu má i správce zpětnou vazbu o tom, že aplikace na PXE serveru právě běží a zpracovává úlohy.

Zdrojový kód programu je zapsán v jazyce Java do jediného balíčku („pxe“), který obsahuje třídy zajišťující vlastní logiku programu, zpracování konfigurace, napojení na databázi, implementaci obsluhy jednotlivých typů úloh a logování do souboru.

Detailnější popis struktury programu pro správu PXE serveru je uveden v příloze C.

5.7 Správa infrastruktury

Prostředí pro konfiguraci infrastruktury tenkých klientů je zpracováno jako webový management. Bude tak dostupné přes libovolný internetový prohlížeč, kde administrátorovi poskytne nástroje k modifikaci jednotlivých součástí infrastruktury, nebo vybrané informace o uživatelích využitelné pro jejich podporu. Vzhled aplikace je navržen velmi jednoduše a jde o kombinaci přehledových a editačních formulářů.

K dispozici jsou zejména formuláře pro editaci a zobrazení:

- základních parametrů infrastruktury,
- tenkých klientů,
- tiskáren,
- terminálových serverů,
- organizační struktury (lokality, nákladová střediska),
- uživatelů.

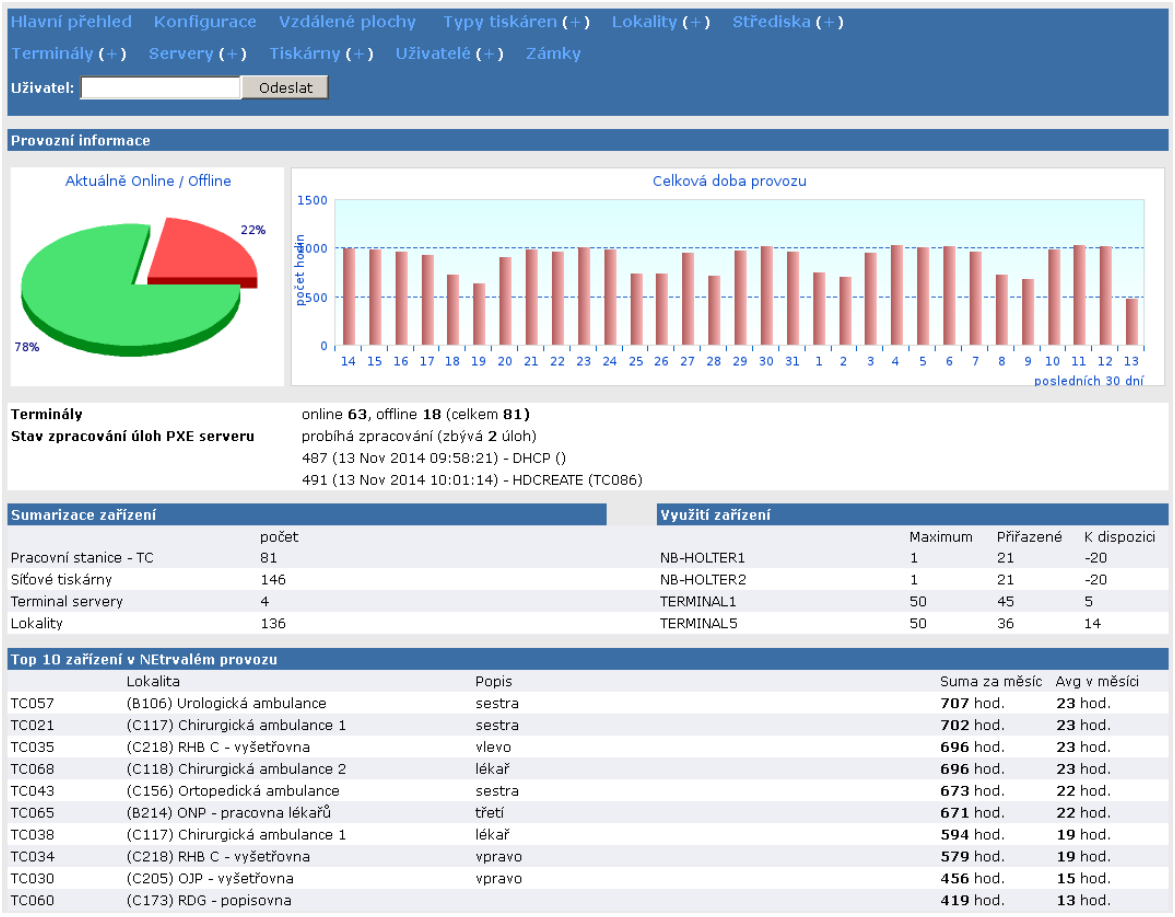
Je zde také jednoduchý úvodní dashboard, kde jsou uvedeny vybrané aktuální provozní nebo statistické údaje.

5.7.1 Volba http serveru

Webový management je provozován na stroji s operačním systémem Windows Server 2008 R2, který disponuje webovým serverem IIS (Internetové informační služby) přímo jako jednou z rolí. Přesto však byl zvolen opensource projekt Apache httpd, což je nejpopulárnější webový server na Internetu od dubna 1996. Na vývoji projektu se podílí nadace Apache Software s cílem vyvíjet a udržovat opensource http server pro moderní operační systémy zahrnující Unix a Windows Server a poskytovat bezpečný, výkonný a rozšiřitelný server, který nabízí http služby podle současných standardů.[26] Důvodem byly především dosavadní zvyklosti v organizaci.

[26] THE APACHE SOFTWARE FOUNDATION. Apache HTTP SERVER PROJECT [online]. [cit. 2014-11-13]. Dostupné z: http://httpd.apache.org/

5.7.2 Dashboard



	počet
Pracovní stanice - TC	81
Síťové tiskárny	146
Terminal servery	4
Lokality	136

	Maximum	Přiřazené	K dispozici
NB-HOLTER1	1	21	-20
NB-HOLTER2	1	21	-20
TERMINAL1	50	45	5
TERMINAL5	50	36	14

	Lokalita	Popis	Suma za měsíc	Avg v měsíci
TC057	(B106) Urologická ambulance	sestra	**707** hod.	**23** hod.
TC021	(C117) Chirurgická ambulance 1	sestra	**702** hod.	**23** hod.
TC035	(C218) RHB C - vyšetřovna	vlevo	**696** hod.	**23** hod.
TC068	(C118) Chirurgická ambulance 2	lékař	**696** hod.	**23** hod.
TC043	(C156) Ortopedická ambulance	sestra	**673** hod.	**22** hod.
TC065	(B214) ONP - pracovna lékařů	třetí	**671** hod.	**22** hod.
TC038	(C117) Chirurgická ambulance 1	lékař	**594** hod.	**19** hod.
TC034	(C218) RHB C - vyšetřovna	vpravo	**579** hod.	**19** hod.
TC030	(C205) OJP - vyšetřovna	vpravo	**456** hod.	**15** hod.
TC060	(C173) RDG - popisovna		**419** hod.	**13** hod.

Obrázek 12: Dashboard

Zdroj: Vlastní zpracování

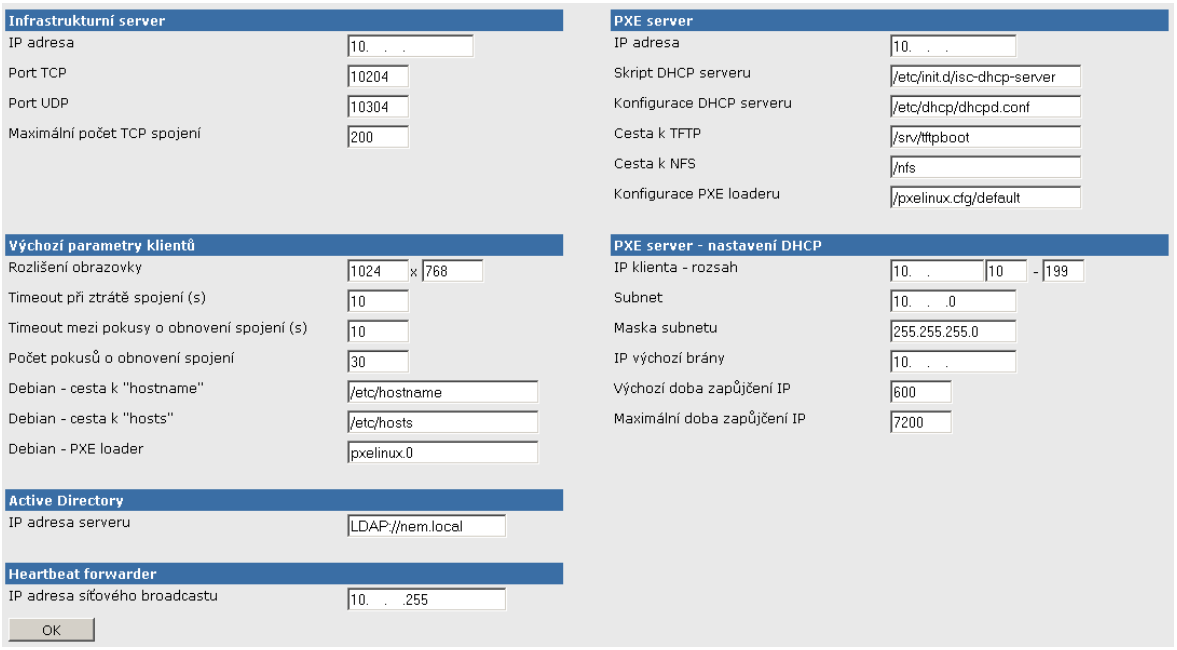
Dashboard představuje úvodní stránku webového rozhraní. V horní části je ve všech formulářích k dispozici menu, které umožňuje rychlý přístup do přehledů nebo pomocí ovládacího prvku (+) spuštění editačních formulářů pro přímé zakládání nových položek. Dále zobrazuje základní informace o infrastruktuře:

- koláčový graf - aktuální počet spuštěných stanic,
- sloupcový graf - celková provozní doba stanic v hodinách v posledních 30 dnech,
- stav zpracování úloh PXE serveru – přehled jednotlivých prováděných úloh,
- sumarizace zařízení – celkový výskyt zařízení (stanic, tiskáren, serverů) a lokalit v infrastruktuře,
- využití zařízení – alokace stanic na terminálové servery,

- top 10 zařízení netrvalého provozu – identifikace míst, kde může docházet k delšímu provozu zařízení než se předpokládá (typicky pokud uživatelé terminály nevypínají).

5.7.3 Základní konfigurace

Slouží k nastavení parametrů jednotlivých modulů celého řešení. Protože se nepočítá s přítomností více infrastrukturních ani PXE (resp. DHCP) serverů, mohlo dojít ke zjednodušení a sjednocení konfigurace do jednoho formuláře. Kromě toho je zde možné nastavit společné parametry tenkých klientů, napojení na Active Directory nebo cílovou adresu heartbeat forwarderu. Při použití formuláře je třeba brát na vědomí, že změny nastavení infrastrukturního serveru se projeví až po jeho restartu. V případě PXE (resp. DHCP) serveru dochází k aktualizaci prakticky okamžitě, protože software na serveru je spouštěn v pravidelných intervalech časovačem.



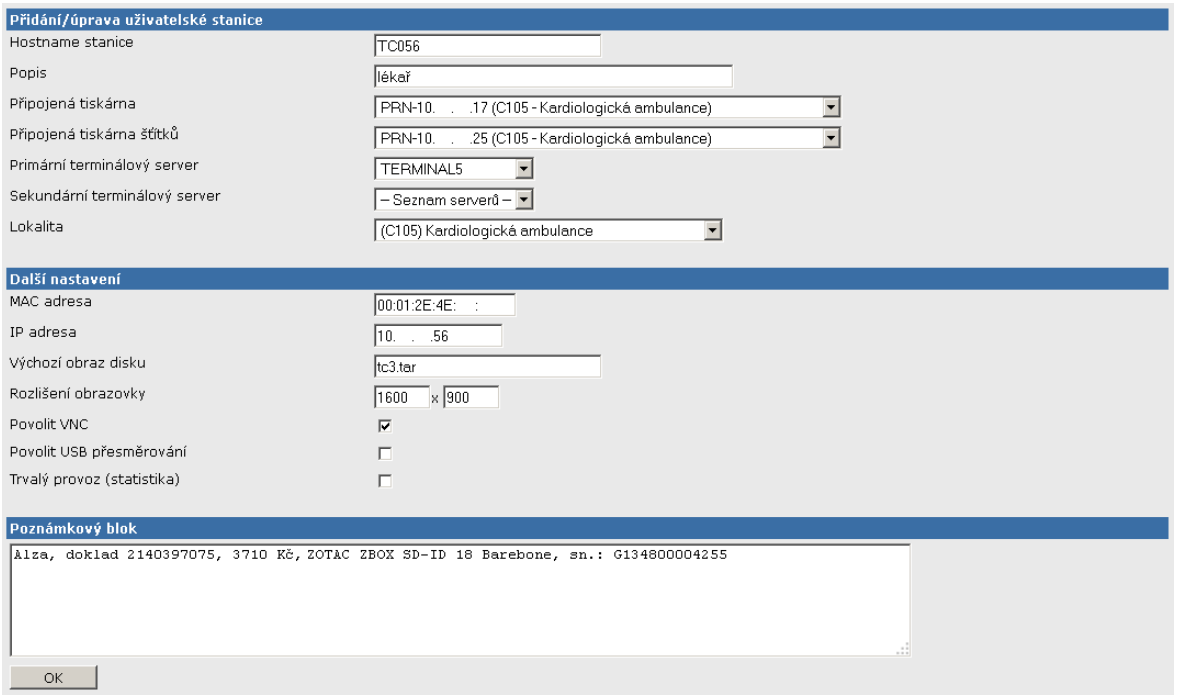
Obrázek 13: Základní konfigurace

Zdroj: Vlastní zpracování

Na tomto ani dalších obrázcích nebudou uváděny reálné IP adresy v kompletním tvaru.

5.7.4 Správa tenkých klientů

Umožňuje zobrazit stanice, sledovat jejich využití, přiřazovat disponibilní vzdálené plochy, vykazovat servisní práce a editovat nastavení. To se provádí pomocí jednoduchého formuláře, kde část z údajů vyplní správce ručně a zbylé vybírá ze seznamů, což napomáhá eliminovat chyby v zadání a udržet kvalitu dat. Ve spodní části je připraven poznámkový blok, kam lze volným textem zapsat doplňující informace. Při ukládání formuláře se na pozadí automaticky generují příslušné úlohy pro PXE server.



Obrázek 14: Konfigurace stanice

Zdroj: Vlastní zpracování

Konfigurují se následující parametry:

- síťové nastavení - HOSTNAME, MAC adresa, IP adresa,
- přidělené tiskárny – pro tisk dokumentů a pro tisk štítků,
- primární terminálový server (případně sekundární k zajištění vysoké dostupnosti),
- umístění zařízení a doplňující popis,
- rozlišení připojené obrazovky (nastavení se vynutí pokud jej displej podporuje),
- výchozí obraz disku - název archivu ve formátu tar s obrazem operačního systému stanice uloženém na PXE serveru.

Dále příznaky:

- aktivace VNC serveru - umožní správci vzdálený přístup na konkrétní stanici pomocí jednorázového, náhodně vygenerovaného hesla,
- aktivace USB přesměrování - má uživatelům na dané stanici umožnit přesměrování vybrané USB periferie (typicky flash disku) do vzdálené plochy,
- trvalého provozu - slouží pro rozlišení stanic s předpokládaným permanentním provozem, má význam pro některé přehledy (viz. Dashboard).

Přehledový formulář zobrazuje všechny stanice a vybranou část výše uvedených údajů. Disponuje indikací stavu podbarvením v pravé části (zelené = online, červené = offline) a obsahuje navigační ikony pro přechod do dalších formulářů (editace, přiřazení vzdálených ploch, přehled využití a výkaz servisu nebo smazání záznamu). Umožňuje také přímý proklik do webového managementu tiskáren.

Seznam uživatelských stanic (TC) EXPORT

Terminál/ MAC	IP adresa	Rozlišení	Tiskárna	Terminal	Lokalita	Popis
TC012 (00:01:2E:4C: :)	10. . .12 VNC: jzwd3Buj	1600x900	PRN-10. . .114 PRN-10. . .19 (Š)	TERMINAL1	(B103) Závodní ambulance	sestra
TC048 (00:01:2E:4D: :)	10. . .48 VNC: hHotrzq5	1600x900	PRN-10. . .114 PRN-10. . .19 (Š)	TERMINAL5	(B103) Závodní ambulance	lékař
TC080 (00:01:2E:55: :)	10. . .80 VNC: n3mnnfaK	1600x900	PRN-10. . .139	TERMINAL1	(B104) Plicní ambulance	sestra
TC081 (00:01:2E:55: :)	10. . .81 VNC: 4uWoxjof	1600x900	PRN-10. . .139	TERMINAL5	(B104) Plicní ambulance	lékař
TC057 (00:01:2E:4D: :)	10. . .57 VNC: kyhtvCy0	1280x1024	PRN-10. . .70 PRN-10. . .20 (Š)	TERMINAL1	(B106) Urologická ambulance	sestra
TC058 (00:01:2E:4E: :)	10. . .58 VNC: Hrdcc0er	1280x1024	PRN-10. . .70 PRN-10. . .20 (Š)	TERMINAL5	(B106) Urologická ambulance	lékař

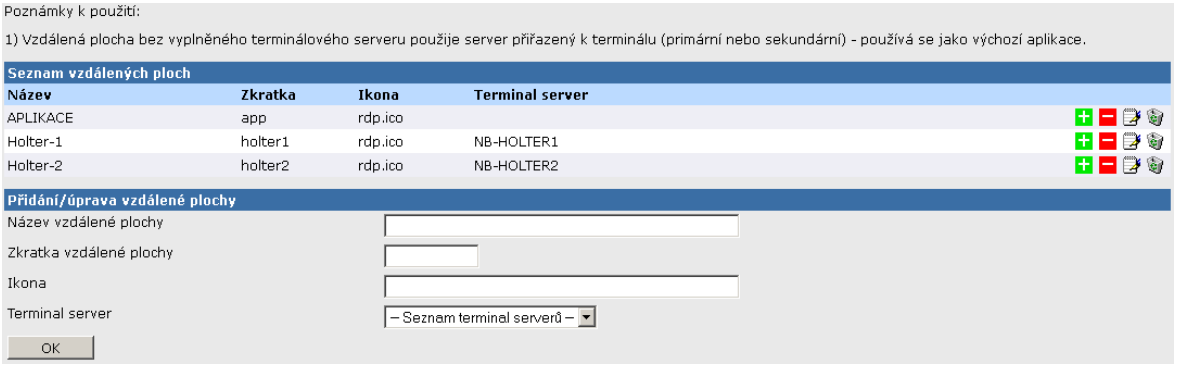
Obrázek 15: Přehled stanic

Zdroj: Vlastní zpracování

Není-li vyžadována vysoká dostupnost jednotlivých stanic, je vhodné v rámci jedné lokality alokovat stanicím různé terminálové servery, aby v případě výpadku některého z nich nedošlo k úplném přerušení provozu na pracovišti.

Tenký klient má umožnit připojení na jednu nebo více vzdálených ploch, což prakticky znamená na několik různých terminálových serverů. Dosavadní konfigurace však počítá pouze se dvěma servery (primárním a sekundárním), které jsou přiřazeny stanici a jejichž použití nemůže uživatel ovlivnit. Je nutné najít způsob, jak zpřístupnit i další servery.

Z toho důvodu byl zaveden pomocný záznam, nazývaný jako vzdálená plocha, ke kterému lze přiřadit libovolný z dostupných terminálových serverů. Tyto vzdálené plochy mohou být potom přiřazeny stanicím. Konfigurační formulář obsahuje kromě již známých ovládacích prvků také ikony pro hromadné přidělení (+) nebo hromadné odebrání (−) konkrétní vzdálené plochy všem stanicím.

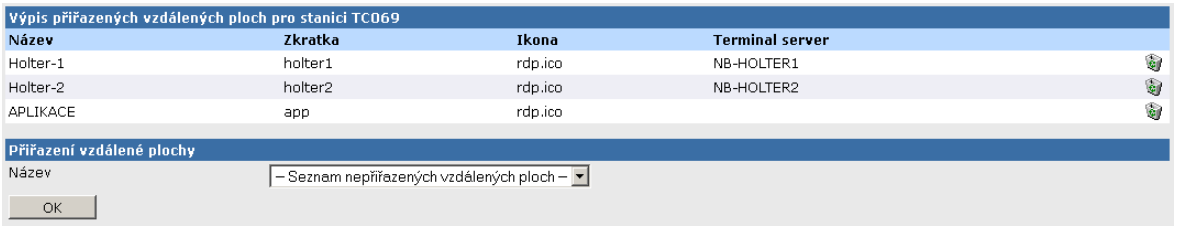


Obrázek 16: Konfigurace vzdálených ploch

Zdroj: Vlastní zpracování

Pro nastavení vzdálených ploch platí:

- není-li zvolen terminálový server = stanice použije ten ze své konfigurace,
- je-li zvolen terminálový server = stanice explicitně použije tento server, ale pak není zajištěna redundance pokud dojde k jeho výpadku.

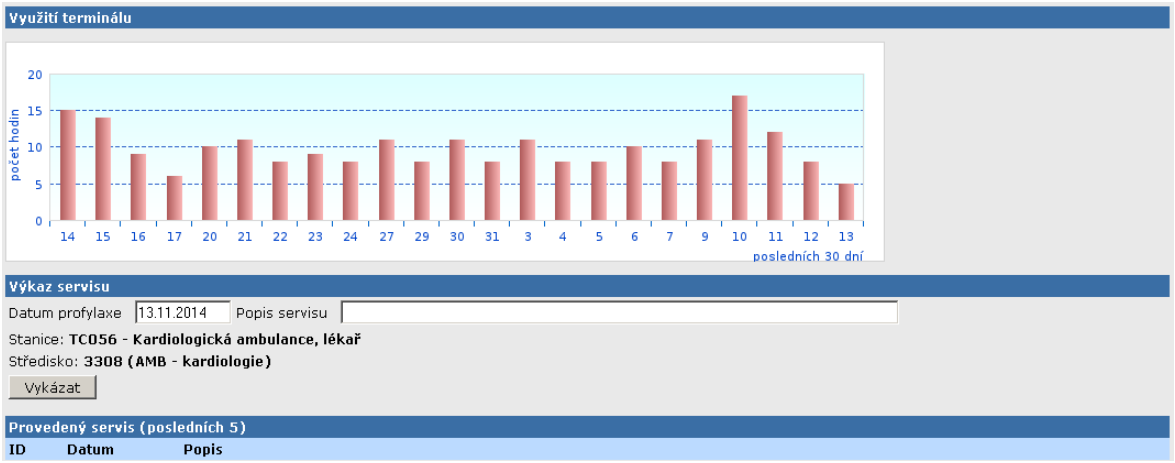


Obrázek 17: Přidělení vzdálených ploch

Zdroj: Vlastní zpracování

Na předcházejícím obrázku je znázorněn formulář pro přidělování vzdálených ploch jednotlivé stanici. V uvedeném příkladu vzdálená plocha „APLIKACE“ využije terminálových serverů z konfigurace stanice, naopak plocha s názvem „Holter-1“ použije uvedený server NB-HOLTER1.

U stanic je možné zobrazit celkovou provozní dobu v hodinách v posledních 30 dnech. Na stejném formuláři lze také vykazovat provedené servisní nebo profylaktické práce.



Obrázek 18: Přehled využití stanice a výkaz servisu

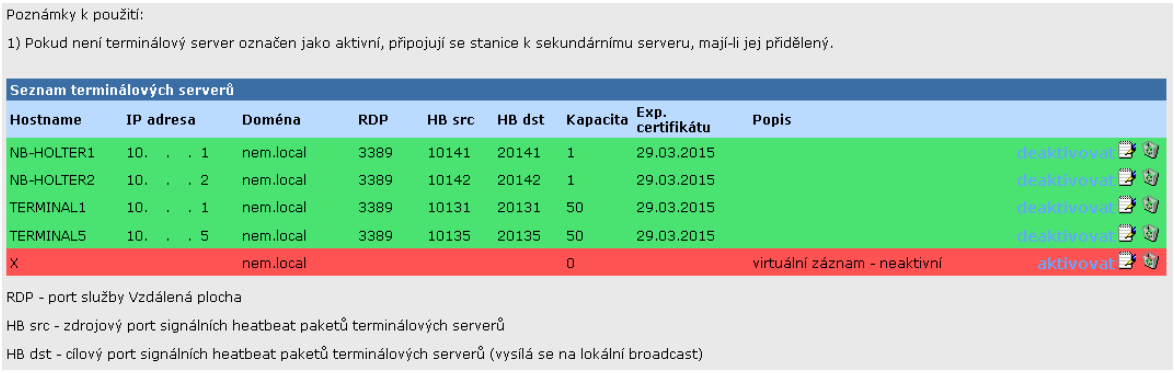
Zdroj: Vlastní zpracování

5.7.5 Správa terminálových serverů

Podobně jako u tenkých klientů je i u terminálových serverů k dispozici editační formulář, kde lze modifikovat následující parametry:

- síťové nastavení terminálových serverů - HOSTNAME, IP adresu, doménu služby Active Directory, port RDP a porty určené pro signální pakety (HB src, HB dst),
- správcem předpokládaný maximální počet připojených stanic (uživatelů),
- doplňující popis,
- datum expirace certifikátu pro připojení ke vzdálené ploše,
- otisk certifikátu v podobě dvaceti dvojic hexadecimálních čísel.

Přehledový formulář rozlišuje podbarvením aktivní a neaktivní terminálové servery (zelené = aktivní, červené = neaktivní). Vzhledem k dosavadním zkušenostem z praktického provozu nebyla do infrastrukturního serveru implementována logika, která by vyhodnocovala reálnou provozuschopnost terminálových serverů. Z toho důvodu je rozhodnutí o jejich stavu ponecháno na administrátorovi, který je může na seznamu aktivovat nebo deaktivovat. Podle toho poté probíhá jejich přidělování stanicím. Na formuláři nechybí navigační ikona pro přechod k editaci ( ) nebo ikona pro mazání záznamů ( ).



Poznámky k použití:

1) Pokud není terminálový server označen jako aktivní, připojují se stanice k sekundárnímu serveru, mají-li jej přidělený.

Seznam terminálových serverů

Hostname	IP adresa	Doména	RDP	HB src	HB dst	Kapacita	Exp. certifikátu	Popis	
NB-HOLTER1	10. . . 1	nem.local	3389	10141	20141	1	29.03.2015		deaktivovat
NB-HOLTER2	10. . . 2	nem.local	3389	10142	20142	1	29.03.2015		deaktivovat
TERMINAL1	10. . . 1	nem.local	3389	10131	20131	50	29.03.2015		deaktivovat
TERMINAL5	10. . . 5	nem.local	3389	10135	20135	50	29.03.2015		deaktivovat
X		nem.local				0		virtuální záznam - neaktivní	aktivovat

RDP - port služby Vzdálená plocha

HB src - zdrojový port signálních heatbeat paketů terminálových serverů

HB dst - cílový port signálních heatbeat paketů terminálových serverů (vysílá se na lokální broadcast)

Obrázek 19: Přehled terminálových serverů

Zdroj: Vlastní zpracování

5.7.6 Správa tiskáren

Je třetí částí konfigurace zařízení. Umožňuje zobrazit a editovat tiskárny, sledovat jejich využití nebo vykazovat spotřební materiál.

Konfigurují se následující parametry:

- název tiskárny – tak jak je uveden na tiskovém serveru,
- IP adresa – slouží pro testování dostupnosti tiskárny,
- umístění zařízení a doplňující popis,
- typ tiskárny – pro účely výkaznictví spotřebního materiálu.

Přehledový formulář zobrazuje všechny zadané údaje a navíc poskytuje informaci o aktuálním využití tiskárny (kolika stanicím je přiřazena). Zeleným zvýrazněním jsou indikovány ty tiskárny, které nejsou v danou chvíli asociovány k žádné pracovní stanici. Na formuláři nechybí navigační ikony pro přechod do dalších formulářů (editace, přehled využití a výkaz spotřebního materiálu nebo smazání záznamu).

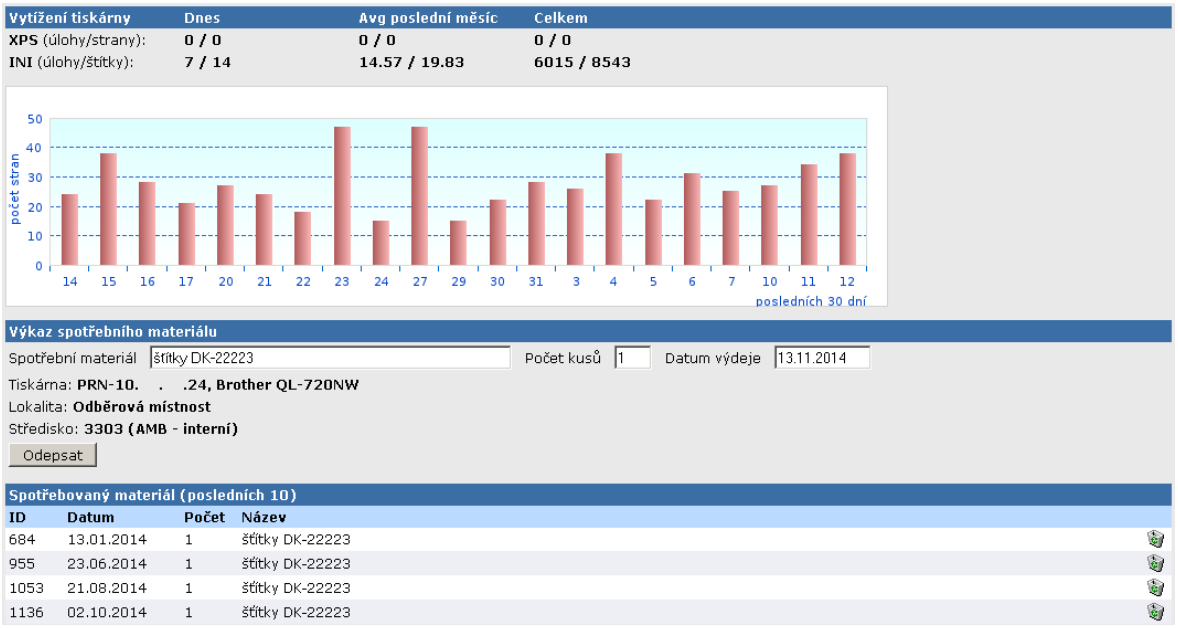
Seznam tiskáren EXPORT

Název tiskárny	IP adresa	Typ	Lokalita	Popis	Využití
PRN-10. . .130	10. . .130	Canon 2380i	(A203) Sekretariát		4
PRN-10. . .114	10. . .114	HP 1606dn	(B103) Závodní ambulance		2
PRN-10. . .19	10. . .19	Brother QL-720NW	(B103) Závodní ambulance		2
PRN-10. . .139	10. . .139	HP 1606dn	(B104) Plicní ambulance		2
PRN-10. . .89	10. . .89	HP CM2320nf MFP	(B105) Sociální pracovnice		1
PRN-10. . .70	10. . .70	HP 1606dn	(B106) Urologická ambulance		2
PRN-10. . .20	10. . .20	Brother QL-720NW	(B106) Urologická ambulance		2

Obrázek 20: Přehled tiskáren

Zdroj: Vlastní zpracování

Kompletní evidence tiskáren byla využita pro zavedení velmi jednoduchého výkaznictví spotřeby tiskového materiálu. Zaměstnanec podpory provádí při jeho výdeji záznam do formuláře, kde má předvyplněny konkrétní údaje (typ materiálu podle typu tiskárny a nákladové středisko podle lokality). Nasbíraná data je možné následně vyexportovat do účetního programu. Na stejném formuláři jsou k dispozici také informace o vytížení tiskárny za různá časová období – sledují se počty úloh a počty listů (štítků).



Obrázek 21: Přehled vytížení tiskárny a výkaz spotřebního materiálu

Zdroj: Vlastní zpracování

5.7.7 Zámky

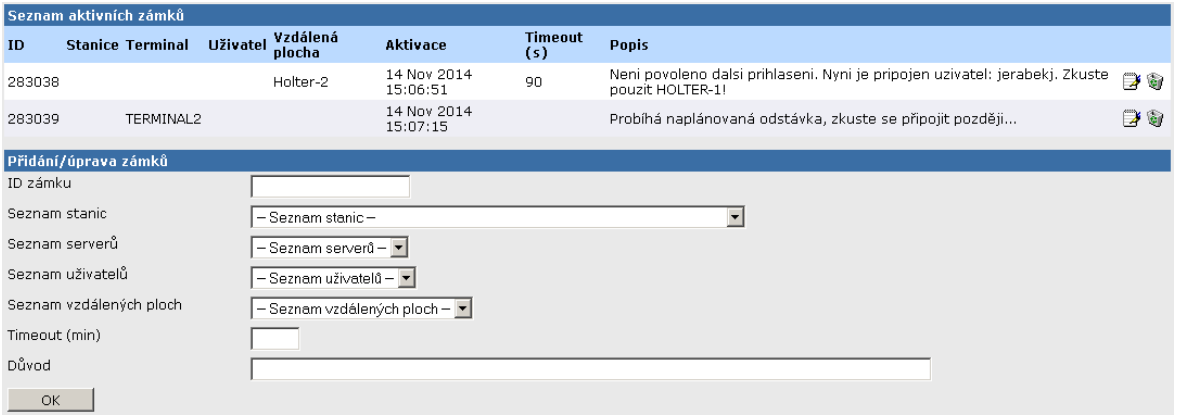
Zámky jsou funkcí, která umožňuje zablokovat připojení ke vzdálené ploše. Využijí se zejména při upgradech softwaru nebo haváriích, kdy uživateli znemožní připojení a zároveň mohou podat zprávu o příčině, odhadu doby řešení a dalších detailech problému. Uživatel je ihned informován a nemusí zbytečně kontaktovat technickou podporu.

Zámek je aplikovatelný na:

- terminálový server,
- stanici,
- uživatele,
- vzdálenou plochu.

Lze přesně specifikovat dobu trvání uzamčení, kdy po jejím vypršení dojde k automatickému odstranění zámku. Pokud se jedná o zámek s neomezenou platností, je nutné provést jeho smazání manuálně. Formulář obsahuje navigační ikonu pro přechod k editaci ( ) nebo ikonu pro mazání zámků ( ).

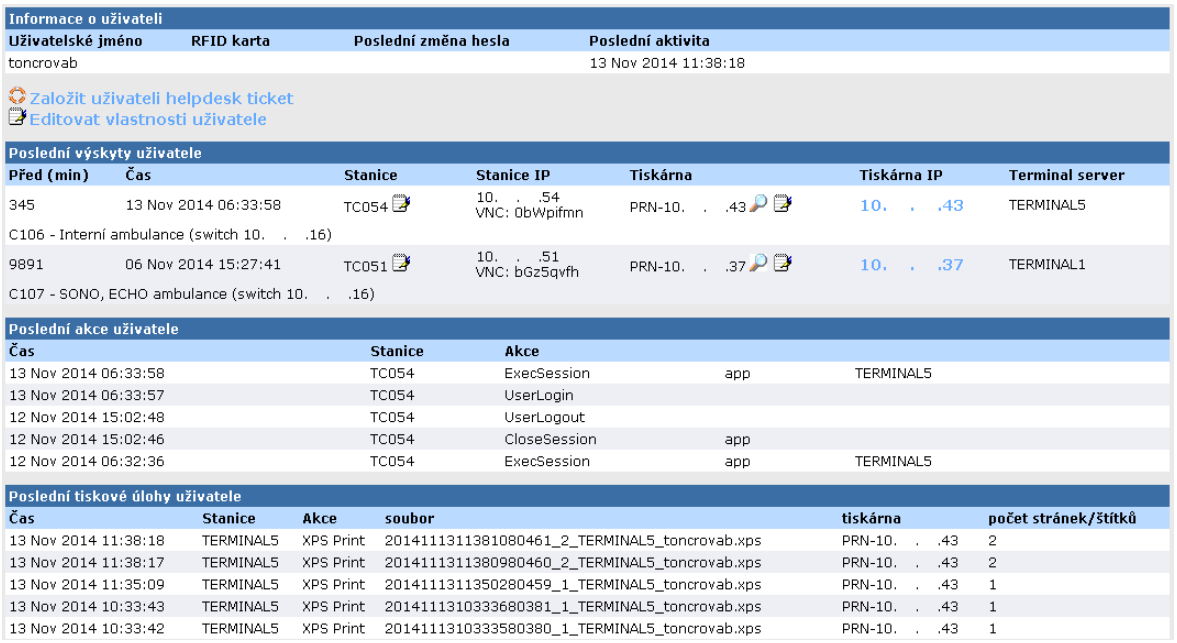
Zámky mohou být generovány také automaticky některou z aplikací, která s jejich pomocí zajišťuje exkluzivitu vybraných prostředků.



Obrázek 22: Přehled a editace zámků

Zdroj: Vlastní zpracování

5.7.8 Přehled uživatele



Obrázek 23: Přehled uživatele

Zdroj: Vlastní zpracování

Formulář koncentruje dostupné informace týkající se konkrétního uživatele a umožňuje přímý přechod do systému uživatelské podpory (Helpdesk).

V sekci *poslední výskyty* lze na první pohled vidět pracovní stanici, tiskárnu, lokalitu, terminálový server nebo switch, které uživatel ke své práci naposledy použil. K dispozici jsou také navigační ikony pro přímé spuštění editačního formuláře u konkrétního zařízení (), nebo formuláře pro výkaz spotřebního materiálu u tiskáren (). Stránka dále zobrazuje *poslední akce uživatele* (přihlášení, odhlášení, připojení ke vzdálené ploše apod.) nebo *seznam nejnovějších tiskových úloh* přijatých z terminálových serverů.

6 Zhodnocení výsledků a doporučení

Výsledkem této diplomové práce je funkční a ekonomicky atraktivní řešení, které využívá v rutinním provozu Rehabilitační Nemocnice Beroun a Nemocnice Hořovice.

Obrázek 24: Ukázka pracoviště vybaveného tenkými klienty ZOTAC ZBOX SD-ID18
Zdroj: Vlastní zpracování

Vlastní realizace započala experimentální instalací nezávislého tenkého klienta se systémem Debian Wheezy 7.0. K tomu byla vytvořena první verze klientské aplikace a infrastrukturního serveru. Na čtyřech terminálech byl zahájen měsíční ověřovací provoz na vybraném pracovišti nemocnice s využitím existujících terminálových serverů.

Během tohoto období se ukázaly problémy především v implementaci RDP klienta (freerdp-x11), který byl standardní součástí distribuce. Šlo o chybnou interpretaci rozložení kláves u některých národních klávesnic (včetně české), kde na vzdálené ploše docházelo

k záměně některých znaků, dále k chybné synchronizaci stavu přepínačů NumLock, CapsLock či ScrollLock. Dalším problémem byl citelný nárůst síťového provozu ve srovnání s klientem RDP provozovaným pod operačním systémem Windows 7. Docházelo také k nahodilým chybám grafiky, kdy chyběly některé oblasti zobrazení. Pokud navíc došlo k výpadku WAN sítě na dobu delší jak deset sekund, bylo nutné proces RDP klienta ukončit a znovu spustit. Většinu problémů se následně podařilo odstranit instalací poslední stabilní verze softwaru přímo z repositáře webové služby GitHub. Problém při výpadku WAN sítě byl vyřešen vlastní cestou pomocí UDP signalizace.

Současně probíhaly práce na řešení síťového zavádění operačního systému. K tomu byla zvolena jednoduchá varianta spočívající ve zpřístupnění obrazu pevného disku prostřednictvím NFS. Každý tenký klient má na serveru svůj diskový obraz, naklonovaný z určeného výchozího obrazu. Nevýhodou tohoto řešení je vysoká redundance, neboť diskové obrazy jsou prakticky identické. Z toho plyne vyšší náročnost na výkon úložiště i jeho kapacitu. V důsledku toho může dojít ke zpomalení startu jednotlivých zařízení, je-li spuštěn jejich větší počet ve stejném čase.

Řešení se ukázalo jako životaschopné a bylo rozhodnuto o dalším rozšíření. Došlo ke zhotovení webového managementu pro konfiguraci a správu infrastruktury, zakoupení nových terminálových serverů a postupnému nahrazování zastaralých desktopů novými tenkými klienty. Vše probíhalo za plného provozu bez omezení uživatelů. Díky důrazu na maximální jednoduchost kontaktního prostředí klientské aplikace nebylo vůbec potřeba provádět proškolení uživatelů. Ti byli schopni s novými stanicemi okamžitě pracovat a neskrývali překvapení z fyzické velikosti a naprosto tichého provozu. Vzhledem k jejich častému pohybu mezi různými pracovišti ocenili také objektivně rychlejší procesy přihlašování, odhlašování nebo startu zařízení vzhledem k běžným desktopům.

Již v zadání byl projekt fixován na využití technologie firmy Microsoft. Hlavními důvody byly zakoupené softwarové licence a snaha o minimální zásah do funkční infrastruktury. Za výhodu lze považovat dlouhodobou předchozí zkušenost, během které se podařilo vyřešit celou řadu problémů, se kterými se v rámci této práce nebylo potřeba zabývat (např. tisková řešení). Jistou nevýhodou je použití RDP protokolu, který očividně za svými

konkurenty PCoIP nebo ICA zaostává. V praxi se bohužel potvrdily závěry výkonnostních testů, uvedených v teoretické části, kdy například při přehrávání videozáznamů došlo k výraznému nárůstu síťového provozu a praktickému paralyzování WAN sítě jediným tenkým klientem. Vzhledem k tomu, že uživatelé ke své pracovní činnosti multimédia nepotřebují, nešlo o kritický problém. Na straně terminálových serverů byla možnost přehrávat videozáznamy jednoduše zablokována.

Realizovaná infrastruktura tenkých klientů na bázi prezentační virtualizace představuje jeden z řady možných moderních způsobů, jak vytvořit informační infrastrukturu v organizaci větší velikosti. V případě této konkrétní práce lze výsledek doporučit k nasazení do provozů, kde se očekává převážně použití aplikací kancelářského typu bez vysokých nároků na multimediální výkon. Řešení splňuje předem deklarovaná očekávání (zjednodušení a zlevnění provozu a správy díky centralizaci, snížení spotřeby elektrické energie či zvýšení zabezpečení) a v reálném provozu vykazuje prozatím naprostou spolehlivost.

Projekt je možné v případě potřeby dále rozvíjet a nabízí prostor pro implementaci nových funkcí. Na realizaci čeká možnost přesměrování různých USB periferií do vzdálené plochy, které je rozpracováno, ačkoli nebylo prvotně požadováno. Webové konfigurační rozhraní by jistě dokázalo nabídnout ještě detailnější přehledy, více podrobnějšího nastavení nebo modernější vzhled. Velký posun k nezávislosti by znamenalo vytvoření vlastního tiskového ovladače virtuální tiskárny pro generování souborů tiskové fronty. Slabšími místy bez zásadního dopadu na zdejší provoz jsou vysoká redundance dat na PXE serveru díky prakticky stejnému obsahu jednotlivých diskových obrazů tenkých klientů nebo manuální řízení infrastruktury při potenciálním výpadku některého z terminálových serverů. Sofistikovanější řešení těchto oblastí by mohlo být přínosem v případě ještě rozsáhlejšího nasazení.

7 Závěr

Při zpracování této diplomové práce jsem využil nově získaných znalostí při studiu na České zemědělské univerzitě a svých dosavadních zkušeností z praxe. Mohl jsem tak úspěšně zrealizovat komplexní projekt, vyžadující přehled napříč informatickými disciplínami. Ať už jde o principy operačních systémů, počítačové sítě, databázové systémy či internetové technologie. Podstatná část práce spočívala v instalaci a přizpůsobení operačních systémů, v naprogramování webového managementu v PHP a zhotovení několika aplikací v jazyce Java, kde šlo především o práci se sítí, grafickým rozhraním nebo o tvorbu vícevláknových aplikací.

Cíl práce, stanovený v jejím úvodu, se podařilo splnit. V teoretické části bylo provedeno srovnání jednotlivých infrastrukturních řešení reprezentovaných standardní desktopovou infrastrukturou, infrastrukturou pro prezentační virtualizaci a virtuálními desktopy (VDI). Byly charakterizovány vlastnosti jednotlivých modelů a komunikačních protokolů, které se obvykle využívají. Zmíněno bylo i ekonomické hledisko, které se zabývalo věcí z pohledu pořizovacích a provozních nákladů, s využitím ukazatelů TCO (Total Cost of Ownership) a ROI (Return on Investment).

Praktická část práce byla zahájena představením organizace, analýzou tamějšího ICT prostředí a stručným popisem jeho aktuálního stavu. Na základě požadavků managementu byly představeny možnosti řešení a jejich finanční vyjádření formou orientačního výpočtu TCO v pětiletém životním cyklu. Výsledkem bylo očekávané rozhodnutí zajistit v organizaci revitalizaci zastaralého hardwarového vybavení a reimplementaci stávající infrastruktury využívající prezentační virtualizaci. Podle modelových výpočtů i aktuálních trendů v oblasti informačních technologií bylo k naplnění požadavků zvoleno řešení prostřednictvím infrastruktury tenkých klientů.

Vlastní realizace se zabývala především instalací terminálových serverů s operačním systémem Windows Server 2008 R2, instalací tenkých klientů a PXE serveru s operačním systémem Debian Wheezy 7.5. Ten slouží pro realizaci startu jednotlivých zařízení přímo ze sítě bez nutnosti použití paměťového média. K tomuto účelu bylo nutné přizpůsobit diskový obraz nainstalovaného tenkého klienta pro síťové zavádění. Aby bylo řešení

funkční jako celek, došlo k vytvoření několika dalších softwarových produktů: klientské aplikace pro tenkého klienta, infrastrukturního serveru, modulu pro správu PXE serveru a webového rozhraní pro konfiguraci celé infrastruktury. Využito bylo vlastního osvědčeného tiskového serveru, který je v organizaci používán již několik let. Všechny součásti infrastruktury jsou bezchybně funkční.

Po pilotním zkušebním provozu na vybraném pracovišti Rehabilitační nemocnice Beroun došlo k nahrazení většiny zastaralých desktopových stanic novými tenkými klienty. Aktuálně je zde v provozu téměř 100 takových zařízení, přičemž postupně dochází k navyšování jejich počtu v souvislosti s odpisem dalších nevyhovujících osobních počítačů a pozvolným nárůstem pracovišť. Projekt se podařilo rozšířit také do partnerské Nemocnice Hořovice, kde aktuálně probíhá instalace a je zde v provozu přibližně 50 tenkých klientů, přičemž očekávaný stav je až trojnásobný.

Práci lze nyní uzavřít tak, že se podařilo vytvořit na míru zpracované, funkční, ekonomicky atraktivní a především rutinně využívané řešení, přinášející prokazatelný užitek, úsporu času i finančních prostředků a nabízející možnosti pro další budoucí rozšíření nebo přizpůsobení.

Seznam použitých zdrojů a literatury

- FRIČ, Michal. Virtualizační technologie. [online]. [cit. 2014-11-13].Dostupné z: http://hippo.feld.cvut.cz/vrbata/gopas/virtualizace-uvod.pdf

- HERTZOG, Raphaël a Roland MAS. The Debian Administrator's Handbook. Freexian, 2013, s. 464. ISBN 979-10-91414-02-9.

- IETF. RFC 1094 - NFS: Network File System Protocol specification. [online]. [cit. 2014-11-13]. Dostupné z: http://tools.ietf.org/html/rfc1094

- IETF. RFC 1350 - The TFTP Protocol (Revision 2). [online]. [cit. 2014-11-13]. Dostupné z: http://tools.ietf.org/html/rfc1350

- INTEL CORPORATION. Preboot Execution Environment (PXE) Specification. [online]. [cit. 2014-11-13]. Dostupné z: ftp://download.intel.com/design/archives/wfm/downloads/pxespec.pdf

- JPGRAPH.NET. JpGraph: Most powerful PHP-driven charts. [online]. [cit. 2014-11-13]. Dostupné z: http://jpgraph.net

- KUKLA, Zdeněk. Řízení vzdálených aplikací v doméně MS Windows [online]. 2013 [cit. 2014-11-13]. Bakalářská práce. Vysoká škola finanční a správní. Vedoucí práce Jan Lánský. Dostupné z: http://is.vsfs.cz/th/22360/vsfs_b

- MICROSOFT. Hostitel relací vzdálené plochy (hostitel relací VP) [online]. [cit. 2014-11-13]. Dostupné z: http://technet.microsoft.com/cs-cz/library/cc742822

- MICROSOFT. Licence pro klientský přístup k Vzdálené ploše (VP CAL) [online]. [cit. 2014-11-13]. Dostupné z: http://technet.microsoft.com/cs-cz/library/cc753650

- MICROSOFT. Net user [online]. [cit. 2014-11-13]. Dostupné z: http://technet.microsoft.com/en-us/library/cc771865

- MICROSOFT. Remote Desktop Protocol [online]. [cit. 2014-11-13]. Dostupné z: https://msdn.microsoft.com/en-us/library/aa383015

- ORACLE. Java: The Best Environment for Network-Based Applications [online]. [cit. 2014-11-13]. Dostupné z: http://www.oracle.com/us/technologies/java/10045230-br-java-c17307-187867.pdf

- PETERKA, Jiří. Počítačové sítě, verze 3.0. [online]. [cit. 2014-11-13]. Dostupné z: http://www.earchiv.cz/l212/slide.php3?&l=12&me=2

- PHP.NET. What is PHP? [online]. [cit. 2014-11-13]. Dostupné z: http://php.net/manual/en/intro-whatis.php

- REIMER, Stan, Conan KEZEMA, Mike MULCARE, Byron WRIGHT. Windows server 2008 Active Directory: Resource Kit. Redmond: Microsoft Press, 2008, s. 827 ISBN 978-07-356-2515-0.

- RUEST, Danielle a Nelson RUEST. Virtualization, A Beginner´s Guide. The McGraw-Hill Companies, 2009, s. 442. ISBN 978-0-07-161402-3.

- RUNGE, Karl. x11vnc: a VNC server for real X displays. [online]. [cit. 2014-11-13]. Dostupné z: http://www.karlrunge.com/x11vnc

- SERWAN, Pawel. Dive into Citrix ICA protocol – Part1 [online]. [cit. 2014-11-13]. Dostupné z: https://pawelserwan.wordpress.com/2014/09/24/dive-into-citrix-ica-protocol-part1

- SOURCEFORGE.NET. Welcome to YAJSW. [online]. [cit. 2014-11-13]. Dostupné z: http://yajsw.sourceforge.net

- SYSLINUX.ORG. The Syslinux Project. [online]. [cit. 2014-11-13]. Dostupné z: http://www.syslinux.org/wiki/index.php/The_Syslinux_Project

- ŠVÍK, Martin. ROI, TCO a NPV: Svatá trojice. [online]. [cit. 2014-11-13]. Dostupné z: http://businessworld.cz/it-strategie/roi-tco-a-npv-svata-trojice-5303

- TERADICI.COM. Teradici PCoIP Solutions: About PCoIP technology. [online]. [cit. 2014-11-13]. Dostupné z: http://www.teradici.com/docs/default-source/resources/brochures/teradici-brochure-120817-web-2.pdf

- THE APACHE SOFTWARE FOUNDATION. Apache HTTP SERVER PROJECT [online]. [cit. 2014-11-13]. Dostupné z: http://httpd.apache.org

- WIKIPEDIA. Advanced Encryption Standard. [online]. [cit. 2014-11-13]. Dostupné z: http://cs.wikipedia.org/wiki/Advanced_Encryption_Standard

- VMWARE. VMware View PC-over-IP Performance and Best Practices [online]. [cit. 2014-11-13]. Dostupné z: http://image.slidesharecdn.com/euc1987-pcoip-improvements-110911145716-phpapp02/95/vmware-view-pcoip-performance-best-practices-26-728.jpg

Přílohy

Příloha A: Přehled programu klientské aplikace

Balíček	*Třída*	*Popis*
client	**Client.java**	**výchozí třída zajišťující chod celého programu**
	Config.java	zpracování konfiguračního souboru
	PasswordGenerator.java	generování náhodného hesla
	ThreadPwr.java	vlákno periodicky odesílající informace o zapnutém terminálu
	ThreadRdp.java	vlákno periodicky testující dostupnost terminálového serveru
	UDPListener.java	příjem UDP zpráv (heartbeat pakety z terminálových serverů)
	XFreeRDPConnect.java	proces spuštění RDP klienta
	XFreeRDPExitCodes.java	převod návratových kódu RDP klienta na textové zprávy
	XFreeRDPReconnect.java	proces obnovy vzdáleného připojení
client.commands	AbstractCommand.java	abstraktní třída zajišťující komunikaci s infrastrukturním serverem
	GetAppList.java	dotazování na seznam přiřazených vzdálených ploch
	GetAuthentication.java	dotazování na autentizaci uživatele dle uživatelského jména a hesla
	GetStationCfg.java	dotazování na konfiguraci stanice
	GetStationInf.java	dotazování na informace o stanici
	SendInfo.java	odesílání názvu stanice, verze softwaru a zašifrovaného VNC hesla
	SendLog.java	odesílání informace pro zápis do logovací tabulky v db
	SetPassword.java	odesílání požadavku na změnu přihlašovacího hesla
	StartSession.java	dotazování na parametry nutné pro sestavení relace vzdálené plochy
client.gui	ChangePassword.java	formulář pro změnu uživatelského hesla
	ImagePanel.java	zobrazení a pozicování tapety na pozadí
	MenuForm.java	přihlašovací formulář aplikace
	MenuFormLogged.java	formulář výběru vzdálených ploch po zalogování
	ReconnectPanel.java	obrazovka zobrazovaná při rozpadu RDP spojení

Tabulka 5: Přehled tříd programu klientské aplikace

Zdroj: Vlastní zpracování

Obsah konfiguračního souboru klienta:

```
# Client configuration
host= IP adresa infrastrukturního serveru
port= TCP port pro komunikaci
portudp= UDP port pro signalizaci
```

Zdrojové kódy programu jsou přiloženy na CD.

Příloha B: Přehled programu infrastrukturního serveru

Balíček	*Třida*	*Popis*
srv	ADAuthenticator.java	autentizace uživatele v Active Directory
	ClientConnHandler.java	obsluha spojení s klientem ve vlastním vlákně
	Config.java	zpracování konfiguračního souboru
	ConfigDB.java	zpracování konfigurace z databáze
	DB.java	napojení na databázi MS SQL
	LogWriter.java	zápis vybraných logovaných událostí do databáze
	Srv.java	**výchozí třída zajišťující chod programu**
	Server.java	TCP server
	UDPForwarder.java	UDP forwarder
	UDPListener.java	UDP listener
srv.handler	AbstractCmdHandler.java	abstraktní třída implementující rozhraní CmdHandler.java
	CmdHandler.java	definuje operaci, která se má provést po rozpoznání příkazu na serveru
	CmdHandlerFactory.java	vytváří instance tříd implementující rozhraní CmdHandler.java na základě jejich textové identifikace (užití návrhového vzoru Factory)
srv.handler.impl	GetAppList.java	vrácení seznamu přiřazených vzdálených ploch
	GetAuthentication.java	vrácení výsledku autentizace uživatele dle uživatelského jména a hesla
	GetStationCfg.java	vrácení konfigurace stanice
	GetStationInf.java	vrácení informací o stanici
	SendInfo.java	příjem názvu stanice, verze softwaru a zašifrovaného VNC hesla
	SendLog.java	příjem informace pro zápis do logovací tabulky v db
	SetPassword.java	vrácení výsledku požadavku na změnu přihlašovacího hesla
	StartSession.java	vrácení parametrů nutných pro sestavení relace vzdálené plochy

Tabulka 6: Přehled tříd programu infrastrukturního serveru

Zdroj: Vlastní zpracování

Obsah konfiguračního souboru serveru:

(varianta s použitím databáze MS SQL)

```
# Database configuration
db.driver=com.microsoft.sqlserver.jdbc.SQLServerDriver
(název balíčku ovladače pro přístup k databázi)

db.jdbc=jdbc:sqlserver://IP nebo hostname serveru;databaseName=název db
(připojovací řetězec do databáze)

db.user=uživatelské jméno
db.passwd=heslo
```

Zdrojové kódy programu jsou přiloženy na CD.

Příloha C: Přehled programu pro správu PXE serveru

Balíček	*Třída*	*Popis*
pxe	Config.java	zpracování konfiguračního souboru
	ConfigDB.java	zpracování konfigurace z databáze
	DB.java	napojení na databázi MS SQL
	DeleteTask.java	odstranění úlohy z rozvrhu
	PXECreateHD.java	proces vytvoření diskového obrazu stanice
	PXEDeleteHD.java	odstranění diskového obrazu stanice
	PXEDHCP.java	generování konfigurace DHCP serveru
	PXEInstance.java	kontrola a blokování dalších instancí aplikace
	PXE.java	**výchozí třída zajišťující chod programu**

Tabulka 7: Přehled tříd programu pro správu PXE serveru

Zdroj: Vlastní zpracování

Obsah konfiguračního souboru programu pro správu PXE serveru:

(varianta s použitím databáze MS SQL)

```
# Database configuration
db.driver=com.microsoft.sqlserver.jdbc.SQLServerDriver
(název balíčku ovladače pro přístup k databázi)

db.jdbc=jdbc:sqlserver://IP nebo hostname serveru;databaseName=název db
(připojovací řetězec do databáze)

db.user=uživatelské jméno
db.passwd=heslo
```

Zdrojové kódy programu jsou přiloženy na CD.

Příloha D: Struktura databáze

Tabulka	*Popis*
STATION	seznam tenkých klientů
TCCONFIG	rozšíření konfigurace o specifické parametry tenkých klientů
TCUSG	záznam využití jednotlivých tenkých klientů
PROFYLAXE	archiv výkazu servisních a profylaktických prací
PRINTER	seznam tiskáren
PRINTERDEV	číselník typů tiskáren
PRINTERUSG	záznam využití jednotlivých tiskáren
TONERY	evidence spotřebního materiálu
TSERVER	seznam terminálových serverů
LOCATION	seznam lokalit
NS	seznam nákladových středisek
RD	seznam vzdálených ploch
ALLOWEDRD	seznam vzdálených ploch přiřazených ke stanici
LASTSTATE	záznamy o posledních výskytech uživatelů na příslušných terminálových serverech
LOCK	seznam aktivních zámků
USERPASSWORD	číselník uživatelů
LOG	evidence událostí
CONFIG	seznam konfiguračních parametrů
TASKS	rozvrh úloh pro PXE server

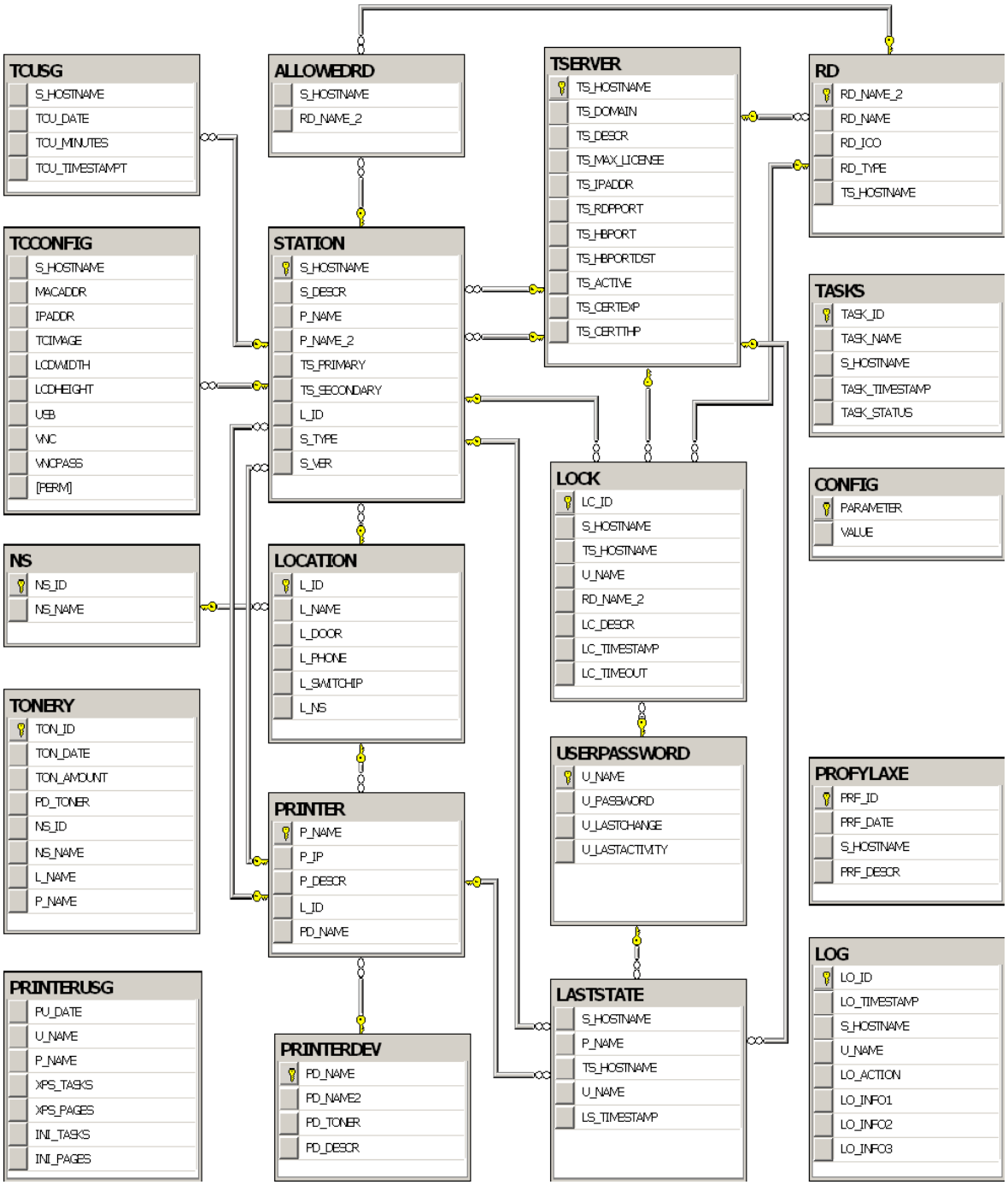
Tabulka 8: Seznam tabulek databáze

Zdroj: Vlastní zpracování

Pro jednodušší zpracování webové aplikace a zautomatizování některých akcí nad daty byly použity následující triggery:

TI_TCCONFIG - generování úloh pro PXE server po vložení nové stanice do databáze,
TU_TCCONFIG - generování úloh pro PXE server po aktualizaci údajů stanice v databázi,
TD_TCCONFIG - generování úloh pro PXE server po výmazu stanice z databáze,

a procedura:
TCONLINE – výpočet a aktualizace doby provozu stanice.



Obrázek 25: Schéma databáze

Zdroj: Vlastní zpracování

Skripty pro založení databáze jsou přiloženy na CD.

Příloha E: Přehled skriptů webového managementu

Skript	*Popis*
dbconnect.php	připojení do databáze
delete.php	obsluha databáze (výmaz dat)
edit_CONFIG.php	editace parametrů infrastruktury
edit_LOCATION.php	editace lokalit
edit_NS.php	editace nákladových středisek
edit_PRINTER.php	editace tiskáren
edit_PRINTERDEV.php	editace typů tiskáren
edit_PROFYLAXE.php	výkaz a přehled servisních činností
edit_TERMINAL.php	editace tenkého klienta
edit_TONERY.php	výkaz a přehled spotřebního materiálu
edit_TSERVER.php	editace terminálových serverů
export.php	předdefinované exporty vybraných tabulek
graf.php	generování grafů na základě přijatých parametrů
header.php	hlavička všech formulářů
index.php	výchozí stránka, Dashboard
save.php	obsluha databáze (ukládání dat)
search_ALLOWEDRD.php	přehled přiřazených vzdálených ploch k tenkému klientovi
search_LOCATION.php	přehled lokalit
search_LOCK.php	přehled a editace zámků
search_NS.php	přehled nákladových středisek
search_PRINTER.php	přehled tiskáren
search_PRINTERDEV.php	přehled typů tiskáren
search_RD.php	přehled a editace vzdálených ploch
search_TERMINAL.php	přehled tenkých klientů
search_TSERVER.php	přehled terminálových serverů
search_USER.php	přehled činnosti uživatele

Tabulka 9: Přehled skriptů webového managementu

Zdroj: Vlastní zpracování

Skripty webového managementu jsou přiloženy na CD.