Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačního inženýrství

Bakalářská práce

Virtual Desktop Infrastructure na platformě Microsoft

Zuzana Kramosilová

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Zuzana Kramosilová

Informatika

Název práce

Virtual Desktop Infrastructure na platformě Microsoft

Název anglicky

Virtual Desktop Infrastructure using Microsoft technologies

Cíle práce

Cílem práce je navrhnout a realizovat infrastrukturu virtuálních klientských počítačů (VDI) s využitím technologií společnosti Microsoft (Windows Server, Hyper-V). Součástí práce bude rešerše současných možností virtualizace klientnských počítačů.

Metodika

Práce se bude skládat z rešeršní a praktické části. V rešeršní části se bude nejdříve zabývat obecnými principy virtualizace a jejím rozdělením. Dále se konkrétněji zaměří na virtualizaci klientských stanic (VDI) a možnosti této technologie. Budou rozebrány dostupné technologie a produkty, které se k virtualizaci desktopů používají. Tato část se bude zabývat převážně řešeními společnosti Microsoft, se kterými se bude dále pracovat v praktické části. Stručně bude zahrnut i přehled dalších využívaných řešení.

V praktické části bude proveden návrh virtuální infrastruktury a její implementace za použití Microsoft Windows Server a stanic s operačním systémem Windows. Součástí bude identifikace výhod a nevýhod implementovaného řešení.

Doporučený rozsah práce

30-40 stran

Klíčová slova

VDI, Hyper-V, RDS, Microsoft Windows Server, tenký klient

Doporučené zdroje informací

FINN, A. Windows Server 2012 Hyper-V Installation and Configuration Guide. Indianapolis: John Wiley&Sons, 2013. ISBN 978-1-118-48649-8.

KRAUSE, J. Windows Server 2016 Administration Cookbook. Birmingham: Packt Publishing Ltd., 2018. ISBN 978-1-78913-593-0.

KUSNETZKY, D. Virtualization : A Manager's Guide. Sebastopol: O'Reilly Media, Inc., 2011. ISBN: 978-1-449-30645-8.

RUEST, D. Virtualizace : podrobný průvodce. Brno: Computer Press, 2010. ISBN 978-80-251-2676-9.

SAVILL, J. Mastering Windows Server 2016 Hyper-V. New Jersey: John Wiley&Sons, 2017. ISBN 978-1-119-28618-9.

Předběžný termín obhajoby

2018/19 LS – PEF

Vedoucí práce

Ing. Marek Pícka, Ph.D.

Garantující pracoviště

Katedra informačního inženýrství

Elektronicky schváleno dne 24. 1. 2019

Ing. Martin Pelikán, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 24. 1. 2019

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 15. 03. 2019

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Virtual Desktop Infrastructure na platformě Microsoft" jsem vypracovala samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autorka uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušila autorská práva třetích osob.

V Praze dne 15.3.2019 _____

Poděkování

Ráda bych touto cestou poděkovala panu Ing. Marku Píckovi, Ph.D. za vedení mé bakalářské práce.

Virtual Desktop Infrastructure na platformě Microsoft

Abstrakt

Tato bakalářská práce popisuje návrh a realizaci infrastruktury virtuálních desktopů s využitím produktů společnosti Microsoft.

V teoretické části je nejprve popsána historie virtualizace společně s jejími obecnými principy. Dále se práce zaměřuje na konkrétní technologie virtualizace, které Microsoft poskytuje. Na závěr teoretické části jsou rozebrány možnosti virtualizace desktopů a jejich správy.

Praktická část se zabývá samotným návrhem virtuální infrastruktury ve firemním prostředí počítačové učebny. Popisuje proces od úvodní identifikace současného stavu, přes návrh až po implementaci řešení v testovacím prostředí.

Klíčová slova: virtualizace, VDI, Hyper-V, Windows Server 2016, tenký klient, RDS, virtuální stroj

Virtual Desktop Infrastructure using Microsoft technologies

Abstract

This bachelor thesis describes design and implementation of virtual desktop infrastructure using Microsoft technologies.

The theoretical part first describes a history of virtualization and basic principles of virtualization. Second, the work presents virtualization technologies provided by Microsoft. Final part is devoted to the possibilities of desktop virtualization and administration.

The practical part deals with design of the virtual infrastructure for the corporate computer classroom. It describes the process from the identification of the current state, through the design to the implementation of the solution within test environment.

Keywords: virtualization, VDI, Hyper-V, Windows Server 2016, thin client, RDS, virtual machine

Obsah

1 Úvod 12

2 Cíl práce a metodika 13

2.1 Cíl práce 13

2.2 Metodika 13

3 Teoretická východiska 14

3.1 Historie virtualizace 14

3.1.1 Virtualizace serverů 15

3.2 Virtuální stroj a hypervisor 16

3.2.1 Virtuální stroj 16

3.2.2 Hypervisor 17

3.3 Technologie Microsoft 20

3.3.1 Hyper-V 20

3.3.2 VMBus 21

3.3.3 Virtuální stroje první generace 21

3.3.4 Virtuální stroje druhé generace 21

3.3.5 Virtuální disky 22

3.3.5.1 VHD 23

3.3.5.2 VHDX 23

3.3.5.3 Pass-trough storage 23

3.3.6 Virtuální přepínače 24

3.4 Virtualizace desktopů 24

3.4.1 Remote Desktop Services (RDS) 25

3.4.2 Remote Desktop Session Host (RDS) 25

3.4.3 Virtual Desktop Infrastructure (VDI) 26

3.4.3.1 Remote Desktop Virtualization Host 27

3.4.3.2 Remote Desktop Connection Broker 27

3.4.3.3 Remote Desktop Web Access 27

3.4.3.4 Remote Desktop Gateway 28

3.4.3.5 Remote Desktop Licensing 28

3.4.4 Klientská zařízení 28

3.4.4.1 Tlustý klient 28

3.4.4.2 Tenký klient 29

3.4.4.3 Nulový klient 29

3.5 Správa VDI 30

3.5.1 Nástroje pro správu Hyper-V 30
3.5.1.1 Hyper-V Manager 30
3.5.1.2 System Center Virtual Machine Manager (SCVMM) 30
3.5.1.3 Power Shell 31
3.5.2 Vytvoření a instalace virtuálního stroje 31
3.5.3 Checkpoint 31
3.5.4 Master image 32
3.5.5 Sysprep 32
3.5.6 Windows System Image Manager (SIM) 32

4 Vlastní práce 34
4.1 Popis výchozího stavu 34
4.2 Návrh řešení 34
4.3 Příprava prostředí 35
4.4 Příprava stanice administrátora 36
4.5 Instalace serverů 36
4.5.1 Instalace Hyper-V Serveru 36
4.5.2 Instalace Remote Desktop Services 37
4.6 Příprava virtuálních stanic 39
4.6.1 Vytvoření referenční stanice a instalace operačního systému 39
4.6.2 Založení kolekce 40
4.6.3 Deployment 42
4.7 Instalace koncových stanic 42
4.7.1 Výběr operačního systému 42
4.7.2 Instalace a nastavení tenkého klienta WTware 43
4.8 Ověření funkčnosti 46
4.8.1 Funkčnost z pohledu uživatele 46
4.8.2 Funkčnost z pohledu administrátora 47

5 Výsledky a diskuse 48
5.1 Výhody řešení 48
5.2 Možnosti zlepšení 48

6 Závěr 49

7 Seznam použitých zdrojů 50

Seznam obrázků

Obrázek 1 – Rozdíl mezi hypervisorem prvního a druhého typu 18
Obrázek 3 – Rozdíl mezi architekturou monolitického a mikrokernelového hypervisoru .. 19
Obrázek 4 – Kontrola požadavků pro provoz Hyper-V 20
Obrázek 5 – Vizualizace komponent Remote Desktop Services 27
Obrázek 6 – Uživatelské rozhraní System Image Manager 33
Obrázek 7 – Konfigurační rozhraní sconfig, stav po instalaci serveru 37
Obrázek 8 – Instalace komponent Remote Desktop Services 39
Obrázek 9 – Průběh vytváření kolekce 42
Obrázek 10 – Uživatelské rozhraní WTware Center 44
Obrázek 11 – Rozhraní pro správu WTware na tenkém klientu 44
Obrázek 12 – Ukázka konfigurace tenkého klienta WTware 45
Obrázek 13 – Přizpůsobená úvodní obrazovka tenkého klienta WTware (testovací verze) 46

Seznam použitých zkratek

BIOS	Basic Input-Output System
CP	Control Program
CMS	Console Monitor System
DHCP	Dynamic Host Configuration Protocol
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
RDP	Remote Desktop Protocol
RDS	Remote Services
RDSH	Remote Desktop Session Host
SCVMM	System Center Virtual Machine Manager
SIM	System Image Manager
SLAT	Second Level Address Translation
TFTP	Trivial File Transfer Protocol
UEFI	Unified Extensible Firmware Interface
VDI	Virtual Desktop Infrastructure
VHD	Virtual Hard Disk
VM	Virtual Machine
VMBus	Virtual Machine Bus
VMDK	Virtual Machine Disk
VMM	Virtual Machine Monitor
XML	eXtensible Markup Language

1 Úvod

Od dob, kdy byly počítače vysoce specializované, a na jeden takový počítač připadal velký počet uživatelů, jsme se posunuli do doby, kdy minimálně jeden počítač nebo podobné zařízení má doma prakticky každý a stejně tak ve firmách se bez výpočetní techniky obejde máloco. Aby bylo možné držet krok se stále rychleji se rozvíjející informační infrastrukturou, je někdy třeba opustit zaběhnuté postupy a nacházet nová řešení pro její organizaci a správu. Za jedno z takových řešení můžeme považovat i virtualizaci – převedení fyzických počítačů na jejich virtuální ekvivalenty, které fungují nezávisle na hardwaru. Myšlenka virtualizace se na první pohled může zdát složitá, ale při správném použití je tato technologie schopna ušetřit čas administrátorů stejně jako náklady na fyzickou infrastrukturu.

2 Cíl práce a metodika

2.1 Cíl práce

Cílem této bakalářské práce je návrh infrastruktury VDI, která bude sloužit jako podklad pro nasazení v počítačové učebně využívané ke školení uživatelů, a následné zprovoznění tohoto návrhu v testovacím prostředí. Řešení bude realizováno s využitím technologií společnosti Microsoft. Součástí práce bude rešerše obecných principů virtualizace a konkrétních technologií společnosti Microsoft využívaných k realizaci virtuální desktopové infrastruktury.

2.2 Metodika

Teoretická část práce bude vycházet ze studia odborné literatury a internetových zdrojů, uvedených v seznamu použitých zdrojů. Úvodní část bude věnována obecné historii virtualizace. Dále budou rozebrány principy fungování základních prvků virtualizace – virtuálního stroje a hypervisoru. Druhá polovina teoretické části bude zaměřena na produkty a technologie společnosti Microsoft a to od obecných principů po konkrétní nástroje ke správě a provozu virtuální infrastruktury.

V praktické části práce budou uplatněny poznatky získané v části teoretické. Bude popsán výchozí stav konkrétní počítačové učebny a na základě jeho analýzy bude navrženo zlepšení pomocí využití VDI. Následně bude tento návrh realizován s využitím produktů firmy Microsoft v připraveném testovacím prostředí. Na konci budou a diskutovány výhody a nedostatky realizovaného řešení.

3 Teoretická východiska

3.1 Historie virtualizace

Zatímco velké rozšíření virtualizace zaznamenáváme převážně až v posledních 10 letech, počátky této technologie bychom našli mnohem dříve - konkrétně v 60. letech 20. století.

Tehdy společnost IBM na svých počítačích typu mainframe vyvinula systém nazývaný CP-67. Systém se skládal ze dvou částí – Control Program a Control Monitor System. Control Program (CP) běžel na mainframu a vytvářel virtuální stanice a na nich se spouštěl Console Monitor Systém (CMS), což byl malý interaktivní operační systém, se kterým pracoval uživatel. Takto mohl každý uživatel používat svůj vlastní operační systém a prakticky svůj vlastní počítač. Tento systém přinášel ve své době řadu výhod. Místo rovnoměrného dělení zdrojů mainframu mezi jednotlivé uživatele, což byl v té době běžný postup, byly tyto zdroje podle potřeby sdíleny mezi virtuálními stroji. Inovativní byla i možnost interakce uživatele s běžícím operačním systémem a jeho programy, na rozdíl od tradičního přístupu, kdy uživatel zadal do počítače svůj program a poté pouze čekal na jeho zpracování. Dále systém přinesl zvýšení bezpečnosti a spolehlivosti, protože každý uživatel pracoval na svém odděleném operačním systému a pokud došlo k problému, projevil se pouze na vlastním operačním systému uživatele a nikoliv na celém systému. Systém CP-67 byl představen veřejnosti v roce 1968, jeho první stabilní verze byla dostupná až o pár let později v roce 1972. Před CP-67 existoval ještě CP-40, který ale nebyl určen pro komerční využití a sloužil pouze pro výzkumné a vývojové účely. CP-67 byl tak prvním komerčně dostupným systémem, který podporoval virtualizaci. Na velmi podobném principu funguje dnes virtualizace desktopů.

V roce 1974 zveřejnili američtí vědci Gerald J. Popek a Robert P. Goldberg článek s názvem Formal Requirements for Virtualizable Third Generation Architectures, ve kterém specifikovali požadavky na systémy podporující virtualizaci. Definovali virtuální stroje (VM – Virtual Machines), které mohly virtualizovat všechny hardwarové zdroje (procesory, paměti, úložiště, síťová připojení) a hypervisory (VMM - Virtual Machine Monitor) jako software, který virtuálním strojům poskytuje prostředí k běhu a zabezpečuje jim přístup k hardwarovým zdrojům. Hlavní podmínky, které musel splňovat VMM, byly tři:

- Přesnost – prostředí vytvořené pro virtuální stroj je stejné jako to, které poskytuje původní fyzický stroj.
- Izolace nebo bezpečnost – VMM musí mít plnou kontrolu nad systémovými zdroji.
- Výkon – mezi výkonem virtuálního stroje a jeho fyzického ekvivalentu by neměl být žádný rozdíl, nebo pouze minimální.

Role a podmínky definované tak, jak je Popek s Goldbergem popsali ve své práci, jsou aktuální dodnes. (3, s. 2)

V roce 1987 představila společnost Insignia Solutions softwarový emulátor pojmenovaný SoftPC. SoftPC umožňoval uživatelům spouštět DOSové aplikace na počítačích s Unixovými systémy, což kvůli rozdílným prostředím obou systémů do té doby nebylo možné. O dva roky později byl vydán SoftPC i pro počítače se systémem Mac a zároveň byl rozšířen o podporu aplikací Windows.

Po úspěchu SoftPC přišly s podobným řešením i další společnosti. Firma Apple vytvořila program Virtual PC, který podobně jako SoftPC umožňoval uživatelům spouštět prostředí Windows na počítačích Mac, v roce 1997. V roce 1999 začala svůj první podobný produkt prodávat i společnost VMware pod názvem VMware Workstation. Společnost VMware také jako první přišla s řešením pro virtualizaci serverů (8).

3.1.1 Virtualizace serverů

Před masivním rozšířením informačních technologií bylo běžné využívat jeden fyzický server pro provoz jedné role. Se stále větším rozšířením informačních technologií se postupně zvyšovaly nároky na serverovou infrastrukturu, což zahrnovalo i zvyšující se náklady na elektrickou energii, rostoucí požadavky na prostor pro umístění stále většího počtu počítačů a také požadavky na personál, který servery spravoval a udržoval v chodu. S rostoucím počtem serverů bylo stále obtížnější a dražší je udržovat. Zároveň tyto servery byly neefektivní, protože při provozu běžně využívaly jen zlomek svého dostupného výkonu. Proto se ukázalo jako nezbytné přistoupit k virtualizaci. Prvním krokem byla takzvaná konsolidace serverů, kdy na je jednom fyzickém serveru provozováno více virtuálních strojů s jednotlivými servery. Při poměru konsolidace 4:1 (čtyři virtuální servery běžící na jednom fyzickém) tak bylo možno snížit počet fyzických počítačů až o tři čtvrtiny. S rostoucím výkonem počítačů pak bylo možné poměr konsolidace dále zvyšovat. (3, s. 13) Dalším vývojem pak bylo používání techniky zvané containment, kdy se pro nově nasazované role serverů rovnou použijí virtuální stroje, což snižuje náklady na

hardware. (3, s. 73) V současnosti se odhaduje, že 50 – 70 procent serverů běžících na systémech Windows a Linux je virtualizovaných. (3, s. 13)

S rostoucí popularitou virtualizace serverů se změnil i pohled na návrh serverů z hardwarového hlediska. Výrobci se začali více soustředit na optimalizaci prostředí pro provoz hypervisorů. Na trhu jsou dnes k dispozici systémy s takzvanou konvergovanou infrastrukturou, které obsahují výpočetní zdroje, síťové prvky a úložiště propojené do jednoho celku a předkonfigurované pro snadné a rychlé nasazení nebo rozšíření virtuálního prostředí. (3, s. 17)

3.2 Virtuální stroj a hypervisor

Pro realizaci virtualizace počítačů, ať už se jedná o servery nebo desktopy, je nutné zajistit dva základní prvky virtualizace – virtuální stroj, který bude abstrakcí fyzického počítače, a hypervisor jako vrstvu, nad kterou virtuální stroje poběží.

3.2.1 Virtuální stroj

Virtuální stroj lze popsat jako fyzický počítač převedený do virtuální podoby, který běží nad hypervisorem na fyzickém počítači. Má stejnou charakteristiku jako fyzický počítač – běží na něm operační systém a aplikace a k dispozici má hardwarové zdroje, které může podle potřeby využívat. Zatímco operační systém může na fyzickém počítači běžet v jednu chvíli jen jeden, virtuálních strojů zde může běžet paralelně velké množství, omezené pouze dostupnými zdroji. (3, s. 38)

Z vnitřního pohledu je virtuální stroj stejný jako jakýkoliv fyzický počítač - obsahuje standardní operační systém a aplikace a má k dispozici běžné hardwarové zdroje, jako procesor, operační paměť, síťové adaptéry, úložiště, nebo periferní zařízení. Tyto zdroje se od svých fyzických protějšků na první pohled neliší. Ve skutečnosti se ale jedná o generická zařízení se speciálními virtuálními ovladači, která poskytuje hypervisor. (3, s. 39)

Z vnějšího pohledu je virtuální stroj soustava souborů, které definují virtuální počítač.(3, s. 38) Jako takové nejsou vázány na konkrétní hardware a dají se libovolně kopírovat, zálohovat a přenášet mezi fyzickými úložišti. Soubory definující virtuální stroj jsou zejména (2, s. 48 a 49):

- Konfigurační soubor obsahující informace o přidělených zdrojích.

- Soubor pevného disku, který je reprezentací fyzického pevného disku. Je na něm nainstalován operační systém a uložena data jako na běžném pevném disku. K jednomu virtuálnímu stroji může být připojen jeden nebo více souborů pevných disků.
- Soubor obsahu paměti obsahující informace, které se nacházejí v paměti běžícího virtuálního stroje. Po vypnutí virtuálního stroje je obsah souboru zapsán do souboru pevného disku.
- Soubor stavu virtuálního počítače, do kterého se ukládá stav po převedení virtuálního stroje do režimu spánku.
- Ostatní soubory obsahující další informace a logy, které se virtuálního stroje týkají.

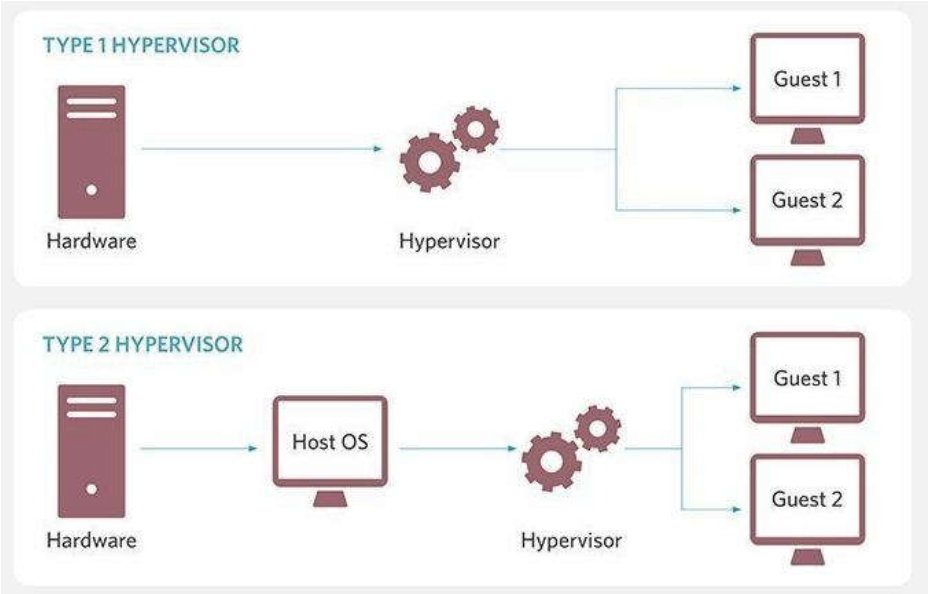
3.2.2 Hypervisor

Na běžném počítači běží v jednu chvíli jeden operační systém, který má přístup k hardwarovým zdrojům, se kterými přímo komunikuje, využívá je a přiděluje nad ním spouštěným aplikacím podle aktuální potřeby. Pokud na počítači běží více virtuálních strojů, má každý svůj vlastní operační systém nezávislý na ostatních a s vlastními potřebami na přidělování zdrojů. Mohlo by tak docházet k situacím, kdy se více operačních systémů pokusí alokovat stejné zdroje ve stejnou chvíli, což by vedlo k nefunkčnosti systému. Aby k těmto situacím nedocházelo, využívá se při virtualizaci hypervisor.

Hypervisor je softwarová vrstva, která zajišťuje interakci mezi hardwarovými zdroji hostitelského počítače a hostovanými virtuálními stroji. Jeho úkolem je poskytovat virtuálním strojům prostředí k provozu shodné s očekávaným fyzickým prostředím, a to s co nejmenšími náklady na výkon. Dále má za úkol řídit hardwarové zdroje a poskytovat je virtuálním strojům podle jejich aktuálních požadavků.

Hypervisory můžeme rozdělit do dvou skupin podle toho, jakým způsobem spolupracují s fyzickým počítačem, na hypervisory prvního a druhého typu (9). Základní rozdíl mezi jejich architekturou je znázorněn na obrázku (Obrázek 1).

Obrázek 1 – Rozdíl mezi hypervisorem prvního a druhého typu



Zdroj: (9)

Hypervisor prvního typu (nazývaný též bare-metal) běží přímo na hardwaru fyzického počítače a komunikuje s jeho zdroji bez dalšího prostředníka. Když virtuální stroj požádá o interakci s hardwarem, hypervisor prvního typu jeho požadavek přímo zpracuje. Ke svému provozu nepotřebuje na fyzickém počítači žádný operační systém. Jeho vliv na virtuální stroje běžící nad ním je tak minimální a také ušetří více zdrojů pro virtuální stroje. Hypervisor prvního typu se využije převážně tam, kde je hlavním a jediným úkolem fyzického počítače provoz virtuálních strojů. Virtualizace pomocí tohoto hypervisoru se také nazývá hardwarová virtualizace. Současným příkladem systému využívající hypervisor prvního typu je Microsoft Hyper-V nebo VMware ESX (9).

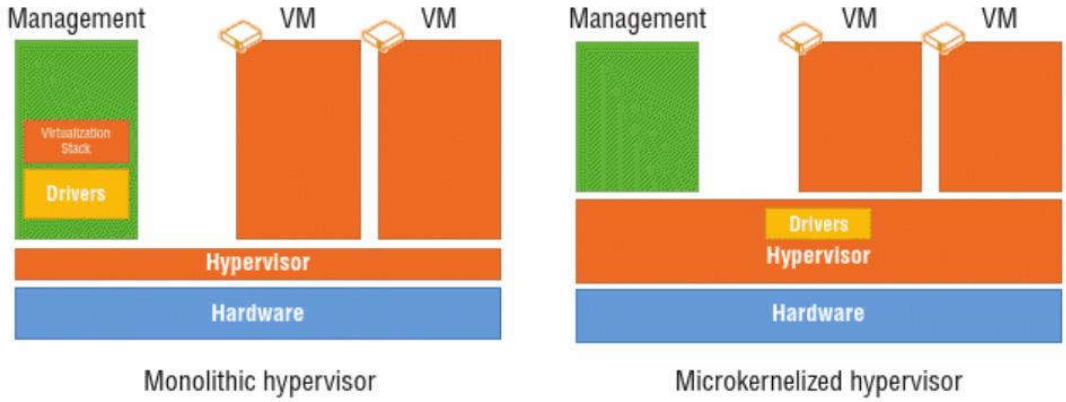
Hypervisory prvního typu se dále dělí podle jejich architektury na monolitické (monolithic) a mikrokernelové (microkernelized).

V monolitické architektuře jsou ovladače (drivery) zodpovědné za komunikaci s hardwarem umístěné přímo v hypervisoru, který je sám o sobě malým operačním systémem. Virtuální stroje přistupují k veškerému hardwaru přímo pomocí těchto specializovaných sdílených ovladačů, což zajišťuje velmi dobrý výkon. Nevýhodou je, že tyto ovladače jsou vždy vytvořené pro konkrétní hypervisor a podporují pouze omezené množství kompatibilního hardwaru. Další nevýhoda se týká bezpečnosti. Ovladače jsou sdílené, takže pokud je některý z nich ovlivněn mallwarem nebo je jinak vadný, ohrozí všechny virtuální stroje.

V mikrokernelové architektuře existuje management oddíl, který používá oficiální ovladače dodávané výrobci hardwaru. Komunikace s virtuálními stroji probíhá pomocí speciální sběrnice nazývané virtual machine bus (VMBus). Tato sběrnice není sdílená, tvoří uzavřený komunikační kanál mezi každým z virtuálních strojů a management oddílem, takže nemůže být ovlivněna ostatními virtuálními stroji (1, s. 42).

Rozdíl mezi oběma architekturami hypervisorů prvního typu je znázorněn na obrázku (Obrázek 2).

Obrázek 2 – Rozdíl mezi architekturou monolitického a mikrokernelového hypervisoru



Zdroj: (1, s. 42)

Na rozdíl od hypervisrou prvního typu vyžaduje hypervisor druhého typu operační systém, na kterém poběží. Tvoří tak vrstvu mezi operačním systémem fyzického počítače a hostovanými virtuálními stroji. Pokud virtuální stroj požádá o interakci s hardwarem, hypervisor druhého typu předá požadavek hostitelskému operačnímu systému, vyčká na jeho odpověď a tu pak dále předá virtuálnímu stroji. Oproti hypervisoru prvního typu tak k vyřízení požadavku potřebuje dva kroky navíc. Hypervisory druhého typu jsou ze své podstaty závislé na fungování hostitelského operačního systému, takže všechny události, které se na tomto operačním systému projeví, ovlivní i hypervisor a všechny virtuální stroje spuštěné nad ním – například restart hostujícího operačního systému způsobí zároveň restart všech hostovaných virtuálních strojů. Tento typ hypervisoru se uplatňuje převážně v prostředích, kde provoz virtuálního stroje je jednou z více různých aktivit provozovaných na fyzickém počítači a virtuální stroj je využíván jen jako jedna z aplikací v prostředí využívaného operačního systému. Model virtulializace s tímto typem hypervisoru bývá také nazýván softwarová virtulizace. Hypervisory druhého typu používá například Microsoft Virtual Server a VMware Workstation (9).

3.3 Technologie Microsoft

Zatímco předchozí text se týkal obecných principů virtualizace, následující část se bude věnovat konkrétním technologiím, které pro virtualizaci poskytuje společnost Microsoft.

3.3.1 Hyper-V

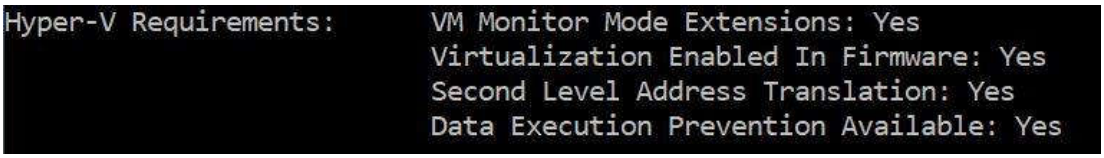
Hyper-V je virtualizační platforma vyvíjená společností Microsoft. Je součástí operačních systémů Windows Server (od verze 2008), Windows 8 a Windows 10 a nahrazuje starší virtualizační produkty, konkrétně Microsoft Virtual PC, Microsoft Virtual Server a Windows Virtual PC. Pro základní použití stačí povolit a spustit Hyper-V na klientském operačním systému, v produkčním prostředí je spíše vhodné nainstalovat Hyper-V jako roli Windows Server Standard nebo Datacenter (17). Další možností je použít samostatný Hyper-V Server, který je na rozdíl od Windows Server zdarma a obsahuje pouze hypervisor a ovladače a komponenty potřebné k virtualizaci (16).

Pro použití hypervisoru Hyper-V je nutné, aby hostitelský systém splňoval následující systémové požadavky (18):

- 64 bitový procesor s překladem adres druhé úrovně (SLAT).
- Rozšíření VM Monitor Mode
- Podporu virtualizace povolenou v BIOS nebo UEFI
- Dostupnou a povolenou technologii Data Execution Prevention

Kontrolu splnění těchto požadavků je možné provést za pomoci příkazového řádku spuštěním příkazu systeminfo. Ten zobrazí kompletní informace o systému, jejichž součástí je i přehled a stav splnění požadavků pro Hyper-V (Obrázek 3).

Obrázek 3 – Kontrola požadavků pro provoz Hyper-V



Zdroj: systeminfo

Hyper-V se řadí mezi hypervisory prvního typu, tedy běží přímo nad hardwarem hostitelského počítače, a využívá mikrokernelovou architekturu. (7, s. 188).

3.3.2 VMBus

Operační systém běžící nad hardwarem počítače očekává, že bude mít k dispozici určité komponenty, jako například BIOS, přístup k úložišti, vstupní a výstupní zařízení nebo síťový adaptér. Pro přístup k nim používá operační systém ovladače (drivery), které jsou buď přímo jeho součástí, nebo mohou být dodatečně přidány. Pokud operační systém běží na virtuálním stroji, tyto očekávané komponenty nejsou fyzicky přítomné, protože neběží nad hardwarem, jak by bylo očekáváno, ale nad hypervisorem, který pro něj hardware simuluje. Úlohou sběrnice VMBus je zajistit komunikaci mezi reálnými ovladači hardwaru, které se nacházejí v management oddílu a virtuálním strojem tak, aby operační systém mohl běžet bez ohledu na abstraktní prostředí, ve kterém se nachází. (1, s. 44)

3.3.3 Virtuální stroje první generace

Starší operační systémy, jako například Windows 2000 nebo Windows XP, nejsou přizpůsobené k virtualizaci a neumí využívat syntetický hardware poskytovaný Hyper-V. Aby bylo možné takové operační systémy instalovat a provozovat na virtuálních strojích, je potřeba nezbytné součásti hardwaru emulovat tak, aby operační systém nepoznal, že běží ve virtuálním prostředí. Hyper-V k tomuto účelu emuluje standardní typy hardwaru – řadič IDE, ethernetový adaptér, myš a klávesnici s konektory PS/2 a základní desku s BIOSem. Hypervisor musí zajistit, aby operační systém tento emulovaný hardware přijal a nepoznal, že neběží na fyzickém hardwaru.

Virtuální stroje s takto emulovaným hardwarem se nazývají virtuální stroje první generace (10).

3.3.4 Virtuální stroje druhé generace

Moderní operační systémy jsou navrženy tak, aby byly schopné běžet jak na fyzických, tak na virtuálních strojích. Dokáží nativně využívat syntetický hardware a nevyžadují bezpodmínečnou přítomnost žádných součástí fyzického hardwaru, aby mohly být nainstalovány a spuštěny. Z tohoto důvodu pro ně není potřeba hardware emulovat. Virtuální stroje, na kterých je možné provozovat tyto operační systémy, se nazývají virtuální stroje druhé generace.

Oproti virtuálním strojům první generace nabízejí určité výhody. První výhodou je zvýšení bezpečnosti využitím funkce Secure Boot, která při startu ověřuje, zda je zavaděč systému podepsán důvěryhodnou autoritou a v případě potřeby zamezí načtení

nedůvěryhodných operačních systémů, ovladačů nebo firmwaru. Secure Boot je zde v základu aktivní, ale v případě potřeby je možné jej manuálně deaktivovat. Další výhoda je možnost většího boot volume. Zatímco ve virtuálních strojích první generace byla maximální velikost boot volume 2TB, zde je možné použít velikost až 64TB, což je i maximální velikost disku podporovaná formátem VHDX.

Virtuální stroje druhé generace neposkytují podporu IDE řadičů, disketových jednotek a legacy network adaptérů. Není možnost přímo připojit CD/DVD mechaniku, CD nebo DVD je nutné připojit jako ISO obraz. V základu není dostupný COM port, ale v případě potřeby je možné jej přidat.

Operační systémy, které mohou běžet na virtuálních strojích druhé generace, jsou Windows Server od verze 2012, 64 bitové Windows od verze 8 a některé 64 bitové distribuce Linuxu (10).

3.3.5 Virtuální disky

Při virtualizaci počítačů je pevný disk reprezentován souborem, nazývaným Virtual Hard Disk. V prostředí Windows Server mají soubory virtuálních disků příponu VHD nebo VHDX. Formát VHD využívají i systémy společnosti Citrix, zatímco VMWare používá vlastní formát VMDK. VHD(X) disky je možné rozdělit podle způsobu využívání prostoru na fyzickém úložišti na tři typy (1, s. 78).

Prvním typem, který je považován za nejefektivnější, jsou disky dynamicky expandující (Dynamically Expanding, někdy také nazývané thinly provisioned). Při použití dynamicky expandujícího disku je na začátku vytvořen soubor virtuálního disku s minimální potřebnou velikostí a v průběhu používání se podle potřeby může zvětšovat až do maximální velikosti povolené konfigurací. Pokud jsou poté z virtuálního disku smazána data, jeho velikost se již nezmenšuje, pokud to není explicitně vyžádáno. Při použití tohoto typu disků je nutné zajistit kvalitní monitoring využití místa na fyzickém úložišti, aby nedocházelo k dynamickému zvětšování virtuálních disků nad rámec jeho kapacity. Dynamicky expandující disk je ze všech typů virtuálních disků nejpomalejší z hlediska přístupu (7, s. 200).

Dalším typem VHD(X) je disk s fixní velikostí (Fixed Size). V tomto případě je velikost virtuálního disku zvolena a alokována při vytvoření VHD(X) souboru a po dobu jeho existence se nemění. Ze všech typů virtuálních disků má tento nejvyšší rychlost přístupu (7, s. 200).

Posledním typem jsou disky rozdílové (Differencing). Tento typ virtuálního disku je svázán s rodičovským diskem. Rodičovský disk je speciálním typem VHD(X) souboru, který je read-only a který je brán jako základ pro rozdílový disk. Na rozdílový disk se pak zapisují pouze změny, které byly provedeny od původního stavu rodičovského disku. Operace zápisu se tedy provádí na rozdílový disk, zatímco operace čtení se provádí v případě nezměněných dat z rodičovského disku a v případě změněných nebo nových dat z rozdílového disku. Velikost rozdílového disku se přizpůsobuje podobně jako u disku dynamicky expandujícího. Rozdílový disk se od ostatních typů disků liší v názvu, koncovka jeho souboru je AVHD(X). Jeho využití se omezuje převážně na testovací prostředí.(7, s. 200) Také se používá při tvorbě checkpointů (5, s. 46).

3.3.5.1 VHD

VHD je starší formát virtuálních disků, používaný před Windows Server 2012. Jeho maximální velikost je 2TB. K jednomu virtuálnímu stroji může být připojeno více virtuálních disků, ale jeden VHD disk nelze připojit zároveň k více virtuálním strojům (7, s. 184).

3.3.5.2 VHDX

VHDX je nový formát virtuálních disků, vyvinutý z formátu VHD a používaný ve Windows Server od verze 2012. Starší formát VHD je novými verzemi Windows Serveru podporován také, ale není doporučeno jej používat, pokud není vyžadován pro zpětnou kompatibilitu s některými staršími systémy. Maximální velikost VHDX je 64TB. VHDX má oproti VHD vylepšený systém logování, který chrání data proti poškození v případě ztráty napájení nebo havárie systému. Poskytuje možnost vložení vlastních metadat, kam si může uživatel například přidat poznámky k virtuálnímu disku. Windows Server 2016 podporuje i takzvaný Shared Virtual Hard Disk, který umožňuje více virtuálním strojům připojit se k jednomu virtuálnímu disku (7, s. 184).

3.3.5.3 Pass-trough storage

Pass-trough storage je specifickým typem disku využívaným ve virtuálním prostředí. Jedná se o fyzický disk přímo připojený k virtuálnímu stroji a využívaný výhradně tímto strojem. Toto řešení je nejlepší z hlediska výkonu, na druhou stranu ale výrazně omezuje výhody virtualizace, protože porušuje úplné oddělení virtuální vrstvy od

fyzické. Pass-trough disky byly dříve využívány tam, kde by výkon nebo velikost disku ve formátu VHD nebyly dostačující, ovšem s přechodem na formát VHDX byla tato omezení z velké části odstraněna (1, s. 83). Pass-trough storage je tedy vhodné využívat pouze v prostředích, kde jsou nejvyšší požadavky na výkon nebo v systémech s vysokou dostupností (7, s. 200).

3.3.6 Virtuální přepínače

Aby virtuální stroje byly schopné komunikovat mezi sebou a případně s okolním prostředím, je nutné zajistit jim síťovou konektivitu. To je zajištěno pomocí virtuálního přepínače. V prostředí Hyper-V jsou k dispozici tři typy virtuálních přepínačů – externí, interní a privátní.

Externí přepínač je svázán s fyzickou síťovou kartou hostitelského serveru. Každý virtuální stroj, který se připojí k externímu přepínači, má přístup k fyzické síti, takže například uvidí ostatní servery v síti a bude moci přímo přistupovat k internetu.

Interní přepínač umožňuje virtuálním strojům komunikovat mezi sebou a navíc s hostitelským serverem. Takto vytvořená virtuální síťová infrastruktura zůstává oddělena od fyzické.

Posledním typem virtuálního přepínače je přepínač privátní. Při použití privátního přepínače mohou virtuální stroje komunikovat mezi sebou, ale nemají spojení s fyzickou sítí ani s hostitelským serverem (7, s. 198).

3.4 Virtualizace desktopů

Virtualizace desktopů umožňuje poskytnout uživateli virtuální pracovní stanici, ke které se může vzdáleně připojit a se kterou může pracovat jako s běžným počítačem. To může být pro uživatele výhodné například v některém z následujících případů (1, s. 512):

- Uživatelé mají vlastní zařízení, ale potřebují využívat podnikové desktopové prostředí.
- Uživatelé používají k práci střídavě více různých zařízení a potřebují konzistentní pracovní prostředí.
- Uživatelé potřebují být připojeni k podnikovému prostředí, ale nemají možnost se k němu fyzicky dostavit.
- Uživatelé mají zařízení Apple, ale potřebují používat prostředí Windows.

- Uživatelé pracují s citlivými daty, která nesmí opustit zabezpečené datové centrum. Virtuální stanice jsou tedy umístěny rovněž v datovém centru a uživatelé k nim pouze vzdáleně přistupují.
- Uživatelé pracují s aplikacemi, které využívají velké množství dat umístěných v datovém centru, a bylo by neefektivní takový objem dat posílat přes síť. Virtuální stanice jsou tedy umístěny v datovém centru na stejné lokální síti jako data vyžadovaná aplikací a uživatelům je k nim poskytnut vzdálený přístup.

Výhody přináší virtualizace desktopů také administrátorům (5, s. 65):

- Správa virtuálních desktopů je snadnější, než správa jejich fyzických ekvivalentů. Protože běží na standardním hardwaru, instalace aktualizací a ovladačů je zpravidla bezproblémová.
- Stanice a data na nich obsažena neopustí podnikové prostředí a jsou pod kontrolou správce, i když uživatelé používají vlastní zařízení nebo pracují na různých místech, což zvyšuje bezpečnost. Také pokud uživatel zařízení ztratí nebo mu je ukradeno, nenachází se přímo na něm podniková data.
- Je velmi usnadněna správa stanic, ke kterým přistupuje více uživatelů a které vyžadují časté reinstalace, jako například kiosky, učebny nebo testovací stanice. Tyto stanice je možné po použití velmi snadno vrátit do původního stavu.

3.4.1 Remote Desktop Services (RDS)

Remote Desktop Services (dříve Terminal Services) je jedna z rolí Windows Server, která umožňuje poskytovat uživatelům virtuální desktopy pomocí protokolu RDP (Remote Desktop Protocol). Windows Server nabízí k této problematice dva přístupy – session-based virtualizaci neboli Remote Desktop Session Host (RDSH) a Virtual Desktop Infrastructure (VDI). (1, s. 507)

3.4.2 Remote Desktop Session Host (RDS)

Jednou z možností virtualizace desktopů je session-based virtualizace, realizovaná pomocí komponenty RDS nazývané Remote Desktop Session Host (RDSH, dříve známé jako Terminal Server). Zatímco při použití VDI je každému uživateli poskytnut kompletní virtuální stroj s vlastním operačním systémem, RDSH vytvoří session s virtuální plochou, kterou uživatel dostane k dispozici, když se připojí k serveru. Tato plocha je odvozena z operačního systému serveru, kde je také nastaveno, jak má vypadat a jaké funkce bude mít

uživatel k dispozici. K jednomu serveru může být zároveň připojeno více uživatelů a hardwarové zdroje serveru se sdílí mezi nimi. Jedná se o velmi efektivní řešení, protože je možné provozovat velké množství desktopů při využití poměrně malého množství hardwarových zdrojů. Na druhou stranu je nutno počítat s omezeními, která vyplývají ze sdíleného systému. Připojení uživatelé nemohou mít v rámci přidělené session administrátorská práva a nemají možnost restartovat systém. Aplikace, které mají mít uživatelé k dispozici, musí být nainstalovány na serveru, ke kterému se připojují, takže tyto aplikace musí být kompatibilní s operačním systémem serveru (5, s. 62) (6, kap. 7) (1, s. 508).

3.4.3 Virtual Desktop Infrastructure (VDI)

Při použití Virtual Desktop Infrastructure (VDI) dostane připojený uživatel k dispozici kompletní virtuální stroj s vlastním operačním systémem. S touto virtuální stanicí může pracovat stejně, jako kdyby používal fyzický počítač – může si přizpůsobit prostředí, provádět restarty a mít vyšší práva, než by bylo možné v prostředí RDSH. Na druhou stranu je použití VDI náročnější na hardwarové zdroje.

Při použití VDI jsou pro přidělování desktopů uživatelům k dispozici dvě metody - osobní desktopy nebo takzvané pooled desktopy.

Osobní desktop znamená, že uživatel má přiřazen jeden konkrétní virtuální stroj, který je mu poskytnut při každém připojení. To umožňuje specifické přizpůsobení operačního systému pro konkrétního uživatele nebo instalaci individuálních aplikací.

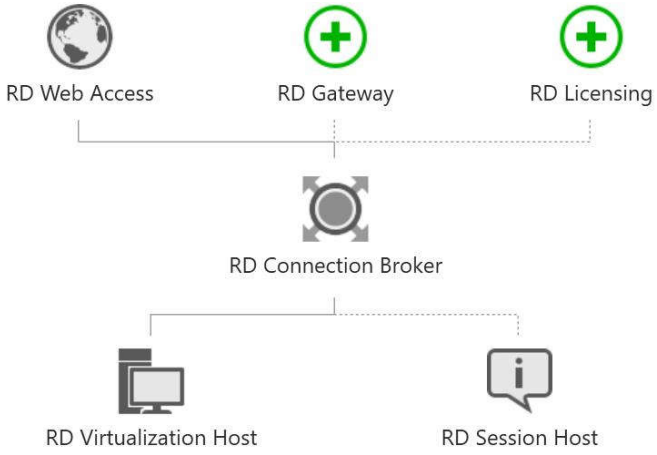
V modelu pooled VDI existuje skupina virtuálních strojů, která je umístěna v takzvaném poolu. Pokud se připojí uživatel, je mu z poolu přidělen jeden z volných virtuálních strojů. Po odhlášení uživatele se virtuální stroj vrací do výchozího stavu a je umístěn zpět do poolu. Uživatelský profil a data jsou uchovány odděleně (1, s. 510).

Pro realizaci VDI je zapotřebí několika komponent RDS:

- Remote Desktop Virtualization Host
- Remote Desktop Connection Broker
- Remote Desktop Web Access
- Remote Desktop Gateway
- Remote Desktop Licensing

Z výše uvedených jsou první tři komponenty povinnými součástmi, instalovanými zároveň s rolí RDS. Poslední dvě komponenty je možno přidat dodatečně (12) (Obrázek 4).

Obrázek 4 – Vizualizace komponent Remote Desktop Services



Zdroj: Windows Server 2016

3.4.3.1 Remote Desktop Virtualization Host

Remote Desktop Virtualization host je komponenta běžící na serveru s Hyper-V, který bude hostit poskytované virtuální desktopy. Umožňuje komunikaci Hyper-V s Connection Brokerem, spouští a zastavuje virtuální stroje a shromažďuje informace potřebné pro připojení klientů. Také zpřístupňuje virtualizaci grafických karet pomocí RemoteFX (1, s. 516).

3.4.3.2 Remote Desktop Connection Broker

Komponenta Remote Desktop Connection Broker řídí připojování k virtuálním desktopům a aplikacím. Slouží jako vstupní bod pro příchozí klientská RDP připojení, odkud jsou přesměrována k odpovídajícímu virtuálnímu stroji s desktopem požadovaným klientem. Po odpojení uživatele Connection Broker vyčistí VDI instanci, vynutí navrácení virtuálního stroje do původního stavu a připraví ho pro připojení nového uživatele (1, s. 515). V případě infrastruktury s více hostujícími servery se stará o jejich rovnoměrné využití (12).

3.4.3.3 Remote Desktop Web Access

Komponenta Remote Desktop Web Access poskytuje jednoduché webové rozhraní, které slouží jako vstupní bod do VDI. Uživatelé si zde si mohou zobrazit a zvolit virtuální desktop nebo aplikaci, ke kterým se chtějí připojit. (1, s. 514) Portál je přizpůsobitelný a umožňuje nastavit, jaké aplikace nebo desktopy budou k dispozici jednotlivým uživatelům

nebo skupinám uživatelů. Komunikace mezi uživatelem a webovým rozhraním probíhá pomocí HTTPS a server i klient musí mít nainstalovány odpovídající digitální certifikáty (12).

3.4.3.4 Remote Desktop Gateway

Remote Desktop Gateway je komponenta, která umožňuje zabezpečené připojení do virtuální infrastruktury z vnějšího prostředí bez nutnosti otevírat porty na firewallu nebo využívat VPN. Gateway je umístěna v demilitarizované zóně nebo za firewallem. Požadavky klientů na připojení RDP jsou zabaleny do HTTPS paketů a přichází na Gateway, kde jsou rozbaleny a přesměrovány do požadované RDP destinace. Při komunikaci opačným směrem Gateway naopak zabalí přijatá RDP data do HTTPS paketu a poté odešle klientovi. Na Gateway je možné nastavit, komu bude umožněno se připojit nebo jaká nastavení RDP budou podporována (1, s. 517). Stejně jako v případě Web Access je pro správnou funkčnost potřeba odpovídající digitální certifikát na straně serveru i klienta (12).

3.4.3.5 Remote Desktop Licensing

Komponenta Remote Desktop Licensing se stará o licence potřebné k provozování virtuálních desktopů a aplikací (11).

3.4.4 Klientská zařízení

Poslední, ale neméně důležitou součástí VDI infrastruktury jsou klientská zařízení, pomocí kterých budou uživatelé pracovat s poskytnutými virtuálními stanicemi. Existují tři typy klientských stanic, které můžeme použít – tlustý klient, tenký klient a nulový klient.

3.4.4.1 Tlustý klient

Tlustý klient (thick client, fat client) je standardní počítač s běžným operačním systémem, který navíc obsahuje software pro připojení k virtuálnímu desktopu. Uživatel má plný přístup ke všem funkcím fyzického počítače a v případě potřeby se může připojit k virtuálnímu desktopu. Tento přístup je tak vhodný například pro uživatele, kteří používají vlastní zařízení a připojení k virtuálnímu desktopu je pro ně jen jedním ze způsobů jeho používání.

Alternativou je uzamknout všechny komponenty operačního systému a uživateli nechat k dispozici pouze aplikaci pro připojení k virtuálnímu desktopu, čímž vznikne pseudotenký klient. Tento způsob se může zdát výhodný pro již zaběhnuté podnikové počítače, které mohou bez větších úprav začít sloužit jako koncová zařízení pro přístup k virtuálním desktopům. Z pohledu správce je ovšem tento přístup nevýhodný, protože na stanici zůstává původní kompletní operační systém, který musí být udržován a aktualizován. Na druhou stranu je u tlustých klientů snadnější řešení hardwarových problémů, protože se jedná o standardní počítače s běžně dostupnými a vyměnitelnými hardwarovými komponentami (21).

3.4.4.2 Tenký klient

Tenký klient (thin client) je specializovaný počítač, který slouží výhradně pro připojení k virtuálnímu desktopu. Zpravidla obsahuje základní operační systém, který se omezuje na pár jednoduchých možností konfigurace a provoz komponenty pro připojení k VDI. Není potřeba výkonný hardware, protože zpracování většiny procesů probíhá na serveru. Díky omezenému operačnímu systému je velmi malá pravděpodobnost, že tenký klient bude napaden mallwarem a navíc může běžet bez vnitřního úložiště a portů pro připojení externích zařízení, takže zamezuje uživatelům ukládat na stanici data.

Tenký klient je možné pořídit jako hotové zařízení s připraveným operačním systémem, které stačí nakonfigurovat a zapojit do infrastruktury. Další variantou je použít starší počítače a vybavit je specializovaným operačním systémem pro tenké klienty (21).

3.4.4.3 Nulový klient

Nulový klient je nejminimalističtější verzí klienta. Je to jednoduché zařízení, jehož jediným účelem je komunikovat s VDI serverem a vykreslovat plochu virtuální stanice. Na rozdíl od klientů popsaných výše na něm neběží žádný operační systém. Místo toho je vybaven speciálním procesorem navrženým pro ovládání připojení ke vzdálené ploše. Kromě operačního systému neobsahuje nulový klient ani žádný pevný disk nebo jiné lokální úložiště, ani jiné komponenty, které přímo nesouvisí s podporou přístupu k VDI. Vzhledem k těmto vlastnostem se jedná o nejbezpečnější variantu ze všech variant klientů. Nulový klient nevyžaduje žádnou nebo jen minimální konfiguraci, nevyžaduje moc údržby a v porovnání s ostatními typy klientů má menší spotřebu energie (21).

3.5 Správa VDI

V následující části bude uveden přehled základních technologií a nástrojů nezbytných pro práci s virtuálními stroji a VDI.

3.5.1 Nástroje pro správu Hyper-V

Za předpokladu že Hyper-V server je instalován jako Server Core, tedy bez grafického uživatelského rozhraní, bude většina správy probíhat vzdáleně. K tomuto účelu bude na stanici administrátora zapotřebí odpovídající nástroj. Microsoft nabízí tři možnosti – základní Hyper-V Manager, pokročilý System Center Virtual Machine Manager a univerzální PowerShell (1, s. 248).

3.5.1.1 Hyper-V Manager

Hyper-V Manager je základní nástroj pro správu Hyper-V. Je součástí každého systému, který Hyper-V podporuje a před prvním použitím ho stačí pouze povolit jako součást systému Windows. Aby umožňoval správu vzdálených serverů, je potřeba navíc doinstalovat Remote Server Administration Tool, který je volně dostupný na webu Microsoftu (1, s. 249). Hyper-V Manager je plně dostačující pro základní správu jednotlivých hostitelských serverů a virtuálních strojů na nich běžících. Je pomocí něj možné nastavit prostředí hostitelského serveru, vytvářet, editovat a rušit virtuální stroje, disky a přepínače a vytvářet a spravovat checkpointy a jednoduché šablony virtuálních strojů (19).

3.5.1.2 System Center Virtual Machine Manager (SCVMM)

Systém Center Virtual Manager je pokročilý nástroj pro správu virtuální infrastruktury. V základu není součástí žádného operačního systému a je potřeba jej zvlášť zakoupit. Na rozdíl od Hyper-V Manageru umožňuje spravovat všechny hostitelské servery a na nich běžící virtuální stroje hromadně z jednoho rozhraní. Navíc se neomezuje jen na správu virtuálních strojů a jejich hostitelů, ale je možné pomocí něj spravovat další součásti infrastruktury, jako například disková pole, servery aktualizačních služeb nebo dokonce servery VMware vCenter. Poskytuje také snadnější správu systémů s vysokou dostupností. Další užitečnou funkcí je možnost pokročilé automatizace při vytváření virtuálních strojů. Vzhledem k množství funkcí a ceně, která pohybuje v řádu tisíců dolarů,

je SCVMM vhodný spíše pro velké organizace s rozsáhlými informačními infrastrukturami (19).

3.5.1.3 Power Shell

PowerShell je univerzální a výkonný nástroj dostupný v operačních systémech Windows. Jedná se o vylepšenou verzi příkazového řádku a zároveň skriptovací jazyk. S jeho pomocí je možné provádět téměř všechny úkony ke správě systému Windows. (6/1) Stejně tak je možné ho použít ke správě Hyper-V, stačí jen načíst příslušný modul pomocí PowerShell příkazu Import-Module Hyper-V. (1, s. 249) Poté poskytuje veškeré nástroje ke kompletní správě Hyper-V. Nevýhodou je relativní náročnost na schopnosti administrátora, protože vzhledem k absenci grafického uživatelského rozhraní probíhá veškerá správa pomocí příkazů a skriptů (17).

3.5.2 Vytvoření a instalace virtuálního stroje

Nový virtuální stroj lze vytvořit pomocí zvoleného nástroje správy. Při jeho založení je potřeba specifikovat následující parametry:

- Název virtuálního stroje a umístění jeho konfiguračních souborů
- Generaci virtuálního stroje
- Operační paměť, která bude virtuálnímu stroji přidělena a případně možnost využití dynamické paměti
- Virtuální přepínač, pokud má být virtuální stroj připojen k síti
- Parametry a umístění přiděleného virtuálního disku
- Médium, ze kterého bude instalován operační systém (tato část je volitelná a může být specifikována i dodatečně po vytvoření virtuálního stroje)

Po vytvoření je virtuální stroj připraven ke spuštění a instalaci operačního systému.

3.5.3 Checkpoint

Checkpoint je v prostředí Hyper-V název pro zachycený stav virtuálního stroje, ke kterému se lze v případě potřeby vrátit. Při vytvoření checkpointu je původní virtuální disk (VHD(X) soubor) uzamčen proti zápisu a je z něj vytvořen nový rozdílový disk (AVHD(X) soubor), do kterého jsou od té chvíle zaznamenávány všechny změny stavu virtuálního stroje. Pokud se rozhodneme vrátit ke stavu zaznamenanému checkpointem, je rozdílový disk vymazán a k použití se vrací původní virtuální disk. Pokud je checkpoint

zrušen, je obsah rozdílového disku sloučen s obsahem původního disku a dále se používá takto vzniklý virtuální disk (5, s. 46).

3.5.4 Master image

Před tím, než bude virtuální stroje možné distribuovat uživatelům, je třeba nainstalovat na ně operační systém. V případě hromadné distribuce stanic pomocí VDI by manuální instalace a konfigurace každého jednotlivého virtuálního stroje byla značně neefektivní a prakticky by se nelišila od přípravy fyzické počítačové infrastruktury. Proto je vhodné připravit jeden virtuální stroj, který bude nadále sloužit jako šablona, podle které může být následně generován libovolný počet virtuálních strojů připravených k okamžitému použití. Tato základní šablona bývá nazývána master image nebo golden image. V rámci VDI se typicky jedná o virtuální stroj s čistě nainstalovaným a dle požadavků nakonfigurovaným operačním systémem a základní sadou aplikací. Každý nově vygenerovaný virtuální stroj pak bude ve výchozím stavu kopií master image (15).

3.5.5 Sysprep

Master image není možné vytvořit z libovolného virtuálního stroje. Po instalaci operační systém Windows obsahuje unikátní prvky, který by při vytváření kopií z image byly duplikovány, což by vedlo k problémům. Proto je nejdříve nutné operační systém náležitě upravit.

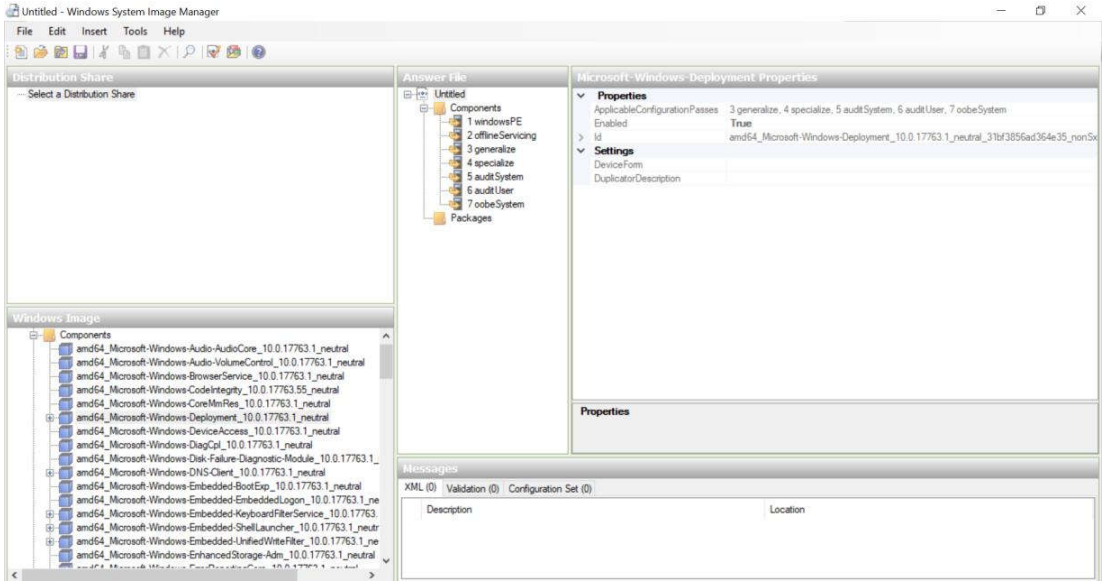
V operačních systémech Windows k tomuto účelu existuje nástroj s názvem System Preparation Tool, zkráceně sysprep. Je to spustitelný soubor, který se typicky nachází v adresáři C:\Windows\System32\Sysprep a který je možné spustit jako aplikaci s grafickým rozhraním nebo ve formě příkazu v příkazovém řádku. Po spuštění sysprep s parametrem generalize (zobecnit) jsou z operačního systému odstraněny prvky vázané na konkrétní počítač, jako identifikátor SID, licenční klíč nebo specializované ovladače (13).

3.5.6 Windows System Image Manager (SIM)

Windows System Image Manager (Obrázek 5) je nástroj, kterým je možné optimalizovat instalaci operačního systému z image. Je součástí balíku Windows Assessment and Development Kit, který je dostupný ke stažení na webu Microsoftu. SIM slouží k vytváření a editaci konfiguračních souborů pro bezobslužnou instalaci Windows. Tento konfigurační soubor se nazývá answer soubor a jeho obsah je definován v jazyku

XML. V answer souboru jsou specifikována uživatelská nastavení, která chceme automaticky aplikovat při instalaci operačního systému z image (20).

Obrázek 5 – Uživatelské rozhraní System Image Manager



Zdroj: Windows System Image Manager

4 Vlastní práce

4.1 Popis výchozího stavu

Firma má malou výukovou a školící místnost, vybavenou jako počítačová učebna. V učebně se nachází celkem 11 počítačů – 1 stanice pro školitele a 10 stanic pro účastníky školení. Všechny stanice mají stejnou hardwarovou konfiguraci. Jedná se o standardní kancelářské počítačové sestavy s procesorem Intel Core i3, 4GB RAM, integrovanou grafickou kartou a 128 GB SSD úložištěm. Součástí každé sestavy jsou základní periferie - klávesnice, myš a monitor. Na všech stanicích je instalován operační systém Windows 10 Pro. Stanice jsou připojeny k firemní síti, ale nemají přístup na internet.

Učebna je využívána nepravidelně, s přibližnou průměrnou frekvencí pěti akcí za měsíc s možným navyšováním do budoucna. Učebnu využívají převážně tři skupiny uživatelů, které byly identifikovány na základě účelu a četnosti využití učebny:

1. Běžní uživatelé z řad klientů, kteří jsou školeni k používání aplikací produkovaných firmou. Tato skupina využívá učebnu přibližně v 60 % případů.
2. Běžní uživatelé z řad zaměstnanců firmy, kteří jsou školeni k používání aplikací, které potřebují ke své práci. Tato skupina využívá učebnu přibližně ve 30 % případů.
3. Správci a vývojáři aplikací z řad zaměstnanců firmy, kteří chtějí vyzkoušet nově nasazované nebo upravené aplikace v běžném uživatelském prostředí, nebo je chtějí demonstrovat a konzultovat se svými kolegy. Tato skupina využívá učebnu přibližně v 10 % případů.

Za provoz učebny zodpovídá jeden administrátor, který má na starost udržovat technické vybavení v dobrém stavu a před každým školením zajistit na všech stanicích odpovídající uživatelské prostředí a dostupnost aplikací potřebných pro dané školení. Toho je docíleno fyzickou kontrolou stanic, aktualizací aplikací a případnou kompletní reinstalací stanice z image. Tento proces je značně časově náročný, a proto je mezi běžnými školeními prováděn spíše nepravidelně. Před a po využití učebny 3. skupinou uživatelů je nutné provést reinstalaci vždy.

4.2 Návrh řešení

Pro zjednodušení správy a standardizaci procesů v učebně bylo navrženo nasazení VDI. Prvotní zprovoznění infrastruktury bude probíhat v testovacím prostředí a v případě

úspěchu bude sloužit jako prototyp, na základě kterého bude řešení navrženo pro zavedení do firemního prostředí.

Požadavkem ze strany firmy je zachování stávající výpočetní techniky, která se v učebně nachází, protože současně provozované počítače jsou poměrně nové a není žádoucí je v blízké době vyměňovat za jiná zařízení. Tato zařízení budou tedy v souladu s požadavkem ponechána v provozu a v průběhu řešení transformována na tenké klienty, což bylo přijato jako vyhovující.

Vzhledem k existující firemní infrastruktuře postavené na technologiích Microsoft budou tyto technologie použity i při realizaci VDI. Jako hypervisor bude vytvořen nový počítač s operačním systémem Hyper-V Server 2016. Jiný existující server s operačním systémem Windows Server 2016 bude rozšířen o roli Remote Desktop Services. Uživatelé přihlašující se do VDI budou používat k tomu vyhrazené uživatelské účty. Celá infrastruktura bude spravována vzdáleně ze stanice administrátora.

4.3 Příprava prostředí

Pro testovací prostředí bude k dispozici:

- Microsoft Hyper-V Server 2016 a stroj s odpovídajícím hardwarovým vybavením, na kterém bude provozován.
- Přístup k Windows Server 2016 pro instalaci komponent RDS.
- Vyhrazená organizační jednotka v Active Directory pro počítače a uživatele související s VDI a administrátorský účet vdiadmin určený pro jejich správu.
- Vyhrazený rozsah IP adres pro použití ve virtuální infrastruktuře.
- Sdílené úložiště.
- Administrátorská stanice pro vzdálenou správu serverů.
- Operační systém Windows 10 pro instalaci na virtuální stanice.
- Dvě stanice sloužící jako koncová zařízení pro připojení k VDI.

Na základě skupin uživatelů definovaných v kapitole 4.1 byly v organizační jednotce VDI založeny dvě sady účtů pro přihlašování k virtuálním stanicím:

- Účty vdiuser s pořadovými čísly 0–10 budou používat k přihlašování uživatelé ze skupin 1 a 2. Tyto účty budou považovány za veřejné a budou mít omezená oprávnění. Vyjímkou bude účet vdiuser0, což bude účet pro školitele ze skupin 1 a 2, který bude mít nastavena oprávnění podle aktuální potřeby.

- Účty vdidev s pořadovými čísly 0–10 budou využívat uživatelé ze skupiny 3. Tyto účty budou mít rozšířená oprávnění.
- Pro každou sadu uživatelů byla založena skupina, kde jsou odpovídající účty sdruženy. Názvy těchto skupin jsou vdiusers a vdidevs.

4.4 Příprava stanice administrátora

Aby bylo možné spravovat VDI z jednoho centrálního místa, bylo potřeba k tomuto účelu přizpůsobit pracovní stanici administrátora, což je standardní pracovní stanice s operačním systémem Windows 10 Pro.

Jako hlavní nástroj pro správu byl instalován softwarový balík Remote Server Administration Tool, který je dostupný ke stažení na webu Microsoftu. Jeho součástí je aplikace Server Manager, která poskytuje uživatelské rozhraní pro přístup k serverům a jejich konfiguraci a to i v případě, že samotný server grafickým uživatelským rozhraním nedisponuje.

4.5 Instalace serverů

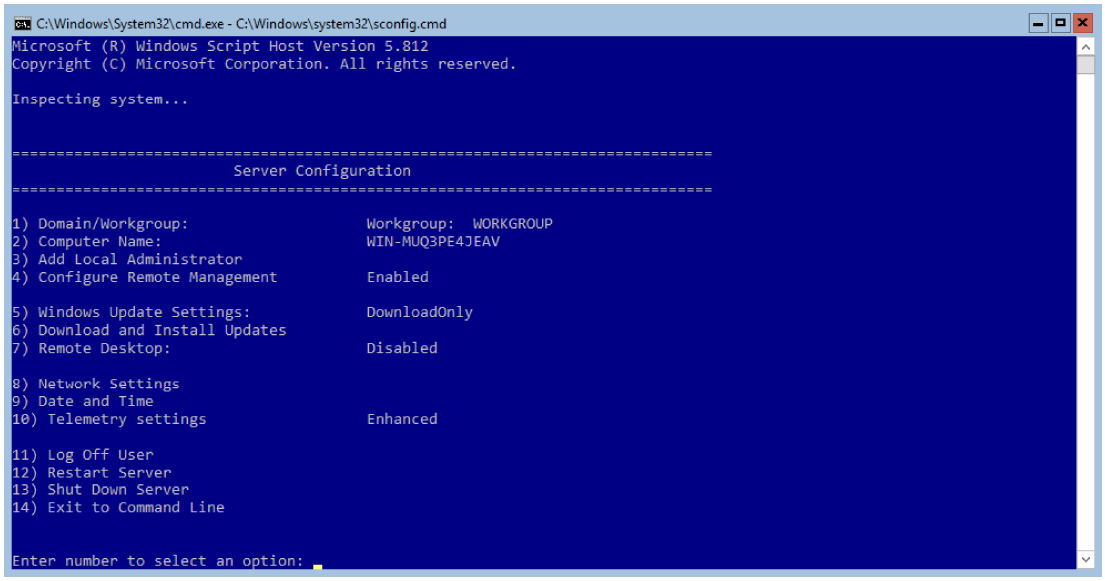
4.5.1 Instalace Hyper-V Serveru

Jako další krok byla na připravený počítač provedena instalace Hyper-V Serveru. Hyper-V Server se instaluje jako Server Core – nemá grafické uživatelské rozhraní. Tento přístup je výhodný, protože šetří hardwarové prostředky, které budou potřeba pro provoz virtuálních strojů, a navíc zvyšuje bezpečnost. Tento server bude sloužit jako hypervisor.

Po spuštění serveru a přihlášení uživatele je zobrazeno konfigurační rozhraní
sconfig (

Obrázek 6). Možnosti konfigurace v tomto rozhraní jsou velmi omezené. Je zde možnost přidat server do domény, nastavit jeho název a v případě potřeby přidat účet lokálního administrátora. Dále lze zde určit, jakým způsobem bude server přistupovat k aktualizacím a odesílání telemetrických dat, nastavit parametry sítě nebo změnit datum a čas. V našem případě byl server přidán do domény a jeho název nastaven na HYPERV-SERVER. Server je po instalaci v základu nastaven na přijetí síťové konfigurace z DHCP a má povolenou vzdálenou správu, tudíž zde nebylo potřeba nic měnit. Posledním krokem bylo zajištění rezervace IP adresy na DHCP serveru a po té byl Hyper-V server připraven k použití.

Obrázek 6 – Konfigurační rozhraní sconfig, stav po instalaci serveru



Zdroj: Microsoft Hyper-V Server 2016

HYPERV-SERVER je nyní přístupný přes Server Manager na stanici administrátora, odkud bude dále spravován. Odtud je také pro tento server možné otevřít Hyper-V Manager, zmiňovaný v kapitole 3.5.1.1. V Hyper-V Manageru bylo nutné konfigurovat některé možnosti:

- Nastavení úložiště pro nově vytvářené virtuální stroje a disky. Úložiště nastavená po instalaci jako výchozí jsou C:\Users\Public\Documents pro virtuální harddisky a C:\ProgramData\Microsoft\Windows v případě souborů virtuálních strojů. Jedná se tedy o stejný svazek, na kterém je nainstalován operační systém serveru a který je z tohoto důvodu jako úložiště nevhodný. Místo něj bylo použito úložiště speciálně vyhrazené pro tyto účely.
- Vytvoření virtuálního přepínače. Pro připojení virtuálních strojů do sítě byl vytvořen externí přepínač.

4.5.2 Instalace Remote Desktop Services

Další potřebnou součástí pro zprovoznění VDI jsou komponenty Remote Desktop Services. Instalovány byly na existující Windows Server 2016, který bude pro účely této práce nazýván RDS-SERVER. Nezbytnou podmínkou pro tento krok je existence

grafického rozhraní přímo na serveru, protože bez jeho přítomnosti některé z komponent není možné nainstalovat.

Instalace probíhala ze stanice administrátora pomocí nástroje Sever Manager, kde byla nejprve zvolena možnost Add Roles and Features. Průvodce instalací provede následující kroky s volbou možností:

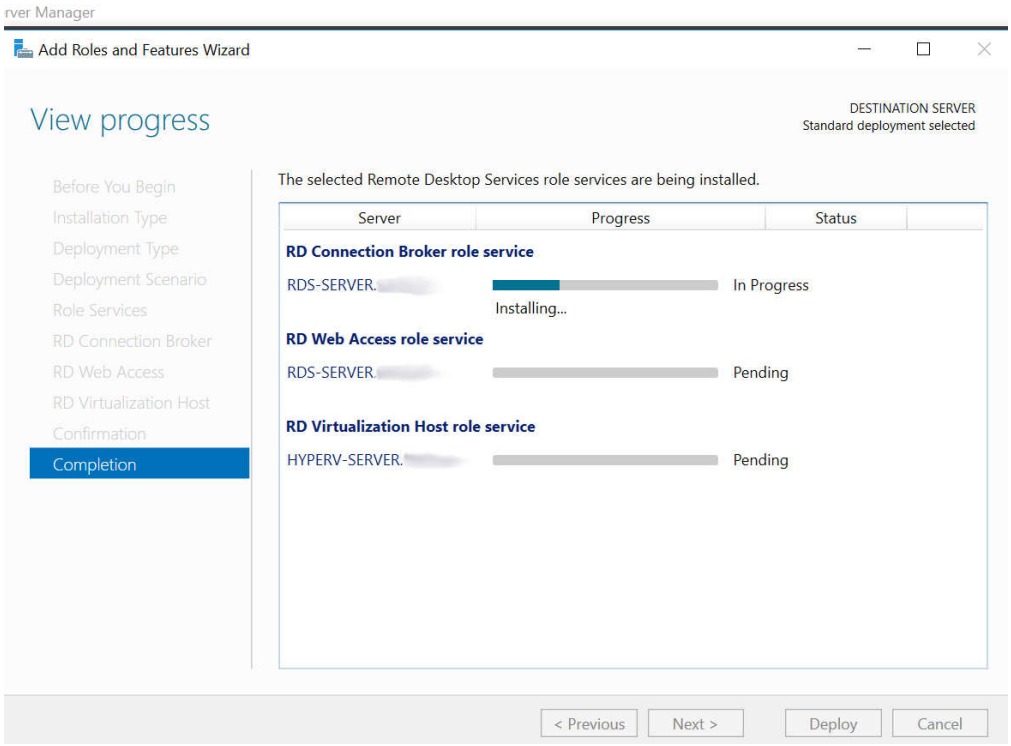
1. Typ instalace – Instalace služby vzdálená plocha.
2. Typ nasazení – Standardní.
3. Scénář nasazení – nasazení Virtual machine-based desktop. Toto nastavení je nutné použít, pokud chceme VDI, druhá dostupná možnost by vytvořila terminálový server pro RDSH.
4. Role – zde je zobrazeno, které role budou instalovány a jejich stručný popis. V tomto případě se jedná o role Connection Broker, Web Access a Virtualization Host.
5. RD Connection Broker – výběr serveru, na který bude instalována role Connection Broker. V tomto případě byl zvolen RDS-SERVER.
6. RD Web Access – výběr serveru, na který bude instalována role Web Access. Zde byl zvolen rovněž RDS-SERVER.
7. RD Virtualization Host – výběr serveru, který bude poskytovat roli Virtualization Host. Jedná se o server, na kterém poběží virtuální stroje, tedy hypervisor. V naší infrastruktuře je to HYPERV-SERVER.
8. Potvrzení – přehled předchozích voleb.

Dokončení – role jsou nainstalovány na servery dle konfigurace. (Po dokončení instalace jsou nové role zpřístupněny v Server Manageru a připraveny k použití.

9. Obrázek 7)

Po dokončení instalace jsou nové role zpřístupněny v Server Manageru a připraveny k použití.

Obrázek 7 – Instalace komponent Remote Desktop Services



Zdroj: uživatelské rozhraní Server Manager (upraveno)

4.6 Příprava virtuálních stanic

4.6.1 Vytvoření referenční stanice a instalace operačního systému

Jako referenční stanice pro připravovanou kolekci virtuálních desktopů byl na serveru HYPERV-SERVER pomocí Hyper-V Manageru vytvořen nový virtuální stroj s názvem Windows10Master. Následně na něj byl nainstalován operační systém Windows 10. Po instalaci byl nabootován do auditního módu a byly na něj nainstalovány potřebné aplikace. Posledním krokem pro vytvoření image bylo spuštění nástroje sysprep s parametrem generalize, kterým byl systém zobecněn a připraven ke kopírování.

Vytvoření answer souboru pomocí Systém Image Manageru se ukázalo bez předchozích znalostí jako velmi komplikovaná záležitost, proto pro základní vytvoření pro testovací účely byl použit online generátor Windows Answer File Generator (http://windowsafg.com/index.html), který umožňuje vygenerování základního answer souboru na základě několika zadaných voleb.

4.6.2 Založení kolekce

Další nastavení byly provedeny na RDS-SERVER pomocí Server Manageru. Zde bylo třeba nejdříve nastavit parametry deploymentu pomocí volby Edit Deployment Properties z rozbalovacího seznamu TASKS. Podstatné jsou dvě poslední možnosti:

- Active Directory – Zde je specifikována doména a organizační jednotka, kam budou vloženy stanice z kolekce po jejich vytvoření. Connection Broker musí mít oprávnění pro vkládání stanic do tohoto umístění v doméně.
- Export location – Zde je nastavena cesta k umístění šablony pro generování virtuálních stanic do kolekce.

V dalším kroku bylo možné přistoupit k tvorbě kolekce. Kolekce je založena pomocí volby Create Virtual Desktop Collection z rozbalovacího seznamu TASKS. Tím je spuštěn průvodce vytvořením kolekce, k jejímuž vytvoření je nutné projít následujícími kroky:

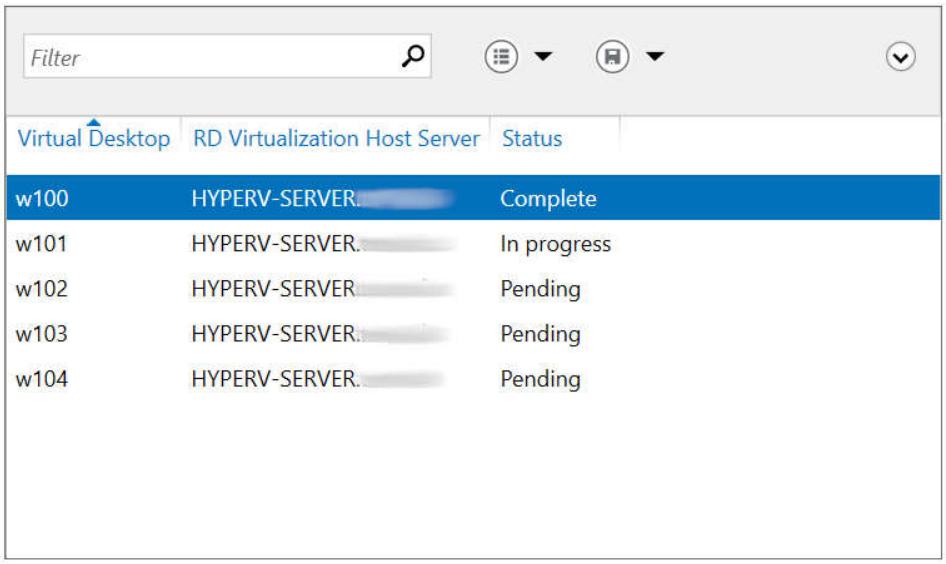
1. Zadání názvu kolekce.
2. Specifikace typu kolekce. Je zde na výběr mezi pooled kolekcí a kolekcí osobních desktopů a volba pro automatické generování stanic v kolekci. Zde byl zvolen model pooled kolekce s automatickým generováním stanic.

3. Šablona pro virtuální desktopy. Jako šablona může být zvolen jeden z virtuálních strojů, které jsou na HYPERV-SERVER k dispozici. Zde byl vybrán virtuální stroj Windows10Master, který byl k tomuto účelu vytvořen v předchozím kroku.
4. Nastavení virtuální stanice. Zde je specifikováno výchozí nastavení stanice po přihlášení uživatele. K tomuto účelu bude připojen answer soubor vytvořený v předchozím kroku.
5. Specifikace uživatelů a skupin, které budou mít přístup k virtuálním strojům z kolekce. Byla odebrána výchozí obecná skupina Domain Users a místo ní přidány skupiny vdiusers a vdidevs. Dále je zde specifikováno, kolik stanic bude v kolekci vytvořeno. Zde bylo pro testovací účely zadáno vytvoření 5 stanic. Poslední možností v tomto kroku je nastavení názvu generovaných stanic. Je možné nastavit prefix, což je název stanice a suffix, který určuje číslo, od kterého budou stanice v kolekci vzestupně číslovány. Pod těmito názvy budou stanice vloženy do domény. Jako název byl zadán řetězec WIN10 a číslování stanic bylo ponecháno od 0.
6. Rozdělení virtuálních stanic. Pokud existuje více Virtualization Host serverů, mohou být stanice z kolekce mezi ně rozděleny. V tomto kroku je možné určit, kolik stanic poběží na kterém serveru. V naší infrastruktuře existuje jen jeden Virtualization Host – HYPERV-SERVER. Všechny vytvořené virtuální stanice tedy poběží na něm.
7. Nastavení úložiště virtuálních stanic. Zde je potřeba nastavit, kam se budou ukládat virtuální disky a soubory virtuálních strojů vytvořených stanic. Na výběr je nastavit některé ze sdílených úložišť nebo ponechat na Virtualization Host serverech, aby umístění zvolili sami v souladu se svou konfigurací. Zde bylo nastaveno ukládání na Virtualization Host, což je HYPERV-SERVER, který má k tomuto účelu přidělené úložiště, specifikované v nastavení Hyper-V. Další volbou zde je možnost automaticky vrátit virtuální stanice po odhlášení uživatele do výchozího stavu. Tato funkce je žádoucí, a proto byla využita.
8. Nastavení ukládání uživatelských profilů. V tomto kroku je možné nastavit ukládání dat a profilů uživatelů po jejich odhlášení z virtuální stanice, s možností specifikace cesty k úložišti a maximální velikosti takto uloženého

profilu. Tato možnost nebyla využita, protože vzhledem k povaze veřejných profilů není žádoucí uživatelské změny ukládat.

Následuje shrnutí všech provedených nastavení. Po potvrzení tlačítkem Create je exportován virtuální stroj určený pro vytvoření šablony a následně je vygenerována kolekce virtuálních stanic (Obrázek 8).

Obrázek 8 – Průběh vytváření kolekce



Zdroj: Server Manager (upraveno)

4.6.3 Deployment

Stanice v kolekci byly vytvořeny a automaticky spuštěny. Jejich běh a využití prostředků je možné vidět v Hyper-V Manageru na serveru HYPERV-SERVER. Od této chvíle jsou k dispozici pro uživatele, kteří požádají o desktop z této kolekce.

4.7 Instalace koncových stanic

4.7.1 Výběr operačního systému

Posledním krokem bylo zprovoznění koncových stanic pro přístup k VDI. Na základě výchozího požadavku zachovat stávající výpočetní techniku bylo rozhodnuto tyto počítače transformovat na tenké klienty pomocí použití vhodného operačního sytému. Operační systém nebyl specifikován, preferována ovšem byla snadná konfigurace, co nejjednodušší uživatelské rozhraní pro připojování uživatelů k virtuálním stanicím a nízké

náklady. Do užšího výběru se dostaly tři produkty – ThinStation, Poertus Kiosk ThinClient a WTware.

ThinStation (https://thinstation.github.io/thinstation/) se ukázal jako velmi komplexní nástroj s velkým množstvím možností využití a poměrně komplikovanou konfigurací a zprovozněním, takže i přes to, že se jedná o zdarma dostupné řešení, nebyl nakonec vybrán.

Další možností byl Poertus Kiosk ThinClient (https://porteus-kiosk.org/thinclient.html). Tento produkt je rovněž dostupný zdarma, s žádostí o dobrovolný příspěvek v případě komerčního využití. Poertus Kiosk ThinClient se vyznačoval poměrně snadnou instalací i konfigurací a jednoduchým uživatelským rozhraním. Z nezjištěných příčin ovšem skrze něj nebylo možné navázat spojení s virtuálními stroji pomocí protokolu RDP. Problém se ani přes značnou časovou investici nepodařilo vyřešit, tudíž tento systém rovněž využit nebyl.

Jako poslední varianta byl zvolen WTware (http://wtware.com/). WTware je volně ke stažení pro testovací účely, v případě nasazení je nutné zakoupit licenci (30€ za licenci při nákupu 10-19 kusů). Produkt je na webu prezentován jako velmi snadný k použití a kompatibilní s Windows Server 2016. Instalace a konfigurace WTware se opravdu ukázala jako velmi snadná a celý systém byl zprovozněn přibližně do 15 minut od získání instalačního souboru. Nainstalovaný operační systém se navíc vyznačuje naprosto minimalistickým uživatelským rozhraním, které uživateli neumožňuje nic jiného, než přihlášení k virtuální stanici. Na základě těchto skutečností byl WTware zahrnut do řešení.

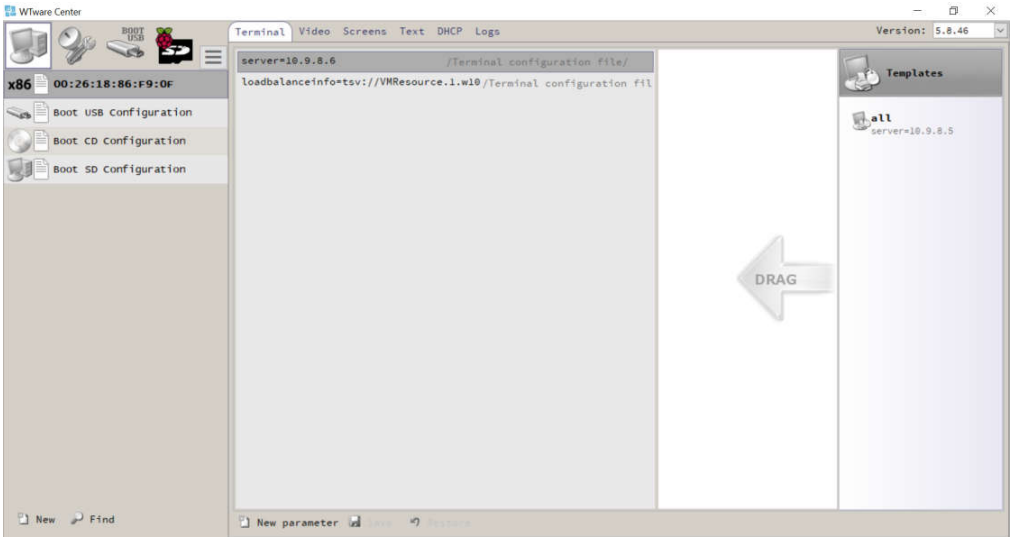
4.7.2 Instalace a nastavení tenkého klienta WTware

Pro použití WTware je nejprve nutné na administrátorskou stanici nainstalovat aplikaci WTware Center (Obrázek 9)Obrázek 9, pomocí které je možné vytvořit bootovací disk, ze kterého bude operační systém instalován na tenké klienty. Příprava instalačního média se skládá z několika jednoduchých kroků:

1. Výběr flash disku, který bude sloužit jako instalační médium.
2. Specifikace síťového nastavení. Zde bylo zvoleno získání konfigurace z DHCP.
3. Umístění konfiguračního souboru. Soubor je možné uložit lokálně na stanici tenkého klienta nebo zpřístupnit pomocí HTTP nebo TFTP serveru. V tomto případě bude konfigurace uložena lokálně.

4. Možnost výběru výchozího konfiguračního souboru a možnost zápisu licence na instalační médium.
5. Nastavení hesla a způsobu přístupu ke konfiguraci tenkého klienta.
6. Zápis instalačního média na flash disk.

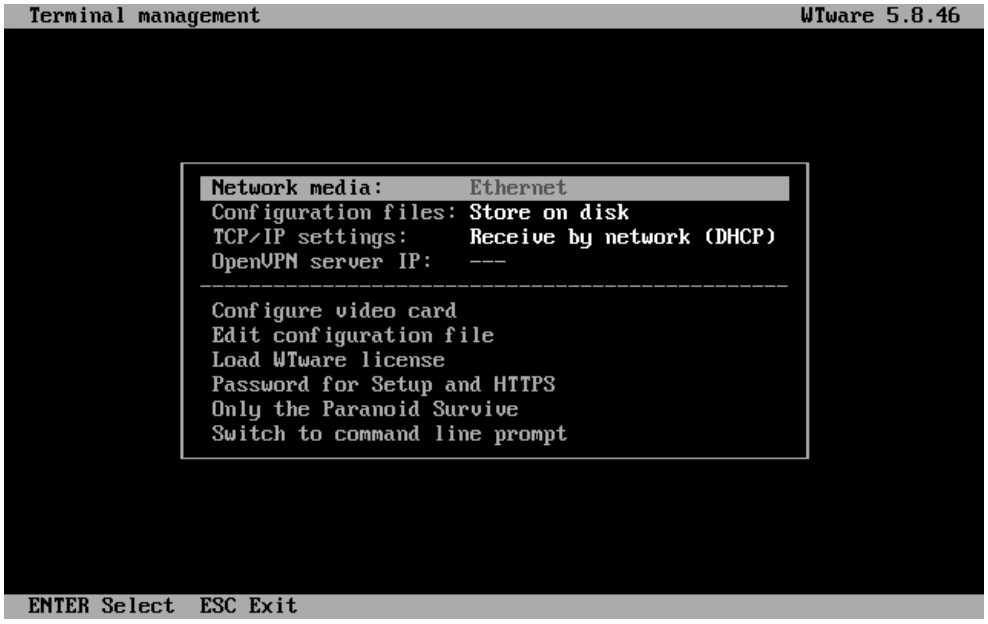
Obrázek 9 – Uživatelské rozhraní WTware Center



Zdroj: WTware Center

Z připraveného instalačního disku byla nabootována stanice určená k transformaci na tenkého klienta. Operační systém je možné ihned používat přímo z flash disku, nebo jej nechat zapsat na pevný disk počítače. Protože cílové stanice jsou vybaveny pevnými disky a použití vyměnitelného zařízení pro provoz systému v prostředí s často se střídajícími uživateli nebylo považováno za vhodné, byla zde použita možnost zápisu systému na pevný disk. V systému je přístupné jednoduché rozhraní pro správu (Obrázek 10).

Obrázek 10 – Rozhraní pro správu WTware na tenkém klientu



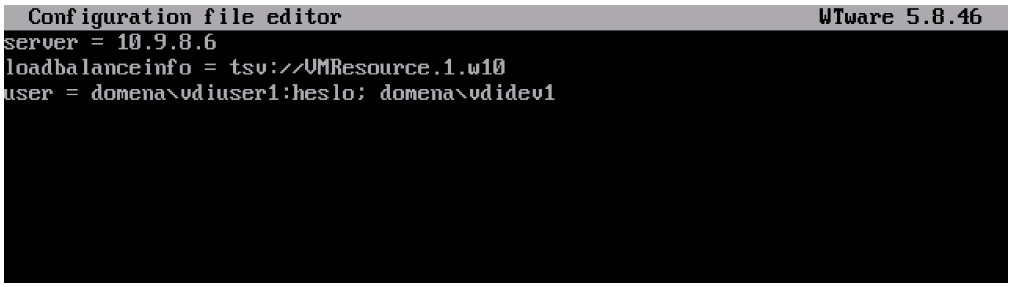
Zdroj: WTware

Konfigurační soubor je v tuto chvíli uložen na pevném disku tenkého klienta a je možné ho přímo v něm editovat. Pro provoz klienta stačí minimální konfigurace:

- Položka server specifikuje IP adresu nebo název RDS serveru.
- Položka loadbalanceinfo určuje kolekci, ze které bude poskytnuta virtuální stanice.

Tato jednoduchá konfigurace plně postačuje pro funkčnost tenkého klienta. V tuto chvíli pro přístup k virtuální stanici stačí, aby uživatel zapnul počítač a vyplnil přihlašovací údaje. Aby ovšem systém více odpovídal reálným požadavkům na využívání učebny, byl konfigurační soubor ještě upraven přidáním položky user (Obrázek 11).

Obrázek 11 – Ukázka konfigurace tenkého klienta WTware



Zdroj: WTware, vlastní tvorba

Na začátku při přípravě prostředí byly vytvořeny dvě sady uživatelských účtů – vdiuser a vdidev. Počet účtů v každé skupině je stejný jako počet tenkých klientů. Tyto účty byly pomocí konfiguračních souborů přiřazeny k jednotlivým tenkým klientům. Po

správně provedené konfiguraci je při zapnutí tenkého klienta zobrazen výběr ze dvou dostupných účtů (Obrázek 12).

Obrázek 12 – Přizpůsobená úvodní obrazovka tenkého klienta WTware (testovací verze)

Zdroj: WTware (upraveno), vlastní práce

Účet vdidev je chráněn heslem, které uživatel musí pro přístup k tomuto účtu zadat. Účet vdiuser je veřejně přístupný – heslo je předvyplněné přímo v konfiguraci a uživateli pro přihlášení stačí kliknout na název účtu. Výjimkou je účet vdiuser0, což je účet přiřazený k tenkému klientu školitele a pro který platí stejné podmínky, jako pro účty vdidev.

Po dokončení konfigurace tenkých klientů je infrastruktura připravena k použití.

4.8 Ověření funkčnosti

Ověření funkčnosti řešení bylo provedeno simulací průchodu několika jednoduchých scénářů.

4.8.1 Funkčnost z pohledu uživatele

1. Účastníkovi školení je po příchodu do učebny přidělena stanice, na kterou se má přihlásit. Na displeji je zobrazena úvodní obrazovka s výběrem uživatelského účtu

(Obrázek 12 – Přizpůsobená úvodní obrazovka tenkého klienta WTware (testovací verze). Na základě instrukce školitele zvolí uživatel první položku a je připojen k operačnímu systému Windows 10. Jedinou další možností na přihlašovací obrazovce je výběr druhého uživatelského účtu. Pokud by uživatel zvolil ten, bude vyzván k zadání hesla. Protože heslo nezná, jedinou možností pro něj zbývá použít první volně přístupný účet.

2. Učebnu chce využít uživatel ze skupiny vývojářů. Na počítač se může přihlásit pod účtem vdidev s heslem, které při rezervaci učebny obdržel od administrátora. Případně může využít i volně přístupný účet vdiuser. Po přihlášení je dle očekávání připojen ke stanici s Windows 10.

4.8.2 Funkčnost z pohledu administrátora

1. Administrátor má na následující den ohlášenou rezervaci učebny pro školení běžných uživatelů. Z administrátorské stanice zkontroluje dostupnost virtuálních strojů. Stroje se po předchozím použití automaticky obnovily do výchozího stavu, tudíž není nutné s nimi momentálně nic dalšího dělat.
2. Je dodána nová aplikace, která bude používaná při školeních. Administrátor zálohuje master image, tuto aplikaci zahrne do aktivní master image a přes Server Manager přegeneruje kolekci. Nová aplikace je následně dostupná na všech virtuálních stanicích. V případě problémů s novou aplikací je možné vrátit se k zálohované verzi master image a vygenerovat stanice do stavu před instalací aplikace.
3. Na jednom z počítačů v učebně je zaznamenána porucha harddisku. Administrátor vymění vadný disk za nový a nakopíruje na něj systém tenkého klienta spolu s konfiguračním souborem. Stanice je okamžitě znovu uvedena do provozu, protože virtuální stanice s operačním systémem nebyla poruchou dotčena.

5 Výsledky a diskuse

5.1 Výhody řešení

Řešení je funkční a plně vyhovuje požadavkům firmy i potřebám uživatelů. Pro administrátora představuje zlepšení oproti výchozímu stavu, protože mu umožňuje provádět většinu správy vzdáleně a automatizovat reinstalace stanic, což představuje časovou úsporu.

5.2 Možnosti zlepšení

Určité výhrady by se mohly týkat konfigurace tenkých klientů. V současném řešení probíhá konfigurace pomocí konfiguračních souborů uložených na pevných discích stanic. V případě změny konfigurace musí administrátor všechny stanice fyzicky obejít a lokálně editovat konfigurační soubor. Toto řešení není maximálně efektivní, ale vzhledem k malému počtu stanic, jednoduchosti konfigurace a faktu, že změny konfigurace není plánováno provádět často, je považováno za vyhovující. Problém by mohl nastat například při rozšiřování infrastruktury o další tenké klienty, čímž by stoupl počet stanic, které je nutné místně konfigurovat. Dalším problémovým případem by mohla být změna v četnosti editací konfigurace – například pokud by administrátor vytvořil více specializovaných VDI kolekcí, které by chtěl zpřístupňovat podle požadavků školení. Protože odkaz na kolekci je rovněž uložen v konfiguračním souboru tenkého klienta, bylo by nutné před každým takovým školením stanice znovu obejít a překonfigurovat. V obou případech by se správa tenkých klientů stala neefektivní a neúměrně časově náročnou. Proto by bylo vhodné využít možnosti WTware editovat konfigurační soubory z administrátorské stanice a distribuovat je klientům pomocí HTTP nebo TFTP serveru, čímž by bylo dosaženo větší efektivity správy.

6 Závěr

Cílem této práce bylo navrhnout jednoduchou virtuální desktopovou infrastrukturu pro zefektivnění provozu a správy firemní počítačové učebny využívané převážně pro školení uživatelů a tento návrh realizovat v testovacím prostředí jako podklad pro nasazení. Jako hlavní platforma řešení byly určeny produkty společnosti Microsoft.

Zpracováním rešeršní části byl vytvořen teoretický základ pro porozumění technologiím využívaným v části praktické. Zkoumáním principů virtualizace počítačů bylo zjištěno, jak taková virtualizace funguje, co od ní lze očekávat a v čem může být výhodná. Zaměřením se na produkty Microsoftu byl teoretický základ prohlouben o poznatky týkající se konkrétních technologií, které mohly být následně zúročeny v praktické části práce. Podrobně prozkoumány byly hlavně nástroje a technologie týkající se virtualizace desktopů a správy VDI.

V praktické části práce byl nejprve popsán a analyzován výchozí stav. Byly rozebrány procesy využití firemní počítačové učebny a následně identifikovány problémy s její správou. Pro řešení těchto problémů bylo navrženo řešení s využitím technologie VDI. Bylo připraveno testovací prostředí realizované s použitím produktů dostupných ve firmě, konkrétně Windows Server 2016, Microsoft Hyper-V Server a Windows 10 Pro. V tomto prostředí byla zprovozněna infrastruktura virtuálních desktopů, která poslouží jako ukázkové řešení pro následné nasazení do učebny. V průběhu řešení bylo rozhodnuto o transformaci stávajících počítačů v učebně na tenké klienty. K tomuto účelu byl vybrán operační systém WTware a jeho vhodnost ověřena implementací do testovacího prostředí.

Na závěr byla ověřena funkčnost řešení a identifikováno očekávané zjednodušení správy učebny. Cíl práce byl splněn.

7 Seznam použitých zdrojů

1. SAVILL, John. *Mastering windows server Hyper-V*. Indianapolis, NY: John Wiley, 2016. ISBN 978-1-119-28618-9.
2. RUEST, Danielle a Nelson RUEST. *Virtualizace: podrobný průvodce*. Brno: Computer Press, 2010. ISBN 978-80-251-2676-9.
3. PORTNOY, Matthew. *Virtualization essentials*. Second edition. Indianapolis, Indiana: John Wiley, 2016. ISBN 9781119267720.
4. KRAUSE, Jordan. *Mastering Windows Server 2016* [online]. Packt Publishing, 2016. ISBN 9781785888908. Dostupné z WWW: http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&an=1403413&scope=site
5. FRYER, Andrew. *Getting started with Windows VDI*. United Kingdom: Packt Publishing Ltd, 2014. ISBN 9781782171478.
6. KRAUSE, Jordan. *Windows Server 2016 CookBook.* United Kingdom: Packt Publishing Ltd, 2016. ISBN 978-1-78588-383-5.
7. PANEK, Will. *MCSA Windows server 2016 Study Guide: exam 70-740*. Indianapolis: John Wiley, 2017. ISBN 1119359341.
8. CONROY, Sean. *History of virtualization* [online]. [cit. 2019-03-10]. Dostupné z WWW: https://www.idkrtm.com/history-of-virtualization/
9. BIGELOW, Stephen J. *What's the difference between Type 1 and Type 2 hypervisors?* [online]. [cit. 2019-03-10]. Dostupné z WWW: https://searchservervirtualization.techtarget.com/feature/Whats-the-difference-between-Type-1-and-Type-2-hypervisors
10. MICROSOFT, Windows IT Pro Center. *Should I create a generation 1 or 2 virtual machine in Hyper-V?* [online]. [cit. 2019-03-10]. Dostupné z WWW: https://docs.microsoft.com/cs-cz/windows-server/virtualization/hyper-v/plan/Should-I-create-a-generation-1-or-2-virtual-machine-in-Hyper-V
11. BRINKMANN, Dan. *Breaking down Remote Desktop Services roles* [online]. [cit. 2019-03-10]. Dostupné z WWW: https://searchvirtualdesktop.techtarget.com/tip/Breaking-down-Remote-Desktop-Services-roles
12. MICROSOFT, Windows IT Pro Center. *Remote Desktop Services roles* [online]. [cit. 2019-03-10]. Dostupné z WWW: https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/rds-roles
13. BAILEY, Richard. *When and How to use Sysprep* [online]. [cit. 2019-03-10]. Dostupné z WWW: https://www.vmware.com/solutions/virtualization.html

14. MICROSOFT, Windows IT Pro Center. *Hyper-V Technology Overview* [online]. [cit. 2019-03-10]. Dostupné z WWW: https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/hyper-v-technology-overview

15. SHIELDS, Greg. Using *Virtual Machine Manager for rapid Hyper-V deployment* [online]. [cit. 2019-03-10]. Dostupné z WWW: https://searchservervirtualization.techtarget.com/tip/Using-Virtual-Machine-Manager-for-rapid-Hyper-V-deployment

16. MICROSOFT, Windows IT Pro Center. *Microsoft Hyper-V Server 2016* [online]. [cit. 2019-03-10]. Dostupné z WWW: https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/hyper-v-server-2016

17. POSEY, Brien. *5 common misconceptions about Microsoft Hyper-V* [online]. [cit. 2019-03-10]. Dostupné z WWW: http://techgenix.com/misconceptions-about-microsoft-hyper-v/

18. MICROSOFT, Windows IT Pro Center. *System requirements for Hyper-V on Windows Server* [online]. [cit. 2019-03-10]. Dostupné z WWW: https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/system-requirements-for-hyper-v-on-windows

19. POSEY, Brien. *SCVMM vs. Hyper-V Manager: Which tasks are best suited to each?* [online]. [cit. 2019-03-10]. Dostupné z WWW: https://searchservervirtualization.techtarget.com/tip/SCVMM-vs-Hyper-V-Manager-Which-tasks-are-best-suited-to-each

20. ROUSE, Margaret. *Microsoft Windows System Image Manager (SIM)* [online]. [cit. 2019-03-10]. Dostupné z WWW: https://searchenterprisedesktop.techtarget.com/definition/Microsoft-Windows-System-Image-Manager-SIM

21. SHELDON, Robert. *Comparing three options for VDI endpoints* [online]. [cit. 2019-03-10]. Dostupné z WWW: https://searchvirtualdesktop.techtarget.com/tip/Comparing-three-options-for-VDI-endpoints