UNIVERZITA PARDUBICE

FAKULTA ELEKTROTECHNIKY A INFORMATIKY

BAKALÁŘSKÁ PRÁCE

2016 Martin Mazurek

Univerzita Pardubice

Fakulta elektrotechniky a informatiky

Využití Microsoft Virtual Desktop Infrastructure pro správu podnikové infrastruktury

Martin Mazurek

Bakalářská práce

2016

Univerzita Pardubice
Fakulta elektrotechniky a informatiky
Akademický rok: **2015/2016**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Martin Mazurek**
Osobní číslo:	**I12183**
Studijní program:	**B2646 Informační technologie**
Studijní obor:	**Informační technologie**
Název tématu:	**Využití Microsoft Virtual Desktop Infrastructure pro správu podnikové infrastruktury**
Zadávající katedra:	**Katedra informačních technologií**

Zásady pro vypracování:

Cílem práce je provést analýzu možností využití Microsoft Virtual Desktop Infrastructure (VDI) pro správu podnikové infrastruktury. V teoretické části autor představí principy virtualizace a virtualizačních nástrojů s důrazem na produkty Microsoft. Zaměří se na způsob a důvody využívání virtualizace a její správu pomocí nástroje VDI. V praktické části autor provede nasazení VDI v podnikové infrastruktuře, představí a implementuje základní a pokročilá nastavení. Na závěr autor provede kritické porovnání správy fyzické a virtualizované infrastruktury a vypracuje seznam doporučení a kroků pro přechod z fyzické na virtualizovanou firemní infrastrukturu.

Rozsah grafických prací:

Rozsah pracovní zprávy: **40**

Forma zpracování bakalářské práce: **tištěná**

Seznam odborné literatury:

*** PORTNOY, Matthew. Virtualization essentials. Indianapolis, IN: John Wiley & Sons, Inc., 2012, xviii, 286 p.**
*** Managing virtualization of networks and services: 18th IFIP/IEEE International Workshop on Distributed Systems: Operations and Management, DSOM 2007 : San José, CA, USA, October 29-31, 2007 : proceedings. Berlin: Springer, c2007, xiii, 267 s. Lecture notes in computer science, 4785. ISBN 9783540756934.**

Vedoucí bakalářské práce: **Mgr. Josef Horálek, Ph.D.**
Katedra informačních technologií

Datum zadání bakalářské práce: **31. října 2015**
Termín odevzdání bakalářské práce: **13. května 2016**

Univerzita Pardubice Česká republika

L.S.

prof. Ing. Simeon Karamazov, Dr.
děkan

Mgr. Josef Horálek, Ph.D.
vedoucí katedry

V Pardubicích dne 31. března 2016

Prohlášení autora

Prohlašuji, že jsem tuto práci vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne 7. 5. 2016

podpis autora
Martin Mazurek

PODĚKOVÁNÍ

V první řadě patří ohromné poděkování mému vedoucímu bakalářské práce panu Mgr. Josefu Horálkovi, Ph.D. za perfektní spolupráci a výbornou pomoc při konzultacích. Další velké poděkování patří mému nejlepšímu kamarádovi Bc. Filipu Majeríkovi, který mi byl nápomocen během studia a vždy mě dokázal podpořit, stejně jako má rodina, které tímto také velmi děkuji. V neposlední řadě děkuji svému kolegovi z práce panu Ing. Jiřímu Semrádovi, který mi již několik let předává spoustu praktických zkušeností v oboru IT a poskytl mi hardware s množstvím výkonu, který byl potřebný k nasazení praktické části této práce. Na závěr děkuji za poskytnutí vynikajících informací týkajících se licencování Microsoft Virtual Desktop Infrastructure paní Zuzaně Sobotkové, která působí ve společnosti DAQUAS, s.r.o. jako licenční konzultantka.

ANOTACE

Tato práce se zabývá tématem virtualizace z pohledu poskytování služeb klientům. Poskytované služby spočívají v přístupu ke vzdáleným virtuálním strojům pomocí vzdálených ploch. Tyto vzdálené plochy následně slouží jako virtuální klientské počítače, které mohou být uživatelům poskytovány kdekoliv, kde je k dispozici připojení k Internetu a vždy jsou uživatelům schopny poskytnout jejich vlastní data a nastavení.

KLÍČOVÁ SLOVA

virtualizace, hypervisor, systém, server, stroj, klient

TITLE

The use of Microsoft Virtual Desktop Infrastructure for managing business infrastructure.

ANNOTATION

This bachelor thesis deals with a topic of virtualisation from the perspective of providing services to clients. Provided services are based on the access to remote virtual machines through a remote desktops. These remote desktops subsequently serve as virtual client computers which can be provided to users anywhere with available Internet connection and which are always able to provide them with their own data and settings.

KEYWORDS

virtualization, hypervisor, system, server, machine, client

OBSAH

SEZNAM ILUSTRACÍ A TABULEK

SEZNAM ZKRATEK A ZNAČEK

AD-DS	Active Directory Domain Services
API	Application Programming Interface
APIC	Advanced Programmable Interrupt Controller
App-V	Microsoft Application Virtualization
BIOS	Basic Input-Output System
BYOD	Bring Your Own Device
COM	Communication port
CPU	Central Processing Unit
CSV	Cluster Shared Volume
DEP	Data Execution Prevention
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
GB	Gigabyte
Gbps	Gigabit per second
GT/s	Giga Transfers per second
HDD	Hard Disk Drive
I/O	Input/Output
IC	Integration Component
IOMMU	Input Output Memory Management Unit
IOPS	Input/Output Operations Per Second
IP	Internet Protocol
iSCSI	internet Small Computer System Interface
Kbit	Kilobit

LAN	Local Area Network
MB	Megabyte
Mbps	Megabit per second
MED-V	Enterprise Desktop Virtualization
MSR	Memory Service Routine
NUMA	Non-Uniform Memory Access
NX	No eXecute
OEM	Original Equipment Manufacturer
OU	Organizational Unit
POST	Power On Self Test
QoS	Quality of Service
QPI	QuickPath Interconnect
RAID	Redundant Array of Independent Disks
RAM	Random Access Memory
RD	Remote Desktop
RDCB	Remote Desktop Connection Broker
RDG	Remote Desktop Gateway
RDP	Remote Desktop Protocol
RDS	Remote Desktop Services
ROM	Read-Only Memory
SAS	Serial Attached SCSI
SCSI	Small Computer System Interface
SMB	Server Message Block
SSL	Secure Sockets Layer

TB	Terabyte
TLS	Transport Layer Security
UEFI	Unified Extensible Firmware Interface
USB	Universal Serial Bus
vCPU	virtual Central Processing Unit
VDA	Virtual Desktop Access
VDevs	Virtual Devices
VDI	Virtual Desktop Infrastructure
VID	Virtualization Infrastructure Driver
VLAN	Virtual Local Area Network
VM	Virtual Machine
VMBus	Virtual Machine Bus
VMWP	Virtual Machine Worker Process
VPN	Virtual Private Network
VSC	Virtualization Service Client
VSP	Virtualization Service Provider
WAN	Wide Area Network
WinHv	Windows Hypervisor Interface Library
WMI	Windows Management Instrumentation
XD	eXecute Disable

1 ÚVOD

Tato bakalářská práce si pokládá za úkol seznámit čtenáře s problematikou virtualizace a zejména jejím využitím při nasazení technologie Microsoft Virtual Desktop Infrastructure. Jelikož je virtualizace v posledních letech čím dál tím více využívána, přicházejí tak na trh i nové funkce a možnosti v tomto odvětví.

V první kapitole teoretické části se čtenář seznámí s historií vzniku virtualizace a jejím postupným vývojem až do současné doby.

Druhá kapitola se bude zabývat virtualizací z teoretického pohledu. Čtenář se seznámí s definicí virtualizace a zjistí, jaké jsou různé typy virtualizací. Dále získá povědomí o tom, že novodobé virtualizační nástroje využívají několik typů virtualizací současně a dynamicky se rozhodují, který typ bude pro daný scénář virtualizace nejvhodnější. V další části druhé kapitoly budou zmíněny doporučené hardwarové požadavky virtualizace, kdy bude čtenáři vysvětleno několik pojmů tykajících se hardwarové podpory ze strany nejvýznamnějších výrobců procesorů. V závěru druhé kapitoly bude čtenáři poskytnuta polemika o výhodách a nevýhodách serverové virtualizace.

Ve třetí kapitole dojde k zaměření na hypervisor Hyper-V od společnosti Microsoft. S tímto hypervisorem budeme následně pracovat v praktické části bakalářské práce, jejíž celá náplň klade důraz na produkty společnosti Microsoft. Čtenář bude ve třetí kapitole seznámen se stručným vývojem hypervisoru Hyper-V a jeho architekturou. Dále bude popsáno porovnání výkonnostních limitů druhé a třetí generace tohoto hypervisoru. Závěrem třetí kapitoly bude výčet novinek, které byly implementovány do nejnovější generace serverového operačního systému Microsoft Windows Server 2012 R2.

Čtvrtá kapitola teoreticky popíše nejzásadnější část této bakalářské práce, kterou je technologie Microsoft Virtual Desktop Infrastructure. Čtenář bude v této kapitole seznámen se zmíněnou technologií a jejími alternativami. Dále získá povědomí o způsobu licencování zařízení přistupujících k virtuální vzdálené ploše.

Pátá kapitole bude zaměřena na praktické nasazení technologie Microsoft Virtual Desktop Infrastructure. Čtenář získá doporučení k nasazení VDI na základě praktických zkušeností autora této práce. Dále bude čtenáři popsán celý postup nasazení konkrétního scénáře Virtual Desktop Infrastructure. Na závěr páté kapitoly obdrží čtenář informaci nad rámec této práce a tou bude provedení aktualizace šablony klientského operačního systému.

2 ÚVOD DO PROBLEMATIKY

Virtualizací, která během pár uplynulých let nabrala na svém významu, se mimo jiné zabývají tři významné společnosti. Těmito společnostmi jsou Citrix, VMware a Microsoft. Společnost, která je považována za průkopníka virtualizace a která s touto myšlenkou přišla jako první, se jmenuje Citrix. Budeme brát v úvahu pouze základy virtualizace tak, jak je známe dnes. Mohli bychom jako průkopníka jmenovat IBM s jejich technologií využívanou nad sálovými počítači v 60. a 70. letech označovaných, jako mainframes, ale nás bude zajímat skutečný počátek novodobé virtualizace. Produkt námi jmenovaného průkopníka virtualizace nesl název Citrix WinFrame, do provozu byl uveden v roce 1995 a jednalo se o víceuživatelskou verzi Windows NT 3.51. Díky této aplikaci bylo možné, aby se uživatelé hlásili na WinFrame server a spouštěli aplikace. Microsoft zaregistroval, že by tato novinka mohla být příležitostí, a tak spojil síly se společností Citrix a společně nechali vzniknout speciální edici Windows NT 4.0 Terminal Server. Později se u Microsoftu stala tato technologie samostatnou součástí Windows, i když dnes je již známá jako Remote Desktop Services. Touto technologií disponují nejnovější operační systémy Microsoft Windows. (Computer Desktop Encyclopedia, 1981-2016)

Implementace Remote Desktop Services společností Microsoft nebyla konec pro společnost Citrix. Citrix nadále vyvíjí svá vlastní virtualizační řešení. Posledním produktem je Citrix XenApp, který slouží pro virtualizaci aplikací, a lze pomocí něho pouštět podnikové aplikace, které jsou umístěny na centrálním serveru. Dále vyvíjí Citrix XenServer, což je serverový hypervisor poskytující rozhraní pro virtualizaci hardwaru a běh více operačních systémů na jednom fyzickém serveru současně. Důležité je to, že velká část nástrojů pro virtualizaci od společnosti Citrix je distribuována zdarma a náklady na licence jsou spojené s koupí nástrojů pro správu virtuálního prostředí. (Computer Desktop Encyclopedia, 1981-2016)

VMware poprvé předvedl svůj produkt v roce 1999; nesl název VMware 1.0. Dnes je tento produkt známý pod názvem VMware Workstation. Jednalo se o první virtualizaci pracovní stanice na trhu. Nejprve se jednalo o prostředí sloužící k účelům vývoje, či testování různých operačních systémů. (Virten.net, 2015)

Na základě úspěchu této technologie se očekávalo rozšíření na trh serverů. Lidé si však zpočátku netroufali přenést svá produkční prostředí do prostředí virtuálního. K postupnému přechodu začalo docházet poté, když si firmy začaly uvědomovat, jaké nemalé finanční prostředky lze díky virtualizaci ušetřit.

Díky tomu, že lze na jeden fyzický server nasadit více serverů virtuálních vyplývá, že je efektivněji využit výkonnostní potenciál fyzického serveru a jsou sníženy nároky na energetickou spotřebu. Dále pak dochází k efektivnějšímu využívání IT infrastruktury z pohledu nabízení služeb a zdrojů. V případě nasazení nové služby není již nutné pořizovat nový fyzický server. Od toho se odvíjí i rychlost nasazení nového serveru. U virtuálních serverů tím také částečně odpadá starost o ovladače hardwaru, jelikož se o komunikaci s hardwarem stará samotný hypervisor. Celá infrastruktura je zároveň spravována z centrální konzole, takže je vše přehledně uspořádáno a přitom na jednom místě.

Díky virtualizaci je relativně snadné zajištění vysoké dostupnosti, což je konfigurace, kdy výpadek jednoho serveru nezpůsobí pád služeb celku. Výpadek jednoho fyzického serveru může být kompenzován dalšími servery. O tuto skutečnost se stará právě centrální konzole pro správu, která v případě poruchy fyzického serveru zajistí přesun služby na jiný definovaný fyzický server. Dle centrálního nástroje a jeho verze může dojít k přesunu, kdy bude výpadek velmi krátký nebo dokonce žádný. V oblasti virtualizace serverů už ale zabíháme k nástrojům, jako je například VMware ESX / ESXi Server.

I když už byl Microsoft zmíněn na začátku této kapitoly, ani služba Windows Server nazvaná Remote Desktop Services nezůstala dlouho osamocena. Microsoft vyvinul technologii Hyper-V, která tuto společnost posouvá do světa virtualizace koncových stanic a serverů. Hyper-V je k dispozici buď jako samostatná edice Microsoft Hyper-V Server, která je distribuována zdarma, nebo jako role instalovaná do operačního systému Windows Server. Hypervisor Hyper-V bude cílem této bakalářské práce. (Microsoft Corporation, 2015)

Prací na téma virtualizace koncových stanic se zabýval například Petr Lenz ve své bakalářské práci, kde popisoval přehled aktuálních virtualizačních řešení na trhu. Jeho práce se v první části zabývá dosavadními poznatky v oblasti virtualizace a ve druhé části je zaměřena na implementaci v komerčním sektoru. Práce není čistě zaměřena na řešení virtualizace od společnosti Microsoft. Dalším, kdo se věnoval zpracování informací o Microsoft Virtual Desktop Infrastructure, byl Bc. Luboš Mercl, který ve své diplomové práci zkoumá využití této technologie ve firemním prostředí. V rámci jeho diplomové práce vznikl návrh technického řešení virtuálních ploch, který je založen na řešení za použití nástrojů společnosti Microsoft. Tento návrh byl porovnán především z finančního hlediska s řešením využívajícím klasickou fyzickou infrastrukturu serverů.

3 VIRTUALIZACE

V následující kapitole budou zmíněny základní informace o virtualizaci a jejích jednotlivých typech. Mimo jiné bude pozornost věnována typům virtualizace, hardwarovým požadavkům virtualizace a dále pak jejím kladům a záporům.

3.1 Definice virtualizace

Virtualizací lze rozumět způsoby a techniky umožňující v jednom fyzickém počítači přistupovat k dostupným hardwarovým zdrojům jiným způsobem, než jakým skutečně existují, jsou vzájemně propojeny apod. Takové prostředí může být uživatelům jednodušeji přizpůsobeno a lze lépe skrýt pro ně nepodstatné detaily, jako například rozmístění hardwarových prostředků. Jedná se o abstrakci fyzických zdrojů od ostatních kooperujících zdrojů. (PANEK, 2013)

3.2 Typy virtualizace

Virtualizaci je možné provozovat na několika úrovních. V typech virtualizace vždy záleží na tom, v jakém prostředí je hostovaný operační systém provozován, jaký je mu poskytnut hardware a jaké má možnosti přístupu k tomuto hardwaru. Mezi základní typy virtualizace patří typy, které jsou uvedeny níže.

Softwarová emulace a simulace jsou nejstaršími technikami virtualizace. Základním principem emulátoru je překlad strojových instrukcí hostovaného systému na strojové instrukce hostitelského stroje. Jinými slovy: emuluje se i procesor včetně registrů a dalších částí. Dále se emuluje paměť ROM cílové platformy a zbytek hardwaru. I přes různé optimalizace (jednou přeložené úseky aplikace se ukládají do paměti, takže je není třeba při příštím volání znovu překládat) se jedná o nejméně efektivní způsob virtualizace. Jedná se o typ virtualizace, kdy je virtuální počítač vytvořen pomocí softwarových prostředků hostujícího operačního systému. Výhodou tohoto typu virtualizace je provoz hostovaného operačního systému a jeho aplikací i pro počítač s jinou architekturou, než má sám hostující systém, což znamená, že tu jde o nezávislost na hardwaru. Emulace je jediný způsob, jak virtualizovat jinou architekturu.

Paravirtualizace doprovázená **hardwarovou podporou virtualizace** využívá prvek, který se nazývá hypervisor. Ten vytvoří hardwarové prostředí pro virtuální stroj emulací fyzického hardwaru. Operační systém provozovaný ve virtuálním stroji je jakkoliv neupravený, nicméně v případě čisté paravirtualizace je nutné upravit jádro hostovaného operačního systému, aby

pracovalo se stupněm ochrany ring 1. S podporou hardwarové virtualizace musí hypervisor běžet na speciálním stupni ochrany (ring −1). Operační systém však na stejné úrovni běžet nemůže, protože by mohl ovlivnit práci hypervisoru. Nové procesory Intel a AMD mají zabudovánu podporu pro virtualizaci, která se v případě Intel jmenuje VT. Pro AMD je to AMD-V a zpřístupňuje již zmíněný speciální stupeň ochrany (ring -1) a další instrukce pro podporu virtualizace uvnitř procesoru. Procesory mají definovány 4 úrovně ochrany, tzv. okruhy (rings). Programy uživatelů běží s nejnižší úrovní ochrany (ring 3). Ring 1 a ring 2 jsou na podobné úrovni a využívají se jen zřídka. Hypervisor běží s nejvyšší úrovní ochrany (ring -1). Z toho tedy plyne, že operační systém, který na normálním počítači bez virtualizace běží s nejvyšší úrovní ochrany (ring 0), je zde provozován s druhou nejvyšší úrovní ochrany (tím pádem opět ring 0). Díky tomu je hostovaný systém nemodifikovaný a pracuje se standardními úrovněmi ochrany. Na druhé straně už nemůže provádět operace vyžadující privilegovaný přístup. Privilegované instrukce jsou automaticky identifikované hypervisorem, který se následně postará o jejich případné zpracování. (KRÁL & KRAHULEC, 2008)

Plná (nativní) virtualizace se nejčastěji používá na klientských pracovních stanicích. Virtuálnímu stroji je simulován potřebný hardware. Kompatibilita instrukční sady u hostovaného a hostujícího operačního systému není vyžadována, protože je kód vykonáván přímo na procesoru hostujícího systému, který je stejného typu. Výkon virtualizace nikdy nedosáhne výkonu fyzického stroje, protože musíme brát v úvahu režii na provoz hostujícího systému. Nejčastějšími zástupci tohoto typu virtualizace jsou: Microsoft Virtual PC, VMware Workstation a Oracle VirtualBox.

Bare-metal[1] a **hosted-based**[2] typy virtualizací jsou další dva pojmy, se kterými se lze setkat. Jedná se označení virtualizace z jiného pohledu. První uvedený typ bare-metal se vyznačuje tím, že virtualizační prostředí je instalováno přímo na fyzickém vybavení počítače, tedy přímo na hardware. Pro snížení režie je možno provést instalaci například na USB flash disk. Jednoduše lze tedy chápat tento typ jako virtualizaci bez mezičlánku v podobě hostujícího operačního systému. Proti tomu hosted-based, jak už název napovídá, je pravým opakem. U hosted-based typu virtualizace je nutné mít k dispozici hostující operační systém, který poskytne prostředí pro hostované virtuální stroje.

K typům virtualizace je vhodné na závěr dodat, že současné virtualizační nástroje nevyužívají striktně pouze jeden typ virtualizace, ale jsou schopny zmíněné typy kombinovat. Poté se na

[1] Holé železo – volný překlad autora.
[2] Na bázi hostitele – volný překlad autora.

základě instalovaného operačního systému ve virtuálním stroji a použitého hardwaru rozhodují, jaký typ virtualizace a jeho metody budou pro konkrétní virtuální stroj používat.

(GOLDEN, 2011)

3.3 Obecně doporučené hardwarové požadavky serverové virtualizace

Již z principu virtualizace vyplývá, že by měl mít hostitelský stroj dostatečný výkon pro běh více virtualizovaných systémů či aplikací. Jedním z důležitých požadavků pro dostatečný výkon je procesor s 64bitovou architekturou. Díky této vlastnosti může zařízení adresovat teoreticky až 2^{64} bajtů operační paměti, což odpovídá velikosti 16 exbibajtů v bajtově adresovatelné paměti, nebo také $1{,}8\times10^{19}$ různých hodnot. Tuto architekturu lze považovat za standard, takže ji již dnešní virtualizační nástroje uvádějí ve svých minimálních požadavcích pro jejich úspěšnou funkci a některé ji dokonce striktně vyžadují.

Jak jsme si vysvětlili výše, další důležitou vlastností moderních procesorů je hardwarová podpora virtualizace. V případě společnosti Intel je to již zmíněné VT a v případě společnosti AMD je to AMD-V. Nestačí, aby procesor tuto vlastnost pouze podporoval, je nutné mít ji v BIOS, případně v UEFI aktivovánu.

Další funkcionalitou moderních procesorů, která je využívána virtualizačními nástroji, je DEP (Data Execution Prevention). Jednotliví výrobci procesorů mají pro tuto funkcionalitu odlišné značení. AMD ji označuje jako NX (No eXecute), Intel jako XD (eXecute Disable). Data Execution Prevention slouží jako ochrana systému před malwarem a nesprávně napsaným softwarem pomocí sledování čtení a zápisů do paměti a zajišťuje, aby se stránky paměti obsahující data nemohly spouštět. Jelikož se při určitých typech virtualizace spouští na jednom systému více virtuálních strojů, je tudíž klíčové zajistit stabilitu hostitelského systému.

Dále můžeme mezi hardwarové požadavky zařadit určité typy (rozhraní) úložišť a různá vstupní a výstupní rozhraní. Mezi rozhraní úložišť se řadí například SCSI (Small Computer System Interface), SAS (Serial Attached SCSI), Fibre Channel a iSCSI (internet Small Computer System Interface). Pro všechna tato a další rozhraní musí být k dispozici ovladač, který bude spolupracovat s hostitelským systémem. Stejně tak pro další vstupní či výstupní rozhraní, jako například USB, COM a další. Pokud by nebyl ovladač k dispozici, hostitelský systém by nedokázal se zařízením pracovat.

Poslední hardwarový požadavek v našem stručném přehledu, o kterém se zmíníme, je síťové rozhraní. V ideálním případě je dobré mít více síťových rozhraní, kde se každé z nich bude starat o něco jiného, nebo spolu budou vzájemně kooperovat pro získání vyšší datové propustnosti. Více síťových rozhraní může být jednotlivě použito například ke komunikaci serveru s ostatními počítači v síti; další rozhraní může být vyčleněno na zálohování a nakonec je vhodné mít jedno síťové rozhraní určené na správu hostitele a virtuálních strojů.

(KELBLEY & STERLING, 2011)

3.4 Výhody a nevýhody serverové virtualizace

Výhody virtualizace jsou zřejmé už z její podstaty. V první řadě je dobré uvést využitelnost hardwarového vybavení fyzického stroje (serveru). V případě instalace operačního systému přímo na hardware se stává, že hardware je o mnoho výkonnější, než je pro daný operační systém zapotřebí. Tím dochází k tomu, že výkonnostní potenciál serveru není využit, a tomu lze předejít právě virtualizací. Díky virtualizaci jsme schopni na výkonný server nainstalovat více hostujících operačních systémů. Hostující operační systémy, z pohledu fyzického stroje, společně sdílí hardwarové prostředky, které jsou jim přiděleny. Tím zajistíme vyšší efektivitu využití celého serveru a samozřejmě také lepší využití jednotlivých hardwarových prostředků.

Ze zvýšené efektivity využití hardwaru vyplývá další výhoda, kterou je snížení nákladů na jejich pořízení a následný provoz. Kdybychom měli opět operační systém instalovaný přímo na server a potřebovali bychom více takových serverů, nezbývalo by nám nic jiného, než mít k dispozici potřebný počet fyzických serverů. Díky virtualizaci a vyšší efektivitě využití hardwaru je možné provést tzv. konsolidaci serverů, kdy je například několik fyzických serverů spojeno do jednoho virtuálního serveru. Tím je zajištěno snížení energetické náročnosti na provoz serverů a zároveň jsou sníženy náklady na jejich pořízení. Místo několika slabších serverů je zakoupen jeden výkonnější. Díky snížení počtu serverů snížíme i potřebu velkých rozvaděčů, místností, množství kabeláže, dalších síťových prvků a vydávaného tepla.

Když nebudeme provozovat více fyzických serverů, ale budeme provozovat například pouze jeden fyzický server, na kterém poběží více virtuálních strojů, bude to dále znamenat snížení náročnosti na údržbu a přehlednější správu fyzického stroje. Díky tomu dále docílíme toho, že v případě potřeby nasazení nového serveru v organizaci nemusíme připravovat jeho hardwarové prostředí, pouze vytvoříme nový virtuální server. Z toho tedy plyne časová úspora při správě a rychlejší nasazení nových virtuálních strojů. Přehlednost oceníme zejména

v případě vzdálené správy organizace, kdy vstoupíme do jediné administrační konzole, ze které jsme schopni provést většinu potřebných úkonů k zajištění provozu virtuálního serveru. Server lze vzdáleně restartovat, vypnout, spustit a celý proces sledovat. V případě vzdáleného přístupu na fyzický server, který má operační systém instalovaný přímo na hardware, nejsme schopni sledovat POST proces spuštění, pokud server nemá zabudovánu kartu pro vzdálenou správu nebo, v případě některých výrobců, nemá zaplacenu licenci pro využití této funkce. Takový server jsme schopni ovládat až po spuštění jeho síťových služeb, kdy se připojí k počítačové síti, nebo v našem případě k Internetu.

Již víme, že díky virtualizaci máme možnost provozovat více virtuálních strojů na jednom fyzickém serveru. To s sebou nese možnost instalace různých typů a distribucí operačních systémů. Na jednom fyzickém serveru lze například provozovat souběžně několik virtuálních strojů s operačním systémem Linux, klidně v různých distribucích. Na tom samém fyzickém serveru může být případně spuštěn jeden nebo více virtuálních strojů s operačním systémem Microsoft Windows. Kolik virtuálních strojů smíme souběžně spustit, nám určuje to, jak výkonný máme hardware a jaký výkon potřebujeme pro konkrétní virtuální stroje. Každý virtualizační nástroj má ve své specifikaci určeno, pro jaký typ a distribuci operačního systému, umožňuje bezproblémový provoz. Pokud operační systém, který potřebujeme instalovat, není uveden v seznamu podporovaných operačních systémů daného virtualizačního nástroje, neznamená to, že ho nelze provozovat. V takovém případě musí každý správce sám ověřit, zda vše funguje korektně. Jednoduše lze tedy na jednom fyzickém serveru provozovat virtuální telefonní ústřednu založenou na operačním systému Linux a zároveň serverový operační systém Microsoft Windows 2012 R2 s nainstalovanou rolí doménového řadiče.

U virtualizovaného operačního systému lze dále dynamicky přidělovat výkon, a to jak zvýšením, tak i snížením. Proto pokud je nějaký virtuální stroj nevytížený, může své prostředky uvolnit a poskytnout je jinému virtuálnímu stroji, který je zrovna potřebuje. Veškeré takové úkony řídí virtualizační nástroj (hypervisor) a on rozhodne, kterému virtuálnímu stroji přidělí či odebere prostředky. Dynamické přidělování výkonu však nepodporují všechny virtualizační nástroje.

Kladnou vlastností virtualizace je do jisté míry také zjednodušené zálohování. Jedná se o zálohování pomocí nástrojů přímo od výrobce virtualizačního nástroje, nebo častěji pomocí nástrojů třetích stran. Takový nástroj se připojí do konzole hypervisoru administrátorskými

právy, případně jinými právy umožňujícími zálohování. Postupně přenese na záložní medium soubory virtuálního stroje pomocí nastaveného typu zálohování (plné, přírůstkové, rozdílové).

Poslední významnou funkcionalitou virtualizace, kterou si stručně popíšeme, je živá migrace virtuálních strojů. Využijeme ji tehdy, pokud už máme v provozu nějaký virtuální stroj a potřebujeme z jistých důvodu pracovat s úložištěm, na kterém je daný virtuální stroj uložen, nebo po koupi nového diskového pole, případně při přesunu na rychlejší, pomalejší, či volnější disky. V takovém případě nám živá migrace umožní přesun virtuálního stroje do cílového umístění, které si zvolíme, aniž by byl zaznamenán jakýkoliv výpadek virtuálního stroje. Během migrace je virtuální stroj stále v provozu a je postupně přesunut do cílového umístění, aniž by byl narušen jeho chod. Pouze jeho výkon bude pravděpodobně částečně omezen, ale dostupnost zůstane zachována. (Microsoft Corporation, 2013)

Virtualizace s sebou nese spoustu výhod a dobrých funkcí, jak je patrné z předchozích odstavců. Nevýhody se hledají poměrně špatně. Jako možnou nevýhodu lze uvést například způsob licencování, kdy se může některým administrátorům zdát příliš komplikovaný, pokud nerozumí licenční politice daného výrobce virtualizačního nástroje nebo výrobce operačních systémů instalovaných ve virtuálních strojích.

Nejpodstatnější nevýhodou je však ta, že virtuální stroje jsou v menších firmách umístěny na jednom centrálním serveru. Když se porouchá, pak zkolabuje téměř vše podstatné. Velké firmy řeší tento problém pomocí clusterů, kdy je více serverů spojeno do jedné skupiny. V případě selhání některého ze serverů v clusteru na sebe přebírají odpovědnost ostatní servery. Při vysoké dostupnosti se dá případně využít i automatické vyvažování zátěže mezi servery, což není náplní této práce. Veškerý hardware, data i vše ostatní nezbytné ke správné funkci je v clusteru redundantní. U menších firem se spoléhá na tvorbu záloh a pravidelnou údržbu hardware. Díky vysoké dostupnosti a pravidelným zálohám se eliminuje nevýhoda centrálního serveru a tím pádem u virtualizace převažují její klady. Díky převaze kladných vlastností a možnosti pořízení bezplatných virtualizačních nástrojů postupně dochází k narůstajícímu využívání virtualizace nejen u velkých firem, ale i u těch menších.

Nutnost využití virtualizace je důležité vždy pečlivě promyslet a posoudit, zda se vyplatí, nebo jestli je vůbec vhodné ji využít. Ne každá počítačová infrastruktura je vhodná pro její nasazení. Například v případě, kdy firma využívá pouze jednu instalaci serverového operačního systému.

4 MICROSOFT HYPER-V

V předchozím textu jsme se seznámili s obecnými informacemi týkajícími se virtualizace. Dále se budeme zabývat virtualizačním nástrojem z dílny společnosti Microsoft a tím je Hyper-V. Tento hypervisor využijeme v praktické části jako roli instalovanou na serverovém operačním systému Microsoft Windows Server 2012 R2. Zmíněný operační systém i hypervisor Hyper-V jsou stěžejní pro naší další práci a budeme se zabývat zejména jimi.

4.1 Stručný přehled vývoje Hyper-V

Hypervisor Hyper-V byl ve své první verzi uveden na trh v červnu roku 2008 jako instalovaná role některých edic Windows Serveru 2008. V říjnu roku 2008 byl na trh uveden samostatný celek Microsoft Hyper-V Server 2008. Poté v říjnu roku 2009 byla vydána druhá generace, dostupná jako role ve Windows Serveru 2008 R2, případně jako samostatný produkt Microsoft Hyper-V Server 2008 R2, který je k dispozici zdarma. Funkcionalitu Hyper-V doplnily v únoru roku 2011 technologie Dynamic Memory a RemoteFX, obsažené v Service Packu 1 pro Windows Server 2008 R2. V září roku 2012 byla představena třetí generace Hyper-V, která je integrovanou součástí Windows Serveru 2012 a také klientského operačního systému Windows 8 Pro. V současné době je Hyper-V k dispozici jako integrovaná součást Windows Serveru 2012 R2 a Windows 8.1 Pro a Enterprise. Windows Server 2016 byl v době psaní této práce vydán pouze ve verzi Technical Preview 4, což je čtvrté vydání jeho testovací verze, takže zde nejsou uvedeny informace o chystaných změnách v nové verzi serverového operačního systému. (Microsoft Corporation, 2015)

4.2 Porovnání výkonnostních limitů Hyper-V

Pro představu si srovnáme druhou a třetí (prozatím aktuální) generaci hypervisoru Hyper-V z pohledu výkonnostních limitů. Nejprve začneme s limity hardwaru hostitelského stroje. U druhé generace hypervisoru byl maximální limit pro počet logických procesorů nastaven na hodnotu 64. U třetí generace se počet zvýšil až na 320 vláken procesorů. Kapacita fyzické operační paměti byla u druhé generace nastavena na maximální hodnotu 1 TB. Třetí generace navýšila limit na 4 TB. Množství virtuálních procesorů, které lze přidělit hostitelem se zvýšil z 512 u druhé generace na 2048 u generace třetí. V těchto limitech je patrný přibližně pětinásobný nárůst výkonnostních limitů z pohledu fyzického stroje.

Virtuálnímu stroji lze ve druhé generaci hypervisoru přidělit 4 virtuální procesory na jeden virtuální stroj, kdežto u třetí generace byl limit navýšen na 64 virtuálních procesorů, což je 16× více. Maximální limit pro fyzickou operační paměť přidělenou jednomu fyzickému stroji

je opět ve třetí generaci navýšen z původních 64 GB na rovný 1 TB, což také znamená 16× vyšší hodnotu. Množství současně spuštěných virtuálních strojů bylo ve třetí generaci navýšeno přibližně 2,7× z 384 na 1024 virtuálních strojů.

Třetí generace hypervisoru Hyper-V začala poskytovat hostujícím systémům funkci nazvanou NUMA (Non-Uniform Memory Access). NUMA optimalizuje přístup k lokální paměti v počítačových architekturách s více procesory, kde požadovaný čas přístupu k paměti závisí na umístění paměti vzhledem k procesoru. S NUMA může procesor přistupovat k paměti, která se vůči němu dá nazvat lokální, namísto přístupu ke vzdálené paměti. Tuto funkcionalitu využívají kromě hypervisoru Hyper-V třetí generace také jiné moderní operační systémy nebo aplikace vyžadující vysoký výkon, jakou je například SQL Server. Díky NUMA a svým optimalizacím mohou moderní systémy lépe plánovat běh vláken procesoru a zlepšit přidělování paměti. Následkem je pak zvýšení výkonu. Porovnání zmíněných parametrů ukazuje Tabulka 1.

Tabulka 1 – Porovnání výkonnostních limitů druhé a třetí generace Hyper-V, zdroj: (Microsoft Corporation, 2013)

	Množství zdrojů	Windows Server 2008 R2 Hyper-V	Windows Server 2012 R2 Hyper-V	Faktor zlepšení
Hostitel	Logické procesory	64	320	5×
	Fyzická operační paměť	1 TB	4 TB	4×
	Virtuální CPU na hostitele	512	2048	4×
Virtuální stroj (VM)	Virtuální CPU na VM	4	64	16×
	Operační paměť VM	64 GB	1 TB	16×
	Aktivních VM na hostiteli	384	1024	2,7×
	Podpora NUMA	Ne	Ano	

(Microsoft Corporation, 2013)

4.3 Architektura Hyper-V

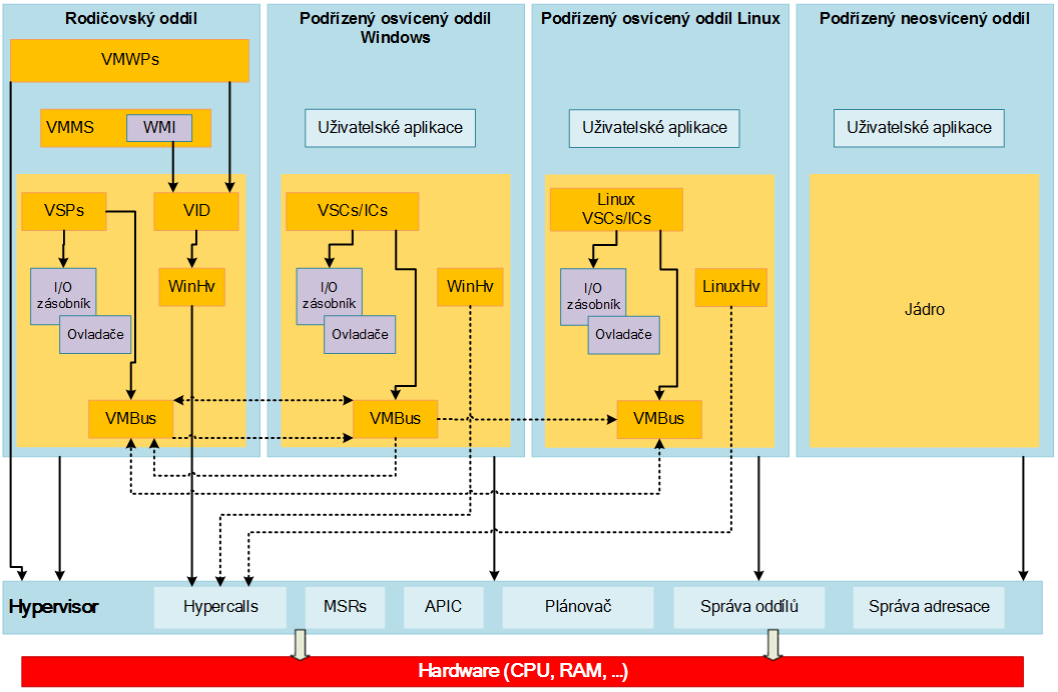
Hyper-V podporuje izolaci ve smyslu oddílů. Oddíl je logická jednotka izolace s podporou hypervisoru, kde je možné spouštět operační systémy. Hypervisor od společnosti Microsoft musí mít alespoň jeden rodičovský, neboli kořenový (root) oddíl, ve kterém je spuštěn Windows Server s Hyper-V. Virtualizační zásobník je spuštěn v rodičovském oddílu a má přímý přístup k hardwaru hostitelského stroje. Kořenový oddíl vytváří oddíly potomků nebo

je lze nazvat také podřízené oddíly, ve kterých jsou spuštěny hostující operační systémy. Tyto oddíly vytváří pomocí tzv. hypercall API (Application Programming Interface).

Oddíly s hostovanými operačními systémy nemají přístup k fyzickému procesoru, ani nemohou zacházet s přerušeními procesoru. Místo toho mají virtuální pohled na procesor a běží ve virtuálním adresním prostoru fyzické operační paměti, který je pro každý virtuální stroj privátní. O vše se stará hypervisor, který zachází s přerušeními procesoru a přesměrovává je na příslušný oddíl. Hyper-V umí také hardwarově urychlit překlad adres mezi různými virtuálními prostory hostů pomocí jednotky IOMMU (Input Output Memory Management Unit), která funguje nezávisle na hardwarové správě operační paměti pomocí procesoru. IOMMU se používá k přemapování adres fyzické operační paměti na adresy, které jsou používány podřízenými oddíly.

Podřízené oddíly nemohou přistupovat ani k dalším hardwarovým prostředkům. Oddílům potomků je poskytnut virtuální pohled na dané hardwarové zdroje pomocí virtuálních zařízení (VDevs). Požadavky na virtuální zařízení jsou směrovány buď na VMBus, nebo hypervisorem na zařízení v rodičovském oddílu, kde dojde k jejich obsluze. VMBus je logický vnitřní komunikační kanál. Rodičovský oddíl obsahuje poskytovatele virtualizačních služeb (Virtualization Service Providers, nebo zkráceně VSPs), které komunikují přes VMBus a slouží k obsluze požadavků přístupu k zařízení od podřízených oddílů. Podřízené oddíly naopak obsahují konzumenty virtualizačních služeb (Virtualization Service Consumers, nebo zkráceně VSCs), které přesměrovávají požadavky zařízení k VSPs v rodičovském oddílu přes VMBus. Celý tento proces je pro hostovaný operační systém transparentní.

Virtuální zařízení také mohou využít virtualizační funkci Windows Serveru, která se jmenuje Osvícený I/O (Enlightened I/O). Tato funkce je k dispozici pro úložná zařízení, síťové karty, grafické karty a vstupní periferie. Osvícený I/O je specializovaná funkce k podpoře virtualizace implementující vysokoúrovňové komunikační protokoly (například iSCSI), které využívají VMBus přímo a obcházejí ostatní emulační vrstvy zařízení. Díky tomu probíhá komunikace účinněji, ale jsou vyžadovány chytré prvky, kterými jsou hypervisor a VMBus. Hyper-V Osvícený I/O a hypervisor vědomý jádra jsou poskytnuty pomocí instalace integračních služeb Hyper-V. Integrační komponenty, které obsahují ovladače klienta virtuálního serveru, jsou k dispozici také pro ostatní klientské operační systémy.



Obrázek 1 – Architektura Hyper-V, upraveno dle: (Microsoft Corporation, 2016)

Popis jednotlivých bloků v diagramu:

- **APIC** – Advanced Programmable Interrupt Controller – zařízení, které povoluje přiřazení úrovní priorit k přerušením výstupů.
- **Podřízený oddíl** – Oddíl, který hostí hostovaný operační systém – veškerý přístup k fyzické paměti a zařízením podřízeného oddílu je poskytnut pomocí Virtual Machine Bus (VMBus), nebo hypervisorem.
- **Hypercall** – Rozhraní pro komunikaci s hypervisorem – rozhraní hypercall uzpůsobuje přístup k optimalizacím, které jsou poskytnuty hypervisorem.
- **Hypervisor** – Softwarová vrstva, která je umístěna mezi hardwarem a jedním nebo více operačními systémy. Jeho hlavní náplní je poskytnout izolované spouštěcí prostředí, které se nazývá oddíl, případně více oddílů. Hypervisor řídí a rozhoduje o přístupu k základnímu hardwaru.
- **IC** – Integration Component – komponenta, která umožňuje podřízenému oddílu komunikaci s ostatními oddíly a hypervisorem.
- **I/O zásobník** – Input/Output zásobník – vstupně výstupní zásobník.
- **MSR –** Memory Service Routine – běžné paměťové služby.

- **Rodičovský oddíl** – Spravuje funkce na úrovni počítače, jako jsou ovladače zařízení, správa napájení a připojení a odpojení zařízení za běhu. Rodičovský, neboli kořenový či root oddíl, je jediný oddíl, který má přímý přístup k fyzické operační paměti a ostatním zařízením.

- **VID** – Virtualization Infrastructure Driver – poskytuje služby pro správu oddílu, dále služby pro správu virtuálního procesoru a služby pro správu virtuální paměti daného oddílu.

- **VMBus** – Kanálově založený komunikační mechanismus používaný pro komunikaci mezi oddíly a specifickými zařízeními na systémech, které mají více aktivních virtualizovaných oddílů.

- **VMMS** – Virtual Machine Management Service – je zodpovědný za správu stavu všech virtuálních strojů v podřízených oddílech.

- **VMWP** – Virtual Machine Worker Process – komponenty uživatelského módu pro virtualizační zásobník. Pracovní proces poskytuje hostujícím operačním systémům v podřízeném oddílu služby pro správu z instance Windows Serveru v rodičovském oddílu. VMMS založí samostatný pracovní proces pro každý běžící virtuální stroj.

- **VSC** – Virtualization Service Client – instance umělého zařízení, které je umístěno v podřízeném oddílu. VSC zpracovává hardwarové zdroje, které jsou zprostředkovány poskytovateli virtualizačních služeb (VSPs) v rodičovském oddílu. Komunikují s odpovídajícími VSPs v rodičovském oddílu přes VMBus k obsloužení vstupně výstupních požadavků z podřízeného oddílu.

- **VSP** – Virtualization Service Provider – je umístěn v rodičovském oddílu a poskytuje podporu umělým zařízením v podřízených oddílech přes VMBus.

- **WinHv** – Windows Hypervisor Interface Library – je v podstatě mostem mezi ovladači operačního systému v podřízeném oddílu a hypervisorem. WinHv umožňuje ovladačům volat hypervisor pomocí standardních konvencí pro systémová volání v rámci systému Windows.

- **WMI** – VMMS odhaluje sadu nástrojů Windows Management Instrumentation na bázi rozhraní API pro správu a řízení virtuálních strojů.

(Microsoft Corporation, 2016)

4.4 Novinky Hyper-V ve Windows Serveru 2012 R2

- **Automatická aktivace virtuálních serverů** – Windows Server v edici Datacenter umožňuje provoz libovolného množství operačních systémů Windows Server, které jsou pokryty serverovou licencí. Nicméně je nutné servery aktivovat a stejně tak se musí provést opakovaná aktivace při přesunu virtuálního stroje mezi fyzickými servery. Windows Server 2012 R2 tuto starost odbourává, pokud je hostovaný operační systém také Windows Server 2012 R2. V takovém případě se virtuální server aktivuje automaticky.

- **Sdílený virtuální pevný disk** – je možné ho využít v případě propojení serverů do vysoce dostupného clusteru. Lze využít virtuální pevný disk s příponou .VHDX a zpřístupnit jej více virtuálním strojům najednou.

- **Klonování virtuálních strojů za běhu** – vybereme běžící virtuální stroj a bez přerušení jeho činnosti vytvoříme klon. Takový klon využijeme například ke zjištění problémů s daným softwarem. Klon necháme spuštěný mimo produkční prostředí. Po zjištění potíží pak opravíme závadu na problémovém virtuálním stroji v produkčním prostředí s minimální časovou náročností.

- **Storage QoS** – jedná se o minimální garantovanou a maximální možnou propustnost v IOPS (Input/Output Operations Per Second) vůči diskovému subsystému, kterou si sami zvolíme. Tuto možnost lze samozřejmě nastavit pro každý virtuální stroj samostatně tak, aby to dávalo smysl. Lze tím docílit zlepšení přístupové doby pro vytížené servery a ty méně využívané v rychlosti přístupu omezíme.

- **Nová generace virtuálních strojů** – v podstatě se od počátku role Hyper-V (tedy ve Windows Serveru 2008) využívá pro spuštění virtuálních strojů emulace dnes již staršího rozhraní BIOS se všemi jeho nevýhodami. Bylo však nutné zareagovat na nová rozhraní UEFI, Secure Boot a další novinky. Hyper-V ve Windows Serveru 2012 R2 tudíž přináší novou generaci virtuálních strojů, které emulují rozhraní UEFI a mohou využít již zmíněné Secure Boot a podobně. Podpora první generace virtuálních strojů zůstala však zachována.

- **Enhanced session mode** – často zmiňované omezení u Hyper-V bylo to, že pokud bychom se k virtuálnímu stroji připojili z Hyper-V konzole, nemohli bychom kromě pokynů z klávesnice a myši přenášet nic jiného. Zařízení USB, která byla připojená

k fyzickému počítači, virtuální stroj neviděl a nebylo ani možné přenášet soubory z fyzického počítače do virtuálního a naopak. Jediný způsob, jak se tomu dalo předejít, byl přístup přes klienta Remote Desktop. V tu chvíli už však bylo nutné mít virtuální stroj dostupný po síti a povoleny služby vzdálené plochy a bylo nutno znát jeho název nebo IP adresu. Windows Server 2012 R2 a Windows 8.1 tento nedostatek odbouraly. Pokud se na ně připojíme z Hyper-V konzole, máme k dispozici veškerý komfort, který by nám poskytlo RDS připojení.

- **Komprese živých migrací** – neboli live migration. Ta umožňuje přenos virtuálního stroje z jednoho hostitele na druhého bez přerušení jeho činnosti. Živá migrace je k dispozici už od Windows Serveru 2008 R2, ale byla zde značně vylepšena. Vylepšení přináší řazení migrací za sebou, paralelní migrace v libovolném počtu, migrace mimo cluster a další. Nejvýraznější změnou je to, že migrované stroje mohou být během migrace komprimovány a tím lze zajistit zkrácení času nutného k přenosu mezi hostiteli přibližně na polovinu.

- **Migrace mezi Windows Serverem 2012 a 2012 R2** – jedná se o usnadnění aktualizace fyzických hostitelů. Shared Nothing Live migrace umožňuje přenos virtuálního stroje z hostitele s Windows Serverem 2012 na hostitele s Windows Serverem 2012 R2 bez přerušení běhu virtuálního stroje.

- **Dynamická změna velikosti virtuálního pevného disku** – u dřívějších generací Hyper-V nebylo možné tento úkon provést bez vypnutí virtuálního stroje. V nové generaci je možné virtuální pevný disk připojený přes virtuální rozhraní SCSI libovolně zmenšovat a zvětšovat za chodu virtuálního stroje.

- **Hyper-V Replica** – již v předchozí verzi systému bylo možné provést repliku virtuálního stroje do vzdálené lokality, kde mohl být v případě havárie primárního datacentra uveden do provozu. Windows Server 2012 R2 tuto funkci posouvá ještě o krok dále, kdy je možné udělat repliku z repliky. Virtuální stroj tak může být v primárním datacentru a zároveň může být replikován do dvou dalších datacenter.

- **Podpora pro linuxové distribuce** – linuxové distribuce bylo možné provozovat již v předchozích generacích. Nicméně až nyní je možné takovému virtuálnímu stroji měnit velikost paměti za běhu.

- **Multi-tenant VPN gateway** – pokud v datacentru hostuje více různých klientů, je možné jim vytvořit vlastní virtuální síť a do ní připojit všechny jejich virtuální stroje. Jednotlivé sítě mohou mít dokonce stejné adresní rozsahy a navzájem se neovlivní a neuvidí. Když bylo v předchozí generaci hypervisoru nutné propojit virtuální síť s jinou virtuální sítí, s jejím připojením k Internetu, či VPN tunelem do vzdálené pobočky nebo sídla zákazníka, nastal problém. Musel k tomu být dokoupen hardwarový router, což bylo poměrně drahé zařízení. Windows Server 2012 R2 řeší tento problém integrovanou součástí systému, která se jmenuje Multi-tenant VPN gateway. Ta se stará o propojení a směrování mezi jednotlivými, ať už fyzickými, či virtuálními sítěmi.

Jelikož se budeme dále zabývat virtualizací klientských stanic, což je hlavní náplní této práce, zmíníme také vylepšení, kterých se VDI dočkala.

- **Práce s monitory** – nově je ve VDI podporováno otáčení monitorů, které se hodí zejména u přenosných dotykových zařízení. Dále je možné dynamicky přidávat a odebírat monitory, se kterými virtuální počítač pracuje, aniž bychom přerušili relaci.

- **Podpora DirectX 11.1** – využijeme ji v případě, pokud je v serveru umístěna výkonná grafická karta, která funkci DirectX 11.1 podporuje. Poté díky funkci RemoteFX dokážeme potenciál takové grafické karty využít.

- **Vylepšené znovupřipojení session** – v případě výpadku session, pokud jsme například na cestách, kde je připojení nestabilní, umožňuje Windows Server 2012 R2 rychlejší opětovné připojení k session. Většinou se dokonce obejde bez manuálního zásahu uživatele.

- **Zmenšení nároků na přenosové pásmo a diskový prostor** – vylepšené kompresní mechanismy umožnily snížení nároků na šířku síťového pásma o 50% oproti Windows Serveru 2012. Zároveň je v datacentru možné využít deduplikaci dat, která zajistí, že stejné sektory jsou na pevném disku uloženy pouze jednou, bez ohledu na to, v kolika virtuálních počítačích je daný sektor využit.

Dále budou stručně zmíněny ještě novinky, které pomohou správcům, kteří potřebují uživatelům jednodušeji zpřístupnit aplikace, soubory, nebo rovnou využít BYOD (Bring Your Own Device).

- **Workplace Join** – jedná se o nový stupeň autentizace v rámci firemního doménového prostředí. Je to stupeň, který nevyžaduje zařadit do domény soukromé zařízení uživatele a zároveň mu umožní přístup do sdílených složek a spouštění firemních aplikací. Takové zařízení se pouze zanese do Active Directory, a stane se tak důvěryhodným.
- **WorkFolders** – jde o novinku, která umožňuje zpřístupnění firemního souborového úložiště dokumentů do Internetu. Díky tomu mohou uživatelé pracovat s firemními daty ze svých zařízení. Jedná se o bezpečné řešení, které zajišťují další pokročilé mechanismy.
- **Web Application Proxy** – možnost, jak bezpečně a jednoduše publikovat firemní aplikace do Internetu. Uživatel je poté smí stáhnout, spustit a pracovat s nimi téměř odkudkoliv.
- **Active Directory Federation Services (ADFS)** – služby umožňující propojení našeho Active Directory prostředí s okolními aplikacemi a službami v cloudu. Jedná se o služby, díky kterým lze zajistit centrální autentizaci a autorizaci uživatelů.

(Externí autoři, 2013)

5 VIRTUAL DESKTOP INFRASTRUCTURE

V této kapitole se dostáváme k nejdůležitější části naší práce, která se zabývá tématem Virtual Desktop Infrastructure, dále jen VDI. Popíšeme si, co je VDI a probereme její výhody a nevýhody. Také si stručně představíme alternativy k VDI v případě nasazení v malých firmách nebo při scénářích nasazení, kde by se VDI nehodila. Na závěr stručně nastíníme způsob licencování a bezpečnost provozu VDI. Po teoretické stránce se o všem zmíníme jen krátce a některé další věci si popíšeme v praktické části této práce.

5.1 Seznámení s VDI

Jak jsme si řekli v předchozím odstavci, VDI je zkratka Virtual Desktop Infrastructure. Jedná se tedy o infrastrukturu virtuálních klientských počítačů. Tyto počítače jsou virtuální z pohledu jejich provozu, kdy jsou provozovány jako virtuální stroje na vybraném serveru nebo celém clusteru v datacentru. VDI umožňuje správcům IT poskytovat aplikace a virtuální plochy uživatelům na jejich různých zařízeních, jako jsou mobily, tablety, notebooky a osobní počítače. Centralizované poskytování aplikací a dat přes vzdálenou plochu umožňuje uživatelům přistupovat k jejich pracovním věcem odkudkoliv a z jakéhokoliv zařízení, je-li připojeno k Internetu a podporuje připojení ke vzdálené ploše pomocí protokolu RDP.

Na VDI je možné nahlížet ze třech různých pohledů:

- **Počítače na bázi relací sdílené plochy** – zde jsou zahrnuty nové zjednodušené způsoby pro konfiguraci a správu, takže lze snadno a rychle nasadit infrastrukturu pro jeden nebo více serverů Hostitele relace vzdálené plochy. Nastavení a přizpůsobení sady relací je umožněno zachovat pomocí disků profilů uživatelů.

- **Osobní a sdílené virtuální klientské počítače** – pomocí těchto nástrojů jsme schopni nasadit a spravovat sdílené virtuální klienty s využitím šablon virtuálních klientů. Dále podporují více typů úložišť, jako je SMB (Server Message Block) pro virtuální počítače nebo lokální úložiště. Uživatelská nastavení je možné zachovat díky diskům profilů uživatelů. Tento typ nás bude zajímat nejvíce v rámci praktické části.

- **RemoteApp** – jedná se o způsob, jak poskytnout uživatelům aplikace z hostitele místo úplné vzdálené plochy. Pomocí služby RemoteApp publikujeme aplikace, kterým je umožněn běh na klientských zařízeních souběžně s jejich lokálními aplikacemi. Publikované aplikace můžeme integrovat s nabídkou Start pro snazší spouštění.

(Microsoft Corporation, 2015)

5.2 Alternativy k VDI

Ne vždy je VDI tím nejlepším řešením využití infrastruktury pro daný scénář. Někdy je to z důvodu bezpečnosti, nebo když každý uživatel vyžaduje specifické nastavení své pracovní stanice. Mezi alternativní řešení, která Microsoft poskytuje, patří tři následující možnosti.

5.2.1 App-V

Jedná se o zkratku Application Virtualization, kde nám tato alternativa nenabízí specifická nastavení pracovních stanic, nicméně díky ní můžeme snáze nasadit software na klientské stanice. Funguje na následujícím principu. Máme vytvořený balíček, který je umístěný na centrálním serveru. Uživatel má k dispozici ikonu, po jejímž otevření se aplikace stáhne a zároveň spustí. Jedná se o řešení pro nasazení softwaru a do jisté míry lze tímto řešit i potíže s kompatibilitou.

5.2.2 MED-V

Microsoft Enterprise Desktop Virtualization využijeme nejvíce v případě, kdy je naším problémem kompatibilita aplikací. Zejména se tak děje v případě, kdy nasazujeme nejnovější operační systémy od společnosti Microsoft, avšak naše aplikace již nejsou schopné s nimi spolupracovat. Jedná se o obraz systému Windows XP, který běží v odděleném virtuálním stroji ve Virtual PC. Z takto vytvořeného virtuálního stroje máme možnost spouštět aplikace, standardizovat tento virtuální stroj a případně ho nasadit k využití dalším uživatelům nebo ho nasadit k využití centralizovaně.

5.2.3 RDS

Remote Desktop Services, nebo starším názvem Terminálové služby. Zde se nejedná o žádnou virtualizaci hardwarových prvků, ale v rámci jednoho serveru nám běží několik virtuálních desktopů, neboli session. Uživatel není nijak izolován od serverového operačního systému, takže chyba jednoho uživatele v jeho připojené relaci může ovlivnit práci ostatních uživatelů, nebo dokonce způsobit pád serveru. Jedná se však o řešení, které je ekonomicky velice přívětivé, a zároveň je jeho nasazení poměrně snadné a rychlé.

5.3 Způsob licencování VDI

V první řadě budeme uvažovat to, že serverové operační systémy pro námi využívané servery určené k běhu prostředí VDI máme správně licencovány a současně s tím i operační systémy pro virtuální klientské počítače. Za takového předpokladu bude předchozí část vynechána. Je velmi důležité si uvědomit, že právo na přístup k virtuální instanci plochy vychází vždy ze správně licencovaného zařízení, ze kterého k virtuální ploše přistupujeme.

Licence, která zajišťuje právo přístupu k virtuální ploše, se jmenuje Virtual Desktop Access (VDA). Pořizuje se pro každé zařízení přistupující k virtuální ploše a dává zařízení právo přistupovat až ke čtyřem virtuálním plochám.

Licence VDA je předplatným se stabilní měsíční cenou a dodává se prostřednictvím tříletých smluv, kde se pokrytí hradí vždy předem až do následujícího výročí (tedy na rok). VDA je součástí aktivního pokrytí služby Software Assurance pro pracovní stanice. Software Assurance je služba, kterou můžeme k pracovní stanici pořídit v některém z multilicenčních programů společně s Windows Upgrade.

V případě, že máme zařízení, které nespouští operační systém Windows (například tenký klient) a není k němu možné pořídit službu Software Assurance, je pro něho potřeba pořídit samostatnou licenci VDA také v některém z tříletých multilicenčních programů. Samostatná licence VDA je vhodná rovněž v případě, kdy potřebujeme udělit právo přistupovat k virtuální ploše externímu uživateli se zařízením, které není v majetku společnosti provozující VDI. Pokud totiž společnost nevlastní podkladový operační systém, nemůže na něho pořídit ani upgrade se Software Assurance.

Licenci VDA je možné zakoupit jak ve formě per User (na uživatele), tak per Device (na zařízení). Licence typu per User opravňuje jejího nositele přistupovat k virtuální infrastruktuře odkudkoliv a z jakéhokoliv zařízení.

Dále je potřeba nezapomenout, že VDI se obvykle nedělá kvůli virtuální ploše jako takové, ale kvůli aplikacím, které bude uživatel využívat. Ty mají také svá licenční pravidla. V případě aplikací Microsoft jde o fakt, že krabicové ani OEM licence takový provoz nedovolují. Musí jít o aplikaci pořízenou prostřednictvím multilicenčního programu.

Závěrem je dobré si uvědomit, že VDI neznamená úsporu po licenční stránce. Ve většině případů je to spíše naopak – licenčně je to dražší řešení. Platí se totiž dodavateli licencí a produktů navíc za to, že úspora pro zákazníka přichází někde jinde, a to na úrovni správy a provozu.

5.4 Bezpečnost VDI

Na bezpečnost VDI je možné nahlížet minimálně ze dvou různých pohledů, které si nastíníme. Zaprvé z pohledu komunikace po síti WAN a zadruhé z pohledu práce s daty.

5.4.1 Bezpečnost z pohledu komunikace

Připojení k virtuální ploše probíhá přes protokol RDP. Tento protokol využívá šifrovaný kanál využívající šifrovací vrstvu SSL/TLS, který zabraňuje komukoliv sledovat spojení odposloucháváním na síti. Nicméně měl tento protokol před pár lety bezpečnostní trhlinu, kdy bylo možné uskutečnit neautorizovaný přístup ke spojení pomocí útoku Man in the middle[3]. Tento problém je však již od verze 6.0 vyřešen. Aktuální verze protokolu RDP se nachází ve verzi 8.0.

Pokud však budeme provozovat vzdálenou plochu po sítích WAN, existuje spousta opatření, která je dobré zvážit z důvodu vyšší bezpečnosti. Takovými řešeními jsou například ta, že je vhodné mít nainstalovaného vždy nejnovějšího klienta vzdálené plochy, omezit pravidla na firewallu, využít Network Level Authentication, které je standardně využíváno již od Windows Vista, nebo definovat maximální počet přihlášeních uživatelů vzdálené plochy.

Nejlepšími praktikami jsou však změna portu, který naslouchá komunikaci pro připojení vzdálené plochy, čímž se předejde útokům hackerů, kteří skenují výchozí RDP port, a zejména je důrazně doporučeno využít tzv. RDP Gateway, dále jen RDG, kterou si představíme.

V případě, že je nutné publikovat přístup na vzdálené plochy, do vnitřní podnikové sítě nebo přístup k RemoteApp přes síť WAN nebo Internet, přichází na řadu již zmíněná RDG. Služba RDG přináší zabezpečený přístup navázáním tunelového SSL spojení mezi klientem a RDG serverem. RDG server pak působí jako prostředník v komunikaci. Klient s RDG serverem komunikuje na zabezpečeném portu 443 a RDG server komunikuje se zařízeními ve vnitřní síti dále na portu 3389, což je výchozí port pro RDP.

RDG umožňuje specifikovat uživatelům, kam mají ve vnitřní síti přístup, a lépe řídit jejich restrikce, což je ohromná výhoda oproti VPN, kde většinou uživatel dostane přístup k celé síti. Díky RDG je možné přistupovat do vnitřní sítě i z různých hotspotů nebo veřejných internetových kaváren, protože port 443 bývá pro komunikaci standardně povolen. Dále je možné vystavit certifikát pro klientská zařízení, kdy je komunikace mezi RDG a klientem lépe šifrována. V tom okamžiku se dá komunikace mezi nimi považovat za dokonale bezpečnou.

[3] Člověk uprostřed – volný překlad autora. Jedná se o útok, kdy útočník přesměruje síťovou komunikaci na sebe a pro stranu A se jeví jako strana B a naopak. Poté dokáže komunikaci nepozorovaně odposlouchávat a případně měnit.

Hlavní benefity, které RDG přináší, jsou tedy zřejmé. Uživatel nedostane přístup k celé firemní síti, je zjednodušena komunikace díky lepšímu průniku přes firewally pomocí zabezpečené komunikace na portu 443 a umožňuje sdílet síťové připojení s dalšími programy běžícími na počítači. To znamená, že nám k odesílání a přijímání dat přes vzdálené připojení umožní používat připojení našeho poskytovatele Internetu namísto využívání podnikové sítě.

(University of California Berkley, 2016)

5.4.2 Bezpečnost z pohledu práce s daty

Bezpečnost je v této situaci zajištěna díky nejnovějším dostupným technologiím poměrně dobře. Bezpečnosti uložení dat napomáhají technologie, jako jsou například RAID, kde jsou data uložena na více discích, a tím pádem odolná proti poškození disků, nebo vysoká dostupnost, díky níž je provoz zajištěn i v případě poruchy fyzického serveru.

Nad tím vším je ochrana proti síťovým napadením, která spočívá v dobře navržených pravidlech na firewallu, nebo správné užití VLAN a již zmíněná Remote Desktop Gateway, ale to už se opět blíží k ochraně z pohledu komunikace, kterou jsme již probrali.

5.5 Plánování kapacity výkonu pro provoz VDI

V první řadě je velmi důležité podotknout, že hardwarové požadavky se mohou pro jednotlivé scénáře nasazení VDI lišit. Proto je doporučeno mít pro nasazení VDI, ať už v novém firemním prostředí, nebo při přechodu ze stávajícího fyzického prostředí, vypracován projekt, který bude zkoumat požadavky uživatelů. Na základě toho budeme schopni odhadnout potřebné hardwarové vybavení. Dále je pak dle dokumentu od Microsoftu, který se zabývá plánováním kapacity, vhodné využít možnost simulace na základě nasbíraných dat. Další možností je nasazení pilotního serveru, na který se budou uživatelé připojovat. Na základě jejich zpětné vazby bude vyhodnocen závěr a získána představa o náročnosti daného scénáře nasazení. Takový server by však neměl obsahovat důležitá firemní data, aby jej bylo možné jakkoliv modifikovat, či úplně zrušit a nahradit novou instalací.

Již zmíněný dokument od Microsoftu vychází z výsledků testování, kterých bylo dosaženo společně se společností Dell na jejich fyzických serverech. Popisuje plánování výkonnostní kapacity až pro 2 000 klientských spojení. Dokument je uveden v seznamu použité literatury pro tuto práci a je online k nahlédnutí.

Dle daného dokumentu lze říci, že faktorů, které ovlivňují požadavky na hardware, je nepřeberné množství. Mezi takové faktory se řadí například počet uživatelů, kteří se budou

současně připojovat k serveru, nebo typ softwaru, který budou uživatelé používat. Je rozdíl, zda budou uživatelé psát dokumenty v Poznámkovém bloku nebo ve Wordu, případně budou využívat modelovací software, který zatěžuje procesor a je náročný na operační paměť.

Vzdálené virtuální stroje mohou pracovat s dynamickým přidělováním operační paměti, kdy jim lze nastavit hodnoty startovací a maximální kapacity spotřebované operační paměti. Znamená to tedy, že virtuální stroj, který není plně vytížený, může uvolnit své prostředky jinému virtuálnímu stroji. Doporučuje se mít vše dostatečně dimenzováno tak, aby nám kupříkladu nechyběla operační paměť v případě plného vytížení všech virtuálních strojů, které mohou být spuštěny současně.

Následující tabulky vycházejí ze stejného dokumentu, který byl již zmíněn. Shrnují naměřené údaje na softwarově jednoduchém scénáři nasazení VDI, kdy virtuální plochy uživatelů obsahovaly vzdálený operační systém Microsoft Windows 8, kancelářský balík Microsoft Office 2013, běžně dostupný prohlížeč Internet Explorer a manipulovalo se s nimi.

Tabulka 2 – Střední pracovní zátěž serveru, zdroj: (Microsoft Corporation, 2013)

Hustota VM	10 uživatelů/jádro @ ~80% CPU, s jedním vCPU na uživatele
Operační paměť	1 GB RAM pro jednu instanci Windows 8 s Office 2013
IOPS	10 IOPS/VM
Vytížení sítě LAN	~400 Kbit/sekunda (střední zátěž měřená pomocí Login VSI)

Údaje v Tabulce 2 byly měřeny pomocí softwaru Login VSI na serveru s procesorem Intel® Xeon® E5-2690 (20MB Cache, 2.90 GHz, 8.00 GT/s Intel® QPI).

Tabulka 3 – Paměťové požadavky pro různé počty uživatelů, zdroj: (Microsoft Corporation, 2013)

Počet uživatelů	Počet patic CPU	Velikost RAM	Velikost HDD	Zatížení úložiště dat	Provozní zátěž LAN
150	2	192 GB	1 TB	1 500 IOPS	60 Mbps
600	8	768 GB	3 TB	6 000 IOPS	240 Mbps
1 200	16	1,5 TB	5 TB	12 000 IOPS	480 Mbps
2 100	28	3 TB	10 TB	21 000 IOPS	1 Gbps

Údaje v Tabulce 3 byly měřeny na serverech v clusteru s procesorem Intel® Xeon® E5-2690 (20MB Cache, 2.90 GHz, 8.00 GT/s Intel® QPI), 192 GB operační paměti a 10× HDD s 15 000 otáčkami v konfiguraci RAID 1 + 0.

Tabulka 4 – Počty serverů pro různé počty uživatelů, zdroj: (Microsoft Corporation, 2013)

Počet uživatelů	Počet serverů VDI
150	1
600	4
1 200	8
2 100	14

Tabulka 4 vychází z hodnot v předchozích tabulkách. Dále byly v testovacím scénáři využity další dva servery pro běh doprovodných služeb. Jednou z doprovodných služeb byl například SQL server, kde si Remote Desktop Connection Broker v případě vysoce dostupného clusteru ukládá informace o nastavení nasazení virtuálních strojů. Další doprovodnou službou byl samotný Remote Desktop Connection Broker, který slouží jako mezičlánek mezi klientem a servery ve vysoce dostupném clusteru v datacentru poskytujícími služby VDI.

K tomu všemu bylo využito ještě diskové pole, které obsahovalo data profilů uživatelů. Velikost úložného prostoru pro data uživatelů se odhaduje poměrně dobře, jelikož se jedná o součin počtu uživatelů a množství diskového prostoru, který chceme jednotlivým uživatelům přiřadit. Pokud tedy požadujeme přiřadit 10 GB diskového prostoru pro 50 uživatelů, budeme potřebovat diskové úložiště o kapacitě alespoň 500 GB. Takové úložiště je vyhrazeno pouze pro profily (data) uživatelů a přičítá se k požadované velikosti úložiště pro běh serverů s VDI.

(Microsoft Corporation, 2013)

6 PRAKTICKÉ NASAZENÍ MICROSOFT VDI

V následující kapitole bude popsán způsob instalace rolí a služeb na servery, které jsou požadovány pro provoz VDI. Dále bude popsán způsob rozmístění rolí na jednotlivé servery, aby bylo docíleno nejvyššího možného výkonu serverů. Celá kapitola bude poté sloužit jako návod pro nasazení VDI v produkčním prostředí. Názvy prvků budou většinou pojmenovány v anglickém jazyce, jelikož je to v terminologii informačních technologií běžné a předpokládá se, že ten, kdo následující návod využije, má již alespoň drobné znalosti z oboru IT. Některé názvy dokonce nemají plnohodnotné synonymum v českém jazyce.

6.1 Doporučení před instalací VDI

Podstatnou informací k nasazení VDI je ta, že role hypervisoru Hyper-V musí být nainstalována na fyzickém serveru, nikoliv ve virtualizovaném prostředí. Jsou tedy dva různé způsoby, jak toho docílit. Prvním způsobem je instalace hypervisoru Microsoft Hyper-V Server 2012 R2 přímo na fyzický server. Druhým způsobem je instalace serverového operačního systému Microsoft Windows 2012 R2 přímo na fyzický server a do této instalace operačního systému bude přidána role hypervisoru Hyper-V. Tuto podmínku je možné obejít, nicméně se to však nedoporučuje, a proto je vhodné držet se této podmínky.

Důležitým předpokladem je dále to, že v počítačové síti by měl být aktivní DHCP server, který bude přidělovat IP adresy virtuálním počítačům. Tento DHCP server musí mít správně nastavenu IP adresu primárního DNS serveru, která bude našemu DNS serveru přiřazena po jeho instalaci. V případě, že by DHCP server přiděloval špatnou IP adresu DNS serveru, vznikl by problém s přiřazením virtuálních počítačů do počítačové domény.

6.2 Přehled požadovaných rolí k nasazení Pooled VDI

Následující role jsou vyžadovány pro nasazení VDI. Jejich množství je upraveno na nejnižší možný počet pro bezproblémové nasazení scénáře v prostředí, kde není využívána vysoká dostupnost služeb.

AD-DS – Active Directory Domain Services jsou adresářové služby řídící komunikaci mezi uživatelem a doménou, nebo počítačem a doménou. Dále zajišťují proces přihlašování uživatelů do operačního systému a autentizaci a autorizaci uživatelů, počítačů a služeb. Data jsou uchována v hierarchicky uspořádané databázové struktuře. Server, který provozuje roli AD-DS je v českém jazyce označován jako doménový řadič.

DNS – Domain Name System je role serveru, využívající hierarchické uspořádání doménových jmen. Slouží k překladu IP adres na doménová jména a naopak. Jeho využití je naprosto zřejmé, jelikož si lidský mozek mnohem lépe pamatuje slovní názvy oproti číselným adresám. Tato role bude automaticky přidána v průběhu instalace AD-DS.

Remote Desktop Services – role Vzdálená plocha nabízí technologie, které uživatelům umožňují připojovat se k virtuálním klientům, aplikacím RemoteApp a klientům na bázi relace. Se službou Vzdálená plocha mají uživatelé přístup ke vzdáleným připojením z firemní sítě nebo Internetu. Následující služby jsou dostupné pomocí Remote Desktop Services.

- **Remote Desktop Connection Broker** – jedná se o Zprostředkovatele připojení ke vzdálené ploše. Lze ho označit jako mezičlánek mezi klientem a serverem v datacentru. Pokud se klient pokusí přistoupit do datacentra k serveru poskytujícímu terminálové služby, RDCB se postará o jeho obsloužení. Funkce RDCB spočívá v kontrole pověření přistupujícího uživatele a v případě, že má uživatel již aktivní relaci, zabrání vytvoření nové relace a přiřadí mu již vytvořenou. To znamená, že pokud se uživatel ať už úmyslně, nebo neúmyslně odpojí z jeho relace, může se znovu do této relace připojit, aniž by přišel o svou neuloženou práci. RDCB rovnoměrně distribuuje zátěž v případě, že se v serverové farmě nachází více hostitelů relací vzdálené plochy. Další významnou funkcí je poskytování přístupu k virtuálním plochám a programům RemoteApp hostovaným na hostitelských serverech.
- **Remote Desktop Virtualization Host** – hostitel virtualizace vzdálené plochy je propojen s hypervisorem Hyper-V k nasazení vyčleněného (pooled), nebo osobního (personal) virtuálního počítače z předdefinované kolekce virtuálních počítačů.
- **Remote Desktop Session Host** – umožňuje serveru hostovat programy RemoteApp, nebo vzdálené plochy na bázi relace.
- **Remote Desktop Web Access** – tato služba umožňuje přistupovat k programům RemoteApp a vzdáleným plochám na bázi relace přes nabídku Start nebo pomocí webového prohlížeče.
- V prostředí, kde se požaduje, aby bylo VDI dostupné přes Internet, je využívána služba **Remote Desktop Gateway**. Pomocí této brány lze k VDI přistupovat bez nutnosti využití připojení k firemní počítačové síti pomocí VPN, pokud je v ní správně nastaveno směrování. Dále je pro přístup k Remote Desktop Session Host a VDI nutné

využít službu **Remote Desktop Licensing**, pomocí níž je zajištěno přiřazení licencí uživatelům (per User), nebo zařízením (per Device), která k nim přistupují.

Hyper-V – hypervisor, který zprostředkovává virtuální prostředí. Více detailů bylo popsáno v teoretické části. Tuto roli můžeme mít předinstalovanou ve formě fyzické instalace na server a v případě instalace role serverového operačního systému bude instalována během nasazení VDI, pokud nebyla předem připravena.

Internet Information Services – jedná se o roli Microsoft Windows Serveru poskytující webové služby. Tato role se nainstaluje automaticky během nasazení VDI.

File and Storage Services – souborové služby zajišťující sdílení složek a správu souborových serverů a úložišť. Tyto služby se nainstalují automaticky, jakmile bude u některé složky nastaveno sdílení.

6.3 Rozložení rolí mezi servery

Tato kapitola je napsána spíše pro zamyšlení. V případě, že bude čtenář této praktické části nasazovat VDI dle informací v ní uvedených, je vhodné, aby uvážil, jakou roli na který server nainstalovat. Rozložení rolí není možné nijak jednoznačně předepsat, jelikož záleží na aktuálním scénáři nasazení, počtu dostupných serverů, množství dostupného výpočetního výkonu a rychlosti, množství nebo typu úložišť. Tyto parametry nejsou jediným omezením, ale dají se považovat za velmi důležité. Jistě by se dala najít i další podstatná omezení, která by se k požadovanému scénáři nasazení vztahovala.

Příkladem úvahy čtenáře může být například to, že Terminálové služby není vhodné instalovat společně s Active Directory Domain Services a Domain Name System na jeden serverový operační systém. Jednoduše lze říci, že není vhodné instalovat Terminálové služby na doménový řadič provozující DNS z důvodu bezpečnosti. V takovém případě by uživatelé přistupovali vzdáleně k doménovému řadiči a ve chvíli výskytu nějaké chyby by nad ním mohli získat kontrolu, případně ho zavirovat, nebo dokonce odstavit mimo provoz.

Pokud by k takové situaci došlo, mohly by v případě výpadku AD-DS přestat fungovat určité služby na serverech, které se spouští s oprávněním definovaného doménového uživatele a tím pádem se ověřují jeho doménovým účtem. Dále by se uživatelům nemuselo podařit přihlášení k operačnímu systému, případně k jiným firemním portálům, které by používaly doménové ověření.

V případě nedostupnosti DNS by pak vyvstal problém v síťové komunikaci, kde by se využívala doménová jména namísto IP adres. Například při zálohování na síťové úložiště, nebo pokud by DHCP server přiděloval klientským stanicím právě tento DNS server, bylo by uživatelům znemožněno prohlížení Internetu, jelikož by opět nedošlo k překladu doménového jména na IP adresu.

Tato úvaha je jen jednou z možných variant a slouží jako vzorová úvaha. Podobný rozbor všech rolí by měl před jejich instalací na servery provést každý administrátor, aby předešel případným problémům, vhodně rozložil zátěž mezi servery a zajistil jejich bezpečný provoz.

6.4 Instalace Hyper-V

Tato kapitola popisuje instalaci Hyper-V přímo na fyzický server, nebo jako roli serverového operačního systému. Tato instalace není nijak složitá, stačí se pouze držet průvodce instalací a dostatečně číst vše, co napovídá.

6.4.1 Instalace jako samostatný operační systém

Instalaci tohoto typu provedeme pomocí zaváděcího média typu DVD nebo USB flash disk. Na takovém médiu máme připravenu instalaci systému, kterou na fyzickém serveru spustíme a pomocí průvodce nastavíme všechna požadovaná nastavení, jako je jazyk, poloha, kapacita disku a další. Následně necháme vše automaticky proběhnout a na závěr na vyžádání nastavíme heslo administrátorského účtu. Poté lze nainstalovat aktualizace nebo nastavit další detaily pro běh systému a pro jeho komunikaci v počítačové síti. Po instalaci aktualizací a provedení nastavení je nutné připojit fyzický server do počítačové domény, pokud je k dispozici již funkční doménový řadič. To lze případně provést dodatečně.

6.4.2 Instalace jako role serverového operačního systému

V tomto případě je požadováno mít nainstalovaný serverový operační systém Windows Server 2012 R2. Po spuštění Správce serveru (Server Manager) zvolíme Manage a následně Add Roles and Features. Po otevření průvodce přidáním rolí přeskočíme první krok a poté ve druhém kroku zvolíme Role-based or feature-based installation. Třetí krok umožňuje provést výběr serveru ze skupiny serverů, které v ní jsou přidány. Pokud zatím není vytvořena žádná skupina serverů a průvodce přidáním rolí je spuštěn na serveru, na kterém bude Hyper-V instalováno, bude k dispozici výběr pouze tohoto serveru. Čtvrtý krok slouží k výběru role, která bude instalována. V něm zatrhneme volbu Hyper-V a potvrdíme dialogové okno s výzvou k přidání doplňků, které necháme ve výchozím stavu. Klikneme na tlačítko Next a v pátém kroku také, jelikož v něm není možné provádět změny. Šestý krok zůstane

ponechán ve výchozím stavu a klikneme na tlačítko Next. V sedmém kroku na záložce Virtual Switches zvolíme síťový adaptér serveru, pro který požadujeme vytvořit virtuální přepínač (switch) sloužící ke komunikaci virtuálních strojů se serverem a zbytkem firemní počítačové sítě. Záložka Migration by měla být ve výchozím stavu nezatržená, takže ji v tomto stavu ponecháme a klikneme na tlačítko Next. V devátém kroku na záložce Default Stores bude proveden výběr výchozích umístnění pro konfiguraci virtuálních strojů a pro jejich virtuální pevné disky. Na předposlední záložce Confirmation zatrhneme volbu Restart the destination server if required a klikneme na tlačítko Install. Spustí se instalace a po restartu serveru se otevře okno s informací o jejím výsledku.

6.5 Vytvoření nového virtuálního stroje

Ke správě hypervisoru Hyper-V bude v tomto případě sloužit Hyper-V Manager. Po jeho spuštění zadáme nové připojení k serveru a zadáme jeho IP adresu nebo doménové jméno. Tuto variantu využijeme při instalaci hypervisoru Hyper-V přímo na fyzický server. V případě instalace role Hyper-V do serverového operačního systému je možné využít Hyper-V Manager instalovaný přímo daném serveru, který se s hypervisorem Hyper-V spojí automaticky.

Pokud je spojení navázáno, zvolíme v pravé horní části Správce Hyper-V položku New a následně Virtual Machine. Průvodce vytvořením nového virtuálního stroje poté zařídí definici virtuálního stroje, u kterého bude hypervisor znát jeho název, kde budou uloženy jeho virtuální disky, jakou kapacitu budou tyto virtuální disky mít, k jakému virtuálnímu přepínači bude připojen, jakou bude mít kapacitu startovací operační paměť nebo zda se bude využívat její dynamické přidělování.

Detailnější nastavení virtuálního stroje se provádí až po jeho definici. V přehledu virtuálních strojů na něho klikneme pravým tlačítkem myši a zvolíme položku Settings. Následně lze nastavit detailní požadavky na virtuální hardware, kolik čeho bude virtuální stroj mít a jakými komunikačními porty bude disponovat.

Důležitým nastavením je i to, že je virtuálnímu stroji možné vložit do virtuální mechaniky obraz DVD s instalačními soubory klientského operačního systému. Zmíněná možnost usnadní práci při instalaci operačního systému virtuálnímu stroji.

Tato nastavení je vhodné provádět, když je virtuální stroj vypnutý, jelikož při zapnutém virtuálním stroji není možné měnit všechna jeho běžně dostupná nastavení.

6.6 Vytvoření šablony klientského operačního systému

Šablona (template) klientského operačního systému bude sloužit k běhu tohoto systému na automaticky vytvořených virtuálních strojích při nasazení VDI.

Pro vytvoření šablony je nejprve nutné provést instalaci klientského operačního systému do virtuálního stroje v jazyce, který budeme chtít využívat. V našem případě byla pro klientský operační systém zvolena česká lokalizace. V době psaní této bakalářské práce bylo doporučeno využívat pro uvedené účely nanejvýš Microsoft Windows 8.1 Pro. Po instalaci klientského operačního systému je doporučeno provést instalaci všech dostupných aktualizací operačního systému.

Pokud je ve virtuálním stroji k dispozici takto nainstalovaný klientský operační systém, bude následovat instalace všech požadovaných aplikací, které budeme chtít uživatelům poskytnout. Jejich instalaci provedeme standardním způsobem.

Když je virtuální stroj kompletně připraven, spustíme na něm System Preparation tool, neboli Sysprep. Tento nástroj zajistí přípravu a konfiguraci klientského operačního systému ke klonování, přenosu na jiné PC se stejným hardwarem nebo pro předání koncovému uživateli.

Ještě než bude spuštěn nástroj Sysprep, je vhodné vytvořit v Hyper-V Manager konzoli Checkpoint virtuálního stroje. Díky němu bude v budoucnu zajištěna snazší aktualizace šablony. V případě potřeby se template virtuálního stroje vrátí do bodu před provedením úprav nástrojem Sysprep, nainstalují se na něho potřebné aktualizace, provedou se požadované změny softwaru či nastavení a poté se znovu provede Sysprep. Tím bude připraven nový aktualizovaný template, který bude připraven k nasazení.

Nástroj Sysprep najdeme v umístění *%windir%\system32\sysprep\sysprep.exe*, odkud ho spustíme v režimu nazvaném jako Zobrazit prostředí prvního spuštění počítače. U položky Zobecnit zatrhneme políčko a v části Možnosti vypnutí zvolíme Vypnout. Celý proces se dá provést také přes příkazový řádek, který je spuštěn s oprávněním administrátora. Do příkazového řádku je nutné uvést cestu k nástroji Sysprep a spustit ho s danými parametry. Příkaz poté vypadá následovně *%windir%\system32\sysprep\sysprep.exe /generalize /oobe /shutdown* v případě Microsoft Windows 7 a v našem případě pro Microsoft Windows 8/8.1 je to *%windir%\system32\sysprep\sysprep.exe /generalize /oobe /shutdown /mode:vm*.

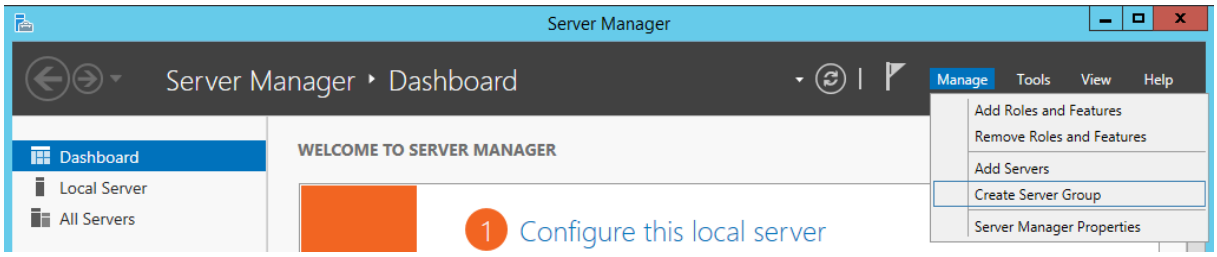
Tímto je vytvořena šablona klientského operačního systému.

6.7 Seznámení s nástrojem Server Manager a funkcí Server Group

Server Manager je nástroj, pomocí něhož je možné instalovat do serverového operačního systému role a funkce, odebírat je, vytvářet skupiny serverů nebo spravovat všechny role z různých serverů s instalovaným operačním systémem Microsoft Windows Server 2012 R2 na jednom místě.

Přehled instalovaných rolí je k dispozici v levém svislém pásu, kde je možné na požadovanou roli kliknout a následně se dostat k jejím detailnějším nastavením.

Pod záložkou Manage v pravé horní části je možné využít tlačítka pro již zmiňované nainstalování nebo odinstalování rolí, či přidat více serverů do skupiny serverů pomocí tlačítka Create Server Group. Skupiny serverů umožňují zobrazit a spravovat menší podmnožinu sdružených serverů, jako logický celek. V našem případě postupně dojde k vytvoření Server Group z předem připravených serverů. Takto vytvořená skupina serverů je poté k dispozici opět v levém svislém pásu nástroje Server Manager.



Obrázek 2 – Vzhled nástroje Server Manager, zdroj: vlastní

Pod záložkou Tools je k dispozici kompletní seznam konfiguračních nástrojů instalovaných rolí a obecně veškeré nejdůležitější nástroje pro správu rolí, funkcí a operačního systému.

6.8 Přehled instalovaných serverů pro testovací nasazení VDI

Počet instalovaných serverů byl z důvodu co nejmenší zátěže firemní sítě, ve které bylo toto testovací nasazení VDI provedeno, ustálen na počtu 3. Jednotlivé servery si s jejich názvem a instalovanými rolemi nyní stručně popíšeme. Pro toto testovací nasazení byl vyhrazen jeden fyzický server, který obsahoval instalaci Microsoft Hyper-V Server 2012 R2 a byl pojmenován VDI-MAZU. Ten následně obsahoval další dva virtuální servery DC-MAZU a CB-MAZU. Všechny tyto servery byly zapojeny do domény s názvem ITMAMA.local.

Tento způsob nasazení byl proveden pouze pro vytvoření testovacího prostředí, jinak je doporučeno mít pro hypervisor Hyper-V vyčleněn samostatný server, nebo více serverů

v clusteru. Každopádně není vhodné provozovat doménový řadič, Connection Broker, Hyper-V a DNS na jediném fyzickém serveru.

- VDI-MAZU.ITMAMA.local – server obsahující hypervisor Hyper-V pro poskytnutí virtuálního prostředí.
- DC-MAZU.ITMAMA.local – server, sloužící jako doménový řadič; obsahoval tím pádem nainstalované role AD-DS a DNS. Zároveň tento server sloužil jako úložiště pro User Profile Disks, které obsahují data a nastavení pro konkrétní množinu uživatelů. Jelikož byla složka s disky profilů uživatelů sdílená, automaticky se na server nainstalovala i role File and Storage Services.
- CB-MAZU.ITMAMA.local – server obsahující roli Remote Desktop Services a sloužící jako Remote Desktop Connection Broker. V rámci úspory místa byla serveru přidána i služba Remote Desktop Web Access, která do serverového operačního systému nainstalovala roli Internet Information Services (IIS).

6.9 Předpoklady pro nasazení Virtual Desktop Infrastructure

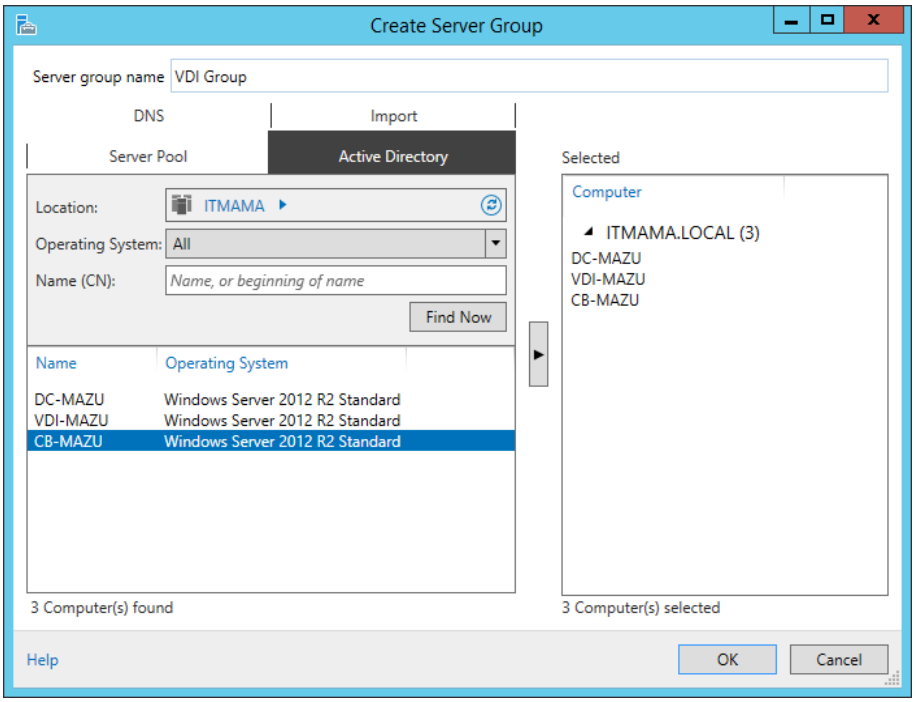
Než přejdeme k samotnému nasazení Microsoft VDI, shrneme si důležité předpoklady, aby nasazení VDI proběhlo bez komplikací.

- Všechny servery musí být pomocí IP adres adresovány staticky a správně.
- V síti musí být doménový řadič a DNS server. V našem případě je to DC-MAZU.
- Pro přidání serverů a virtuálních klientských stanic do domény jim musí být jako adresa primárního DNS serveru nastavena IP adresa námi instalovaného serveru DC-MAZU.
- V počítačové síti je nutné mít funkční DHCP server, který bude přidělovat správnou adresu primárního DNS serveru, což bude opět náš server DC-MAZU.
- Musíme mít k dispozici funkční server s hypervisorem Hyper-V, což je v našem případě VDI-MAZU.
- Všechny servery musí být správně licencovány.

6.10 Nasazení Virtual Desktop Infrastructure

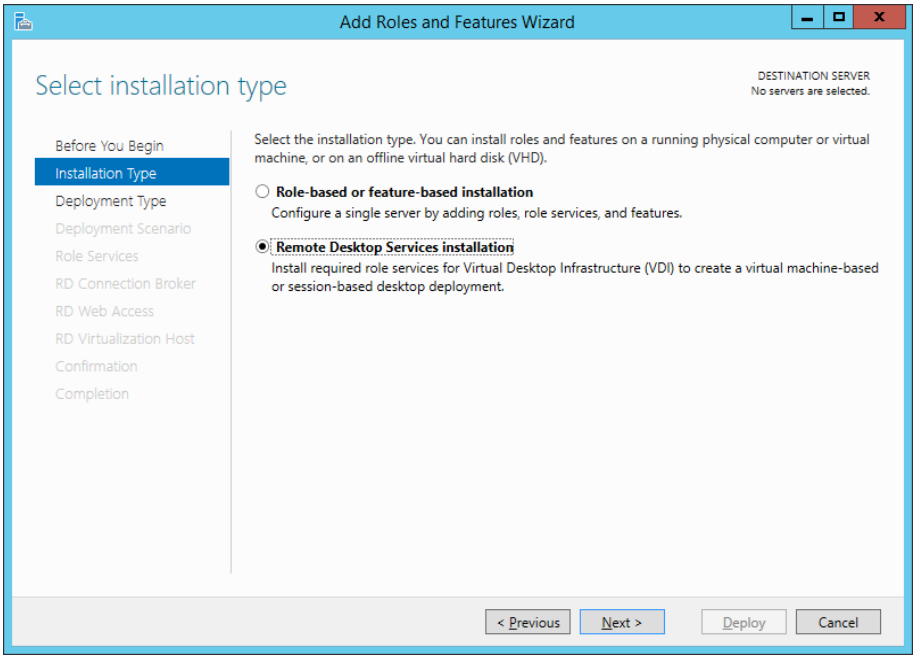
Pokud jsou splněny všechny výše uvedené body, je možné přejít k nasazení VDI. Tuto roli budeme instalovat přes Server Manager ze serveru DC-MAZU. Pomocí klienta Připojení ke

vzdálené ploše se připojíme na tento server a spustíme Server Manager. V něm v pravé horní části rozevřeme záložku Manage a zvolíme Create Server Group, jak ukazuje Obrázek 2. V průvodci vytvořením skupiny serverů klikneme na záložku Active Directory, abychom vyhledali servery, které jsme zařadili do domény a stiskneme tlačítko Find Now. Nalezené servery, které budeme požadovat pro nasazení a provoz VDI, označíme a pomocí tlačítka se šipkou přesuneme do výběru serverů.



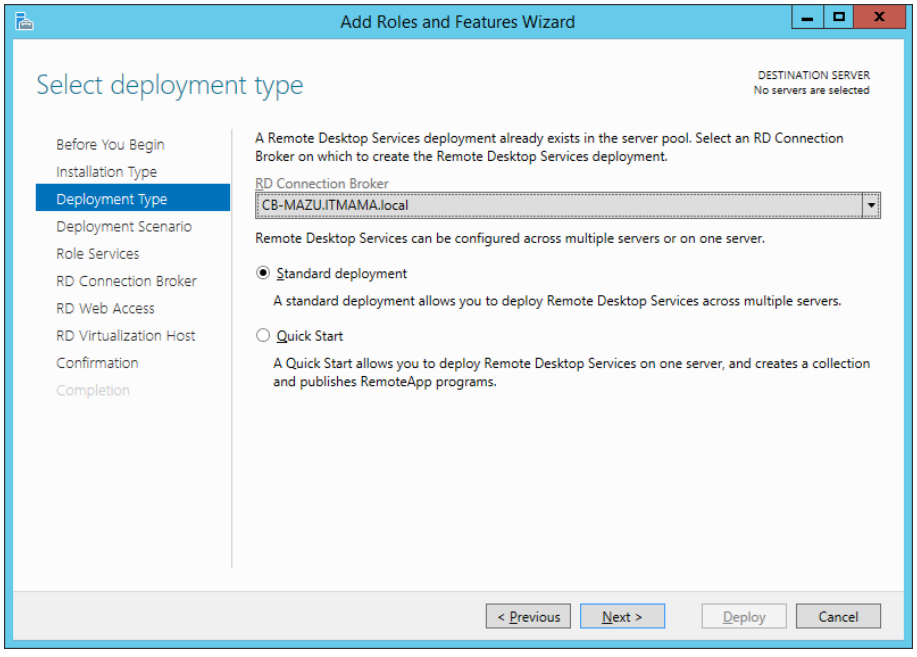
Obrázek 3 – Průvodce vytvořením Skupiny serverů, zdroj: vlastní

Po vytvoření Server Group znovu rozevřeme záložku Manage a tentokrát zvolíme možnost Add Roles and Features. Otevře se okno Průvodce přidáním rolí a funkcí. Jeho první krok přeskočíme, jelikož obsahuje pouze informace o seznámení s průvodcem. Ve druhém kroku zvolíme Remote Desktop Services installation a klikneme na tlačítko Next. Pomocí této volby nainstalujeme všechny potřebné role a služby požadované pro provoz Virtual Desktop Infrastructure.



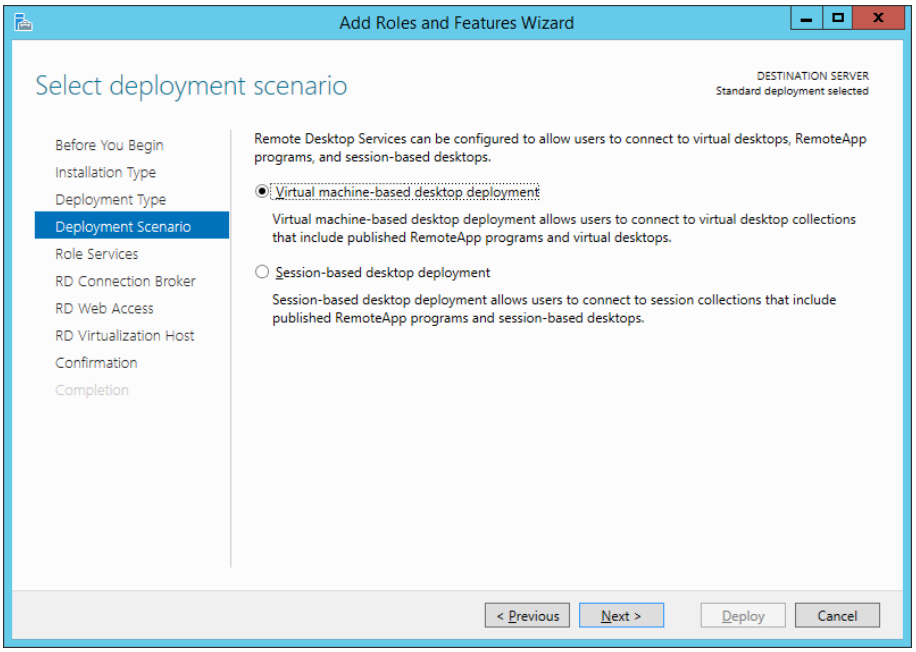
Obrázek 4 – Průvodce přidáním RDS, 2. krok, zdroj: vlastní

Ve třetím kroku, nazvaném Deployment Type, budeme vybírat požadovaný typ nasazení VDI. V našem případě zvolíme možnost Standard deployment, jelikož požadujeme nasazení VDI na více serverů, které budou poskytovat jednotlivé role. V případě, že máme ve skupině serverů, kterou jsme vytvářeli, spuštěn server s rolí RD Connection Broker, najde si ho průvodce sám. Pokud máme takových serverů více, je možné z nich vybírat. Pokud není RD Connection Broker instalován vůbec, dojde k instalaci automaticky v následujících krocích.



Obrázek 5 – Průvodce přidáním RDS, 3. krok, zdroj: vlastní

Ve čtvrtém kroku vybíráme požadovaný scénář nasazení. Máme na výběr ze dvou možností. První možností je Virtual machine-based desktop deployment, která umožňuje uživatelům připojit se ke kolekci virtuálních ploch, které mohou zahrnovat i programy RemoteApp. Druhou možností je Session-based desktop deployment, což je vytvoření běžného terminálového serveru, ke kterému se uživatelé připojují. Zvolíme tedy možnost Virtual machine-based desktop deployment.

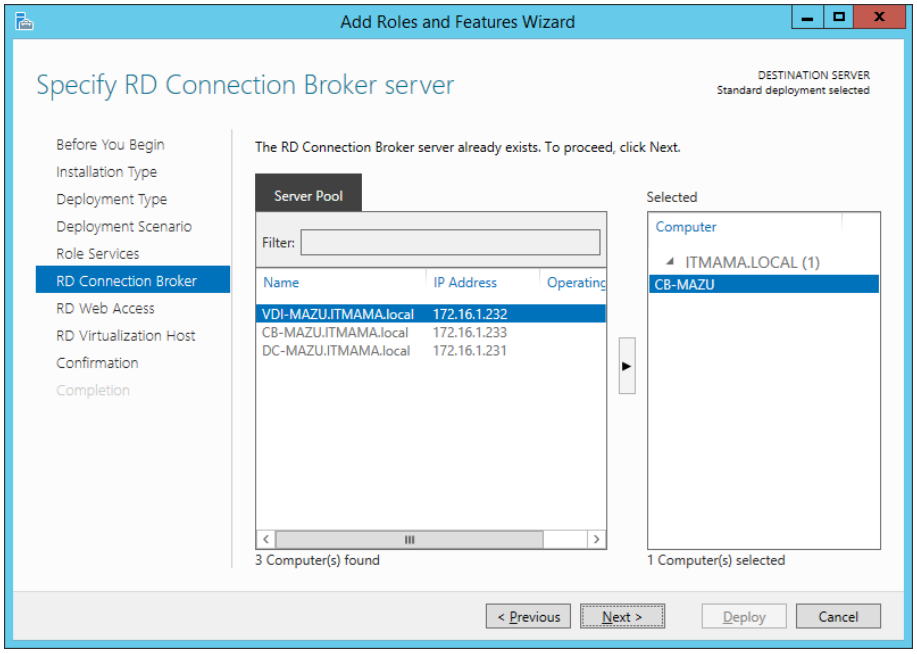


Obrázek 6 – Průvodce přidáním RDS, 4. krok, zdroj: vlastní

V pátém kroku, nazvaném Role Services, obdržíme pouze přehled rolí, které se budou instalovat pro aktuální scénář nasazení VDI. Klikneme na tlačítko Next.

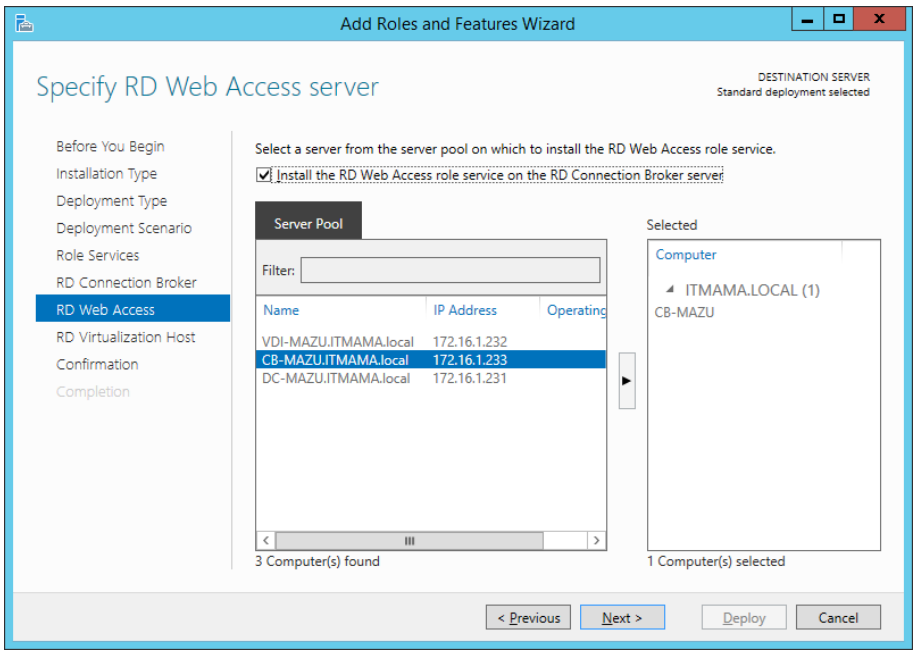
V šestém kroku dojde ke zmiňované instalaci RD Connection Broker, pokud již není vytvořen. Ze seznamu dostupných serverů v levém sloupci vybereme server, u kterého požadujeme, aby provozoval službu RD Connection Broker; pokud již takový server existuje, vybereme ho. Pokud vybereme server, na kterém tato role ještě není instalována, proběhne na něm instalace automaticky. V našem případě bude službu Connection Broker obsahovat server s názvem CB-MAZU.

V tuto chvíli je opět zřejmá výhoda využití Server Group a nástroje Server Manager, jelikož nemusíme na každém serveru instalovat role ručně a vše provedeme z jednoho centrálního nástroje.



Obrázek 7 – Průvodce přidáním RDS, 6. krok, zdroj: vlastní

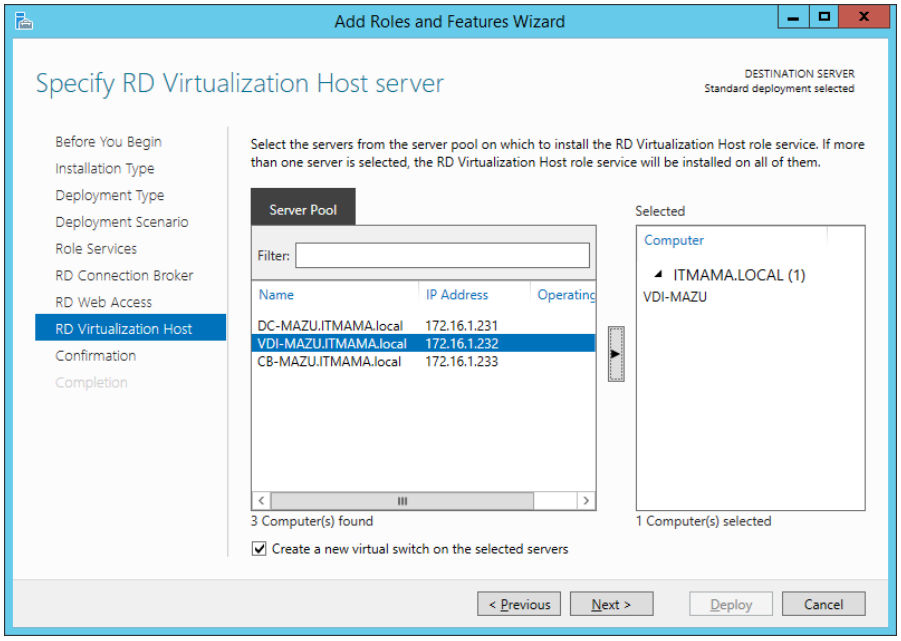
V sedmém kroku dojde k výběru serveru pro instalaci služby RD Web Access. Popis této služby je uveden v kapitole 6.2. V našem případě požadujeme tuto službu instalovat na stejný server, jako je instalována služba RD Connection Broker, proto pouze zatrhneme volbu Install the RD Web Access role service on the RD Connection Broker server.



Obrázek 8 – Průvodce přidáním RDS, 7. krok, zdroj: vlastní

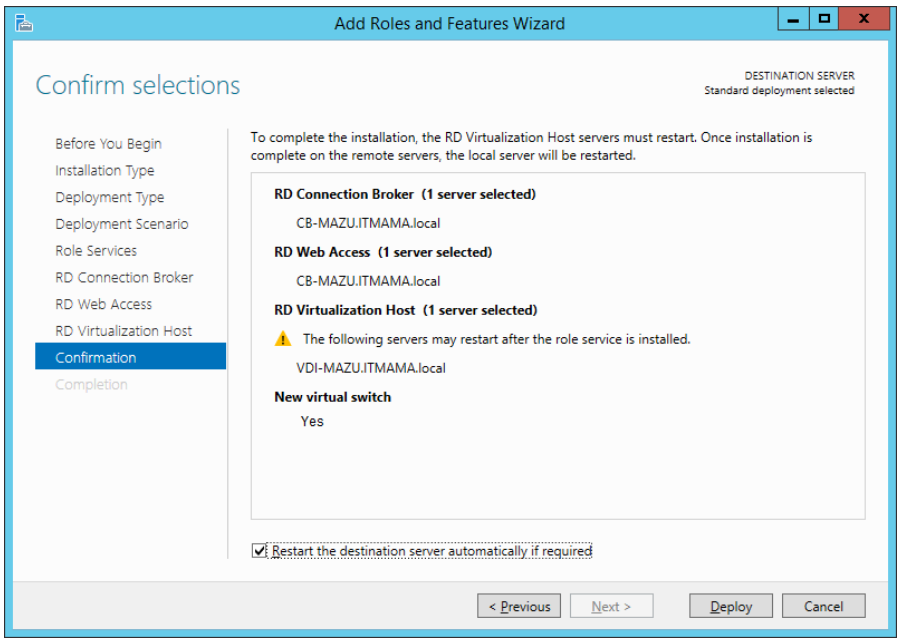
Osmý krok, nazvaný jako RD Virtualization Host, slouží k výběru severu poskytujícího virtualizační prostředí s hypervisorem Hyper-V. V našem scénáři nasazení plní tuto funkci

server pojmenovaný jako VDI-MAZU. Vybereme jej přemístěním do pravého sloupce a zatrhneme možnost Create a new virtual switch on the selected servers. Zatržením této možnosti dojde k vytvoření virtuálního přepínače v hypervisoru Hyper-V a ten bude přiřazen virtuálním strojům, aby mohly využívat počítačovou síť. Následně klikneme na tlačítko Next.



Obrázek 9 – Průvodce přidáním RDS, 8. krok, zdroj: vlastní

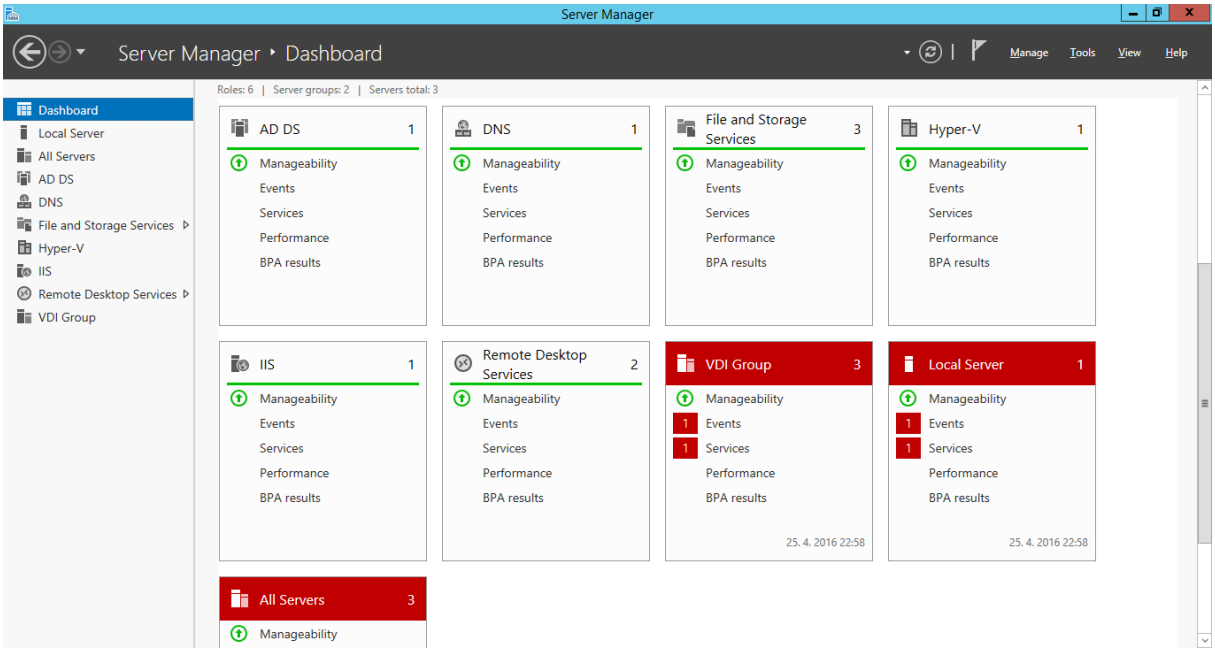
V předposledním, devátém kroku obdržíme přehled služeb, které se budou instalovat na konkrétní servery. Pod přehledem je důležité zatrhnout možnost Restart the destination server automatically if required a klikneme na tlačítko Deploy.



Obrázek 10 – Průvodce přidáním RDS, 9. krok, zdroj: vlastní

V posledním kroku uvidíme stav instalace služeb. Po úspěšné instalaci služeb, kdy za každým ukazatelem stavu instalace bude napsáno Succeeded, klikneme na tlačítko Close.

Po zavření průvodce se dostaneme zpět k nástroji Server Manager, kde uvidíme nově instalované role, které lze dále spravovat. Nový vzhled nástroje Server Manager ukazuje Obrázek 11.

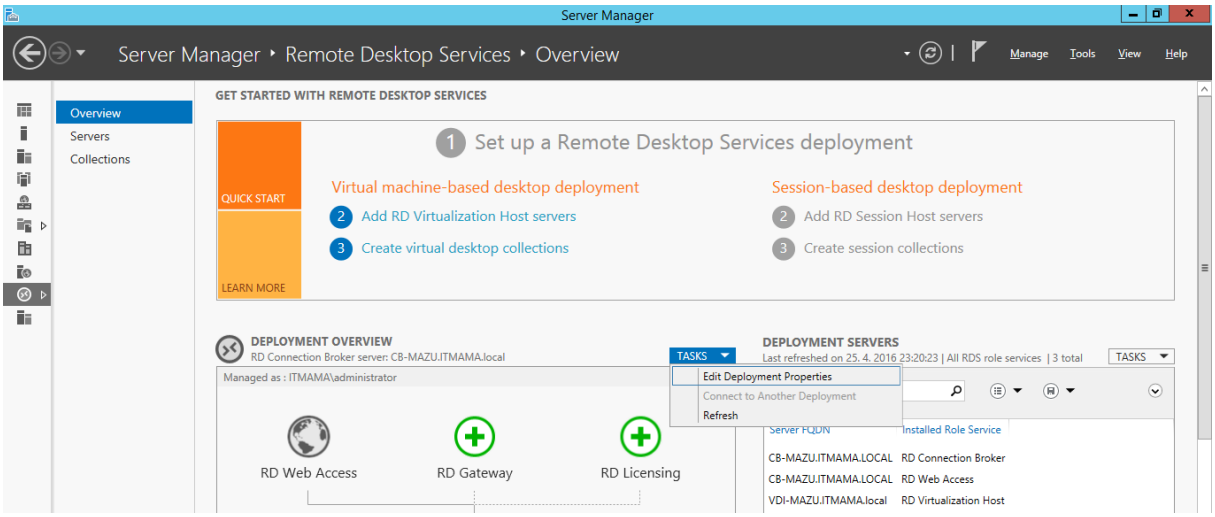


Obrázek 11 – Nástroj Server Manager na serveru DC-MAZU, zdroj: vlastní

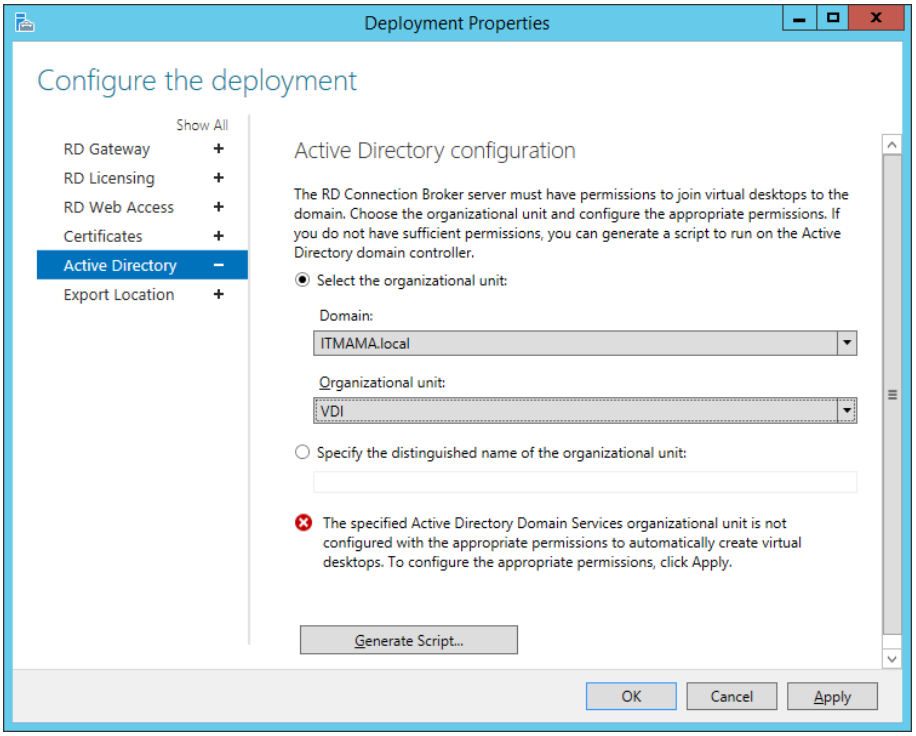
6.11 Konfigurace vlastností nasazení VDI

Nyní když je RD Virtualization Host nasazen, zaměříme se na konfiguraci vlastností nasazení naší farmy virtuálních strojů. V AD-DS v doméně ITMAMA.local vytvoříme novou Organizační jednotku (Organizational Unit) pojmenovanou VDI. Tato OU musí mít v jejích vlastnostech správně nastavena oprávnění, aby s ní mohl server CB-MAZU libovolně manipulovat.

V nástroji Server Manager klikneme v levém svislém sloupci na roli Remote Desktop Services a v části Deployment Overview rozevřeme záložku Tasks. Na této záložce stiskneme tlačítko Edit Deployment Properties, čímž se nám otevře nové okno, ve kterém nás budou zajímat zejména dvě nové záložky. První z nich je Active Directory a druhá je Export Location.



Obrázek 12 – Tlačítko Edit Deployment Properties v roli RDS, zdroj: vlastní

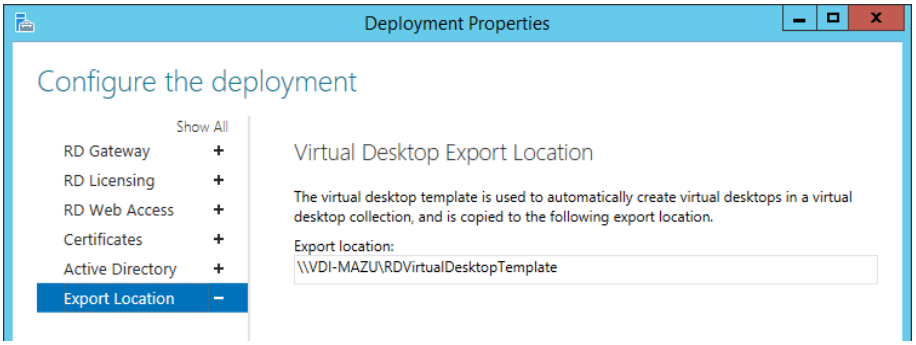


Obrázek 13 – Záložka Active Directory v konfiguraci nasazení, zdroj: vlastní

Na záložce Active Directory vybereme volbu Select the organizational unit. Z rozbalovacího prvku vybereme doménu ITMAMA.local a jako Organizational Unit zvolíme VDI, kterou jsme si před chvílí vytvořili. Průvodce nás bude ve spodní části okna varovat, že již zmiňovaná oprávnění nejsou správně konfigurována, proto stiskneme tlačítko Apply a průvodce je za nás správně nastaví.

Na záložce Export Location zvolíme síťovou cestu, kam bude uložena kopie námi vytvořené šablony klientského operačního systému. V našem případě uložíme tuto kopii na server

VDI-MAZU do sdílené složky s názvem RDVirtualDesktopTemplate. Tato složka musí mít opět nastavena správná oprávnění, aby do ní bylo možné zapisovat a číst z ní.



Obrázek 14 – Záložka Export Location v konfiguraci nasazení, zdroj: vlastní

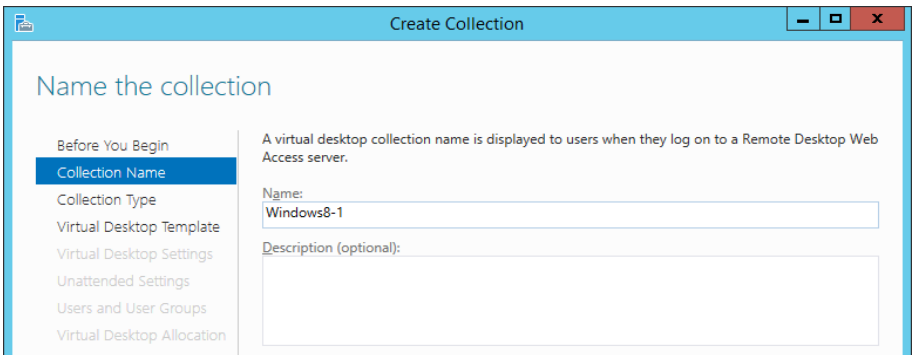
V případě využití RD Gateway nebo automatické správy licencí pro klientský přístup nalezneme nastavení opět v okně Deployment Properties pod požadovanou záložkou v levém sloupci.

6.12 Vytvoření a publikace kolekce virtuálních ploch

Pokud máme provedeno nasazení VDI a vytvořen template virtuálního klientského operačního systému, můžeme přejít k nasazení a publikaci virtuálních klientských stanic.

Spustíme nástroj Server Manager a klikneme v levém svislém sloupci na roli Remote Desktop Services. V části Deployment Overview klikneme pravým tlačítkem na ikonu RD Virtualization Host a z nabídky vybereme volbu Create Virtual Desktop Collection.

Po otevření průvodce přeskočíme úvodní obrazovku stiskem tlačítka Next a přejdeme ke druhému kroku. Ve druhém kroku zvolíme název naší kolekce, který vepíšeme do textového formuláře pod položkou Name, a přejdeme na třetí krok. Jako název kolekce jsme zvolili Windows8-1.



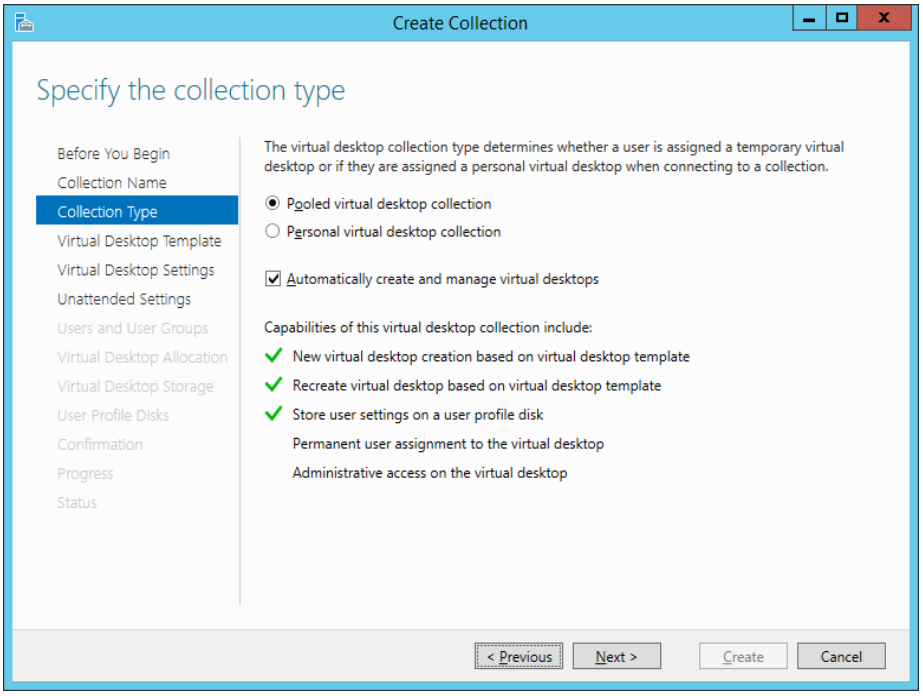
Obrázek 15 – Vytvoření kolekce virtuálních ploch, 2. krok, zdroj: vlastní

Ve třetím kroku máme na výběr dva typy kolekcí. První kolekce se nazývá Pooled virtual desktop collection. Tento typ kolekce je založen na šabloně klientského operačního systému. V případě odhlášení uživatele dojde k navrácení šablony do původního stavu.

Druhá kolekce se jmenuje Personal virtual desktop collection. Funkce této kolekce spočívá v přiřazení osobní virtuální plochy konkrétnímu uživateli. Jakékoliv změny, které uživatel provede, zůstanou zachovány.

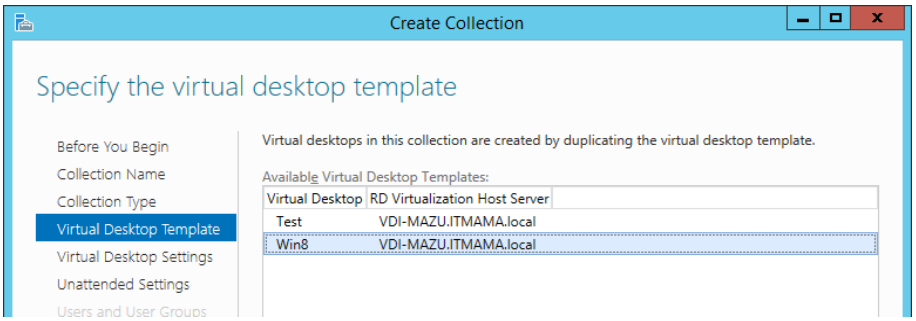
Další volbou, která je pojmenována Automatically create and manage virtual desktops, umožňuje Službám vzdálené plochy (RDS) automaticky vytvářet a spravovat virtuální plochy. V případě zatržení této volby bude RDS vytvářet virtuální plochy založené na virtuální šabloně, znovu nasadí upravené virtuální šablony a bude ukládat uživatelská data a nastavení v User Profile Disks. Pokud bychom tuto volbu nezvolili, došlo by při každém odhlášení uživatele ke ztrátě jeho dat a nastavení.

Při změně nastavení zvýrazní průvodce pomocí zeleného zatržení možnosti kolekce.



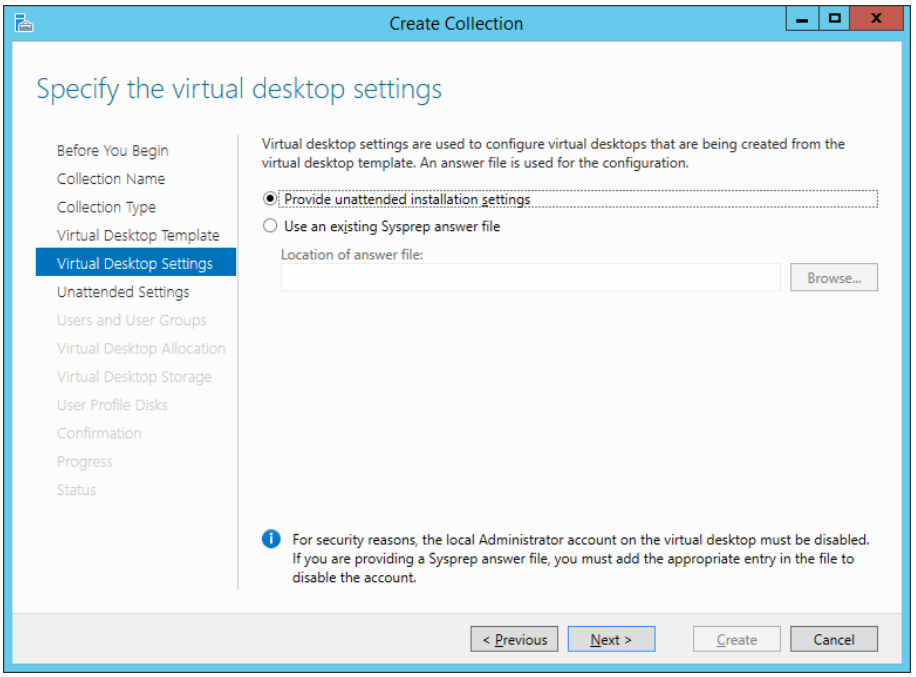
Obrázek 16 – Vytvoření kolekce virtuálních ploch, 3. krok, zdroj: vlastní

Ve čtvrtém kroku vybereme šablonu klientského operačního systému, kterou jsme si vytvořili pomocí nástroje Sysprep. Průvodce ověří její správnost a v případě, že by šablona nebyla vytvořena nástrojem Sysprep, obdržíme chybové hlášení. V případě úspěchu nám bude umožněn postup na pátý krok.



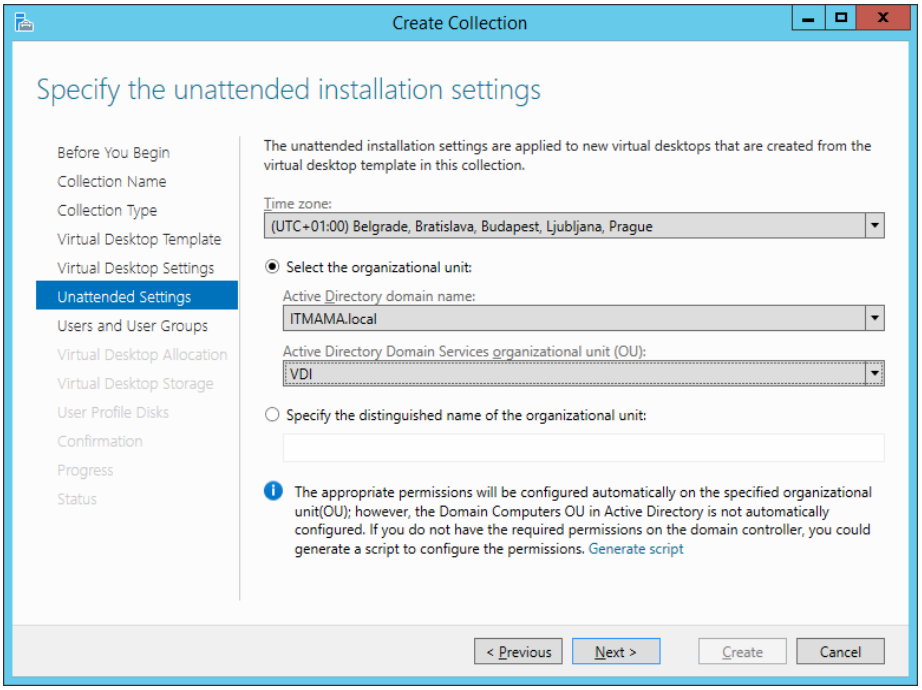
Obrázek 17 – Vytvoření kolekce virtuálních ploch, 4. krok, zdroj: vlastní

V pátém kroku zvolíme možnost Provide unattended installation settings. Touto volbou nám průvodce umožní detailní nastavení virtuálních klientských stanic. Pokud bychom měli nastavení připravena v souboru Sysprep answer file, zvolili bychom druhou možnost.



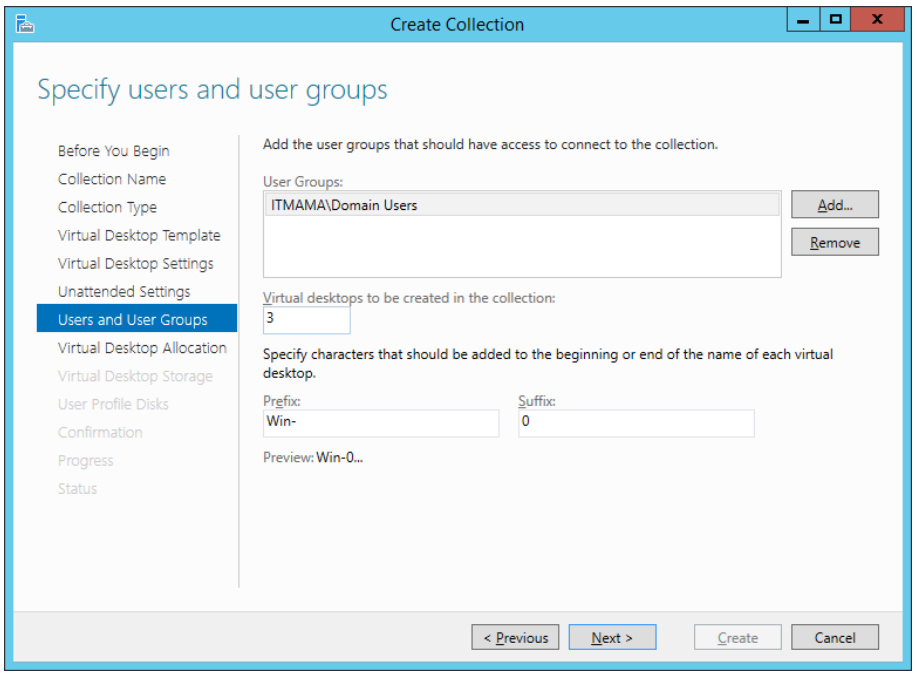
Obrázek 18 – Vytvoření kolekce virtuálních ploch, 5. krok, zdroj: vlastní

Šestý krok umožňuje virtuálnímu klientskému počítači nastavit časové pásmo, členství v doméně a zařadit jej do Organizační jednotky. Vybereme správné časové pásmo, jako doménu zvolíme ITMAMA.local a jako Organizační jednotku vybereme VDI. Následně stiskneme tlačítko Next.



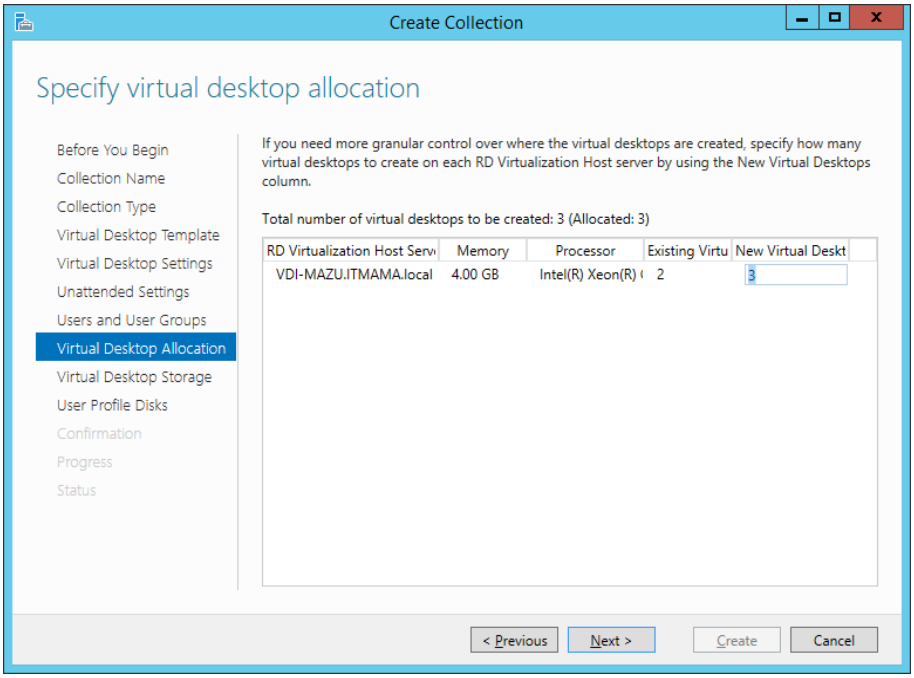
Obrázek 19 – Vytvoření kolekce virtuálních ploch, 6. krok, zdroj: vlastní

V sedmém kroku, pojmenovaném Users and User Groups, povolíme konkrétním uživatelům a skupinám uživatelů právo přistupovat ke kolekci virtuálních ploch. V našem případě povolíme přístup všem doménovým uživatelům. Na této záložce dále volíme množství virtuálních klientských počítačů, které požadujeme vytvořit, a jejich název v podobě předpony (Prefix) a číselné přípony (Suffix). Pro testování nám stačí dva nebo tři virtuální stroje.



Obrázek 20 – Vytvoření kolekce virtuálních ploch, 7. krok, zdroj: vlastní

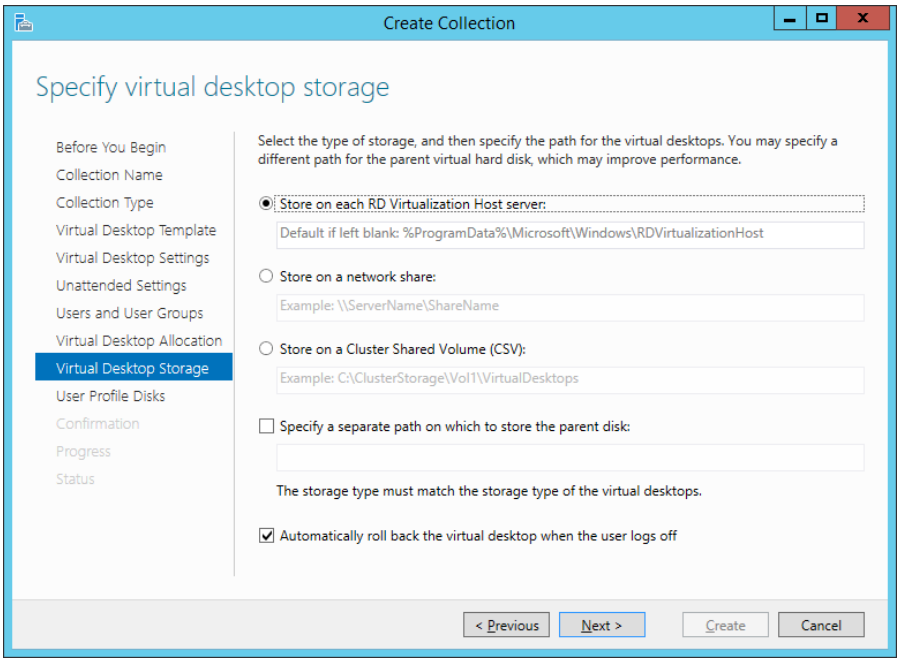
Pokud využíváme více hostitelů RD Virtualization Host server, můžeme v osmém kroku využít možnost rozmístění konkrétního počtu virtuálních klientských počítačů na konkrétní hostitele. Počet uvádíme ke každému hostiteli v posledním sloupci nazvaném New Virtual Desktops. V případě, že máme pouze jednoho hostitele, uvedeme u něho stejný počet virtuálních strojů jako v sedmém kroku.



Obrázek 21 – Vytvoření kolekce virtuálních ploch, 8. krok, zdroj: vlastní

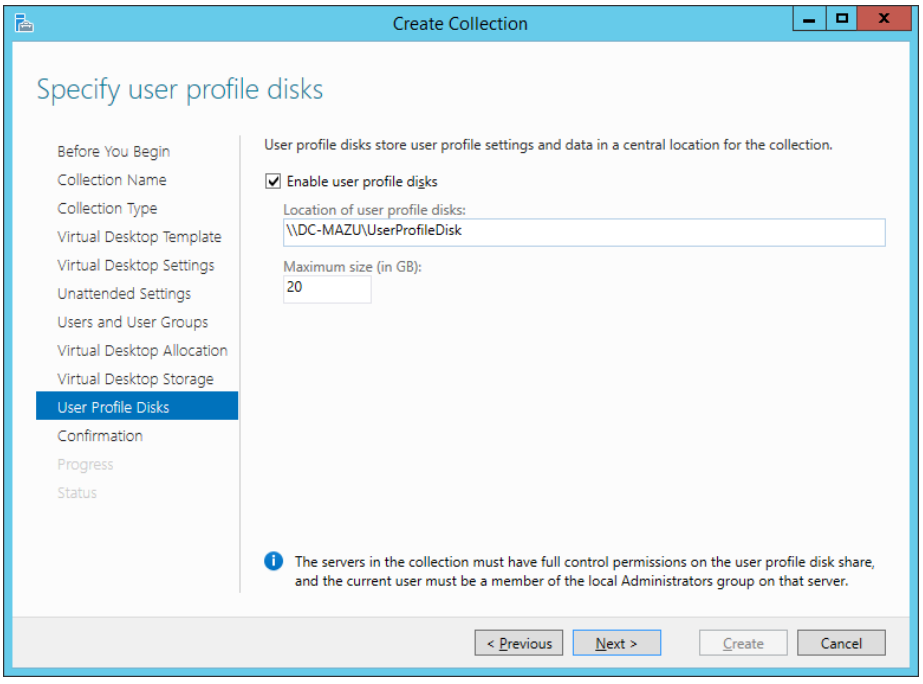
Devátý krok specifikuje úložiště šablon virtuálních ploch. V produkčním prostředí je nejlepší volbou Store on a Cluster Shared Volume (CSV), pokud je takový typ úložiště k dispozici. Jelikož máme pouze jeden RD Virtualization Host server, zvolíme první možnost, kdy se šablony uloží v hostiteli. Pokud bychom měli hostitelů více, nedoporučuje se tato volba použít, a doporučuje se použít CSV.

Ve spodní části průvodce je volba Automatically roll back the virtual desktop when the user logs off. Tato volba po odhlášení uživatele zajistí vrácení šablony zpět do původního stavu. Necháme ji tedy zatrženu.



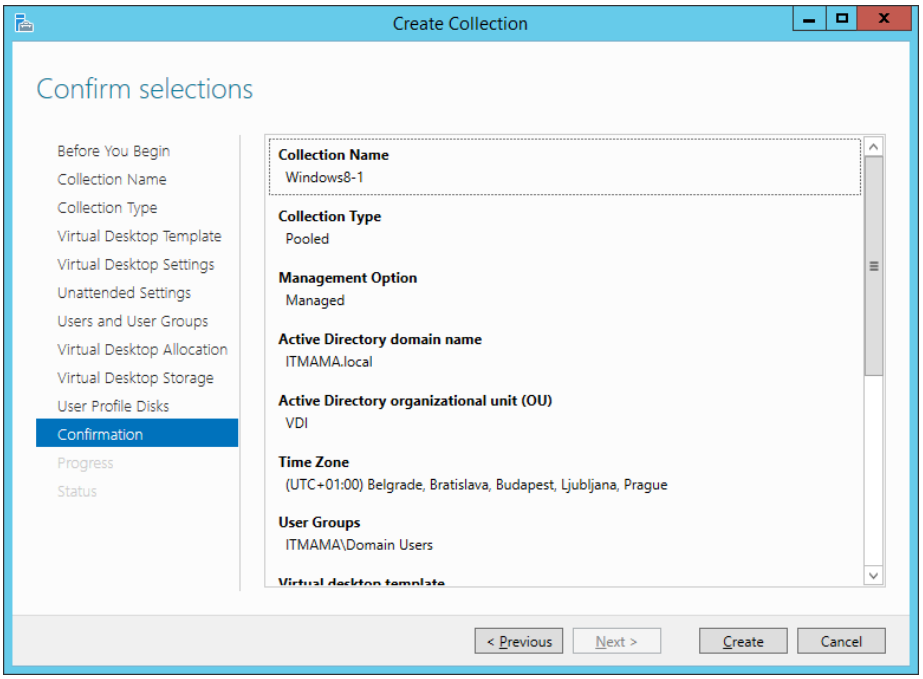
Obrázek 22 – Vytvoření kolekce virtuálních ploch, 9. krok, zdroj: vlastní

V desátém kroku zatrhneme volbu Enable user profile disks. Díky ní uživatelé po odhlášení neztratí svá data a nastavení. Vše bude uloženo na jejich soukromém virtuálním disku v umístění, které zde specifikujeme. Cestu ke sdílené složce musíme uvést v UNC (síťovém) tvaru. Samozřejmě musíme dbát na to, aby bylo možné do sdílené složky zapisovat a číst z ní. Pod položkou pro zadání cesty zvolíme maximální kapacitu disků uživatelů v GB.

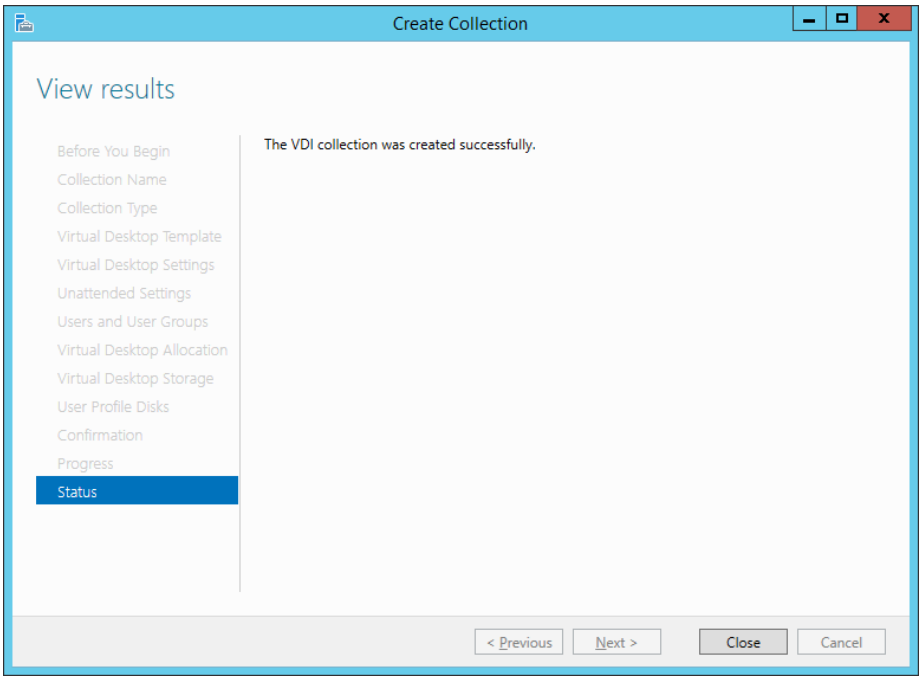


Obrázek 23 – Vytvoření kolekce virtuálních ploch, 10. krok, zdroj: vlastní

Jedenáctý krok shrnuje veškerá nastavení, která jsme zadali. Provedeme kontrolu a v případě, že je vše správně nastaveno, stiskneme tlačítko Create. Dále nás bude průvodce informovat o průběhu vytváření kolekce a po úspěšném dokončení procesu ukončíme průvodce stiskem tlačítka Close.

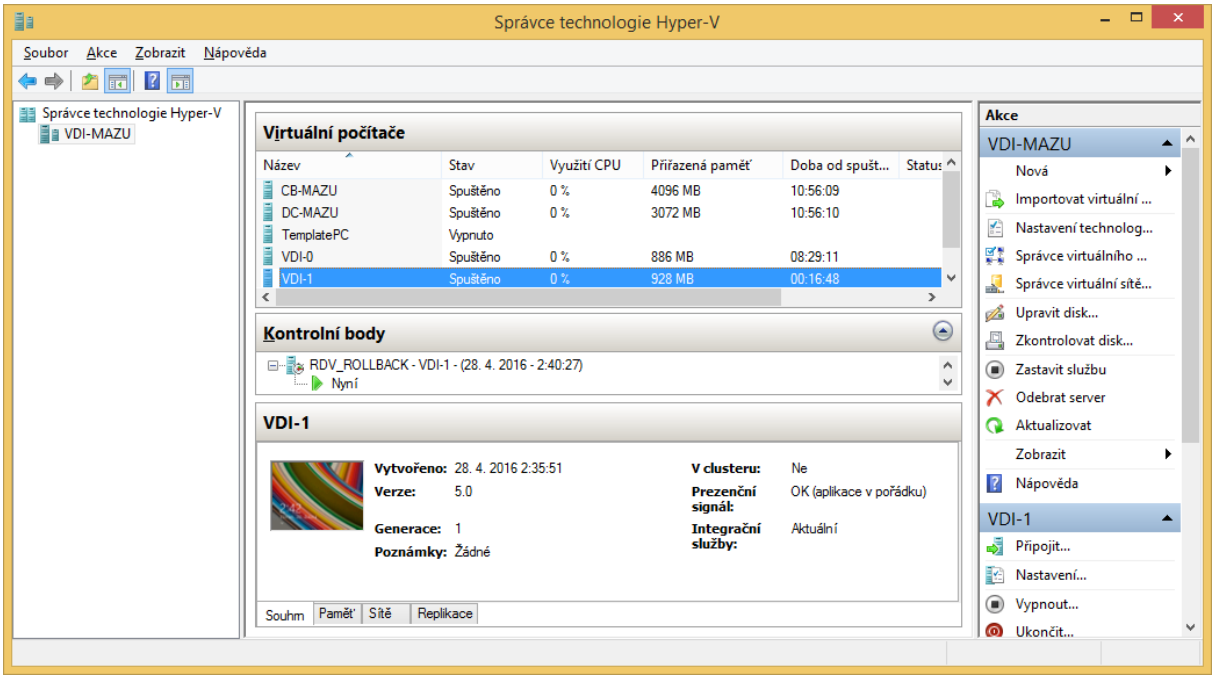


Obrázek 24 – Vytvoření kolekce virtuálních ploch, 11. krok, zdroj: vlastní



Obrázek 25 – Úspěšné vytvoření kolekce virtuálních ploch, 13. krok, zdroj: vlastní

Abychom si ověřili skutečnost, že se všechny požadované virtuální klientské počítače vytvořily, připojíme se k hypervisoru Hyper-V pomocí nástroje Hyper-V Manager (Správce technologie Hyper-V). Vytvořené virtuální počítače by v něm nyní již měly být vidět.



Obrázek 26 – Přehled virtuálních strojů pomocí nástroje Hyper-V Manager, zdroj: vlastní

V případě potřeby upravení vlastností vytvořené kolekce stačí pouze spustit nástroj Server Manager a kliknout na námi vytvořenou kolekci virtuálních ploch. V části Properties klikneme na tlačítko Tasks a následně zvolíme požadovanou akci.

V části RemoteApp Programs můžeme zrušit publikování celé virtuální plochy a lze publikovat pouze konkrétní aplikace, které jsou na virtuálních klientských počítačích nainstalovány. Tato varianta se dá využít v případě, že aplikace není kompatibilní s daným serverovým operačním systémem a vyžaduje pro svůj běh klientský operační systém.

V části Virtual Desktops můžeme sledovat stav virtuálních klientských počítačů, případně kdo je k nim připojen. Dále je lze v tomto okně spustit či vypnout nebo odstranit. V případě, že je vytvořena nová šablona klientského operačního systému, můžeme zde vytvořit nové virtuální klientské počítače, které ji budou využívat. Tím se bude zabývat následující část textu.

6.13 Aktualizace šablony klientského operačního systému

V nástroji Hyper-V Manager vrátíme vypnutý virtuální klientský počítač do požadovaného kontrolního bodu (Checkpoint), který jsme si vytvořili před spuštěním nástroje Sysprep. Následně virtuální stroj spustíme. Po spuštění virtuálního klientského počítače provedeme

úpravy a instalaci všech požadovaných aplikací a potřebných aktualizací. Po provedení úprav vytvoříme nový kontrolní bod pro příští aktualizaci šablony. Kontrolní bod je vhodné přejmenovat, aby byly na první pohled patrné změny, které se v něm odehrály. Spustíme nástroj Sysprep a provedeme přípravu nové šablony stejně jako v kapitole 6.6.

Pokud máme vytvořenu aktualizovanou šablonu, spustíme na serveru DC-MAZU nástroj Správce serveru. V něm vybereme roli Remote Desktop Services a následně zvolíme námi vytvořenou kolekci virtuálních vzdálených ploch, kterou jsme pojmenovali Windows8-1. V části Virtual Desktops klikneme na tlačítko Tasks a zvolíme možnost Recreate All Virtual Desktops.

Po spuštění průvodce vybereme virtuální stroj s aktualizovanou šablonou klientského operačního systému. V následujícím kroku vybereme způsob odhlášení uživatelů pro provedení obnovy virtuálních klientských počítačů. První volba umožňuje provést obnovu u virtuálních klientských počítačů, ke kterým není během zvoleného časového okna nikdo přihlášen. Pokud budou v daném časovém okně někteří uživatelé stále přihlášeni, dojde k jejich automatickému odhlášení. Druhá možnost provede automatické odhlášení uživatelů okamžitě, nebo ve zvolený čas.

Následně v průvodci potvrdíme obnovu virtuálních klientských počítačů stiskem tlačítka Create. Po úspěšném dokončení obnovy zavřeme průvodce stiskem tlačítka Close.

6.14 Připojení k virtuální ploše

Připojení k virtuální vzdálené ploše je možné provést několika způsoby. První z nich provedeme otevřením webového prohlížeče Internet Explorer a zadáním odkazu obsahujícím název serveru, který provozuje službu RD Web Access. V našem případě slouží k těmto účelům server CB-MAZU, takže zadáme adresu *https://CB-MAZU/RDWeb* a potvrdíme na klávesnici stiskem tlačítka Enter. Budeme varováni, že následující stránka obsahuje neověřený certifikát, což budeme ignorovat a potvrdíme vstup na tuto stránku. Poté zadáme uživatelské údaje uživatele, který má povolen přístup ke kolekci virtuálních ploch. Uživatelské jméno zadáváme ve tvaru *doména\uživatelské jméno*. Po přihlášení uvidíme ikonu s názvem Windows8-1 Desktop. Po spuštění této ikony potvrdíme ověření certifikátu a dojde ke spuštění a přihlášení na vzdálenou plochu.

Pokud bychom k přihlášení nevyužili prohlížeč Internet Explorer, nedošlo by k automatickému přihlášení na vzdálenou plochu. Byli bychom vyzvání ke stažení souboru

a po jeho spuštění bychom opět zadali přihlašovací údaje. Následně by došlo k přihlášení na vzdálenou plochu bez využití prohlížeče.

V případě, že bychom se chtěli k virtuálním plochám přihlašovat ze zařízení, která neobsahují plnohodnotné verze operačních systémů Microsoft Windows (mobily, tablety, tencí klienti, ostatní PC), může být požadováno nastavení přesměrování.

Přesměrování v našem případě nastavíme na serveru CB-MAZU pomocí drobné úpravy v registrech operačního systému. Spustíme nástroj Regedit a ve struktuře *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\ClusterSettings* vytvoříme nový stringValue, který pojmenujeme *DefaultTsvUrl*. Jako hodnotu vložíme *tsv://VMResource.1.VDI*. Následně se lze k virtuálním plochám přihlásit z jakéhokoliv klienta podporujícího protokol RDP.

Pokud přesměrujeme Connection Broker na kolekci virtuálních ploch, znemožníme si tím přístup k serveru CB-MAZU přes nástroj Připojení ke vzdálené ploše. K tomuto serveru se za účelem správy budeme muset hlásit tak, že stiskneme klávesovou zkratku Win+R, do pole Otevřít zadáme příkaz *mstsc /admin* a stiskneme klávesu Enter, nebo tlačítko OK. Přes nově spuštěný nástroj Připojení ke vzdálené ploše se nám přihlášení k serveru CB-MAZU již podaří.

7 ZÁVĚR

V této bakalářské práci byla popsána technologie Virtual Desktop Infrastructure s důrazem na produkty od společnosti Microsoft. Téma bakalářské práce bylo zvoleno na základě analýzy možností využití prostředků pro zjednodušení správy podnikové infrastruktury.

Nyní je již možné kriticky porovnat fyzickou a virtuální firemní infrastrukturu. Fyzická infrastruktura přináší výhodu z pohledu jednotlivých uživatelů. Uživatelům je možné nezávisle na ostatních uživatelích instalovat různé druhy aplikací a dalšího softwarového vybavení. Tuto výhodu však není možné brát doslovně, jelikož ji Virtual Desktop Infrastructure umí s využitím Personal virtual desktop collection také poskytnout. Druhou výhodou jsou ve většině případů nižší náklady na pořízení licencí produktů Microsoft. Poslední výhodou, kterou lze zmínit, je ta, že se uživatelé v běžných případech dostanou ke svým datům uloženým ve fyzickém počítači i v případě výpadku internetového připojení nebo lokální sítě. Ke sdíleným firemním datům se v takovém případě také nedostanou.

Naopak výhody Microsoft Virtual Desktop Infrastructure převažují. Nasazení této technologie není nijak výrazně komplikované. Náročnost samozřejmě stoupá s množstvím potřebných serverů a množstvím uživatelů, kteří se budou k virtuálním plochám připojovat. Nejvýznamnější výhodou je ta, že pokud firma poskytuje svým uživatelům standardní sadu softwarového vybavení, je velmi jednoduché vytvořit šablonu klientského operačního systému s požadovanými aplikacemi a tu uživatelům poskytnout. V případě nutnosti aktualizace některé z aplikací bude aktualizace provedena jen na jednom zařízení a následně bude distribuována ostatním uživatelům. V případě, že ve firmě využívá stejnou sadu softwarového vybavení několik desítek nebo stovek uživatelů, se bude jednat o výrazné zjednodušení správy. Další výhodou je to, že oprávnění uživatelé mohou mít přístup ke svému virtuálnímu firemnímu počítači odkudkoliv, kde je k dispozici přístup k Internetu. Poslední významnou výhodou je uchování dat ve firemním datacentru. Data tím pádem neopouští firemní prostory.

Microsoft Virtual Desktop Infrastructure se nevyplatí nasadit ve firemním prostředí, kde je malé množství uživatelů. V tu chvíli by veškeré výhody VDI postrádaly smysl.

Všechny body zadání bakalářské práce byly úspěšně splněny. Nejvíce komplikací vyvstalo v praktické části při publikaci kolekce virtuálních ploch. Při dodržení postupu v této bakalářské práci se jim čtenář spolehlivě vyhne a je před nimi dostatečně varován s uvedením všech důležitých souvislostí.

8 POUŽITÁ LITERATURA

Remote Desktop Services. *The free dictionary by Farlex* [online]. Computer Desktop Encyclopedia, ©1981-2016 [cit. 2016-02-10]. Dostupné z: http://encyclopedia2.thefreedictionary.com/Remote+Desktop+Services

Terminal Services. *The free dictionary by Farlex* [online]. Computer Desktop Encyclopedia, ©1981-2016 [cit. 2016-02-10]. Dostupné z: http://encyclopedia2.thefreedictionary.com/TERMINAL+SERVICES

WinFrame. *The free dictionary by Farlex* [online]. Computer Desktop Encyclopedia, ©1981-2016 [cit. 2016-02-10]. Dostupné z: http://encyclopedia2.thefreedictionary.com/Citrix+WinFrame

Windows Server 2012 R2 – co je nového? *DAQUAS* [online]. Externí autoři, 2013 [cit. 2016-03-15]. Dostupné z: http://www.daquas.cz/articles/621-windows-server-2012-r2-co-je-noveho

GOLDEN, Bernard. *Virtualization for dummies (R).* Indianapolis: Wiley Publishing, ©2008. Bestselling computer book series, 1. ISBN 9780470148310.

KELBLEY, John a Mike STERLING. *Microsoft Windows Server 2008 R2 Hyper-V: podrobný průvodce administrátora*. Brno: Computer Press, 2011. ISBN 9788025132869.

KRÁL, Jan a Lukáš KRAHULEC. *Virtualizace a virtualizace s podporou procesoru* [online]. Ostrava: VŠB-TU, 2008 [cit. 2016-04-13]. Dostupné z: http://wh.cs.vsb.cz/mil051/images/f/f5/PAP_Virtualizace_refer%C3%A1t_(Krahulec_Kr%C3%A1l).pdf

Capacity planning for a Microsoft Virtual Desktop Infrastructure pooled 2,000-seat virtual machine collection in Windows Server 2012. *Microsoft Corporation* [online]. Microsoft Corporation, 2013 [cit. 2016-04-11]. Dostupné z: http://download.microsoft.com/download/2/4/b/24b5ec7d-1d03-49a2-b792-c7edf24549ee/windows_server_2012_capacity_planning_for_vdi_white_paper.pdf

Competitive Advantages of Windows Server 2012 R2 Hyper-V over VMware vSphere 5.5. *Virtualization*[online]. Microsoft Corporation, 2013 [cit. 2016-02-17]. Dostupné z: https://www.microsoft.com/en-us/server-cloud/solutions/virtualization.aspx

Hyper-V Architecture. *MSDN* [online]. Microsoft Corporation, 2016 [cit. 2016-02-29]. Dostupné z: https://msdn.microsoft.com/en-US/library/cc768520(v=bts.10).aspx

Microsoft Hyper-V. *TechNet Blog* [online]. Microsoft Corporation, 2015 [cit. 2016-02-01]. Dostupné z: http://blogs.technet.com/b/technetczsk/p/microsoft-hyper-v.aspx

Microsoft virtualizace. *TechNet Blog* [online]. Microsoft Corporation, 2015 [cit. 2016-02-10]. Dostupné z: http://blogs.technet.com/b/technetczsk/p/microsoft-virtualizace.aspx

PANEK, William. *MCSA Windows Server 2012 complete study guide: exams 70-410, 70-411, and 70-412*. Indianapolis IN: John Wiley & Sons, 2013. ISBN 1118544072.

Securing Remote Desktop (RDP) for System Administrators. *University of California Berkley* [online]. University of California Berkley, 2016 [cit. 2016-04-09]. Dostupné z: https://security.berkeley.edu/resources/best-practices-how-articles/securing-remote-desktop-rdp-system-administrators

VMware Workstation Release and Build Number History. *Virten.net* [online]. Virten.net, 2015 [cit. 2016-02-10]. Dostupné z: https://www.virten.net/vmware/workstation-release-and-build-number-history/