

Univerzita Hradec Králové
Fakulta informatiky a managementu
Katedra informačních technologií

**Analýza využití Microsoft Virtual Desktop
Infrastructure ve firemní síti**

Diplomová práce

Autor: Bc. Luboš Mercl
Studijní obor: Informační management
Vedoucí práce: Mgr. Josef Horálek, Ph.D.

Hradec Králové

duben 2015

Prohlášení:

Prohlašuji, že jsem diplomovou práci zpracoval samostatně a s použitím uvedené literatury a uvedených zdrojů.

V Hradci Králové dne 24. dubna 2015

Bc. Luboš Mercl

Poděkování:

Na tomto místě bych chtěl především velice poděkovat vedoucímu mé diplomové práce Mgr. Josefu Horálkovi, Ph.D. za věnovaný čas, jeho přístup a pomoc s vypracováním této diplomové práce po formální a obsahové stránce.

Název diplomové práce:

Analýza využití Microsoft Virtual Desktop Infrastructure ve firemní síti

Anotace práce:

Tato diplomová práce se zabývá analýzou nasazení technologie virtuálních desktopů ve firemní síti a porovnáním tohoto řešení s klasickými pevnými osobními počítači. V práci jsou uvedeny základní principy virtualizace, které jsou zaměřeny především na technologii Hyper-V a technologii Microsoft Virtual Desktop Infrastructure.

V rámci diplomové práce vznikl návrh technického řešení virtuálních desktopů, který je založen na řešení za použití nástrojů společnosti Microsoft, a tento návrh byl porovnán především z finančního hlediska s řešením za použití klasické infrastruktury.

Title of diploma thesis:

Analysis of Microsoft Virtual Desktop Infrastructure Usage in the corporate network

Annotation:

This diploma thesis analyzes the deployment of Virtual Desktop Infrastructure technology in a corporate network and comparing this solution to traditional personal computer infrastructure. Thesis presents basic principles of virtualization which are primarily focused on Hyper-V technology and Microsoft Virtual Desktop Infrastructure.

Within the diploma thesis technical proposal virtual desktop solution was created which is based on solutions by using Microsoft tools. This proposal has been compared with traditional personal computer solution primarily from a financial point of view.

Obsah

1	ÚVOD	1
2	ANALÝZA POŽADAVKŮ PODNIKU.....	3
2.1	IT strategie.....	3
2.2	Aplikační požadavky podniku	3
2.3	Modely architektury	5
2.4	Vzdálený přístup k aplikacím a zdrojům.....	6
2.5	Úspora nákladů v oblasti ICT.....	8
2.6	Základní výhody virtualizace serverů pro obchodní a provozní činnost podniku	12
2.7	Základní výhody virtualizace desktopů pro obchodní a provozní činnost podniku	13
2.8	SWOT analýza řešení virtuálních desktopů	16
3	PRINCIPY VIRTUALIZACE	19
3.1	Definice virtualizace	19
3.2	Serverová virtualizace.....	20
3.3	Výhody využití virtualizace	20
3.4	Typy virtualizace.....	21
3.5	Komponenty virtuálního serveru v Hyper-V.....	22
4	ARCHITEKTURA INFRASTRUKTURY VIRTUÁLNÍCH DESKTOPŮ.....	26
4.1	Windows Server 2012 R2	26
4.2	Hyper-V	29
4.3	Nástroje System Center	40
4.4	Další komponenty VDI infrastruktury	45
4.5	Licencování architektury VDI	48
4.6	Infrastrukturální a další aplikační systémy.....	49

5	NÁVRH ŘEŠENÍ PRO STŘEDNĚ VELKOU SPOLEČNOST	52
5.1	Návrh postupu implementace	52
5.2	Analýza prostředí a požadavků	54
5.3	Návrh infrastruktury	56
5.4	Detailní popis technologické implementace pilotní fáze – fyzický návrh řešení	61
5.5	Detailní popis technologické implementace pilotní fáze – logický návrh řešení	70
5.6	Škálovatelnost a další možný rozvoj	84
6	POROVNÁNÍ VIRTUALIZOVANÉHO A KLASICKÉHO ŘEŠENÍ.....	87
6.1	Funkční porovnání	87
6.2	Finanční porovnání	88
7	ZÁVĚR.....	92
	SEZNAM POUŽITÉ LITERATURY	94
	SEZNAM OBRÁZKŮ	96
	SEZNAM TABULEK.....	96
	PŘÍLOHY	98

1 Úvod

Jedním z trendů v informačních technologiích je virtualizace desktopů, která vychází z tradičních principů virtualizace, ovšem není zaměřena na tradiční virtualizaci serverů, ale na virtualizaci klientských operačních systémů.

Virtualizace desktopů je též označována zkratkou VDI, která vychází z anglického názvu Virtual Desktop Infrastructure. Tento anglický název již napovídá, že se nejedná pouze o jeden nástroj, který se implementuje, ale jedná se o celou infrastrukturu, tedy souhrn několika nástrojů a principů, díky kterým se docílí implementace virtualizace desktopů a výhodám použití tohoto řešení, které jsou přenášeny nejenom do běžného provozu podniku, ale ovlivňují i finanční stabilitu podniku a podporují úsporu nákladů.

VDI řešení tedy zahrnuje konsolidaci a virtualizaci klientských operačních systémů, které jsou provozovány v datovém centru společnosti a uživatelé k těmto desktopům přistupují buď pomocí tzv. tenkých nebo zero klientů, pomocí protokolu pro vzdálené připojení nebo pomocí webového prohlížeče.

Virtualizace desktopů napomáhá k eliminaci potřebných zdrojů, zajišťuje automatizaci v oblasti doručování aplikací, dále napomáhá v oblasti bezpečnosti a dalších benefitů spojených s VDI.

Tato diplomová práce se zabývá virtualizací desktopů v podání společnosti Microsoft, kdy představuje virtualizaci obecně a VDI řešení od společnosti Microsoft a použití dalších nástrojů od této společnosti, které s virtualizací desktopů a virtualizací obecně souvisejí.

Samotná práce je členěna do několika částí, které odpovídají kapitolám této práce.

Druhá kapitola bude věnována analýze požadavků podniku na IT infrastrukturu především z manažerského pohledu, výhodám využití virtualizace virtuálních desktopů a úsporám nákladů.

Třetí kapitola se bude věnovat obecným principům virtualizace, především zaměřeným na platformu Hyper-V.

Čtvrtá kapitola bude obsahovat popis komponent infrastruktury virtuálních desktopů od společnosti Microsoft a nástrojům, které s virtualizací desktopů a serverů přímo nebo nepřímo souvisejí.

V páté kapitole bude popsán návrh řešení pro středně velkou společnost, zanalyzovány požadavky a popsána technická implementace návrhu pro pilotní provoz.

Šestá kapitola porovná virtualizované a klasické řešení a následně budou vyvozeny závěry o vhodnosti řešení, které budou zaměřeny především na funkční a finanční hlediska obou řešení.

Teoretická část práce bude věnována především principům řízení IT, principům IT infrastruktury, principům virtualizace a architektuře virtuálních desktopů. Teoretická část bude především rozvrhnutá v kapitolách 2, 3 a 4.

Praktická část práce bude věnována virtualizaci desktopů a virtualizaci systémů, které poskytují podporu virtualizaci desktopů. V praktické části bude vycházeno z principů popsaných v teoretické části této diplomové práce. V praktické části bude popsána implementace virtualizace ve fiktivní firmě a dále porovnání virtualizovaného a klasického řešení. Praktické části budou věnovány především kapitoly 5 a 6.

Cílem práce je provést analýzu technického řešení infrastruktury virtuálních desktopů ve fiktivním prostředí, které vychází za standardních potřeb podniků v oblasti IT a především pracovnímu nástroji většiny pracovníků, tedy počítači. Toto řešení poté porovnat s klasickým a stávajícím řešením pomocí klasických osobních počítačů, a to především z hlediska finančního a funkčního.

2 Analýza požadavků podniku

Tato kapitola je věnována požadavkům podniku na služby poskytované IT odděleními, které podporují primární náplň podniku, tedy jeho výdělečnou činnost.

Uvedené požadavky jsou orientované na provozované aplikace, síťovou infrastrukturu a dostupnost služeb a v neposlední řadě mobilitu a efektivitu práce pracovníků. Důležitým faktorem jsou ale především náklady na jednotné informační zdroje a služby.

2.1 IT strategie

Voříšek a Pour (2012, s. 48) rozdělují strategii IT na 3 možná zaměření a cíle, na které se strategie IT může zaměřit za účelem zefektivnění a vyšších přínosů pro podnik:

- Snížení IT nákladů a zároveň udržení dosavadních IT služeb, což může zahrnovat zastavení plánovaných projektů, které nemají podstatný efekt na zvýšení výkonnosti podniku, konsolidaci aplikací, centralizaci a virtualizaci zdrojů, cenový tlak na dodavatele služeb, snížení parametrů smluv o poskytování služeb, případně propuštění neproduktivních pracovníků.
- Zvýšení výkonnosti podnikové informatiky při stejných nákladech, což zahrnuje změnu IT Governance modelu, který bude zefektivňovat práci IT oddělení, zvýšení efektivity IT procesů a služeb, možnost zavedení outsourcingu IT služeb, zajištění škálovatelnosti IT infrastruktury a služeb, zefektivnění práce uživatelů případným školením a motivací a revize a zefektivnění smluv s dodavatelem služeb.
- Optimální IT podporu nového byznys modelu, což zahrnuje prosadit nový byznys model organizace za podpory IT, například zavedením nových služeb, outsourcingem celého nebo části IT.

2.2 Aplikační požadavky podniku

Význam IT technologií a jejich vlivu na činnost podniku se liší podle sektoru, ve kterém podnik vykonává svou činnost. (Voříšek a Pour, 2012, s. 41)

Lze ale určit několik aplikací a systémů, které podniky využívají bez rozdílů významu IT technologií.

Mezi tyto aplikace patří editory pro tvorbu dokumentů, kterými jsou produkty z kancelářského balíku Microsoft Office, mezi které patří především textový editor Microsoft Word, tabulkový editor Microsoft Excel, nástroj na tvorbu prezentací Microsoft PowerPoint, klient elektronické pošty Microsoft Outlook nebo další aplikace. Tento kancelářský balík lze případně nahradit open source řešením Apache OpenOffice.

Podnikové aplikace by především měly zjednodušovat práci uživatelů a zefektivňovat a podporovat podnikové procesy.

Dalším typem aplikací jsou aplikace pro komunikaci uživatelů v reálném čase, kterými může být například Microsoft Lync, Skype, případně další jiné aplikace pro komunikaci.

Významným prvkem v aplikacích a strategiích IT je existence a výběr infrastrukturních aplikací, kterými jsou například programy pro antivirovou ochranu počítačů a serverů v síti nebo webové prohlížeče, které slouží zároveň pro přístup do aplikací, které jsou přístupné z webového prohlížeče, čímž může být například Microsoft Dynamics nebo i samotný Internet.

Samotné používané podnikové aplikace určuje především IT strategie, která určuje, které aplikace budou patřit do základních aplikací používaných ve společnosti, aplikace které budou podporované, anebo aplikace, které budou v podniku přímo zakázané. Z tohoto hlediska bude také poskytována podpora těchto aplikací provozním IT oddělením a v případě požadavků na novou aplikaci by měla být zvažena především možná existence již používané aplikace v podnikovém prostředí, která nabízí stejnou nebo podobnou funkčnost, tak aby se dbalo na konsolidovanou správu aplikací.

Samotná strategie v ohledu aplikací je především ale dána již zmíněným zaměřením společnosti a dále velikostí organizace a IT strategií a IT Governance, tedy přístup ke sladění IT a obchodní strategie podniku.

Z pohledu doručování aplikací lze aplikace rozdělit na následující typy:

- Aplikace, které je potřeba nainstalovat na počítač a jsou samostatně provozu schopné.
- aplikace, které se instalují na počítač uživatele, ale slouží jako klient pro připojení k serveru,
- webové aplikace, které jsou přístupné přes webové rozhraní,
- virtualizované aplikace, které se spouští na počítači uživatele, ale pro běh jsou využívány zdroje serveru.

Dále ze základního pohledu pořízení aplikací lze rozdělit aplikace na aplikace pořízené nákupem hotového softwaru, vlastním vývojem softwaru, objednáním a nákupem softwaru na zakázku nebo využitím nějakého open source nástroje volně dostupného pro komerční využití.

2.3 Modely architektury

Mezi základní modely architektury ICT patří jednotná infrastruktura, privátní cloud a hybridní cloud. (Smoot a Tan, 2012, s. 2-9)

Jednotná infrastruktura

Infrastruktura je vytvořena pouze pro používání virtuálních strojů, který lze rozdělit do několika segmentů, ale je potřeba řešit selhání a předcházení selhání tohoto prostředí, takže mezi nevýhody tohoto řešení je potřeba mít dostatečně kvalifikovaný personál. Oproti tomu výhodou jsou nižší náklady na vlastnictví.

Privátní cloud

Tento model přináší snížení rizika chyby díky kombinací několika systémů na stejném hardwaru, ale to přináší potřebu výkonných zařízení a zkušeností.

Dále je v tomto modelu potřeba rozdělit zdroje do několika datacenter, což přinese výhodu v tom, že pokud by jedno datacentrum selhalo, tak uživatelé mohou přistupovat k výpočetnímu výkonu v datacentru druhém, což u jednotné infrastruktury nelze.

Hybridní cloud

Tento model kombinuje vlastní infrastrukturu a využívá i zdroje hostované nějakým poskytovatelem služeb. Takže část infrastruktury běží v datacentru společnosti a část v datacentru poskytovatele.

Veřejný cloud

Dalším modelem je veřejný cloud, kdy společnost využívá infrastrukturní výpočetní zdroje hostované v datacentru poskytovatele služeb, kdy služby a výpočetní zdroje jsou nabízeny více společností.

2.4 Vzdálený přístup k aplikacím a zdrojům

Jedním z typů pracovníků, kteří přistupují k firemní infrastruktuře, jsou tací, kteří přistupují k aplikacím a zdrojům, které běží v sídle společnosti nebo v datacentru přes vzdálené rozlehlé sítě, kterými jsou například WAN sítě.

Tito pracovníky musí návrh infrastruktury a aplikací respektovat a optimalizovat datové přenosy pro limitace rozlehlých sítí. (Smoot a Tan, 2012, s. 100)

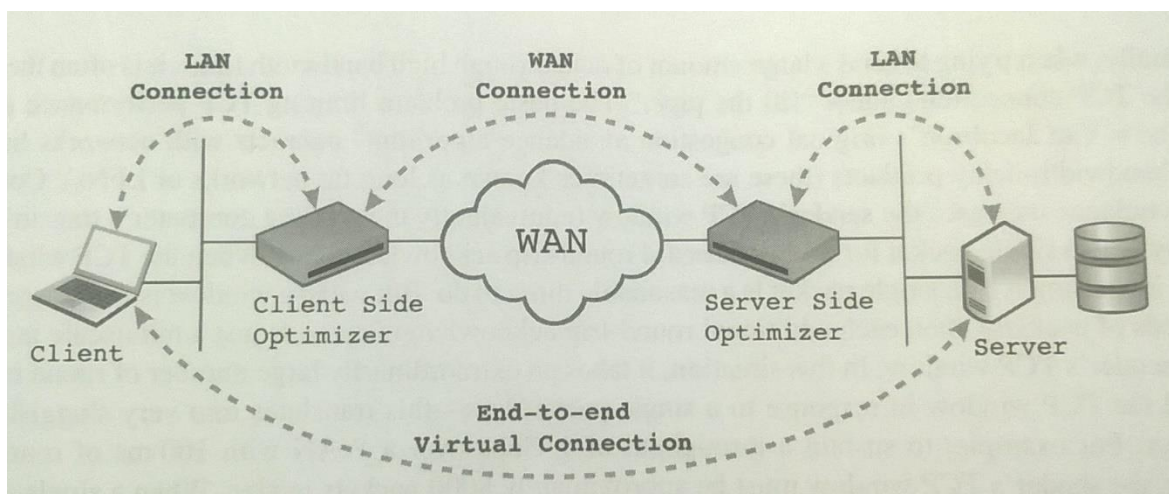
Smoot a Tan (2012, s. 122) tyto architektury infrastruktury označují jako optimalizované pro rozlehlé počítačové sítě (WAN), a dále je dělí na 3 základní typy, kterými jsou konsolidovaná architektura, architektura virtuálních desktopů a architektura virtuálních serverů a rozlišují se podle toho, kde jsou uložena data aplikací a kde probíhá výpočet nad těmito daty.

2.4.1 Konsolidovaná architektura

Prvním typem je konsolidovaná architektura, která respektuje, jak jsou služby nabízeny přímo servery, které nabízejí služby přímo do WAN sítě (např. Internetu). Mezi tyto služby patří například poštovní servery, databáze a další. Samotný hlavní aplikační a výpočetní výkon poté probíhá na klientském počítači uživatele.

Optimalizace je zde cílena na protokoly, jakými jsou například CIFS, MAPI, FTP, http a další. Tato konsolidace nabízí výhody, mezi které patří úspora nákladů, kvalitnější zálohování, vyšší pružnost a další. Nevýhodou je ovšem plná závislost na WAN síti.

Jedna z optimalizovaných architektur za použití jednoúčelového hardwaru, který optimalizaci provádí, je vidět na následujícím obrázku 1: Optimalizace WAN.



Obrázek 1: Optimalizace WAN, převzato z: Smoot a Tan (2012, s. 113)

Optimalizace dat probíhá především pomocí deduplikace, komprese, optimalizace latence spojení, ukládáním obsahu do mezipaměti a dalšími technikami.

Například společnost Microsoft nabízí technologii BranchCache, která optimalizuje datový tok pro WAN spojení pomocí ukládání kopií dat z hlavní lokality to vzdálených lokalit (například vzdálených kanceláří). Tyto kopie se nemusí poté několikrát denně stahovat z hlavní lokality, ale jsou uloženy na serveru, který je ve vzdálené umístěn lokalitě a ze kterého jsou nabízeny klientům v této vzdálené lokalitě. (Minasi et al., 2014, s. 14)

Technologie BranchCache je obsažena v systému Windows Server 2012 R2, ovšem hodí se pouze pro souborové systémy.

2.4.2 Architektura virtuálních desktopů

Druhým typem je architektura virtuálních desktopů (VDI), kde jsou zdroje, tedy výkonové a souborové servery centralizovány, resp. také konsolidovány v datacentru, ale přístup je řízen přes protokoly pro vzdálené připojení, mezi které patří Microsoft Remote Desktop Protocol, VMware View nebo Citrix ICA.

U těchto typů protokolů je optimalizace cílena právě na ty protokoly, kterými jsou uživatelé připojováni do datacentra. Výhody jsou podobné jako u konsolidované architektury, ale navíc je zde zredukována cena správy vzdálených počítačů a zlepšena bezpečnost.

Mezi důležité vlastnosti patří VDI komprese, která dokáže zredukovat využití linek nativními aplikacemi o 60 až 80 %. Dále dochází ke zlepšení zavedením kvality služeb (anglicky Quality of Service, tedy QoS) uvnitř VDI streamování, které dokáže zlepšit odezvu virtuálního desktopu uživateli. Mezi další techniky patří tradiční techniky pro WAN sítě v oblastech, jakými jsou tisk, nahrávání souborů a dalších.

Všechny tyto techniky přinášejí především úsporu a zlepšení návratnosti investic (ROI, Return on investment) a dále zlepšení produktivity uživatelů díky lepší reakci aplikací.

2.4.3 Architektura virtuálních serverů

Posledním, tedy třetím typem, je VSI architektura, tedy architektura virtuálních serverů, kdy data serverů jsou uložena na konsolidovaných úložištích v datacentru, ale samotné aplikační servery jsou u uživatelů a mezi datacentrem a těmito servery je rozlehlá WAN síť.

V této architektuře probíhá optimalizace na úrovni protokolu iSCSI nebo komunikačního rozhraní Fibre Channel, tedy technologie pro připojení síťového úložného pole (respektive disků).

Díky konsolidaci síťových úložišť toto řešení přináší úsporu nákladů, jednodušší management a zlepšení možností spojených se zálohováním.

2.5 Úspora nákladů v oblasti ICT

V oblasti analýzy nákladů v ICT, a nejenom v této oblasti, jsou základní ukazatele celkových nákladů na pořízení a návratnost investic. (Petřivalský, 2007)

Celkové náklady na vlastnictví

Celkové náklady na vlastnictví, anglicky Total Cost of Ownership (TCO) jsou celkové náklady na pořízení a držení daného aktiva. Tento ukazatel tedy zahrnuje nejenom

náklady na pořízení, ale i budoucí náklady na držení, které může být složité vyčíslit v době pořízení.

Návratnost investic

Oproti tomu návratnost investic, anglicky Return On Investment (ROI) je ukazatel, který ukazuje návratnost investice.

Rozdíl mezi TCO a ROI je především v tom, v jakých jsou uváděny jednotkách. TCO je suma veškerých nákladů a je uváděna v určité měně, například korunách. Oproti tomu ROI je poměrový ukazatel, který se uvádí v procentech.

Ukazatel ROI je spočítán jako poměr mezi náklady a přínosy, tedy:

$$ROI = (Přínosy/Náklady) * 100$$

Ve vzorci se jedná o přínosy, které řešením problematiky danému podniku přinese dodatečné úspory, takže jsou v nich zohledněny i počáteční výdaje.

V případě, že by se jednalo o investiční záměr, který přináší podniku zisk, by bylo potřeba vzorec rozšířit o výpočet přínosů:

$$ROI = ((Zisk - Náklady)/Náklady) * 100$$

Náklady

Mezi náklady v oblasti IT uvádí Petřivalský (2007) především následující položky:

- Hardware,
- software,
- technická podpora a upgrady,
- náklady na instalaci,
- náklady na školení,
- implementace a konzultace,
- záložní, vývojové, testovací a školicí prostředí,
- rozvoj, změny a rozšíření,
- lidské zdroje,

- energie.

Přínosy

Oproti tomu mezi přínosy, které informační a komunikační technologie podnikům přinášejí, patří především:

- Úspory,
- odvrácené ztráty,
- zvýšení obrátu a výnosů.

Alander (2013, s. 31) poukazuje, že celkové vyjádření celkových nákladů na pořízení (TCO) a návratnosti investic (ROI) se formuluje již ve fázi plánování projektu v oblasti ICT nebo alespoň jeho hrubý odhad.

Metody a nástroje snižování nákladů v oblasti IT

Jak již bylo zmíněno v kapitole 2.1 IT strategie, je jednou z možných strategií podniku snížení IT nákladů při stejné úrovni IT služeb, které jsou důležité pro konkurenceschopnost podniku. (Voříšek a Pour, 2012, s. 48)

Mezi základní nástroje, které lze použít pro snížení nákladů na informační technologie a související služby a zdroje použít patří:

- Zastavení IT projektů, které nemají zásadní vliv na zvýšení výkonnosti podniku. Pro úspěch této metody je důležité zanalyzovat nejenom plánované výdaje na IT projekt, ale i plánovaný efekty, které ovlivní činnost a hlavně výkonnost podniku.
- Konsolidace aplikací, což znamená snížení počtu aplikací, kde je důležité používané aplikace standardizovat (například výběr jednotného podporovaného webového prohlížeče) a dále ukončení provozu aplikací, které nejsou v podniku standardizovány a ušetřit tím výdaje na provoz těchto aplikací. S konsolidací aplikací souvisí i jejich integrace tak, aby všechny aplikace využívaly stejnou datovou základnu a eliminovala se duplicita dat.

- Dalším nástrojem je centralizace IT zdrojů a sdílení softwarových, hardwarových a lidských zdrojů efektivněji s ohledem na možné negativní dopady na flexibilitu a provoz.
- Mezi moderní nástroje k eliminaci nákladů na IT patří virtualizace, která poskytuje především zvýšení využití zdrojů a zjednodušení správy těchto zdrojů. Virtualizaci je možné využít ke zvýšení efektivity využívání lidských zdrojů tvorbou virtuálních týmů. Samotnému využití virtualizace hardwarových zdrojů jsou věnovány další části této práce, které jsou věnovány virtualizaci serverů a virtualizaci desktopů.
- Dalším moderním a neméně důležitým nástrojem je outsourcing IT zdrojů a služeb, který vede k získání potřebné IT služby bez nutnosti vlastnictví IT zdroje, resp. zdrojů, kterými mohou být například aplikace, infrastruktura nebo lidský kapitál. Samotný outsourcing je označován jako XaaS, neboli Everything as a Service (česky cokoliv jako služba). Například se může jednat o software jako službu (SaaS), infrastrukturu jako službu (IaaS), desktop, tedy klientský operační systém jako službu (DaaS) nebo další. Společnost tedy může využít služeb, které by pro ni nebylo efektivní samotné nakupovat, ať už z důvodu využití, cenové nedostupnosti a neefektivnosti pořízení. Na takto pořízených IT službách lze ušetřit i díky platbě za jejich reálné využití a v případě, že podnik nepotřebuje využít celou kapacitu, tak tuto odebíranou kapacitu snižuje.
- Další metodou, která má navíc téměř nulové náklady, je cenový tlak na dodavatele, kdy podniky mohou nabízené služby vybírat na trhu od více dodavatelů a tím vzniká tlak na dodavatele na zlepšení cenových a platebních podmínek.
- Možnost snížení parametrů smlouvy o IT službě a jejím poskytování (Service Level Agreement, SLA) díky kterým lze ovlivnit náklady snížením požadavků na kvantitativní a kvalitativní parametry služby, čímž lze ušetřit na nákladech za služby, které nejsou nutné a kritické pro potřeby a provoz podniku a tudíž jejich případný výpadek neovlivní krátkodobě činnost podniku.
- Posledním možným nástrojem pro snížení nákladů IT je propuštění neproduktivních pracovníků, které je ovšem nutné pečlivě zvážit, protože s pracovníkem odchází nejenom náklady na něho, ale i v mnoha případech podstatné a pro podnik kritické know-how.

Green IT a energetická úspora

Pojem Green IT zahrnuje postupy a přístupy, které jsou zaměřeny na ekologické inovace v oblastech informačních technologií, které vedou k úsporám energií a eliminaci ekologické zátěže a které definují uživatelsky akceptovatelné změny a podporují inovativní přístup. (Faucheux a Nicolai, 2011, s. 2026)

Úspora energií vede především k úsporám nákladů v oblastech, kam zasahuje především možnost využití regulace, měření a sledování spotřeby, využití technologií s malou energetickou náročností a další.

Typické plýtvání elektrické energie je v případě, že má společnost mnoho zastaralých fyzických serverů běžících v datacentru. (Minasi et al., 2014, s. 9)

Tyto běžící servery spotřebovávají elektrickou energii, která také přináší další náklady, které by mohly být využity k nákupu nového fyzického serveru, který by lépe využil možné kapacity zdrojů, uspořil energii a snížil potřebu chlazení.

2.6 Základní výhody virtualizace serverů pro obchodní a provozní činnost podniku

Marshall (2006, s. 47) uvádí jako první krok pro nasazení serverové virtualizace uvědomění si, jak může být nasazena v souladu s obchodními cíli podniku a tím vyřešení obchodních a provozních problémů v činnosti podniku.

Serverová virtualizace byla vytvořena především jako pomoc s řešením obchodních problémů, kterými jsou například konsolidace serverů, kdy se šetří náklady běhu několika systémů na svém dedikovaném hardwaru použitím virtualizovaných instancí pro tyto systémy na jednom hardwarovém zdroji.

Virtualizace také přináší možnost řešení problémů s nedostupností a nedosažitelností systémů a dále přináší možnosti v oblasti zotavení po havárii, vysoké dostupnosti a automatizace v případě havárie nebo nežádoucím chování systémů.

Další výhodou virtualizace je abstrakce mezi fyzickou a virtuální vrstvou, kde je nepodstatné na jakém hardwaru virtuální stroj běží.

Mnohé podniky musí používat aplikace, pro které ještě nebyla, anebo nikdy nebude, vytvořena verze pro aktuální operační systémy. Pomocí virtualizace je možné zachovat běh těchto aplikací.

2.7 Základní výhody virtualizace desktopů pro obchodní a provozní činnost podniku

Problematika řešená v této diplomové práci se týká virtualizace desktopů a jejich přínosů pro podniky, v následující části jsou shrnuty zásadní a základní přínosy, které by nasazení této technologie podniku přineslo.

Především by ale mělo být mezi klíčovými otázkami řešeno, jaký problém daný projekt dokáže vyřešit a co bude jeho přínosem. (Alander, 2013, s. 31)

Mezi základní výhody virtualizovaných desktopů, které ovšem nesou sebou i další možnosti a povinnosti patří následující oblasti.

Úspora nákladů

Úspora nákladů je jedním z hlavních možných výhod. Úsporu nákladů lze docílit i využitím stávajících zdrojů, jakými jsou například servery a počítače.

Samozřejmostí je tedy celková minimalizace nákladů na vlastnictví dané technologie (TCO) a maximalizaci návratnosti investice (ROI), které byly probírány v předchozí kapitole.

Upgrade operačních systémů

Díky upgradu operačních systémů, ke kterému dojde, může nastat zlepšení stávající infrastruktury a především služeb poskytovaných ICT oddělením, díky využití funkcionalit nových systémů.

Dále upgradem dochází k eliminaci nepodporovaných operačních systémů.

Mobilita

Zavedením virtuálních desktopů může dojít k větší mobilitě pracovníků, kteří se tak mohou připojit ke svému pracovnímu desktopu odkudkoliv a dokonce ani nemusí mít

přidělený pracovní hardware a mohou se připojit z vlastního zařízení díky novému konceptu BYOD (více v kapitole 2.6.3 – Koncepce BYOD).

Bezpečnost

V porovnání s klasickými desktope a notebooky je virtuální prostředí bezpečnější, protože dochází v první řadě pouze k přenosu obrazu k uživateli.

2.7.1 Úspora nákladů v oblasti virtuálních desktopů

Projekty v oblasti virtualizace desktopů mají vysoké prvotní náklady a návratnost investice nemusí být pokryta do 4 až 5 let, takže je potřeba sladit tento projekt se strategickými cíli organizace.

Mezi důležité faktory k úspěšnému projektu v oblasti virtuálních desktopů Alander radí především následující faktory:

- **Sledování poptávky po výpočetních zdrojích**, tedy využití hardwaru a softwaru a dalších služeb uživateli.
- **Ověření proveditelnosti návrhu řešení**, které ukáže, jestli je požadovaný návrh na architekturu virtuálního prostředí realizovatelný. Pro ověření je dobré rozdělení projektů do několika menších fází a pilotní ověřování funkčnosti.
- **Nastavení očekávaných přínosů**, které dané řešení a projekt přinese. Základním předpokladem by ale měl být fakt, že konečné řešení bude mít větší aktuální úroveň služeb, než bylo před započítáním projektu.
- **Představa o konečném návrhu**, což znamená držet se jasné představy o konečném návrhu řešení a zaměřit se především na klíčové oblasti, kterými jsou počítačové sítě, model architektury, koncová zařízení, kterými se budou uživatelé moci připojit do virtuálního prostředí a zálohování celého prostředí.

2.7.2 Koncová zařízení

Podstatnou problematikou architektury virtuálních desktopů a především přístupu k ní je problematika koncových zařízení, protože je nutné dopředu promyslet, jak se uživatelé budou do infrastruktury připojovat.

Tato problematika se netýká jenom IT služeb, ale ovlivňuje fungování celého podniku a zavedení virtuálních desktopů může změnit fungování napříč celou společností.

Mezi možná koncová zařízení lze zařadit a zvažovat následující typy:

- Přístup přes software, který je nainstalovaný na uživatelskému zařízení.
- Zero klient, což jsou zařízení, která se spouštějí ze sítě a připojují se přímo do virtuálního prostředí.
- Tenký klient, který oproti zero klientu má nainstalovaný vlastní operační systém a především umožňuje vyšší výkon.
- Stávající počítače, pomocí kterých se uživatelé připojují do virtuálního prostředí (například pomocí speciálního softwaru nebo pomocí protokolu RDP).

2.7.3 Koncepce BYOD

Koncepce BYOD, což je zkratka anglického spojení Bring Your Own Device, znamená využívání chytrých telefonů, tabletů, přenosných počítačů a dalších zařízení zaměstnanci k pracovním povinnostem. (Waterfill a Dilworth, 2014, s. 26-36)

Společnost by ale neměla řešit v případě, že uvažuje zavedení koncepce BYOD, pouze technická řešení zavedení, ale především zavést komplexní politiku, která bude zahrnovat všechny aspekty koncepce, kterými jsou například: jaká zařízení budou podporována, co bude uživatel muset zaručit v tomto zařízení (například funkčnost a aktuálnost antiviru), jak bude kontrolována činnost uživatele, kdy se uživatel bude moci do virtuálního prostředí připojit, jak se bude postupovat, pokud uživatel zařízení ztratí nebo mu bude odcizeno, jak bude IT podpora společnosti řešit technické problémy s těmito zařízeními a řadu dalších aspektů.

Ve spojitosti s architekturou virtuálních desktopů lze koncept BYOD využít jako koncové zařízení uživatele při připojení se do virtuálního prostředí, kdy se uživatel může připojit pomocí speciálního softwaru nebo pomocí protokolu Remote Desktop Protocol k virtuálnímu počítači v datacentru a na něm pracovat. Toto řešení přináší i bezpečnostní ochranu, protože jediná data, která se do zařízení dostanou, je pouze stream obrazovky virtuálního počítače.

Waterfill a Dilworth poukazují na přínosy, které přinášejí flexibilní pracovní prostředí a další výhody, kterými jsou například:

- Úspora nákladů na pořízení pracovních zařízení pro zaměstnance,
- úspora nákladů na opravy zařízení, protože zaměstnanci se pak o tato zařízení lépe starají, protože jsou jejich vlastní,
- spokojenost zaměstnanců, protože si tato zařízení vybírají sami,
- efektivita zaměstnanců, protože jsou na práci s tímto zařízením zvyklí,
- větší flexibilita zaměstnanců v pracovním čase,
- zaměstnanci jsou více kreativní a inovativní.

Oproti tomu nevýhody nebo rizikem koncepce BYOD je především bezpečnost, protože tato zařízení nemusí být pod takovým dohledem, jako jsou standardní zařízení zaměstnavatele.

Dále pak kontrola využití těchto zařízení, protože nelze efektivně kontrolovat, co uživatelé dělají a zda se věnují pracovním nebo soukromým záležitostem.

Politika BYOD také musí zohledňovat, že data společnosti mohou být uložena na těchto zařízeních a je potřeba tedy řešit možnost návratu těchto dat nebo jejich smazání společností v případě, že například zaměstnanec společnost opustí.

2.8 SWOT analýza řešení virtuálních desktopů

Pro analýzu příležitostí, hrozeb silných a slabých stránek řešení virtuálních desktopů byla využita SWOT analýza zavedení řešení virtuálních desktopů, která je vidět v následující tabulce 1: SWOT analýza řešení virtuálních desktopů – silné a slabé stránky VDI řešení a v tabulce 2: SWOT analýza řešení virtuálních desktopů – příležitosti a hrozby VDI řešení.

Silné stránky	Slabé stránky
<ul style="list-style-type: none"> • Jednoduchá správa klientských operačních systémů a distribuce aktualizací Windows a aplikací. • Úspora elektrické energie v případě použití tenkých nebo zero klientů. • Výpadek klienta uživatele znamená pouze výměnu terminálu a uživatel se poté připojí ke svému virtuálnímu desktopu. • Dynamické přidělování výpočetních zdrojů a sdílení výkonu. • Škálovatelnost řešení. • Bezpečnost dat díky uložení v datacentru a data nemusí být ukládána lokálně a jednoduše zcizena. • Prodloužení doby výměny klientských systémů (tedy klientů pro připojení). 	<ul style="list-style-type: none"> • Vyšší prvotní investiční náklady. • Nutnost licencování některých doposud nepoužívaných technologií. • V případě výpadku celé virtualizační infrastruktury může dojít k výpadku fungování celé společnosti. • Vyšší nároky na IT personál, především IT administrátory. • Nemožnost provozu některých více hardwarově náročných aplikací. • V mnoha případech je implementace VDI spojena s nákupem doposud neznámých technologií pro společnost, což zvyšuje náklady na licence a externí konzultace.

Tabulka 1: SWOT analýza řešení virtuálních desktopů – silné a slabé stránky

Příležitosti	Hrozby
<ul style="list-style-type: none"> • Konsolidace a standardizace prostředí klientských operačních systémů a aplikací. • Nižší časové nároky na osobní IT podporu jednotlivým uživatelům. • Oddělení závislosti na jediném hardwaru (typicky jediný disk v klasickém PC a další). • Možnost využití deduplikace uživatelských dat. • Možnost integrace zálohování. • Kratší doba pro migraci mezi verzemi operačních systémů. • Možnost využití konceptu BYOD. • Jednodušší integrace principů vysoké dostupnosti systémů a aplikací. 	<ul style="list-style-type: none"> • Nutnost správné identifikace a eliminace slabých míst infrastruktury. • Nesprávný návrh infrastruktury. • Opomenutí základních principů a dosavadního fungování společnosti. • V případě využití konceptu BYOD je nutné zajistit procesy kontroly připojovaných zařízení. • V případě implementace je mnohdy potřeba se obrátit na externího partnera v případě nevlastnění know-how ohledně virtualizace desktopů a souvisejících technologií.

Tabulka 2: SWOT analýza řešení virtuálních desktopů – příležitosti a hrozby

3 Principy virtualizace

V následující kapitole budou rozebrány a představeny jednotlivé typy virtualizačních konceptů a technologií.

3.1 Definice virtualizace

Nejdříve je potřeba virtualizaci jako takovou definovat. Amit Singh, autor portálu kernelthread.com, definuje virtualizaci jako rámec nebo metodologii dělení zdrojů počítačů do několika výkonných prostředí aplikováním jednoho nebo více konceptů nebo technologií, mezi které patří hardwarové nebo softwarové dělení, sdílení času, částečná nebo kompletní simulace počítačů, emulace, kvality služeb a mnoha dalších. (Olzak et al., 2010, s. 3)

Dále ovšem Olzak dodává, že tato definice nezvažuje obchodní pohled a měla by být více založena na očekávané přínosy.

Podle Olzaka je tedy virtualizace konfigurace serverů nebo klientských systémů, jejímž výsledkem je rozdělení zdrojů do několika izolovaných výkonových prostředí, díky čemuž dojde pomocí aplikování jednoho nebo více konceptů nebo technologií k redukování nákladů a zvýšení flexibility spojené se získáváním, implementací, řízením, rozšiřováním a obnovou kritických podnikových systémů.

Další možná definice virtualizace popisuje, že se jedná o metodu abstrakce fyzických zdrojů od ostatních kooperujících prostředků. (Panek, 2013, s. 367).

Panek dále dělí virtualizaci na 4 typy virtualizace:

- **Serverová virtualizace**, která umožňuje běh několika virtualizovaných operačních systémů na jednom fyzickém zdroji, tedy serveru. Typickým příkladem v podání společnosti Microsoft je technologie Hyper-V.
- **Prezentační virtualizace**, která umožňuje oddělení běhu aplikace a výsledek výpočtů, které aplikace provádí na jiném fyzickém zdroji. Příkladem této virtualizační technologie je například Microsoft Remote Desktop Services pro vzdálené připojení k virtualizovaným operačním systémům v datacentru.

- **Desktopová virtualizace**, která poskytuje využití virtualizace na klientském operačním systému. Díky čemuž uživatel může na jednom klientském počítači využívat více instancí operačních systémů nebo více platforem (např. Windows a Linux). Tento typ virtualizace je podobný serverové virtualizaci a od Windows 8 se technologie Hyper-V nachází i v typicky klientském operačním systému.
- **Aplikační virtualizace**, která umožňuje spouštění aplikací v odděleném režimu a pomáhá chránit běh aplikací a konflikty mezi nimi. Dále umožňuje izolovat běh aplikace od běhu operačního systému a řešit nekompatibilitu mezi aplikacemi. Příkladem může být například technologie App-V od společnosti Microsoft.

3.2 Serverová virtualizace

Definice virtualizace napovídají, že virtualizace je především o dělení zdrojů, které fyzický server poskytuje. Komponenty serverů jsou děleny (Marshall, Reynolds, McCrory, 2006, s. 27) do několika vrstev hardwaru a softwaru, které spolu vytvářejí systém serveru.

Voříšek a Pour (2012, s. 49, s. 174) označuje virtualizaci výpočetních strojů jako metodu, která dopomáhá k centralizaci IT zdrojů, čímž snižuje náklady na IT. Dále pak poskytuje snadno škálovatelnou platformu požadovaných charakteristik, kterými jsou požadovaný operační systém běžící ve virtuálním prostředí a jeho nastavení.

3.3 Výhody využití virtualizace

Výhody vyplývající z využití virtualizace v podnikovém prostředí jsou popsány v následující části. (Marshall, Reynolds, McCrory, 2006, s. 6)

1. Přenosnost systémů,
2. zjednodušená správa prostředí,
3. efektivnost využití zdrojů,
4. konsolidace serverů,
5. podpora starších typů aplikací,
6. podpora několika operačních systémů na jednom hardwaru,
7. vývoj, testování a ladění softwarů,
8. technické vzdělávání a E-Learning.

Dále ovšem Marshall zmiňuje, že není dobré a efektivní využívat virtualizaci pro využití se specializovaným hardwarem a periferiemi, pro výkonnostní testování a pro řešení problémů s ovladači hardwarových prostředků.

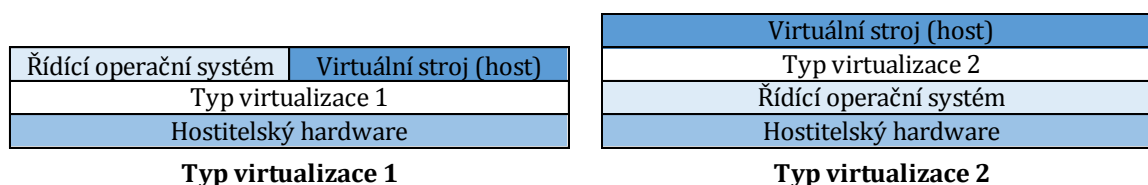
3.4 Typy virtualizace

Virtualizace je technologie, kde software simuluje hardware individuálního počítače na jednom počítači, kde běží nějaký typ virtualizační technologie. Tento počítač se nazývá hostitel a počítače, které na něm běží, se nazývají virtuální stroje, anglicky virtual Machines, resp. VM, nebo host. (Finn et al., 2013, s. 6)

Každý tento host má simulovaný hardware, který je specifikovaný alokací procesoru, úložiště, operační paměti a sítí. Dále má vlastní operační systém, který je izolován od operačního systému hostitele.

Na hostiteli běží několik hostů, kteří konzumují hardwarové zdroje hostitele podle svých nastavení a priorit. Principům alokace zdrojů se zaměřením na platformu Hyper-V je věnována kapitola 3.5 Komponenty virtuálního serveru v Hyper-V.

Existují 2 typy virtualizace – typ 1 a typ 2. Oba typy se od sebe rozlišují především tím, jestli hypervizor běží přímo na hostitelském hardwaru nebo hypervizorem a hostitelským hardwarem běží ještě hostitelský operační systém, což je vidět na následujícím obrázku 2: Typy virtualizace 1 a 2.



Obrázek 2: Typy virtualizace 1 a 2, převzato z: Finn et al. (2013, s. 6)

Vlevo je znázorněn typ virtualizace 1 a vpravo je znázorněn typ virtualizace 2 a oba obrázky nastiňují rozdíly ve vrstvách v obou typech virtualizace.

Typ virtualizace 1

Virtualizace typ 1 běží přímo na hostitelském hardwaru a mezi produkty, které tento typ virtualizace používají, patří například ESXi od společnosti VMware nebo Hyper-V od verze operačního systému Windows Server 2008.

Mezi jeho vlastnosti patří dobrá škálovatelnost, dobré výkonové vlastnosti a stabilita, protože se zde neobjevuje mezivrstva mezi virtuálním operačním systémem a hostitelským hardwarem.

Typ virtualizace 1 je znám též jako hypervizor.

Typ virtualizace 2

Oproti tomu virtualizace typu 2 se objevuje například ve starších verzích Hyper-V pro operační systémy Windows Server 2003 R2 a starší nebo produkt VMware Workstation od společnosti VMware.

Tento typ virtualizace má limitovanou škálovatelnost a výkonové limity a je závislý na hostitelském operačním systému.

3.5 Komponenty virtuálního serveru v Hyper-V

Samotná hardwarová konfigurace virtuálního serveru je podobná fyzickému serveru, tedy virtuálnímu serveru se také přiděluje procesor, operační paměť, pevné disky, síťové adaptéry a další.

Mezi základní komponenty virtuálních strojů v Hyper-V jsou operační paměť, procesor, řadič disků a síťový adaptér.

Operační paměť

Jedním z důležitých atributů virtuálního stroje v Hyper-V je operační paměť.

Mezi atributy, které se nastavují v oblasti operační paměti, je velikost paměti při spuštění virtuálního počítače. Po nastavení této hodnoty si systém alokuje tuto paměť po celou dobu běhu virtuálního stroje bez ohledu, zda ji využije nebo nevyžije.

Díky možnosti povolení dynamické paměti můžeme systému určit, jak bude nakládat dynamicky s přidělenou pamětí.

Povolením dynamické paměti získáme možnost určit:

- Minimální velikost paměti, což indikuje minimální alokovanou paměť virtuálního počítače, která bude alokována při běhu systému, která může být dokonce nižší než paměť při spuštění, díky čemuž zajistíme možnost vrácení nevyužité paměti hostitelskému systému.
- Maximální velikost paměti, což indikuje maximální velikost operační paměti, kterou si může daný virtuální počítač alokovat ze zdrojů hostitele.
- Vyrovňovací paměť, což je procento paměti, které technologie Hyper-V pokusí vyhradit jako vyrovňovací paměť pro daný virtuální počítač.
- Váhu paměti, což určuje prioritu dostupnosti paměti pro daný virtuální počítač.

Procesor

V oblasti procesoru lze určit počet virtuálních procesorů, které lze virtuálnímu počítači přidělit.

Dále je možné řídit prostředky pro vyvážení zatížení procesoru mezi virtuálními počítači pomocí následujících atributů:

- Vyhrazení pro virtuální počítač v procentech,
- limit virtuálního počítače v procentech,
- relativní váhu.

Dále lze v rozšířených možnostech povolit virtuálnímu počítači, aby mohl být migrován na fyzický počítač s jinou verzí procesoru.

Další rozšířenou možností je možnost konfigurace NUMA technologie, což je architektura neuniformního přístupu k paměti virtuálního počítače. Mezi atributy, které je možné nastavit, patří maximální počet procesorů, maximální velikost operační paměti a maximální počet uzlů NUMA, které jsou povolené v soketu.

Technologie NUMA je navržena pro multiprocesorové systémy, kde je možné nastavit možnost přístupu procesory do jiných paměťových bank, než které jsou vyhrazené pro jeho socket. (Finn et al., 2013, s. 97)

Virtuální úložiště

Jako řadič pro disky v technologii Hyper-V lze využít v generaci 1 virtuálního řadič IDE nebo SCSI a pro generaci 2 řadič SCSI a oba řadiče umožňují připojit virtuální disk, fyzický nebo optickou mechaniku, respektive ISO image nebo fyzickou optickou mechaniku. (Finn et al., 2013, s. 100)

Technologie Hyper-V nabízí možnost použití 3 typů disku pro virtuální počítač:

- Pass-through disk, což je fyzický disk připojený k danému počítači,
- formát VHD, což je virtuální disk, který se využívá v Hyper-V od verze Windows Server 2008 a může mít velikost pouze 2 TB,
- formát VHDX, který byl přidán do Windows server 2012, podporuje velikost až 64 TB, má lepší vlastnosti v případě nenadálého vypnutí počítače než předchozí verze.

Virtuální disky ve formátech VHD a VHDX poté nabízejí možnosti v alokaci jejich velikosti, která může být:

- Fixní disky, kdy je kapacita disku alokována již při jeho vytvoření, díky čemuž je disk rychlejší než ostatní typy virtuálních disků a je doporučován pro aplikace, které jsou náročné na čtení (Microsoft SQL Server nebo Microsoft Exchange).
- Dynamicky expandující se disk, kdy je nastavena maximální kapacita a disk se zvětšuje až do této kapacity, díky čemuž zabírá jen skutečnou potřebnou kapacitu.
- Rozdílový disk, kdy se vytvoří mateřský disk, ke kterému se poté vytváří rozdílové disky se změnami v tomto mateřském disku. Tento disk se hodí pro některé scénáře využití VDI řešení.

Pro virtuální disky lze dále nastavit maximální a minimální počet vstupně-výstupních operací, díky čemuž lze spravovat a eliminovat nežádoucí využití a zatížení fyzických disků, na kterých jsou virtuální disky uloženy.

Dále je možné v případě disků, které jsou připojeny přes rozhraní SCSI, povolit sdílení virtuálního disku mezi více virtuálními počítači.

Síťový adaptér

Připojením virtuálních počítačů k síti v Hyper-V lze zajistit přidělením syntetického síťového adaptéru nebo emulovaného staršího síťový adaptéru v generaci 1 a v generaci 2 pouze pomocí syntetického síťového adaptéru.

Typy virtuálních síťových adaptérů v Hyper-V lze zajistit pomocí následující typů virtuálních přepínačů:

- Externí přepínač, kterému se alokuje přímo fyzický adaptér připojený fyzicky k hypervizoru, který může buď dedikován pouze danému VM, nebo může být zapnuto sdílení v rámci více VM.
- Interní přepínač, který komunikuje v rámci daného přepínače, tzn. virtuálních strojů, které mají daný přepínač přidělen a se serverem Hyper-V.
- Privátní přepínač, který komunikuje pouze v rámci daného přepínače, tzn. virtuálních strojů, které mají daný přepínač přidělen.

Na úrovni síťového adaptéru lze zapnout tagování VLAN, omezit minimální a maximální šířku pásma a zajistit bezpečnost fyzické sítě pomocí zapnutí ochrany DHCP a ochranu směrovače.

Další komponenty

Mezi další komponenty patří například BIOS nebo Firmware, kde se nastavuje pořadí spuštění, ze kterých komponent se má systém spustit.

Dále adaptér Fibre Channel pro přístup k úložišti založením na technologii Fibre Channel.

V generaci 1 lze navíc přiřadit disketovou jednotku a COM porty.

4 Architektura infrastruktury virtuálních desktopů

Tato kapitola se převážně věnuje virtualizaci v podání společnosti Microsoft a je zde popisována technologie Hyper-V v návaznosti na předchozí kapitolu.

Dále je zde převážně popsáno využití dalších technologií, které se využívají pro správu celého virtuálního prostředí a jak napomáhají k virtualizaci desktopových operačních systémů a doručování těchto služeb koncovému uživateli.

Mezi tyto technologie patří především nástroje z rodiny System Center mezi které patří Configuration Manager, Operation Manager, Data Protection Manager, Service Manager a především Virtual Machines Manager.

4.1 Windows Server 2012 R2

Operační systém Windows Server je základem síťových technologií založených na platformě Windows.

Aktuální verzí je verze Windows Server 2012 R2, která vyšla v říjnu 2013.

Windows Server nabízí několik rolí a nástrojů, které se využívají především v infrastrukturní části výpočetních technologií. Mezi tyto role například patří Active Directory Domain Services pro správu celé sítě a vytvoření domény, DHCP server pro přidělování IP adres, DNS server pro překlad názvů počítačů a serverů v síti na IP adresy, role souborových služeb pro správu připojených disků a síťových úložišť a role Hyper-V serveru pro aktivaci virtualizace a platformy Hyper-V a mnoha dalších.

4.1.1 Edice Windows Server 2012 R2

Windows Server 2012 R2 má 4 hlavní edice – Datacenter, Standard, Essentials a Foundation. (Panek, 2013, s. 9)

Windows Server 2012 R2 Datacenter

Tato edice má plnou funkcionalitu a hodí se pro společnosti, které mají vysoce virtualizovanou infrastrukturu, protože umožňuje instalaci neomezeného počtu instancí virtuálních strojů.

Windows Server 2012 R2 Standard

Edice Standard se hodí pro společnosti, které mají spíše fyzické než virtuální servery. Dále má také neomezenou funkcionalitu, ale umožňuje aktivaci pouze dvou virtuálních instancí.

Windows Server 2012 R2 Essentials

Pro malé podniky, které mají minimum uživatelů, se hodí edice Essentials, která umožňuje pouze 25 uživatelů a 50 zařízení. Edice může být zvirtualizovaná, ale nemůže na ní být aktivována role Hyper-V.

Tato edice má zabudované jednoduché rozhraní pro integraci s cloudovými službami.

Windows Server 2012 R2 Foundation

Edice Foundation se hodí pro podniky, které mají méně jak 15 uživatelů, kde jsou potřeba pouze základní funkce (například DHCP a DNS server, doména, souborové sdílení a další).

4.1.2 Virtualizace ve Windows Server

Aktivace virtualizace ve Windows Server se provádí aktivací (přidáním) role Hyper-V Windows Serveru, která lze ovšem aktivovat pouze v edicích Datacenter a Standard, nebo případně lze využít speciální edici Microsoft Hyper-V 2012 R2, která je zmiňována dále v samostatné kapitole 4.1.3 - Microsoft Hyper-V 2012 R2. (Panek, 2013, s. 373)

Hardwarové požadavky Hyper-V

Minimální hardwarové požadavky pro aktivaci role Hyper-V jsou (Finn et al, 2013, s. 11; Panek, 2013, s. 372):

- Procesor, který umožňuje běh 64 bitových aplikací s podporou technologie Intel VT nebo AMD-V technologie. Minimální frekvence procesoru musí být minimálně 1,4 GHz, ale doporučeny jsou 2 GHz a vyšší.
- Minimálně 1 GB RAM, ale doporučeno je 2 GB RAM a více.
- Minimálně 8 GB místa na harddisku, ale doporučeno je 20 GB a více.
- Funkce zabránění spuštění dat – pro chránění před spuštěním škodlivého kódu je potřeba, aby byl povolen Data Execution Protection (DEP), kde data v paměti jsou označeny tak, aby procesor je nemohl spustit. Toto je potřeba povolit v BIOS nastavení serveru. Tato funkcionality chrání procesor od útoku zevnitř virtuálního stroje.

4.1.3 Microsoft Hyper-V 2012 R2

Microsoft vytvořil a vydal edici pouze pro použití jako hypervizor Hyper-V, tato edice se jmenuje Microsoft Hyper-V 2012 R2 a je dostupná zdarma ke stažení a obsahuje stejné Hyper-V funkcionality jako Hyper-V role v placeném Windows Server 2012 R2, ale má několik omezení. (Finn et al., 2013, s. 23)

Tato edice neobsahuje žádná virtualizační práva, takže nemůže být nainstalována jako virtuální host, lze ji ovšem využít:

- Jako hostitel pro licencovaný host pro Windows Server 2008 R2,
- pro výukové účely virtualizace trial verzí operačních systémů,
- pro virtualizaci linuxových operačních systémů,
- pro virtualizaci VDI řešení.

Dalším omezením je, že Hyper-V Server 2012 R2 nemá žádné grafické rozhraní a jedná se tedy o core instalaci, kde existuje základní textové rozhraní pro základní správu, ale rozšířená správa je nutná buď pomocí PowerShellu, nebo pomocí nástroje Remote Server Administration Toolkit (RSAT) pro Windows Server 2012 R2 nebo například pomocí nástrojů z rodiny System Center 2012 R2.

Pokud by společnost chtěla virtualizovat na produktu Hyper-V Server 2012 R2 klasický Windows Server 2012 R2, musela by nakoupit licenci pro tento operační systém.

4.1.4 Licencování Windows Server 2012 R2

Licencování Windows Server 2012 R2 je založeno na procesorech, kdy jedna licence může být přiřazena až 2 procesorům na jednom fyzickém serveru.

Samotný základní přehled licencování je vidět v následující tabulce 3: Licencování Windows Server 2012 R2.

<i>Edice</i>	Licencování	Serverové role, nástroje a možnosti škálovatelnosti	Virtualizační práva	Orientační cena
<i>Standard</i>	1 licence = 2 procesory na serveru	Bez omezení	2 volné virtuální instance	\$ 900
<i>Datacenter</i>	1 licence = 2 procesory na serveru	Bez omezení	Nelimitovaný počet virt. instancí	\$ 4800

Tabulka 3: Licencování Windows Server 2012 R2, převzato z: Finn et al. (2013, s. 22) a Microsoft© (2015b)

Nelimitovaný počet virtuálních instancí v případně edice Datacenter znamená virtuální instance pouze pro Windows Server. Virtualizace desktopů není zahrnuta a je nutné jí licencovat na základě klientských přístupových licencí (CALs) a VDA licencí.

Samotné srovnání rolí a omezení edicí Windows Server 2012 R2 a produktu Microsoft Hyper-V Server 2012 R2 je uvedeno v přílohách 1, 2 a 3.

4.2 Hyper-V

Platforma Hyper-V je základní virtualizační technologií pro virtualizaci čistě na platformě Windows.

Jak již bylo uvedeno, technologii Hyper-V lze získat buď instalací operačního systému Windows Server a následně aktivováním role Hyper-V nebo pomocí samostatného volně dostupného produktu Microsoft Hyper-V.

K pochopení architektury technologie Hyper-V patří základní pojmy, kterými jsou hypervizor, host a mateřský oddíl, též nazýván řídicí operační systém. (Cerling et al., 2010, s. 9)

Hypervizor je softwarová vrstva mezi fyzickým (hostitelským) hardwarem a minimálně jedním operačním systémem a jeho hlavním účelem je izolace prostředí do oddílů.

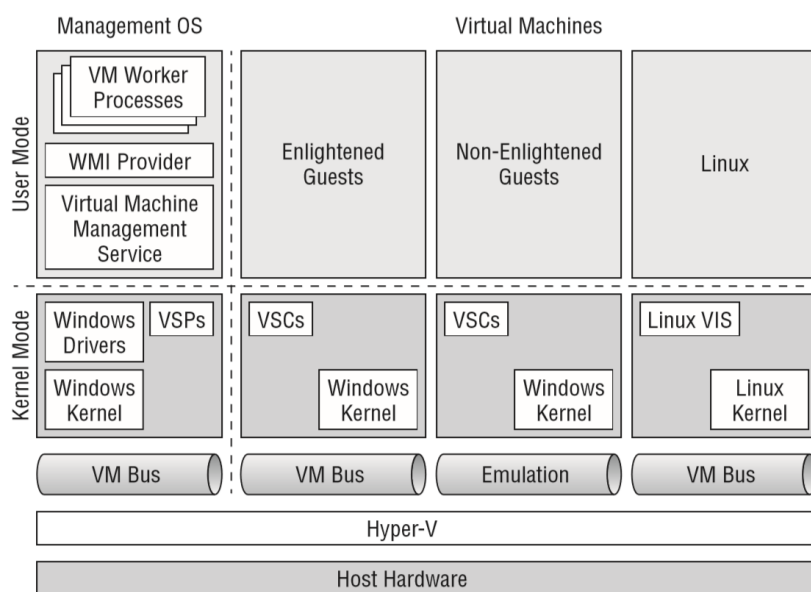
Host je operační systém, který běží na oddílu hypervizoru a často bývá nazván též virtuální stroj nebo VM.

Mateřský oddíl je oddíl, kde se nachází řídicí operační systém a chová se jako vlastník fyzických hardwarových zdrojů. Po vytvoření hostovaného oddílu přiřadí mateřský oddíl zdroje tomuto hostovanému oddílu, který se o ně poté stará sám.

4.2.1 Architektura technologie Hyper-V

Architektura technologie Hyper-V sestává z několika základních částí.

Na následujícím obrázku 3: Hyper-V architektura je vidět architektura technologie Hyper-V, která je tedy virtualizací typu 1.



Obrázek 3: Hyper-V architektura, převzato z Finn et al. (2013, s. 13)

Režimy pro řídicí operační systém

V Hyper-V existují 2 základní stupně oprávnění – Kernel Mode, tedy režim jádra, a User Mode, tedy uživatelský režim. (Minasi et al., 2014, s. 1354)

Režim jádra pro řídicí operační systém

Režim jádra, též někdy označován jako ring 0, je nejnižší blok, který běží s nejvyššími oprávněními k hostitelskému hardwaru a zahrnuje 4 bloky:

- Jádro Windows,
- rozhraní VMBus, které slouží k datové komunikaci mezi hostem a hostitelem,
- ovladače Windows pro řídicí operační systém,
- poskytovatele virtualizačních služeb (VSPs), který se stará o překlad dat mezi VMBus a ovladači Windows a klientech virtualizačních služeb (VSCs) ve virtuálních hostech.

Uživatelský režim pro řídicí operační systém

Uživatelský režim, též někdy označován jako ring 3, je nevyšší blok a má nejnižší oprávnění k hostitelskému hardwaru a zahrnuje:

- Službu management virtuálních strojů (VMMS), která se stará o správu všech virtuálních strojů,
- pracovní procesy virtuálních strojů (VMWP), který spravuje procesy pro konkrétního virtuálního hosta,
- poskytovatel WMI, který se stará o přenos ze vstupních zařízení (myši a klávesnice), přístup do BIOSu VM, správu konfigurace a stavu VM.

Typy virtuálních strojů v Hyper-V a režimy pro hostované oddíly

Na obrázku architektury Hyper-V jsou uvedeny 3 typy virtuálních strojů, které jsou využívány v Hyper-V (Finn et al., 2013, s. 13):

- Enlightened Windows Guest, tedy tzv. osvětlený host založený na Windows,
- Non-Enlightened Windows Guest, který bývá označován jako emulovaný host,
- Linux Guest, který bývá také označován jako osvětlený host založený na Linux.

Osvícený Windows host

Tento virtuální stroj má instalované integrační komponenty, které zajišťují, že operační systém si uvědomuje, že je virtualizován v Hyper-V, takže tyto komponenty přidávají podporu ovladačů pro virtuální zařízení, které Hyper-V může nabídnout hostu.

Dalšími možnostmi, které integrační komponenty přidávají, jsou například možnost čistého vypnutí z konzole Správce technologie Hyper-V bez nutnosti se do VM připojovat, možnost sdílení informací s řídicím operačním systémem, kterým jsou prezenční signál o stavu VM, synchronizace času, výměna dat, možnost vytváření kontrolních bodů a další.

Tento operační systém má rozhraní VMBus, které slouží k datové komunikaci mezi hostem a hostitelem, dále jádro v hostu instalovaného operačního systému Windows a klienta virtualizačních služeb (VSCs), který komunikuje s poskytovatelem virtualizačních služeb (VSPs) v řídicím operačním systému.

Emulovaný Windows host

Emulovaný Windows host je takový host, pro kterého neexistují integrační komponenty a je využíván pro virtualizaci například Windows 2000 Server a dalších zastaralých operačních systémů.

Takto emulované virtuální systémy bez integračních komponent nemohou využít naplno všechny vlastnosti technologie Hyper-V, kterými jsou například podpora SCSI rozhraní, syntetického síťového adaptéru nebo dynamické paměti.

Emulovaná zařízení v těchto hostech potřebují zvláštní rozhraní mezi uživatelským režimem a režimem jádra, což snižuje výkon virtuálního stroje v porovnání s osvíceným Windows hostem.

Emulovaný Windows host nemá nainstalované integrační komponenty, takže nemá klienta virtualizačních služeb, a nevyužívá ani rozhraní VMBus, takže využívá pouze emulace, nad kterou běží jádro hostovaného operačního systému.

Osvícený Linux host

Posledním typem virtuálních strojů v Hyper-V jsou osvícení virtuální hosté, kteří jsou založeni na nějaké podporované linuxové distribuci.

Pro tyto virtuální stroje existují linuxové integrační komponenty, které nabízejí takřka shodnou funkcionalitu pro linuxové distribuce jako hostitelé založení na Windows s integračními komponenty.

Linuxový host s instalovanými integračními komponenty má rozhraní VMBus, jádro systému Linux a klienta virtualizačních služeb.

4.2.2 Funkce technologie Hyper-V

Výčet klíčových funkcí, které umožňuje a poskytuje nejnovější verze technologie Hyper-V, je uveden v následující kapitole. (Panek, 2013, s. 368; Tulloch, 2013b, s. 5)

Nová architektura Hyper-V

Architektura založená na hypervizoru, který má 64 bitové jádro a umožňuje nové možnosti podpory zařízení a zlepšuje výkon a bezpečnost.

Nová architektura dále provádí zvětšení efektivity využití zdrojů, kterými jsou například disky a počítačové sítě.

Nový formát disků virtuálních strojů VHDX

Nový formát virtuálních disků VHDX nahrazuje předchozí verzi VHD.

Formát VHDX podporuje velikost až 64 TB, má vestavěnou ochranu před poškozením z důvodu násilného vypnutí a ochranu před snížením výkonu při použití fyzických disků s velkými sektory.

Zlepšení škálovatelnosti

Hyper-V hostitel, který běží na operačním systému verze Windows Server 2012, podporuje až 320 logických procesorů a 4 TB operační paměti.

Dále virtuální stroje, které na tomto hostiteli běží, mohou mít přiděleno až 64 virtuálních procesorů a 1 TB operační paměti.

Podpora operačních systémů

Podpora 32 a 64 bitových operačních systémů, které mohou běžet najednou na jednom fyzickém zdroji a také multiplatformní podpora, tedy různé platformy (Windows, Linux, apod.) na jednom zdroji v jeden čas.

Hyper-V ve verzi 2012 R2 podporuje operační systémy Windows XP se Service Packem 2 (SP 2) v 64 bitové verzi a vyšší nebo Windows XP se Service Packem 3 (SP3) v 32 bitové verzi. (Microsoft, © 2015a)

Dále pak edice Windows Server 2003 se Service Packem 2 a vyšší, včetně produktů Windows Small Business Server 2011 a Windows Home Server 2011.

Mezi linuxové distribuce, které jsou podporované v Hyper-V patří:

- Red Hat Enterprise Linux ve verzích 5.7 až 6.4,
- SUSE Linux Enterprise Server 11 SP2,
- CentOS ve verzích 5.7 až 6.4,
- Ubuntu Server 12.04, 12.10 a 13.04,
- Debian 7.0.

S podporou operačních systémů v Hyper-V souvisí i otázka integračních komponent, které slouží pro komunikaci mezi hypervizorem a virtuálním strojem.

Podpora pro symetrické mikroprocesory

Podpora až čtyř procesorů podporuje rychlejší výpočty a tudíž i běh aplikací je rychlejší ve virtuálním prostředí. Fyzický zdroj dokáže nabídnout virtuálním systémům vyšší výpočetní výkon.

Rozložení síťové zátěže

Hyper-V provádí podporu pro rozložení síťové zátěže, aby rozložila zatížení sítě mezi instancemi virtuálních systémů na různých serverech.

Rozšiřitelný virtuální přepínač

Hyper-V nově podporuje rozšiřitelný virtuální síťový přepínač, který zahrnuje nové funkcionality, kterými jsou monitoring síťových paketů, přeposílání paketů a filtrování paketů na úrovni virtuálního přepínače.

Rychlé přepnutí

Funkce rychlé migrace provádí možnost přesunutí a přepnutí instance virtuálního systému mezi rozdílnými fyzickými zdroji v klastru při selhání, což redukuje dopad na běh aplikace, redukuje čas, kdy aplikace, kterou systém poskytuje, je nedostupná a zvyšuje dostupnost virtualizovaného systému.

S touto funkcionalitou souvisí Hyper-V replika, která umožňuje replikaci virtuálních strojů mezi úložišti, klastry a datacentry, které jsou geograficky rozdílně umístěné, což zaručuje zlepšení v oblasti kontinuity podnikání a zotavení po havárii.

Snímkování virtuálních strojů

Tato funkcionalita poskytuje možnost vytvoření snímku běžícího virtuálního systému, který je poté možné rychle a jednoduše obnovit do stavu, v jakém byl v době pořízení snímku systému.

Měření využívaných zdrojů

Měření využívaných zdrojů poskytuje sledovat využití zdrojů jednotlivými uživateli, takže je možné nejenom toto využití sledovat, ale i poskytovat informace pro tvorbu další strategie a plánování zdrojů.

Skriptování

S využitím Windows Management Instrumentation (zkráceně WMI) rozhraní a API lze jednoduše vytvořit skripty pro automatizaci procesů v celém virtuálním prostředí.

Nedílnou a velice důležitou součástí skriptování ve Windows Server, ale i všech systémech založených na Windows, je Windows PowerShell, což je nástroj pro zadávání příkazů z příkazové řádky a slouží tak pro správu systému a jeho nastavení.

Windows PowerShell je založen na .NET Framework common language runtime (CLR) a .NET Framework a využívá, tzn. cmdllety, což jsou jednoduché a jednoúčelové příkazy, které jsou zadávány do příkazové řádky. (Panek, 2013, s. 23)

Výhody, které PowerShell přináší, jsou možnost správy několika zařízení najednou, možnost automatizace a správy několika systému nebo komplexní správy celého výpočetního prostředí. Dále je to možnost automatizace zotavení po chybě, kdy je možné naskriptovat, co se má stát v případě nežádoucí akce v systému (například přepnutí na záložní server v případě pádu serveru včetně dodatečné konfigurace záložního serveru).

Navíc síla PowerShellu v pokročilé správě systémů roste, jelikož ve Windows server 2012 existují funkce, které jinak, než za použití PowerShellu, zapnout nelze.

Ve Windows Server 2012 PowerShell zahrnuje více než 160 příkazů pro práci a automatizaci platformy Hyper-V.

Využití optických vláken

Tato funkcionality umožňuje připojit zařízení přes rozhraní Fibre Channel přímo do virtualizovaného systému. Mezi tato zařízení převážně patří úložiště dat, která využívají rychlé rozhraní Fibre Channel.

Dynamická paměť

Dynamická paměť umožňuje automatizovat přidělování operační paměti virtuálním systémům, díky čemuž mohou systémy, které aktuálně přidělenou paměť nevyužívají, tuto paměť poskytnout jiným systémům, které jí efektivně využijí.

Dále došlo k zavedení tzv. minimální paměti, která umožňuje nastavit nižší přidělení paměti během běhu virtuálního stroje. Díky tomuto je možné nastavit virtuálnímu systému vyšší paměť při startu, kterou poté systém podle potřeby vrátí k dalšímu využití.

Single-root I/O virtualizace

Tato technologie umožňuje síťovému adaptéru, který podporuje Single-root I/O virtualizaci (SR-IOV), přidělit adaptér přímo virtuálnímu stroji, který běží na Hyper-V hostiteli, což umožní maximalizaci síťové propustnosti a minimalizaci síťové latence a nutnosti zapojení procesorového času pro zpracování síťového provozu.

4.2.3 Strategické zaměření vývoje technologie Hyper-V

Nejnovější verze technologie Hyper-V je verze 2012 R2, která je zaměřena na několik strategických zaměření, která jsou vyjmenována v následující části (Finn et al, 2013, s. 10):

Automatizace

Automatizace je ve Windows Server řešena především pomocí skriptovacího jazyka PowerShell, který obsahuje přes 2500 příkazů a přes 160 jich je zaměřeno na technologii Hyper-V.

Síťování

V nové verzi Hyper-V a OS Windows Server došlo ke zlepšení výkonnosti, byla přidána funkce týmování síťových adaptérů na úrovni operačního systému, byly přidány partnerská řešení pro síťování v Hyper-V (např. Cisco Nexus 1000V).

Datové úložiště

Díky zlepšení v síťování došlo ke zlepšení souborového systému, jako ekonomický a škálovatelný systém, který je schopen neustále bez výpadků skladovat data virtuálních systémů. Dále díky implementaci průmyslových standardů byla přidána podpora řízení a výkonu datového úložiště.

Hyper-V v operačním systému Windows Server 2012 podporuje použití souborového sdílení Server Message Block 3.0 (SMB 3.0) pro uložení dat virtuálních strojů, což umožňuje využít cenově dostupný Scale-Out File Server vestavěný ve Windows Server na místo nutnosti nákupu drahých SAN (storage area network) řešení.

Pracovní mobilita

Řešení VDI v předchozí verzi Windows Server 2008 R2 bylo složité a komplikované, Microsoft zjednodušil architekturu VDI a zlepšil protokol Remote Desktop Protocol (RDP), který je využíván pro připojení k virtuálnímu stroji.

Microsoft zlepšil využívání periferií, které jsou připojeny na straně klienta, dále streamování médií a kvalitu služeb při využití pomalých linek, jako jsou linky WAN a Internet.

Byly přidány komponenty, které zlepšují pracovní mobilitu uživatelů.

Cloud

Mnoho zlepšení v Hyper-V bylo provedeno v kombinaci s modely cloudových služeb.

Platforma Hyper-V přináší zlepšení v ohledech na typ cloudu, tedy veřejný, privátní a hybridní. Tyto zlepšení jsou například měření využití zdrojů na úrovni virtuálních strojů.

4.2.4 Požadavky Hyper-V

Mezi požadavky pro využívání Hyper-V patří (Finn et al, 2013, s. 11) :

- Hardwarová podpora systému Windows Server 2012,
- 64 bitový procesor,
- podpora virtualizace na straně CPU (což znamená podpora VT-x pro procesory Intel a AMD-V pro procesory AMD),
- funkce zabránění spuštění dat – pro chránění před spuštěním škodlivého kódu je potřeba, aby byl povolen Data Execution Protection (DEP), kde data v paměti jsou označeny tak, aby je procesor nemohl spustit. Toto je potřeba povolit v BIOSu serveru. Tato funkcionality chrání procesor od útoku zevnitř virtuálního stroje.

4.2.5 Generace virtuálních strojů v Hyper-V

Technologie Hyper-V od verze operačního systému Windows Server 2012 R2 poskytuje dvě generace virtuálních strojů.

Obě generace mají společné rysy, ale obě mají i rozdílné vlastnosti. Rozdíl je ale především v poskytování virtuálního hardwaru každé generaci.

Výběr generace se provádí při vytváření virtuálního stroje a automatická konverze není možná. Proces konverze zahrnuje mnoho manuální práce.

Generace 1 i generace 2 mohou fungovat na stejném hostitelském hypervizoru souběžně, ale mezi oběma generacemi nelze jednoduše přepínat a je potřeba generaci vybrat již při vytváření virtuálního stroje.

Generace 1

Generace 1 vychází z původních standartních virtuálních strojů a je identická.

Tato generace využívá emulaci hardwarových zdrojů, které jsou k dispozici virtuálnímu stroji. Tato emulace především snižuje výkon hardwaru a zvýšenou konzumaci procesorového času.

Generace 2

Oproti generaci 1 nabízí generace 2 lepší výkon, nasazení a bezpečnost.

Mezi vlastnosti generace 2, které uvádí Tulloch (2013b, s. 7) patří podpora UEFI, takže umožňují bezpečné startování systému a jeho ochranu již od startu systému.

Další vlastností je odebrání emulovaných hardwarových zdrojů, které byly nahrazeny syntetickými ovladači a softwarově založenými zdroji.

Generace 2 virtuálních strojů také umožňuje bootování virtuálního stroje ze SCSI virtuálního zařízení (předchozí generace umožňovala pouze bootování z IDE virtuálního disku). Toto zařízení může být SCSI virtuální disk nebo SCSI virtuální optické médium.

Dále tato nová generaci přináší rychlejší nasazení díky možnosti síťové instalace operačního systému a standardní síťový adaptér umožňuje PXE boot (bootování ze sítě), takže není nutné virtuálnímu stroji přidělovat starší síťový adaptér (Legacy Network Adapter). Díky podpoře SCSI řadiče je instalace operačního systému rychlejší než v předchozí generaci.

Limitací generace 2 je fakt, že na takto vytvořeném hostiteli lze provozovat pouze operační systémy Windows 8 a vyšší a Windows Server 2012 a vyšší a ještě k tomu v 64 bitové verzi.

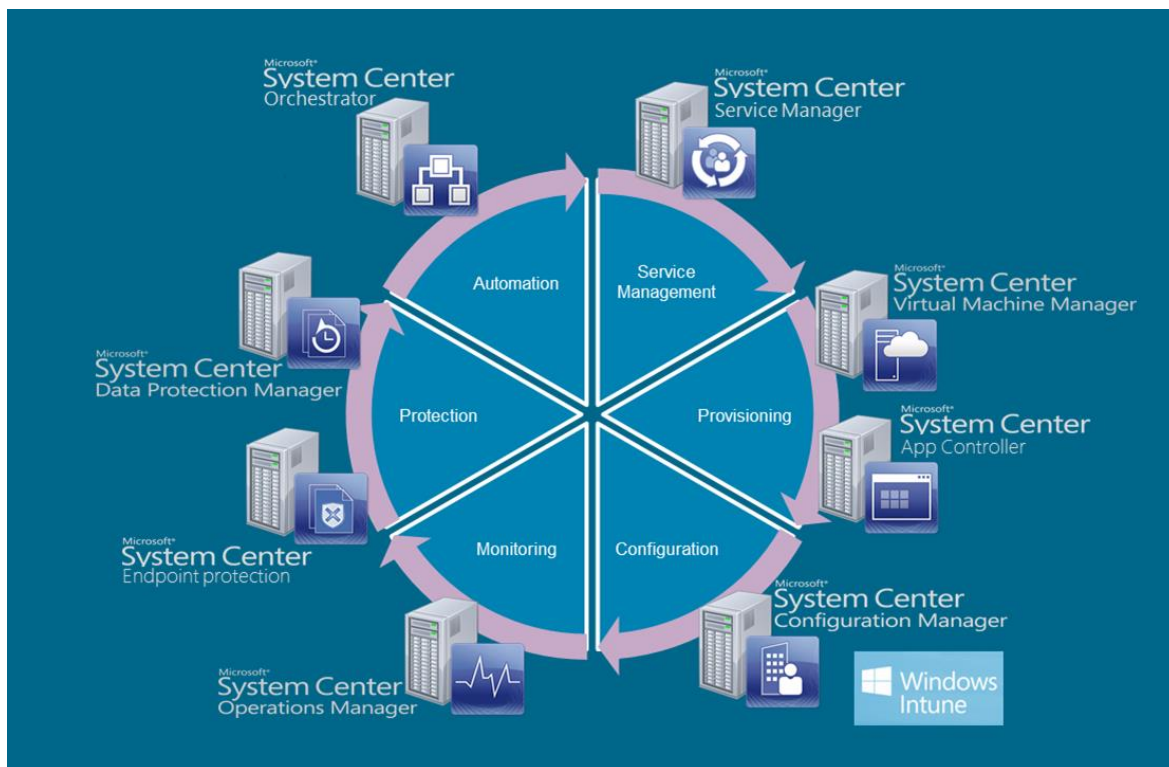
4.3 Nástroje System Center

Důležitými a mocnými nástroji pro použití v datacentrech a podnicích jsou nástroje z rodiny System Center, které dokáží pomoci s automatizací, správou a zjednodušením rutinních činností v oblasti IT a infromatické infrastruktury podniku.

Mezi tyto základní nástroje patří Virtual Machines Manager pro správu virtuálních strojů a virtualizované infrastruktury, Configuration Manager pro správu a konfiguraci operačních systémů, Operation Manager pro správu a monitoring služeb a aplikací, Data Protection Manager pro zálohování systémů, Service Manager jako nástroj pro správu incidentů a problémů, který vychází z ITIL.

Nástroje System Center nabízí možnost správy napříč celou infrastrukturou, ať už se jedná o on-premise řešení, které má společnost pod výhradní kontrolou, řešení, které poskytuje poskytovatel služeb nebo řešení pomocí prostředí Windows Azure. Tato správa je jednoduchá, cenově efektivní, aplikačně zaměřená a je založena na podnikové úrovni. (Tulloch, 2013a, s. 4)

Na následujícím obrázku 4: Nástroje z rodiny Systém Center je vidět provázanost všech nástrojů z rodiny System Center.



Obrázek 4: Nástroje z rodiny Systém Center, převzato z: Acevedo (2015)

4.3.1 System Center Virtual Machines Manager

System Center Virtual Machines Manager (dále VMM) nabízí možnost zajištění a možnost správy virtualizačních hostitelů, hostitelských klastrů a infrastrukturních zdrojů. (Tulloch, 2013a, s. 9)

VMM slouží ke správě virtualizačního prostředí a umožňuje vytvářet a nasazovat virtuální stroje a služby.

Tento nástroj umožňuje spravovat nejenom virtualizační platformu společnosti Microsoft – Hyper-V, ale umí pracovat i s platformami Citrix XenServer a VMware ESX.

Nástroj umožňuje dále správu síťových zdrojů a datových úložišť pro virtualizační platformu.

Pro správu tohoto nástroje slouží Management server, na kterém je VMM nainstalovaná, a tento server se stará o komunikaci s VMM databází, knihovnou serverů a virtuálními stroji.

4.3.2 System Center App Controller

Tento nástroj umožňuje vytvoření samoobslužné platformy, která umožňuje koncovým uživatelům nasadit a spravovat virtuální stroje a služby v cloudovém prostředí - privátním, veřejném i hostovaném. (Tulloch, 2013a, s. 25)

App Controller provádí rozhraní mezi všemi cloudovými řešeními, tedy privátním cloudu, který je vytvořen pouze pro danou společnost a společnost se o něho stará svépomocí, veřejném cloudu, tedy Windows Azure, a hostovaném cloudu, který je možné vytvořit pomocí balíčku Windows Azure Pack. Díky tomu umožňuje společnosti spravovat zdroje s použitím konzistentní a jednotné praxe a postupů.

System Center App Controller zahrnuje jeden nebo více serverů, webových stránek hostovaných na Internet Information Services (IIS), Microsoft SQL databázi a Microsoft PowerShell modul.

4.3.3 System Center Configuration Manager

Nástroj Configuration Manager (dále jen CM) umožňuje komplexní řešení pro řízení změn a správu konfigurací na úrovni operačních systémů, aplikací a softwarových aktualizací. (Tulloch, 2013a, s. 39)

Dále je pomocí CM možné provádět inventarizaci hardwaru a softwaru, zajistit monitorování a nápravu škod v případě nestandardních nastavení, provádět vzdálenou administraci a správu klientů přes Internet.

CM umí pracovat nejenom s fyzickými zdroji, ale i virtuálními, a to na úrovni serverových operačních systémů nebo i klientských operačních systémů. Pro zajištění správy zařízení je potřeba na něj nainstalovat klienta, který bude komunikovat se serverem, který slouží pro správu klientů.

Mezi zařízení, se kterými CM umí pracovat, patří počítače s Windows nebo i Mac OSX, tablety s Windows, Windows RT, Apple iOS nebo Android a chytré telefony s Windows Phone, Apple iOS nebo Android.

Dále CM podporuje servery Windows, Linux a UNIX systémy. Mezi podporované linuxové distribuce patří Red Hat, SUSE, CentOS, Ubuntu, Debian a Oracle a mezi podporované unixové systémy patří AIX, HP-UX a Solaris, ale pro tyto systémy nenabízí CM stejné možnosti správy jako pro systémy založené na Windows.

4.3.4 System Center Operation Manager

System Center Operation Manager (dále jen OM) slouží pro monitorování prostředí v reálném čase a umí monitorovat stav operačních systémů, služeb, aplikací, zařízení a provoz zařízení a systémů v IT prostředí. (Tulloch, 2013a, s. 67)

Nástroj OM může být využit nejenom ve velkých společnostech, ale i malých, v datacentrech a pro monitoring privátního, veřejného a hostovaného cloudového řešení.

OM umí monitorovat serverové i klientské operační systémy, které běží na platformě Windows a dále i podporované linuxové a unixové operační systémy a virtualizační platformy VMware a Citrix.

Pomocí OM lze monitorovat také zařízení fyzické sítě, kterými jsou směrovače, přepínače, firewally a zařízení starající se o rozdělení zátěže (tzv. load balancery).

4.3.5 System Center Advisor

Nástroj System Center Advisor slouží pro proaktivní monitoring zatížení systémů v prostředí a identifikaci potenciálních problémů v budoucnu. (Tulloch, 2013a, s. 81)

Mezi sledované systémy, které umí Advisor monitorovat, patří Windows Server 2008 a novější, Microsoft Hyper-V Server 2008 R2 a novější a dále je možné sledovat zatížení Microsoft SQL Server, Microsoft Exchange Server, Microsoft Lync server a Microsoft SharePoint.

Samozřejmostí je také správa nástroje System Center 2012 SP1 Virtual Machine Manager.

4.3.6 System Center Data Protection Manager

Data Protection Manager (dále jen DPM) je nástroj pro zálohování a obnovu serverů, virtuálních strojů, Microsoft SQL databází, Microsoft Exchange a Microsoft SharePoint. (Tulloch, 2013a, s. 55)

Server DPM umí zálohovat jak virtuální, tak fyzické stroje, které umí zálohovat na disky, pásky nebo na kombinaci disků a pásek. Také umí data zálohovat na jiný DPM server nebo zálohovat do Windows Azure.

4.3.7 System Center Orchestrator

Tento nástroj slouží pro automatizaci prostředí pomocí předefinovaných a vytvořených pracovních postupů, tzv. workflow. (Tulloch, 2013a, s. 113)

Automatizace prostředí zahrnuje oblasti vytvoření, konfiguraci, správu a monitoring IT systémů, plánování nového hardwaru, softwaru, uživatelských účtů, datových úložišť a dalších zdrojů, se kterými Orchestrator pracuje a dokáže pracovat.

Orchestrator je klíčová komponenta pro vytvoření privátního cloudu pomocí nástrojů z rodiny System Center protože dokáže komplexně propojit akce a procesy, zautomatizovat je pomocí vytvoření plánovaných úloh nebo uživatelských žádostí.

Nástroj Orchestrator pracuje s tzv. runbooky, což jsou logické reprezentace sekvencí aktivit, které vytváří tzv. workflow, což je série akcí, které jsou pomocí Orchestratoru a spuštěním daného runbooku provedeny na cílovém systému, resp. systémech nebo dalších zdrojích.

Pomocí Orchestratoru a integračních balíčků lze ovládat například Active Directory, Microsoft Exchange, Microsoft SharePoint, System Center nebo i Microsoft Windows Azure a další. Dále lze ovládat nejenom systémy společnosti Microsoft, ale i další produkty, mezi které patří IBM Tivoli, HP Operations Manager, HP Service Manager, VMware vSphere, BMC Remedy, CA Service Desk, Cisco UCS, Dell AIM a další.

4.3.8 System Center Service Manager

Nástroj System Center Service Manager (dále jen SM) je integrovaná platforma pro automatizaci, samoobsluhu systémů, standardizaci a jejich dodržování a hlavně je to nástroj pro doručování IT jako služby. (Tulloch, 2013a, s. 99)

System Center Service Manager umožňuje organizaci:

- Automatizaci IT Service Management procesů, jako jsou Incident, Problem, Change management a další,
- vytvoření samoobslužného portálu pro uživatele, který jim umožní zadávání požadavků na IT oddělení,
- standardizování IT Service Management procesů,
- uchovávání a logování každé akce v tomto systému pro pozdější analýzu nebo případně pro proaktivní zlepšování služeb a reporting.

4.3.9 Windows Azure Pack

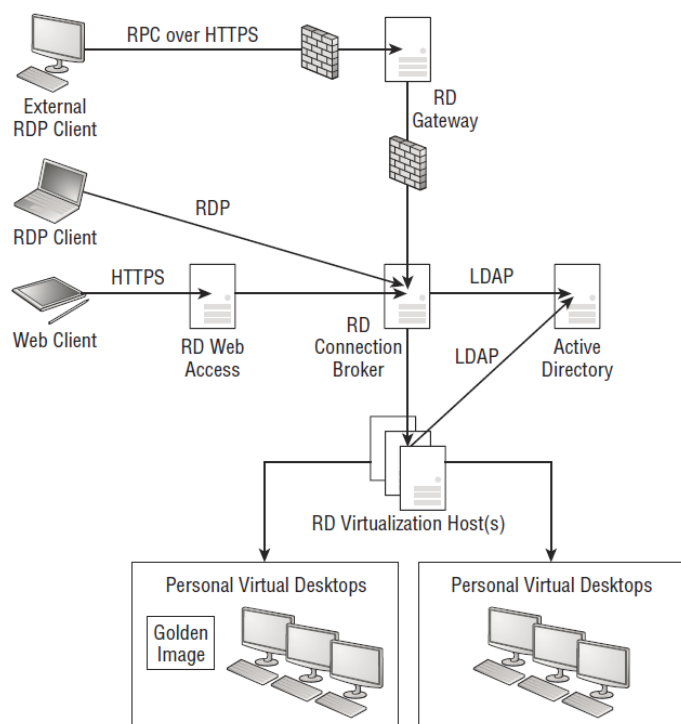
Balíček Windows Azure Pack poskytuje vytvoření privátního nebo hostovaného cloudu, který je podobný a je založen na platformě Windows Azure. (Tulloch, 2013a, s. 127)

Windows Azure Pack zahrnuje především možnost vytvořit privátní cloud se samoobslužnými funkcemi pro poskytování a správu instancí webových služeb, virtuální strojů, rozhraní mezi službami, SQL a MySQL databázemi a další cloudových služeb založených na platformě Windows Azure.

4.4 Další komponenty VDI infrastruktury

Tato kapitola je věnována dalším technologiím a principům, které s infrastrukturou virtuálních desktopů v podání společnosti Microsoft úzce souvisí.

Na následujícím obrázku 5: Architektura VDI řešení je vidět možný návrh základní infrastruktury virtuálních desktopů. Na tomto obrázku je vidět několik komponent, které budou následně v kapitole rozebrány.



Obrázek 5: Architektura VDI řešení, převzato z: Finn at el. (2013, s. 529)

Na obrázku jsou vidět jednotlivé komponenty řešení VDI desktopů, které budou následně představeny v kapitole 4.4.2: Role Remote Desktop Services.

4.4.1 Typy virtuálních desktopů

Na obrázku ve spodní části jsou vidět personální virtuální desktopy, které jedním z typů virtuálních desktopů a scénářů. Těmito scénáři jsou sdružená kolekce virtuálních strojů, osobní kolekce virtuálních strojů a relační virtualizační nasazení. (Finn at el., 2013, s. 522)

Sdružená kolekce

V tomto scénáři všichni uživatelé sdílí jednu hlavní image a změny uživatelů jsou uchovávány na virtuálním disku a po odhlášení uživatele jsou tyto změny smazány.

Výhodou je zde menší čas nutný ke starání se o tuto jednu image, menší nároky na diskové úložiště a levnější cena nasazení.

Osobní kolekce

Tento scénář je založen hlavním virtuálním stroji, kde se následně uživateli vytvoří osobní instance tohoto stroje a následně je tento virtuální stroj v podstatě identický s fyzickým počítačem a všechny změny jsou v něm zachovány.

Relační nasazení

Scénář relačního nasazení je založen na relacích technologie Remote Desktop Services, které jsou známy jako terminálové služby.

Windows Server 2012 nabízí jednodušší způsob vytvoření této architektury integrováním scénáře nasazení.

Porovnání typů VDI scénářů

V následující tabulce 4: Porovnání VDI scénářů je vidět porovnání typů scénářů virtuálních desktopů. Každý z těchto scénářů se hodí v jiných situacích.

	Sdružená kolekce	Osobní kolekce	Relační nasazení
Personalizace	<i>Průměrná</i>	<i>Dobrá</i>	<i>Průměrná</i>
Kompatibilita aplikací	<i>Dobrá</i>	<i>Dobrá</i>	<i>Průměrná</i>
Správa image	<i>Průměrná</i>	<i>Špatná</i>	<i>Dobrá</i>
Cenová efektivnost	<i>Průměrná</i>	<i>Špatná</i>	<i>Dobrá</i>

Tabulka 4: Porovnání VDI scénářů, převzato z: Finn at el. (2013, s. 522)

4.4.2 Role Remote Desktop Services

Technologie Remote Desktop Services, což je role ve Windows Server, nabízí samostatné role pro vzdálené připojení. Finn at el. (2013, s. 525)

Těmito rolemi jsou:

- RD Management Services, která má na starosti správu vzdálených připojení a poskytuje konzoli pro tuto správu,

- RD Connection Broker, která má na starosti připojení VM k uživatelům a jedná se o centrální řešení správy pro RDS scénáře ve Windows Server 2012,
- RD Web Access, která povoluje přistupovat do prostředí virtuálních desktopů a aplikací pomocí webového prohlížeče,
- RD Virtualization Host, která se stará o Hyper-V,
- RD Gateway, která umožňuje se připojit z nespravovaných zařízení přes Internet pomocí protokolu vzdáleného připojení (RDP),
- RD Licensing, která se stará o správu připojení a potřebný počet licencí.

4.4.3 RemoteFX

Technologie RemoteFX nabízí zvýšený grafický výkon přes protokol RDP díky využití speciální grafické karty, která podporuje RemoteFX. (Finn at el., 2013, s. 527)

RemoteFX nabízí využití virtuálního desktopu na podobné úrovni jako je běžný osobní počítač díky 3D virtuálnímu adaptéru, inteligentních kodecích a dostupnosti přesměrování USB zařízení do virtuálního stroje a podporu multidotykového ovládání obrazovky.

4.5 Licencování architektury VDI

Dalším důležitým faktorem pro řešení architektury virtuálních desktopů a náklady na implementaci VDI řešení je samotné licencování řešení a jednotlivých komponent. (Daquas, 2015)

Licencování systému Windows Server bylo představeno v kapitole 4.1.4 Licencování Windows Server 2012 R2 ovšem toto nejsou jediné licence, které je potřeba pořídit.

Licence desktopového operačního systému

Koncová zařízení, ze kterého bude uživatel do prostředí přistupovat, musí být licencovány třemi možnými způsoby:

- Koncovému zařízení je přidělena licence desktopového operačního systému v edici Professional a vyšší včetně Software Assurance.

- Pokud je zařízení bez desktopového OS (tenčí nebo zero klienti), není možné dokoupit Software Assurance pro edici Professional, nejedná se o edici Professional nebo se jedná o nějaké non-Microsoft OS zařízení, tak je potřeba dokoupit licenci Windows VDA (Virtual Desktop Access).
- Nákup služby Windows Intune, která zahrnuje práva na upgrade operačního systému včetně Software Assurance.

Licence desktopových aplikací

Aplikace by měly být pořízeny včetně licencí pro jejich virtualizaci a ideálně pořízeny pomocí multilicenční smlouvy pro uplatnění nároku spuštění třetí kopie na síťovém zařízení.

Dále je vhodné pořídit Software Assurance, který zahrnuje roamingová práva pro přístup z více zařízení.

Licence pro serverovou infrastrukturu

Licencování serverové infrastruktury bylo již zmíněno v souvislosti s Windows Server 2012 R2, ale je potřeba zohlednit licence pro vzdálené připojení (Remote Desktop Services, virtualizaci aplikací App-V, technologie System Center nebo případně Microsoft SQL Server).

Toto licencování lze vyřešit pomocí licence VDI Suite, který se přiděluje koncovému zařízení a zahrnuje potřebné přístupové licence pro VDI infrastrukturu s výjimkou Windows Server CAL). Jedná se ovšem ale o přístupové licence, tedy nejedná se o licence pro balík nástrojů System Center, Microsoft SQL Server 2014 a dalších nástrojů.

4.6 Infrastrukturální a další aplikační systémy

S virtualizací v podání Microsoftu, podnikovou informatikou a IT infrastrukturou souvisí několik dalších základní systémů a nástrojů, které slouží v dalších ohledech IT a obchodní činnosti podniku.

Microsoft SQL Server

System Microsoft SQL Server nabízí možnost vytvoření databázového serveru, který může sloužit jako databáze pro podnikové aplikace, jako databáze pro nástroje System Center nebo jako databáze pro Remote Desktop.

Microsoft Exchange

Produkt Microsoft Exchange slouží především pro elektronickou poštovní komunikaci mezi uživateli uvnitř nebo i mimo společnost, dále pro práci s kalendáři, kontakty a další možnosti, které produkt nabízí.

Microsoft SharePoint

Microsoft SharePoint slouží pro týmovou spolupráci, ukládání dokumentů, sdílení informací, tvorbu intranet a extranet portálů, webových stránek a dalších možností například v ohledu Business Intelligence.

Microsoft Lync Server

Produkt Microsoft Lync slouží pro komunikaci v reálném čase, tedy pro zasílání zpráv a především telefonování, buď v rámci společnosti, nebo je možné telefonovat mimo společnost a na pevné telefonní linky.

Windows ADK

Windows Assessment and Deployment Kit je sada nástrojů pro nasazení operačních systémů Microsoft Windows. (Stanek, 2012, s. 8) Mezi tyto nástroje patří:

- Application Compatibility Toolkit (ACT) pro otestování kompatibility aplikací,
- nástroje pro nasazení a správu image Windows,
- User State Migration Tool (USMT) pro migraci stavu uživatelů,
- Volume Activation Management Tool (VAMT) pro hromadnou aktivaci,
- Windows Assessment Services pro vzdálenou inventarizaci SW a HW,
- Windows Assessment Toolkit pro analýzu a simulaci zatížení aktivity uživatele,
- Windows Performance Toolkit (WPT), což jsou nástroje pro monitorování zatížení systémů a aplikací,

- Windows Preinstallation Environment (Windows PE), což je minimalistický základní operační systém, který je vytvořen pro přípravu počítače během instalace OS.

Microsoft Deployment Toolkit

Microsoft Deployment Toolkit je bezplatný nástroj, který umožňuje a poskytuje nástroje pro nasazení operačních systémů Windows.

Tento nástroj umožňuje v kombinaci s rolí Windows Deployment Services ve Windows Serveru nebo System Center Configuration Manager vytvořit automatizovanou instalaci operačních systémů.

Microsoft Desktop Optimization Pack

Microsoft Desktop Optimization Pack je balík nástrojů pro správu operačního systému Windows a zahrnuje:

- Microsoft Diagnostics and Recovery Toolset (DaRT), což jsou nástroje pro opravu systému,
- Microsoft Advanced Group Policy Management pro rozšířené možnosti správy skupinových politik,
- Microsoft BitLocker Administration and Monitoring pro monitorování a správu technologie BitLocker,
- Microsoft Application Virtualization (App-V) pro virtualizaci aplikací,
- Microsoft Enterprise Desktop Virtualization (MED-V) pro rozšířenou virtualizaci na desktopu,
- User Experience Virtualization (UE-V) pro virtualizaci uživatelských profilů pro přenos mezi několika rozdílnými zařízeními.

Licence MDOP je možné pořídit v rámci Software Assurance s pořízením operačního systému Windows.

5 Návrh řešení pro středně velkou společnost

Tato kapitola zahrnuje návrh a technologické řešení virtualizované architektury pro fiktivní firmu, která vznikla především pro definování aplikačních a funkčních požadavků na budoucí infrastrukturu.

V této kapitole je nejdříve tato společnost popsána a požadavky definovány, dále byl popsán návrh fyzické infrastruktury, která zahrnuje virtualizační vrstvu a úložiště, dále návrh logické infrastruktury, která obsahuje všechny infrastrukturní virtualizované servery, dále byl navrhnout postup implementace a přechodu na virtualizované desktopy a tato implementace detailně popsána. Nakonec byla provedena analýza řešení a popsány možnosti dalšího rozvoje a škálovatelnosti řešení.

5.1 Návrh postupu implementace

Samotný návrh postupu implementace by měl vycházet především z analýzy prostředí a potřeb zdrojů pro infrastrukturu provozních serverů a pro infrastrukturu virtuálních desktopů.

Postup návrhu implementace a vytvoření služby virtuálních desktopů by mělo zahrnovat několik základních kroků, které jsou nezbytné pro funkční a správný návrh a implementaci služby virtuálních desktopů a souvisejících infrastrukturálních změn, které daná technologie do fungování podniku a IT infrastruktury přinese. Těmito základní kroky jsou:

1. Analýza prostředí a požadavků na službu virtuálních desktopů, která je v této práci v základním konceptu zahrnuta především v kapitole 5.2 Analýza prostředí a požadavků.
2. Návrh infrastruktury a technologie tak, aby služba virtuálních desktopů plnila přesně to, co uživatel požaduje. Této části je věnována především kapitola 5.3 Návrh infrastruktury.
3. Dalším krokem by měla být pilotní fáze implementace řešení, kdy dojde k základnímu otestování návrhu řešení. Tato problematika je popsána

především v kapitolách 5.4 a 5.5, které se věnují detailnímu popisu technologické implementaci v pilotní fázi.

4. Funkční testování testovacího řešení, kdy dojde především k otestování základních funkcionalit řešení, otestování potřebných aplikací a případné připomínkování pro další fáze. Z tohoto bodu může dojít k akceptaci řešení nebo jeho přepracování.
5. V případě akceptace řešení by mělo dojít k implementaci infrastruktury, které může být řešeno kompletní implementací, kdy by celá infrastruktura byla postavena a implementována najednou, nebo případně po částech, kdy by byly jednotlivé části postupně vertikálně implementovány¹, nebo implementací plně funkční, ale omezené infrastruktury a jejím postupným horizontálním rozšiřováním².
6. Nakonec by mělo dojít ke zhodnocení celého projektu a navrhnutí dalšího možného budoucího rozšíření implementace. Této části se věnuje částečně kapitola 5.6 Škálovatelnost a další možný rozvoj. Dále případně může být navrhnutá analýza pravidelné údržby řešení a jeho průběžné hodnocení, což ale je spíše otázkou provozu infrastruktury virtuálních desktopů

V každém kroku řešení by měla být také uvažována rizika a jejich analyzování, další nové informace, které se objeví během dané fáze projektu, technická dokumentace řešení a především sledování rozpočtového hlediska, finanční a funkční analýza.

Hlavním výstupem této analýzy by tedy mělo být zjištění, jestli za cenu jaká byla předpokládána, společnost dostala funkcionalitu, kterou očekávala.

Technická dokumentace řešení by měla zahrnovat především základní nastavení a atributy všech částí infrastruktury a průběžně by měla být aktualizována v případě změn nebo tyto změny by měly být řízeny například pomocí procesu řízení změn. Tato

¹ Vertikální implementací je myšleno vystavení infrastruktury postupně od nejnižších částí, tedy například v prvotní fázi vybudování fyzické infrastruktury virtuálních desktopů (např. úložiště dat, virtualizační platforma, základní infrastrukturální služby a další) a dále vybudování dalších rozšiřujících řešení implementace (např. dohled a automatizovaná správa infrastruktury a řešení, možnost vzdáleného připojení se i z Internetu, a dalších).

² Horizontální implementace znamená vytvoření funkčního, ale omezeného a škálovatelného řešení (např. menší počet virtualizačních serverů, menší kapacita úložiště a další), které sice omezí možnost nabídnout službu virtuálních desktopů omezenému počtu uživatelů, ale zajistí průběžné dotestování funkcionality a případné rozdělení prvotní investice do několika období.

dokumentace by měla zahrnovat dále běžné provozní postupy, které zajistí běžný chod infrastruktury a případné řešení a odstraňování potíží.

5.2 Analýza prostředí a požadavků

Pro návrh řešení byla vytvořena fiktivní společnost, která má klasické požadavky na aplikace a funkce, které nabídne navrhované technologické řešení virtuálních desktopů a dalších nástrojů.

Před započítáním projektu všichni uživatelé vlastní standardní desktopový počítač a část uživatelů pracuje z notebooku (cca 20% z celkového počtu zaměstnanců).

5.2.1 Popis společnosti

Společnost se zabývá finančními službami, takže většina zaměstnanců vykonává převážně kancelářskou činnost a tudíž k ní potřebují standardní kancelářské nástroje, mezi které patří Word, Excel, PowerPoint a Outlook a další nástroje z balíku Microsoft Office.

Počet zaměstnanců ve společnosti je 200 a všichni tito zaměstnanci potřebují k práci standardní balík nástrojů pro kancelářskou činnost a komunikaci napříč společností a mimo společnost s externími partnery.

Samotné IT oddělení, které se stará o podporu uživatelů, se skládá ze 4 pracovníků, kteří jsou pracovníky kontaktního centra IT (helpdesk), a ze 4 administrátorů, kteří se zabývají infrastrukturou IT prostředí společnosti.

Základní náplň práce pracovníků kontaktního centra IT je:

- Základní podpora uživatelů,
- řešení nefunkčnosti pracovních stanic uživatelů,
- řešení problémů s nefunkčními aplikacemi,
- konzultace uživatelům,
- řešení ostatních nefunkčních periférií (tiskárny, skenery a další),
- kontaktní místo první úrovně podpory pro řešení incidentů.

Základní náplň práce IT administrátorů je:

- Rozšířená podpora uživatelů na druhé úrovni,
- řešení nefunkčnosti infrastrukturálních aplikací a systémů,
- analýza provozu infrastruktury,
- změny a optimalizace infrastruktury,
- druhá úroveň podpory pro řešení incidentů.

5.2.2 Aplikační požadavky

Mezi standardní aplikační vybavení pracovníka patří operační systém Windows a balík Microsoft Office Standard a dále komunikační nástroj, například Microsoft Lync.

Antivirový program by měl být používán například Windows Defender, který je integrován ve Windows 8.1.

Jako podporovaný webový prohlížeč bude použit Internet Explorer, který je také integrován ve Windows 8.1, čímž se zajistí vývoj a optimalizace webových aplikací pro tento prohlížeč napříč celým podnikem.

Toto je základní popis standardu, který budou mít dostupní všichni uživatelé, ale další aplikace mohou být poskytnuty na vyžádání v případě potřeby.

Dále by uživatelé měli mít přístup do dalších aplikací pomocí klienta, kterým je například SAP Front End pro připojení k systémům SAP.

Do dalších systémů by měly být přístupové aplikace primárně řešeny pomocí tzv. tenkých klientů, což jsou aplikace, které se neinstalují, ale slouží k připojení do pokročilých systémů, takže bez nutnosti instalace složitých aplikací (tzv. prezentační virtualizace).

5.2.3 Funkční požadavky

Uživatelé by měli mít možnost pracovat kdykoliv v běžný pracovní den v prostředí, ve kterém mají všechny potřebné nástroje pro svou pracovní činnost, tedy především přístup k aplikacím, přístup k firemním, osobním, ale i pracovním datům.

Dále by návrh měl respektovat požadavky v kontinuitě podnikání, a tudíž by měl být odolný vůči hardwarovým a softwarovým chybám a měla by být možnost obnovení většiny součástí v co nejkratší době.

Někteří uživatelé by měli mít přístup ke svým pracovním desktopům skrz Internet pomocí webového prohlížeče.

Základními možnostmi, jak se připojit k virtuálnímu desktopu by měly být:

- Pomocí zero nebo tenkého klienta (pro možnosti tenkého klienta lze případně využít stávající počítače),
- přes webový portál,
- pomocí protokolu pro vzdálenou plochu z jakéhokoliv jiného počítače v síti, tedy pracovních notebooků.

Všechny systémy a nástroje by měly být používány v nejnovějších verzích, což znamená Windows 8.1, Windows Server 2012 R2, Hyper-V Server 2012 R2, nástroje z rodiny System Center ve verzích 2012 R2, databázový systém Microsoft SQL Server 2014 a dalších nástrojů a systémů.

Dále se předpokládá, že virtualizační vrstva nebude sloužit pouze virtuálním desktopům, ale celé infrastrukturu a fyzické servery se omezí pouze na servery, které slouží jako hostitelé pro virtuální servery.

Celá infrastruktura by měla být centrálně řízena a spravována pomocí pokročilých nástrojů pro centralizovanou správu, tedy Systém Center Configuration Manager nebo System Center Virtual Machines Manager a dalších.

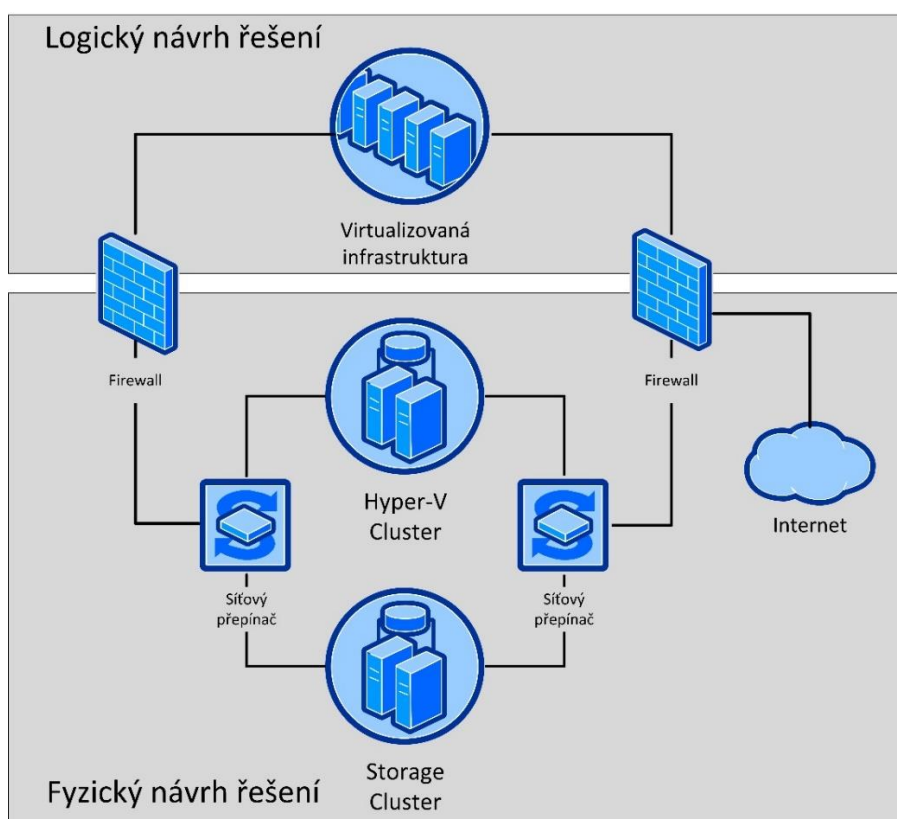
5.3 Návrh infrastruktury

Samotný návrh infrastruktury je rozdělen na 2 části, které budou vzájemně oddělené – fyzický a logický návrh řešení.

Fyzický návrh řešení obsahuje vrstvu úložiště dat a virtualizační vrstvu, tedy sadu hypervizorů, které budou nabízet zdroje logické vrstvě. Jedná se tedy o množinu fyzických serverů, které nabízí možnost škálovatelnosti, která poskytuje možnost dalšího rozšíření v případě nutnosti rozšířit výpočetní zdroje infrastruktury.

Oproti tomu logický návrh, představuje virtualizované servery, které zajišťují infrastrukturu počítačové sítě. Tato vrstva bude kompletně virtualizovaná a bude využívat zdroje fyzické vrstvy a zároveň poskytovat své zdroje uživatelům a ostatním virtuálním serverům.

Návrh infrastruktury je vidět na následujícím obrázku 6: Celkový návrh řešení.



Obrázek 6: Celkový návrh řešení (zdroj: autor)

Na předchozím obrázku návrhu řešení je několik součástí, které jsou pro infrastrukturu důležité. Těmito součástmi jsou:

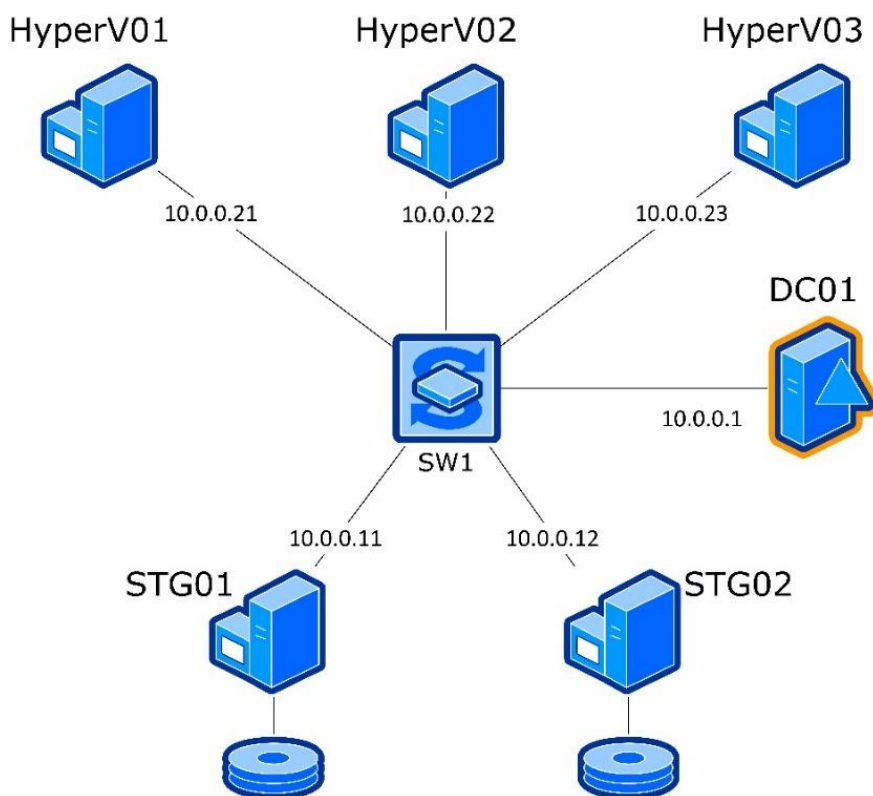
- Storage cluster – vysoce dostupné řešení ukládání dat,
- Hyper-V cluster – vysoce dostupné řešení virtualizační platformy Hyper-V,
- Virtualizovaná infrastruktura – množina virtualizovaných serverů,
- Síťový přepínač – vysoce dostupné řešení síťového propojení mezi Hyper-V a Storage clusterem,
- Firewall – zajišťující oddělení provozu fyzické (virtualizační) a logické (virtualizované) vrstvy,

- Internet – reprezentuje připojení infrastruktury do veřejného Internetu a také připojení k dalším veřejně poskytovaným informačním službám.

5.3.1 Fyzický návrh řešení

Fyzický návrh řešení obsahuje 3 základní komponenty – infrastrukturní server, souborové úložiště a množinu serverů, na kterých běží hypervizor, tedy virtualizační platforma Hyper-V.

Na následujícím obrázku 7: Návrh zapojení fyzické vrstvy je vidět fyzický návrh řešení, které bude použito pro testování základní funkcionality řešení na podmnožině virtuálních strojů, tedy virtuálních serverů a virtuálních desktopů.



Obrázek 7: Návrh zapojení fyzické vrstvy (zdroj: autor)

Tento náčrt a jeho implementace umožní otestovat základní funkce řešení a díky své škálovatelnosti bude možné tuto strukturu dále rozšířit pro potřebný počet virtuálních strojů.

Na obrázku jsou vidět dva servery, pojmenované jako STG01 a STG02, které budou sloužit hlavně jako úložiště dat pro virtualizované stroje, jejichž instance poběží na serverech ve virtualizačních platformě Hyper-V.

Virtualizační platforma je na obrázku zastoupena třemi servery, které jsou pojmenované jako HyperV01, HyperV02 a HyperV03.

Dále bylo potřeba vytvořit doménu, která bude na serveru, který není umístěn v žádném clusteru, takže bylo nutné do infrastruktury přidat ještě server DC01, který bude mít roli doménového řadiče a DNS serveru.

Všechny servery jsou připojeny pomocí virtuálního přepínače SW1 v jedné síti, která je tvořena IP rozsahem 10.0.0.0/24 a jsou připojeny v jedné doméně HyperV.local.

Datové úložiště

Úložiště poskytuje především prostor pro data virtuálních strojů a data uživatelů.

Na obrázku 7 je úložiště tvořeno servery STG01 a STG02, které mají oba 4 disky – jeden pro systém a další tři pro data virtuálních strojů.

Z těchto tří disků je vytvořen jeden disk v RAID5 a dále je z tohoto disku pomocí sdílení vytvořen síťový prostor pro možnost uložení dat přes síť.

Oba servery jsou v clusteru z důvodu zajištění vysoké dostupnosti.

Virtualizační platforma Hyper-V

Virtualizační platforma Hyper-V slouží pro virtualizaci virtualizovaných strojů a na obrázku 7 je tvořena tato vrstva servery HyperV01, HyperV02 a HyperV03.

V návrhu pro testovací fázi je počítáno s třemi hypervizory, nicméně toto řešení je díky škálovatelnosti možné rozšířit podle potřeb výpočetního výkonu.

Mezi těmito servery by mělo být možné přesouvat virtuální stroje a dále by měla být popsána implementace Hyper-V repliky pro možnost přepnutí virtualizovaného systému na jiný hypervizor.

Infrastrukturní služby

Jak již bylo zmíněno, bylo potřeba vytvořit doménu pro vytvoření clusteru, takže byl do infrastruktury přidán server, který se bude starat o infrastrukturní služby.

Tento server byl pojmenován DC01, bude mít pouze jeden systémový disk a bude na něm nainstalována role Active Directory Domain Services a role DNS serveru.

5.3.2 Logický návrh řešení

Logický návrh, tedy virtualizované servery a celou infrastrukturu, která nabízí zdroje a služby uživatelům zahrnuje především následující servery a role:

- Doménový řadič,
- DNS server, pro překlad jmen,
- DHCP server, pro dynamické přidělování IP adres,
- SQL server, pro databáze,
- System Center Virtual Machine Manager,
- System Center Configuration Manager.

Další systémy, kterými jsou například Microsoft Exchange, Microsoft SharePoint, ostatní nástroje z rodiny System Center a další nejsou v návrhu uvažovány, protože přímo nesouvisí s virtuálními desktope, nicméně tyto systémy je možné implementovat.

Samotná implementace těchto systémů do infrastruktury by byla provedena vytvořením virtuálních strojů s požadovanými parametry ve fyzickém návrhu v hypervizoru, instalací potřebných součástí těchto nástrojů a případně další konfigurací s nimi související.

Samozřejmou nutností v logickém návrhu je přítomnost hypervizoru pro instance virtuálních desktopů. Pro testovací fázi bude využit jeden virtualizační hostitel v logickém návrhu řešení, ale v reálném návrhu by tento virtualizační hostitel měl být součástí fyzického návrhu řešení, které bude nabízet fyzické zdroje nejenom virtuálním serverům v infrastruktuře, ale i virtuálním desktope.

Toto samé platí i pro úložiště pro data virtuálních desktopů a uživatelů. V testovací fázi bude úložiště dat implementováno připojením jednoho virtuálního souborového úložiště k jednomu ze serverů a jeho síťové sdílení.

5.4 Detailní popis technologické implementace pilotní fáze – fyzický návrh řešení

Konfigurace fyzického návrhu řešení pro pilotní fázi projektu zahrnuje konfiguraci a instalaci šesti serverů – serveru DC01 pro infrastrukturní služby, serverů STG01 a STG02, které zajišťují vysoce dostupné souborové úložiště pro ukládání virtualizovaných serverů, a serverů HyperV01, HyperV02 a HyperV03, které zajišťují virtualizační infrastrukturu pro virtualizované systémy.

Postup byl implementován na omezené možnosti výpočetních zdrojů, které nabízí notebook s procesorem Intel Core i7-4700MQ (4 jádra o frekvenci 2,4 GHz), 12 GB operační paměti a 2 disky – jeden primární integrovaný 500 GB a externí USB 3.0 disk s kapacitou 500 GB.

5.4.1 Konfigurace serveru DC01

Server DC01 slouží jako doménový řadič pro snadnější správu ostatních serverů a je na nich instalována role DNS serveru pro překlad doménových jmen.

Jedná se o doménu HyperV.local, která slouží pouze pro fyzickou vrstvu.

Hardwarová konfigurace serveru DC01

V následující tabulce 5: Konfigurace serveru DC01 je vidět hardwarová konfigurace virtuálního stroje pro server DC01.

Hardware	Server DC01
Název VM	DC01
Operační paměť	1024 MB
Procesor	Virtuální procesor: 1
Řadič SCSI - pevný disk	DC01_C.vhdx (velikost 25 GB)
Síťový adaptér	SW1
Doinstalované role ³	Active Directory Domain Services DNS server
Doinstalované nástroje	Failover Clustering Hyper-V Management Tools

Tabulka 5: Konfigurace serveru DC01

Jak je vidět v tabulce, tak server má pouze jeden disk, který je určen pro operační systém Windows Server 2012 R2 Datacenter.

Systémová konfigurace serveru DC01

Po nainstalování operačního systému bylo změněno heslo lokálního administrátora na *Password1* a dále byla provedena základní konfigurace operačního systému, tedy:

1. Přejmenování názvu serveru z příkazové řádky:
 - `netdom renamecomputer %COMPUTERNAME% /NewName:DC01`
2. Zjištění ID síťové karty pro následující nastavení statické IP adresy:
 - `netsh interface ipv4 show interfaces`
3. Nastavení statické parametrů síťové karty adresy z příkazové řádky:
 - `netsh interface ipv4 set address name="12" source=static
address=10.0.0.1 mask=255.255.255.0 gateway=10.0.0.1`
4. Po tomto základním nastavení serveru je potřeba restartovat server například z příkazové řádky pomocí:
 - `shutdown /r /t 0`
5. Instalace role Active Directory Domain Services a role DNS Server včetně potřebných nástrojů pomocí průvodce, který je dostupný z konzole Server Manager, která slouží pro základní správu serveru.

³ Server obsahuje i role a nástroje, které jsou standardně obsaženy již po instalaci (např. File Services).

6. Konfigurace role Active Directory Domain Services, buď pomocí průvodce pro povýšení serveru na doménový řadič nebo pomocí PowerShell příkazů:
 - *Import-Module ADDSDeployment*
 - *Install-ADDSForest -CreateDnsDelegation:\$false -DatabasePath "C:\Windows\NTDS" -DomainMode "Win2012R2" -DomainName "HyperV.local" -DomainNetbiosName "HYPERV" -ForestMode "Win2012R2" -InstallDns:\$true -LogPath "C:\Windows\NTDS" -NoRebootOnCompletion:\$false -SysvolPath "C:\Windows\SYSVOL" -Force:\$true*
 - Během druhého příkazu je uživatel požádán o zadání hesla pro obnovu domény a po dokončení příkazu se stroj restartuje.
7. Nastavení primárního DNS serveru z příkazové řádky:
 - *netsh interface ipv4 add dnsserver name="12" address=10.0.0.1 index=1*

Díky těmto příkazům je nyní server nainstalován a připraven k základnímu použití a je tedy možné vytvořit vrstvu úložiště dat a virtualizační vrstvu.

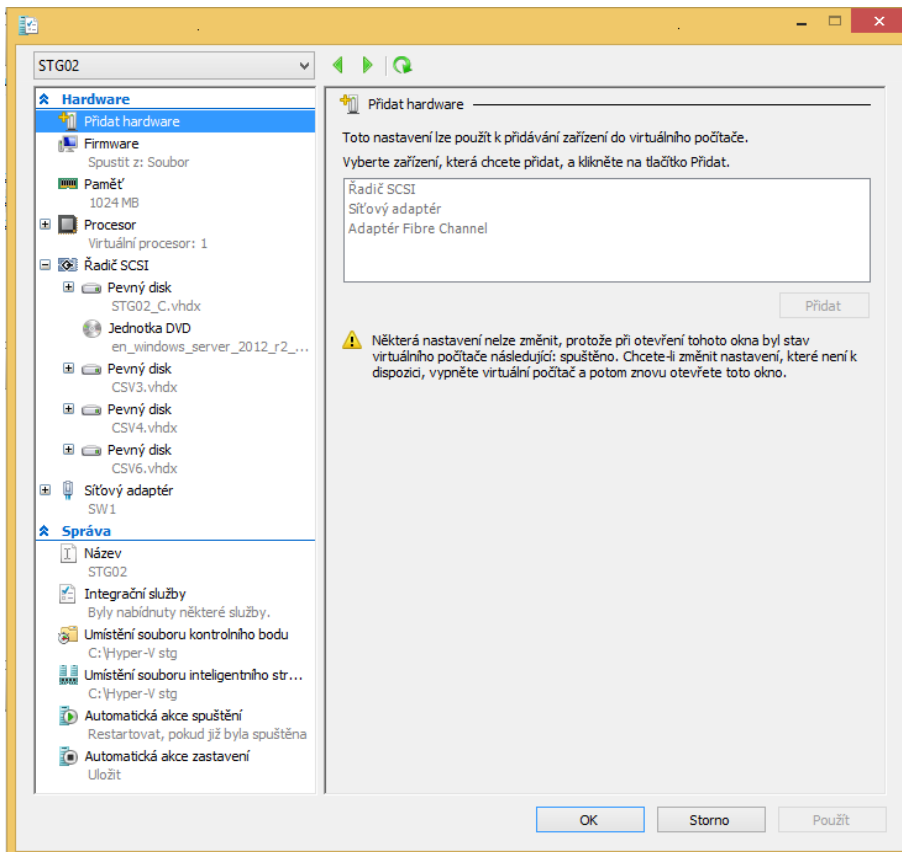
5.4.2 Konfigurace serverů STG01 a STG02

Servery ST01 a ST02 poskytují především síťové souborové úložiště, které poskytuje prostor pro ukládání virtualizovaných serverů, které běží na virtualizační infrastruktuře serverů HyperV01, HyperV02 a HyperV03.

Aby bylo možné oba tyto servery doinstalovat a nastavit, tak je potřeba, aby byl před připojením do domény již nainstalován server DC01 a doména funkční.

Hardwarová konfigurace serverů STG01 a STG02

Na následujícím obrázku 8: Nastavení virtuálního stroje pro server STG02 je vidět konfigurace virtuálního stroje STG02 v testovacím prostředí na platformě Hyper-V a v následující tabulce 6: Konfigurace STG01 a STG02 je vidět souhrn parametrů obou virtuálních strojů pro úložiště dat.



Obrázek 8: Nastavení virtuálního stroje pro server STG02 (zdroj: autor)

Hardware	Server STG01	Server STG02
Název VM	STG01	STG02
Operační paměť	1024 MB	1024 MB
Procesor	Virtuální procesor: 1	Virtuální procesor: 1
Řadič SCSI – pevný disk	STG01_C.vhdx (velikost 25 GB)	STG02_C.vhdx (velikost 25 GB)
Řadič SCSI – pevný disk	STG01_E.vhdx (velikost 100 GB) STG01_F.vhdx (velikost 100 GB) STG01_G.vhdx (velikost 100 GB)	STG02_E.vhdx (velikost 100 GB) STG02_F.vhdx (velikost 100 GB) STG02_G.vhdx (velikost 100 GB)
Síťový adaptér	SW1	SW1
Doinstalované nástroje	Failover Clustering	Failover Clustering

Tabulka 6: Konfigurace serverů STG01 a STG02

Další konfigurace fyzických zdrojů nejsou na virtuálních strojích v testovacím prostředí nastaveny.

Systémová konfigurace serveru STG01

Jelikož jsou pro servery STG01 a STG02 použity v podstatě identické příkazy jako pro server DC01, tak nebudou jednotlivé kroky jejich konfigurace dále blíže popisovány a popis všech příkazů je uveden v části věnované konfiguraci serveru DC01.

Postup pro systémovou konfiguraci serveru STG01 je následující:

1. netdom renamecomputer %COMPUTERNAME% /NewName:STG01
2. netsh interface ipv4 show interfaces
3. netsh interface ipv4 set address name="12" source=static address=10.0.0.11
mask=255.255.255.0 gateway=10.0.0.1
4. Instalace nástroje Failover Clustering včetně všech potřebných nástrojů.
5. netsh interface ipv4 add dnsserver name="12" address=10.0.0.1 index=1
6. shutdown /r /t 0
7. netdom join %COMPUTERNAME% /domain:HyperV.local
/userd:Administrator /passwordd:*
8. shutdown /r /t 0
9. Vytvoření RAID5 disku ze tří sekundárních disků a jeho síťové sdílení.

Systémová konfigurace serveru STG02

Dále příkazy pro systémovou konfiguraci serveru STG02 jsou následující:

1. netdom renamecomputer %COMPUTERNAME% /NewName:STG02
2. netsh interface ipv4 show interfaces
3. netsh interface ipv4 set address name="12" source=static address=10.0.0.12
mask=255.255.255.0 gateway=10.0.0.1
4. Instalace nástroje Failover Clustering včetně všech potřebných nástrojů.
5. netsh interface ipv4 add dnsserver name="12" address=10.0.0.1 index=1
6. shutdown /r /t 0
7. netdom join %COMPUTERNAME% /domain:HyperV.local
/userd:Administrator /passwordd:*

8. shutdown /r /t 0
9. Vytvoření RAID5 disku ze tří sekundárních disků a jeho síťové sdílení.

Vytvoření clusteru pro servery STG01 a STG02

Pro vysokou dostupnost úložiště mezi servery STG01 a STG02 je potřeba vytvořit cluster pro tyto servery.

Cluster se vytváří z konzole Failover Cluster Manager, kde se spustí průvodce pro validaci vybraných členů v clusteru. V případě validní konfigurace je možné dále pokračovat vytvořením clusteru pomocí průvodce, pomocí kterého se tento cluster nakonfiguruje.

Během průvodce je potřeba nejdříve vybrat servery, které mají být v clusteru, zvolit jestli je vyžadována podpora od společnosti Microsoft pro tento cluster (zvoleno, že není vyžadována), název clusteru (zvoleno FSCLUSTER) a jeho IP adresu (10.0.0.10).

Dále byl v clusteru vytvořen vysoce dostupný souborový prostor Cluster Shared Volumes, který je dostupný v síti pod cestou \\FSCLUSTER\VM a je tvořen z disků pro data virtuálních strojů, které jsou připojeny k serverům STG01 a STG02.

Tímto řešením se docílí vysoké dostupnosti, která ochrání od pádu virtualizované servery, které dokáží být odolné chybě jednoho ze serverů STG01 nebo STG02 nebo výpadku jednoho z disků.

5.4.3 Konfigurace serverů HyperV01, HyperV02 a HyperV03

Servery HyperV01, HyperV02 a HyperV03 jsou identické, liší se pouze názvem a přiřazenou IP adresou.

Všechny 3 servery jsou založeny na edici Microsoft Hyper-V® Server 2012 R2.

Hardwarová konfigurace

V následující tabulce 7: Konfigurace serverů HyperV01, HyperV02 a HyperV03 je vidět hardwarová konfigurace serverů virtualizační platformy Hyper-V.

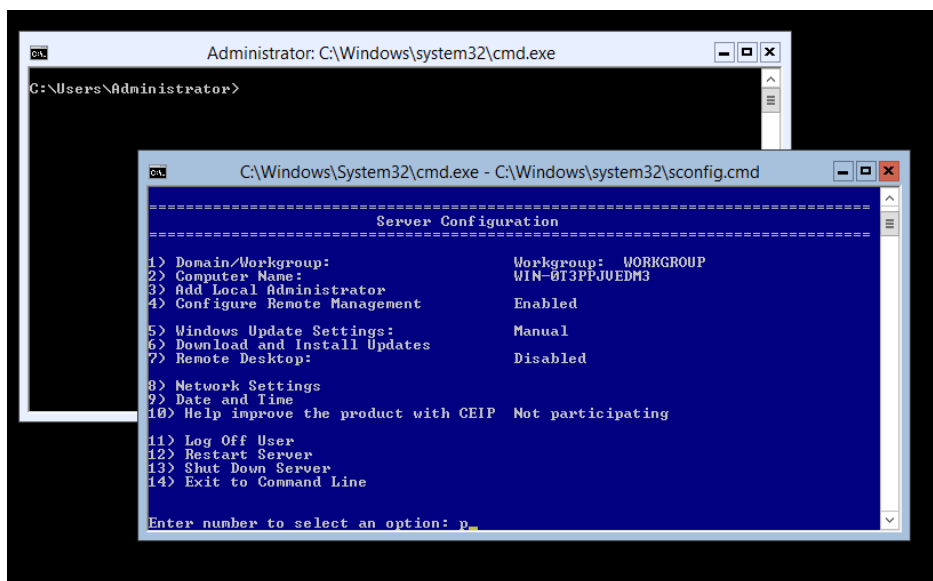
Hardware	Server HyperV01	Server HyperV02	Server HyperV03
Název VM	HyperV01	HyperV02	HyperV03
Operační paměť	2048 MB	2048 MB	2048 MB
Procesor	Virtuální procesor: 1	Virtuální procesor: 1	Virtuální procesor: 1
Řadič SCSI – pevný disk	HyperV01.vhdx (velikost 20 GB)	HyperV02.vhdx (velikost 20 GB)	HyperV02.vhdx (velikost 20 GB)
Řadič SCSI – jednotka DVD	ISO soubor instalace	ISO soubor instalace	ISO soubor instalace
Síťový adaptér	SW1	SW1	SW1
Další nástroje	Failover Clustering	Failover Clustering	Failover Clustering

Tabulka 7: Konfigurace serverů HyperV01, HyperV02 a HyperV03

Systémová konfigurace serveru HyperV01

Všechny virtualizační servery mají nainstalovaný systém Microsoft Hyper-V® Server 2012 R2, který je dostupný zdarma a nepodléhá žádnému licencování.

Po instalaci systému a změně hesla naběhne v tomto systému rozhraní pro základní změnu nastavení serveru sconfig.cmd a okno příkazové řádky. Tato obě okna jsou vidět na obrázku 9: Microsoft Hyper-V® Server 2012 R2.



Obrázek 9: Microsoft Hyper-V® Server 2012 R2 (zdroj: autor)

V konfiguračním dialogu sconfig.cmd se naviguje pomocí zadávání čísel, která odpovídají volbám pro změnu a správu tohoto serveru. Pro konfiguraci ale bylo použito příkazů, které byly představeny v jedné z předchozích kapitol, která se věnuje konfiguraci serveru DC01, tedy:

1. netdom renamecomputer %COMPUTERNAME% /NewName:HyperV01
2. netsh interface ipv4 show interfaces
3. netsh interface ipv4 set address name="13" source=static address=10.0.0.21
mask=255.255.255.0 gateway=10.0.0.1
4. Instalace nástroje Failover Clustering včetně všech potřebných nástrojů.
5. netsh interface ipv4 add dnsserver name="13" address=10.0.0.1 index=1
6. shutdown /r /t 0
7. netdom join %COMPUTERNAME% /domain:HyperV.local
/userd:Administrator /passwordd:*
8. shutdown /r /t 0

Pro další správu serverů HyperV1, HyperV2 a HyperV03, tedy platformy Hyper-V, bude využita konzole Hyper-V Manager, která je nainstalovaná na serveru DC01.

Systemová konfigurace serveru HyperV02

Pro nastavení systému serveru HyperV02 jsou příkazy následující:

1. netdom renamecomputer %COMPUTERNAME% /NewName:HyperV02
2. netsh interface ipv4 show interfaces
3. netsh interface ipv4 set address name="13" source=static address=10.0.0.22
mask=255.255.255.0 gateway=10.0.0.1
4. Instalace nástroje Failover Clustering včetně všech potřebných nástrojů.
5. netsh interface ipv4 add dnsserver name="13" address=10.0.0.1 index=1
6. shutdown /r /t 0
7. netdom join %COMPUTERNAME% /domain:HyperV.local
/userd:Administrator /passwordd:*
8. shutdown /r /t 0

Systémová konfigurace serveru HyperV03

Základní nastavení serveru HyperV03 se provede těmito příkazy:

1. `netdom renamecomputer %COMPUTERNAME% /NewName:HyperV03`
2. `netsh interface ipv4 show interfaces`
3. `netsh interface ipv4 set address name="13" source=static address=10.0.0.23
mask=255.255.255.0 gateway=10.0.0.1`
4. Instalace nástroje Failover Clustering včetně všech potřebných nástrojů.
5. `netsh interface ipv4 add dnsserver name="13" address=10.0.0.1 index=1`
6. `shutdown /r /t 0`
7. `netdom join %COMPUTERNAME% /domain:HyperV.local
/userd:Administrator /passwordd:*`
8. `shutdown /r /t 0`

Vytvoření clusteru pro servery HyperV01, HyperV02 a HyperV03

Následně byl vytvořen cluster pro servery, kde běží Hyper-V.

Tento cluster byl pojmenován HV a adresa mu byla přidělena 10.0.0.20 a poté na něm byla vytvořena role Hyper-V Replica Broker, která povoluje vytvořit vysoce dostupné virtualizační řešení, které umožňuje replikaci mezi Hyper-V hostiteli.

Tento broker byl pojmenován BROKER a adresa mu byla přidělena 10.0.0.2.

Nakonec je potřeba povolit replikaci, což se provede v konzoli Failover Cluster Manager pro daný cluster, tedy HV.HyperV.local a roli BROKER, kde se v nastavení vybere položka Replication Settings.

Následně se spustí Hyper-V Replica Broker Configuration dialog, kde se povolí replikace v clusteru, zadá se typ ověření (pomocí Kerberos nebo certifikátu) a autorizuje se datové úložiště, které bude použito pro replikaci a ukládání replikačních souborů, tedy již vytvořené síťové úložiště \\FSCUSTER\VM.

5.5 Detailní popis technologické implementace pilotní fáze – logický návrh řešení

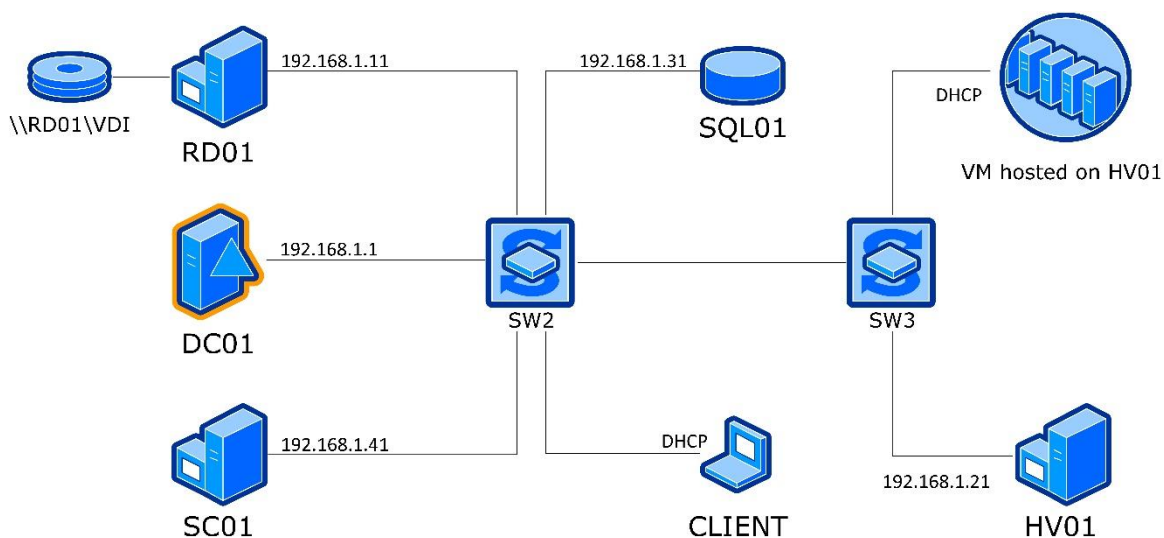
Konfigurace logického návrhu řešení pro pilotní fázi projektu obsahuje instalaci několika serverů, přípravu prostředí, instalaci klientského operačního systému pro otestování funkčnosti

Postup a počet serverů byl dimenzován na fyzické možnosti zařízení pro testování, které bylo popsáno na začátku kapitoly 5.4, tedy standardního notebooku s procesorem se čtyřmi jádry a 12 GB RAM.

Pro testování logického návrhu řešení byla vytvořena počítačová infrastruktura, která tvoří doménu CORP.local a využívá IP rozsahu sítě 192.168.1.0/24, která je tvořena rozsahem 192.168.1.1 - 192.168.1.99 pro statické přidělování a adresním rozsahem 192.168.1.100 - 192.168.1.254 pro dynamické přidělování protokolem DHCP.

Dále byl využit jeden fyzický stroj, který v logickém návrhu reprezentuje hypervizor, protože nelze využít pro virtuální desktopy Hyper-V, které je virtualizované v jiném Hyper-V.

Serverové zapojení pro testovací fázi logického návrhu řešení infrastruktury je vidět na obrázku 10: Návrh zapojení logické vrstvy, kde jsou vidět všechny zapojené servery a jeden klient pro testování připojení.



Obrázek 10: Návrh zapojení logické vrstvy (zdroj: autor)

Na obrázku je vidět i farma serverů VM hosted on HV01, které jsou fyzicky virtualizované na hypervizoru HV01 a které nejsou exaktně jmenovány, protože se může jednat o virtuální desktopy nebo virtuální servery.

Dále je zde zobrazen doménový řadič DC01, databázový server SQL01, server pro nástroje System Center SC01 a server RD01 pro Remote Desktop Services, ke kterému je navíc připojen a sdílený disk pro ukládání dat virtuálních strojů, které jsou hostovány na serveru HV01.

Na obrázku je dále vidět stroj CLIENT pro testování připojení do infrastruktury VDI z klientského operačního systému a 2 virtuální přepínače, které se starají o síťový provoz.

5.5.1 Seznam strojů v logickém návrhu

V této kapitole jsou vyjmenovány virtuální stroje, které jsou využity pro testování v logickém návrhu a jejich základní popis a nastavení.

Virtuální stroj DC01

Virtuální stroj DC01 má nainstalovaný systém Windows Server 2012 R2 Datacenter a slouží jako doménový řadič, takže má nainstalovanou roli Active Directory Domain Services, DNS server a DHCP server.

Dále tento server bude sloužit jako centrální správce ostatních serverů, takže tyto servery odtud budou spravovány pomocí připojení do nástroje Server Manager, čímž se eliminuje nutnost častého přepínání mezi připojeními mezi virtuálními stroji a omezí se tím i nároky virtuálních strojů, na kterých nebude nainstalováno uživatelské rozhraní, ale pouze Core Edice systému Windows Server.

IP adresa serveru DC01 je 192.168.1.1.

Virtuální stroj RD01

Tento stroj, který je postaven na systému Windows Server 2012 R2 Datacenter a slouží primárně pro poskytování rolí, které slouží pro vzdálené připojení, takže má

nainstalovanou roli serveru Remote Desktop Services a dále obsahuje následující role pro vzdálené připojení:

- Remote Desktop Web Access,
- Remote Desktop Gateway,
- Remote Desktop Licensing,
- Remote Desktop Session Host.

Dále tento server slouží jako síťové úložiště pro data virtuálních serverů, takže má připojený další virtuální disk, který je sdílený do sítě.

Server RD01 má přidělenou IP adresu 192.168.1.11.

Virtuální stroj SQL01

Další virtuální stroj SQL01 slouží jako databázový server pro všechny potřebné databáze v infrastruktuře.

Pro tento stroj je využita edice Windows Server 2012 R2 Datacenter a dále je zde nainstalován SQL server v edici Microsoft SQL Server 2014 Enterprise Edition.

IP adresa databázového serveru je 192.168.1.31.

Virtuální stroj SC01

Pro další virtuální stroj SC01 je použita edice Windows Server 2012 R2 Datacenter a jsou zde hostovány nástroje z rodiny System Center, tedy především:

- System Center Virtual Machine Manager,
- System Center Configuration Manager.

SC01 server má nastavenou IP adresu 192.168.1.41.

Virtuální stroj CLIENT

Tento virtuální stroj má jako jediný nainstalovaný klientský operační systém Windows 8.1 a slouží pro otestování připojení k virtuálním desktopům pomocí RDP protokolu, přes Remote Desktop Gateway a přes webový prohlížeč.

Pro asociaci IP adresy pro tohoto klienta je využito protokolu DHCP.

Fyzický stroj HV01

Pro stroj HV01 je využita edice Microsoft Hyper-V® Server 2012 R2 a slouží především jako hypervizor pro hostování instancí virtuálních desktopů.

Dále zde je nainstalována serverová role Remote Desktop Services, která poskytuje roli Remote Desktop Virtualization Host.

IP adresa serveru je 192.168.1.21.

5.5.2 Hardwarová konfigurace virtuálních strojů

Hardwarová konfigurace všech virtuálních strojů, které byly využity pro testování funkcionalit v logickém návrhu řešení, je pro všechny virtuálních stroje stejná s menšími odlišnostmi, které jsou uvedeny dále. Standardní konfigurace je vidět v tabulce 8: Standardní konfigurace virtuálních strojů v logickém návrhu.

Hardware	Atribut
Název VM	„Název VM“
Operační paměť	1024 MB
Procesor	Virtuální procesor: 1
Řadič SCSI - pevný disk	„Název VM“.vhdx (dynamická velikost)
Řadič SCSI - jednotka DVD	ISO soubor s instalací operačního systému
Síťový adaptér	SW2

Tabulka 8: Standardní konfigurace virtuálních strojů v logickém návrhu

Odlišnosti v jednotlivých konfiguracích jsou:

- Virtuální stroj RD01 má připojen druhý disk STORAGE.vhdx, který slouží ukládání virtuálních strojů a je sdílený v síti. Tento stroj byl vybrán z důvodu předpokládaného nejnižšího zatížení. Velikost tohoto disku je pevná a je to 100 GB.
- Virtuální stroj RD01 má přiděleno 2048 MB RAM z důvodu nutnosti obsloužit více relací vzdáleného připojení v jeden čas.

- Virtuální stroj SC01 má přiděleno 4096 MB RAM z důvodu kontroly velikosti operační paměti během instalace nástroje System Center Virtual Machine Manager, kde je potřeba alespoň 4000 MB RAM.

5.5.3 Konfigurace jednotlivých virtuálních strojů v logickém návrhu

Základní konfigurace virtuálních strojů v logickém návrhu využívá stejné nebo podobné příkazy, které byly použity už v logickém návrhu, takže další popis těchto příkazů není uveden a jsou uváděny pouze jednotlivé příkazy.

Konfigurace stroje DC01

Systémová konfigurace stroje DC01 zahrnuje:

1. `netdom renamecomputer %COMPUTERNAME% /NewName:DC01`
2. `netsh interface ipv4 show interfaces`
3. `netsh interface ipv4 set address name="12" source=static address=192.168.1.1 mask=255.255.255.0 gateway=127.0.0.1`
4. `shutdown /r /t 0`
5. Instalace role Active Directory Domain Services, DNS Server a DHCP server včetně potřebných nástrojů pomocí průvodce, který je dostupný z konzole Server Manager, která slouží pro základní správu serveru. Dále instalace Hyper-V Management Tools pro pozdější správu serveru HV01.
6. Konfigurace role Active Directory Domain Services, buď pomocí průvodce pro povýšení serveru na doménový řadič nebo pomocí PowerShell příkazů:
 - `Import-Module ADDSDeployment`
 - `Install-ADDSForest -CreateDnsDelegation:$false -DatabasePath "C:\Windows\NTDS" -DomainMode "Win2012R2" -DomainName "CORP.local" -DomainNetbiosName "CORP" -ForestMode "Win2012R2" -InstallDns:$true -LogPath "C:\Windows\NTDS" -NoRebootOnCompletion:$false -SysvolPath "C:\Windows\SYSVOL" -Force:$true`
 - Během druhého příkazu je uživatel požádán o zadání hesla pro obnovu domény a po dokončení příkazu se stroj restartuje.

7. Konfigurace role DHCP serveru zahrnuje povolení vytvoření bezpečnostních skupin v Active Directory a dále vytvoření přidělovaného adresního rozsahu, který obsahuje přidělované IP adresy. Tento rozsah byl zvolen v rozmezí IP adres 192.168.1.100 až 192.168.1.254 a jako defaultní brána je propagována IP adresa 192.168.1.1 a jako DNS server 192.168.1.1. Nakonec byl DHCP server autorizován v Active Directory.

Konfigurace stroje RD01

Virtuální stroj RD01 byl nakonfigurován následujícími příkazy:

1. `netdom renamecomputer %COMPUTERNAME% /NewName:RD01`
2. `netsh interface ipv4 show interfaces`
3. `netsh interface ipv4 set address name="12" source=static
address=192.168.1.11 mask=255.255.255.0 gateway=192.168.1.1`
4. `netsh interface ipv4 add dnsserver name="12" address=192.168.1.1 index=1`
5. `shutdown /r /t 0`
6. `netdom join %COMPUTERNAME% /domain:CORP.local /user:Administrator
/passwordd:*`
7. `shutdown /r /t 0`
8. Připojení serveru RD01 do správy konzole Server Manager na serveru DC01.
9. Vzdálené nainstalování serverové role Remote Desktop Services a jeho rolí Connection Broker, Gateway, Licensing, Session Host a Web Access. V rámci této instalace bylo potřeba ještě vybrat službu role Network Policy and Access Services a službu role Web Server Role (IIS), kde u obou rolí byly ponechány defaultní role.
10. K serveru je připojen druhý disk pro ukládání dat v síti. Tento disk byl ve virtuálním stroji RD01 inicializován, vytvořen svazek, připojen jako jednotka N, pojmenován jako VDI a zformátován na souborový systém NTFS. Následně byl v síti sdílen jako souborové úložiště \\RD01\VDI. Dále bylo potřeba nastavit plné oprávnění na tuto sdílenou složku pro všechny Hyper-V hypervizory, aby měly přístup do těchto složek.

Konfigurace stroje HV01

Konfigurace systému na serveru HV01 obsahuje:

1. `netdom renamecomputer %COMPUTERNAME% /NewName:HV01`
2. `netsh interface ipv4 show interfaces`
3. `netsh interface ipv4 set address name="13" source=static
address=192.168.1.21 mask=255.255.255.0 gateway=192.168.1.1`
4. `netsh interface ipv4 add dnsserver name="13" address=192.168.1.1 index=1`
5. `shutdown /r /t 0`
6. `netdom join %COMPUTERNAME% /domain:CORP.local /userd:Administrator
/passwordd:*`
7. `shutdown /r /t 0`
8. Připojení serveru HV01 do správy konzole Server Manager na serveru DC01.
9. Vzdálené nainstalování serverové role Remote Desktop Services a jeho role Virtualization Host.
10. Nakonec bylo změněny v nastavení technologie Hyper-V cesty pro ukládání virtuálních strojů a virtuálních disků.

Konfigurace stroje SQL01

Server SQL01 je možné nastavit následujícími příkazy:

1. `netdom renamecomputer %COMPUTERNAME% /NewName:SQL01`
2. `netsh interface ipv4 show interfaces`
3. `netsh interface ipv4 set address name="12" source=static
address=192.168.1.31 mask=255.255.255.0 gateway=192.168.1.1`
4. `netsh interface ipv4 add dnsserver name="12" address=192.168.1.1 index=1`
5. `shutdown /r /t 0`
6. `netdom join %COMPUTERNAME% /domain:CORP.local /userd:Administrator
/passwordd:*`
7. `shutdown /r /t 0`
8. Připojení serveru SQL01 do správy konzole Server Manager na serveru DC01.

Instalace a konfigurace SQL databáze na stroji SQL01

Na serveru SQL01 došlo k instalaci databázového serveru, který bude hostovat databáze v infrastruktuře. Tento databázový server je založen na produktu Microsoft SQL Server 2014 Enterprise Edition.

Instalace a konfigurace byla provedena pomocí instalačního průvodce, který během svého běhu kontroluje stav systému a kontroluje požadavky na operační systém a hardwarové a softwarové zdroje.

Na serveru byly nainstalovány všechny nástroje se základním nastavením, kvůli čemuž musel být doinstalován Microsoft .NET Framework 3.5, který není standardním vybavením instalace Windows Server, ale musí být doinstalován, což lze provést například pomocí průvodce pro přidání rolí a nástrojů ve Windows Server.

Název instance SQL serveru byl zvolen MSSQLSERVER.

Konfigurace stroje SC01

Virtuální stroje SC01 byl nakonfigurován následujícím postupem:

1. `netdom renamecomputer %COMPUTERNAME% /NewName:SC01`
2. `netsh interface ipv4 show interfaces`
3. `netsh interface ipv4 set address name="12" source=static
address=192.168.1.41 mask=255.255.255.0 gateway=192.168.1.1`
4. `netsh interface ipv4 add dnsserver name="12" address=192.168.1.1 index=1`
5. `shutdown /r /t 0`
6. `netdom join %COMPUTERNAME% /domain:CORP.local /userd:Administrator
/passwordd:*`
7. `shutdown /r /t 0`
8. Připojení serveru SC01 do správy konzole Server Manager na serveru DC01.

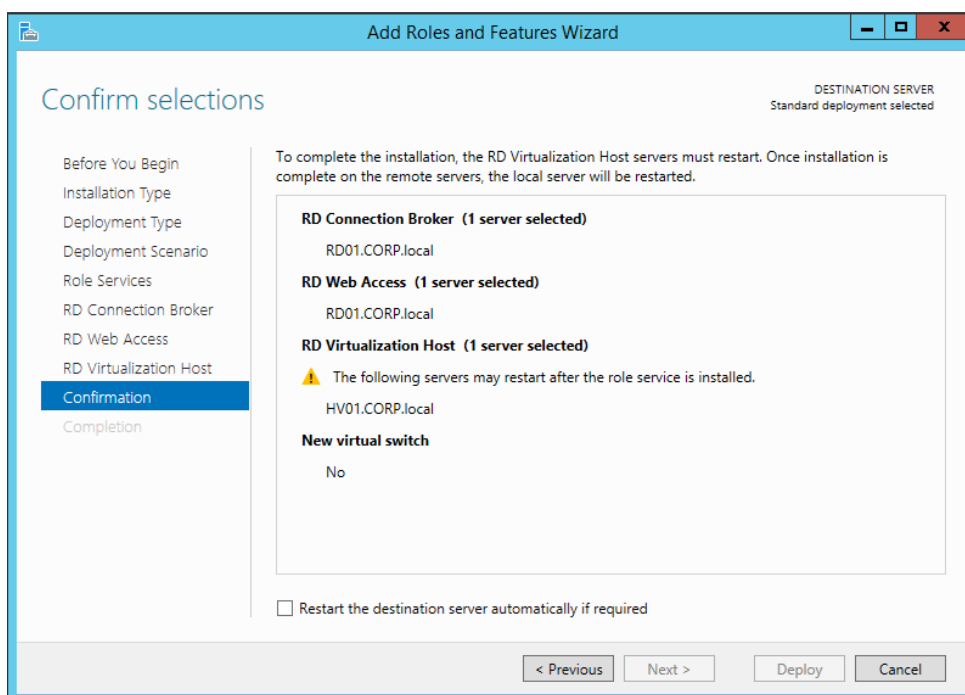
Instalace a konfigurace VDI infrastruktury

Následně bylo potřeba vytvořit samotnou VDI infrastrukturu, která lze vytvořit z průvodce přidáním rolí a nástrojů ve Windows Serveru.

Na serveru RD01 byl tento průvodce spuštěn a byl vybrán typ instalace založený na Remote Desktop Services (Remote Desktop Services installation), následně bylo vybráno standardní nasazení (Standard deployment) a následně typ nasazení Virtual machine-base desktop deployment.

V dalších krocích bylo potřeba vybrat server, který bude mít roli Remote Desktop Connection Broker, tedy RD01, roli Remote Desktop Web Access, tedy také RD01 a nakonec Remote Desktop Virtualization Host, takže server, kde budou běžet virtualizované desktop, tedy server HV01.

Souhrn všech serverů je vidět na obrázku 11: Průvodce nasazení VDI infrastruktury, kde je vidět souhrn všech vybraných serverů a u serveru HV01 je vidět, že na tomto serveru není ještě instalovaná role RD Virtualization Host a server bude tedy během instalace restartován.



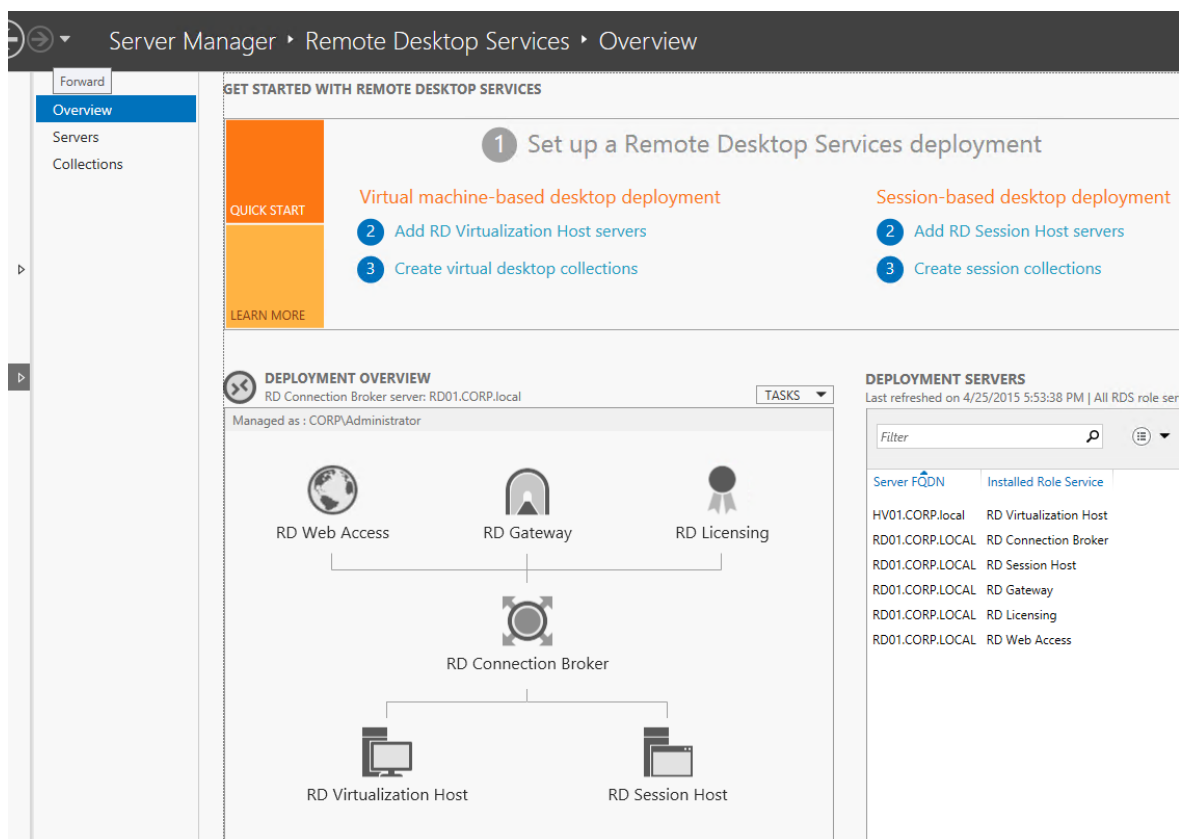
Obrázek 11: Průvodce nasazení VDI infrastruktury (zdroj: autor)

Stejný postup byl poté zopakován pro typ nasazení založeném na relacích (session-based desktop deployment).

Dalším krokem je přidání RD Gateway serveru, kterým bude server RD01. Během průvodce přidáním serveru se zde generuje certifikát pro komunikaci mezi Remote Desktop Services klienty a RD Gateway serverem.

Nakonec je potřeba přidat licenční server, kterým bude také server RD01.

Po dokončení základní konfigurace je nyní možné pokračovat dál v nasazení infrastruktury virtuálních desktopů. Jak je vidět na následujícím obrázku 12: Rozhraní Remote Desktop Services, dalším krokem je možné přidání dalších virtualizačních hostů nebo serverů pro relační nasazení, ovšem v tomto testovacím scénáři bylo pokračováno rovnou ve vytvoření kolekcí virtuálních desktopů a vytvoření relační kolekce.



Obrázek 12: Rozhraní Remote Desktop Services (zdroj: autor)

Následně byla vytvořena relační kolekce s názvem Relační kolekce, pro skupinu uživatelů, kteří jsou v doméně ve skupině „VDI – session“, která byla pro tyto účely v doméně vytvořena. Dále bylo nastaveno, že data uživatelů se ukládají do síťové složky \\RD01\VDI\Users a každý uživatel může mít alokováno maximálně 20 GB.

Pro relační kolekci byly dále vypublikovány aplikace Kalkulačka, Malování a WordPad.

Pro vytvoření kolekce virtuálních desktopů je potřeba nejdříve vytvořit na serveru HV01 předlohu virtuálního desktopu WIN8-template. Další postup spočívá ve vytvoření kolekce „VDI – kolekce“, která je typu sdružené kolekce, následně se vybere vzor virtuálního desktopu, tedy vytvořený WIN8-template. Dále se vybere, podle jakého souboru má být stroj nastaven a nastaví se další nastavení, kterými jsou například časová zóna, organizační jednotka v doméně. Dále uživatelé, kteří mají právo se k desktopu připojit, tedy uživatelé ve skupině „skupině „VDI – kolekce“ přiřazení zdrojů, umístění souborů virtuálního stroje a uživatelů, kde bylo vybráno \\RD01\VDI\VMs a \\RD01\VDI\VMusers.

Instalace a konfigurace nástroje System Center Virtual Machine Manager

Instalace nástroje System Center Virtual Machine Manager byla provedena na serveru SC01, kdy byl nainstalován VMM management server, který se stará o správu prostředí, a nástroj VMM console pro správu systému Virtual Machine Manager.

Před samotnou instalací nástroje bylo potřeba na server nainstalovat Windows Assessment and Deployment Kit for Windows 8.1 a Microsoft SQL Server 2012 Command Line Utilities.

Nástroj byl připojen k databázi na serveru SQL01 a instanci MSSQLSERVER, kde byla vytvořena nová databáze VirtualManagerDB.

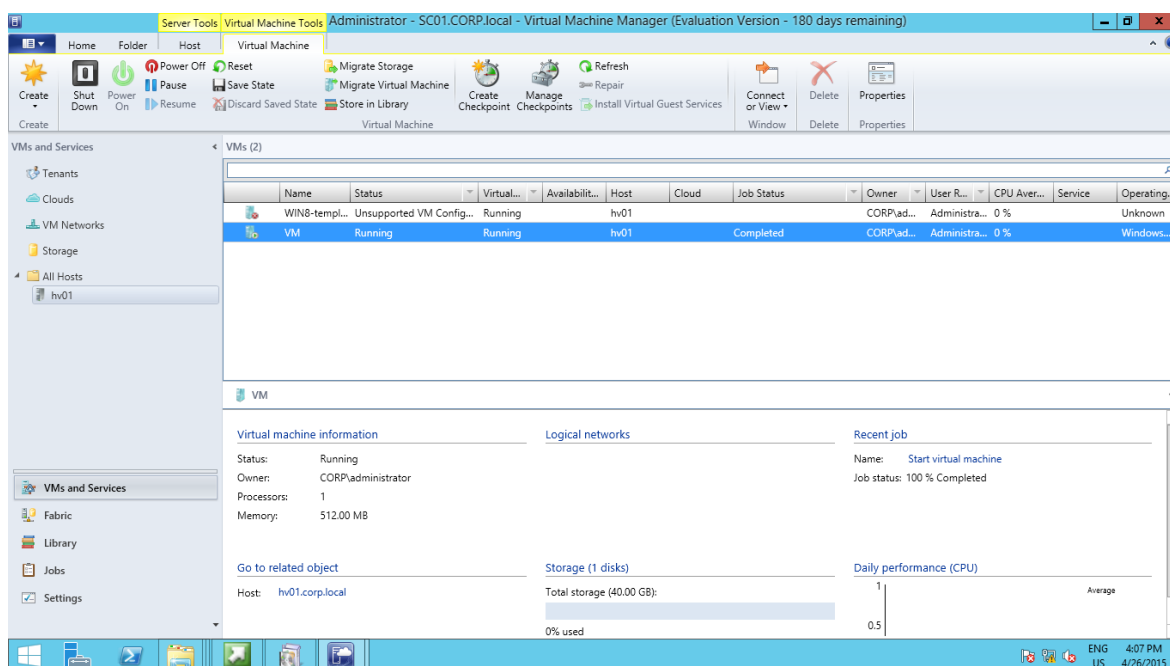
Dále bylo potřeba nastavit servisní účet, pod kterým nástroj poběží, nastavit porty pro komunikaci serveru pro správu nástroje s ostatními komponentami a zařízeními a nastavit složku pro sdílení knihovny Virtual Machine Manager.

Po nainstalování je potřeba připojit virtualizační hostitele do správy nástrojem Virtual Machine Manager, což se provede v nainstalované konzoli, která se připojí k serveru, kde je nástroj provozován.

Po spuštění konzole se klikne v menu VMs and Services pravým tlačítkem myši na volbu All Hosts a vybere se volba Add Hyper-V Hosts and Clusters, což spustí průvodce přidáním hypervizorů Hyper-V.

V průvodci se zadají přihlašovací údaje, pod kterými bude služba běžet a komunikovat s hypervizorem, a dále jak mají být nalezeny hypervizory v Active Directory nalezeny nebo je možné zadat přímo jejich název.

Po přidání hypervizoru je v konzoli tento hypervizor vidět a byly přidány také jeho virtuální stroje. Na obrázku 12: Konzole Virtual Machine Manager jsou po přidání hypervizoru HV01.CORP.local vidět virtuální stroje hostované na tomto serveru a je možné s nimi z této konzole dále pracovat a diagnostikovat.



Obrázek 13: Konzole Virtual Machine Manager (zdroj: autor)

Nyní je možné spravovat virtuální stroje a virtualizační platformu přímo z této konzole, která nabízí správu více hypervizorů z jednoho místa bez nutnosti se na dané zdroje přímo připojovat.

Instalace a konfigurace nástroje System Center Configuration Manager

Na server SC01 byla nainstalována a zkonfigurována centrální administrativní lokalita nástroje System Center Configuration Manager.

Před samotnou instalací bylo potřeba ještě na server doinstalovat Microsoft .NET Framework 3.5 Service Pack 1.

Po spuštění instalace byly nejdříve staženy z Internetu potřebné soubory, poté byla vytvořena samostatná primární lokalita CORP s kódem COD a dále byla na serveru nainstalována konzole pro správu nástroje System Center Configuration Manager.

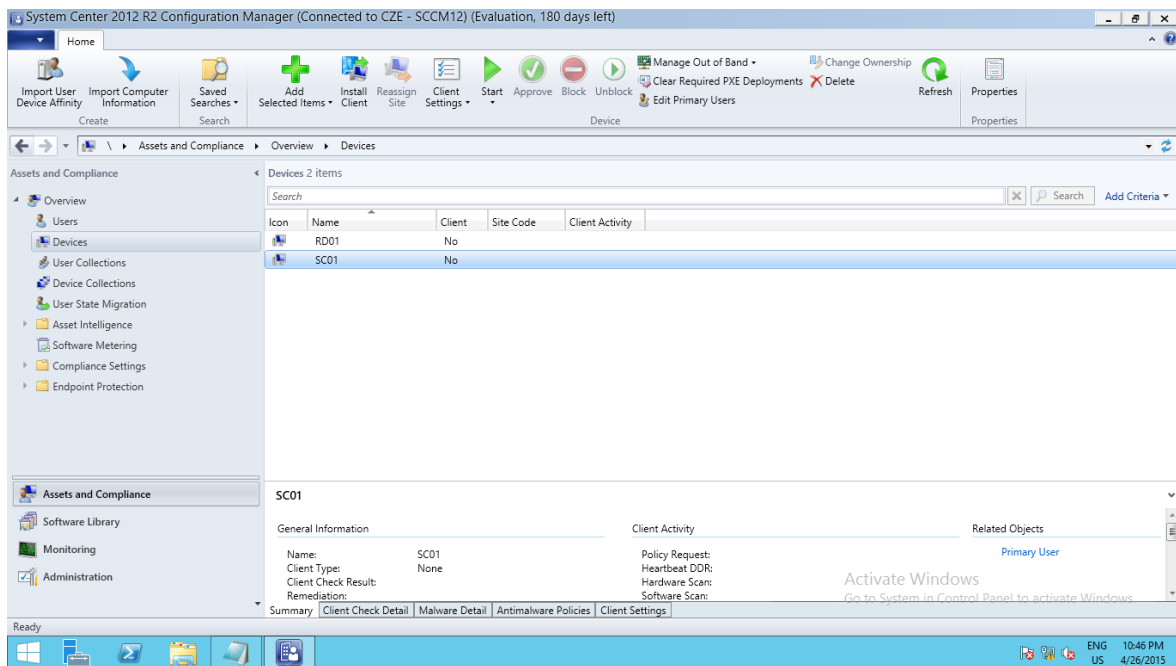
Dále byl nástroj připojen k databázi serveru SQL01.CORP.local na portu 4023, vytvořena zde instance SCCM12 a název databáze byl nastaven na CM_COD.

Server SC01 byl zvolen také jako distribuční bod a bod správy pro hierarchii nástroje Configuration manager. V rámci instalačního průvodce byly dále vybrány složky, kde budou uloženy data, jakým protokolem budou klienti komunikovat s bodem správy a další nastavení.

Před samotným spuštěním instalace proběhla ještě kontrola, která odhalila nesprávný běhový účet databázového serveru, který bylo potřeba přenastavit na doménový.

Kontrola také odhalila potřebu rozšíření schématu Active Directory o další atributy, vytvoření kontejneru System Management v doméně a instalaci funkce serverové Remote Differential Compression (RDC).

Po úspěšném nainstalování a spuštění konzole nástroje System Center Configuration Manager se zobrazila konzole, která je vidět na obrázku 14: Konzole Configuration Manager, kde jsou vidět dvě připojené zařízení ve správě.



Obrázek 14: Konzole Configuration Manager (zdroj: autor)

Na obrázku jsou vidět čtyři základní komponenty nástroje Configuration Manager, kterými jsou Assets and Compliance pro správu zařízení a uživatelů, Software Library pro správu aplikací, aktualizací a operačních systémů, které mohou být nasazovány pomocí Configuration Manageru, dále položku Monitoring pro monitorování klientů a položku Administration pro správu nástroje System Center Configuration Manager.

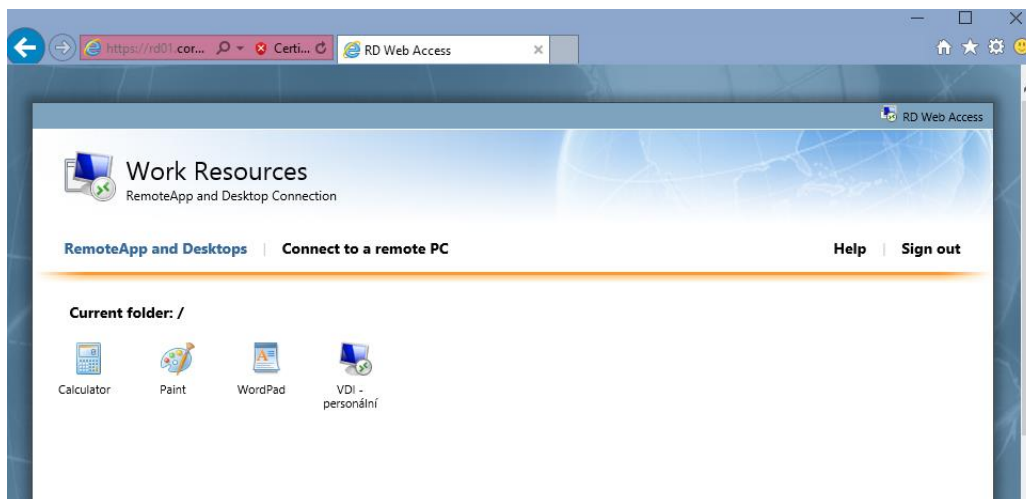
Konfigurace stroje CLIENT

Jelikož stroj CLIENT je stroj s klientským operačním systémem, tak nejdříve bylo potřeba projít konfiguraci systému Windows 8.1 a následně až přejít ke konfiguraci systému, kdy byl počítač přejmenován a přidán do domény CORP.local.

5.5.4 Otestování funkcionality virtuálních desktopů

Pro testování byl vytvořen doménový uživatel user1, který je členem skupiny „VDI – session“, a uživatel user2, který je členem skupiny „VDI – kolekce“

Po přihlášení uživatele do portálu <https://rd01.corp.local/RDWeb> se uživateli user1 zobrazí portál s jeho vypublikovanými aplikacemi, který je vidět na obrázku 15: Portál RemoteApp and Desktop Connection, kde uživatel vidí jeho aplikace a dále má možnost se připojit ke vzdálenému virtuálnímu desktopu.



Obrázek 15: Portál RemoteApp and Desktop Connection (zdroj: autor)

Dále bylo otestování připojení se k vypublikovanému virtuálnímu desktopu pomocí ikony VDI – personální, kdy po kliknutí na tuto ikonu se spustil virtuální počítač a uživatel se k němu připojil.

Otestování připojení k virtuálnímu desktop bylo provedeno uživatelem user2 připojením se k IP adrese Connection Brokeru, který provedl přesměrování k virtuálnímu stroji, který se automaticky vytvořil pro daného uživatele.

Pro otestování nástroje System Center Virtual Machine Manager byl pomocí tohoto nástroje vytvořen kompletně nový virtuální stroj, včetně všech zdrojů.

Dále byl stroj spuštěn a po instalaci operačního systému byla otestována základní správa virtuální stroje,

5.6 Škálovatelnost a další možný rozvoj

Důležitým faktorem řešení bylo stanovit takové řešení, které bude škálovatelné a nebude značně limitováno pro další rozvoje infrastruktury.

Základním kritickým konceptem bylo neomezit infrastrukturu na fyzické vrstvě a navrhnout takové řešení, které bude možné rozšířit v budoucích obdobích, kdy se identifikuje potřeba infrastrukturu rozšířit.

5.6.1 Fyzický návrh řešení

Testovací koncept, který je představen na obrázku 7: Návrh zapojení fyzické vrstvy a který vychází z celkové koncepce řešení znázorněného na obrázku 6: Celkový návrh řešení, je navrženo zapojen je několika málo serverů a tudíž omezené možnosti toto řešení využít pro celou infrastrukturu.

Tento koncept bude potřeba doplnit především dalším úložištěm pro data virtuálních serverů, navýšením fyzických zdrojů všech serverů a především rozšíření počtu Hyper-V hostitelů, tak aby výkonově pokryly celkovou náročnost infrastruktury virtuálních desktopů a virtuálních serverů.

Dále je nutné v tomto konceptu odstranit neredundantní zapojení, takže do tohoto konceptu přibude další síťový přepínač a všechny servery budou muset být síťově zapojeny do obou přepínačů.

Koncept je také vybudován pouze na jedné síti a jednom adresním rozsahu, což je nežádoucí a měly by být odděleny datové toky, které by měly být již ze své podstaty izolovány. Tato izolace by se měla týkat především:

- Oddělení sítě pro správu infrastruktury,
- oddělení sítě pro oba clustery tak, aby replikace v clusteru nebyla limitována dalším provozem,
- oddělení sítě, která se stará o kontrolu činnosti členů v clusteru (tzv. heartbeat) ideálně za pomoci přímého propojení serverů,
- oddělení sítě zajišťující veškerou komunikaci mezi servery starající se o datová úložiště a mezi servery starající se o virtualizační platformu Hyper-V.

Další otázkou implementace je možnost řešení komunikace mezi fyzickou a logickou vrstvou, tedy virtualizační a virtualizovanou platformou, která by měla být řešena pomocí filtrování síťového toku, čímž dojde k eliminaci nežádoucích chování systémů na síťové vrstvě a k zajištění bezpečnosti jednotlivých systémů.

Tyto základní kroky by měly být v reálném prostředí implementovány, což ale reflektuje reálné požadavky na infrastrukturu, používané aplikace a další požadavky

na infrastrukturu virtuálních desktopů. Tyto požadavky se mohou lišit v závislosti na společnosti, ve které bude řešení implementováno.

5.6.2 Logický návrh řešení

Kritické servery by měly být redundantní a tudíž v clusteru nebo by měla být řešena vysoká dostupnost a odolnost vůči chybám.

Dále by oproti testovacímu scénáři mělo být využito rozdělení rolí vzdáleného připojení mezi několika servery, čímž bude možné konfigurace serverů uzpůsobit jejich účelu a logicky shlukovat na serverech stejné role, atributy a podobný význam. Takže je možné například roli RD Web Access, která zahrnuje serverovou roli Internet Information Services (IIS), dát na stejný server například s webovými stránkami dané společnosti, čím se využije daná serverová role dvakrát a nemusí být instalována na více serverů.

Dále by podle potřeb měl nebo mohl být portál podle potřeb společnosti dostupný přes Internet, čímž se docílí možnosti připojení se uživatelů bez nutnosti mít firemní počítač stále u sebe nebo nutnosti VPN spojení. Ovšem v tomto případě by se mělo zajistit zabezpečení tohoto webu a zvážit vícefaktorová autentifikace.

Síťování v logickém návrhu řešení, které by mělo vycházet ze skutečných potřeb podniku, by mělo rozdělit adresy do různých oddělených sítí. Mělo by být počítáno, že jedna síť bude určena pro virtuální servery, kde bude využito statického přidělování IP adres, a druhá síť by měla být určena pro virtuální desktopy, kde bude využito dynamického přidělování IP adres.

Fyzické servery (hypervizory, servery poskytující úložiště dat a případně další) by měly mít také svůj adresní rozsah a také by mělo být počítáno s oddělenou sítí pro fyzické klienty podle potřeb a požadavků společnosti.

V technologickém popisu implementace nástrojů System Center byly popsány pouze nástroje Virtual Machine Manager a Configuration Manager, takže v detailní implementaci by měly být využity i delší nástroje, především Data Protection Manager, Service Manager, App Controller a dalších.

6 Porovnání virtualizovaného a klasického řešení

Tato kapitola je věnována především porovnání virtualizovaného a klasického řešení klientských operačních systémů, které bylo provedeno z hlediska funkčního a finančního.

Obě řešení mají své výhody a nevýhody, ke kterým se musí přihlídnout v případě implementace jednoho nebo druhého řešení.

6.1 Funkční porovnání

Funkční porovnání zohledňuje fakt, jak klientský operační systém funguje z pohledu zaměstnance a jeho běžných pracovních povinností a podnikových procesů.

Z funkčního pohledu jsou si obě řešení velice podobné, což je ovšem závislé na implementaci a zvoleném návrhu infrastruktury.

Hlavní rozdíl, kde může být z pohledu uživatele vnímán největší rozdíl, je komfort práce se zařízením a složitost přihlášení se a připojení se, takže je vhodné se zaměřit především na intuitivní ovládání klasického nebo virtuálního desktopu.

Výhody a nevýhody obou řešení v ohledu funkce jsou nastíněny v následující části práce, kde je základní výčet jednotlivých vlastností.

Výhody virtualizovaného řešení jsou:

- Jednoduchá centrální správa, podpora a dohled,
- uživatelské prostředí stejné při připojení z více fyzických míst,
- vysoká dostupnost řešení,
- škálovatelnost řešení,
- jednodušší zabezpečení infrastruktury a dat,
- možnost nasazení deduplikace dat,
- nižší energetická náročnost,
- menší tepelná náročnost.

Mezi funkční nevýhody virtualizovaného řešení patří:

- Nemožnost běhu některých aplikací,
- umístění dat v síti zvyšuje náročnost na síťové přenosy a změnu způsobu práce,
- odkázání na infrastrukturní služby a počítačovou síť,
- limitace síťového připojení obzvláště při připojení přes Internet,
- práce pomocí protokolu vzdáleného připojení je mnohdy nekomfortní.

Výhody klasického řešení z funkčního pohledu:

- Dostatečný výpočetní výkon pro více náročné aplikace,
- možnost práce i při výpadku centrálních infrastrukturních služeb,
- možnost mobility bez počítačové sítě v případě notebooků,
- zažitý způsob práce a fungování a tím i vyšší efektivita,
- nižší pravděpodobnost zanesení globální chyby konfigurace.

Nakonec nevýhody klasického řešení jsou:

- Málo standardizované prostředí,
- nízká úroveň automatizace,
- data jsou uložena mnohdy na jednom disku fyzického počítače,
- vyšší energetická náročnost,
- velikost klasického počítače.

Mnoho z těchto výhod a nevýhod je spojeno s faktem, jak je počítač virtuální nebo klasický vnímán, takže je důležité uvědomit si, jak dané řešení funguje a kde jsou jeho výhody, nevýhody a případné limitace. Po tomto uvědomění si je možné poté využívat dané řešení efektivněji s převahou výhod daného řešení.

6.2 Finanční porovnání

Finanční porovnání obou řešení vychází z analýzy současných nákladů a předpokládaných budoucích nákladů v případě implementace virtuálních desktopů.

V následující tabulce 9: Finanční analýza - klasické řešení je vidět předpokládaný a plánovaný finanční vývoj klasické infrastruktury.

Klasické řešení	0. rok	1. rok	2. rok	3. rok	4. rok	5. rok
Hardware						
servery + hardware	1 000 000	500 000	600 000	700 000	800 000	1 000 000
desktoxy	0	1 125 000	1 125 000	1 125 000	1 125 000	1 125 000
celkem	1 000 000	1 625 000	1 725 000	1 825 000	1 925 000	2 125 000
Software						
licence - servery	0	150 000	150 000	150 000	150 000	150 000
licence - desktoxy	800 000	800 000	800 000	800 000	800 000	800 000
celkem	800 000	950 000	950 000	950 000	950 000	950 000
Technická podpora						
administrátoři	0	1 320 000	1 372 800	1 427 712	1 484 820	1 544 213
helpdesk	0	1 848 000	1 921 920	1 998 797	2 078 749	2 161 899
celkem	0	3 168 000	3 294 720	3 426 509	3 563 569	3 706 112
Náklady na instalaci						
nová instalace - administrátoři	0	20 000	25 000	30 000	35 000	40 000
nová instalace - helpdesk	0	105 000	105 000	105 000	105 000	105 000
údržba - administrátoři	0	125 000	137 500	150 000	162 500	175 000
údržba - helpdesk	0	280 000	280 000	280 000	280 000	280 000
celkem	0	530 000	547 500	565 000	582 500	600 000
Náklady na školení						
IT zaměstnanci	0	0	0	0	0	0
ostatní uživatelé	0	0	0	0	0	0
celkem	0	0	0	0	0	0
Implementace a konzultace						
externí podpora	100 000	100 000	100 000	100 000	100 000	100 000
Záložní, vývojové, testovací a školící prostředí						
	0	20 000	20 000	20 000	20 000	20 000
Rozvoj, změny a rozšíření						
rozvoj	0	200 000	200 000	200 000	200 000	200 000
Elektrická energie						
servery	0	224 256	224 256	224 256	224 256	224 256
desktoxy/klienti	0	432 000	432 000	432 000	432 000	432 000
	0	656 256	656 256	656 256	656 256	656 256
	3 700 000	14 178 512	14 666 952	15 165 530	15 674 650	16 394 736

Tabulka 9: Finanční analýza - klasické řešení

Pro klasické řešení je předpokládána roční výměna čtvrtiny počítačů ve čtyřletém cyklu a v nultém roce zahrnuje pořízení nástrojů System Center.

V tabulce 10: Finanční analýza – virtualizované řešení je vidět předpokládaný a plánovaný finanční vývoj virtualizovaného řešení infrastruktury.

Virtualizované řešení	0. rok	1. rok	2. rok	3. rok	4. rok	5. rok
Hardware						
servery + hardware	5 000 000	50 000	100 000	150 000	180 000	200 000
desktohy	2 100 000	0	0	42 000	105 000	105 000
celkem	7 100 000	50 000	100 000	192 000	285 000	305 000
Software						
licence - servery	2 000 000	0	0	0	0	0
licence - desktohy	4 000 000	0	0	0	0	0
celkem	6 000 000	0	0	0	0	0
Technická podpora						
administrátoři	0	1 760 000	1 830 400	1 903 616	1 979 761	2 058 951
helpdesk	0	739 200	768 768	799 519	831 499	864 759
celkem	0	2 499 200	2 599 168	2 703 135	2 811 260	2 923 711
Náklady na instalaci						
nová instalace - administrátoři	250 000	100 000	100 000	120 000	120 000	120 000
nová instalace - helpdesk	52 500	10 500	12 250	14 000	15 750	17 500
údržba - administrátoři	0	300 000	200 000	200 000	250 000	300 000
údržba - helpdesk	0	35 000	26 250	17 500	17 500	17 500
celkem	302 500	445 500	338 500	351 500	403 250	455 000
Náklady na školení						
IT zaměstnanci	0	120 000	0	0	0	0
ostatní uživatelé	0	200 000	0	0	0	0
celkem	0	320 000	0	0	0	0
Implementace a konzultace						
celkem	480 000	480 000	480 000	480 000	480 000	480 000
Záložní, vývojové, testovací a školící prostředí						
celkem	200 000	100 000	100 000	100 000	100 000	100 000
Rozvoj, změny a rozšíření						
celkem	0	0	50 000	50 000	50 000	50 000
Elektrická energie						
servery	0	336 384	336 384	336 384	336 384	336 384
desktohy/klienti	0	144 000	144 000	144 000	144 000	144 000
celkem	0	480 384	480 384	480 384	480 384	480 384
CELKEM	27 485 000	8 170 168	7 666 104	8 084 037	8 589 788	8 958 189

Tabulka 10: Finanční analýza - virtuální řešení

Obě předchozí tabulky vychází z celkové analýzy a zahrnují všechny výdaje, které jsou relevantní pro problematiku pracovních stanic, takže nezahrnují další aplikační servery, další náklady týkající se ostatních procesů a zdrojů.

Obě předchozí tabulky jsou shrnuty následující tabulce 11: Celkový souhrn nákladů a celková úspora, kde jsou vidět celkové náklady obou řešení a úspora v jednotlivých letech.

<i>Celkový souhrn</i>	<i>0. rok</i>	<i>1. rok</i>	<i>2. rok</i>	<i>3. rok</i>	<i>4. rok</i>	<i>5. rok</i>	<i>Celkem</i>
<i>Klasické řešení</i>	<i>3 700</i>	<i>14 178</i>	<i>14 667</i>	<i>15 165</i>	<i>15 675</i>	<i>16 395</i>	<i>79 780</i>
<i>Virtualizované řešení</i>	<i>27 485</i>	<i>8 170</i>	<i>7 666</i>	<i>8 084</i>	<i>8 590</i>	<i>8 958</i>	<i>68 953</i>
<i>Úspora</i>	<i>-23 785</i>	<i>6 008</i>	<i>7 001</i>	<i>7 081</i>	<i>7 085</i>	<i>7 437</i>	<i>10 827</i>

Tabulka 11: Celkový souhrn nákladů a celková úspora (v tisících Kč)

Jak je vidět v tabulce výše, tak jediná záporná úspora je v nultém roce, což ukazuje náklady, které jsou spojeny s implementací řešení.

Celková úspora za celé sledované období je 10 827 000 Kč, což nasvědčuje výhodnost přechodu na virtualizované řešení.

V každém období jsou náklady virtualizovaného řešení podstatně nižší, a jelikož je pravděpodobnější dodatečný vyšší nárůst nákladů v klasické řešení z důvodu zastaralejších zařízení, tak by mělo být rozhodnuto pro virtualizaci pracovních desktopů.

Dalším podstatným parametrem pro rozhodnutí by ale měl být i fakt, jestli má společnost dostatečné finance pro implementaci řešení, protože případné financování z cizích zdrojů by mohlo celé modelové řešení podstatně ovlivnit.

7 Závěr

Cílem diplomové práce bylo provést analýzu technického řešení nasazení virtuální desktopové infrastruktury ve firemním prostředí a dále představeny principy virtualizace především od společnosti Microsoft. Toto řešení bylo dále komparativně porovnáno s klasickým řešením osobních počítačů.

V druhé kapitole práce byly zanalyzovány principy základní informatiky a IT strategie především zaměřené na finanční úsporu a běžné fungování obecného provozu podniku. Tyto principy byly analyzovány se zaměřením na další části práce – tedy virtualizace serverů a hlavně virtualizace desktopů.

Třetí kapitola se věnuje obecným principům virtualizace a popisuje co virtualizace je, její principy a typy, výhody jejího využití a jsou popsány komponenty virtuálního serveru v Hyper-V.

Čtvrtá kapitola představuje architekturu infrastruktury virtuálních desktopů a představuje především nástroje společnosti Microsoft, které jsou využívány v podnikové IT infrastruktuře, tedy Windows Server 2012 R2, Hyper-V, nástroje System Center a další nástroje a aplikační systémy.

Pátá kapitola je věnována návrhu řešení pro středně velkou fiktivní společnost o 200 zaměstnancích. V rámci této kapitoly je navrhnut fyzický a logický návrh řešení, takže ve fyzickém návrhu je zahrnuta vrstva úložiště dat a virtualizační vrstva a v logickém virtualizovaná vrstva virtuálních serverů a strojů.

Dále je zde popsán návrh postupu implementace a detailně popsána celá implementace pilotního projektu v testovacím prostředí, které ovšem reflektuje omezené, především fyzické, zdroje pro testování.

Ze závěrů a zjištění, které z implementace vyplývají lze usoudit, že nejdůležitější fází je návrh řešení, protože pokud není implementace virtuálních desktopů náležitě a komplexně zanalyzována, tak je možné se dostat do stavu, kdy podniková infrastruktura má nejenom méně komfortní řešení, ale může dojít i k prudkému nárůstu nákladů.

Návrh řešení musí zahrnovat nejenom komplexní pohled na celou infrastrukturu, ale musí se zabývat i nejnižšími prvky infrastruktury, které sice nejsou v práci přímo zaměřeny, ale měly by být v rámci projektu řešeny. Mezi tyto prvky patří například síťování, datové úložiště, grafický výkon a další.

Důležitá je zde také analýza potřebného výkonu jednotlivých fyzických zdrojů celé infrastruktury především se zaměřením na odezvu při práci s virtuálním desktopem, která dopomůže k efektivnímu využití všech zdrojů – hardwarových, softwarových, finančních a také personálních.

Šestá kapitola shrnuje a porovnává rozdíl mezi virtualizovaným a klasickým řešením a porovnává ho především v oblasti finančním a funkčním.

Funkční porovnání řešení virtuálních a klasických desktopů ukazuje několik výhod řešení virtuálních desktopů, ovšem tyto výhody musí být podpořeny správným návrhem a správným fungováním.

Podporu virtualizace pracovních desktopů podporuje i provedená finanční analýza nákladů, které je možné odhadnout pro následující období.

Během této analýzy byla sice zjištěna podstatně vysoká počáteční investice do řešení virtualizovaných desktopů a infrastruktury, ale tuto vysokou investici kompenzují takřka poloviční roční náklady, takže v konečném důsledku dojde k vysoké úspoře finančních zdrojů.

Virtualizace desktopů a virtualizace obecně přinášejí mnoho možností v optimalizaci a zlepšení efektivity využívání všech zdrojů společnosti, ve které byla implementována, ale z textu práce je zřejmé, že tato problematika je velice závislá na správném návrhu řešení a jeho optimalizaci pro budoucí rozvoj.

Seznam použité literatury

1. ACEVEDO, David, © 2015. *Update Rollup 5 for System Center 2012 R2 (UR5 for SCOM, SCSM,SCVMM)* [online]. [cit. 2015-03-23]. Dostupné z:
<http://www.netdavidic.com/2015/02/update-rollup-4-for-system-center-2012.html>
2. ALANDER, Link, 2013. *4 Keys to Designing a Virtual Desktop Environment*, *THE Journal*, 40, 9, stránka 31-35, *Academic Search Complete*, EBSCOhost, citováno 14. března 2015.
3. AMARIS, Chris, 2010. *Microsoft System Center Enterprise Suite unleashed*. Indianapolis: Sams. ISBN 978-0-672-33319-4.
4. AMARIS, Chris a Guy YARDENI, 2012. *Microsoft System Center 2012 unleashed*. Indianapolis: Sams. ISBN 978-0-672-33612-6.
5. CARDOSO, Edvaldo Alessandro, 2013. *Microsoft System Center Virtual Machine Manager 2012 Cookbook*. Birmingham: Packt Publishing. ISBN 978-1-84968-632-7.
6. CERLING, Tim, 2010. *Mastering Microsoft virtualization*. Indianapolis: Sybex. ISBN 978-0-470-44958-5.
7. DAQUAS, 2015. *VDI je cesta. Ale k čemu?* [online]. [cit. 2015-04-13]. Dostupné z:
<http://www.daquas.cz/articles/519-vdi-je-cesta-ale-k-cemu>
8. FAUCHEUX, Sylvie a NICOLAI, Isabelle, 2011. 'IT for green and green IT: A proposed typology of eco-innovation', *Ecological Economics*, 70, 11, s. 2020-2027, *Business Source Complete*, EBSCOhost, citováno 30. března 2015.
9. FINN, Aidan et al., 2013. *Windows Server 2012 Hyper-V installation and configuration guide*. Indianapolis: Sybex. ISBN 978-1-118-54407-5. ISBN 978-1-118-48649-8.
10. HONEYCUT, Jerry, 2012. *Introducing Windows 8: an overview for IT professionals*. Farnham: O'Reilly. ISBN 978-0-7356-7050-1.
11. MARSHALL, David, Wade A Reynolds a Dave McCrory, 2006. *Advanced server virtualization: VMware and Microsoft platforms in the virtual data center*. Boca Raton: Auerbach Publications. ISBN 978-0-8493-3931-8.
12. MASON, Brian, 2012. *Microsoft System Center 2012 Configuration Manager: Administration Cookbook*. Birmingham: Packt Publishing. ISBN 978-1-84968-494-1.
13. MEYLER, Kerrie, 2013. *System Center 2012 Configuration Manager unleashed*. Indianapolis: Sams. ISBN 978-0-672-33437-5.

14. MICROSOFT, © 2015a. *Microsoft TechNet: Materiály pro IT odborníky [online]. [cit. 2015-03-18]. Dostupné z: <https://technet.microsoft.com/cs-cz/>*
15. MICROSOFT, © 2015b. *Windows Server 2012 R2 [online]. [cit. 2015-03-22]. Dostupné z: <http://www.microsoft.com/cs-cz/server-cloud/products/windows-server-2012-r2/>*
16. MINASI Mark et al., 2014. *Mastering Windows Server 2012 R2*. Indianapolis: Sybex. ISBN 978-1-118-28942-6.
17. OLZAK, Thomas et al., 2010. *Microsoft virtualization: master Microsoft server, desktop, application, and presentation virtualization*. Boston: Syngress/Elsevier. ISBN 978-1-59749-431-1.
18. PANEK, William, 2013. *MCSA Windows Server 2012 Complete Study Guide: Exams 70-410, 70-411, 70-412, and 70-417*. Indianapolis: Sybex. ISBN 978-1-118-54407-5.
19. PETŘIVALSKÝ, Dan, 2007, *TCO, ROI za vším hledej peníze. CIO Business Wolrd [online]. 5. prosinec 2007, [cit. 2015-03-14]. Dostupné z: <http://businessworld.cz/ostatni/tco-roi-za-vsim-hledej-penize-2532>*
20. STANEK, William R., 2012. *Microsoft Windows 8 administration: pocket consultant*. Redmond: Microsoft Press. ISBN 978-0-7356-6613-9.
21. SMOOT, Stephen R a Nam Kee TAN, 2012. *Private cloud computing: consolidation, virtualization, and service-oriented infrastructure*. Waltham, MA: Morgan Kaufmann. ISBN 978-0-1238-4919-9.
22. TULLOCH, Mitch et al., 2013a. *Introducing Microsoft System Center 2012 R2 Technical Overview*. Redmond: Microsoft Press. ISBN 978-0-7356-8283-2.
23. TULLOCH, Mitch et al., 2013b. *Introducing Windows Server 2012 R2 Technical Overview*. Redmond: Microsoft Press. ISBN 978-0-7356-8278-8.
24. VOŘÍŠEK, Jiří a Jan POUR, 2012. *Management podnikové informatiky*. 1. vyd. Praha: Professional Publishing. ISBN 978-80-7431-102-4.
25. WATERFILL, Mark R. a Christopher A. DILWORTH, 2014, *BYOD: Where the Employee and the Enterprise Intersect*, *Employee Relations Law Journal*, 40, 2, s. 26-36, *Business Source Complete*, EBSCOhost, citováno 14. března 2015.
26. ZACKER, Graig, 2014. *Exam ref 70-410: installing and configuring Windows Server 2012 R2*. Redmond: Microsoft Press. ISBN 978-0-7356-8424-9.

Seznam obrázků

Obrázek 1: Optimalizace WAN, převzato z: Smoot a Tan (2012, s. 113).....	7
Obrázek 2: Typy virtualizace 1 a 2, převzato z: Finn at el. (2013, s. 6).....	21
Obrázek 3: Hyper-V architektura, převzato z Finn et al. (2013, s. 13).....	30
Obrázek 4: Nástroje z rodiny System Center, převzato z: Acevedo (2015)	41
Obrázek 5: Architektura VDI řešení, převzato z: Finn at el. (2013, s. 529).....	46
Obrázek 6: Celkový návrh řešení (zdroj: autor)	57
Obrázek 7: Návrh zapojení fyzické vrstvy (zdroj: autor)	58
Obrázek 8: Nastavení virtuálního stroje pro server STG02 (zdroj: autor).....	64
Obrázek 9: Microsoft Hyper-V® Server 2012 R2 (zdroj: autor).....	67
Obrázek 10: Návrh zapojení logické vrstvy (zdroj: autor)	70
Obrázek 11: Průvodce nasazení VDI infrastruktury (zdroj: autor).....	78
Obrázek 12: Rozhraní Remote Desktop Services (zdroj: autor)	79
Obrázek 13: Konzole Virtual Machine Manager (zdroj: autor).....	81
Obrázek 14: Konzole Configuration Manager (zdroj: autor)	83
Obrázek 15: Portál RemoteApp and Desktop Connection (zdroj: autor)	84

Seznam tabulek

Tabulka 1: SWOT analýza řešení virtuálních desktopů – silné a slabé stránky	17
Tabulka 2: SWOT analýza řešení virtuálních desktopů – příležitosti a hrozby.....	18

Tabulka 3: Licencování Windows Server 2012 R2, převzato z: Finn et al. (2013, s. 22) a Microsoft© (2015b)	29
Tabulka 4: Porovnání VDI scénářů, převzato z: Finn at el. (2013, s. 522)	47
Tabulka 5: Konfigurace serveru DC01.....	62
Tabulka 6: Konfigurace serverů STG01 a STG02.....	64
Tabulka 7: Konfigurace serverů HyperV01, HyperV02 a HyperV03	67
Tabulka 8: Standardní konfigurace virtuálních strojů v logickém návrhu.....	73
Tabulka 9: Finanční analýza - klasické řešení	89
Tabulka 10: Finanční analýza - virtuální řešení.....	90
Tabulka 11: Celkový souhrn nákladů a celková úspora (v tisících Kč).....	91

Přílohy

Příloha 1: Porovnání základních edic Windows Server 2012 R2 – limity a omezení

	Windows Server 2012 R2 Edice Datacenter	Windows Server 2012 R2 Edice Standard	Microsoft Hyper- V® Server 2012 R2
Maximální počet uživatelů	Založeno na licenci	Založeno na licenci	Neomezeno
Maximální počet SMB spojení	16 777 216	16 777 216	16 777 216
Maximální počet RRAS spojení	Neomezeno	Neomezeno	250
Maximální počet IAS spojení	2 147 483 647	2 147 483 647	50
Maximum 64 bitových soketů	64	64	64
Maximální počet operační paměti	4 TB	4 TB	4 TB
Připojení do domény	Ano	Ano	Ano
DirectAccess	Ano	Ano	Ne

Převzato z: Microsoft© (2015b).

Příloha 2: Porovnání základních edic Windows Server 2012 R2 – serverové role

	Windows Server 2012 R2 Edice Datacenter	Windows Server 2012 R2 Edice Standard	Microsoft Hyper- V® Server 2012 R2
Active Directory Certificate Services	Ano	Ano	Ne
Active Directory Domain Services	Ano	Ano	Ne
Active Directory Federation Services	Ano	Ano	Ne
AD Lightweight Directory Services	Ano	Ano	Ne
AD Rights Management Serv.	Ano	Ano	Ne
Application Server	Ano	Ano	Ne
DHCP Server	Ano	Ano	Ne
DNS Server	Ano	Ano	Ne
Fax Server	Ano	Ano	Ne
File Services	Ano	Ano	Limitováno

Hyper-V	Ano	Ano	Ano
Network Policy and Access Services	Ano	Ano	Ne
Print and Document Services	Ano	Ano	Ne
Remote Access	Ano	Ano	Ne
Terminal Services Application Sharing	Ano	Ano	Ne
Terminal Services Gateway	Ano	Ano	Ne
Web Services (IIS)	Ano	Ano	Ne
Windows Deployment Services	Ano	Ano	Ne
Windows Essentials	Ano	Ano	Ne
Windows Media Services support	Limitováno	Limitováno	Ne
WINS Server	Ano	Ano	Ne

Převzato z: Microsoft© (2015b).

Příloha 3: Porovnání základních edic Windows Server 2012 R2 – serverové funkce

	Windows Server 2012 R2 Edice Datacenter	Windows Server 2012 R2 Edice Standard	Microsoft Hyper-V® Server 2012 R2
RODC - read only domain controller	Ano	Ano	Ne
Automatic Virtual Machine Activation	Hostitel i host	Pouze jako host	Ne
Best Practices Analyzer	Ano	Ano	Ano
BranchCache Hosted Server	Ano	Ano	Ne
BranchCache P2P Cache	Ano	Ano	Ne
Windows Control Panel	Ano	Ano	Ne
Distributed File System Replication	Ano	Ano	Ne
Data Deduplication	Ano	Ano	Ne
ISCSI target support	Ano	Ano	Ne
DirectAccess	Ano	Ano	Ne

Dynamic Memory (in virtualization)	Ano	Ano	Ne
Failover Clustering	Ano	Ano	Ano
"Hot" add/replace RAM	Ano	Ano	Ano
IPAM (IP Address Management)	Ano	Ano	Ne
Microsoft Management Console	Ano	Ano	Pouze vzdáleně
Minimal Server Interface	Ano	Ano	Ne
Network Load Balancing	Ano	Ano	Ne
Support for Non-volatile Memory Express	Ano	Ano	Ano
Windows PowerShell	Ano	Ano	Ano
Server Core mode	Ano	Ano	Ano (pouze tento mód)
Server license logging	Ano	Ano	Ano
Server Manager	Ano	Ano	Pouze vzdáleně
SMB Direct and SMB over RDMA	Ano	Ano	Ano
Storage Management Service	Ano	Ano	Pouze základní souborový server
Storage Spaces	Ano	Ano	Ano
Volume Activation Services	Ano	Ano	Ne
Volume Shadow Copy Service	Ano	Ano	Ne
Windows Server Update Services	Ano	Ano	Ne

Převzato z: Microsoft© (2015b).

Podklad pro zadání DIPLOMOVÉ práce studenta

PŘEDKLÁDÁ:	ADRESA	OSOBNÍ ČÍSLO
Mercl Luboš	Kostnická 191, Pardubice - Svítkov	I1300387

TÉMA ČESKY:

Analýza využití Microsoft Virtual Desktop Infrastructure ve firemní síti

NÁZEV ANGLICKY:

Analysis of Microsoft Virtual Desktop Infrastructure Usage in the corporate network

VEDOUCÍ PRÁCE:

Mgr. Josef Horálek, Ph.D. - KIT

ZÁSADY PRO VYPRACOVÁNÍ:

Cílem práce provést analýzu a komparativní analýzu technického řešení nasazení virtuální desktopové infrastruktury v reálném firemním prostředí. Autor podrobně představí principy a druhy virtualizace se zaměřením řešení od Microsoft. V praktické části pak autor vybere nejvhodnější řešení nasazení a využití virtuální desktopové infrastruktury včetně analýzy finančních dopadů.

Návrh osnovy práce:

- 1) Úvod,
- 2) Analýza požadavků podniku,
- 3) Principy virtualizace,
- 4) Architektura infrastruktury virtuálních desktopů,
- 5) Návrh řešení pro středně velkou společnost,
- 6) Porovnání virtualizovaného a klasického řešení,
- 7) Závěr.

SEZNAM DOPORUČENÉ LITERATURY:

OLZAK, Thomas et al., 2010. Microsoft virtualization: master Microsoft server, desktop, application, and presentation virtualization. Boston: Syngress/Elsevier. ISBN 978-1-59749-431-1.

MINASI Mark et al., 2014. Mastering WIndows Server 2012 R2. Indianapolis: Sybex. ISBN 978-1-118-28942-6.

PANEK, William, 2013. MCSA WIndows Server 2012 Complete Study Guide: Exams 70-410, 70-411, 70-412, and 70-417. Indianapolis: Sybex. ISBN 978-1-118-54407-5.

CERLING, Tim, 2010. Mastering Microsoft virtualization. Indianapolis: Sybex. ISBN 978-0-470-44958-5.

AMARIS, Chris a Guy YARDENI, 2012. Microsoft System Center 2012 unleashed. Indianapolis: Sams. ISBN 978-0-672-33612-6.

Podpis studenta:

Datum:

Podpis vedoucího práce:

Datum: