Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Virtualizace-servery

Martin Slávik

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Martin Slávik

Informatika

Název práce

Virtualizace – servery

Název anglicky

Server virtualization

Cíle práce

Diplomová práce je tematicky zaměřena na problematiku využití serverové virtualizace v souvislosti se zvyšováním její kvality a zabezpečení

- objasnit teoretický princip serverové virtualizace
- zmapovat současnou úroveň virtualizačních služeb
- vymezit požadavky kladené na virtualizaci
- návrh virtualizačního prostředí
- formulace doporučení a závěrů.

Metodika

Použitá metodika zadané diplomové práce bude založená na studiu a analýze dostupných informačních zdrojů a existujících řešení se zaměřením na zvyšování kvality a zabezpečení virtualizačních řešení. V rámci práce budou objasněny teoretické principy virtualizace. Stěžejní pro vypracovaní závěrečné práce budou metody, nástroje a techniky využívané ve virtualizaci, zejména platforma Microsoft Azure a Hyper-V, využívaní virtualizace v praxi a požadavky, které musí virtualizační řešení splňovat. Současně bude Navrhované řešení zohledňovat identifikované požadavky a očekávání spojená s řešenou problematikou a její výhody a případné nevýhody oproti klasickému řešení. Následně budou na podklade syntézy teoretických poznatků a dosažených výsledku formulovány závěry diplomové práce a následně zobecněny pro další možná použití.

Doporučený rozsah práce

50 – 60 stran

Klíčová slova

server,virtualizace,microsoft Azure,VMware,Hyper-V,Windows server,datové centra

---

Doporučené zdroje informací

Kelbley John.: Microsoft Windows Server 2008 R2 Hyper-V. Computer Press 2011, 1.vyd.,978-80-251-3286-9

Marshall D, Reynolds W, McCrory D.:Advanced Server Virtualization: VMware and Microsoft Platforms in the Virtual Data Center. Auerbach Publications 2006, 1.vyd .,ISBN 978-08-493-3931-8

Ruest Danielle , Ruest Nelson.:Virtualizace. Computer Press 2010, 1.vyd.,ISBN: 978-80-251-2676-9

Šika Michal.:333 tipů a triků pro VMware. Computer Press 2012, 1 vyd.,ISBN:978-80-251-3659-1

Předběžný termín obhajoby

2017/18 LS – PEF

Vedoucí práce

Ing. Jiří Vaněk, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 22. 5. 2017

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 24. 5. 2017

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 26. 03. 2018

Čestné prohlášení

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

V Praze dne _____

Poděkování

Rád bych touto cestou poděkoval Ing. Jiřímu Vaňkovi, Ph.D., za konzultace a odborné rady při vedení diplomové práce.

Virtualizace – servery

Abstrakt

Práce se zabývá tematikou serverové virtualizace. Popisuje historický vývoj služby, poskytování výhody oproti hardwaru a hlavní serverové virtualizační platformy. Porovnává virtualizační platformy Hyper-V a VMware a posuzuje technologii nejvhodnější pro firmy, které začínají migrovat IT infrastrukturu do virtuálního prostředí, nebo cloudu. Ponouká doporučená nastavení, která zlepšují výkon virtuálních strojů.

Klíčová slova: server, virtualizace, Microsoft Azure, VMware, Hyper-V, Windows server, datová centra

Server virtualization

Abstract

The thesis deals with the topic of server virtualization. Describes historical service development, providing benefits over hardware and the main server virtualization platform. It compares the Hyper-V and VMware virtualization platforms and assesses the technology most suited for businesses that are starting to migrate the IT infrastructure to a virtual environment or cloud. It offers recommended settings that could improve the performance of virtual machines.

Keywords: server, virtualization, Microsoft Azure, VMware, Hyper-V, Windows server,data center

Obsah

1 Úvod

Rozvoj IT technologií neustále postupuje. Trend zbavit se drátů a jakýchkoliv jiných omezení začíná být samozřejmostí. Neustále roste potřeba nepřetržité dostupnosti a vysoké spolehlivosti jednotlivých aplikací. Zároveň se firmy snaží minimalizovat své náklady. Jedním z možných řešení dané problematiky je použití virtualizací.

Virtualizace je oblast IT která, v současné době významně ovlivňuje trh s informačními technologiemi. Počátky virtualizace sahají do 60. let minulého století. V současné době dochází k masivnímu rozvoji virtualizace a rozšiřování oblastí, kde se virtualizace vyskytuje a využívá.

Virtualizace se již nevyužívá pouze ke konsolidaci datových center, nýbrž se začínají již prosazovat techniky využití virtualizace stolních počítačů, aplikací a datových uložišť. Diplomová práce je zaměřená na oblast serverové virtualizace, která je v současné době nejrozšířenější. Rovněž se zabývá představením principů virtualizace. V oblasti serverové virtualizace se jedná zejména o virtualizační platformy Microsoft Hyper-V a VMware ESX Server. Práce opisuje výhody ale i nevýhody virtualizačního řešeni za pomoci dané platformy. Získané informace mohou sloužit jako podklad pro rozhodování lidem zodpovědným za směrování IT oddělení, kterou ze nabízených variant zvolit, popřípadě pomoci k rozhodnutí aplikace i data přenést do virtualizačního prostředí a využít plný potenciál virtualizačního prostředí.

Virtualizace se stala velice populární a žádanou službou zejména kvůli svým výhodám, ať už se jedná o virtualizaci serverovou, virtualizaci na úrovni desktopů nebo samotných aplikací. Trendem současné doby se stává virtualizace infrastruktury. Jedná se o způsob, jak mohou firmy snížit své náklady, vznikající provozem hardwaru, pro který nemají 100 % využití. Virtualizace má podstatně širší využití, pro které se oplatí pro ni sáhnout.

V diplomové práci jsou shrnuty základní pojmy serverové virtualizace, nastiňuje výhody aplikace daného způsobu řešení, opisuje a hodnotí servery a software, nevyhnutný pro vytvoření vlastního virtuálního řešení.

2 Cíle práce a metodika

2.1 Cíl práce

Diplomová práce je tematicky zaměřena na problematiku využívání serverové virtualizace. V spojitosti se zvyšováním její kvality a zabezpečení, jejích dílčích cílů můžeme rozdělit na:

- objasnění teoretického principu serverové virtualizace
- zmapování současné úrovně virtualizačních služeb
- vymezení požadavků kladených na virtualizaci
- navržení virtualizačního prostředí
- formulování doporučení a závěrů.

2.2 Metodika

Použitá metodika zadané diplomové práce je založená na studiu a analýze dostupných informačních zdrojů a existujících řešení se zaměřením na zvyšování kvality a zabezpečení virtualizačních řešení. V rámci práce jsou objasněny teoretické principy virtualizace. Stěžejní pro vypracovaní závěrečné práce, budou metody, nástroje a techniky využívané ve virtualizaci, zejména platforma Microsoft Azure a Hyper-V, využívaní virtualizace v praxi a požadavky, které musí virtualizační řešení splňovat. Současně bude navrhované řešení zohledňovat identifikované požadavky a očekávání spojená s řešenou problematikou a její výhody a případné nevýhody oproti klasickému řešení. Následně budou na podklade syntézy teoretických poznatků a dosažených výsledku formulovány závěry diplomové práce a následně zobecněny pro další možná použití.

Pro vlastní řešení byla zvolena následující metodika:

1. Sumarizace dostupné lieratury na základe studia dostupných informačních zdrojů, literární i internetové, dotýkající se dané problematiky realizace teoretických principů serverové virtualizace, definice, výhod a nevýhod a zabezpečení dat.

2. Rozbor získaných informací, jejich třídění a následná analýza virtualizačního řešení.

3. Vyhodnocení dostupných nástrojů a hodnocení technické stránky platforem určených pro virtualizaci serverů, jako například Microsoft hyper-v, Microsoft Azure a VMware, které ovlivňují zavedení virtualizace.

4. Shrnutí a třídění dostupných zdrojů virtualizace v praxi.

5. Z vybraných řešení jsou v práci uvedeny ty, které nejlépe splňovali podmínky zadané v diplomové práci.

6. Vlastní návrh řešení a zlepšení v rámci vytipovaného nástroje a zobecnění pro další použití na základě rozboru dostupných materiálů a získaných informacích o virtualizaci ve firemním prostředí.

3 Teoretická východiska

3.1 Historie

Pojem virtualizace se začal používat již od 60. let minulého století. V té době se využívali sálové počítače IBM mainframe S/360 a operační systém CP-40. Umožňovalo to současné spuštění až čtrnácti virtuálních strojů. Virtualizace byla postavena na programové vrstvě, která přímo komunikovala s fyzickým zařízením počítače a zajišťovala virtualizaci ostatních součástí počítače, tedy procesoru, paměti, síty a disky. Jednotlivé virtuální počítače byly spouštěny jako procesy hypervisoru. Uživatel si pak mohl ve svém virtuálním počítači instalovat samostatný operační systém a v něm si pak spouštět aplikace.

Proti řešení, které nabízelo IBM, však mluvil požadavek na konkrétní hardwarovou podporu, po které se razantně zvýšila cena za využívání virtualizace. Následně byla vytlačena příchodem osobních počítačů, které v té době ponoukli stejný výkon za menší investici.

Potřeba virtualizace se obnovila až po zvýšení výkonů osobních počítačů a serverů. Stále zde setrvávala nedůvěra v tuto technologii. Virtualizace je v podstatě další vrstva mezi hardwarem a systémem. Nastávali tak otázky ohledem stability a dopadu na výkon systémů.

Dalším otazníkem byla otázky podpory od vydavatele největšího dodavatele operačního systému pro platformu x86, Microsoft. Microsoft byl ale přeběhnut firmou VMware, která se stala rozšířeným standardem ohledem virtualizace pro platformy x86.

Microsoft přišel se svou novinkou až v roku 2008. Jednalo se o technologii Hyper-V a byla součástí nového operačního systému Microsoft Windows Server 2008 x64bit, ve třech verzí Standard,Enterprise a Datacenter. Jedná se o podporu pouze u 64-bitových procesorů AMD, později i firmy Intel.

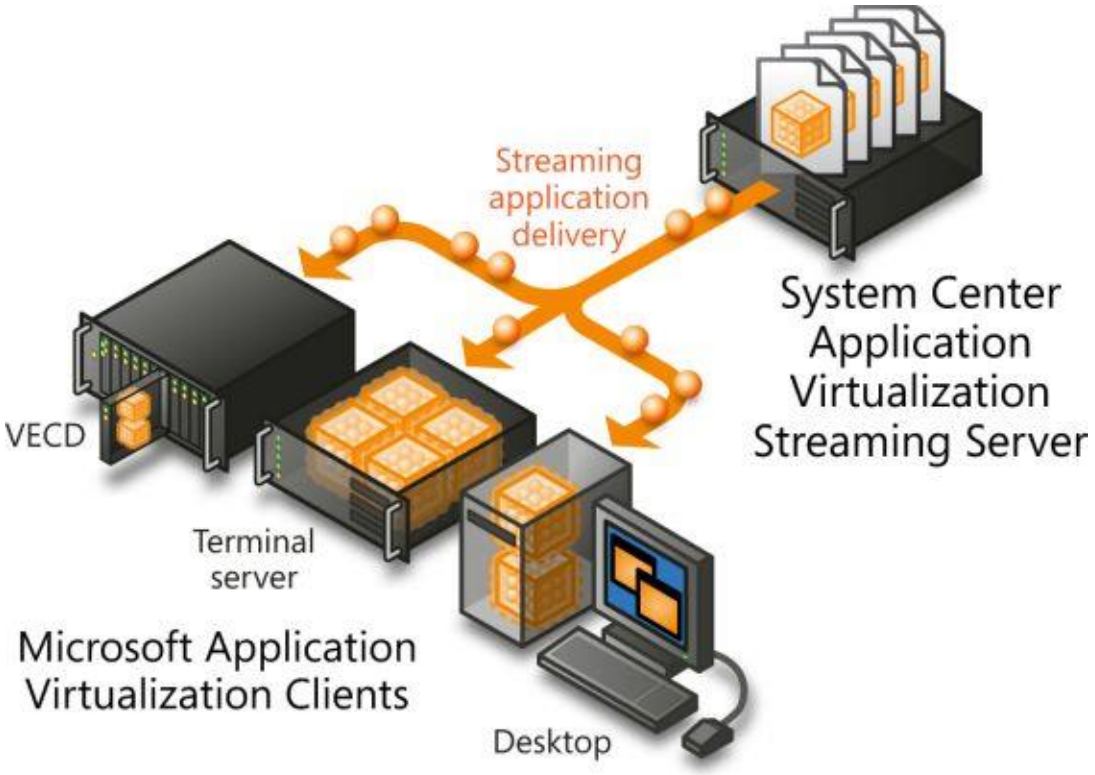
V současné době jsou řešení firmy VMware (ESX Server 3.x) a řešení firmy Microsoft (Hyper-V) považovány za standard v oblasti virtualizace serverů založených na Intel, resp. AMD procesorech. Firmu VMware má větší zkušenosti se specializací v oblasti virtualizace a stále ještě mírný technologický náskok před ostatními konkurenty. Microsoft má svoje postavení na trhu s operačními systémy, kancelářskými produkty apod. Rovněž má firma Microsoft prostředky, jak svůj produkt prosadit na trhu.

Oba způsoby řešení jsou však v současnosti již stabilní a provozovatelná a obě společnosti budou svá řešení i nadále podporovat a rozvíjet. V dohledné době cca 4 let nelze předpokládat, že by ať už jeden nebo druhý výrobce přišel s takovou novinkou, která by mu zajistila

okamžitou a silnou technologickou převahu. Obě řešení budou koexistovat a maximálně budou vznikat stále dokonalejší nástroje na vzájemnou konverzi virtuálních serverů mezi nimi. Váhání v dnešní době pouze znamená oddálení poznání toho kouzla, které mu virtualizace přináší. (1)

3.2 Současné trendy

V dnešní době je již jasné, že odpověď na otázku „zda virtualizovat a případně co", s trochou nadsázky by mohla znít „virtualizovat všechno, co je možné". Určitě je pravda, že prostředí každé společnosti je specifické, ale zkušenosti potvrzují, že většinu systémů lze provozovat jako virtuální servery. Samozřejmě existují jednotlivá omezení – technologická, provozní, ekonomická. Současné virtualizační technologie nepodporují např. více než emulaci čtyř procesorů, nepodporují připojení některých periferií atd. Nicméně hrubý odhad hovoří, že až 90 % serverů u typického zákazníka virtualizovat lze. Toto číslo potvrzuje i studium virtualizace pro zákazníka (Feasibility study průzkum enterprise prostředí, datová centra, SAN infrastruktura), která analyzovala možnost virtualizace cca 70 serverů, na kterých již končila HW podpora. Výsledkem studie bylo hodnocení – pouze 4 servery nebyly pro danou virtualizaci vhodné. V rámci této studie byl počítán i „business case“ pro tři různé alternativy – virtualizace, náhrada novým HW, nákup extra podpory. Pokud byly do výpočtu zahrnuty i náklady na provoz v datovém centru, cena práce při případných reinstalacích, příp. cena za nový HW a jeho maintenance, tak varianta „virtualizace" byla asi o 20 % levnější než druhá v pořadí (náhrada novým hardware). (1)



Obrázek 1- princip virtualizace

3.3 Princip virtualizace

Virtualizace poskytuje možnost, aby na jednom fyzickém serveru (na jednom hardware) běželo více oddělených serverů s vlastním operačním systémem. Fyzický server každému takovému virtuálnímu serveru emuluje virtuální hardware (procesor, paměť, disk, síťová karta, mechaniky, periferní zařízení a další). Samotnou skutečnost, že je server virtualizovaný, však zákazník na první pohled nepozná. Má samostatný server s procesory, pamětí a dalšími komponentami, na tom mu běží konkrétní operační systém dle jeho volby, má k němu plný přístup a pracuje s ním, jako by jeho operační systém běžel na vlastním hardware.

S touto koncepcí přišla u svých sálových počítačů, již v šedesátých letech dvacátého století, firma IBM. Výhoda tohoto řešení spočívala stejně jako dnes ve vytvoření několika zdánlivých počítačů v rámci jednoho fyzického. (3)

Virtualizace ve svých začátcích znamenala především hledání možností, jak se systémů, které byly schopné zpracovávat jen jeden úkol v konkrétní okamžik, vytvořit vícevláknová zařízení, která by jednotlivé operace prokládala, a tím lépe využívala možností tehdejšího hardwaru. Jedním z prvních strojů využívající virtualizaci byl počítač IBM 704 s technologií Compatible Time Sharing System. Další vývoj v této oblasti nastavil víceuživatelská prostředí jako jakýsi standard a virtualizace se v těchto letech začala podobat tomu, jak ji známe dnes. Systém byl postaven na dispečeru nazývaném „virtual machine monitor“, který měl přímý přístup k fyzickým prostředkům počítače (hardwaru) a následně spravoval jednotlivé virtuální počítače. Systém postaven na principu dispečera dnes nazýváme jako hypervisor – jednoúčelový „tenký“ operační systém vyvinutý a vyladěný pro virtualizaci. Hypervisor je zodpovědný za rozdělování celkového výpočetního výkonu, management paměti a management I/O operací.

Osobní počítače založené na x86 (intelovských) procesorech dlouho o něčem podobném nemohly uvažovat, jelikož výpočetní výkon ani kapacita paměti těchto strojů na něco podobného jednoduše nestačily. Vývoj ale od té doby značně pokročil, a tak jako jedna z prvních firma VMware, později následovaná množstvím dalších společností včetně opensource komunity, přišla s řešením. Vytvořila v počítači skutečném počítač virtuální. (3).

Serverová virtualizace začala tak, že virtualizační produkty pracovaly nad obecnými operačními systémy. Obecný operační systém však bude mít vždy vyšší režii, než jednoúčelový tenký operační systém vyvinutý a vyladěný pro virtualizaci. Takovýto tenký operační systém se označuje jako hypervisor. Vlastní virtualizaci obstarává pro každý virtuální server samostatná komponenta VMM – Virtual Machine Monitor, zajišťující komunikaci mezi virtuálním serverem a hypervisorem pracujícím přímo nad fyzickým hardwarem. V principu se v rámci VMM používají tři typy virtualizačních metod:

1. Softwarová emulace hardwaru (Full Virtualization-Binary Translation) – Výhodou emulace je absolutní nezávislost na hardwaru a možnost provozovat ve virtuálních serverech nezměněné operační systémy. Nevýhodou je výkonnostní režie.
2. Virtualizace s hardwarovou asistencí (Hardware Assisted Virtualization) – S rostoucími požadavky na virtualizaci se výrobci hardwarových komponet zaměřili na hardwarovou podporu virtualizace na úrovni procesorů, chipsetů, paměti, síťových karet a host bus adaptérů. Pomocí přenechání některých činností hardwarovým komponentám je možné minimalizovat virtualizační režii hypervisorů.

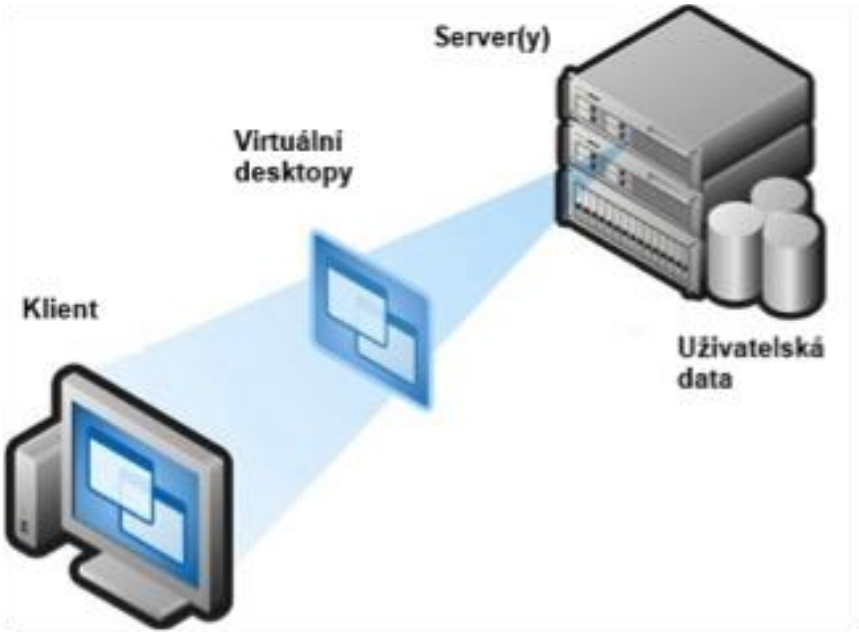
3. Paravirtualizace – Metoda virtualizace, která vyžaduje zásah do jádra operačního systému provozovaného ve virtuálním prostředí. V jádře paravirtualizovaného operačního systému existují speciální rutiny, které přesměrovávají určité instrukce, které by jinak byly vykonány hardwarem do hypervisoru přes tzv. root partition (často nazývanou Domain0, nebo kontrolní doménou). Výhodou paravirtualizace je obecně nižší výkonnostní režie než u plné softwarové emulace.

Každá z výše uvedených metod má své výhody i nevýhody a většina platforem používá více virtualizačních metod. (3)

Hypervisor VMware ESX používá všech třech metod a podle použitého hardwaru a nainstalovaného operačního systému ve virtuálním serveru se rozhoduje, které metody virtualizace bude pro konkrétní virtuální server používat.

Xen Server a Hyper-V využívají hardwarovou asistenci a paravirtualizaci, a proto tyto produkty vyžadují hardwarovou podporu virtualizace minimálně na úrovni procesoru. Pro paravirtualizaci musí mít procesor 64 bitovou podporu (Intel EM64T nebo AMD64), musí podporovat virtualizační instrukce (INTEL VT nebo AMD-V) a podporovat bezpečnostní rozšíření (NX – non eXecute nebo XD – eXecute Disable). U nových enterprise serverů patří tyto vlastnosti k běžnému standardu, a tudíž reálně nepředstavují žádná omezení. (3) (4)

Obrázek 2- virtualizace



Obrázek 2- virtualizace

3.4 Techniky realizování soudobé virtualizace

3.4.1 Plná virtualizace

U tohoto způsobu virtualizace se virtualizují všechny součásti počítače, běžící operační systém nemůže žádným způsobem rozpoznat, že nemá přístup k fyzickému technickému vybavení (hardware). Operační systém ani aplikační programy nepotřebují žádné dodatečné modifikace. Jedná se v podstatě o ideální stav, kdy dochází k plnému oddělení fyzické vrstvy, veškeré programy běží pouze na virtuálním hardware a přístup k fyzickému vybavení je vždy zprostředkován. To má samozřejmě řadu výhod – můžeme virtuální prostředí navrhnout tak, aby nám vyhovovalo (velikost paměti, typ procesoru, typ a kapacitu disku apod.). Programy jsou rovněž nezávislé na konkrétním technickém vybavení, jeho změna nemá na virtuální prostředí vliv (samozřejmě kromě výkonnostních charakteristik, tj. náš virtuální počítač může běžet rychleji nebo pomaleji, ale v každém případě poběží).

U plné virtualizace nemusí existovat žádná jednoduchá vazba mezi virtuálním prostředím a konkrétním hardware, na němž je virtuální počítač provozován. To umožňuje plnou přenositelnost – operační systém a aplikace běžící na procesoru Intel s architekturou IA-32 můžeme spouštět třeba na počítačích, vybavených procesory PowerPC. A následně je můžeme přenést na počítače vybavené jiným procesorem, aniž bychom provedli jedinou úpravu na úrovni virtuálního počítače. Podobně můžeme vytvořit virtuální počítač vybavený procesorem, který je teprve ve vývoji – návrh a ladění operačního systému a aplikací tak může probíhat paralelně s vývojem vlastního hardware.

Mezi profesionální systémy, které nabízí plnou virtualizaci počítačů s procesorem Intel patří Microsoft Virtual Server a VMWare ESX ServerTM.

3.4.2 Paravirtualizace

U plné virtualizaci dochází k oddělení fyzické a programové vrstvy, je tedy nemožné dosáhnout plného výkonu i v tom případě, že virtuální počítač je víceméně přesným obrazem hardware, na kterém běží (především nabízí identický procesor a další periferie). Virtuální monitor musí kompletně odstínit virtuální počítač od jakékoliv možné změny hardware. Toho lze dosáhnout emulací fyzického vybavení a většinu operací (včetně řady instrukcí procesoru, práce s pamětí, operace přístupu na disk a další) provádět ve vlastním software namísto toho,

aby ho přímo vykonával hardware. Nemá-li dojít k výraznému zpomalení virtuálního počítače, je virtualizace omezena pouze na virtuální prostředí, které se maximálně podobá tomu fyzickému.

Pokud však předpokládáme, že se alespoň některé komponenty virtuálního a fyzického počítače shodují (např. virtuální počítač bude vždy nabízet stejný procesor, nanejvýš s poněkud nižším výkonem), můžeme odstoupit od principu plné virtualizace a pracovat s tzv. paravirtualizací. Vyznačuje se tím, že provádí jen částečnou abstrakci na úrovni virtuálního počítače, tj. nabízí virtuální prostředí, které je podobné tomu fyzickému, na kterém virtuální počítač provozujeme. Virtualizace v tomto případě není úplná, některé vlastnosti např. vlastnosti procesoru mohou být omezeny a operační systém může rozpoznat, že běží ve virtuálním prostředí. Na druhou stranu skutečnost, že virtuální a fyzický hardware se příliš neliší, umožňuje, aby virtuální počítač v maximální míře využíval vlastnosti základního fyzického prostředí (nemusíme emulovat všechny komponenty virtuálního počítače).(5)

Paravirtualizace je široce využívána při tvorbě virtuálních prostředí nad procesory Intel (a AMD). VMWare workstation a Xen patří mezi neznámější systémy, které jsou postaveny na paravirtualizaci. Základní principy paravirtualizace si představíme na (zjednodušeném) modelu, který používá právě prostředí Xen.

Každý procesor pracuje alespoň ve dvou různých režimech – privilegovaném, který je přístupný pouze jádru operačního systému, a uživatelském, ve kterém běží všechny programy. Účelem privilegovaného režimu je zajistit, aby uživatelé měli kontrolovaný přístup k hardware a nemohli přímo provádět operace, které by měli možnost ohrozit jiné programy či integritu dat (např. přímý přístup na disk či složitější operace s virtuální pamětí). Pokud ale počítač virtualizujeme, potřebujeme navíc ještě jednu úroveň, na které poběží virtuální monitor. U plné virtualizace to není zapotřebí, u tohoto způsobu emulujeme celý procesor se všemi úrovněmi ochrany, v případě paravirtualizace je to však mnohem složitější. (5)

Virtuální monitor musí běžet na nejvyšším stupni ochrany. Na stejné úrovni však nemůže automaticky běžet operační systém, protože by mohl ovlivnit stav virtuálního monitoru. Jednou z možností je pozměnit kód operačního systému tak, že nebude provádět žádnou operaci, pro jejíž provedení je třeba oprávnění té nejvyšší úrovně. Provedení instrukce se změní ve volání příslušné funkce virtuálního monitoru, který nejprve zkontroluje, zda je operace povolena a následně ji provede tak, aby změnila stav virtuálního, nikoliv fyzického počítače. Problém může

vzniknout v přístupu instrukce čtení paměti. Jádro operačního systému předpokládá, že má přímý přístup k libovolné části fyzické paměti, to však samozřejmě v případě virtuálního počítače není možné. Protože nelze předem poznat, zda konkrétní operace čtení z paměti bude přistupovat k privilegovaným údajům, museli bychom nahradit v operačním systému všechny instrukce čtení - tím se ale začneme velmi nepříjemně přibližovat k plné virtualizaci. Další problém paravirtualizace spočívá v ochraně operačního systému před běžícími uživatelskými programy. Pokud bychom měli jen dvě úrovně ochrany (privilegované a neprivilegované), musel by operační systém virtuálního počítače pracovat neprivilegovaně, tím by však byl vystaven ohrožení ze strany aplikací. (5)

Paravirtualizace je tak možná jen díky tomu, že konkrétní procesory podporují více úrovní ochrany. Procesory Intel mají definovány 4 úrovně ochrany, tzv. okruhy (rings). Na nejvyšším stupni ochrany (ring 0) běží operační systém, uživatelské programy běží s nejnižším stupněm ochrany (ring 3). Ostatní stupně se běžně nevyužívají. Pokud použijeme paravirtualizaci, pak virtuální monitor pracuje na nejvyšším stupni ochrany, tj. v okruhu 0. Operační systém virtuálního počítače se posune o jeden stupeň (do okruhu 1), aplikační programy běží stále s nejmenší ochranou. Operační systém má stále vyšší úroveň ochrany než aplikační programy, na druhé straně už nemůže provádět operace, které vyžadují plně privilegovaný přístup. Úrovně ochrany můžeme využít i kromě výše zvýšené modifikace privilegovaných instrukcí – necháme operační systém ve virtuálním počítači provádět všechny instrukce, pokud však bude chtít provést "zakázanou" operaci (tj. takovou, na kterou teď nemá dostatečná oprávnění), pak dojde k přerušení a řízení převezme virtuální monitor. Ten operaci zkontroluje a provede ji tak, aby správně změnila stav virtuálního počítače. Není v principu třeba měnit operační systém, většina instrukcí běží přímo, pouze privilegované instrukce jsou výrazně pomalejší, protože je musí provést virtuální monitor. Operační systém však může zjistit, že běží ve virtuálním prostředí, protože může mít i na úrovni 1 možnost číst některé části paměti, které jsou ve virtuálním počítači jiné, něž ve fyzickém. Pro paravirtualizaci je proto třeba modifikovat některé součásti operačního systému, změny jsou však malé a dobře lokalizovatelné (zvlášť dobře je pak možné provést tyto změny u operačních systémů, k nimž jsou k dispozici zdrojové kódy; i proto začala být tak oblíbená (para)virtualizace v prostředí Linuxu).

Přístup k hardware je v prostředí Xen zajišťován vrstvou virtuálního monitoru (Virtual Machine Monitor, VMM). Nad touto vrstvou jsou pak vytvářeny virtuální počítače (Virtual Machines, VM). Jeden z těchto virtuálních počítačů má speciální postavení – v terminologii

Xenu se nazývá Doménou 0 (Dom 0). Operační systém, který běží v tomto virtuálním počítači, má přímý přístup k rozhraní virtuálního monitoru, může tedy definovaným způsobem měnit jeho stav a může vytvářet a rušit ostatní virtuální počítače běžící nad VMM. Další zajímavou vlastností Xenu (opět související s paravirtualizací) je to, že může konkrétnímu virtuálnímu počítači přímo zpřístupnit konkrétní rozhraní. Představme si, že v jednom z virtuálních počítačů běží uživatelský program, který intenzivně komunikuje s jiným počítačem prostřednictvím počítačové sítě. Pokud používá virtuální síťovou kartu, pak její propustnost je omezena a velmi zatěžuje procesor. Pokud ale příslušnému virtuálnímu počítači po dobu běhu tohoto uživatelského programu přímo exportujeme rozhraní na fyzickou kartu, pak může síťová komunikace probíhat plnou rychlostí, kterou podporuje příslušný hardware. Samozřejmě v takovém případě kartu může používat pouze tento virtuální počítač, to ale nemusí být na závadu (fyzický počítač může mít více síťových rozhraní, ostatní virtuální počítače pak sdílí ta ostatní).

I když má paravirtualizace oproti plné virtualizaci řadu výhod, potřebuje určité modifikace operačních systémů, co může zkomplikovat její nasazení (zejména u proprietárních operačních systémů) a vede k určité neefektivnosti. Intel proto v poslední době zavedl další systém podpory virtualizace v podobě tzv. Intel Virtualization Technology (IVT). Jedná se o rozšíření možností procesorů tím způsobem, že přibývá další úroveň ochrany (ring -1) pro VMM a přibývají speciální instrukce na této úrovni. Virtuální monitor tak může obsluhovat několik virtuálních počítačů, které již pracují v prostředí, které se neliší od toho, jež je k dispozici ve standardních procesorech bez podpory virtualizace. Operační systémy ve virtuálních počítačích není potřeba modifikovat, přitom zůstávají základní výhody paravirtualizace, tj. přímé vykonávání instrukcí virtuálního počítače fyzickým procesorem. (5)

3.4.3 Server

Pro případ, kdy všechny virtuální počítače sdílející hardware pracují se stejným operačním systémem, byl navržen koncept „Virtuálních privátních serverů Virtual Private Servers“, který implementuje např. systém VServer. V tomto případě je virtualizace realizována až na úrovni aplikačních programů. Mimo virtuálního monitoru běží na počítači jádro standardního operačního systému, v něm jsou pak spouštěny uživatelské virtuální servery, které toto jádro sdílí. Každý z virtuálních serverů tak nabízí pouze uživatelské prostředí (v němž

běží uživatelské programy). Vzájemná ochrana programů i virtuálních serverů je pak řešena standardními prostředky jádra operačního systému. Koncept VServeru využívá řadu standardních technik, které jsou běžně dostupné v Linuxu a jemu podobných operačních systémech, jejich kombinací pak dosahuje virtualizačního efektu. Pomocí systému "způsobilostí" (capabilities) chrání jednotlivé procesy mezi virtuálními servery (proces je oprávněn provést určité operace jen v prostředí jeho virtuálního serveru, nikoliv v prostředí základního operačního systému). Omezení přidělených zdrojů (resource limits) zase umožňuje zajistit, že i při chybě aplikace si žádný virtuální server nebude využívat větší část výkonu či paměti, než mu bylo přiděleno. Prostředí chroot společně s důsledným využitím atributů souborů pak zajišťuje bezpečný přístup k přidělené části systému souborů a v něm uložených souborech.

Pokud však v případě paravirtualizace je nutné modifikovat operační systém, v případě VServeru je nunto modifikovat aplikace, zejména pokud používají některé z vlastností (např. způsobilosti), na nichž je tento koncept postaven. Je třeba rovněž upravit celou řadu systémových programů, které poskytují informace o stavu celého systému. Např. systémové volání uptime udává, jak dlouho je operační systém aktivní. V případě VServeru by však volání uptime nemělo vracet čas běhu základního operačního systému, ale pouze virtuálního privátního serveru, v němž byl uptime volán. Jakmile je ale prostředí VServeru vytvořeno, má ze všech virtualizačních technik nejmenší režii a garantuje tak nejlepší využití hardware. (5)

3.5 Zabezpečení virtualizačního prostředí

Virtualizací se rozumí simulace normálního hardwarového prostředí, jejímž cílem je umožnit softwaru (včetně malwaru), aby se choval tak, jako běžně. Autoři malwaru se totiž zaměřují na jakákoliv slabá místa ve firemní síti, aby dosáhli svých nekalých cílů. Z tohoto důvodu jsou pak virtuální stroje podobně zranitelné vůči většině forem malwaru jako ty fyzické – ať jde o malware v podobě zákeřné e-mailové přílohy, drive-by-download (škodlivé kódy na webu, které se stáhnou při zobrazení v prohlížeči), botnetové typy trojanů, síťové červy a dokonce i cílené „spear-phishingové“ útoky.

Nezabezpečené virtuální prostředí často slouží jako otevřené dveře ke zbytku jinak zabezpečené sítě. Pokud například, útočník nalezne cestu do jednoho virtuálního stroje a zjistí, jak přeskočit k hypervizoru, získá tím přístup ke všem virtuálním strojům daného hostitele.

Kromě virtuálních desktopů by útočník potenciálně mohl získat přístup k jakýmkoliv zálohám či úložištím virtuálních dat, a tak by vlastně mohla být pro něj zpřístupněna veškerá data dané organizace.

Stále přetrvává mýtus, že virtuální stroje jsou ze své podstaty bezpečnější než ty fyzické. Pravdou je, že virtuální stroje bývají méně náchylné k hrozbám jako spyware a ransomware, ale jak už bylo uvedeno výše, tyto systémy lze stále infikovat jinými formami malwaru. Dá se říci, že virtuální stroje jsou jako brány k serverům a kyberzločinci usilují o přístup k datům na těchto serverech.

Vedle zabezpečení samotných virtuálních strojů je potřebné zajistit bezpečnost síťového provozu mezi virtuálními stroji a hypervizorem. V podstatě lze tak umožnit, aby jeden virtuální stroj „odposlouchával" provoz jiného virtuálního stroje, což znamená ohrožení soukromí a bezpečí.

3.5.1 Agent-based

Bezpečnostní software v koncových zařízeních, který má chránit fyzické počítače a servery, bývá znám jako „agent-based" řešení. V nevirtualizovaném prostředí bývají kompletní bezpečnostní řešení a antimalwarová databáze instalovány na konkrétním zařízení (serveru nebo desktopu).

Ve virtualizovaných prostředích však tyto typy produktů nebývají příliš efektivní. Každý virtuální stroj vyžaduje kompletního agenta a musí na něm být nainstalována kompletní antimalwarová databáze. Pokud například společnost vlastní 100 virtuálních strojů na jednom virtuálním hostiteli, musí mít 100 instancí bezpečnostního agenta a 100 instancí malwarové databáze na daném virtuálním hostiteli.

Jedním z důvodů, proč se k virtualizaci přistupuje, je snaha „zvládnout více práce a zároveň k tomu použít méně hardwaru". Pokud něco na poměr konsolidace působí negativně, výrazně se snižuje potenciál virtualizačního projektu přinést výhodnou návratnost investic. Kromě toho, že dochází k nehospodárnému duplikování bezpečnostního softwaru a databází, může „agent-based" řešení rovněž přispívat k dalšímu snižování výkonu nebo vést k potenciálním „dírám" v zabezpečení.

K vyřešení těchto problémů se zabezpečením virtualizace lze přistupovat různými způsoby. Vedle „agent-based“ přístupů, které jsme právě popsali, existují i řešení typu „agentless“ a „light agent“.

3.5.2 Agentless

Zatím, co u bezpečnostních produktů typu „agent-based“ je nutné kompletního bezpečnostního agenta a jeho databáze replikovat na všechny virtuální stroje všech hostitelů, „agentless“, bezpečnostní aplikace vyžadují pouze jednu instanci antimalwarové databáze. Ta se specializuje na bezpečnost a chrání všechny virtuální stroje, které na daném hostiteli běží. Ve srovnání s tradičním „agent-based“ zabezpečením kladou „agentless“ řešení mnohem menší nároky na centrální procesorovou jednotku hostitele, na paměť i úložiště. Vzhledem k tomu, že je na bezpečnost vyhrazen jen jeden virtuální stroj, eliminují se „skenovací bouře“ při hledání malwaru a „aktualizační bouře“ při aktualizaci bezpečnostních databází a aplikací. Navíc se nevyskytují zranitelné situace při čekání na aktualizaci („instant on gaps“).

Rovněž „agentless“ řešení nicméně mají určitá omezení. Technologie vShield umožňuje přístup k chráněným virtuálním strojům pouze na úrovni souborového systému. To znamená, že nelze implementovat jiná řešení pro ochranu koncových zařízení jako Application Control s technologií Dynamic Whitelisting, která jsou navržena tak, aby poskytovala další vrstvy intenzivní doplňkové ochrany.

Agentless řešení jsou k dispozici pouze s využitím technologie VMware vShield, a proto je nelze použít pro virtuální prostředí jako Citrix nebo Microsoft.

3.5.3 Light Agent

Toto bezpečnostní řešení propájí výhody přístupů „agentless“ a „agent-based“. Podobně jako agentless řešení využívá specializovanou virtuální aplikaci na úrovni hypervizoru, kde jsou uloženy databáze a provádí se skenování souborů. Tato konfigurace současně instaluje na každý virtuální stroj menší softwarové agenty, kteří jsou speciálně nastaveni tak, aby systém nezatěžovali a využívali méně procesní síly než tradiční softwarový agent. Výhodou je pak

skutečnost, že „těžká práce“ se odvede mimo virtuální stroje, avšak na každém z nich nadále zůstává přímé spojení k provádění pokročilých bezpečnostních úkonů.

I když je na každém virtuálním stroji „lehký agent“, nedochází k „aktualizačním bouřím“ – existuje totiž pouze jedna instance bezpečnostní databáze nacházející se ve virtuálním zařízení – a výskyt „skenovacích bouří“ se snižuje.

Řešení typu „Light Agent“ nabízejí bezpečnostní a řídící technologie, které „agentless“ produkty poskytnout nemohou, například:

- skenovat paměť a odhalit paměťově rezidentní malware
- poskytovat ovládací nástroje, které jsou obzvlášť užitečné ve virtuálních desktopových prostředích
- Host-based network security – včetně firewallu a systému prevence průniku (HIPS). (6)

3.6 Princip serverů

Server obecně spravuje webové stránky s Internetovými prezentacemi. V závislosti na programech a nastaveních může např. automaticky odpovídat na e-maily, spravovat databáze zákazníků, Internetové obchody, DNS atd.

Služby server poskytuje klientům, co označujeme jako model klient-server (odlišné modely jsou peer-to-peer nebo friend-to-friend). Služby mohou být nabízeny v rámci jednoho počítače (lokálně) nebo více počítačům pomocí počítačové sítě (síťové služby). Lokální službou může být například obsluha připojené tiskárny, správa automatických aktualizací a podobně.

Služby, které server poskytuje v lokální síti (LAN) mohou být například sdílení disků, tiskáren nebo schopnost ověřit uživatele podle jména a hesla (RADIUS). Ve větších sítích, jako je Internet, servery uchovávají a nabízejí webové stránky a poskytují další služby (DNS, e-mail atd.).

Poskytování služeb zajišťuje speciální program. V unixových systémech je označován jako démon (anglicky daemon), v Microsoft Windows pak jako služba (anglicky service), který s klientem komunikuje pomocí definovaného protokolu (SMB pro sdílení disků a tiskáren ve Windows, HTTP pro webový server a podobně).

Podle toho, zda je server vyhrazen jen pro poskytování služeb, nebo může sloužit i uživatelům servery rozlišujeme na:

- dedikovaný – vyhrazený pro speciální účely, bez přímého přístupu uživatelů
- nededikovaný – server slouží uživateli zároveň jako obyčejný počítač

Servery jsou dnes využívány ve velké míře na poskytování hostingů. Oproti běžnému hostingu se vyplatí vlastní server např. při individuálních požadavcích na nastavení parametrů hostingu. Např. někdo se může specializovat na rozesílání emailů svým zákazníkům – je proto vhodné objednat si virtuální server, kde má nájemce serveru pod kontrolou jak mailový server, tak prostor pro svou webovou prezentaci. (3)

3.6.1 Využití serverů v praxi

Servery jsou podstatní prvky počítačové sítě. Jejich pomocí si mohou ostatní počítače vyměňovat, sdílet ukládat či zálohovat data, provozovat sdílené počítačové aplikace, a prakticky provozovat cokoliv v rámci počítačové sítě. Některé typy serverů (ty které potřebují svůj vlastní výkonný hardware, jako je například souborový server, aplikační server) jsou provozovány v serverovně a potřebují velké zázemí, jiné mají podobu malého aktivního síťového prvku (například tiskový server).

V praxi se setkáme s tím, že se jako server označuje spíše hardware, na kterém je tento serverový software spuštěný. Zejména výrobci počítačů a dalšího hardware používají pojem server pro označení specializovaných, velmi výkonných počítačů určených pro provoz serverových programů. Existuje mnoho různých druhů serverů podle jejich použití. Některé z nich mohou běžet i na běžných zařízeních v kanceláři, například tiskový server bývá součástí tiskárny:

- Aplikační server – slouží k provozu aplikací
- Databázový server – slouží k provozu databáze
- Souborový server (File server) - slouží k ukládání souborů
- Faxový server (Fax Server) - obsluhuje přijímání a odesílání faxových zpráv
- Poštovní server (Mail server) – je server, který zajišťuje e-mailovou komunikaci
- Síťový server (Network Server) - zajišťuje fungování počítačové sítě
- Webový server – zajišťuje provoz a zobrazování webových stránek

- Tiskový server (Print server) - koordinuje tiskové úlohy na tiskárně
- Proxy server – zajišťuje a zprostředkovává přístup do jiné sítě

Výkonné serverové počítače, které běží v serverovnách nebo datových centrech se dělí podle své architektury na základní tři kategorie:

- Věžový server (Tower Server)
- Rackový server (Rack server)
- Blade server

Jestliže kdysi platilo, že každý server měl svůj vlastní hardware (serverový počítač), v současné době díky velkému nárůstu výkonnosti hardware dochází ke sdílení výkonu hardware a tzv. virtualizaci – stále více se tedy používají virtuální servery. Stejně tak je více patrná tendence, kdy si firmy své výkonné servery nespravují sami ve svých vlastích serverovnách, ale využívají služeb datových center (jako data hosting, privátní cloud a podobně). Zejména pro malé a střední firmy to znamená značné úspory a stejně tak zvýšení spolehlivost, dostupnosti a bezpečnosti. (4)

3.7 Systémy virtualizace

3.7.1 Hyper-V

Základním stavebním kamenem systému Hyper-V je virtualizační vrstva neboli hypervisor. Hyper-V, který ve své první verzi spatřil světlo světa v roce 2008 jako součást specifických edic Windows Serveru 2008. Další generace, dostupná jako role ve Windows Serveru 2008 R2, případně jako samostatný produkt Microsoft Hyper-V Server 2008 R2, který je k dispozici zdarma. Funkcionalitu doplnily technologie Dynamic Memory a RemoteFX, obsažené v Service Packu 1 pro Windows Server 2008 R2. Třetí generace Hyper-V, je integrovanou součástí Windows Serveru 2012 a klientského operačního systému Windows 8 Pro. Aktuálně je k dispozici Hyper-V coby integrovaná součást Windows Serveru 2012 R2 a Windows 8.1 Pro a Enterprise.

V rámci Hyper-V jsou podporovány následující oprační systémy:

- Windows Server od verze 2003 výše
- Windows Client od verze XP Professional SP2 výše

- SUSE® Linux Enterprise Server verze 10 a 11
- Oracle Linux 6.4 a vyšší
- Open SUSE 12.3
- Red Hat Enterprise Linux verze 5.5 a vyšší
- CentOS Linux 5.5 a vyšší
- Ubuntu 12.04 a vyšší
- FreeBSD 8.2
- Debian 7.0 a vyšší

Při využití Windows Server 2008 R2 Hyper-V na jednom fyzickém hostiteli můžete provozovat až 384 virtuálních hostů, osazených až 512 virtuálními procesory. V rámci Hyper-V clusteru lze dokonce provozovat až 1000 virtuálních strojů. (7)

Technologie Hyper-V umožňuje vytvořit a spravovat virtualizované výpočetní prostředí pomocí technologie virtualizace, která je součástí Windows Serveru. Instalace role Hyper-V nainstaluje požadované součásti a volitelně nainstaluje nástroje pro správu. Požadované součásti zahrnují hypervisor systému Windows, službu Správa virtuálních počítačů technologie Hyper-V, zprostředkovatele rozhraní virtualizace WMI a další součásti virtualizace, například sběrnici virtuálního počítače (VMbus), poskytovatele služeb virtualizace (VSP) a ovladač virtuální infrastruktury (VID).

Nástroje pro správu Hyper-V se skládají z:

- Nástrojů pro správu grafického uživatelského rozhraní: Správce technologie Hyper-V, modulu Microsoft Management Console (MMC) snap-in a připojení k virtuálnímu počítači, které poskytuje přístup k výstupu videa virtuálního počítače, takže můžete s virtuálním počítačem komunikovat.
- Konkrétní rutiny technologie Hyper-V pro Windows PowerShell. Windows Server 2012 zahrnuje modul Hyper-V, který poskytuje přístup přes příkazový řádek ke všem funkcím dostupný v grafickém uživatelském rozhraní a také funkcím, které nejsou dostupné pomocí GUI.

Technologie Hyper-V zahrnuje softwarový balíček pro podporované hostované operační systémy, který zlepšuje integraci mezi fyzickým počítačem a virtuálním počítačem. Tento balíček se označuje za integrační služby. Obecně platí, tento balíček nainstalujete do hostovaného operačního systému jako samostatný postupe po nastavení operačního systému ve

virtuálním počítači. Některé operační systémy však obsahují integrované vestavěné systémy a nevyžadují samostatnou instalaci. (9)

3.7.2 VMware VI3

VMware byl jedním z prvních pionýrů v oblasti serverové virtualizace na platformě x86 a v dnešní době je bezesporu leaderem trhu se serverovým a desktopovým virtualzačním softwarem. Již v roce 1999 uvedl svůj první virtualizační produkt VMware Workstation, což byl na tehdejší dobu vyloženě vizionářský počin. V roce 2001 VMware představil serverové virtualizační produkty VMware GSX Server a VMware ESX Server. GSX server se provozoval nad běžným operačním systémem, na rozdíl od ESX serveru, který běžel přímo nad hardwarem. V dnešní době se produkt GSX jmenuje "VMware Server" a je poskytován zdarma. ESX se i dnes jmenuje stejně a zdarma je k dispozici částečně omezená verze „ESX 3i Free", ostatní verze s enterprise vlastnostmi a podporou centrálního managementu se licencují. (4) (8)

Právě z toho důvodu VMware nazývá svůj aktuální produktový balík jako "Virtual Infrastructure 3", co je v podstatě softwarový balík obsahující hypervisor a sadu virtualizačních management nástrojů integrovaných do produktu "VMware Virtual Center", dnes přejmenovaného na "VMware vCenter". VMware navíc aktuálně uvolnil novou verzi své virtualizační infrastruktury, kterou přejmenoval na vSphere 4. Tato verze opět posouvá VMware na poli serverové virtualizace v datovém centru o významný kus před konkurenty, kteří usilovně, a někteří už celkem úspěšně, dohánějí dlouholetý náskok VMware. (9)

4 Analytická část

4.1 Serverová virtualizace a sítě

Virtualizace síťových rozhraní, respektive realizace spojení virtuálních serverů s okolím se děje prostřednictvím takzvaných virtuálních switchů, tedy specifických aktivních prvků, které však mají velké množství funkcí společných s fyzickými aktivními prvky. I na těchto zařízeních totiž lze definovat použití sítí VLAN za pomoci 802.1q VLAN tagingu, privátních sítí nebo určit pravidla pro základní zabezpečení komunikace.

Z pohledu virtualizovaných serverů (VS) je důležitá jedna věc. VS o této struktuře „neví“ – každý z nich je vybaven jednou nebo více síťovými kartami, které se z pohledu použitého operačního systému jeví jako „fyzické“ s vlastním ovladačem, MAC adresou a s přidělenou příslušnou IP adresou. Takové virtuální síťové rozhraní je proto plně funkční a prakticky nikdy neztratí konektivitu, protože virtuální switch je neustále spuštěný.

Poněkud komplikovanější je však připojení takového virtuálního přepínače do fyzického prostředí. Zde existuje několik možností. (11)

4.1.1 Zapojení s jednou fyzickou síťovou kartou

V této konfiguraci dva servery využívají virtuální switch prostřednictvím jediné fyzické síťové karty. Protože každý VS má vlastní kartu s unikátní MAC adresou, jedinečnou IP adresou a zároveň se virtuální switch chová jako běžný aktivní síťový prvek, je komunikace mezi zmíněnými servery a vnějším světem plně transparentní. Jestliže bude docházet k ovlivňování síťového provozu jednotlivých virtuálních serverů, závisí pouze na rychlosti fyzické karty sloužící jako uplink pro onen přepínač a také samozřejmě na intenzitě provozu jednotlivých VS.

V současné době, kdy již v podstatě není nabízen žádný server bez gigabitového rozhraní, ale už nejsou obavy o nedostatečnou propustnost síťového interfejsu pro virtualizovaná prostředí na místě. I ve výše uvedené konfiguraci, tedy u serveru s jednou fyzickou ethernetovou kartou, je však možné zajistit provoz VS v oddělených sítích, a to v případě, pokud jsou tyto segmenty rozlišeny pomocí VLAN. V takovém případě jsou pak na virtuálním přepínači vytvářeny takzvané skupiny portů. Každá z nich pak umožňuje připojit virtuální

server k patřičné VLAN. Režim portu fyzického aktivního síťového prvku, do kterého je připojena fyzická síťová karta serveru, by pak měl být nastaven do tzv. módu Trunk. (11)

4.1.2 Zapojení s více fyzickými síťovými kartami

Další možností zapojení virtuálního switche je nasazení s více fyzickými síťovými kartami v serveru. Funkce takového přepínače jsou přitom naprosto stejné jako v předchozím případě. Jediným, zato však významným rozdílem, je to, že je použito více fyzických síťových karet pro připojení do infrastruktury. Tento způsob dovoluje využít přenosové kapacity více fyzických karet najednou a sloučit je do jednoho „tunelu“ z důvodu zvýšení propustnosti datových toků z, respektive do virtuálních serverů. V případě vysoké koncentrace VS na jednom fyzickém stroji je taková konfigurace odborníky velmi doporučována, protože s rostoucím množstvím serverů na jeden virtuální switch rostou významně i požadavky na jeho propustnost.

Samozřejmostí při použití alespoň dvou fyzických síťových karet je rovněž možnost konfigurace typu fault-tolerant, tedy zajištění bez výpadkového provozu i v případě havárie jedné z fyzických síťových karet.

Ve všech uvedených případech je spojování fyzických síťových karet zajišťováno nainstalovanou virtualizační platformou. Každý virtuální server má jen jedno síťové rozhraní, takže není potřeba řešit specializované ovladače nebo software pro zajištění zmíněných funkcionalit na úrovni operačních systémů zmíněných serverů. (11)

4.1.3 Zapojení bez fyzické síťové karty

Třetí možností využití virtuálního switche je zapojení bez fyzické síťové karty. I když to tak nemusí na první pohled vypadat, jedná se o jedno z velmi používaných zapojení, a to především pro testovací účely anebo pro budování zabezpečených demilitarizovaných zón (DMZ). Virtuální switch bez fyzického propojení s vnějším světem umožňuje komunikaci bez omezení mezi virtuálními servery, jež jsou k němu připojeny.

Tímto způsobem je možné bez potíží vybudovat testovací prostředí například pro vývoj specifické aplikace s vazbou na doménové nebo jiné systémy, které je velmi obtížné nebo dokonce nemožné mít vedle sebe v jedné fyzické síti. Stejně tak je poměrně jednoduché tímto způsobem vybudovat bezpečné DMZ. Možnost zapojení virtuálních serverů v případě potřeby

vytvoření firewallu a zabezpečeného serveru v DMZ v rámci jediného fyzického serveru je znázorněn na příslušném obrázku. (11)

4.2 Dostupnost virtuálního prostředí v praxi

Termín vysoká dostupnost se používá zejména u serverů spojených v tzv. clusteru, tedy seskupení několika serverů (nodů) k zajištění vysoké dostupnosti služeb provozovaných v rámci již zmíněného clusteru. Při virtualizaci vzniká riziko ztráty dat z důvodu chyby hardwaru. Riziko je znásobeno počtem virtuálních serverů, které na daném fyzickém hostiteli byly provozovány. Z těchto důvodů se cluster považuje za nedílnou součást při stavbě virtuální serverové infrastruktury.

Pro začátek je klíčové určit, která služba má být poskytována v rámci vysoké dostupnosti. Pro Windows Failover Cluster, skupinu individuálních serverů, které pracují na zvýšení nezávislosti aplikacích a služeb, je totiž i samotný virtuální stroj služba. Je tedy nutné vše promyslet a rozhodnout, zda je klíčové zajistit vysokou dostupnost virtuálnímu stroji, nebo jen službě ve virtuálním serveru obsažené. Každý z těchto scénářů vyžaduje vytvoření a konfiguraci clusteru na jiné úrovni a má své specifické klady i zápory. Ve všech případech je společná podmínka – vždy je zapotřebí minimálně dvou fyzických hostitelů s nainstalovanou rolí Hyper-V.

Virtualizace ukazuje své výhody zejména v případech, kdy chceme zajistit vysokou dostupnost celku, a ne jenom specifických služeb, které jsou v rámci virtuálního serveru poskytovány. Můžou být využité aplikace a služby, které nejdou v rámci clusteru provozovat, jako například Active Directory nebo DNS. V těchto případech se musí cluster vytvořit na úrovni hostitelů a virtuální stroj je pak konfigurován jako služba, které cluster zajišťuje vysokou dostupnost.

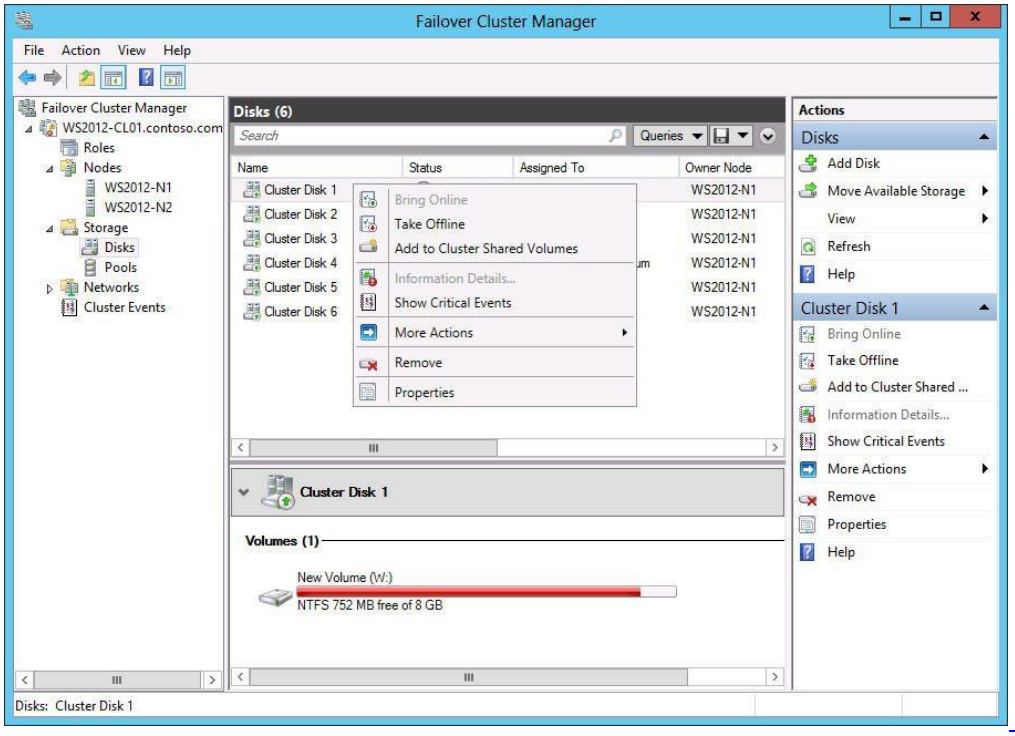
Přínosem clusteru pak je, že v případě havárie některého z nodů clusteru je automaticky ten samý virtuální server nastartován na jednom z dalších nodů. Další výhodou jsou pak přidané hodnoty, například u Hyper-V v2 tzv. Live Migration, která zajistí migraci virtuálních strojů v rámci clusteru bez výpadku služeb. Musí se ovšem počítat s tím, že jak zdrojový, tak cílový nod je ve stavu on-line.

Nevýhodou tohoto modelu je, že v případě výpadku nodu, na kterém virtuální server právě běží, trvá určitý časový rámec, než virtuální stroj nastartuje na jiném nodu v rámci clusteru. Takový výpadek pak může dosáhnouti několika minut.

Protože Windows Failover Cluster lze provozovat i uvnitř virtuálních serverů, můžete zajistit vysokou dostupnost i pro služby běžící uvnitř. Taková vysoká dostupnost je prakticky absolutní a je schopna zajistit, aby služba byla pro uživatele dostupná vždy a nepřerušila se ani v případě výpadku právě aktivního nodu. Typicky a nejčastěji jsou takto clusterovány například souborové služby jako File Services, Distributed File System (DFS) či služba DHCP. Všechny tyto služby jsou pro dnešní moderní společnost naprosto klíčové a běžný uživatel není schopen vykonávat svou práci, aniž by měl k dispozici právě sdílené soubory.

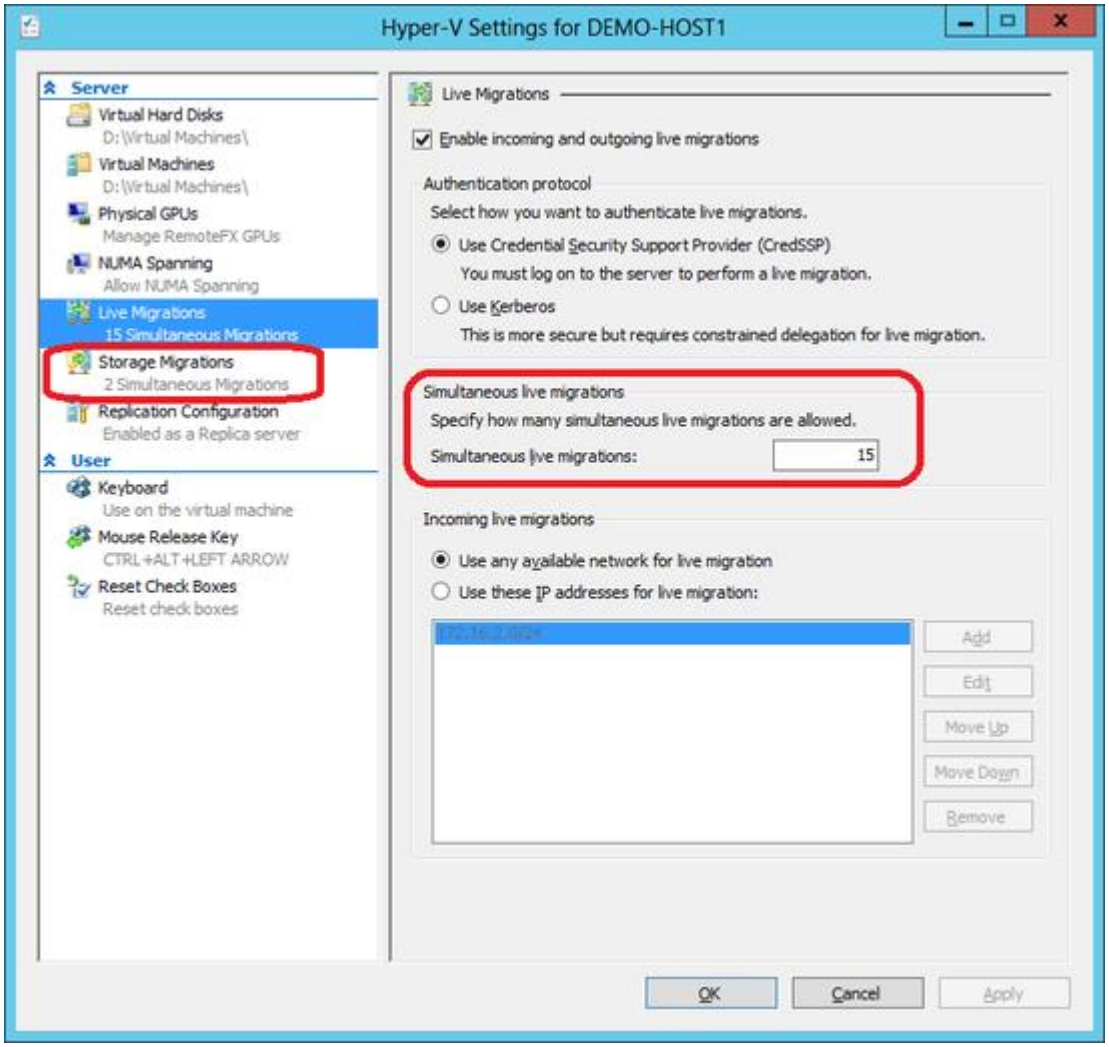
4.2.1 Přínosy Windows Failover Cluster a Hyper-V

Clustered Share Volume – novinka ve Windows Server 2008 R2 nabízí možnost vytvořit pomocí Windows Failover Cluster úložiště na diskovém poli, do kterého budou schopny zapisovat všechny nody v clusteru. Toto úložiště je následně zobrazeno jako mountpoint v C:\Clustered volumes\jméno svazku



Obr.3 Clustered Share Volume

Live Migration – novinka v Hyper-V v2 přináší ve spojení s Clustered Share Volume možnost přenášet virtuální servery mezi jednotlivými nody clusteru za plného chodu. Možnost má využití v případech, kdy se musí resetovat fyzický hostitel, ale nemůžou se zastavit virtuální servery na něm běžící. Při tomto druhu migrace nedochází k výpadkům poskytovaných služeb a koncový uživatel nic nepozná. (10)



Obr.4 Live Migration- Migrace virtuálních strojů v rámci clusteru

Migrací virtuálního stroje se rozumí akce, kdy má virtuální stroj použít jako svého hostitele jiný nod v rámci clusteru. Typy migrací jsou:

Live Migration – vyžaduje speciální konfigurace síťové konektivity a tzv. Clustered Share Volume. Tato migrace přináší výhodu v bezvýpadkovém průběhu. Virtuální stroj je v takovém

scénáři stále aktivní do poslední chvíle na původním nodu a až je cluster plně připraven na přesun, dojde k jeho přepnutí. Výpadek se pak měří v jednotkách paketů. Virtuální disky zůstávají stále v rámci jednoho jediného uložiště.

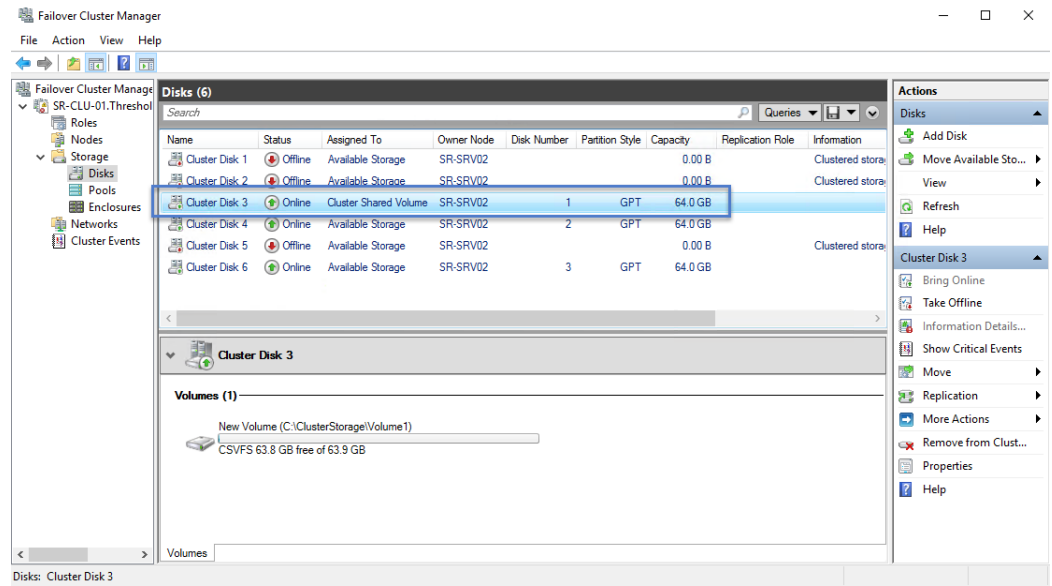
Quick Migration – v tomto typu migrace se virtuální server nejdříve uloží do stavu „saved state“ a dojde k jeho plné migraci včetně virtuálních disků na jiný nod v rámci clusteru. Migrace pak způsobí dočasné odpojení celého virtuálního serveru a jeho migrace trvá i několik minut v závislosti na velikosti virtuálního disku a RAM paměti.

Samozřejmostí jsou i migrace pouze virtuálních disků do jiného úložiště. To je užitečné, v případě, když například nestačí výkon diskového subsystému nebo dochází místo na aktuálně používaném diskovém poli. Konfigurační soubory pak zůstávají stále na původním hostiteli, mění se pouze úložiště virtuálních disků. (10)

Všechny typy migrací lze použít, pouze pokud virtuální server používá virtuální disky VHD. Pokud je k virtuálnímu serveru připojen tzv. pass-through disk neboli fyzický disk či LUN napřímo, migrace virtuálního serveru není umožněna. Pass-through disky tedy nejsou vhodnou konfigurací v rámci failover clusteru právě z výše zmíněných důvodů.

Správa Windows Failover Cluster

Správa Windows Failover clusteru včetně všech jeho přidružených aplikací, jako jsou virtuální stroje, probíhá z mmc konzole například přes Server Manager. Samostatná konzole pro správu je dostupná v nabídce nástrojů pro správu na tom kterém nodu clusteru.(10)



Obr.5 Správa Windows Failover

Konzole se dělí na tři částí. V pravé části správce nalezne stromovou strukturu jednotlivých komponent Windows Failover Clusteru, jako jsou nody clusteru, clusterované aplikace, nakonfigurované Clustered Share Volumes, uložiště v rámci diskového pole či sítě, které jsou do clusteru přidány.

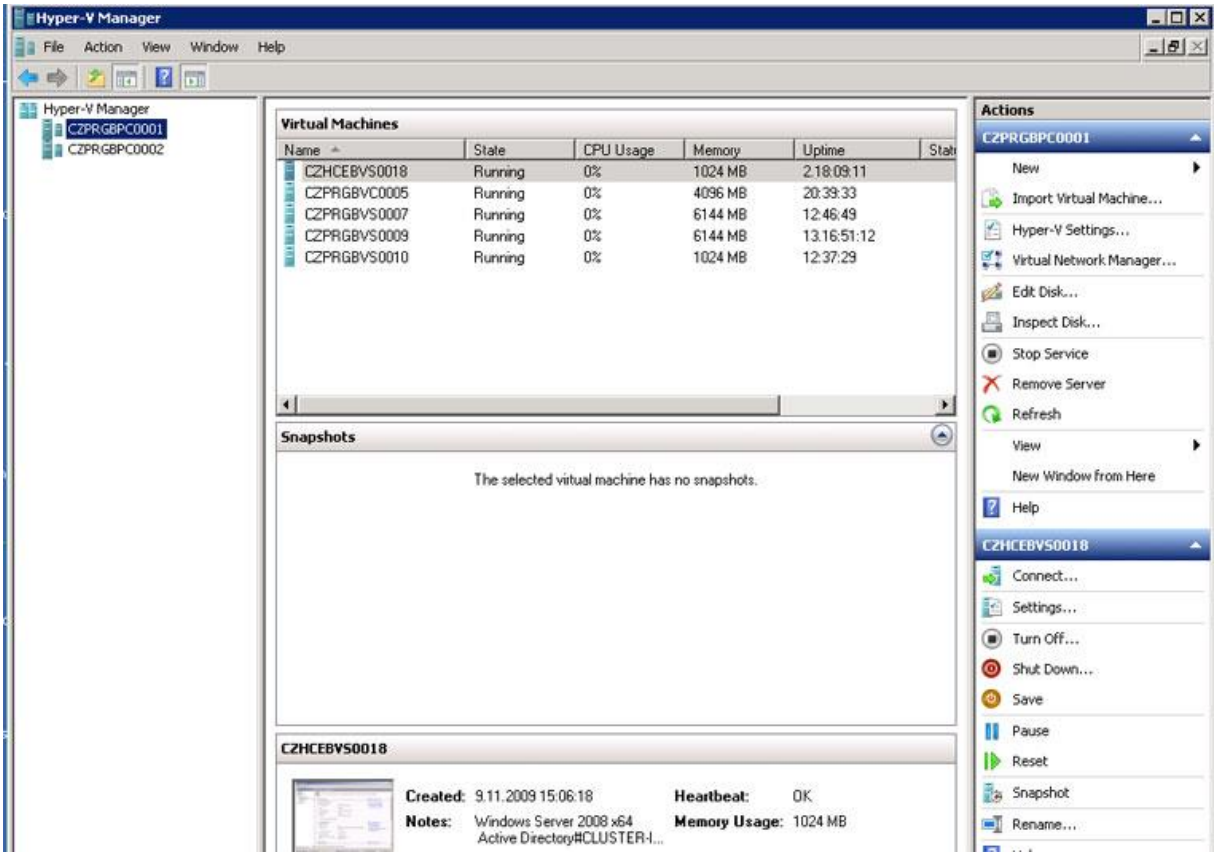
V prostřední části je pak výpis obsahu té které oblasti a napravo se dynamicky zobrazují úkoly či nástroje podle vybrané položky. Zároveň zde najdete i obecné nástroje pro celý cluster. Z tohoto akčního menu může správce ovládat výše zmíněné Live Migration nebo Quick Migration procesy, nastavovat parametry k jednotlivým položkám tak, aby přesně splňovaly požadavky společnosti.

Pro správu z klientské stanice, jako jsou třeba Windows 7, může administrátor použít mmc snap-in, který si doinstaluje pomocí Remote Server Administration Tools (RSAT). Případně je možné nasadit sofistikovanější nástroj z rodiny System Center – Virtual Machine Manager, který umožňuje spravovat nejen virtualizační infrastrikturu s Hyper-V, ale i konkurenční VMware. (10)

4.2.2 Hyper-V Manager

Základní Microsoft Management Console (zkráceně MMC) je zdarma dostupný konzolový nástroj. Tato konzole je k dispozici automaticky s instalací Hyper-V role na Windows Server 2008 (R2), či na klientských operačních systémech instalací Remote Server Administration Tools (zkráceně RSAT).

Z jednoho hostitele lze spravovat všechny virtuální servery či hostitele ve firemní IT infrastruktuře. Podmínkou je, že virtualizační technologie musí být Hyper-V nebo Hyper-V R2 server. Vybrání konkrétního fyzického hostitele se nachází v prostřední části, kde je aktuální výpis virtuálních strojů, které hostuje, jejich stav, aktuální zatížení a uptime. Ve střední části je dostupný náhled „monitoru“, a pokud k virtuálnímu stroji přísluší i nějaké snímky (snapshot), jsou zde také vypsány. V pravé části se nachází akční položky, a to jak z pohledu konkrétního virtuálního stroje, tak i z pohledu globálního. Pro základní administraci menšího virtuálního prostředí je toto řešení dostačující, ale ve chvíli, kdy se spravuje rozsáhlejší prostředí, či snad dokonce heterogenní virtuální prostředí – tedy Hyper-V v kombinaci s jinými virtualizačními technologiemi (např. VMware ESXi) – je zapotřebí rozsáhlejšího řešení. Nástroj, který je určen

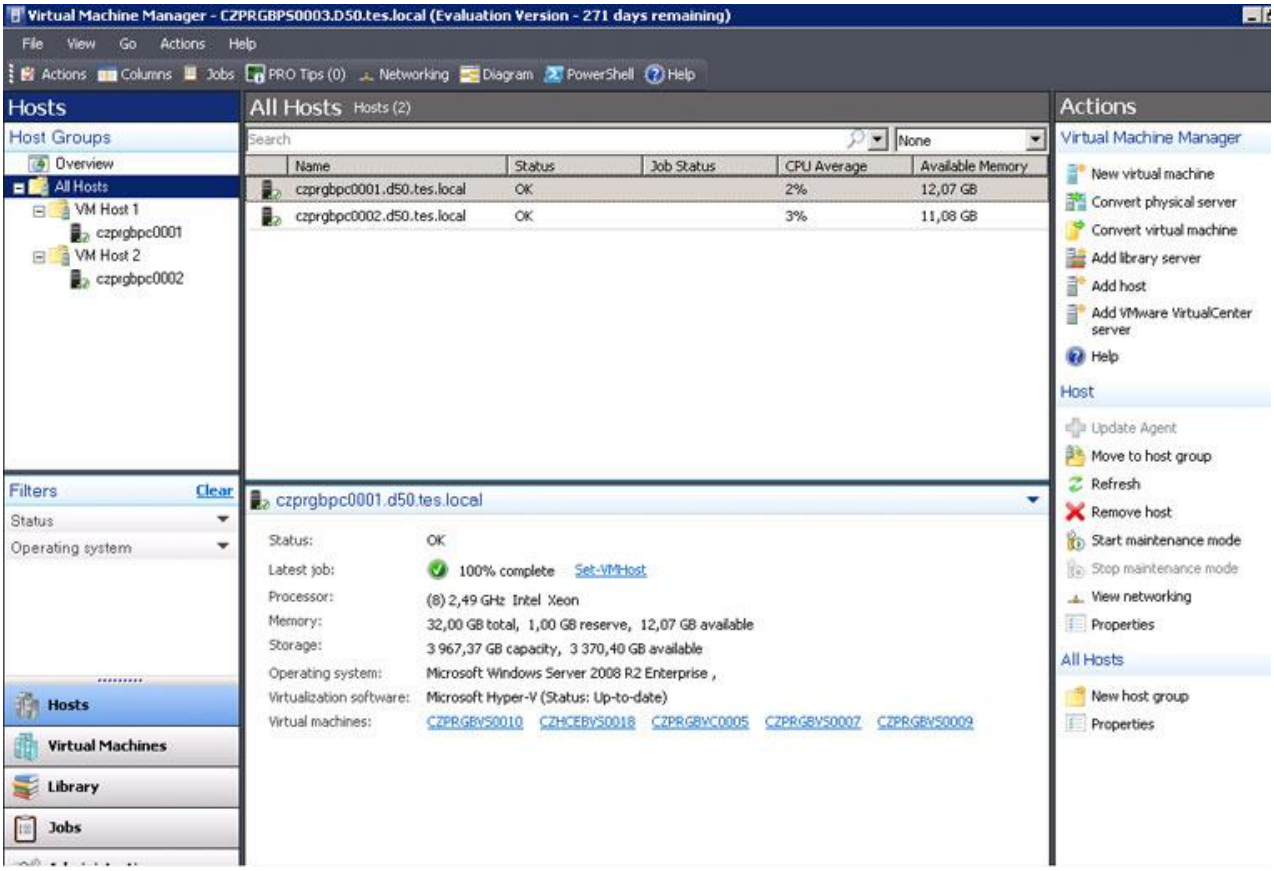


Obr.6 Hyper-V MMC konzola

IT profesionálům přímo z dílny Microsoftu spadá do rodiny produktů System Center a nese plné jméno System Center Virtual Machine Manager (zkráceně SCVMM). (12)

4.2.3 System Center Virtual Machine Manager

Pod tímto produktovým označením se skrývá profesionální produkt, který je určen pro střední a velké virtuální IT infrastruktury (a jejich správce). Jeho možnosti jsou značně rozšířeny oproti Hyper-V Manageru. Pro společnosti, které chtějí mít proaktivní, nikoliv jen reaktivní prostředí, je pak nutností.



Obr.7 System Center Virtual Machine Manager konzola

SCVMM Server

Standardně se instaluje na server, který je určen pro dohled a správu virtuálního IT prostředí. Pro svůj běh vyžaduje buď již existující SQL Server, popřípadě přítomnost SQL Server Express. Tato volba je přímo v instalačním průvodci. K SCVMM serveru se dále přidává System Center Operations Manager, který je s SCVMM schopen úzce kooperovat. Pro instalaci je nutné mít k dispozici alespoň jeden doménový řadič Active Directory a zároveň SCVMM Server musí být členem této domény.

SCVMM Console

Může se instalovat na libovolný klientský či serverový operační systém, který splňuje minimální nároky pro instalaci. Tato konzole se přes síť připojuje k SCVMM serveru a je plně

schopna jej administrovat. Podmínkou je příslušnost počítače/serveru ve stejné doméně, ve které je SCVMM server.

SCVMM Self-Service Portal

Slouží ke správě virtuálních serverů pomocí webového prohlížeče. Tento web můžete například publikovat i do internetu a jednotlivým správcům delegovat úkoly a virtuální stroje, které budou mít na starosti. Nemusí se tedy do firmy přihlašovat pomocí VPN nebo Direct Access přístupů, stačí mít webový prohlížeč. Pracovat se pak dá i z internetové kavárny či z jakékoliv platformy (Mac, Linux, …).

SCVMM Agent

Instaluje na jednotlivé virtuální hostitele a slouží k zajištění komunikace mezi SCVMM serverem a hostitelem. Tento agent je automaticky instalován i na server, na kterém běží SCVMM.

Po spuštění konzole se správci zobrazí prostředí známé z ostatních System Center produktů, případně jiných aplikací společnosti Microsoft, konkrétně Microsoft Outlook. Za pomoci dané aplikační unifikace je jednoduché se již napoprvé v produktu orientovat a neztrácet čas načítáním příruček či specializovaným školením. Na první pohled by se mohlo zdát, že SCVMM Console je taktéž add-in pro MMC, ale není tomu tak.

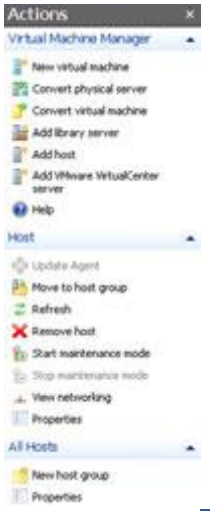
Levá strana slouží k výběru sekce, kterou chceme spravovat. Tedy například hostitelé, či virtuální stroje. Jednotlivé sekce SCVMM konzoly jsou podrobně popsány na obrázku 8,9,10. (12)

Obr.8 Levá strana SCVMM konzole

Prostřední sekce slouží k výpisu obsahu zvoleného v levé části. Tedy právě seznam hostitelů, virtuálních strojů, obsah knihovny atd. Oproti Hyper-V Manageru si sloupce můžete libovolně přidávat. Na výběr máte až 33 sloupců s různými informacemi!

Obr.9 Prostřední část SCVMM konzole

Pravá strana obsahuje výpis jednotlivých akčních položek. Opět platí model – jak z pohledu konkrétní vybrané položky (hostitel, virtuální stroj), tak i z globálního pohledu (Hyper-V).



Obr.10 Pravá část SCVMM konzole

SCVMM konzole oproti Hyper-V Manageru přináší jednotlivé sekce a novinky, které ulehčují konfiguraci a nastavení virtuálních strojů.

Hosts

Tato sekce sdružuje automaticky všechny fyzické hostitele. Novinkou je možnost rozřadit jednotlivé hostitele do skupin, co se může velice hodit v případě nasazení Self-Service Portalu. Díky údajům shromážděným v databázi můžeme vidět přehled vaší infrastruktury – jak jsou na tom virtuální stroje se zdravím, jaká je vytíženost knihovny, a to vše v přehledných grafech. Některé z dalších možností:

- rezervace hardwarových zdrojů pro hostitele v případě plného vytížení virtuálními stroji,
- správa virtuálních sítí na konkrétním hostiteli,
- správa uložišť, kam se virtuální stroje ukládají.

Virtual Machines

V této sekci je seznam všech virtuálních strojů z pohledu konkrétního hostitele. Po vybrání virtuálního stroje vidíte jeho stav a poslední operace s ním prováděné (migrace, editace HW profilu, …). Editovat lze:

- **vlastník** – důležité v případě používání Self-Service Portal,
- **popis** – libovolný text,

- **typ operačního systému**,
- **hardwarový profil**,
- **snímky**,
- **akce** v případě nenadálého vypnutí.

Library

Knihovna sloužící jako uložiště ISO obrazů, virtuálních disků, ať už „fyzických“, či jen šablon, šablon virtuálních strojů, skriptů a mnohého dalšího. Velmi důležitá součást, na kterou je navázáno velké množství funkcí a akcí v SCVMM.

Jobs

Přehled všech akcí a operací, které v rámci virtuálního prostředí byly provedeny.

Administration

Soubor s nastavením SCVMM jako takového:

- připojení k databázi,
- nastavení knihovny,
- nastavení umísťování virtuálních strojů,
- nastavení PRO,
- vzdálená správa,
- kooperace s SCOM,
- definice rolí a skupin k delegaci oprávnění.

Výhody a důvody, nasazení SCVMM:

- **P2V a V2V** – pomocí tohoto nástroje je možno konvertovat fyzický server na virtuální Hyper-V, či konvertovat virtuální stroje z platformy VMware na Hyper-V
- **Správa nejen Hyper-V platformy**, ale plná podpora VMware platformy. Není nutno udržovat dva produkty pro správu heterogenního prostředí. Stačí pouze SCVMM.

- **Spolupráce s SCOM** – velice zajímavá možnost, která zajistí nejen profesionální správu, ale i dohled. Kooperace těchto produktů může předcházet například pádům virtuálních serverů či fyzických hostitelů v případě nadměrného vytížení. Díky dohledu SCOM vyšle signál SCVMM, ten migruje virtuální server na nevytíženého hostitele a všechny služby jsou poskytovány bez negativní reakce uživatelů či zákazníků.
- **PRO (Performance Resource Optimization) tipy** – jedná se o souhrn tipů, jak zoptimalizovat virtuální infrastrukturu. Tipy jsou vydávány na základě kooperace s SCOM a říkají například, kde jsou úzká hrdla nastavení či mohou vzniknout problémy.
- **Šablony virtuálních strojů a disků** – vytváření a instalace nových serverů nikdy nebylo jednodušší. Pomocí šablon si můžete vytvořit například slabý server, středně silný server a silný server. Součástí takové šablony je hardwarový profil, cesta k instalačnímu médiu, produktový klíč a ostatní informace, které byste jinak museli zadávat ručně. Šablony jdou do knihovny ukládat i zpětně na základě již vytvořených virtuálních strojů.
- **PowerShell** – SCVMM přináší správu pomocí PowerShellu. Znamená to, že jednotlivé prováděné operace můžete skriptovat a značně tím ulehčit automatizovaným procesům.
- **Self-Service Portal** – umožňuje delegovat oprávnění vůči jednotlivým virtuálním serverům. Pokud tedy chcete, aby váš kolega mohl pouze dělat snímky a startovat virtuální stroje, není nic jednoduššího než použít tento nástroj.O správě a dohledu virtuálního prostředí by se dala napsat kniha. V rámci prostoru věnovaného tomuto článku jsme si alespoň naznačili, jaké nástroje se ke správě virtuálního prostředí dají použít a jaký je zhruba rozdíl mezi Hyper-V Managerem a nástrojem System Center Virtual Machine Manager.(12)

4.3 Virtualizace aplikací

Nejnovější formou využití virtualizace v praxi je virtualizovat konkrétní aplikace. V praxi to znamená poskytnutí prostředí pro spouštění jednotlivých aplikací odděleně od hlavního operačního systému (OS). Díky této nevázanosti za sebou virtualizované aplikace nemůžou

způsobit případnou nekompatibilitu s OS. Dalším zajímavým přínosem pro firemní potřeby je to, že zajišťují kompatibilitu starších aplikací na nových OS či usnadnění instalaci vybrané aplikace na různé další zvolené platformy. Tým se automaticky zvyšuje úroveň bezpečnosti soukromých firemních dat.

Prvním příkladem virtualizace aplikací je jeden z nejpopulárnějších programovacích jazyků – Java. Programy psané v Javě se typicky nekompilují do nativního kódu, ale do tzv. byte kódu. Ke svému běhu potom potřebují nainstalované runtime prostředí (Java Virtual Machine – JVM), které byte kód až při běhu programu překládá do nativních instrukcí. Díky tomu je možné ve většině případů spustit program v Javě na kterékoli platformě, která Javu podporuje (existuje pro ni JVM). Takový program je potom na platformě nezávislý a přenositelný bez nutnosti rekompilace. To je jeden z atributů virtualizace aplikací. Ovšem pro reálnou virtualizaci aplikací potřebujeme technologii, která něco podobného umožní pro co nejširší okruh aplikací, tedy i ty, které nejsou napsány v Javě. A tady už nám Java moc nepomůže, tedy pokud se nerozhodneme napsat si v ní vlastní virtualizační platformu.

Druhým příkladem jsou produkty vytvářející kompatibilní vrstvu pro běh aplikací jiného typu OS (např. Windows aplikace na Linuxovém OS) a různé emulátory (např. mobilních platforem na PC). Toho se dosahuje za cenu nejrůznějších omezení a nutnosti tuningu pro konkrétní aplikace. Tato omezení ovšem brání nasazení platformy pro širší spektrum aplikací. Dnešní technologie na virtualizaci aplikací proto nemají ambice přenosu aplikací na jiný typ OS. Od myšlenky provozovat aplikace na různých platformách koncových zařízeních se neupustilo. Právě naopak, je to jeden z klíčových cílů.

Co se týče virtualizace aplikací, prakticky všechny produkty se dnes zaměřují na nejpoužívanější desktopový OS – MS Windows. V situaci, kdy se jeho aktuální podíl na trhu pohybuje kolem 85 %, je to asi pochopitelné. Existují samozřejmě i produkty virtualizující aplikace na platformě Linux, např. CDE. Než se dostaneme ke konkrétním technologiím, ujasněme si, co všechno nám tato virtualizace může přinést a jaké situace řešit:

- Provozování starších aplikací na nových verzích OS, kde aplikace již nativně neběží.
- Možnost instalovat a paralelně spouštět různé verze dané aplikace na jednom OS.

- Uzavření aplikace do kontejneru, který jí vytvoří vlastní prostředí pro běh. To může být částečně, nebo i zcela odděleno od prostředí OS.
- Vytvoření balíčku, který umožní různé způsoby doručování aplikace. Může se jednat o streaming po síti, doručení do klientské aplikace běžící na jiném stroji, a dokonce jiné platformě, doručení do HTML 5 web browseru aj.
- Jednoduché vyresetování konkrétní aplikace do stavu těsně po instalaci.
- Možnost provozovat aplikace bez jejich instalace. K registraci komponent či asociaci přípon dojde při prvním spuštění a z pohledu OS se aplikace jeví jako nainstalovaná.

Princip virtualizace aplikací je jednoduchý. Aplikace se spouští nad virtualizační vrstvou, jakýmsi aplikačním hypervisorem, který zajišťuje potřebnou funkcionalitu. Aby byla technologie reálně použitelná, nesmí samozřejmě vyžadovat jakýkoli zásah do vlastní aplikace. Dalším zřejmým požadavkem je schopnost zvirtualizovat ideálně všechny aplikace bez ohledu na jazyk, ve kterém jsou napsány, funkcionalitu a komplexnost apod. To v praxi naráží na problém např. u aplikací, které jsou úzce integrovány s jádrem OS. Nicméně jde jen o velmi malou skupinu aplikací. Z toho vyplývá, že virtualizační vrstva musí být pro aplikaci naprosto transparentní. Na úrovni OS se virtualizační vrstva integruje s prostředím, které OS dává k dispozici pro běh aplikací (runtime environment), případně nahrazuje jeho část. Tak např. může zápisy do určitých částí filesystému přesměrovat jinam apod.

Konkrétní implementace se u jednotlivých platforem velmi liší a stejně se liší i vlastnosti a možnosti, které tyto platformy nabízejí. Některá řešení vyžadují instalaci virtualizační vrstvy předem na koncová zařízení ve formě agenta či klienta. Jiná řešení vytvářejí balíčky, jejichž součástí je kromě samotné aplikace i virtualizační vrstva. Virtualizační vrstva se pak zavádí v rámci zpuštění balíčku a na straně OS není potřeba provádět žádné instalace ani úpravy. Dále jsou platformy, které se prezentují jako virtualizace aplikací, ale řeší spíše jen doručování aplikací na koncové zařízení. Žádnou virtualizační vrstvu vlastně nemají, čemuž odpovídá velice omezená funkcionalita. Je potom na každém, aby si ujasnil, jaké vlastnosti potřebuje, a podle toho vybral optimální platformu. Někteří poskytovatelé produktů pro virtualizaci mají dokonce více produktů spadajících alespoň částečně do portfolia virtualizace aplikací. Příkladem je třeba VMware, který nabízí hned tři produkty (ThinApp, App Vols a Mirage) postavené na odlišných principech a schopné se navzájem doplňovat. Je jasné, že orientovat se v této problematice a množství různorodých produktů vyžaduje nejen jejich detailní znalost, ale také zkušenosti z praxe. (13)

4.3.1 Microsoft App-V

Jedná se o platformu, kterou nabízí přímo dodavatel OS. Má hned několik scénářů nasazení a způsobů doručování virtualizovaných aplikací – instalace a streaming. Výhodou je flexibilita, rozsáhlé konfigurační možnosti, vynikající integrace s OS a s produkty pro správu, jako je System Center Configurations Manager. Dále také možnost použít pro doručování aplikací buď komponenty Windows Serveru, které zákazník již používá (File Server, IIS Server), nebo jakékoli řešení distribuce SW balíčků, a to i třetích stran. Velice dobře je zde řešena závislost balíčků, a to jak vzájemně, tak na instalovaném SW, opět s propojením na centrální správu. Na straně koncového zařízení je potřeba předem nainstalovaný klient. Mezi nevýhody patří omezené možnosti izolovat aplikaci od OS a ostatních aplikací a např. po dobu migrace paralelně provozovat danou aplikaci v různých verzích. Také nutnost instalace klienta může být považována za určitou nevýhodu. (13)

4.3.2 VMware ThinApp

Jedná se o řešení od leadera na poli x86 virtualizace. Umožňuje nasazení několika možností aplikace a nabízí dvě varianty doručení – instalaci a streaming. Samozřejmostí je integrace se souvisejícími produkty ze skupiny End User Computing, především s Horizon View, Mirage, Workspace, App Vols aj. Hlavní předností tohoto řešení je možnost dokonalé izolace virtualizované aplikace od OS a ostatních aplikací a možnost tuto izolaci detailně konfigurovat. Další výhodou je, že se jedná o bezagentní řešení, které pro vlastní provoz nepotřebuje ani žádnou zvláštní infrastrukturu. Virtualizované aplikace fungují na jakémkoli podporovaném OS bez nutnosti cokoli instalovat či konfigurovat. Nevýhodou tohoto řešení je neexistence centrální správy. Tu lze zajistit až integrací s dalšími produkty VMware, např. výše zmiňovanými, nebo s produkty třetích stran. Další nevýhodou je možnost konfigurace aplikačních závislostí pouze mezi ThinApp balíčky navzájem. Zde by hodně pomohla možnost integrace např. s Microsoft System Center Configurations Managerem, která ale chybí. (13)

4.3.3 Citrix XenApp/XenDesktop

Citrix, známý svou úzkou spoluprací s Microsoftem, oznámil, že od verze XenDesktop 7 bude defaultní technologií pro doručování aplikací Microsoft App-V 5. Integrace zatím nepodporuje všechny možnosti App-V 5, ale dá se předpokládat, že do budoucna budou řešení postavená na platformě XenApp/XenDesktop funkčně stejná, jako výše popsaný App-V. S dříve používaným Citrix Application Streamingem se do budoucna už nepočítá.

Existuje samozřejmě více produktů řešících virtualizaci, ale jedná se u nich o menší řešení s omezenou funkcionalitou. Často ani nenabízejí vlastní virtualizační vrstvu, ale stavějí na existující technologii, kterou rozšiřují. Příkladem je třeba Parallels Remote Application Server. Jiné produkty jsou zase zaměřeny vyloženě jednoúčelově, např. poskytují bezpečný přístup k aplikacím (Oracle Secure Global Desktop) nebo řeší uzavření aplikací do sandboxu (Sandboxie). Zajímavý je relativně nový produkt Cameyo. Podobně jako VMware ThinApp řeší běh virtualizované aplikace bez nutnosti instalace klienta na cílový systém a nepotřebuje ani žádnou zvláštní infrastrukturu. Navíc se zaměřuje na běh těchto aplikací v cloudovém prostředí a přístup k nim přes HTML5, což jsou poměrně žádané vlastnosti.

4.3.4 Srovnání platforem Hyper-V a VMware

V rámci serverové virtualizace jsou nejrozšířenějšími platformami hyper v od firmy Microsoft a VMware. Pro firmy, které chtějí využít pro svou IT infrastrukturu privátní virtuální prostředí, s případným přechodem na cloud služby, může být obtížné vybrat si správný produkt. V porovnání produktů je brán důraz na hlavní požadavky kladeny na virtualizaci.

Po konzultaci s odborníky s IT praxi byly shromážděny informace o nasazeních virtualizačních systému, jejich výhody a nevýhody. Byla vykonána vícekriteriální analýza na základe poznatků a následné doporučení systému vhodného pro firemní privátní virtualizaci.

Hlavní výhody produktu Hyper-V

- Rychlé tvorby a nasazení virtuálních strojů
- Údržba nevyžaduje vypnutí hlavního hostitele
- Snadné zálohy
- Komplexní zabezpečení prostřednictvím služby Windows Active Directory

- Nižší pořizovací základy

Nevýhody produktu Hyper-V

- Podpora jenom specifických operačních systému, které mohou být nainstalovány na virtuální stroj
- Vyžaduje Windows OS aktualizace
- Neuspokojivá nebo chybějící podpora pro služby RemoteFX a šablony služeb v nástroji System Center Virtual Machine Manager 2012 R2

Hyper-V je navržen, aby nabízel virtualizaci pro organizace s datovým centrem nebo hybridním cloudem. Je vhodný pro firmy, které chtějí vytvořit privátní nebo i veřejní cloud, škálovat služby nebo virtualizovat pracovní zátěž. Hyper-V je integrován do OS Windows server nebo může být naistalován i jako samostatný server známy jako Hyper-V server. Nabízí sjednocenou sadu integrovaných nástrojů pro správu bez ohledu na to, zda organizace usilují o migraci na fyzické servery, soukromý cloud, veřejný cloud nebo "hybridní" směs těchto tří možností. Samotné uživatelské prostředí Hyper-V je založeno na designe OS Microsoft Windows. Proto je rovněž ideální volbou pro administrátory virtualizace, kteří již mají znalosti a pozadí s produkty společnosti Microsoft, ale nemají zkušenosti se samotnou virtualizací.

Výhody VMware spočívají zejména v

- Intuitivním používáním
- Kvalitní podpore suportu produktu
- Optimální požadavky pro velké podniky
- Široká podpora OS
- Přístup ke schopnosti řízení
- Průhledné sdílení
- Více hostitelských uživatelů na jednom stroji

Nevýhody VMware se projevují zejména v složitém designu platformy, která je sice intuitivní, ale i nepřehledná.

- Free a trial verze má omezené funkce, které jsou nedostatečné na požadavky kladené na firemní virtualizaci
- Složitější pro administrátory, který nemají z virtualizací na VMware žádné zkušenosti

VMware vSphere je populární volbou hypervisoru pro organizace, které chtějí dosáhnout určitého stupně virtualizace. Od verze 6.0 je vSphere vysoce konfigurovatelná, což z něj činí atraktivní volbu pro společnosti, které chtějí nasadit plné virtuální prostředí, nebo popřípadě se rozhodnou pro hybridní přístup. Je ale složitější na konfiguraci a monitoring systémů, než Hyper-V.

Pro následné porovnání a vícekriteriální analýzu byly zvoleny následovné vlastnosti nevyhnutné pro firemní virtualizaci

- Cena
- Škálovatelnost
- UI
- Podpora OS
- Výkon
- Storage a Networking
- Aktualizace – nasazení a podpora
- Podpora záložních zdrojů
- Monitoring
- Celková úspora

Hyper-V je součástí OS Microsoft Windows Server cena standart verze je 19 690 czk (cena se váže na počet jader CPU) až po 79 299czk – Windows Server Datacenter.

VMware má free a trial verzi, kterou poskytuje zdarma. Ti jsou ale nedostatečné pro potřeby virtualizace ve firemním prostředí. VMware essential, který je nevhodnější pro serverovou virtualizaci začíná od 9 236 czk pro 3 uživatelé v základní verzi. VMware vSphere 6 Essential Plus Kit, kompletní balík stojí 96 179 czk. Všechny ceny jsou uvedeny bez dph.

Škálovatelnost Hyper-V mírně překračuje VMware. Podrobný potenciál je zrhnutý v nasledovné tabulce 1.

Typ stroje	Prostředky	Hyper-V	VMware vSphere
Host	Logické CPU	320	320
Host	Fyzická RAM	4	4
Host	Virtual CPU na uživatela	2,048	4,096
Virtual	Virtual CPU na VS	64	64
Virtual	Virtuální paměť na VS	1TB	1TB
Virtual	Aktivní VS na jednoho hostitele	1024	512
Cluster	Maximum nodů	64	32
Cluster	Maximum VS	8 000	4 000

Tab.1 srovnání výkonu Hyper-V a VMware

VMware má výhodu většího počtu virtuálních CPU na jednoho uživatele. Hyper-V má oproti tomu výhodu v lepším zálohování a vetší podpore Clusterů. Další výhodou je i počet aktivních uživatelů na jednom hostiteli, kde je jejich počet dvojnásob nežli u VMware vSphere.

Uživatelské rozhraní Hyper-V je založeno na principu OS Windows. Jeho výhody spočívají zejména v:

- Vrstva hypervisoru nebo VMM jádra nevyžadují pro každé zařízení specifické ovladače
- Je minimalizován povrch, na který jde proniknout hrubou silou, protože hladina Hypervisoru neobsahuje API
- Ovladače nemusejí být „Hypervisor-aware“
- Ovladače mohou být instalovány v operačním systému, který je spuštěný v řídící vrstvě
- Vrstva hypervisoru vyžaduje menší náklady pro údržbu ovladačů zařízení
- V řídící vrstvě lze instalovat libovolné role serveru
- Vyžaduje méně času na inicializaci nežli VMware

Nevýhody Hyper-V:

- Řídící vrstva vyžaduje mít naistalovány operační systém, aby mohlo hypervisor pracovat
- Pokud dojde k selhání řídící vrstvy OS, dojde k selhání všech VS
- Zabezpečení závisí na použití bezpečnostních aktualizací od společnosti Microsoft, které vyžadují, aby byly všechny VMS převedeny do režimu offline nebo přesunuty do jiného uzlu, aby se předešlo vypnutí VS.

Hlavní výhoda VMware spočívá na nezávislosti na operačním systému. K bezpečnému používání tak nepotřebuje velké množství záplat.

Na druhou stranu nevýhodou VMware jsou:

- Funguje jenom na podporovaném hardwaru
- Potřebuje více času na inicializaci
- Nastává tu riziko poškození kódu hypervizoru, který může způsobit zpomalení, ale i poškozený VS

Hyper-V, kromě nativního Windows, podporuje následovné OS:

- CentOS
- Red Hat Enterprise Linux
- Debian
- Oracle Linux
- SUSE
- Ubuntu
- FreeBSD

Podpora OS VM-ware mimo jiné zahrnuje následující OS:

- Oracle Unbreakable Enterprise Kernel Release 3 Quarterly Update 3
- Asianux 4 SP4
- Solaris 11.2
- Ubuntu 12.04.5
- Ubuntu 14.04.1

- Oracle Linux 7
- FreeBSD 9.3
- Mac OS X 10.10

Výkon

Akademický výzkum byl proveden s cílem vyhodnotit výkonnost Hyper-V, VMware a dalších řešení v kontrolovaném laboratorním prostředí pomocí metod hodnocení a testování řízených vědeckou metodou. Podle autorů výsledného dokumentu byly prováděny experimenty s využitím různých scénářů na každém virtualizačním přístupu podporovaných nejnovějšími verzemi zmíněných hypervisorů. Naměřené výsledky ukázaly, že Hyper-V jemně převyšuje výkonnost VMware.

Podpora storage a networkingu jsou zahrnuta tabulkách 2 a 3.

Typ Storage	Hyper-V	VMware
podpora iSCSI/FC	Ano	Ano
Podpora Network File System	Ano(SMB 3.0)	Ano(NFS)
Virtuální Fiber Channel	Ano	Ano
Multipathing třetí strany	Ano	Ano
Podpora 4KB HDD	Ano	Ne
Storage Virtualizace	Ano(Spaces)	Ano(vSAN)
Storage Tiering	Ano	Ano

Tab2. Srovnání Storage podpory Hyper-V, VMware

Typ Networkingu	Hyper-V	VMware
Dynamický VMQ	Ano	NetQueue
IPsec Task Offload	Ano	Ne
SR-IOV pří živí migraci	Ano	Ne
vRSS	Ano	Ano(VMXnet3)

Tab3. Srovnání Networkingu Hyper-V, VMware

U virtuálních storage má Hyper-V výhodu v nativní podpoře 4KB HDD. Menší výhodu získává u networkingu, kde má službu IPsec Task Offload(podpora sítových adaptérů vybavených HW, který snižuje zatížený procesoru prováděním výpočetní intenzivní práce) a podporou živé migraci HDD. (14)

Aktualizovat systém u Hyper-V je relativně snadné. Jedná se o aktualizace klasického Windows Serveru, aktualizuje se přes Windows Update. Při aktualizaci jednotlivých firmwarů, je většina aktualizačních balíčků spustitelná přímo z Windows.

VMware má pro svůj produkt dostatek aktualizací a dobrou podporu, ale nemá dobře vyřešenu instalaci upgradů. Existuje i skupina lidí, který jsou názoru, že VMware se aktualizovat nedá. Musí se použít bootovací update ISO, nebo přes remote management (ILO, iDrac). Pro řadu Enterprise výrobce ponouká upgrade balíčky, které automaticky obsahují upgrade firmwarů.

Propojení z UPS (záložní zdroje)

Hyper-V má nativní podporu propojení UPS. VMware potřebuje plugin od výrobců UPS (stažitelný zdarma) a mít nainstalovanou vCenter konzoli, vCenter server a licenci.

Monitoring pro Hyper-V a VMware je na dostatečné úrovni. Výhodou ale může být u Hyper-V již nastavený systém monitoringu pro Windows, který nemá problém přidání i monitoringu od Hyper-V a všechny údaje se nachází na jednom místě. VMware má svůj vlastní monitorovací systém.

Hyper-V je schopen mít nainstalovaný zálohovací SW přímo na hypervizoru. U VMware je potřeba mít další (fyzický nebo virtuální) server a licenci pro VMware, aby bylo možno zálohovat virtuální servery zvenku.

Pro malé clustery již nově u Hyper-V není zapotřebí mít dedikovanou Active Directory (tzn. další server), protože od Windows Server 2016 lze nově dělat „workgroup clusters“ (4 nodový

cluster = 4 servery). Pro vytvoření VMware clusteru je nutné mít vCenter server (4 nodový cluster = 4+1). (15)

Na vícekriteriální analýzu variant byla použita bodovací metoda výběru nejvhodnější platformy pro serverovou firemní virtualizaci, která je určena primárně pro tvorbu soukromého cloudu, šetřený na HW apod. Hodnoty byli obodovány škálou 1-5, max, metoda. Hodnoty a kritéria byli analyzovaný a vybrány tak, aby co nejlépe splňovali podmínky nového virtualizačního prostředí ve firmách. Kritéria byly vybrány by nejlépe splňovali podmínky pro využívání v IT infrastruktuře podniku. Důležitost kritérií byla konfrontována z IT odborníky z praxi.

- Cena: Jedná se o cenu za jednotlivé licence, které uživatel zaplatí. VMware poskytuje svou platformu zdarma, ale má omezenou funkcionalitu, která je pro využívání ve firemním prostředí nedostatečná. Hyper-V je součástí balíku OS Windows server 2016, ale je možnost ho dokoupit jako samostatnou licenci, když uživatel nemá zájem OS Windows využívat.
- Škálovatelnost: Schopnost systému pracovat s náhlými změnami potřeby uživatelů a zvyšovat parametry systému v případe, že taková situace nastane.
- UI: Uživatelské rozhraní, bere se v dotaz intuitivnost práce s hypervisorem a zejména nutnost instalace ovladačů hypervisoru. Dále se tu zohledňuje i požadavek monitoring systému, který souvisí přímo souvisí z UI.
- Podpora OS: Operační systémy, které mohou mít hypervisory nainstalované.
- Výkon: Celkový výkon hypervisorů, vytažení CPU fyzického serveru a odezva virtuálního serveru.
- Storage/Networking: Podpora zapojení storage serveru, podpora HDD a sítového rozhraní
- Aktualizace: Frekvence aktualizací, kterou výrobci software vydávají a způsob aplikace aktualizace.

Hypervizor	Cena	Škálovatelnost	UI	Podpora OS	Výkon	Storage/Networking	Aktualizace	součet
Hyper-V	3	4	2	2	5	4	3	23
VMware	2	3	1	3	5	3	3	20

Tab.4 vícekriteriální analýza variant

Největší význam má atribut výkon, následován škálovatelností a přací se sítěmi a diskovým úložištěm. Dále je dbán důraz na cenu licence, a aktualizace systému – údržbu od výrobce rychlost reagovat na případné změny v bezpečností politice a celkovou instalaci aktualizací systému. Nejrozšířenější OS systémy jsou podporovány oběma platformami, proto je atribut na nižší úrovni než výkon a škálovatelnost. Do analýzy je zahrnut i uživatelský design, celkové ovládání, nastavený a možnost instalace samostatných ovladačů.

Do vícekriteriální analýzy nebyla zahrnuta podpora propojení z UPS zdroji. Je to z důvodu garance neustále provozu poskytovatelů datových center, a možnost využití vlastních generátorů. I když je tak využít UPS zdroje doporučená možnost, není tak jedinou možností zabezpečení proti výpadku hostitelského serveru. Výsledky analýzy jsou sumarizovány v 5. kapitole.

4.3.5 Návrh a využití cloud architektury

Pokud organizace potřebuje přesunout úlohy a data do cloudu, jejich místní datacentra často pokračují mít důležitou roli. Termín *hybridní cloud* odkazuje na kombinaci veřejného cloudu a místních datových center. Je to nejvýhodnější způsob pro firmy, které plánují kompletní přechod do cloudu, nebo rozšíření vlastní infrastruktury.

Důvody nasazení hybridního cloudu

- Jako strategie přechodu během dlouhodobější migrace do plně nativního cloudového řešení

- Když předpisy nebo zásady nepovolují přesunutí úloh nebo konkrétních dat do cloudu.
- Při havárii pro obnovení a odolnost proti chybám, nastavením replikace dat a služeb mezi místními a cloudovými prostředími.
- Pro snížení latenci mezi místním datovým centrem a vzdáleným umístněním hostitele cloudu

Nevýhody

- Vytváření konzistentního prostředí z hlediska zabezpečení, správu a vývoj a vyloučení duplicitní práce.
- Potřeba vytvořit spolehlivou a nízkou latenci a zabezpečit propojení mezi místním a cloudovým prostředím.
- Potřeba zálohovat a replikovat data a provést úpravu aplikací a nástrojů pro správne použití dat v rámci cloudového prostředí
- Provést šifrování a zabezpečení dat v cloudu a zabezpečit oboustranný přístup

V místním úložišti je vhodné ponechat databáze a interní soubory. Jsou to data, které předpisy nepovolují přesunout do cloudu kvůli otázkám suverenity a ochrany osobních údajů. Během migraci se odporoučí ponechat v místních složkách i aplikace u kterých není spolehlivě určeno jejich bezpečný přesun na cloud.

Pro uložení dat do cloudu je dobré dbát do úvahy i následovné faktory

- Náklady na úložiště v cloudu nemusí být nezbytné nižší než náklady na údržbu vlastních serverů ve vlastním, nebo v pronajatým datacentrem
- **Elastické škálování**. Je relativně obtížné odhadnout nárůst dat a potřebnou kapacitu ve vlastním prostředí. U pronajatého cloudu proto existuje možnost využití prakticky neomezeného zvyšování místa, samozřejmě za příplatek. Proto je potřeba zvážít případnou expanzi. Tento faktor je ale méně relevantní pro aplikace, které se skládají z relativně statické velikosti datové sady.
- **Zotavení po havárii**. Data uložená v cloudu lze automaticky replikovat v rámci oblasti hostitele, poskytuje automatické geografické služby. V hybridních prostředích je možnost technologie použít k replikaci mezi místním a Cloudovým úložištěm. (16)

4.3.6 Rozšíření dat ukládá do cloudu

Existuje několik možností pro rozšíření místního úložiště dat do cloudu. Jednou z možností je, aby místní a cloudové repliky. To může pomoci dosáhnout vysoké úrovně odolnosti proti chybám, ale může vyžadovat provedení změn pro aplikace pro připojení k úložišti příslušná data v případě selhání.

Další možností je přesun částí dat do cloudového úložiště a vysoce načítána data ostanou na místní síti. Tato metoda může ve výsledku poskytnou cenově výhodnější možnost pro dlouhodobé uložení dat, stejně jako vylepšovat dobu odezvy pro přístup snížením provozu sadu dat.

Třetí možností je zachování všech dat místně, ale použít cloud na hostování aplikací. Aplikaci se spustí v cloudu a uživatel se připojte ho k místní datastore prostřednictvím zabezpečeného připojení. (16)

4.3.7 Úložiště dat serveru SQL Server

Při využití místního SQL Serveru, cloud od firmy Microsoft nabízí možnost využít službu Microsoft Azure Blob Storage pro zálohování a obnovení. Tato funkce ponouká neomezené odlehlé úložiště a možnost sdílet stejnou zálohu dat mezi SQL Serverem běžícím na místě a SQL Serverem běžícím ve virtuálním počítači v Azure.

V rámci Azure SQL Database je relační databáze spravovaná jako služba. Vzhledem k tomu, že Azure SQL Database využívá stroje Microsoft SQL Server, aplikace můžou přistupovat k datům stejným způsobem jako u běžných technologií. Databáze SQL Azure dokáže také kombinovat systém SQL Server i pro jiné účely. Například SQL Server Stretch Database funkce umožňuje aplikaci pohled na jednotlivé tabulky v databázi systému SQL Server, a to i v případe že některé nebo dokonce všechny řádky této tabulky jsou uloženy ve službě Azure SQL Database. Technologie automaticky přesune data, která nejsou přístupná v definovaném prostředí a čas do cloudu.

Služby a aplikaci běžící v databázi cloudu, umožnují automatickou obousměrnou synchronizaci napříč více databázemi. Usnadňuje se tím aktuálnost dat. Toto řešení ale není

vhodné využívat pří havárií nebo migraci z místního SQL serveru do cloudu. Pro obnovu dat po havárií je vhodné replikovat data napříč dvěma nebo více instancemi SQL serveru. (17)

5 Zhodnocení výsledků a doporučení

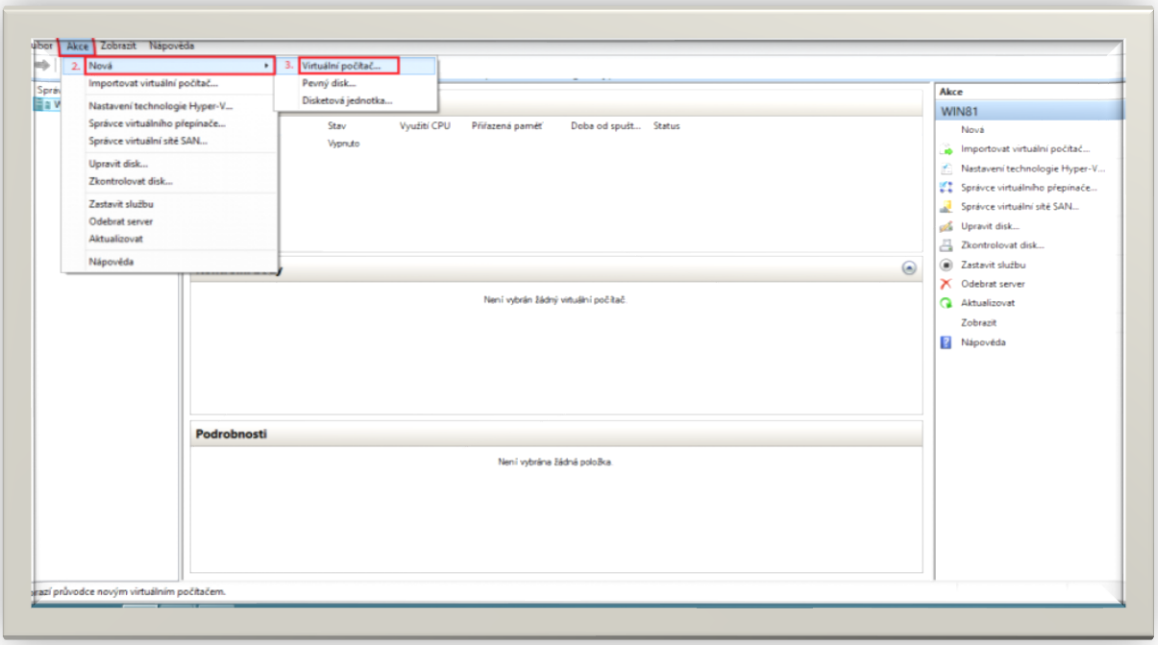
5.1 Zhodnocení analýzy

Jako nevýhodnější virtualizační prostředí ve firmách byla, podle výsledků analýzy, zvolena platforma Hyper-V. Její hlavní výhodou je skutečnost, že je součástí balíčku Windows Server 2016. Firma, která má postavenou IT infrastrukturu na platformě Windows, si tak nemusí připlácet za licenci na Hyper-V. Uživatelé, který preferují Linux nebo jiní OS si mohou zaplatit za samostatnou licenci nebo sáhnout pro VMware který má vetší podporu OS a nejí vázán na Windows. Co se výkonu a škálovatelnosti týče, Hyper-V má malou výhodu v škálovatelnosti, ale výkonově jsou platformy relativně srovnatelné. Hyper-V má převahu v podpoře virtuálního storage a propustnosti sítí. Jedná se o nativní podporu 4K HDD a propustnost sítě. Aktualizace a údržba programu je na srovnatelné úrovní. U Hyper-V aktualizace nejsou vydáváni často jako u VMware, ale je relativně snadnější je aplikovat. VMware má firmware balíčky dostupné jenom pro Enterprise licenci produktu. Hlavním faktorem tak zůstává i individuální preference systému, které jsou ve firmě nasazeny, a taky zvážený na plní přechod do cloudu. U Cloudových služeb má Hyper-V výhodu v platformě Azure. Má vlastní serverové úložiště a lepší podporu SQL serverů. Hyper-V má plnou podporu přechodu na cloud, což je výhoda u dnešního trendu všechno virtualizovat a ukládat na cloud privátní nebo využit veřejné služby dodavatelů. Proto také byla vybrána platforma Hyper-V pro tvorbu privátního virtuálního prostředí. Práce ukazuje tvorbu virtuálního stroje, a dává obecná doporučení po konzultaci s odborníky z praxe u nejvýhodnějšího obecného nastavení novo vytvořeného virtuálního stroje. Nastavení a požadavky se týkají hardwaru i nastavení nového virtuálního stroje.

5.2 Tvorba virtuálního stroje Hyper-V

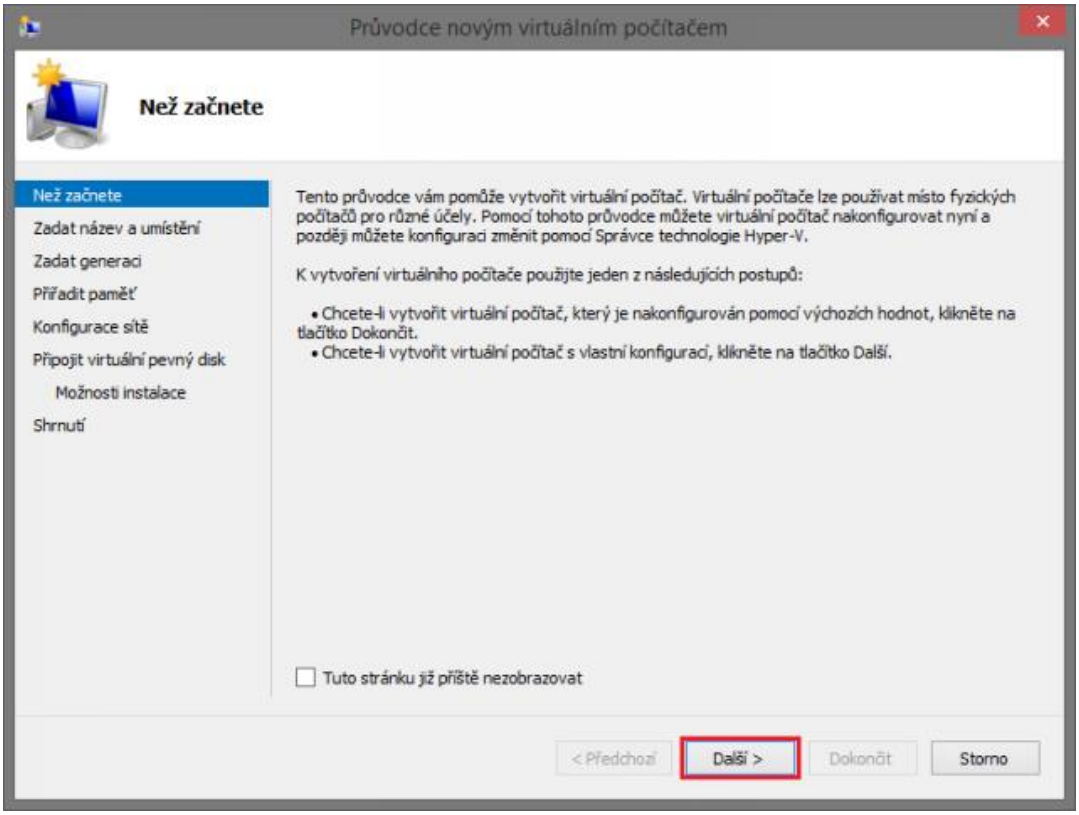
Virtuální prostředí bylo vytvořeno v platformě Hyper-V.

Nástroj *Správce technologie Hyper-V*. Z textové nabídky je zvolena **Akce – Nová – Virtuální počítač**.



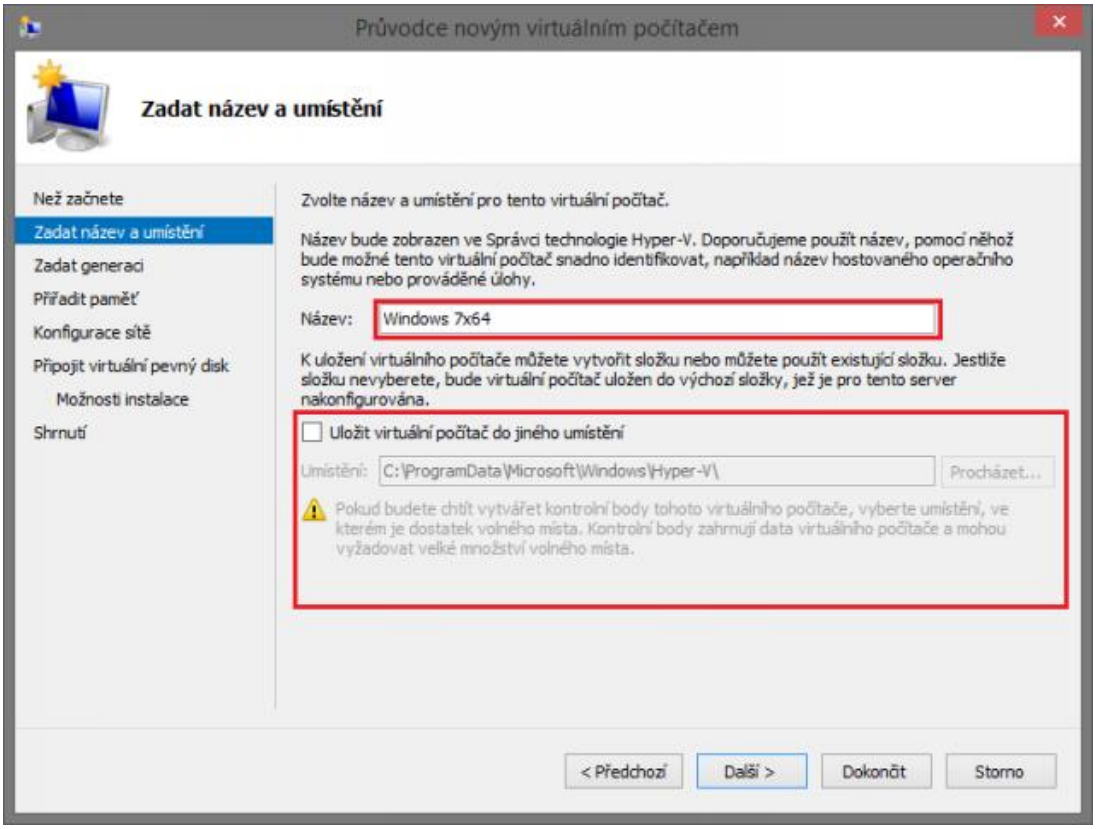
Obr. 11 Správce technologie Hyper-V

Otevře se *Průvodce novým virtuálním počítačem*. První možností nastavení je nechat veškeré hodnoty ve výchozím stavu, kliknout v levém sloupci na **Shrnutí**, a pak **Dokončit**. Tím dojde k vytvoření virtuálního stroje s defaultním nastavením. Pro většinu uživatelů jsou doporučená nastavený nedostatečná, popřípadě nevyužívají kapacitu hostitelského serveru. Doporučenou možností je postupně konfigurovat každou položku, aby vyhovovala potřebám dané firmy. Instalace projde každou položku a uživatel má tak možnost nakonfigurovat si virtuální stroj dle své potřeby.



Obr. 12 Průvodce virtuálním počítačem

Na obrazovce *Název a umístění* se zadává název virtuálního stroje a následně pak i umístnění. Ve výchozím stavu ukládá Hyper-V virtuální stroje na systémový disk. Virtuální stroj s čistou instalací Windows 7×64 zabere cca 15 GB. Pro jeho bezproblémový firemní chod je ale odporučeno rezervovat si velikost v HDD alespoň 20 GB.



Obr. 13 Název a umístnění

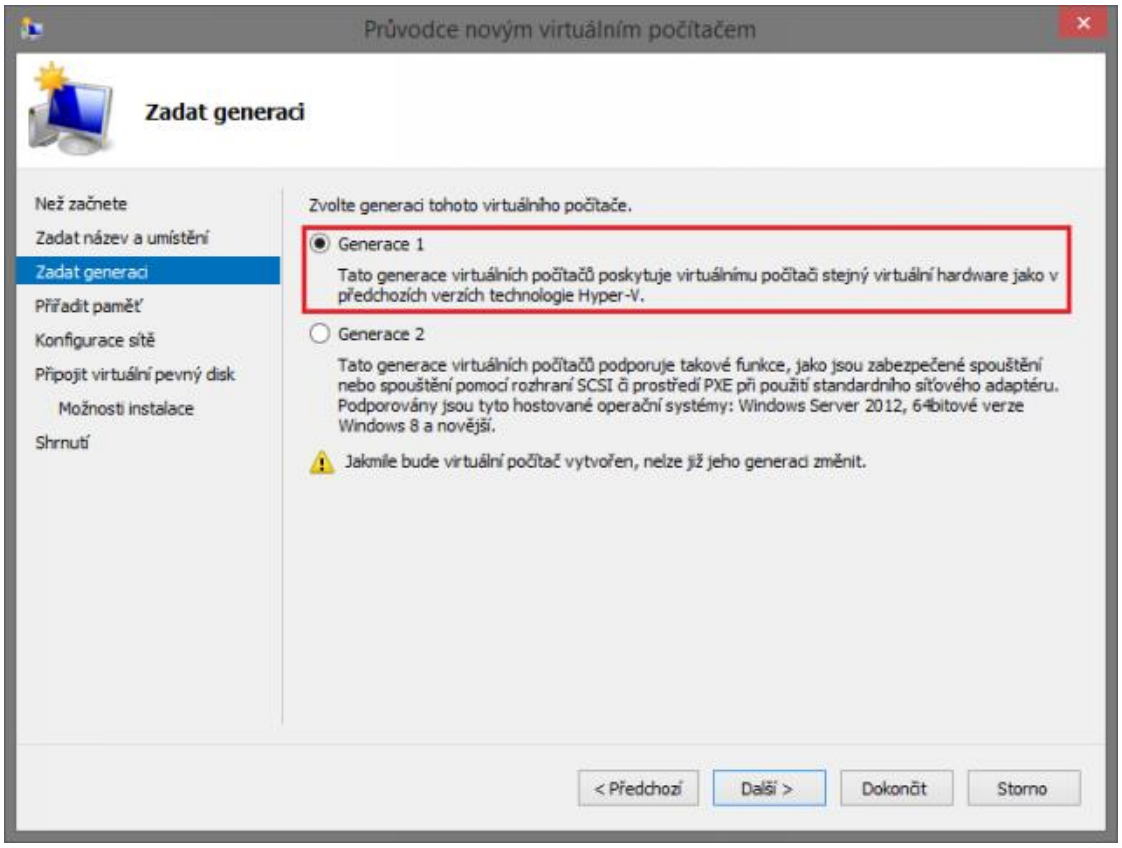
Následuje výběr generací. Rozdíly mezi první a druhou generací jsou široké.

- **Generace 1** je určena pro všechny operační systémy Microsoft Windows až do verze Windows 7.
- **Generace 2** pak pouze pro 64-bitové operační systémy Windows 8/8.1 x64, Windows Server 2012/R2 x64 a novější.

Volba k vytvoření virtuálního počítače generace 1 nebo generace 2 by měla záviset na tom, který hostující operační systém se bude instalovat, a způsob zavádění, který bude využíván k nasazení virtuálního počítače. Doporučuje se už vytvářet virtuální počítače generace 2, který má oproti generace 1 nové funkce jako například zabezpečené spuštění. Pokud ale uživatel plánuje přechod na cloud Azure, je vhodné zvolit Generaci 1. Generace 1 se v praxi využívá v případech:

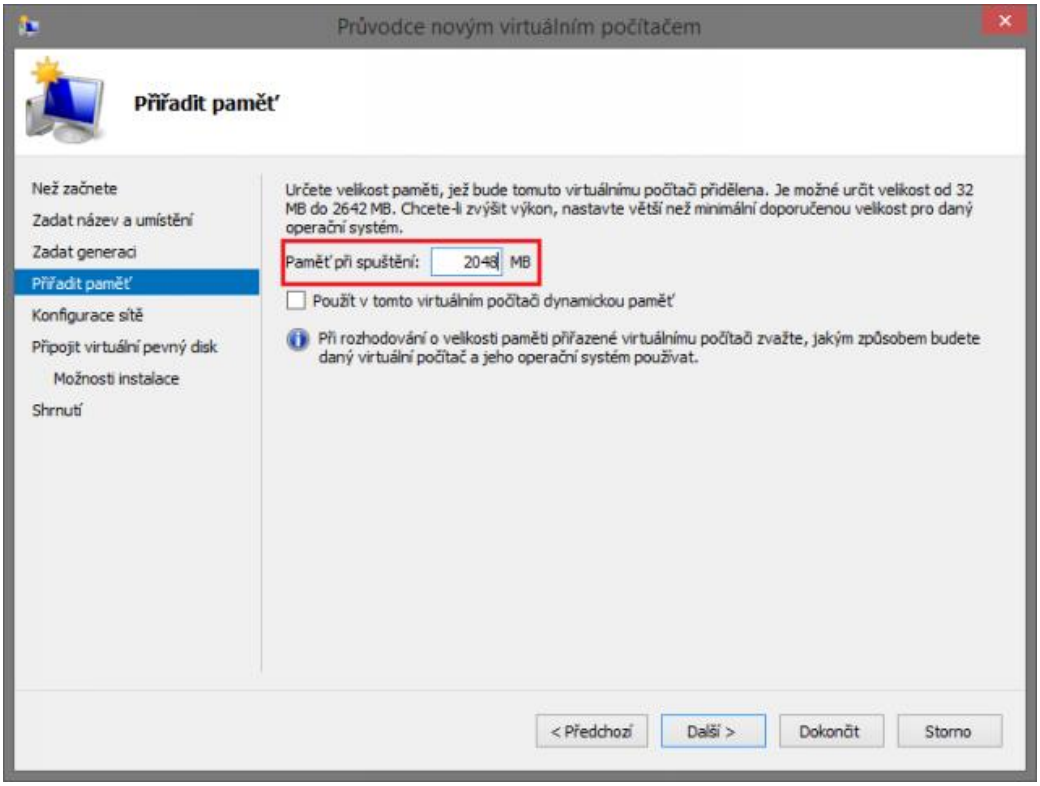
- Bootovací VHD není kompatibilní s UEFI
- Plánován přesun virtuálního stroje do cloudu
- Generace 2 nepodporuje operační systém, který se bude instalovat na virtuální počítač
- Generace 2 nepodporuje metodu bootování

Nezávisle od výběru generace je volba využívání HDD. Pokud je do budoucna plánováno využívat pevný disk vytvářeného virtuálního počítače v clusteru, je vhodné zvolit možnost uložení virtuálního počítače do nové složky a zadat sdílené umístění.



Obr. 14 Výběr generace

Na kartě *Přiřadit paměť* se podle uživatelský potřeby přiřaďuje virtuálnímu stroji paměť RAM. Výchozí hodnota je nastavena na 512 MB která je pro dnešní potřebu nedostatečná. Odporoučí se zadat dostatečnou hodnotu pro běh aplikací a operačního systému současně. Obecné pravidlo na přirazení RAM ravidla, říká, každé jádro má mít min. 2 GB RAM, doporučeno je pak mít 4 GB RAM na jádro. Doporučeno je počítat z 1 GB rezervou na OS Na této kartě se nachází rovněž možnost *Použít v tomto počítači dynamickou paměť*. To znamená, že paměť RAM bude přidělována dynamicky, podle potřeby. Uživatel tak bude efektivněji využívat dostupnou paměť v případě, že často spouští více virtuálních strojů najednou.



Obr. 15 Přiřazení paměti

U položky *Konfigurace sítě*, se zvolí typ připojení (virtuální přepínač). Jedná se o externí virtuální přepínač, tedy takový, který virtuálnímu stroji umožní připojení k internetu.

Doporučení nastavení sítě pro firemní provoz je následující:

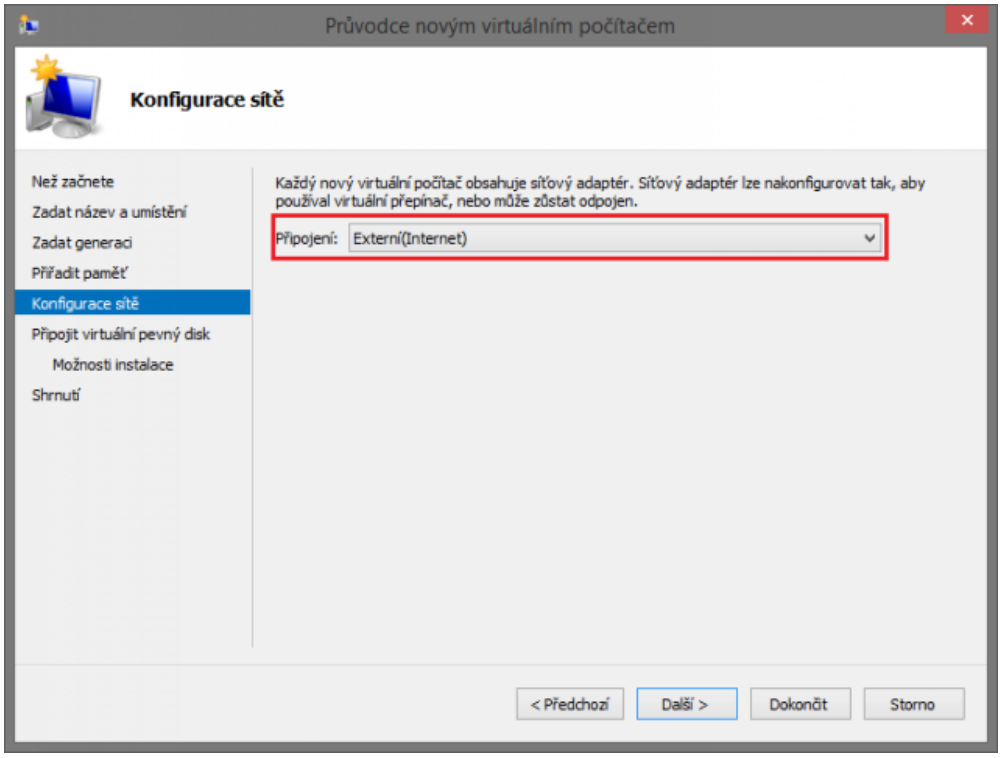
- používat 64-bitové ovladače, které podporují DMA větší než 4GB
- používat single port adaptéry (v praxi skoro nemožné kvůli omezení počtu PCIe)
- offload sítové karty a iSCSI HBA používat s rozmyslem – konzultovat předem dopady s prodejcem (offload síťovky mohou brzy znamenat úzké hrdlo, které nelze snadno odstranit)
- pro ne-clusterový stroj navrhovat 6-7 fyzických sítových karet
- pro clusterový stroj navrhovat 8-9 fyzických síťových karet
  1x dedikovaný management fyzického stroje
  2x iSCSI síťová karta (nevužívat tzv. teaming) využívaná výhradně “Parent” instancí Hyper-V
  2x iSCSI síťová karta (žádný teaming) dedikovaná pro iSCSI konektivitu přímo z virtuálních mašin

2x+ síťová karta (možný a doporučený teaming, VLAN atd.) pro aplikační využití serveru (tj. klasický back-end, front-end)

1x dedikovaná síťová karta pro Cluster Heartbeat

1x dedikovaná síťová karta pro Cluster Live Migration (doporučuje se raději 10Gbps)

- k výše uvedenému lze přidat ještě další síťovou kartu dedikovanou pro zálohování
- dodatečné přidání síťové karty do Core edice je docela problém
- nesnažit se rozchodit Hyper-V na Marvell síťových kartách, používat výhradně Broadcom/Intel (18)

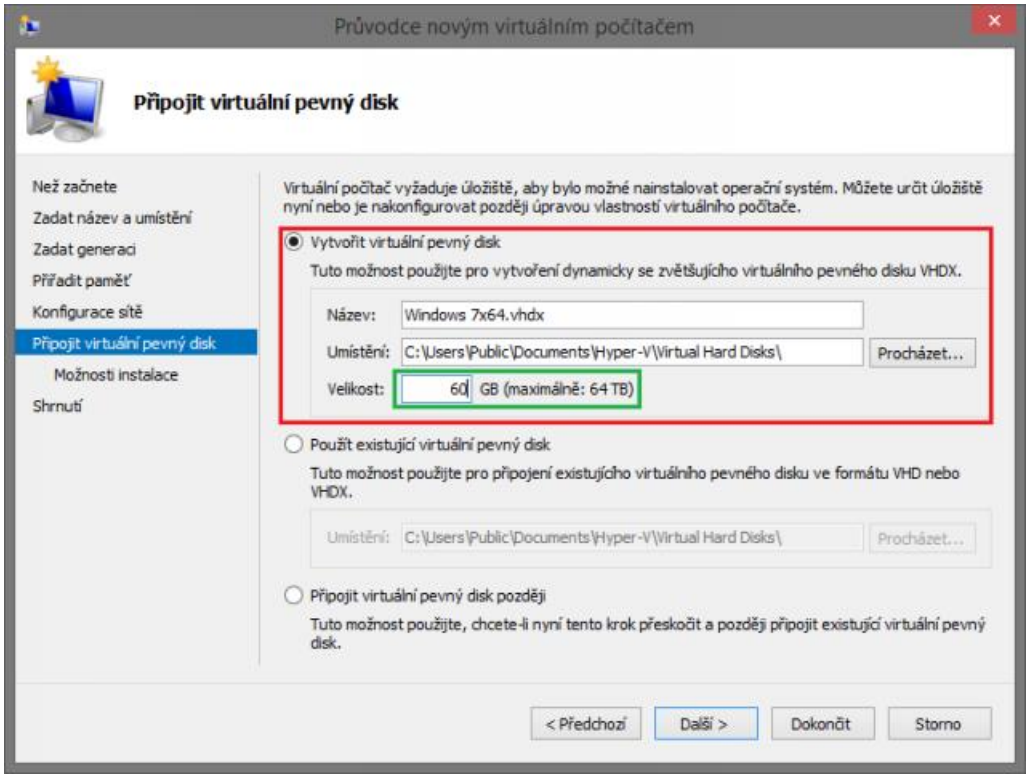


Obr. 16 Konfigurace Sítě

V dalším kroku, s názvem *Připojit virtuální pevný disk*, se může vytvořit nový virtuální pevný disk, použít již existující virtuální pevný disk nebo nakonfigurovat parametry disku později. Pokud se ponechá umístění disku beze změny, bude uložen do složky, která byla předtím vybrána jako výchozí pro celý virtuální stroj. Virtuální stroj může mít virtuální pevné disky na jiném oddílu nebo v jiné složce, podle potřeby. Soubor disku je dynamický a jeho velikost roste postupně. Je možné taky připojit již existující virtuální disk.

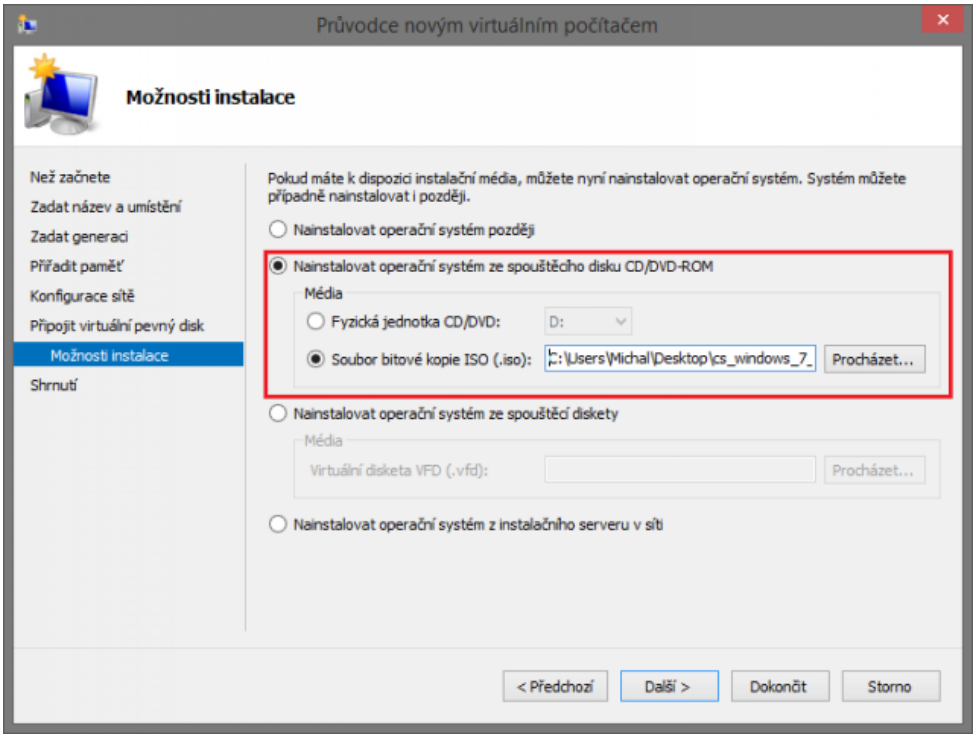
Doporučení na HDD pro tvorbu virtuálního serveru

- oddělit LUNy pro OS, LUNy pro uložení VHD s OS virtuálů, LUNy pro data aplikací virtuálů
- používat vhodný typ RAID
- instalovat MPIO software výrobce HW
- Zvolit správný typ disku reprezentovaného virtuálu – může to být VHD, pass-through disk nebo přímo připojený disk, nejčastěji prostřednictvím iSCSI. VHD má limit 2TB, ale výhodu v podpoře Hyper-V VSS Writeru. Pass-through může být větší než 2TB, ale musí se řešit extra podpora VSS, složité nastavení např. v Hyper-V clusteru atd. Přímé připojení iSCSI může být větší než 2TB, ale musí se řešit VSS, třeba pomocí EqualLogic ASM/ME nainstalovaného do virtuálu.
- VHD – vždy volit fixed size disky
- používat syntetický iSCSI řadič
- pokud je aplikačních dat méně, umístit je přímo do VHD disku
- a LUNech Hyper-V, které bude řízeno VMM, počítat nejen s velikostí vlastního VHD, ale započítat ještě velikost paměti virtuálu a maximální velikost ISO obrazu, který může být k virtuálu namapován ve virtuálním DVD (19)



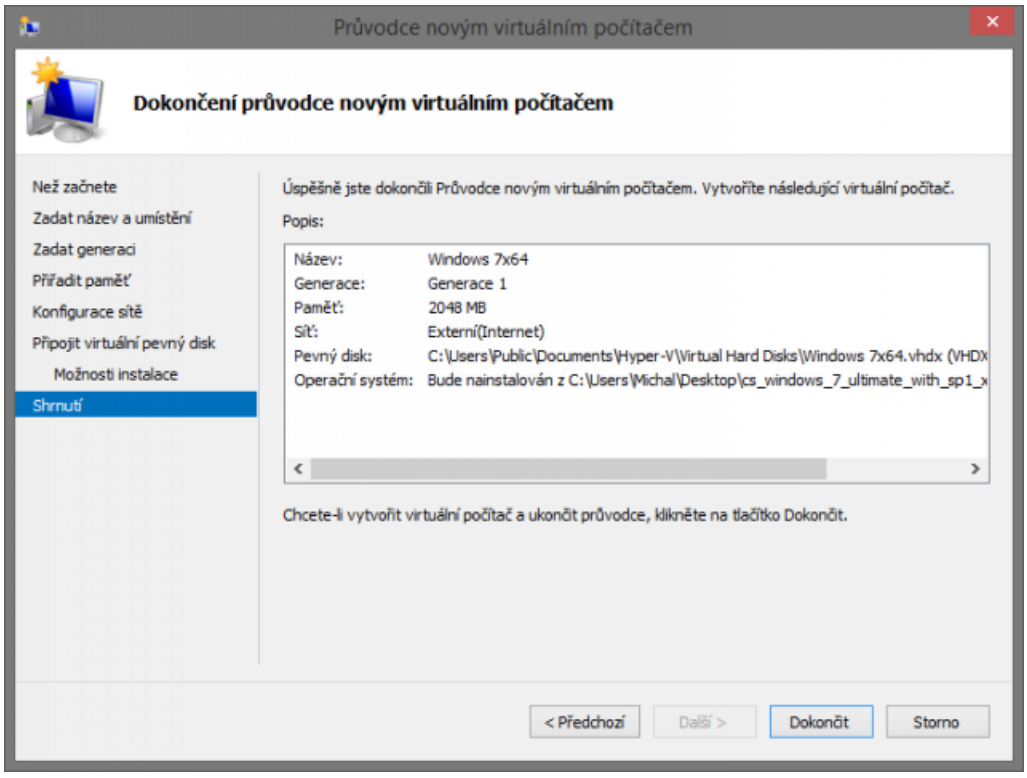
Obr. 17 Virtuální disk

V *Možnostech instalace* se volí instalační médium přes DVD mechaniku, .ISO soubor, virtuální VFD disk nebo nainstalovat operační systém ze síťového umístění. Jedná se o systém, který bude na virtuálním stroji naistalován po vytvoření. Je výhodnější systém nainstalovat při vytvoření virtuálního stroje kvůli přehlednější instalaci. Operační systém musí být podporován platformou Hyper-V.



Obr.18 Možnosti instalace

V celkovém shrnutí pak dostanete přehled o dosavadním nastavení. V tomto bodě je požadovaný virtuální stroj hotov. V celkovém přehledu se zobrazují údaje o vytvořením stroji.



Obr. 19 Dokončení instalace

Po dokončení se nově vytvořený virtuální stroj objeví v přehledu virtuálních počítačů. (18)

Doporučení pro vytvoření virtuálního stroje:

- Uvnitř virtuálů nainstalovat vždy nejnovější Integration Services (nemusí to být verze, kterou nainstaluje VMM)
- Volit zálohování, které využívá VSS (typicky Microsoft DPM Server), kombinovat s řešením výrobce HW, např. EqualLogic Auto-Snapshot Manager / Microsoft Edition
- Pokud to HW umožní, preferovat HW snapshoty proti SW snapshotům. Vetší rychlost zálohy/obnovy. Nutností je samozřejmě dostatečná disková kapacita na poli.
- Dbát na to, že u Hyper-V, které je nutné přenést na jiný HW, je nejprve potřeba provést export virtuálního stroje
- U kritických aplikací replikovat snapshoty do backup lokace (pro účely Disaster recovery)
- U nejkritičtějších aplikací počítat s geografickým clusterem
- Na virtuálním AD částečně zakázat synchronizaci času s hostitelem
- Nikdy neexportovat virtuální stroj, který je doménovým řadičem
- V Hyper-V serveru, na němž běží virtuální AD, nepoužívat ATA/IDE disky, ale SCSI
- Ve virtuálním AD nepoužívat virtuální IDE disk, místo toho použít virtuální SCSI disk
- Nepoužívat snapshot na AD, tj. při vypínání Hyper-V se musí virtuální AD korektně kompletně vypnout (Shut down guest OS), tj. nikoliv Save state
- Ve virtuálním AD nepoužívat diferenciální disky
- Případný restore virtuálního AD provádět výhradně podporovanými zálohovacími nástroji (tj. např. neobnovit bezhlavě snapshot z pole), podporovanou cestou je spustit Windows Server Backup ve virtuálním OS (pak existuje samozřejmě možnost DPM klienta nainstalovaného ve virtuálním OS)
- Nepoužívat VHD soubor, jenž pochází z již nainstalovaného doménového řadiče, k vytvoření nového doménového řadiče – vyhneme se tím problému při rollbacku update sequence number (USN)
- Spuštění sysprep na doménovém řadiči není podporováno (nikde, tj. ani na fyzickém stroji) (19)

6 Závěr

Cílem práce bylo objasnit a analyzovat serverovou virtualizaci ve firemním prostředí. Teoretická část diplomové práce se věnuje vývoji serverové virtualizace a jejím hlavním výhodám, které provádí uživatelům. V rámci teoretické části diplomové práce je analyzován historický vývoj serverové virtualizace až po její dnešní stav a úroveň, která se podřizuje trendu: virtualizovat všechno co je možné. Vzniká to z hlavní výhody virtualizace, která je šetření peněz a času které vznikají z údržby serverového hardwaru. V rámci teoretické části se diplomová práce věnuje i nástrojům serverové virtualizace, které ovlivňují úroveň virtualizačního prostředí. Hlavní podíl na trhu serverové virtualizace mají firmy Microsoft a platforma Hyper-V. Hlavni konkurent je firma VMware a platforma stejného jména. Právě proto je v rámci práci dbán zvlášť důraz na dané virtualizační nástroje. JE to zejména kvůli hlavnímu slovu v určování trendů ve virtualizace a taky postupnému přesouvání informační architektury do cloudu, který se ukazuje jako budoucnost pro úložiště dat i chod aplikací. V rámci teoretické části práce jsou platformy teoreticky objasněni. Práce se věnuje historickému vývoji a nárůstu kvality služeb potřebným k vytvoření virtualizačního prostředí.

Analytická část práce je věnovánu způsobům vytvořený virtualizačního prostředí, které by splňovalo požadavky, které jsou na virtualizaci kladeny. V rámci analytické části jsou zvrhnuty možnosti virtualizace. Konkrétně virtualizace sítí a sítového switche a virtualizace aplikací, které se postupně stávají, společně s datovým úložištěm terčem pro přesouvání na cloud nebo privátní virtuální prostředí. V diplomové práci je rozebrán přechod a požadavky firmy na cloud, který postupně začíná převládat ve firemním prostředí, či už se jedná o hybridní formu cloudu, nebo úplný cloud.

Hlavní část analytické části je věnována rozboru nástrojů pro virtualizaci, a to již výše zmiňováních Hyper-V a VMware. Rozbor je založen na analýze požadavků, které jsou vitální pro začínající firemní virtualizaci a umožnují následný přechod do privátního cloudu. Na zaklade prozkoumání a konzultování s odborníky z praxe o důležitosti a celkového hodnocení v jednotlivých kritériích byla provedena vícekriteriální analýza variant, ve které má nástroj Hyper-V malý náskok oproti VMware.

Cílem diplomové práce bylo definovat virtualizaci a její přínos v IT infrastruktuře. Po zhodnocení výsledků byla zvolena a doporučena, pro vytvoření virtuálního prostředí, platforma Hyper-V. Práce se věnuje vytvoření virtuálního stroje pro firmy, které začínají z virtualizací.

Vytvoření obsahuje doporučené nastavení a požadavky, které slouží jak o nápověda pro vytvoření virtuálního stroje určeného pro firemní prostředí. Doporučené nastavení byly zvoleny autorem na základe vlastních zkušeností a po konzultaci s odborníky z praxe. Virtuální stroj vytvořen s doporučeními nastavením často nesplňuje požadavky na virtualizaci. Platforma Hyper-V je pro své uživatelské prostředí, lehčí konfiguraci a v neposlední řade přechod na cloud Azure lepší nástroj pro uživatelé, který začínají modernizovat a migrovat informační prostředí na privátní virtuální servery privátní cloud, nebo využijí cloudové služby Azure, nebo jiného poskytovatele cloudových služeb. Vyplívá to zejména z hlavních výhod virtualizačního prostředí, a to odstranění závislosti na klasickém hardwaru a přinést dostupnost k datům a aplikacím na jakýmkoli místě a stroji.

7 Citovaná literatura

1. *Trask* [online]. Praha [cit. 2017-08-11]. Dostupné z: http://www.trask.cz/publikace/zn-53-soucasny-vyvoj-virtualizace-a-reseni-uzivatelskeho-prostredi/

3. POMAZAL, Jiří. Virtualizace v kostce. *Systemonline* [online]. [cit. 2017-8-07]. Dostupné z: https://www.systemonline.cz/clanky/virtualizace-v-kostce.htm

4. PAŠEK, David. TŘI Z NEJSILNĚJŠÍCH - SROVNÁNÍ SERVEROVÉ VIRTUALIZACE VMWARE VS. CITRIX VS. MICROSOFT. *Vmware* [online]. [cit. 201-8-04]. Dostupné z: http://www.vmwarenews.cz/vmw/vmwnews.nsf/0/53bb1b111be5a818c12575e5005f83a6

5.Techniky virtualizace počítačů. *Zpravodaj ÚVT MU* [online]. Brno [cit. 2017-08-11]. Dostupné z: http://webserver.ics.muni.cz/bulletin/articles/545.html

6. *Zabezpeceni-virtualniho-prostredi: systemonline* [online]. Praha [cit. 2017-08-12]. Dostupné z:https://www.systemonline.cz/virtualizace/zabezpeceni-virtualniho-prostredi.htm

7.TECHNET BLOG CZ/SK. Microsoft Hyper-V. *TechNet Blog CZ/SK* [online]. [cit. 2017-18-10]. Dostupné z: https://blogs.technet.microsoft.com/technetczsk/p/microsoft-hyper-v/

8. Virtualizace serverů. *Schindler-sys* [online]. [cit. 201-08-09]. Dostupné z: http://www.schindler-sys.cz/virtualizace-serveru/

9.*Přehled technologie Hyper-V* [online]. 2017 [cit. 2017-08-13]. Dostupné z: https://msdn.microsoft.com/cs-cz/library/hh831531(v=ws.11).aspx10.

https://m.systemonline.cz/virtualizace/virtualizace-v-praxi-4.-dil.htm

11. *Serverova-virtualizace* [online]. Praha, 2010 [cit. 2018-01-20]. Dostupné z: https://computerworld.cz/technologie/rychlokurz-serverova-virtualizace-a-site-5422

12. *Virtualizace v praxi* [online]. Praha, 2009 [cit. 2018-01-21]. Dostupné z: https://www.systemonline.cz/virtualizace/virtualizace-v-praxi-5.-dil.htm

13. *Virtualizace aplikaci* [online]. praha, 2016 [cit. 2018-01-10]. Dostupné z: http://archive.unicornsystems.eu/cz/novinky/clanek/virtualizace-aplikaci.html

14. COLLINS, Tom. Hyper-V vs. VMware: Which Is Best?. *Atlantech* [online]. 2016, 26.4.2016 [cit. 2018-03-24]. Dostupné z: https://www.atlantech.net/blog/hyper-v-vs.-vmware-which-is-best

15. HALLER, Martin. Hyper-V vs. VMware. *Martinhaller.cz* [online]. 11.12.2017 [cit. 2018-03-24]. Dostupné z: https://martinhaller.cz/know-how/hyper-vs-vmware-proc-si-vybrali-hyper/

16.Azure-Architektura [online]. Praha, 2017 [cit. 2018-03-24]. Dostupné z: https://docs.microsoft.com/cs-cz/azure/architecture/data-guide/scenarios/hybrid-on-premises-and-cloud

17.Windows Server Failover Clustering [online]. 2017 [cit. 2018-03-25]. Dostupné z: https://docs.microsoft.com/en-us/sql/sql-server/failover-clusters/windows/windows-server-failover-clustering-wsfc-with-sql-server

18. *Vytvoreni virtualni stroje v hyper-v* [online]. Praha, 2016 [cit. 2018-01-16]. Dostupné z: http://www.virtualnipc.cz/microsoft-hyper-v-4-vytvoreni-virtualni-stroje-v-hyper-v-2-2255

19. *Hyper-V doporučení* [online]. Praha, 2016 [cit. 2018-03-16]. Dostupné z: http://dolezel.net/post/2011/10/19/Hyper-V-doporuceni#.WrKS--jOWUl