

Univerzita Hradec Králové
Fakulta informatiky a managementu
Katedra informačních technologií

**Virtuální desktopy
na platformě VMware, Hyper-V a Citrix**

Diplomová práce

Autor: Bc. Marek Müller
Studijní obor: AI2

Vedoucí práce: Ing. Jan Budina

Prohlášení:

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

V Hradci Králové dne 12.11.2016

Marek Müller

Poděkování:

Rád bych poděkoval vedoucímu práce Ing. Janu Budinovi za cenné rady v průběhu přípravy a tvorby mé diplomové práce a poskytnutí technické podpory včetně serverů pro účely testování.

Anotace

Tato práce obsahuje a popisuje základní teoretické informace v oblasti virtualizace a virtualizačních platformách firem VMware, Microsoft a Citrix. Popisuje protokoly PCoIP, RDP a ICA, které slouží pro přenos obrazu virtuálních desktopů jednotlivých technologií.

Práce dále obsahuje informace a postupy k vytváření a instalaci virtuální infrastruktury, virtuálních desktopů a porovnává hypervisory ESXI, Hyper-V a XEN.

Práce porovnává tyto hypervisory na základě testů a to z hlediska výpočetního výkonu, nároků na šířku přenosového pásma a uživatelské přívětivosti.

Annotation

The work contains and describes the basic theoretical knowledge in the field of virtualization and virtualization platforms companies named VMware, Microsoft and Citrix. The work describes protocols PCoIP, RDP and ICA that apply to the image transfer of each virtual desktop technologies.

The work also contains information and procedures for creating a virtual infrastructure and compares hypervisors ESXI, Hyper-V and Xen.

The work compares these hypervisors based on tests in terms of computing power, the demands on bandwidth and user friendliness.

Obsah

1. Úvod	1
2. Základní pojmy a historie	2
2.1 Pojem virtualizace	2
2.2 Požadavky virtualizace	2
2.3 Historie	3
2.4 Hypervisor	4
2.5 Architektura hypervisorů	5
2.6. Techniky virtualizace počítačů	6
2.6.1 Plná virtualizace	7
2.6.2 Emulace/Simulace	8
2.6.3 Částečná virtualizace	9
2.6.4 Paravirtualizace	9
2.6.5 Aplikační virtualizace	9
3. Virtualizační technologie pro virtuální desktopy.....	11
3.1 VMware	12
3.1.1 VMware Hypervisor.....	12
3.1.2 Technologie pro VDI	13
3.1.3 Vytváření virtualizovaných desktopů	15
3.1.4 Protokoly pro VDI	16
3.1.4 Přístup k VDI z pohledu uživatele	17
3.2 Citrix	18
3.2.1 Hypervisor Xen	18
3.2.2 Technologie pro VDI	20
3.2.3 Protokol pro VDI	21
3.2.4 Přístup k VDI z pohledu uživatele	22
3.3 Microsoft	23
3.3.1 Hypervisor Hyper-V	23
3.3.2 Technologie pro VDI	26
3.3.3 Protokol pro VDI	27
3.3.4 Přístup k VDI z pohledu uživatele	28
3.4 Hardwarové limity	28
Praktická část.....	29
4. Infrastruktura pro virtuální desktopy.....	30

4.1	Infrastruktura pro virtuální desktopy-VMware	31
4.1.1	Horizon View Connection 7 a View Composer	32
4.1.2	Instalace a konfigurace vCenter Server	32
4.1.3	Instalace a konfigurace desktopů	33
4.2	Infrastruktura pro virtuální desktopy-Microsoft Hyper-V	34
4.2.1	Instalace role Hyper-V a Remote Desktop Services	35
4.2.2	Instalace a konfigurace desktopů	35
4.3	Infrastruktura pro virtuální desktopy-Citrix	36
5	Testovací metodika	37
5.1	Kolekce testovacích desktopů	37
5.2	Testovací skripty a způsob testování	37
6	Testy Infrastruktury	40
6.1	Test 1 – Kopírování souborů	40
6.2	Test 2 – Microsoft Office	40
6.3	Test 3 -Webový prohlížeč Chrome	41
7	Monitoring zátěže serverů a shrnutí výsledků	42
7.1	Test 1 – Kopírování souborů	43
7.2	Test 2 – Microsoft Office	47
7.3	Test 3 – Webový prohlížeč Chrome	50
8	Hodnocení výsledků testování	54
9	Závěr	57
10	Seznam použité literatury	58
	Seznam Zkratk	61
	Seznam obrázků	62
	Seznam tabulek	62

1. Úvod

Virtualizace se stává čím dál tím více populárním trendem v každé společnosti, která se zabývá IT a nabízí uživatelům nečekané technologické možnosti. Kromě technologické stránky věci jako je například maximalizace výkonů serverů nám především také přináší způsob, jak ušetřit náklady na provoz informačních systémů ve společnosti, což je v dnešní době velice důležité. V dnešní době se dá již říci, že virtualizace pokryla potřeby všech uživatelů a podniků.

Pro běžné uživatele osobních počítačů není virtualizace zatím tak rozšířena, ale stále se rozrůstá. Díky dnešním velmi výkonným serverům a cenově dostupnému virtualizačnímu prostředí je dnes virtualizace dostupná prakticky pro každého.

Pojem virtualizace není zdaleka tak nový a počátky virtualizace sahají do 60. let minulého století. Více o historii virtualizace jako takové se lze dočíst v kapitole „2.3 Historie“. U virtualizace je převratná skutečnost, že v současné době dochází k naprosto masivní virtualizaci, a to nejen konsolidací datových center, nýbrž se prosazuje zejména technika virtualizace stolních počítačů, datových úložišť a aplikací.

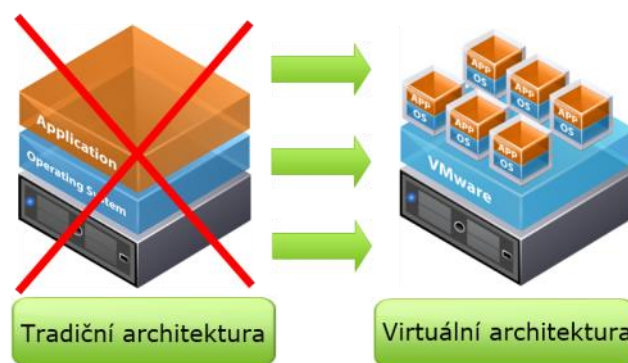
V této práci budou rozebrány základní principy z oblasti virtualizace a virtualizační technologie pro virtuální desktopy na třech různých platformách.

Praktická část této práce popisuje postupy k vytváření infrastruktury pro správu virtuálních desktopů na platformách VMware, Microsoft a Citrix a jejich vzájemné porovnání. Všechny tři platformy nabízí různé konfigurace infrastruktury, jejich výhody a nevýhody, které je zajímavé porovnat a otestovat v praxi.

2. Základní pojmy a historie

2.1 Pojem virtualizace

Pojmem virtualizace se v dnešní době rozumí abstrakce výpočetních zdrojů a rozdělení výpočetních zdrojů jednoho fyzického systému. Nad touto vrstvou abstrakce je tedy možné spustit jednu i více na sobě nezávislých virtuálních stanic. Lze tedy říci, že pomocí virtualizace jsme schopni vytvořit virtuální hardwarové prostředí, pod kterým si můžeme představit celý server, případně jeho části využít pro více než jeden operační systém a tedy jeden počítač se pak z venku jeví jako několik samostatných PC. Tyto virtuální počítače mohou mít různé operační systémy a rozdílné hardwarové počítačové platformy (architektury).



Obrázek 1 Virtualizace (Zdroj: [1])

Instalace operačního systému se do tohoto virtuálního hardwaru provádí stejným způsobem jako na hardware fyzický. Výsledná instalace operačního systému do virtuálního prostředí se pak jeví jako množina souborů, která představuje virtuální disk s nainstalovaným systémem a několika konfiguračními soubory. [1]

2.2 Požadavky virtualizace

V roce 1974 vyšel článek napsaný Geraldem J. Popkem a Robertem P. Goldbergem. Ve svém článku definovali formální požadavky a základní vlastnosti, které musí každý hypervisor neboli Virtual Machine Monitor (VMM) splňovat, aby byla virtualizace co nejvíce efektivní.

- Equivalence / Fidelity – Program spuštěný v rámci VMM by měl vykazovat stejné chování, jako kdyby byl spuštěn na ekvivalentním stroji bez VMM
- Resource control / Safety – VMM musí mít kompletní kontrolu nad virtuálními zdroji

- Efficiency / Performance – Většina strojových instrukcí musí být provedena bez zásahu VMM

Tato kritéria jsou zjednodušená, ale i přesto se dají použít pro rozhodnutí, zda daná architektura podporuje efektivní virtualizaci. [2]

2.3 Historie

První koncept a význam pojmu virtualizace byl navrhnout v 60. letech firmou IBM. Díky této technologii lze rozložit výpočetní výkon mezi jednotlivé oddělené virtuální stroje a tedy umožnit spustit v mainfraimu (sálový počítač) více procesů najednou. Důvodem pro rozložení výpočetního výkonu do několika virtuálních strojů byl požadavek na zvýšení efektivity využití dostupného hardwaru, a zejména fakt, že před nasazením virtualizace nemohl mainframe zpracovávat více jak jeden proces současně, což vedlo k plýtvání zdroji. V 80. -90. letech však byla virtualizace téměř zapomenuta a nepotřebná, jelikož s příchodem architektury na platformě x86 byl vytvořen model klient-server. Tento model na serverových operačních systémech jako Linux a Windows umožňoval administrátorům spojení několika pracovních stanic do jednoho funkčního celku s podstatně levnějšími náklady. Avšak tato situace měla za následek podstatnou řadu problémů. Na každém serveru byla spuštěna pouze jedna aplikace v důsledku, že jedna aplikace způsobí pád té druhé. Bylo tedy zapotřebí velké množství serverů, jejichž provoz stál nemalé prostředky na energii, chlazení, počet zaměstnanců a samotný běh systémů.

Tyto problémy měly za následek zpětné nasazení virtualizace. Zakladatelem virtualizace jakou známe dnes, byla v roce 1999 společnost VMware a představila virtualizační produkt pro virtualizaci počítačů na platformě x86. V roce 2003 uvedla firma Connectix první verzi Virtual PC for Windows. Tuto firmu později koupil Microsoft a začal budovat produkt s názvem HyperV. Poslední velkou firmou, která začala virtualizovat a odkoupila kolos jménem XenSource byla firma Citrix. Velký zlom nastal v roce 2005 kdy firmy AMD a Intel otevřely cestu virtualizace do středních a malých podniků tak, že implementovaly technologii pro podporu virtualizace do svých procesorů.

2.4 Hypervisor

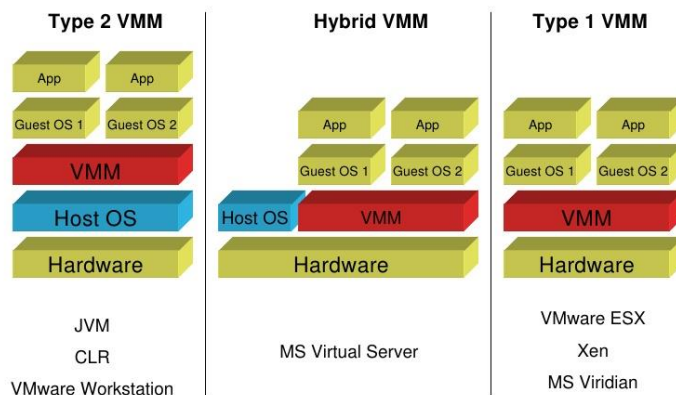
Hypervisor - převážně označovaný jako Virtual Machine Monitor, je označení pro softwarovou komponentu, která umožňuje vytvářet a spouštět více operačních systémů na jednom počítači. Operační systémy jsou spouštěny v oddělených prostorech, nazývaných virtuální stoji. Tyto virtuální stoji sdílí hardwarové prostředky a hypervisor je zodpovědný za přístup virtuálních strojů k tomuto fyzickému hardwaru, řídí jejich běh a zároveň je od sebe odděluje. Dále vykonává privilegované instrukce a přistupuje k fyzickým I/O zařízením. Vrstva hypervisoru musí být nadřazená všem na PC běžícím operačním systémům. John Scott Robin definoval ve svém práci rozlišení na tři třídy hypervisorů, a to podle jejich umístění.

Typ1 (Nativní) – Hypervisor tohoto typu je označovaný jako bare metal nebo nativní a označuje hypervisor umístěný a běžící přímo na hardwaru počítače. Odlišuje se tím, že pro svůj běh nevyžaduje žádný operační systém a instaluje se tak jako samostatný software. Tato metoda umožňuje úplné oddělení jednotlivých virtuálních počítačů a představuje klasické provedení architektury virtuálního stroje jakožto v roce 1960 vyvinutý hypervisor CP/CMS firmou IBM. Tento typ využívá ESXI od firmy VMware, Microsoft Hyper-V a Xen-Server.

Typ2 (Hostovaná) – Hypervisor tohoto typu je označovaný jako hostovaný a označuje hypervisor spouštěný v rámci normálního operačního systému. Hypervisor běží nad operačním systémem fyzického počítače, což způsobuje zpomalení pokynů hostitelských operačních systémů, které musí projít přes větší počet vrstev. Největšími zástupci této třídy jsou VMware Workstation, VirtualBox.

Hybridní – U tohoto typu jsou hostitelský operační systém a hypervisor spuštěny zároveň vedle sebe na hardwarové vrstvě. Virtuální stroje jsou spuštěny nad hypervisorem, který napodobuje celé fyzické prostředí. VMM může privilegované instrukce přímo provádět, kdežto u HVM musí privilegované instrukce být nejdříve softwarově překládány. HVM ale nemusí přímo tyto privilegované instrukce spouštět, jelikož jsou emulované v softwaru.[3]

Virtual Machine Monitor Approaches



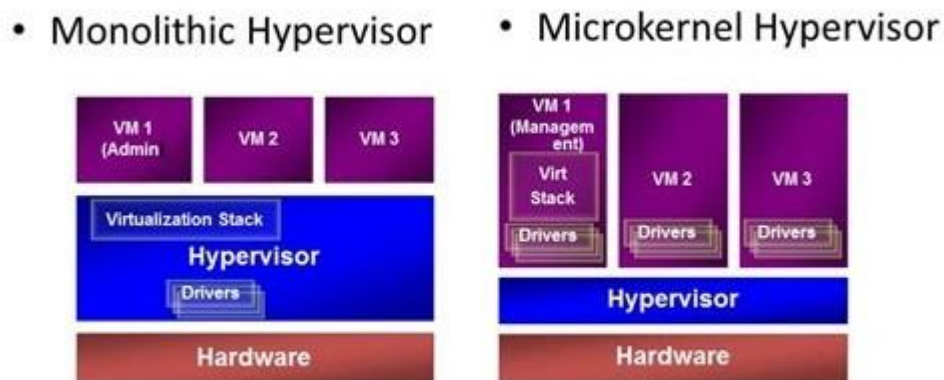
Obrázek 2 Typy Hypervisorů (Zdroj: <http://www.slideshare.net>)

2.5 Architektura hypervisorů

Hypervisor může mít dva druhy architektury. Dá se rozdělit podle použitého designu na monolitický a mikrokernel.

Monolitický – jedná se o hypervisor, jehož architektura nahrazuje jádro operačního systému svým vlastním jádrem (kernel), které je poměrně komplexní a obsahuje veškerou funkcionalitu, kterou očekáváme od operačního systému. Obsahuje veškeré ovladače pro jednotlivá zařízení, plánovač úloh, správu paměti, souborové systémy a musí být podporován výrobcem hardwaru. Virtuální stanice poté přistupují k hardwaru prostřednictvím hypervisoru a ovladačů, které jsou v něm uloženy. Tyto ovladače musí být speciálně vytvořeny pro použití v hypervisoru. Takovýto hypervisor obsahuje větší množství kódu, čímž se zvyšuje pravděpodobnost výskytu nějaké chyby či zanesení kódu třetích stran. Tento hypervisor používá VMware u virtualizace na ESXI serveru.

Mikrokernel – neboli Microhypervisor je na první pohled jednodušší způsob, jak s hypervisorem pracovat a používat ho. Mikrokernel má naprosté minimum funkcí, které jsou nezbytné ke sdílení hardwaru mezi virtuálními stroji. Prvním je plánovač úloh, který přiděluje fyzická jádra procesoru. Druhým je správa paměti, která zajišťuje, že žádné dva virtuální stroje nebudou přistupovat ke stejnému místu fyzické paměti. Nejzásadnějším rozdílem s monolitickou architekturou je, že Microsoft nemusí po výrobcích hardwaru vyžadovat nové verze ovladače pro hypervisor, jelikož všechny ovladače jsou kompatibilní

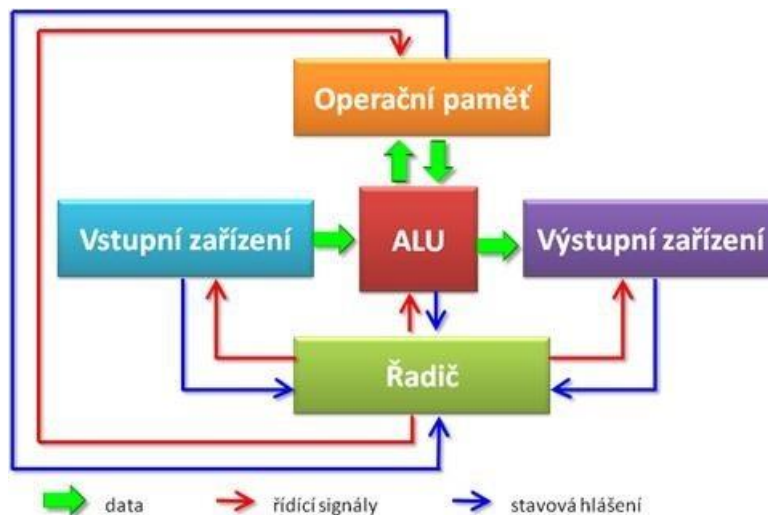


Obrázek 3 Architektura Hypervisorů (Zdroj: [4])

a jsou přímo od výrobců pro zařízení pracující pod Windows. Tímto se zamezí nutnosti používat ovladače třetích stran a zamezíme tím riziku zanesení kódu a nestability, čímž zaručíme vyšší bezpečnost a výkon. Tuto implementaci hypervisoru používá Microsoft Hyper-V. [4]

2.6. Techniky virtualizace počítačů

Běžné počítače odpovídají architektuře modelu John von Neumanna a skládají se z několika základních komponent. Na základní úrovni se jedná o procesor, paměť a periferie. Tyto komponenty dále členíme a explicitně pracujeme s diskem, klávesnicí, myší, grafickým subsystémem, síťovým rozhraním apod. Namísto těchto fyzických komponent si lze představit abstraktní variantu v podobě virtuálních komponent, jejichž složením vytvoříme virtuální počítač. Na něm pak lze spustit operační systém a vytvořit tak virtualizované prostředí. Samotnou virtualizaci lze provádět na několika úrovních. [5]



Obrázek 4 Architektura John Von Neumanna (Zdroj: wiki.sps-pi.cz)

2.6.1 Plná virtualizace

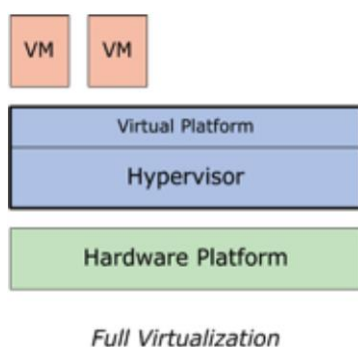
Plná virtualizace je nejčastěji používána na desktopech, kde virtualizujeme všechny součásti počítače. Hostovaný stroj je emulován pomocí virtualizačního hardwaru. V tomto případě se neemuluje procesor, tedy platformy musí být shodné (stejně sady instrukcí procesorů) a hostované operační systémy i aplikace běží v nativním režimu. V tomto prostředí nemůže operační systém žádným způsobem poznat, že nemá přístup k fyzickému vybavení počítače, a tedy že je virtuální. Jedná se o stav, kdy dochází k plnému oddělení fyzické vrstvy, veškeré programy běží pouze na virtuálním hardwaru a přístup k fyzickému vybavení je vždy zprostředkován. Příkladem je například VMware, Virtual Box, Virtual PC a XEN.

Výhody:

- hrubý výpočetní výkon
- snadná přenositelnost aplikací/virtuálních operačních systému na jiný hardware
- hostitelský ani hostovaný operační systém nemusí být nijak upraveny

Nevýhody:

- pomalé I/O operace- umí řešit Intel VT (tato technologie je v procesorech implementováno od listopadu roku 2005) a AMD Pacifica
- velké náklady na nákup licencí na virtuální systémy



Obrázek 5 Plná virtualizace (Zdroj: www.datamation.com)

2.6.2 Emulace/Simulace

Jedná se o nejstarší techniku virtualizace. Základním principem emulátoru je softwarový překlad strojových instrukcí hostovaného systému na strojové instrukce hostitelského stroje, jinými slovy se tedy emuluje i procesor včetně registrů, paměť ROM cílové platformy a zbytek hardware. I přesto, že se jednou přeložené úseky aplikace ukládají do paměti, takže je není třeba při příštím volání znovu překládat. Jedná se o nejméně efektivní způsob virtualizace. Na druhou stranu je to jediný způsob jak virtualizovat jinou architekturu. Lze i emulovat mnohprocesorový stroj na počítači s jedním procesorem a podobně. K nejznámějším emulátorům patří BOCHS, PearPC, QEMU. [6]

Výhody:

- možnost na libovolné platformě spustit systém a aplikace libovolné jiné (danou aplikací podporované) platformy.
- virtualizační software je obyčejnou aplikací, běží i bez administrátorských práv
- hostitelský ani hostovaný systém nemusí být nijak upraveny

Nevýhody:

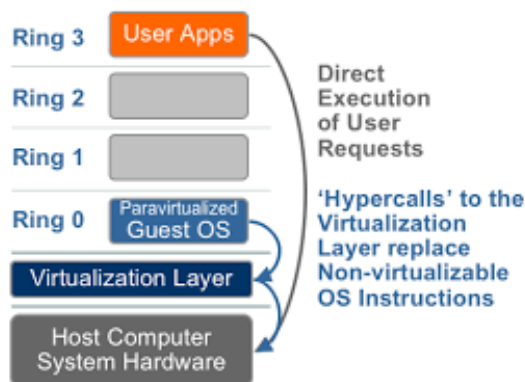
- nízký výkon
- problémy s kompatibilitou emulovaného hardwaru

2.6.3 Částečná virtualizace

V případě této virtualizační techniky jde o simulaci instancí několika prostředí hardwaru. Na tomto hardwaru běží hostitelský stroj a obzvláště pomocí této technologie virtualizujeme adresní prostor. Takovéto prostředí podporuje sdílení zdrojů a izolaci procesů. Nelze zde ale oddělit jednotlivé instance hostovaných operačních systémů a strojů. Obecně zde tedy nelze hovořit o virtuálním stroji, ale jedná se o významný přístup, a to z historického hlediska. V současné době používají tuto techniku operační systémy rodiny Microsoft Windows i operační systémy typu Linux.

2.6.4 Paravirtualizace

Paravirtualizace je příkladem toho, že virtuální stroj nemusí za každou cenu simulovat hardware a je blízká technologii plné virtualizace. Místo toho nabízí v případě potřeby přístup k hardwaru fyzického počítače speciální aplikační programové rozhraní ke sdělení svých požadavků hostujícímu systému, který je označován jako hypervisor. Takto upravené aplikační programové rozhraní může být použito jen z upraveného hostovaného jádra operačního systému. Výhodou tohoto přístupu je docílení vysokého výkonu. Nevýhodou je již zmíněná úprava hostovaného systému, která je nutná a nelze jí provést bez dostupných zdrojových kódů. Většinou tyto úpravy provádí přímo výrobce, který tyto kódy zná. Mezi hlavní zástupce této technologie patří Win4lin a Xen.



Obrázek 6 Paravirtualizace (Zdroj : www.simplex.com)

2.6.5 Aplikační virtualizace

V případě aplikační virtualizace neboli virtualizace aplikací se jedná o aplikace, které se spouští na daném fyzickém počítači, využívají místní zdroje, ale běží ve virtuálním stroji. Poskytuje tedy speciální virtualizované prostředí pro běh serverových a desktopových

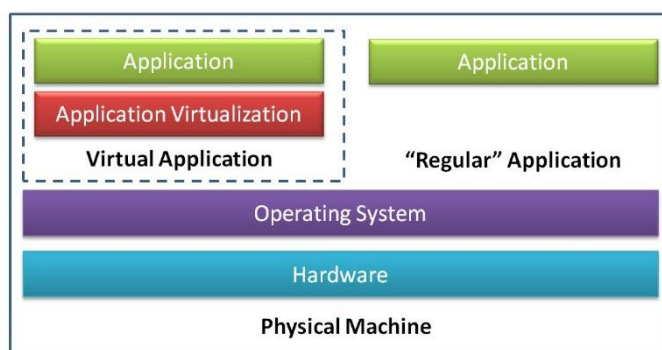
aplikací. Rozdíl mezi tímto a klasickým virtualizačním modelem jsou takové, že u klasického jsou aplikace instalovány přímo do operačního systému. Jednotlivé aplikace se snaží zapisovat do stejných systémových souborů a registrů a právě to, že všechny aplikace využívají tytéž systémové soubory a registry přináší řadu problémů. Vznikají konflikty mezi jednotlivými aplikacemi a často dochází k nestabilitě či dokonce pádu operačního systému. Právě těmto problémům se snaží předcházet jednotlivé techniky aplikační virtualizace tím, že virtualizované aplikace nikdy nezapisují do stejných systémových souborů či registrů, a tedy nemůže (nemělo by) docházet ke konfliktům mezi jednotlivými aplikacemi, které jsou virtualizované.

U klasického prostředí má aplikace velkou řadu závislostí na operačním systému a to ať už se jedná třeba například primárně o registry nebo ovladače. Pokud je aplikace nekompatibilní, lze tento problém vyřešit touto technikou virtualizací aplikací. Jedná se tedy o nejvhodnější řešení při vzájemné nekompatibilitě instalovaných aplikací.

Aplikace přímo nainstalované do operačního systému s sebou přinášejí i další problém. Jedním z nich je, že tyto aplikace sdílejí nejen systémové soubory a registry, které byly již zmíněny, ale i knihovny DLL. Může se tak stát, že jedna aplikace bude vyžadovat určitou verzi této knihovny DLL, načež jiná aplikace bude vyžadovat pro svůj běh odlišnou verzi této samé knihovny. Takovýto stav je u klasického provozování aplikací prakticky neřešitelný, jelikož po instalaci druhé aplikace dojde k přepsání původní verze knihovny DLL a bude tak fungovat pouze poslední nainstalovaná aplikace. Řešení tohoto problému je v případě klasického provozování aplikací velmi nákladné a časově náročné. Naproti tomu techniky aplikační virtualizace řeší tento problém rychle, efektivně a levněji.

Virtualizace aplikací řeší tento problém s přepisováním tak, že vytvoří vlastní sandbox (bezpečnostní mechanismus pro oddělování běžících procesů) a tento sandbox je pak k dispozici pouze pro konkrétní aplikaci. V situaci, kdy jednotlivé aplikace využívají stejné systémové prostředky, jsou tyto prostředky připojeny přímo k aplikaci, kde jsou spuštěny spolu s aplikací v mezipaměti daného operačního systému. Takovýmto způsobem vzniká virtuální aplikace, kde aplikace využívá sandboxu určeného pro danou aplikaci.

Tyto techniky virtualizace aplikací nám usnadňují a urychlují nasazení nových aplikací, řeší nejčastější problémy klasického provozování aplikací a aplikace si vzájemně nepřepisují systémové soubory, kde tak nedochází ke konfliktům mezi aplikacemi. Pro velkou řadu firem se jedná o levnější řešení bez zdlouhavého testování nových aplikací. Mezi hlavní zástupce patří VMware, Citrix a Java Virtual Machine od firmy Oracle.



Obrázek 7 Virtualizace aplikací (Zdroj: www.vmware.com)

3. Virtualizační technologie pro virtuální desktopy

V dnešním světě již nabízí virtualizační řešení několik desítek společností, ale pouze pár z nich se stalo komerčně úspěšnými a jsou po technologické stránce výborně vybaveny. Podle studie, kterou udělala firma Gartner [7] se počet instalovaných serverů VM k roku 2011 téměř zdvojnásobil a domnívá se, že na konci roku 2016 dosáhne 86% veškeré serverové zátěže. Dále se podle této studie zvýšilo přijetí cloudových řešení, a to o 200% za pouhé dva roky, což znamená, že virtualizace je již spíše pravidlem než výjimkou. Na dnešním trhu s virtualizačním řešením jsou tři velcí konkurenti. Předním výrobcem je firma VMware s největším zastoupením na trhu, která, jak už bylo zmíněno, jakožto první dokázala virtualizovat platformu x86 a dodnes si roli leadera udržuje. Dalším zástupcem je firma Citrix, která přišla na trh s open source řešením hypervisoru Xen. Nejmladším zástupcem celého tria virtualizačního řešení je Hyper-V od společnosti Microsoft. Tento produkt byl uveden v roce 2008 a svým rychlým rozvojem a již předešel podíl Citrixu na trhu a pomalým tempem dohání VMware. Procentuální podíl jednotlivých výrobců na trhu se liší, ale odhady k prosinci roku 2015 jsou, že VMware tvoří 69% trhu, Microsoft 34% a Citrix zbylých 12%.[35] V dalších kapitolách budou tyto produkty podrobně představeny a popsány z hlediska návrhu architektury a přístupu k uživateli.[8]

3.1 VMware

Společnost VMware byla založena v roce 1998 v Palo Alto v USA. V současné době se jedná o zdaleka největší společnost na trhu s virtualizačním softwarem pro virtualizaci a cloud computing desktopů a serverů na světě. O šest let později v roce 2004 byla společnost odkoupena společností EMC Corporation, která je největším výrobcem a dodavatelem produktů a služeb v oblasti správy a ukládání informací na světě. V roce 2008 s příjmy okolo 2 miliard amerických dolarů a více než 40 pobočkami se postupně stala nejvíce rostoucí softwarovou firmou na světě. V České republice tato firma pobočku zatím nemá, ale jsou zde certifikovaní partneři firmy, kteří nabízejí různé produkty, řešení a školení. Produkty VMware poskytují prostředí pro běh virtuálních strojů, které zvyšují využitelnost serverů a dalších prostředků. Dále zlepšují výkon, zdokonalují zabezpečení a snižují náklady a složitost poskytování podnikových služeb. [9]

3.1.1 VMware Hypervisor

Z předchozích kapitol víme, že hypervisor převážně označovaný jako Virtual Machine Monitor, je označení pro softwarovou komponentu, která umožňuje vytvářet a spouštět více operačních systémů na jednom počítači. První produkt tohoto typu od společnosti VMware byl vydán v roce 2001 pod názvem ESX. Jedná se o bare-metal (monolitický) hypervisor s binárním překladem instrukcí, který se instaluje přímo na hardware příslušného serveru. Monolitickým modelem je dáno, že hypervisor je od prvního začátku vyvíjen na stejných základech, a to kvůli nepřítomnosti dostupných operačních systémů a procesorů, které by podporovaly virtualizační technologie. Vytváří robustní virtualizační vrstvu mezi hardwarem a operačním systémem.

ESX obsahuje dva prvky, a to VMkernel a Servisní konzole. VMkernel je, jak už název napovídá, vlastní hypervisor, speciálně navržený pro běh více VM a má tři základní komponenty. Tyto komponenty jsou plánovač zdrojů, I/O zásobník a ovladače hardwaru. Servisní konzole je virtuální stroj, ve kterém je nainstalována a upravená verze linuxové distribuce Red Hat. Slouží hlavně jako rozhraní pro správu, zavaděč VMkernelu a k administraci virtuálních strojů, jakožto provádění funkcí skriptů, instalaci komponent třetích stran pro hardwarové monitorování a zálohování systému. [9]

V roce 2004 představil VMware podporu 64 bitové architektury u operačního systému v ESX, a to docílením nových instrukčních sad v procesorech Intel a AMD. O necelé tři roky později byl představen vylepšený hypervisor ESXi, který nahradil verzi 4.1 ESX. Největší rozdíl mezi ESX a ESXi je, že novější verze má servisní konzoli implementovanou přímo v kernelu ESXi. Veškeré úlohy, které konzole zastávala, byly tedy zavedeny do hypervisoru nebo jejich úlohu převzaly speciální programy pro toto navržené. Tyto programy komunikují přes externí komunikační rozhraní. Zatímco ESX zabíralo na disku 2GB, tak ESXi zabírá pouze 32 MB paměti na disku s pouze nejnужnějsími funkcemi pro chod hypervisoru. K administraci na systému ESXi slouží DCUI (Direct Console User Interface). DCUI má konfigurační úkoly jako nastavení administračního hesla, prohlížení logů, restartování do původního nastavení a nastavení síťového rozhraní. Pro IT pokročilou administraci lze použít pomocí VMware vSphere Client. Jedná se o klienta, který provádí úkony vzdáleně přes síťové rozhraní pomocí externích programů. Od verze vSphere 5.0 si hypervisor sám vybírá, zdali pro jednotlivé virtuální stroje použije binární překlad nebo hardwarově asistovanou virtualizaci, aby bylo možné využít co nejvíce potenciálního výpočetního výkonu. Tento výběr probíhá na základě vlastností procesoru a aplikací, které jsou spuštěny nebo pouze ruční změnou nastavení pomocí administrátorských nástrojů. Centralizovanou správu clusterů virtualizovaných serverů provádí služba vCenter. V roce 2010 dochází k přejmenování VMware ESXi na VMware vSphere Hypervisor. [11]

3.1.2 Technologie pro VDI

VDI (Virtual desktop infrastructure) znamená virtualizace pracovních stanic neboli virtualizaci desktopových infrastruktur. Jedná se o technologii, pomocí které lze oddělit operační systém a uživatelská data od klientské pracovní stanice a umístit je do prostředí datacentra, kde poběží zcela bezpečně a virtuálně na serveru.

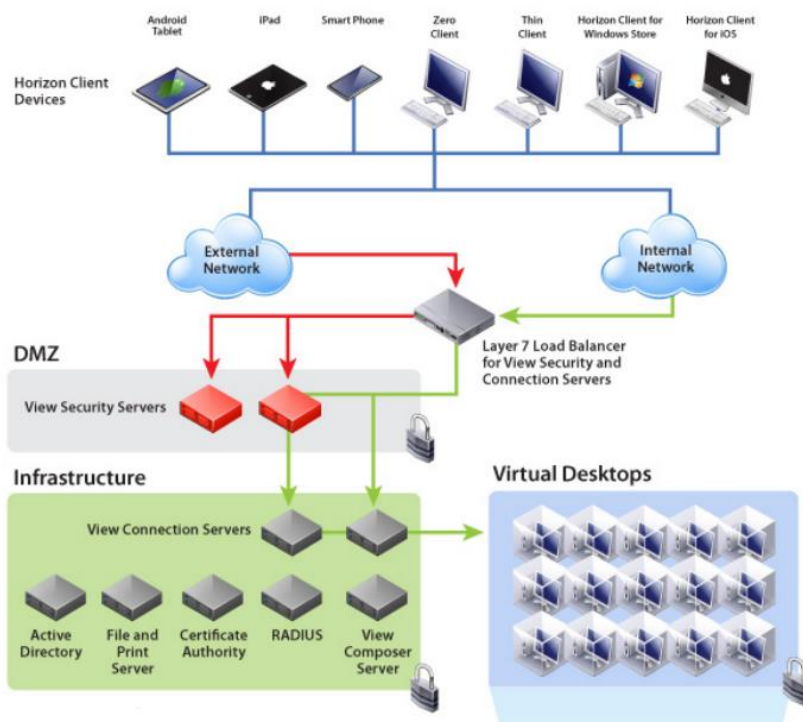
U technologie VDI dochází ke spouštění izolovaného uživatelského virtuálního systému. Takový systém v síti, se pro ostatní síťová zařízení tváří jako oddělený fyzický počítač, avšak ve skutečnosti běží podobně jako virtuální server nad hypervisorem. Pro připojení k takovému desktopu se používá specializovaný klient „*connection broker*“, který poskytuje připojení a validaci uživatele. Ostatní součásti, jako je uživatelské rozhraní nebo terminál, pak již uživatel získává pomocí standardních protokolů TCP/IP. Virtuální desktopy můžeme rozdělit na 3 druhy.

Prvním typem je takzvaný privátní desktop. Jedná se o desktop, který je určen jen pro práci jednoho konkrétního uživatele. Na tomto desktopu má uživatel svůj vlastní hard disk, na kterém se nachází operační systém, aplikace a uživatelská data (user profile data). Dle rozhodnutí správce, je možno povolit uživateli instalaci aplikací. Většinou je používán operační systém z rodiny Microsoft desktopových OS, jako je XP či Windows 7,10.

Další variantou je sdílený desktop. U tohoto typu desktopu dochází k přístupu více uživatelů, kteří pracují hromadně nad jedním operačním systémem. V tomto případě je používán serverový OS, který má možnost hostovat v jednu chvíli více připojení. Na rozdíl od typu privátního desktopu nelze uživateli povolit instanci aplikací. Ovládání jako restart a vypnutí jsou činnosti, které v této variantě má výhradně pod kontrolou správce.

Třetím typem je takzvaný skupinový desktop. Stejně jako v případě privátního desktopu je virtuální desktop v jednu chvíli používán jedním uživatelem. Nicméně je možné, že v jiný časový okamžik s ním bude pracovat druhý uživatel. Jedná se tedy o sdílení desktopu, ale ne v jeden konkrétní okamžik. Typické využití pro tento typ desktopů je pro směnný provoz, kdy dopoledne desktop používá jeden uživatel a odpoledne či navečer zase někdo jiný. U takovýchto desktopů je možné pomocí základních funkcí VDI udělat to, aby jeden virtuální HDD v jednu chvíli používalo jako svůj HDD více skupinových virtuálních desktopů.

Příprava nových desktopů bez VDI znamená použít fyzický počítač, připojit jej k síti a nainstalovat operační systém z předpřipravené image. Zde je složité správně připravit a odladit image, což je vzhledem k nesourodému prostředí často problém. Připravit správnou kombinaci ovladačů a programů bývá obvykle složité a pracné. Ve chvíli, kdy je funkční image, je nutné ji roz distribuovat po síti na cílová místa, což může být náročné na konektivitu, a to hlavně v případě propustnosti linky. Následně proběhne konfigurace na lokálních počítačích, které se tak stávají funkčními. Základní komponenty všech VDI řešení jsou si velice podobné. Jde o virtuální infrastrukturu, virtuální desktopy, connection broker, protokol pro připojení ke vzdálenému virtuálnímu desktopu a přístupovou bránu. [12]



Obrázek 8 Technologie VDI VMware (Zdroj: www.vmware.com)

K připojení na virtualizované desktopy slouží komponenta VMware Horizon Client, a to pomocí tenkých i tlustých klientů. Tlustý klient je reprezentován aplikací VMware View Client, kterou je nutné instalovat v případě uživatele na osobní počítač. Tenkým klientem je webový prohlížeč. Horizon View obsahuje mnoho efektivních nástrojů pro vytváření virtualizovaných desktopů z pohledu administrátora. Tento nástroj je možné využívat ve spolupráci s virtualizovaným operačním systémem. Vhodným řešením je také připojení pomocí fyzického tenkého klienta. Zástupcem je například zařízení Wyse od firmy Dell či zařízení od firmy Igel.

3.1.3 Vytváření virtualizovaných desktopů

Veškeré desktopy, které se vytvářejí, jsou umístěné v takzvaných poolech (logické celky pro virtuální stroje) a to ve stromové struktuře. Technologie Horizon View nabízí při vytváření desktopů několik různých typů, které mají rozdílný dopad na zabrané místo na diskovém poli a způsob používání uživateli. Nás bude zajímat pool s takzvanými plovoucími desktopy a to zejména díky velké úspoře místa. Plovoucí desktopy mají souvislost s technologií linkovaných klonů a vytvářejí kolekci desktopů, kdy uživatel se po opětovném přihlášení nemusí dostat na stejný desktop.

3.1.4 Protokoly pro VDI

Pro připojení k virtuálnímu desktopu se využívají protokoly pro vzdálený přístup. Tyto protokoly poskytují koncovým uživatelům s grafickým rozhraním zobrazení pracovní plochy, která je umístěná v datovém centru. Lze použít protokoly PCoIP, protokol VMware Blast nebo protokol RDP (Remote Desktop Protocol) od firmy Microsoft. Administrátor může nastavit zásady, jaký protokol bude používán nebo umožnit uživatelům zvolit si protokol po přihlášení na pracovní plochu.

PCoIP je proprietární protokol pro vzdálené desktopy, vyvinutý společností Teradici. Protokol licenčně je používán společností VMware a je implementován v nových verzích softwaru VMware View 4 a vyšších. V aktuálním Horizon 7 se od PCoIP upouští a přechází se kompletně na protokol Blast. PCoIP je založen na protokolu UDP a umožňuje efektivnější využívání sítí prostřednictvím zapouzdření zobrazovacích paketů v UDP. PCoIP je zabezpečen šifrovaným spojením AES-128. Protokol funguje jak v lokálních vysokorychlostních sítích LAN, tak i ve WAN sítích s omezenou šířkou pásma. Protokol byl vytvořen speciálně pro síťovou distribuci virtuálních desktopů, kde byl kladen důraz na optimalizaci pro nasazení na sítích s vysokou latencí a nízkou propustností. Protokol je optimalizovaný pro přenos obrazu s vysokým rozlišením, podporuje také vzdálené připojení USB zařízení a je sám o sobě bezpečný, jelikož nepřenáší žádná aplikační data. Celý protokol je postaven na využití vykreslování obrazu a tedy jednotlivých pixelů přímo na hostiteli. Ten obraz vykreslí, následně zašifruje obrazovou informaci a ta je poté přenesena po síti ke klientovi. Díky tomuto principu se tedy nepřenášejí celá data, ale pouze zašifrovaná obrazová informace.

Protokol PCoIP průběžně analyzuje obraz, zkoumá ikony, text a ostatní grafiku, kde hledá pro každou část obrazu optimální kodek pro zkomprimování. Protokol používá multi-kodekovou platformu, umožňující pro každý typ obrazu vybrat správný kodek, který dokáže obraz efektivně komprimovat. Jedná se o bezztrátovou kompresi, aby nedocházelo k deformaci obrazové informace. Protokol je možné použít i pro přenos prostřednictvím internetu. [13]

Dále VMware podporuje doručení virtuálního desktopu prostřednictvím protokolu VMware Blast a jazyka HTML5. Tento způsob umožňuje uživateli přístup k osobnímu VMware View desktopu přímo z jakéhokoliv HTML5 kompatibilního webového prohlížeče

(například Chrome, Internet Explorer, Firefox). Uživatelé tedy stačí vlastnit prohlížeč s podporou HTML 5, který se používá při autorizaci uživatele na úvodní straně. Přenos je oproti PCoIP šifrován pomocí SSL a je více náročný na procesorový výkon serveru. Je to způsobeno dvojnásobným zpracováním obrazové informace, jednou pro jazyk HTML 5 a podruhé pro protokol VMware Blast. [14]

RDP je protokol určený pro přenos grafického uživatelského rozhraní jednoho počítače na jiný počítač a umožňuje tak vzdálený přístup. Serverová část protokolu se nazývá Remote Desktop Services a ve výchozím nastavení pracuje na portu TCP 3389. [15]

3.1.4 Přístup k VDI z pohledu uživatele

Přístup a doručení virtuálního desktopu k uživateli v podobě již zmíněného tlustého klienta Horizon View je nutné instalovat na osobní počítač. Připojení probíhá jak už přes protokol PCoIP nebo jde o připojení k desktopu k View pomocí jakéhokoliv HTML5 kompatibilního webového prohlížeče díky protokolu VMware Blast. U poslední verze Horizon View 7, který již nepotřebuje HTML5 webový prohlížeč je z hlediska uživatele dobré vědět, že podporuje možnost přesměrování USB zařízení, podporu tisku, sériového rozhraní či možnost mapování lokálního disku do virtuálního desktopu.

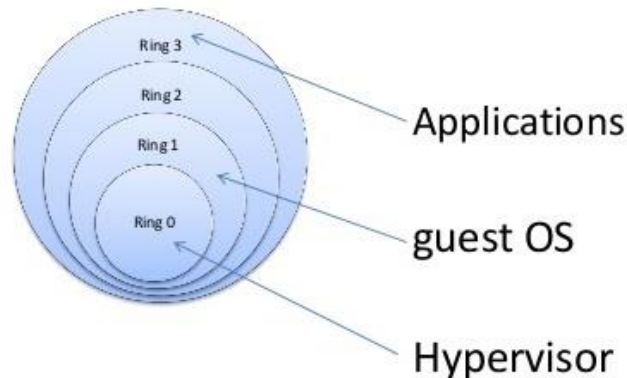
3.2 Citrix

Společnost Citrix založil v roce 1989 bývalý vývojář IBM Ed Lacobucci ve státě Texas. Citrix se původně jmenoval Citrus, ale později změnil svůj název na Citrix kombinací slov Unix a Citrus. Xen vznikl jako výzkumný projekt na univerzitě v Cambridge tvůrcem Ianem Pratterem. V roce 2003 byl oficiálně vydán Xen 1.0, který podporoval v té době pouze jediný 32bitový procesor. Krátce poté byla vydána verze 2.0. V roce 2004 hlavní tvůrce projektu založil firmu XenSource. Tato firma dodávala řadu vylepšení a komerčních nástrojů umožňujících nasazení v podnikové sféře. Verze 2.0 využívala paravirtualizaci, takže bylo možné virtualizovat pouze upravené verze operačního systému Linux. O rok později byla vydána verze 3.0, která přidala možnost využití hardwarově asistované virtualizace a podporu virtualizačních sad v procesorech, díky čemuž již šlo v Xenu provozovat i systémy bez upraveného jádra. Tato verze navíc podporovala technologie Intel VT-x a později u AMD-V. V roce 2007 koupila společnost Citrix Systems společnost XenSource a produkt s označením Xen se začal propagovat pod značkou Citrix. Od této doby je XenSource distribuován jako balíček obsahující hypervisor Xen, aplikaci XenCenter a přednastavený rodičovský oddíl hypervisoru. Aplikace XenCenter je grafická konzole, která se stará o správu virtuálních strojů. Nyní je k dispozici verze Xen Serveru s označením 6.5, která byla vydána na jaře roku 2015. [18]

3.2.1 Hypervisor Xen

Hypervisor Xen řadíme do skupiny mikrokernelizovaných hypervisorů prvotně založené na paravirtualizaci, avšak jak už bylo řečeno od verze Xen3.0 využívá i hardwarově asistovanou virtualizaci, kde již není potřeba využívat upravené jádro operačního systému a je zajištěna úplná podpora. Xen je tedy primárně určen pro běh na linuxových platformách a díky plné virtualizaci dosahuje úctyhodných výkonnostních výsledků. U koncepce asistované virtualizace se nám tedy nabízí, že tu lze provozovat i jiné systémy než linuxové, například od firmy Microsoft.

Hypervisor si lze u Xenu představit jako vrstvu, která odděluje hardware od systému. Hypervisor se inicializuje před samotnou instalací jádra a jeho činnost spočívá v obsluze Input/Output operací a v dohledu nad pamětí jednotlivých virtuálních strojů. Celý systém si lze představit jako rings(kruhy), které představují stupně ochrany. Základní část hypervisor běží v ringu 0, jádra operačních systémů v ringu 1 a ostatní aplikace běží převážně v ringu 3.

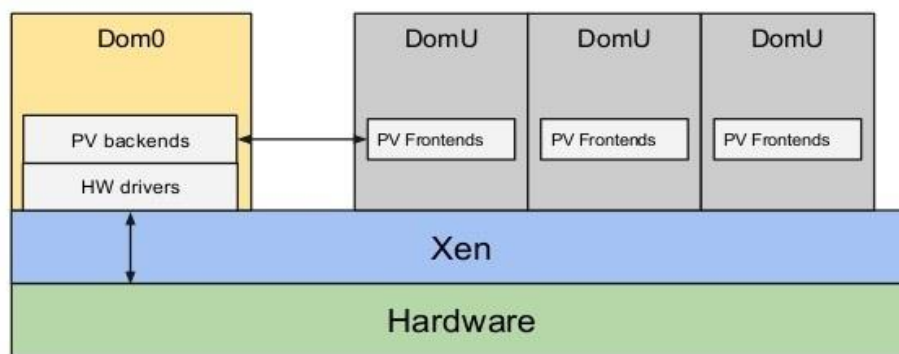


Obrázek 9 Xen Rings (Zdroj: www.slideshare.net)

Virtuální stroje jsou u Xenu nazývány doménami. Existuje několik druhů domén a těmi nejvýznamnějšími doménami jsou doména nula (**Dom0**) jako hostitel a doména u (**DomU**) jako host.

Dom0 neboli privilegovaná doména je hostitelský systém s upraveným jádrem přímo pro Xen. Tato doména je zavedena současně při zavádění hypervisoru ve formě bootloder modulu. Umožňuje nastavovat a spravovat ostatní domény za pomoci démona xend a dalších nástrojů. Dom0 má v architektuře hypervisoru Xen důležitou roli. Součástí Xenu nejsou ovladače zařízení ani uživatelské rozhraní. Tyto ovladače jsou poskytovány nástroji běžící v rámci Dom0 Další důležitou úlohou je obsluha fyzických zařízení, na které má Dom0 jako jediný přístup. Přístup je zprostředkován virtuálním ovladačem, který je rozdělen na dvě části. Jedna část se nachází v Dom0 (backend) a ta druhá v DomU (frontend). Backend část ovladače komunikuje s ovladačem fyzického zařízení, jenž je součástí Dom0. Tímto způsobem je realizováno řízení přístupu k fyzickému zařízení a Dom0 je jediná doména, která je vytvářena přímo Xenem.

DomU neboli neprivilegovaná doména je host a představuje ho každý virtualizovaný počítač. Tato doména je vytvořena pomocí nástrojů běžících v rámci dom0. Standardní úroveň oprávnění této doméne neumožňuje volat již zmíněná hypercall volání, ale tato oprávnění jim mohou být poskytnuta. Pro komunikaci hardwaru a této neprivilegované domény je potřeba, aby doména implementovala frontendovou část rozděleného ovladače. [19][20][21]

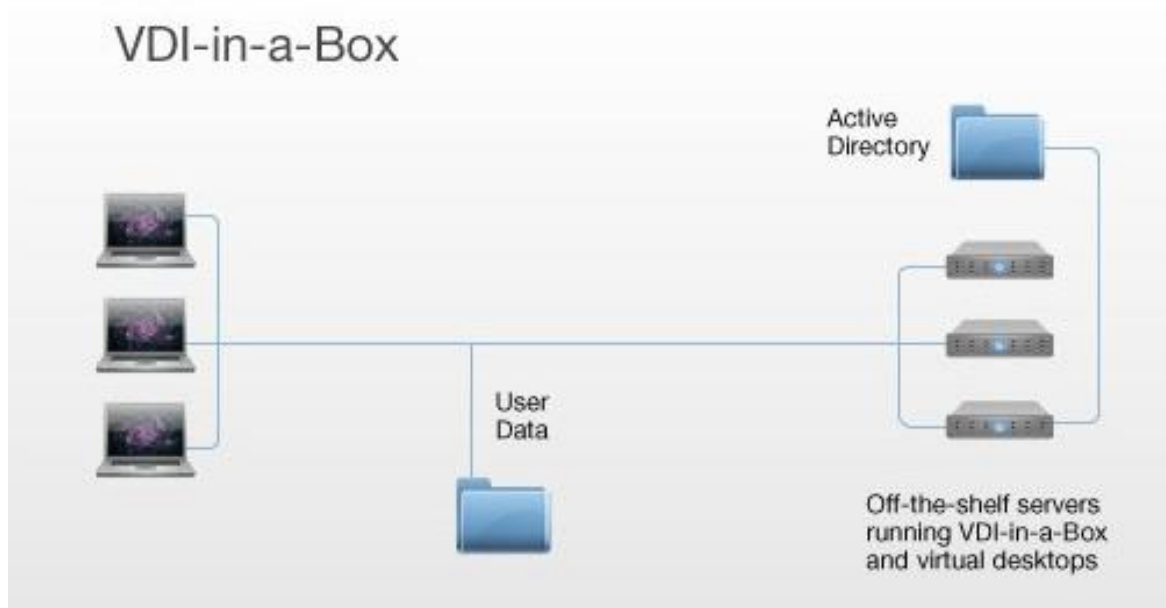


Obrázek 10 Architektura Xen (Zdroj: wiki.xen.org)

3.2.2 Technologie pro VDI

Firma Citrix nabízí dvě VDI řešení. První s názvem XenDesktop. Jedná se o nejstarší VDI řešení ze všech tří zmíněných produktů v diplomové práci a velkou výhodou je nezávislost na použitém hypervisoru. VDI řešení se zaměřuje primárně na management nástroje a komunikační protokoly, přičemž nezáleží na tom, jaké virtuální prostředí je pro běh desktopů použito. XenDesktop VDI je postaveno na technologii přístupu k virtuálním desktopům Citrix FlexCast kde se jedná o hostované nebo lokální, fyzické nebo virtuální desktopy.

Druhé řešení se nazývá VDI-in-a-box. Toto řešení odstraňuje přes 60% součástí z tradiční VDI infrastruktury včetně správy serverů a sdíleného úložiště tak, že vytvoří síť (grid) samostatných serverů s lokálním úložištěm. Toto řešení umožňuje Windows administrátorům rychleji doručit centrálně spravované virtuální desktopy jakémukoliv uživateli, na jakémkoliv zařízení. Jedná se tedy o připravený server, který je nazýván jako vdiManager, který lze nainstancovat, ať už v případě Citrixu do XenServeru nebo do VMware ESXi či Microsoft Hyper-V, a jednoduše dokonfigurovat. [22]



Obrázek 11 VDI-in-a-Box (Zdroj: www.oldanygroup.cz)

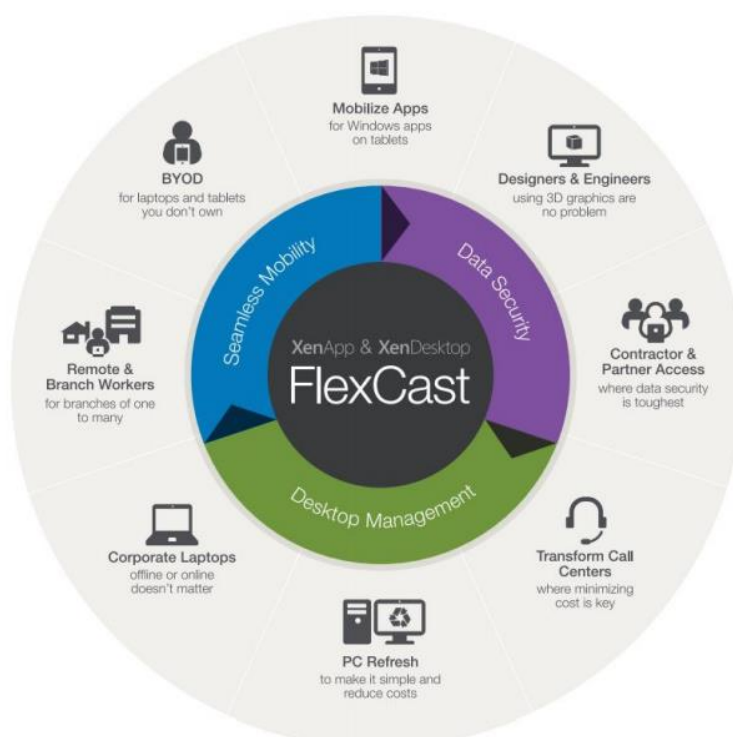
3.2.3 Protokol pro VDI

Independent Computing Architecture (ICA) je proprietární protokol vytvořený firmou Citrix Systems. První verze protokolu byla vyvinuta v roce 1989. ICA určuje specifikace pro přenos dat mezi serverem a klienty, taktéž není vázán na žádnou platformu. Slouží ke vzdálenému ovládání počítače uživatelem, kdy uživatel na klientském počítači využívá klientský software Citrix XenApp nebo Citrix WinFrame k zobrazení grafického rozhraní, které je spuštěno na vzdáleném počítači. Protokol je hodně podobný protokolu RDP, ačkoliv hlavní rozdíl je v tom, že ICA protokol má výhodu v případě omezeného připojení k internetu, a to díky potřebě malé šířky přenosového pásma. ICA protokol je dostupný přes protokol TCP na portu 1494 nebo zapouzdřený v CGP protokolu na portu 2598. Každá relace ICA pak vytváří a používá dynamicky přidělený TCP port v rozsahu od 1025 do 5000, pro komunikaci mezi

serverem a klientským zařízením. Funkčnost protokolu lze snadno zobrazit pomocí prostředků sledování sítě nebo nástroje pro analýzu sítě Wireshark. [23]

3.2.4 Přístup k VDI z pohledu uživatele

Přístup a doručení virtuálního desktopu k uživateli probíhá pomocí klienta Citrix XenDesktop, který je potřeba nainstalovat na osobní počítač. Jedná se o řešení pro virtualizaci desktopů, které poskytuje Windows desktopy ve formě cloudové služby na vyžádání jednotlivým uživatelům. Poskytuje rychle a bezpečně individuální aplikace nebo kompletní desktopy každému uživateli tak, že uživatelé mohou pracovat se svými desktopy na libovolném zařízení, a to kdekoliv. Součástí XenDesktop je i virtualizační aplikace XenApp, která svým uživatelům umožňuje připojit se ke svým aplikacím z různých typů počítačů či mobilních zařízení. XenDesktop využívá speciální technologii, která zajišťuje plnohodnotné použití aplikací na dotykových obrazovkách nebo přizpůsobuje data na přenos vyhovující mobilním sítím. Klient podporuje velké množství platforem (Windows, Mac, Linux, Android, apod.).



Obrázek 12 Vlastnosti XenDesktop a XenApp (Zdroj: [24])

3.3 Microsoft

Společnost Microsoft vstoupila na trh virtualizace v roce 2003, a to koupením společnosti Connectix. Firma se zaměřila především na verzi produktu Virtual PC určenou pro platformu PC a udělala z ní dva produkty. Jedním z nich bylo tedy již zmíněné Virtual PC a druhým Virtual Server. Tímto tahem vznikly první kroky virtualizace firmy Microsoft. Oba produkty představovaly softwarové řešení virtualizace. [25]

K provozu Virtual serveru byly potřeba navíc služby IIS (Internet Information Services), protože rozhraní pro správu bylo realizováno jako webové rozhraní. Později Microsoft vydal integrovanou verzi Virtual Serveru společně s produktem System Center Virtual Machine Manager. V roce 2008, pár měsíců po vydání systému Windows Server 2008, byl vyvinut Hyper-V. Jedná se o hypervisor hardwarové virtualizace, který byl integrován do operačního systému Windows Server 2008. Jedná se o klíčovou virtualizační technologii firmy Microsoft. V roce 2009 přišel na trh Windows Server 2008 R2. V dalších letech byl vydán Windows Server 2012 R2, kde největšími rozdíly oproti verzi 2008 R2 byly hlavně ohledně výkonu. Windows Server 2012 R2 disponoval 320 logickými procesory, 4 TB fyzické paměti, 2 048 virtuálními procesory na jednoho hosta a mohl mít až 1 024 aktivních virtuálních strojů. Místo toho Windows Server 2008 R2 disponoval pouze s 64 logickými procesory, 1 TB fyzické paměti, 512 virtuálními procesory na jednoho hosta a mohl mít 384 aktivních virtuálních strojů, což je opravdu znatelný rozdíl mezi oběma verzemi. [26]

3.3.1 Hypervisor Hyper-V

Hypervisor Hyper-V od společnosti Microsoft byl vyvíjený pod označením Viridian. Jedná se o virtualizační platformu pro 64 bit systémy. Hyper-V je dostupný zdarma ve Windows serverových operačních systémech, a to včetně licencovaného Windows Server Standard edition s omezením na 4TB RAM a maximálního počtu uživatelů založeného na typu licence. Hyper-V je tedy serverová virtualizace postavená na hypervisoru. Hardware tohoto serveru musí podporovat možnost virtualizace na úrovni procesoru Intel VT nebo AMD-V.

Hyper-V vzniklo ve dvou variantách. Ve Windows Server 2008 R2 s Hyper-V je hypervisor přímo součástí operačního systému a je na rozhodnutí správce, jestli daná instalace Windows Serveru 2008 bude obsahovat roli Hyper-V či nikoliv. Druhá varianta vznikla jako Windows Hyper-V Server 2008 R2, kde se jedná pouze o virtualizační platformu a není zde grafické uživatelské rozhraní. Tato varianta obsahuje pouze jádro systému Windows a

samotný hypervisor Hyper-V, tedy má složitější správu prostřednictvím konzole s příkazovým řádkem. Je zde nainstalována služba MCC (Microsoft Management Console), což je konzole pro administraci. Součástí tohoto serveru je vylepšený hypervisor Hyper-V 2.0. Nová verze přinesla oproti předchozí několik funkcí, díky kterým se přiblížila konkurenci, a to hlavně firmě VMware.

Hlavní možností bylo připojit uložště přes SCSI řadič za běhu virtuálního stroje. Tomuto připojení se říká tzv. migraci virtuálních počítačů (live migration), která za provozu technologie Hyper-V přesune běžící virtuální počítače z jednoho fyzického serveru na jiný, aniž by to mělo vliv na dostupnost virtuálního počítače pro uživatele. [27]

Hyper-V řadíme do skupiny mikrokernel hypervisorů využívajících hardwarově asistovanou virtualizaci. To znamená, že pro běh tohoto hypervisoru je nutné mít server s procesory, které podporují virtualizační technologie. Tento hypervisor neobsahuje žádné ovladače pro zařízení a jsou zde obsaženy pouze základní funkce k provádění virtualizačních funkcí. Skutečnost, že v hypervisoru nejsou přítomny ovladače, má za následek větší stabilitu, větší bezpečnost hypervisoru a vyšší výkon samotného systému. Instalace hypervisoru Hyper-V spočívá v nainstalování samotného Windows Serveru a až poté je přidána takzvaná role Hyper-V, která instaluje mezivrstvu hypervisoru mezi hardware a operační systém. Původní operační systém je přesunut do takzvaného rodičovského oddílu a až poté se instalují tzv. dětské oddíly. [28]

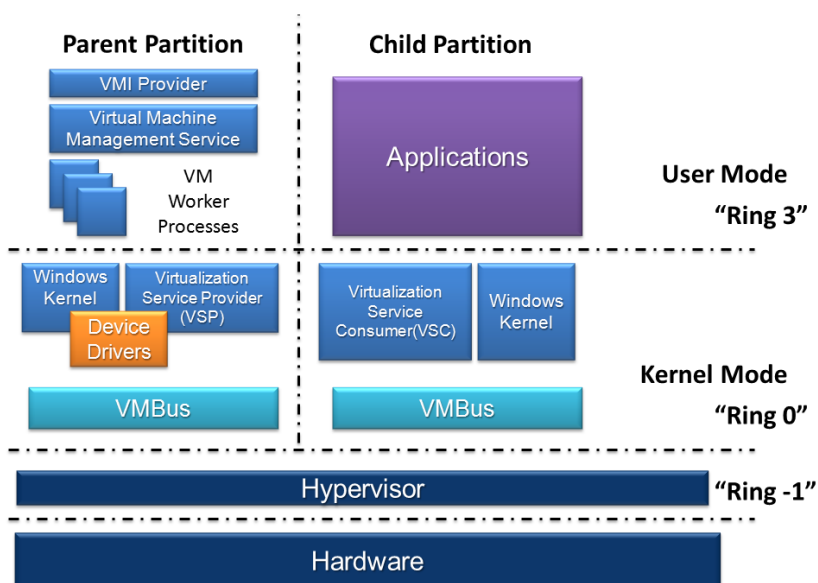
Rodičovský oddíl je někdy nazýván hlavní popř. mateřský oddíl a slouží pro zajišťování virtualizačních služeb. Tento hlavní oddíl je vlastníkem virtualizačního systému a v tomto oddílu jsou přítomny všechny ovladače systému. Tyto ovladače tento oddíl vlastní a dále je předávají virtuálním strojům, v kterých jsou přítomny v dětských oddílech. V poslední řadě jsou v rodičovském oddílu uloženy ostatní komponenty a služby jako fronta požadavků na vstupy/výstupy, jednotlivá zařízení a vlastní jádro systému.

V dětském oddíle, někdy nazývaném jako podřízený, se nacházejí a běží vlastní virtuální počítače. Tento oddíl komunikuje s rodičovským prostřednictvím VMBUS a volání hardwaru jde přes tento kanál. Tento oddíl neposkytuje vždy stejné funkce. Veškeré komponenty a funkce závisí na typu operačního systému, který se bude do tohoto oddílu instalovat. V této závislosti mohou nastat tři různé situace (scénáře) podřízených oddílů. [29]

Prvním scénářem je podřízený oddíl s OS Windows podporující technologii Hyper-V. Tyto oddíly obsahují dvě komponenty. V případě, že operační systém ve virtuální počítači zjistí, že je virtualizován nad hypervisorem, začne využívat první komponentu VSC (Virtualization Service Client). Jedná se o komponentu komunikující přes VMBUS s VSP (Virtualization Service Provider) za účelem využití hardwarových prostředků. Druhou komponentou je tzv. „Enlightenments“. Jedná se o plugin, který umožňuje plné využití podpory Hyper-V ve virtuálním operačním systému. V těchto komponentách se tento případ liší od ostatních a výhodou tohoto řešení je, že operační systém přistupuje k hardwaru nikoli emulovaně, ale přímo přes ovladač disku. [31][30]

Druhým scénářem jsou podřízené oddíly s OS jiným než Windows, ale přesto podporují hypervisor Hyper-V. Podřízený oddíl tedy neví o přítomnosti virtualizačních technologií, natož o přítomnosti hypervisoru. V tomto případě je využita komponenta VSC od poskytovatelů třetích stran. Komunikace komponent VSC a VSP přes kanál VMBUS probíhá stejně jako u předešlého řešení a díky VSC od poskytovatelů třetích stran je tak možné využít výhod hypervisoru Hyper-V.

Posledním scénářem je nainstalovaný operační systém, který není z firmy Microsoft a neobsahuje podporu Hyper-V. Takovýto OS netuší, že běží ve virtualizovaném prostředí. V takovémto případě je veškerý hardware a komunikace s tímto operačním systémem emulována, a proto zde nebude dosahováno takového výkonu než v předcházejících typech podřízených oddílů.



Obrázek 13 Architektura Hyper-V (Zdroj: en.wikipedia.org)

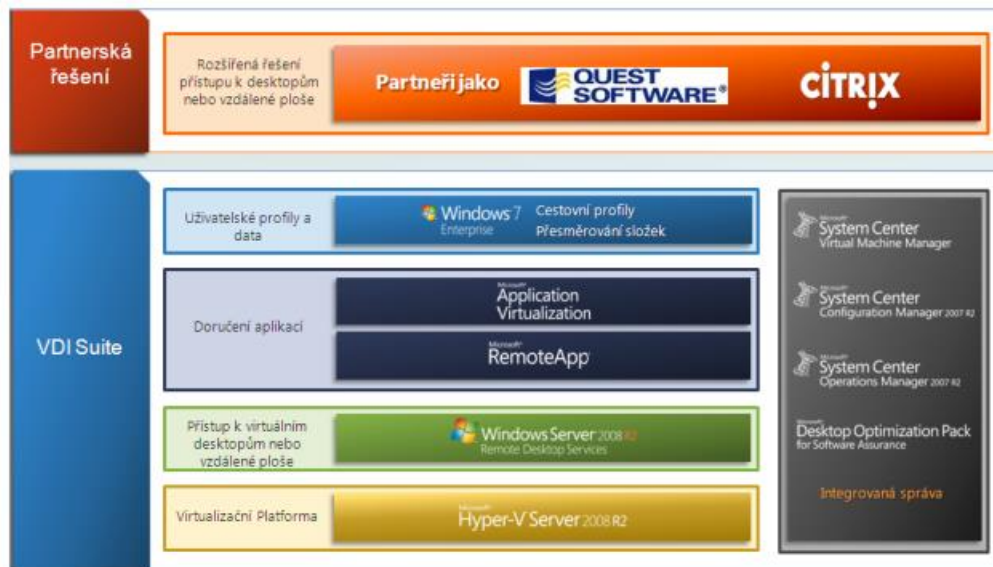
3.3.2 Technologie pro VDI

Virtualizace desktopů v případě společnosti Microsoft funguje pomocí vzdálené plochy RDV (Remote Desktop Virtualization), kde virtuální infrastruktura běží na serveru.

RDS je složena z těchto částí: [30]

- Remote Desktop Services (RDS) – tato služba slouží k přístupu uživatele ke vzdálené ploše nebo virtuálnímu desktopu pomocí protokolu RDP.
- Microsoft Application Virtualization for Remote Desktop Services (App-V for RDS) – tato služba slouží pro převod aplikací do formy centrálně spravovaných služeb a umožňuje distribuci ostatním uživatelům pomocí protokolu RDP. Aplikace běží na serveru a uživatel se zobrazuje pomocí protokolu RDP na jeho klientské stanici.

- Microsoft Virtual Desktop Infrastructure (VDI) – architektura VDI se skládá z komponent Hyper-V, RDS a produktů Microsoft Systém Center. Tento systém umožňuje desktopovým systémům běžet na hypervisoru v datacentru a uživatel k němu přistupuje pomocí RDP protokolu. Jedná se jednak o virtuální desktopy, které jsou identické, anebo o osobní virtuální desktopy upravené podle požadavků uživatele.



Obrázek 14 Microsoft Virtualization (Zdroj: <http://winblog.blob.core.windows.net>)

3.3.3 Protokol pro VDI

Pro připojení ke klientovi Remote Desktop Client (RDC) a komunikaci koncových zařízení s virtualizovanými stroji se využívají u firmy Microsoft protokoly RDP a RemoteFX pro vzdálený přístup.

Remote Desktop Protocol (RDP), jak už bylo řečeno, je síťový proprietární protokol. Připojení pracuje na principu klient-server, kdy uživatel na svém PC využívá jednoduchého klienta pro zobrazení grafického uživatelského prostředí, které je spuštěno na vzdáleném počítači. Poprvé byl protokol představen ve Windows NT 4.0. Protokol RDP je zapouzdřen a zašifrován šifrou RC4 s 128 bitovým klíčem v rámci protokolu TCP. Serverová část protokolu se nazývá Remote Desktop Services a ve výchozím nastavení pracuje na portu TCP 3389. [15]

Technologie RemoteFX navíc nabízí zvýšený grafický výkon přes protokol RDP díky využití speciální grafické karty, která podporuje RemoteFX. Speciální kartou je například karta Grid K1, Grid K2 od firmy NVIDIA či grafické karty od firmy AMD s přívlastkem FirePro. RemoteFX nabízí využití virtuálního desktopu na podobné úrovni jako běžný osobní počítač, a to díky 3D virtuálnímu adaptéru.

3.3.4 Přístup k VDI z pohledu uživatele

Přístup a doručení virtuálního desktopu k uživateli probíhá v případě Microsoftu pomocí balíčku Microsoft VDI Suite. Jedná se o správu vhodnou pro menší nasazení se spolehlivým protokolem RemoteFX využívající MS Hyper-V. Dalším je aplikace pro vzdálený přístup „RemoteApp“, která nabízí a umožňuje virtualizaci pracovní plochy a aplikací systému Windows, a to kdekoli a na jakémkoliv zařízení. Tato aplikace je součástí systému Windows a není jí tedy potřeba nijak stahovat a instalovat.

3.4 Hardwarové limity

	vSphere hypervisor 6.0	Hyper-V 2012 R2	XenServer 6.5
Maximální velikost vRAM na jeden virtuální stroj	1 TB	1 TB	192 GB
Maximální počet logických procesorů na jednoho hosta	480	320	160
Maximální velikost RAM	2 TB	1 TB	1 TB
Maximální počet nodů na clusteru	32 nodů	64 nodů	16 nodů
Virtual NICs na jeden virtuální stroj	10	12	7
Maximum virtuálních procesorů	64	64	160

Tabulka 1 Maximální hardwarové limity (Zdroj: autor)

Každý hypervisor má omezení, kolik hardwarových prostředků může přidělovat jednotlivým virtuálním strojům a jaké množství prostředků může teoreticky a maximálně spravovat. Tyto limity jsou s každou verzí navyšovány a upravovány. V tabulce 1 jsou sepsány limity, a to u každé aktuální verze hypervisoru. [32][33][34]

Praktická část

V této části diplomové práce bude popsána navržená infrastruktura, na které budou postavena jednotlivá VDI řešení a popsány nainstalované vybrané virtualizační nástroje. Budou zde popsány jednotlivé fáze instalace pro správnou funkci virtuálního prostředí. Praktická část práce se bude zabývat testováním a zkoumáním možností virtualizace na odlišných platformách. Další části se zabývají porovnáním platforem z hlediska výkonnosti jednotlivých hypervisorů, a to i z hlediska uživatelské přívětivosti. V další části bude vysvětlen princip a způsob testování i se způsoby provádění jednotlivých testů. Výsledkem tedy bude řada výkonnostních testů a grafů k znázornění jednotlivých rozdílů, a to pomocí aplikace AutoIt , v které se dají vytvořit skripty k potřebným testovacím účelům.

4. Infrastruktura pro virtuální desktopy

V této kapitole bude popsáno řešení sestavení infrastruktur pro virtuální desktopy. Pro každou infrastrukturu bude použito 10 virtuálních desktopů. Výsledkem testování by měly být měřitelné rozdíly v zátěži serverů, náročnost na šířku přenosového pásma a dalších veličin uvedených níže. Každý uživatelský systém bude reprezentován operačním systémem Windows 10 v 32 bitové verzi, kde každý systém obsahuje pouze základní instalaci.

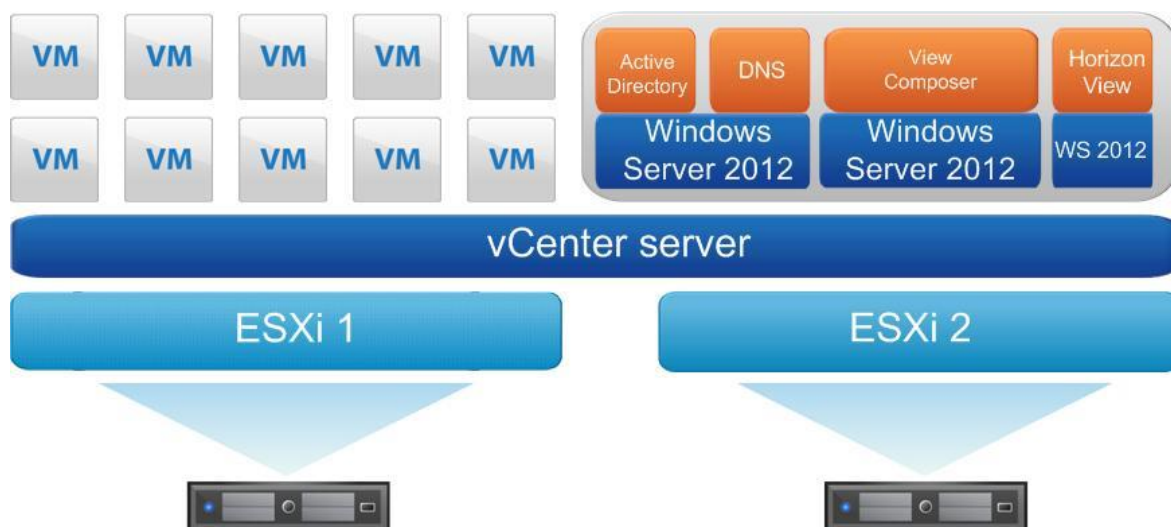
Všechny testy probíhaly na dvou serverech Dell. Konkrétně se jednalo o šasi Dell VRTX a dva servery PowerEdge M620 s dvojicí procesorů Intel Xeon E5-2630 v2. Disky byly použity 4x SAS, každý o velikosti 300GB, a dále 2x SSD o velikostech 200GB.

4.1 Infrastruktura pro virtuální desktopy-VMware

Testovací infrastruktura byla vytvořena z virtuálních desktopů a serverů. Celá zátěž byla rozdělena na dva ESXi 6.0 servery, kde jeden slouží jako virtualizační vrstva pro servery a druhý pro desktopy uživatelů. Nejprve bylo potřeba postavit a nakonfigurovat prostředí a infrastrukturu tak, aby bylo možné posléze využívat virtuální desktopy za pomoci aplikace VMware View Client. Na obrázku je vyznačené schéma, které komponenty byly při výstavbě infrastruktury použity, a jak byly využity fyzické servery, na kterých byla nainstalována celá infrastruktura.

Infrastruktura se skládá z následujících komponent:

- Windows Server 2012 R2, který obsahuje Active Directory a DNS služby
- Windows Server 2012 R2, obsahující View Connection Server
- Windows Server 2012 R2, na kterém je nainstalovaný vCenter server pro řízení virtuálních strojů a ESX serverů a View Composer pro správu uživatelských desktopů



Obrázek 15 Vlastní infrastruktura VMware (Zdroj: autor)

4.1.1 Horizon View Connection 7 a View Composer

Administrátor se přihlašuje k Horizon View Connection Serveru pomocí webového rozhraní a má k dispozici velké množství nastavení každého poolu s desktope, počínaje nastavením profilového adresáře až po nastavení kvality webového obsahu určitého desktopu. Jak již bylo řečeno dříve, zajímá nás technologie plovoucích desktopů, kde uživatelé přistupují k desktopům podle toho, který je v danou chvíli volný. Horizon View Connection musí být nainstalovaný na samostatném serveru, který je připojený k hlavní doméně, která spravuje uživatelské účty. Po tomto kroku je možné nainstalovat komponentu Horizon View Connection Server.

Druhou službou komponenty Horizon View je View Composer. Tato služba je doporučována instalovat na vCenter server, kde server musí být připojený opět do hlavní domény. Jedná se o komponentu, která řídí životní cyklus linkovaných klonů.

Při běhu instalace View Composeru dochází k přidání služby „VMware View Composer“, která běží jako Windows služba. Samotný View Composer po svou funkci potřebuje SQL databázi s připojeným datovým zdrojem (přes ODBC), což není potřeba u Horizon View. V případě View Composeru je nutné si připravit databázi, bez které nelze View Composer nainstalovat. V našem případě se bude jednat o databázi Microsoft SQL Server 2012 Express.

4.1.2 Instalace a konfigurace vCenter Server

Systém vCenter je distribuován v podobě předpřipraveného obrazu systému. Po stažení souboru ze stránek VMware je nutné otevřít a přihlásit se pomocí vSphere Clienta do ESXi serveru za pomoci jeho IP adresy. Zde je vybrán stažený obraz systému a posléze skrze instalační nabídku dojde k přiřazení vCenter do stávající domény, vytvoření doménového jména pro vCenter (výchozí administrator@vsphere.local), vyplnění hesel, nastavení portů a vyplnění IP adresy pro přístup k vCenter a to buď pomocí webového rozhraní nebo vSphere Clienta. V našem případě se bude jednat o adresování IPv4 s konkrétní adresou 192.168.101.30.

Veškerá správa vCenter serveru se dá dělat přehledněji přes vSphere klienta. Zde je potřeba vytvořit datové centrum, ve kterém budou oba hostitelé ESXi odděleni od případných ostatních hostitelů v síti. Jakmile je datové centrum vytvořeno, je nutné znát IP adresu ESXi

serverů nebo doménové jméno a přihlašovací údaje k serverům pro následné přidání do tohoto datového centra. Jakmile jsou oba hosté přidáni, jsou pod centrální správou vCenter. Díky tomu lze jednoduše oba stroje spravovat, a to jak ovládat, tak upravovat a vytvářet nové virtuální stroje a zároveň jednotlivé hostitele vypínat.

4.1.3 Instalace a konfigurace desktopů

Samotný desktop je instalován v prostředí vSphere. Po připojení je třeba vytvořit virtuální stroj, který bude odpovídat minimálním požadavkům daným výrobcem, konkrétně tedy společnosti Microsoft. V tomto testovacím prostředí virtuální stroj obsahuje 2 jádra CPU, 2GB RAM a 18GB HDD. Po naběhnutí základní instalace je potřeba nainstalovat VMware Tools, který zajistí veškeré ovladače pro virtuální zařízení. Následně, po instalaci VMware Tools, je nutné restartování virtuálního stroje a je třeba desktop připojit do aktuální domény. Pro nasazení více desktopů je vhodné optimalizovat systém natolik, aby v něm neběžely nepotřebné služby a další automatizovaná správa a služby jako Xbox Live, BitLocker a další. Všechny tyto virtuální testovací desktopy byly na jiné infrastruktuře, a to z důvodu odstínění činností nesouvisejících s testováním. Pro umožnění automatizované správy desktopů za pomoci Horizon View je nutné doinstalovat View Agenta. Jedná se o komponentu, která zprostředkovává komunikaci mezi Horizon View a virtualizovaným desktopem.

4.2 Infrastruktura pro virtuální desktopy-Microsoft Hyper-V

Na obrázku je obdobně jako u technologie VMware vyznačené schéma, které komponenty byly při výstavbě infrastruktury použity, a jak byly využity fyzické servery, na kterých byla nainstalována celá infrastruktura.

U technologie Hyper-V je veškerá infrastruktura cílena na dva Windows 2012 R2 Server. Jeden slouží jako doménový a na druhém je nainstalována samotná role Hyper-V, která umožňuje vytvářet virtualizované výpočetní prostředí serveru, kde lze vytvářet a spravovat virtuální počítače. Nejprve je tedy potřeba nakonfigurovat prostředí a infrastrukturu tak, aby bylo možné posléze využívat virtuální desktopy za pomoci protokolu RDP pomocí programu Hyper-V-Manager, kde je vytvořeno a nakonfigurováno 10 virtuálních desktopů.

Infrastruktura se skládá z následujících komponent:

- Windows Server 2012 R2, který obsahuje Active Directory a DNS služby
- Windows Server 2012 R2, na kterém jsou nainstalovány virtuální stroje a role Hyper-V



Obrázek 16 Vlastní infrastruktura Hyper-V (Zdroj: autor)

4.2.1 Instalace role Hyper-V a Remote Desktop Services

V případě společnosti Microsoft byl použit hypervisor Hyper-V, který je možné doinstalovat jako roli v systému Microsoft Sever 2012 R2. Instalace na Windows Server spočívá ve spuštění „Správce serveru“, kde vybereme záložku „Správa“, a v ní přidáme ze seznamu roli Hyper-V obdobně jako DHCP či DNS server.

Při instalaci role Hyper-V se mění struktura operačního systému a po nainstalování je třeba provést restart systému. Po úspěšné instalaci role Hyper-V je možná veškerá správa virtualizace prováděna přes konzoli Hyper-V Manager.

U Hyper-V se přistupuje k desktopu přes Remote Desktop Services (RDS). Jedná se o takzvanou „session virtualization“, kde klient musí mít stanici, která podporuje Remote Desktop Client. Desktop, či konkrétní aplikace, běží na serveru, kde se přenášejí pouze obrazovky a signály. RDS se instaluje ve správci serveru obdobně jako role Hyper-V. Poté co je role nainstalována lze vytvořit a spravovat kolekci virtuálních desktopů. V záložce „kolekce“ uvnitř RDS zvolíme „úkol“ a vybereme vytvoření kolekce virtuálních desktopů. Před tímto krokem je ale potřeba mít vytvořenou „golden image“ rodičovského desktopu, kterou vybereme v sadě jednotlivých kroků instalace. Po správném projití jednotlivých kroků a vybrání počtu virtuálních strojů, se postupně vytvoří všech 10 virtuálních strojů pro potřebu našich testů.

4.2.2 Instalace a konfigurace desktopů

Samotný desktop je instalován v prostředí Hyper-V Managera. Systém musí mít opět minimální požadavky dané výrobcem, tedy virtuální stroj obsahuje 2 jádra CPU, 2GB RAM a 18GB HDD. Pro instalaci bylo využito ISO obrazu, který byl uložen na diskovém uložišti serveru. Po instalaci je třeba desktop připojit do aktuální domény a systém restartovat. Pro nasazení více desktopů je vhodné optimalizovat systém natolik jako u předešlé technologie a tedy odstranit nepotřebné položky a služby.

4.3 Infrastruktura pro virtuální desktopy-Citrix

Z obrázku můžeme vidět, že u technologie Citrix jsou virtuální desktopy umístěné na XenServeru a Windows Server 2012 nám slouží pouze k monitorování veškerého provozu na tomto serveru a posléze i pomocí něho lze konfigurovat XenServer a vytvářet virtuální desktopy.

U technologie Citrix je nejprve potřeba nakonfigurovat XenServer, poté nainstalovat Windows Server 2012 a pomocí programu XenDesktop se připojit ke XenServeru. K vytvoření desktopů pomocí techniky linkovaných klonů slouží program Citrix Studio, kde je instalace velice podobná jako u technologie VMware. Aby bylo možné posléze využívat virtuální desktopy, tak k tomuto účelu použijeme Citrix View klient pojmenovaný Citrix Receiver.

Infrastruktura se skládá z následujících komponent:

- Windows Server 2012 R2, který obsahuje Active Directory a DNS služby
- XenServer, na kterém jsou nainstalovány virtuální stroje
- Windows Server 2012 R2, na monitorování XenServeru a k vytvoření virtuálních strojů pomocí programu Citrix Studio



Obrázek 17 Vlastní infrastruktura Citrix (Zdroj: autor)

5 Testovací metodika

5.1 Kolekce testovacích desktopů

Pro účely testování bylo vytvořeno 10 testovacích virtuálních desktopů pro každou technologii se stejnými parametry, lišící se pouze IP adresou a názvem stroje. Pro testování by bylo příliš časově náročné vytvářet každý desktop zvlášť, proto bylo vzhledem k vysokému počtu desktopů využito funkce „Cloned-links“. Tato funkce dokáže provést klonování libovolného počtu desktopů na základě jednoho předpřipraveného desktopu nazvaného „golden image“, z kterého se provede snapshot s aktuálním stavem desktopu. Od tohoto snapshotu se poté budou odvíjet zbylé klony daného desktopu. Ve výsledku bylo vytvořeno pro každou technologii 10 virtuálních desktopů a 1 základní desktop, na kterém byly vytvořeny konfigurace pro testování společně s testovacími skripty.

5.2 Testovací skripty a způsob testování

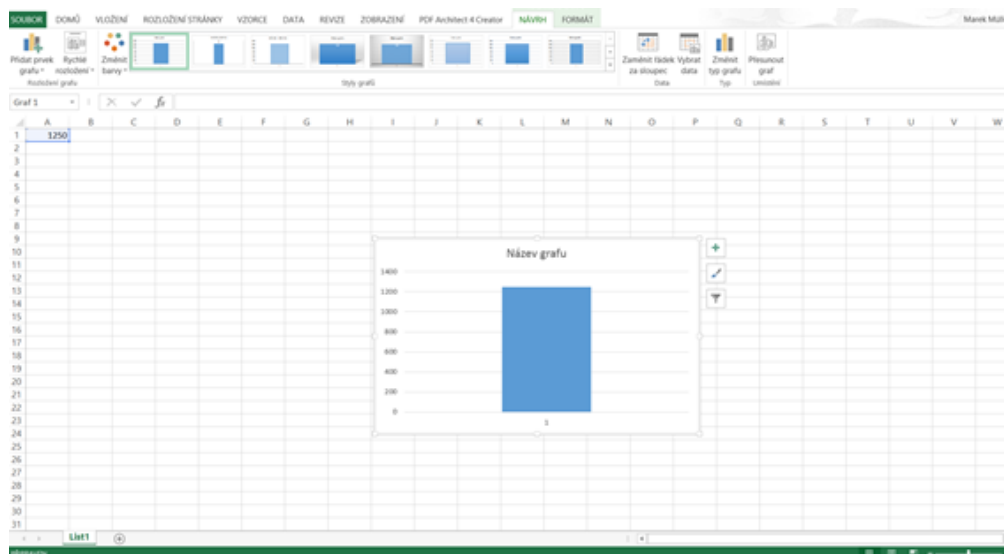
Pro velké množství virtuálních desktopů, na kterých bude testována a simulována činnost uživatelů, je nutné mít vytvořené testovací skripty, pomocí kterých bude ovládán počítač, a to bez interakce uživatele. Existuje mnoho přístupů jak k tomuto problému přistupovat a řešit ho. V nejjednodušším případě jde o napsání skriptu, který bude například přesouvat okna, otevírat a zavírat aplikace. Toto však neodpovídá činnosti běžného uživatele, který pracuje s prostředím pomocí klávesnice a myši.

K tomuto účelu a typu ovládání počítače slouží bezplatný program AutoIt, který dovoluje ovládat klávesnici a myš stejným způsobem jako uživatel. Pomocí toho programu je možné posouvat souřadnice myši na určené souřadnice a používat stisky kláves na klávesnici, jakoby u počítače seděl skutečný uživatel. Navíc lze myši posouvat na určené souřadnice, poklepat levým či pravým tlačítkem, a to společně s rolováním dokumentů či dokonce používat klávesové zkratky.

V diplomové práci jsem využil kombinaci programu AutoIt a skriptů psaných v příkazovém interpretu Batch. Pro vytvoření obou metod skriptů není potřeba nic víc, než obyčejný poznámkový blok, ve kterém lze skripty editovat. Jako příklad zde uvedu jednoduchý skript pro otevření dokumentu v programu Excel a jeho opětovné zavření.

Příklad skriptu:

MouseDown("left",24, 1061,1) ;otevření nabídky Start
Sleep(3000) ;čekání 3 sekundy na její zobrazení
Send("{Excel}") ;napsání Excel do vyhledávací konzole
Sleep(3000) ;čekání na zobrazení nabídky
Send("{Enter}") ;stisknutí enter pro spuštění Excelu
Sleep(3000) ;čekání na načtení programu
Send("{Enter}") ;otevření prázdné stránky Excelu
Send("{1250}") ;napsání čísla z kterého se bude generovat graf
Send("{Enter}") ;potvrzení buňky
MouseDown("left",211, 53,1) ;vložení grafu
MouseDown("left",800, 112,1) ;sloupový graf
Sleep(3000) ;čekání na přesunutí myši
Send("{Enter}") ;potvrzení vybrání grafu
Sleep(6000) ;čekání na vygenerování grafu
MouseDown("left",1913, 23,1) ;zavření
MouseDown("left",233, 110,1) ;zavření dialogové okna s uložením změn



Obrázek 18 Před ukončením skriptu (Zdroj: autor)

Pro získání velmi přesných dat je nutné simulovat zátěž na více než jednom virtuálním desktopu, a proto bylo vybráno deset desktopů. Každý desktop byl instalován se systémem Windows 10 v 32bitové verzi. Programové vybavení bylo u všech desktopů shodné a každý typ testu měl vlastní programy, které budou zmíněny v popisu jednotlivých testů.

Pro testování všech deseti desktopů najednou by bylo potřeba mít 10 fyzických počítačů. Vzhledem k náročnosti obstarávání těchto deseti počítačů bylo mnohem výhodnější vytvořit si dalších 10 virtuálních desktopů, které kopírovaly fyzické počítače jednotlivých uživatelů. Na těchto počítačích byl kromě základní instalace Windows 10 32 bit ještě instalován program Wireshark pro měření síťového provozu.

Testovací skripty se spouštěly půl minuty po sobě, což simuluje právě nepravidelné spuštění jednotlivých aplikací fyzickými uživateli.

Ukázka časového spuštění skriptů:

Čas	Akce
8:00:00	Spuštění testovacího skriptu na desktopu 1
8:00:30	Spuštění testovacího skriptu na desktopu 2
8:01:00	Spuštění testovacího skriptu na desktopu 3
8:01:30	Spuštění testovacího skriptu na desktopu 4

6 Testy Infrastruktury

6.1 Test 1 – Kopírování souborů

Potřebné programy	Verze
Bitvise SSH	7.12
WinSCP	5.77

Prvním testem je komplexní test, a to z hlediska síťového provozu i výpočetního výkonu systému. Jedná se o kopírování dat z Win10 na Windows Server pomocí programu WinSCP. Na Windows Serveru byl nainstalován program Bitvise SSH, jehož serverová část umožnila sdílení adresáře pro kopírování souborů. Na server se přihlašuje z klienta pomocí doménového uživatele sshuser a přenos probíhá šifrovaně pomocí protokolu SFTP.

Tento test byl vykonáván pomocí předpřipraveného skriptu v Batch, který simuloval automatickou práci uživatele. Skript byl přidán jako úloha v plánovači úloh a byla spouštěna vždy v určitém čase, v kterém probíhalo naše měření. Na každé technologii test běžel různou dobu.

6.2 Test 2 – Microsoft Office

Potřebné programy	Verze
Microsoft Office 365	2016
Adobe Reader	11

Druhý test je zaměřen na zpracování velkého množství dat (datových tabulek) v programu Excel, a to celkem 60 000 záznamů. Cílem testu je otevřít takto velký soubor, z patřičných hodnot vytvořit kontingenční tabulku, soubor vytisknout do formátu PDF, uložit PDF na pevný disk počítače a otevřít ho kvůli kontrole a prolístovat pár stránek kvůli ověření zda vše proběhlo správně. Nutností u tohoto testu bylo, že na každém desktopu muselo být nastaveno výchozí tiskárny na Adobe Reader, aby byly dokumenty tisknuty na správné

tiskárně. Celkový čas automatické práce jednoho desktopu byl u tohoto testu 4 minuty a celková doba sledování serveru byla 8 minut.

Čas (mm:ss)	Činnost (Interakce)
00:00	Spuštění testovacího skriptu a otevření souboru excel.xlsx
00:10	Vybrání dat, z kterých bude generována kontingenční tabulka
00:30	Vytvoření kontingenční tabulky a její úprava
00:50	Výběr uložení z nabídky do PDF a uložení dokumentu
03:00	Prohlížení vygenerovaného PDF a rolování stránek
03:45	Uzavření PDF
03:50	Uzavření Excelu
04:00	Smazání souboru PDF

6.3 Test 3 -Webový prohlížeč Chrome

Potřebné programy	Verze
Chrome	51.0.2704
Flash player	22.0.0.209

Poslední test je zaměřený na simulaci zátěže síťového provozu a na zátěž CPU. U tohoto testu je cílem otevření webového prohlížeče Chrome a spuštění daného videa s podporou přehrávače flash player kde video má celkovou délku 15 minut. Dále test simuluje, že během přehrávání videa uživatel vykonává práci na internetu a prohlídí určité webové stránky. Při přehrávání videa dochází k velkému množství změn na obrazovce vzdáleného desktopu, kde příslušné protokoly jednotlivých technologií musí efektně a co nejrychleji přenést informace o obraze ze serveru k uživateli.

Na virtuálních desktopech se objevil problém, kdy došlo k neočekávaným výskytům oken s aktualizací Java update. Na některých desktopech se tento problém nevyskytoval. Později byly tyto aktualizace zakázány a naprosto eliminovány. Při měnění skriptů a opětovném nahrávání na virtuální desktopy bylo hodně využito již zmíněné funkce Recompose, která

velmi usnadnila práci s desktopey při jakékoliv změně. Každý desktop pracoval přibližně 15 minut a doba sledování serveru byla 22 minut.

Čas (mm:ss)	Činnost (Interakce)
00:00	Spuštění testovacího skriptu a otevření Chrome.exe
00:10	Otevření záložky youtube.com a spuštění 15 minutového videa
00:20	Otevření záložky s adresou idnes.cz
00:30	Rolování v idnes.cz a otevírání zpráv
01:30	Otevření záložky youtube.com a spuštění 10 minutového videa
11:30	Zavření záložky 10 minutového videa
15:10	Zavření Chromu

7 Monitoring zátěže serverů a shrnutí výsledků

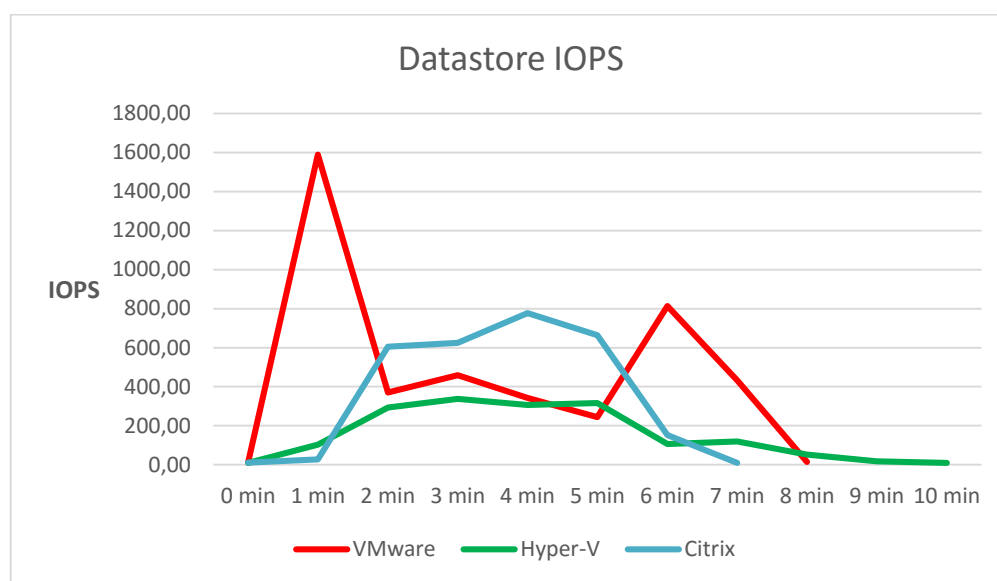
Během provádění testování desktopů byly klíčovými parametry využití CPU, využití disku, latence mezi fyzickým a virtuálním PC a celková přenesená data. Po proběhnutí prvních pár testů bylo zjištěno, že latence není nijak význačná a využití disku není tak kritické a velice málo odráží zátěž, která byla simulována v testovacích skriptech. Z parametrů byly nakonec vybrány zátěž na procesoru, zátěž na diskovém úložišti, celková přenesená data serveru a přenesená data mezi klientem a virtuálním desktopem, které nejvíce popisují náročnost jednotlivých aplikací. Ke sledování těchto parametrů nám posloužily v případě technologie VMware a Hyper-V interní nástroje obou technologií a program Veeam ONE. V případě Citrixu bylo použito monitorovacího nástroje XenCenter. Po každém testu byly hodnoty parametrů zapsány do tabulky v Excelu, ze které byly později vytvořeny grafy. Ve výsledných měřeních jsou výsledky ze tří měření, která proběhla po několika orientačních měřeních.

7.1 Test 1 – Kopírování souborů

První test je komplexní test z hlediska síťového provozu a výpočetního výkonu systému. Tento test byl vykonáván pomocí předpřipraveného skriptu v Batch, který simuloval automatickou práci uživatele a byl přidán jako úloha v plánovači úloh.

7.1.1 Průměrné IOPS

Vzhledem k tomu že je soubor kopírován z disku virtuálního stroje na disk serveru, jsou stanoveny větší požadavky na I/O operace diskového pole.



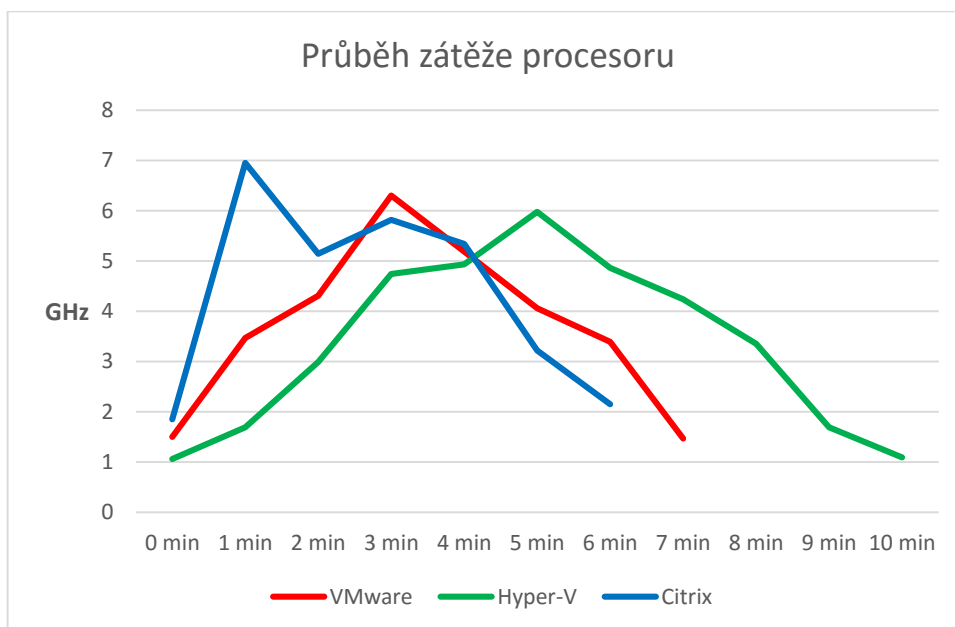
průměrné IOPS	
VMware	475
Hyper-V	152
Citrix	359

Mezi jednotlivými technologiemi je vcelku významný rozdíl, který ukazuje na závislost počtu vstupně výstupních operací na pevném disku a použitém protokolu. Z průměrných IOPS i z grafu průběhu IOPS zátěže je patrné, že při použití technologie Hyper-V nedochází k tak velkému nárůstu vstupně výstupních operací jako u ostatních dvou technologií. Mezi Hyper-V- VMware je rozdíl celých 68 % a mezi Hyper-V-Citrix se jedná o rozdíl 58%. Tyto hodnoty jsou pouze při běžném kopírování souborů z desktopu na server. Tady se domnívám, že největším rozdílem při porovnávání technologií z hlediska IOPS je to, že

Hyper-V neumí funkci linkovaných klonů. To znamená, že u technologie VMware a Citrix je virtuální stroj vytvářen v návaznosti na původní virtuální stroj a sdílí s ním virtuální pevné disky. Je zde však vyžadován přístup k souborům původního virtuálního stroje, a tady zřejmě dochází k nárůstu zatížení diskové pole.

7.1.2 Průměrný spotřebovaný výpočetní výkon

Výpočetní výkon je jistě klíčovou záležitostí při porovnávání námi zkoumaných technologií. Dnešní serverové procesory mají dostatečný výkon, ale výpočetní náročnost je stále dost důležitý prvek.



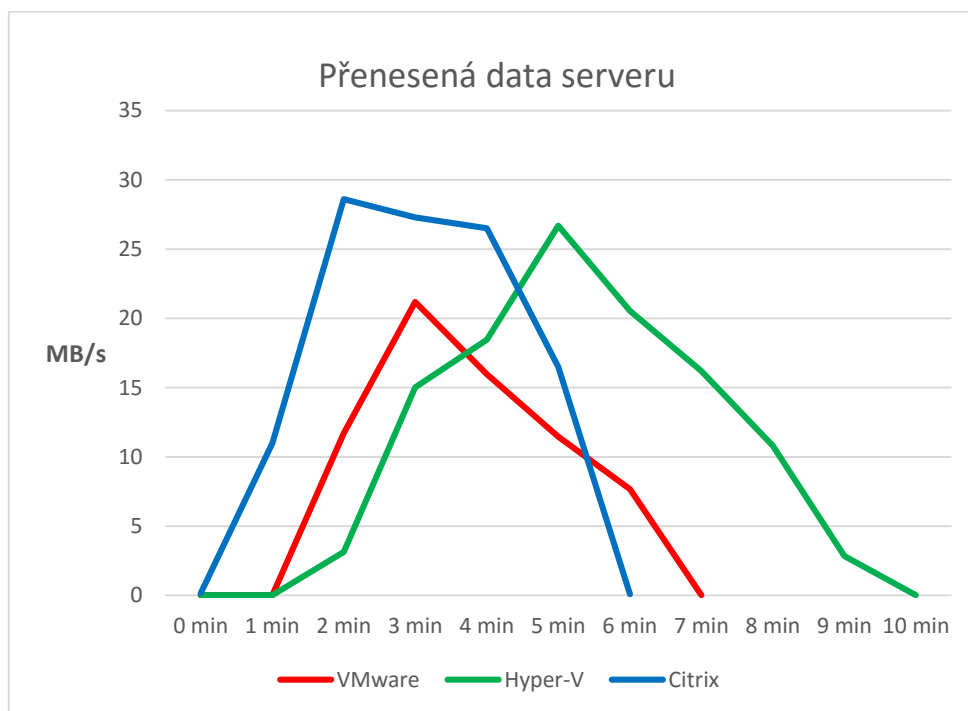
Průměrný spotřebovaný výpočetní výkon (GHz)	
VMware	3,7 GHz
Hyper-V	3,3 GHz
Citrix	4,3 GHz

Z průměrného spotřebovaného výpočetního výkonu i z grafu průběhu zátěže je patrné, že při použití technologie Citrix dochází ke zvýšení nároku na výpočetní výkon až o 24 % při běžném kopírování souborů. Přičemž rozdíl mezi VMware a Hyper-V je pouhých 11%. V případě slabších serverů by mohlo dojít v případě použití technologie Citrix až na limity

výpočetního výkonu CPU. Tedy vhodnějšími technologiemi jsou zde určitě VMware a Hyper-V.

7.1.3 Průměrná přenesená data mezi serverem a virtuálními stroji

Dalším významným kritériem, a to zejména u tohoto testu, jsou průměrná přenesená data a tedy jaká je průměrná rychlost přenosu jednotlivých technologií.

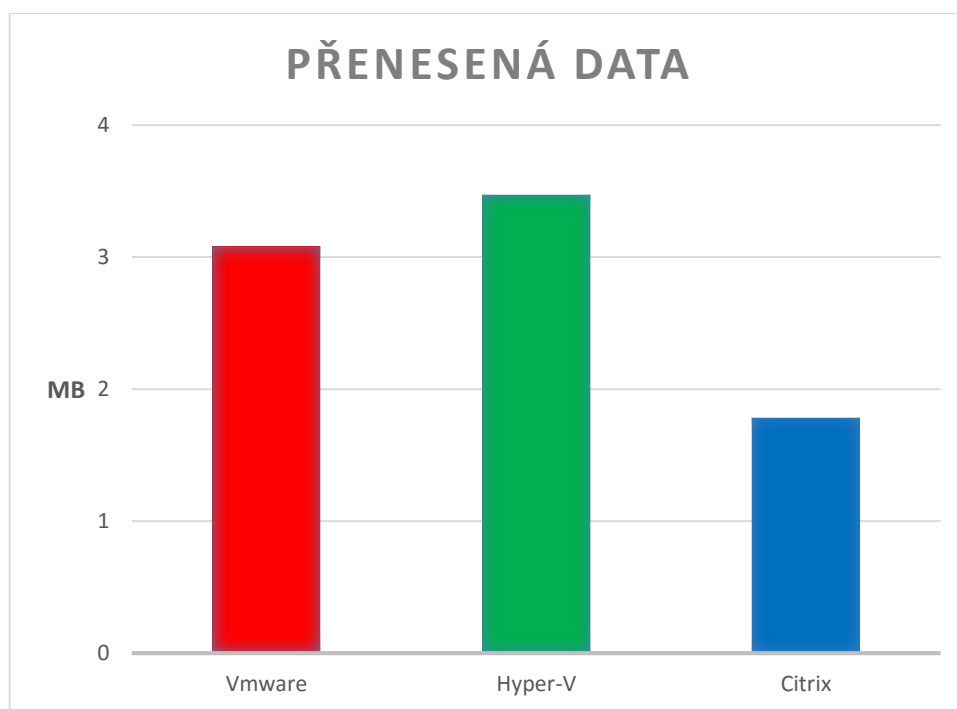


Průměrná přenesená data serveru (MB/s)	
VMware	8,5 MB/s
Hyper-V	10,3 MB/s
Citrix	15,73 MB/s

V případě přenesených dat serveru lze říct, že nejvyšší přenosová rychlost byla u technologie Citrix, což vypovídá o tom, že tato technologie je schopna vyvinout největší přenosovou rychlost a test byl dokončen v co nejrychlejší době, a to 6 minut při spuštění 10 desktopech.

7.1.4 Přenesená data

V tomto případě se jedná o porovnání přenesených dat mezi klientem a virtuálním desktopem, a to pomocí view klientů s rozdílnými protokoly. U VMware se jedná o protokol PCoIP, u Hyper-V o RDP a u Citrix o ICA.



Přenesená data	
VMware	3,08 MB
Hyper-V	3,47 MB
Citrix	1,78 MB

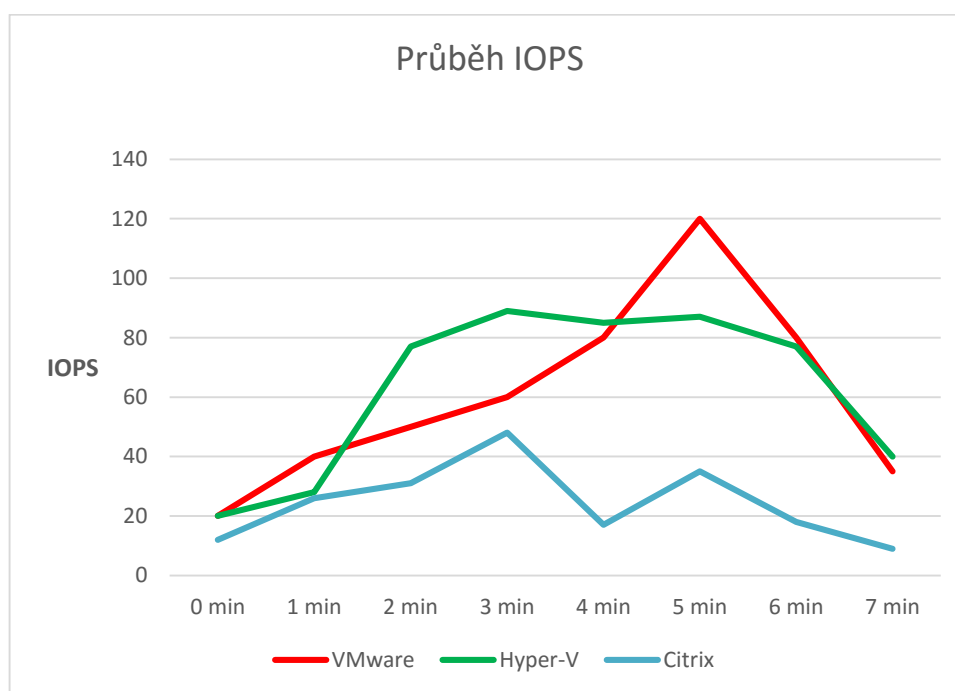
Při testu kopírování souborů není přeneseno mnoho dat, jelikož se jedná o skript prováděný v plánovači úloh a obrazovky se prakticky nepřekreslují. Je zde vidět značná převaha technologie Citrix, u které je zátěž poloviční oproti ostatním technologiím.

7.2 Test 2 – Microsoft Office

Druhý test byl příkladem zpracování velkého objemu dat v Excelu, a to konkrétně 60 000 záznamů. Procházejí se velké tabulky s daty a ve výsledku jsou data převedeny do PDF souboru, který je následně uložen a částečně prohlížen.

7.2.1 Průměrné IOPS

Ze všech tří testů jsou zde nejmenší nároky na diskové pole, kde nejvyšší nároky jsou při převádění souboru do PDF.

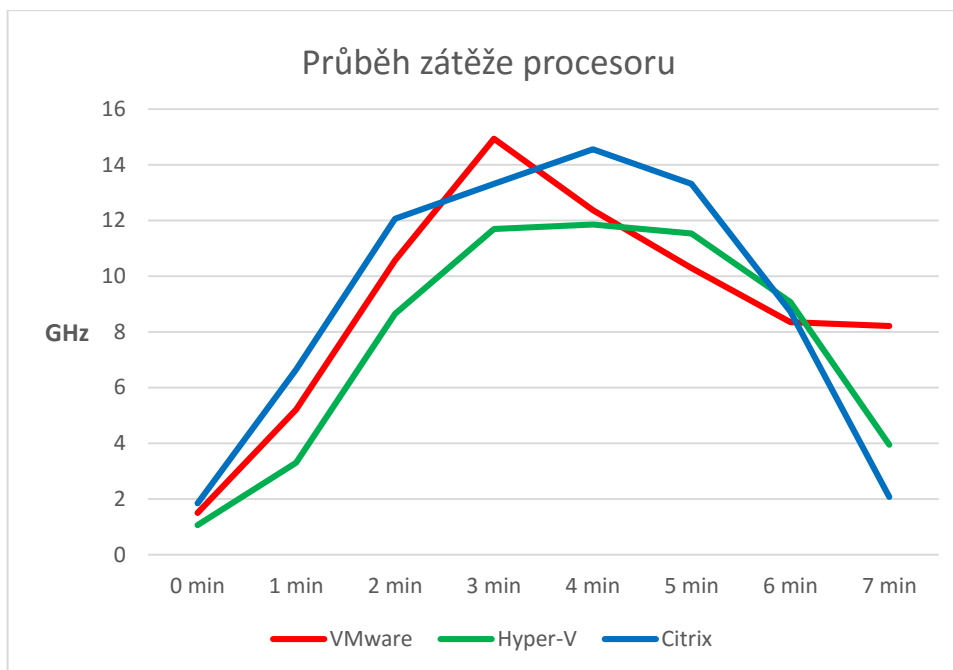


průměrné IOPS	
VMware	61
Hyper-V	63
Citrix	25

Při pohledu na průběh zátěže diskového pole je vidět, že jak technologie Hyper-V tak VMware generují stejnou zátěž. Z pohledu technologie Citrix lze říci, že buď pracuje efektivněji anebo nedokáže využít potenciálu diskového pole a ukládá soubor pomaleji. Nicméně nároky na diskové pole jsou podstatně nižší a oproti oběma technologiím se jedná o 60% efektivitu.

7.2.2 Průměrný spotřebovaný výpočetní výkon

V tomto testu hraje spotřebovaná výpočetní náročnost větší úlohu než u prvního testu, jelikož se tu generuje a vytváří kontingenční tabulka, která se následně se všemi daty zapisuje do PDF souboru.



Průměrný spotřebovaný výpočetní výkon (GHz)	
VMware	8,9
Hyper-V	7,6
Citrix	9

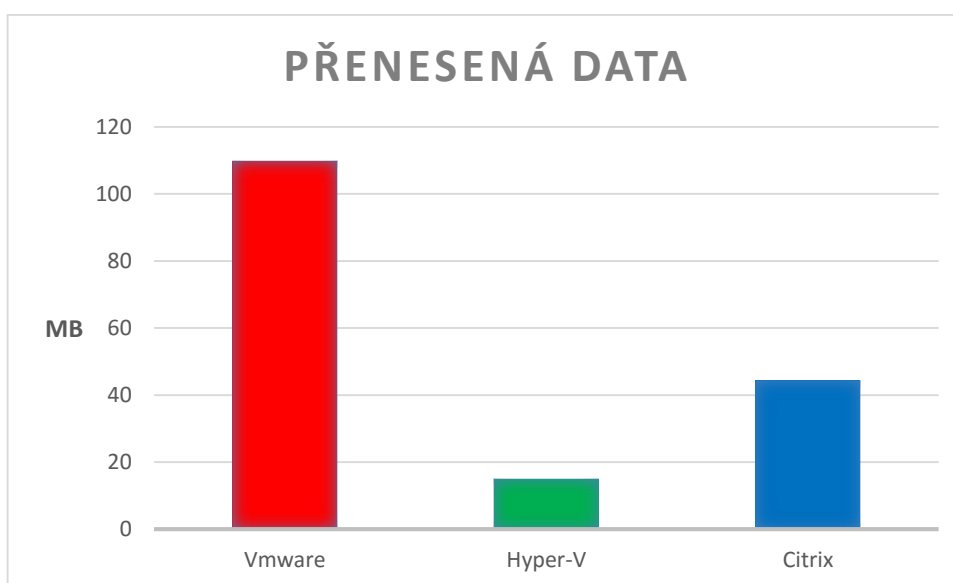
Při pohledu na průběh grafu zátěže procesoru je vidět, že při použití všech technologií je spotřebovaný výpočetní výkon téměř shodný. Rozdíly mezi technologiemi jsou zanedbatelné, a to dokazuje, že výsledná použitá technologie nemá moc velký vliv na zátěž procesoru v případě tohoto testu.

7.2.3 Průměrná přenesená data mezi serverem a virtuálními stroji

V případě zpracování velkého objemu dat v Excelu nemělo samozřejmě význam měřit průměrná přenesená data, jelikož není vytvářen prakticky žádný síťový provoz. Naměřená data se pohybovala v řádech několik desítek kb/s a tento test pro nás tedy nemá žádný význam.

7.2.4 Přenesená data

V tomto případě se obrazovky překreslují velmi často, a to zejména díky generování velkého počtu stránek s tabulkami a výsledky.



Přenesená data	
VMware	109,74 MB
Hyper-V	14,95 MB
Citrix	44,36 MB

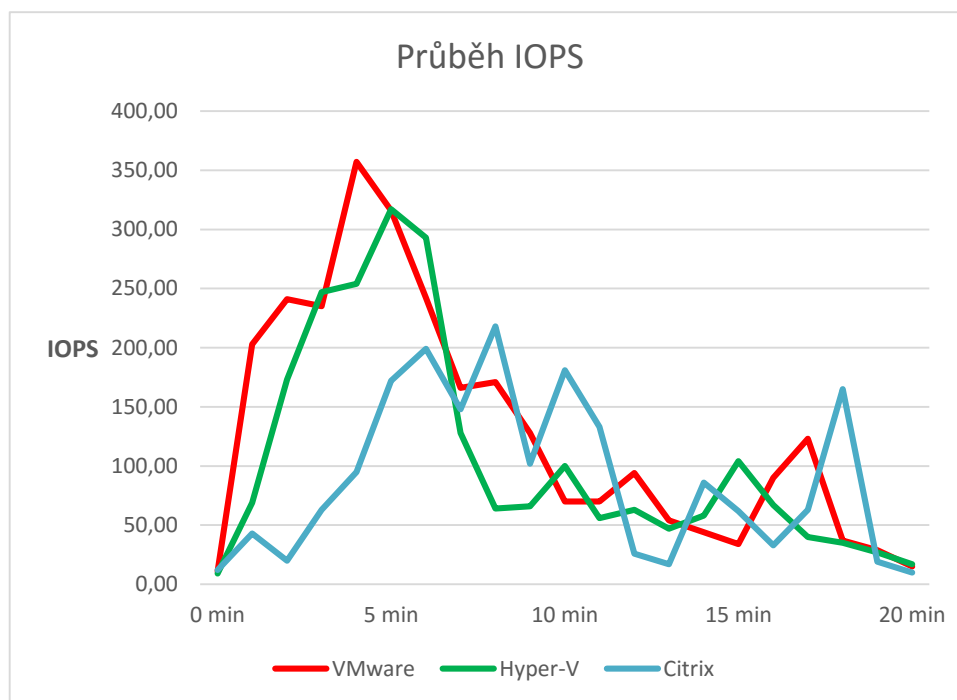
Obrazovky se u tohoto testu překreslovaly často a jednalo se zejména o prostý text s tabulkami. Ve výsledku je rozdíl velmi zajímavý, jelikož nejvíce obrazových dat spotřebuje technologie VMware, ve výsledku o téměř 8x více než technologie Hyper-V, a to je opravdu velký rozdíl ve prospěch technologie Hyper-V.

7.3 Test 3 – Webový prohlížeč Chrome

Poslední test je nejvíce zaměřený na simulaci zátěže síťového provozu a na zátěž CPU, a to díky rychlému překreslování obrazu a přehrávání videí v prohlížeči.

7.3.1 Průměrné IOPS

Během tohoto testu byla zátěž diskového pole z hlediska vstupně výstupních operací minimální, jelikož byl pouze otevřen webový prohlížeč s přehrávanými videi.

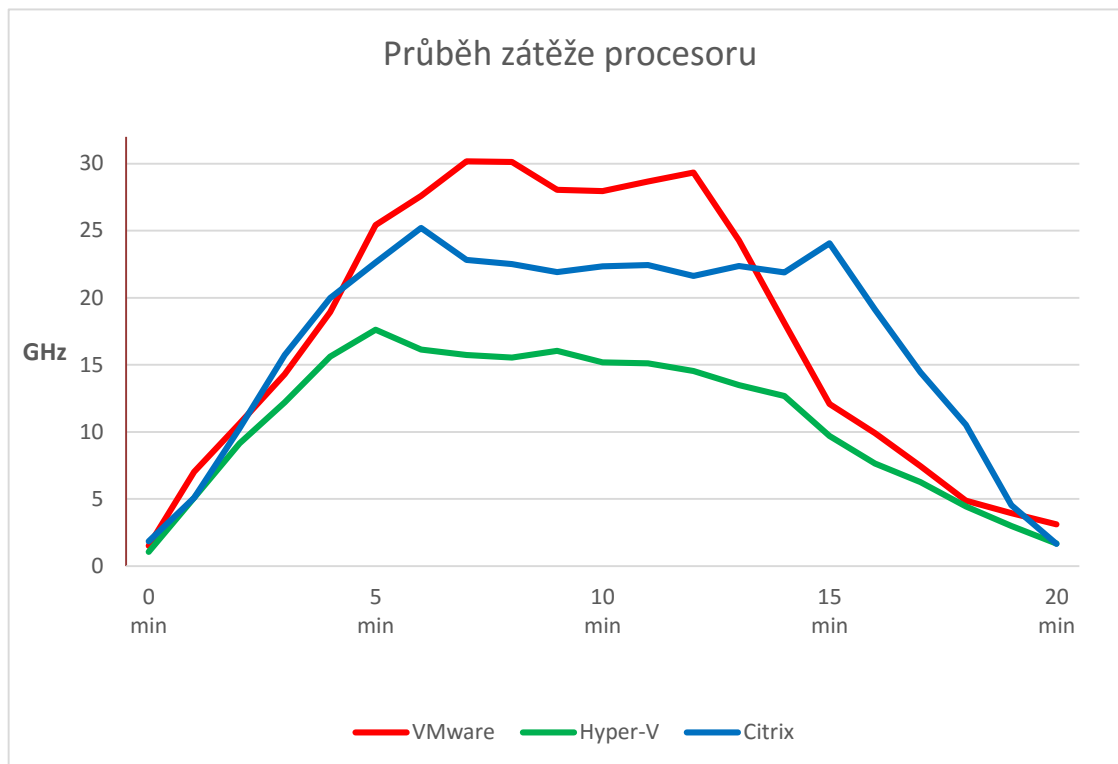


průměrné IOPS	
VMware	130
Hyper-V	106
Citrix	89

Ve výsledku byly všechny tři technologie téměř stejné a rozdíl je u tohoto testu opravdu zanedbatelný.

7.3.2 Průměrný spotřebovaný výpočetní výkon

Při tomto testu byla pozorována vysoká zátěž CPU, a to hlavně v době, kdy bylo video ve stavu přehrávání na všech deseti virtuálních strojích.

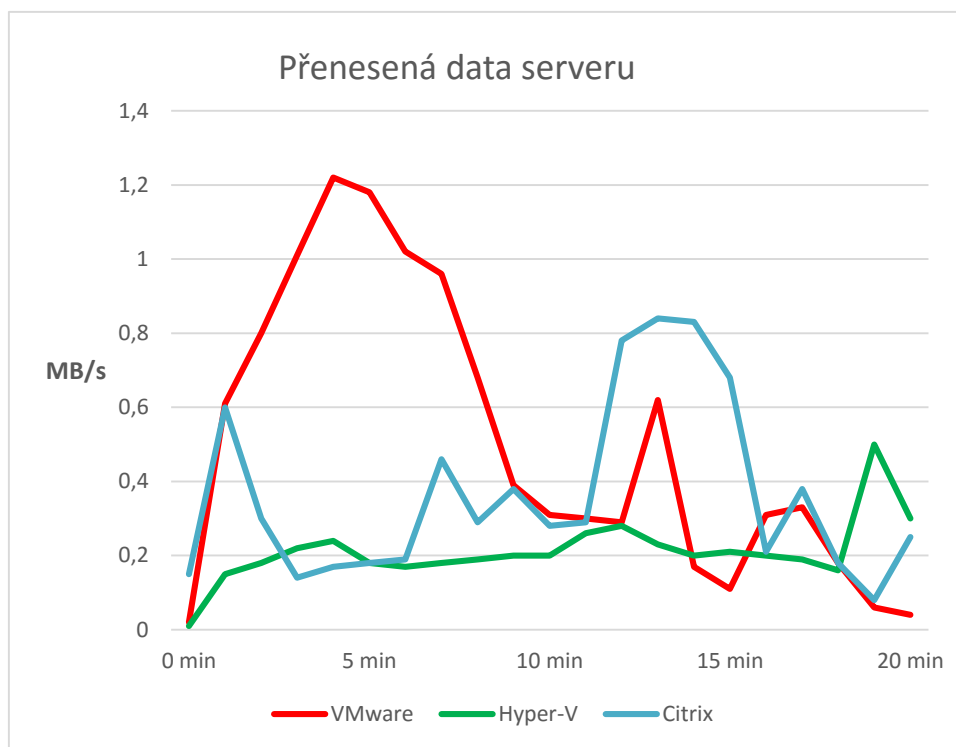


Průměrný spotřebovaný výpočetní výkon (GHz)	
VMware	17,3
Hyper-V	10,9
Citrix	16,8

Z grafu zátěže CPU je vidět, že u technologie VMware se výkon procesoru dostal až na hranici 30 GHz a zátěž byla tedy vyšší než u ostatních konkurentů. Z tohoto pohledu je nejlepším řešením použití technologie Hyper-V, jehož průměrný spotřebovaný výpočetní výkon za dobu 20 minut testu je nejmenší.

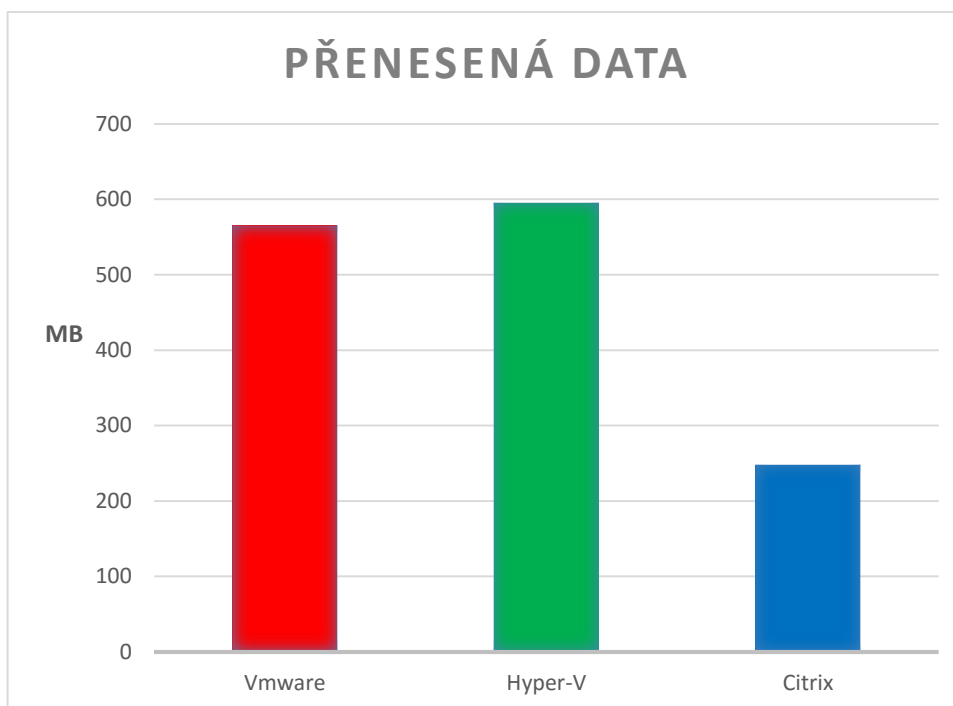
7.3.3 Průměrná přenesená data mezi serverem a virtuálními stroji

V případě přenesených dat serveru lze říci, že nejvíce přenesených dat bylo u technologie VMware a Citrix, což vypovídá o tom, že tyto technologie jsou schopny vyvinout větší přenosovou rychlost nežli Hyper-V a to až s rozdílem 50%.



Průměrná přenesená data serveru (MB/s)	
VMware	0,5
Hyper-V	0,2
Citrix	0,4

7.3.4 Přenesená data



Přenesená data	
VMware	565 MB
Hyper-V	595 MB
Citrix	248 MB

Při pohledu na výsledný graf a srovnání výsledků lze vidět, že technologie VMware a Hyper-V dopadly v podstatě stejně. U technologie Citrix lze vidět až 60% rozdíl úspory přenesených dat. Do přehrávání videa, a tedy načtení prohlížeče a stránek, si vedly všechny technologie stejně, ale jakmile došlo k přehrávání videa, Citrix byl na tom lépe. Při použití technologie Hyper-V a tedy protokolu RDP, se video občas sekalo a nebylo moc plynulé. Ostatní technologie byly téměř plynulé a to jen s občasným zaseknutím. Závěrem lze tedy říci, že technologie Citrix má na přenos obrazu u tohoto testu nejmenší požadavky a navíc je video při přehrávání velmi dobře sledovatelné.

8 Hodnocení výsledků testování

K hodnocení technologií z hlediska přenesených dat mezi klientem a virtuálním desktopem, jsem se rozhodl použít statistických metod v programu IBM SPSS Statistics. Hladina významnosti, na které jsem testoval, byla 5%. Konkrétně jsem použil analýzu rozptylu a následně jeden z post-hoc testů, a to test Bonferroniho. Analýza rozptylu zkoumá rozdíly průměrů závislé proměnné mezi 3 technologiemi (skupinami), danými jednou nezávisle kategoriální proměnnou. Předpokladem tohoto testu je rovnost rozptylů v testovaných podskupinách.

Zkoumáme hypotézy:

H0: všechny průměrné hodnoty jsou v jednotlivých populacích stejné

H1: minimálně jedna skupina je odlišná z hlediska průměru od ostatních

ANOVA

Data

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	4,684	2	2,342	39,262	,000
Within Groups	,358	6	,060		
Total	5,042	8			

Post Hoc Tests

Multiple Comparisons

Data
Bonferroni

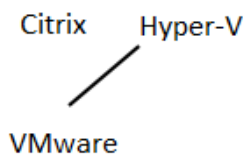
(I) Programy	(J) Programy	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
1	2	-1,68667*	,19943	,000	-2,3423	-1,0311
	3	-1,30000*	,19943	,002	-1,9556	-,6444
2	1	1,68667*	,19943	,000	1,0311	2,3423
	3	,38667	,19943	,302	-,2689	1,0423
3	1	1,30000*	,19943	,002	,6444	1,9556
	2	-,38667	,19943	,302	-1,0423	,2689

*. The mean difference is significant at the 0.05 level.

Obrázek 19 Analýza rozptylu, Bonferroniho test – Test Kopírování

Z tabulek vidíme, že $Sig < 0,05$ a tedy zamítáme hypotézu H0 o tom, že jsou všechny průměrné hodnoty mezi technologiemi stejné. Samotný test ale neříká, které skupiny se liší navzájem. Proto byl proveden Bonferroniho test mnohonásobného porovnávání, kde se porovnává každá dvojice průměrů navzájem. Hvězdička značí, kde jsou rozdíly v průměru statisticky signifikantní.

Výsledek si lze přehledně graficky znázornit, kde spojnice značí shodu průměru na hladině významnosti alfa 0,05.



U druhého a třetího testu můžeme vidět rozdíly na obrázcích níže.

ANOVA

Data

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	14126,293	2	7063,146	32,033	,001
Within Groups	1322,983	6	220,497		
Total	15449,275	8			

Post Hoc Tests

Multiple Comparisons

Dependent Variable: Data
Bonferroni

(I) Programy	(J) Programy	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
1	2	29,41667	12,12428	,154	-10,4413	69,2747
	3	-65,38000*	12,12428	,005	-105,2380	-25,5220
2	1	-29,41667	12,12428	,154	-69,2747	10,4413
	3	-94,79667*	12,12428	,001	-134,6547	-54,9387
3	1	65,38000*	12,12428	,005	25,5220	105,2380
	2	94,79667*	12,12428	,001	54,9387	134,6547

*. The mean difference is significant at the 0.05 level.

Citrix — Hyper-V

VMware

Obrázek 20 Analýza rozptylu, Bonferroniho test – Test Microsoft Office

ANOVA

Data

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	221989,556	2	110994,778	615,119	,000
Within Groups	1082,667	6	180,444		
Total	223072,222	8			

Post Hoc Tests

Multiple Comparisons

Dependent Variable: Data
Bonferroni

(I) Programy	(J) Programy	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
1	2	-347,00000*	10,96797	,000	-383,0567	-310,9433
	3	-317,33333*	10,96797	,000	-353,3900	-281,2766
2	1	347,00000*	10,96797	,000	310,9433	383,0567
	3	29,66667	10,96797	,106	-6,3900	65,7234
3	1	317,33333*	10,96797	,000	281,2766	353,3900
	2	-29,66667	10,96797	,106	-65,7234	6,3900

*. The mean difference is significant at the 0.05 level.

Citrix — Hyper-V

VMware

Obrázek 21 Analýza rozptylu, Bonferroniho test – Test Webový prohlížeč

Z hlediska přenesených dat mezi klientem a virtuálním desktopem je podle výsledků jasná statistická převaha technologie Citrix s protokolem ICA a to u testu kopírování souborů a webového prohlížeče. V případě testu Microsoft Office je statistická převaha technologie VMware, kde klient přenáší méně dat než jeho konkurenti.

Z výsledků měření výpočetního výkonu si jak technologie VMware tak Hyper-V stojí velmi dobře a zde si nedovolím zvolit konkrétního vítěze. Mohu však říci, že technologie Hyper-V je o trochu více jednodušší na instalaci a zprovoznění než VMware, kde člověk musí proniknout více do problematiky a jednotlivých služeb. Na druhou stranu VMware je opravdu velmi propracovaná technologie, kde lze provádět nepřeberné množství funkcí, je zde velmi dobrý monitoring a kvalitní správa virtuálních strojů.

Z hlediska výsledků testů dochází k nejmenšímu nárůstu vstupně výstupních operací na diskovém poli u technologie Hyper-V a Citrix.

Zajímavým zjištěním u testování bylo chování virtuálních desktopů při kopírování souborů, kdy každé technologii trvalo kopírování jiný čas. Na desktopech technologie VMware to bylo 7 minut, u Hyper-V 10 minut a u technologie Citrix pouhých 6 minut. Doba sledování serveru byla tedy různá, ale vždy se měřilo minutu před začátkem testu a minutu po dokončení testu.

Při testování každé technologie se párkrát stalo, že připojený desktop se z ničeho nic sám odpojil nebo vypnul anebo došlo k pádu některé z aplikací. Většinou pomohl restart serveru, v případě pádů aplikací restart konkrétního desktopu.

Na závěr je nejdůležitější říci, že samozřejmě každá technologie má své kladné a záporné stránky. Nejvíce, ale záleží na tom, podle jakých požadavků chce uživatel technologii použít a od tohoto se teprve odvíjí jednotlivá volba konkrétní technologie pro použití a tvorbu virtuálních desktopů.

9 Závěr

Virtualizace jako taková už se netýká pouze serverů, ale jak je možné vidět, tak proniká a myslím si, že již pronikla do většiny firem, nejvíce však kuživatelské sféře a to prostřednictvím virtualizovaných desktopů.

V dnešní době již uživatelé stačí internetové připojení, uživatelské údaje a všechna data jsou přístupná odkudkoliv a prakticky kdykoliv. Jedná se zejména o uživatele, kteří pracují například z domu a přihlašují se vzdáleně na svůj pracovní desktop. Tito uživatelé pak mají přiděleny stejné programy a nastavení jako by seděli přímo na svém pracovišti ve firmě. Postupem času jistě vymizí přihlašování pomocí tlustých klientů a zcela je nahradí již jen webový prohlížeč. Nyní je doba taková, že je uživatelé poskytnuta možnost výběru a může si tak zvolit vhodný typ klienta podle svých potřeb.

V praktické části této práce byly 3 rozdílné technologie podrobeny řadě testů, které simulovaly rozmanitou činnost v používání virtuálních desktopů. Tyto testy se snažily ukázat přednosti technologií a jejich zápory. Ze získaných informací a po výsledku testů lze doporučit produkt firmy Citrix. Jak již ale bylo řečeno, nejvíce záleží na tom, podle jakých požadavků chce uživatel technologii použít a od tohoto se odvíjí jednotlivá volba konkrétní technologie. Všichni výrobci však poskytují svá řešení kvalitní a s dobře promyšlenou strategií, za kterou si však nechají patřičně zaplatit v podobě licencí.

Svým způsobem je výkon virtualizačních technologií na velice dobré úrovni a přiblížil se prakticky k výkonu nevirtualizovaného stroje. Všechny zmíněné technologie a produkty jsou velmi dobře použitelné a nasaditelné v praktickém prostředí.

10 Seznam použité literatury

1. Virtualizace základní informace (on-line). 2016 (cit. 2015-10-10). Přístup z Internetu: <http://www.oldanygroup.cz/virtualizace-vmware-zakladni-informace-9/>
2. Gerald J. Popek, Robert P. Goldberg. Formal Requirements for Virtualizable Third Generation Architectures. 1974 (on-line). 2016 (cit. 2015-12-10). Přístup z Internetu: https://www.princeton.edu/~rblee/ELE572Papers/Fall04Readings/secureOS/popek_virtualizable.pdf
3. John Scott Robin, Hypervisor. Denver, Colorado 2000 (on-line). 2016 (cit. 2015-12-10).
Přístup z Internetu: https://www.usenix.org/legacy/events/sec2000/full_papers/robin/robin.pdf
4. Hypervisor : Monolithic Vs. Micro. Ido Goldberg Tech Blog (on-line) 2016 (cit. 2015-20-10).
Přístup z Internetu: <http://www.vmware.com>
5. Matyska, Luděk. 2007. Techniky virtualizace počítačů Ročník XVII (on-line). 2011 (cit. 2015-25-10). Přístup z Internetu: <http://webserver.ics.muni.cz/bulletin/articles/545.html>
6. Typy virtualizace. (on-line). 2008. (cit. 2015-10-11). Přístup z Internetu: <http://miho.blog.zive.cz/2008/07/typy-virtualizace/>
7. Magic Quadrant for x86 Server. (on-line). 2011 (cit. 2016-15-01). Přístup z Internetu: http://www.citrix.com/site/resources/dynamic/additional/citrix_magic_quadrant_2011.pdf
8. Virtualization surpassed half server workloads. (on-line). 2016 Přístup z Internetu: <http://www.spiceworks.com/marketing/virtualization-surpassed-half-server-workloads/>
9. Virtualizace VMware. (on-line). 2016 Přístup z Internetu: <http://www.oldanygroup.cz/vmware-110/>
10. ESXi architecture. VMware. (on-line). (cit. 2016-28-03). Přístup z Internetu: http://www.vmware.com/files/pdf/ESXi_architecture.pdf
11. VMware ESX and VMware ESXI. VMware. (on-line). 2016 Přístup z Internetu: <https://www.vmware.com/files/pdf/VMware-ESX-and-VMware-ESXi-DS-EN.pdf>
12. VDI aneb Desktopy tak trochu jinak. (on-line) – (cit. 2016-28-03) Přístup z Internetu: <http://www.systemonline.cz/virtualizace/vdi-aneb-desktopy-tak-trochu-jinak.htm>
13. PCoIP Introduction. (on-line). (cit. 2016-27-02). Přístup z Internetu: <http://techsupport.teradici.com/ics/support/kbanswer.asp?deptID=15164&task=knowledge&questionID=516>

14. HTML5 Remote Desktop. (on-line). (cit. 2014-02-25). Přístup z Internetu:
<http://www.brianmadden.com/blogs/gabeknuth/archive/2011/06/24/how-html-5remote-desktop-clients-work.aspx>
15. Microsoft Support. (on-line). (cit. 2016-28-03) Přístup z Internetu:
<https://support.microsoft.com/en-us/kb/186607>
16. View. (on-line). (cit. 2016-28-03) Přístup z Internetu: <https://pubs.vmware.com/view-52/index.jsp?topic=%2Fcom.vmware.view.planning.doc%2FGUID-6C7A534B-085C-4C64-94CE-EA3ABDDDF63F.html>
17. View2. (on-line). (cit. 2016-28-03) Přístup z Internetu: <https://pubs.vmware.com/view-51/index.jsp?topic=%2Fcom.vmware.view.planning.doc%2FGUID-CFAABEB9-9CF2-4098-A01D-1CA118D4B6BD.html>
18. XenServer. (on-line). (cit. 2016-28-03) Přístup z Internetu: <http://xenserver.org/about-xenserver-open-source.html>
19. Xen-Paravirtualizace pro každého. (on-line). (cit. 2016-28-03) Přístup z Internetu:
<http://www.linuxexpres.cz/praxe/para-virtualizace-pro-kazdeho-xen>
20. Xen-Dom0. (on-line). (cit. 2016-28-03) Přístup z Internetu:
<http://wiki.netbsd.org/ports/xen/howto/#netbsd-dom0>
21. HelenOS jako Xen hypervisor. (on-line). (cit. 2016-28-03) Přístup z Internetu:
<http://www.helenos.org/doc/theses/jd-thesis.pdf>
22. VDI-in-a-Box (on-line). (cit. 2016-28-03) Přístup z Internetu:
<http://www.svetsiti.cz/clanek.asp?cid=Citrix-VDI-in-a-Box--v-jednoduchosti-je-sila-1-912012>
23. Citrix ICA protocol (on-line). (cit. 2016-28-03) Přístup z Internetu:
<https://pawelserwan.wordpress.com/2014/09/24/dive-into-citrix-ica-protocol-part1/>
24. Citrix. (on-line) (cit. 2016-17-05) Přístup z Internetu:
http://www.citrix.cz/content/dam/citrix/en_us/documents/productssolutions/xendesktop-datasheet.pdf
25. History of virtualization. (on-line). (cit. 2016-28-03) Přístup z Internetu:
<http://www.everythingvm.com/content/history-virtualization>
26. Windows Server Hyper-V solution. (on-line). (cit. 2016-29-03) Přístup z Internetu:
<http://www.brianmadden.com/blogs/gabeknuth/archive/2008/03/11/microsoft-windows-server-2008-hyper-v-solution-overview.aspx>

27. Windows Server 2008 R2. (on-line). (cit. 2016-29-03) Přístup z Internetu:
<http://blogs.technet.com/b/windowsserver/archive/2009/07/22/when-to-expect-windows-server-2008-r2-rtm.aspx>
28. Lifecycle of Microsoft Products. (on-line). (cit. 2016-28-03) Přístup z Internetu: <http://support.microsoft.com/lifecycle>
29. MSDN. (on-line). (cit. 2016-29-03) Přístup z Internetu: [https://msdn.microsoft.com/en-us/library/cc768520\(v=bts.10\).aspx](https://msdn.microsoft.com/en-us/library/cc768520(v=bts.10).aspx)
30. Virtualization Solutions (on-line). (cit. 2016-29-03). Přístup z Internetu:
http://professorramos.com/Materiais/Documentos/virtualization_solutions.pdf
31. TULLOCH, Mitch. Understanding Microsoft Virtualization Solutions, From the Desktop to the Datacenter (on-line). Second edition. Redmond, Washington: Waypoint Press, 2010 (cit. 2016-29-03). ISBN 9780735693821. Přístup z Internetu:
http://blogs.msdn.com/b/microsoft_press/archive/2010/02/16/free-ebook-understandingmicrosoft-virtualization-r2-solutions.aspx
32. Hardware limits Hyper-V 2012 R2 (on-line). (cit. 2016-5-05). Přístup z Internetu:
<https://technet.microsoft.com/en-us/library/jj680093.aspx>
33. Hardware limits XenServer 6.5 (on-line). (cit. 2016-5-05). Přístup z Internetu:
http://docs.citrix.com/content/dam/en-us/xenserver/xenserver-65/XenServer-6.5.0-Configuration_Limits.pdf
34. Hardware limits vSphere 6.0 (on-line). (cit. 2016-5-05). Přístup z Internetu:
<https://www.vmware.com/pdf/vsphere6/r60/vsphere-60-configuration-maximums.pdf>
35. Rozdělení na trhu (on-line). (cit. 2016-22-05). Přístup z Internetu:
<http://www.enterprisestorageguide.com/hypervisor-choice-increasingly-important>
36. Love, Scott. Mistovství ve VMware vSphere 5: kompletní průvodce profesionální virtualizací. 1. Vyd. Brno: Computer Press, 2013, 728 s. ISBN 978-80-251-3774-1.
37. Prabhakar Chaganti, Xen Virtualization. 1. Vyd. UK: Packt Publishing, 2007, 143 s. ISBN 978-1-847192-48-6
38. Gaspare A. Silvestri, Citrix XenDesktop 5.6 Cookbook. UK: Packt Publishing, 2013, 354 s.

Seznam Zkratek

VMM	Virtual Machine Monitor
ROM	Read-Only Memory
RAM	Random Access Memory
HDD	Hard Disk Drive
AD	Active Directory
CPU	Central Processing Unit
DLL	Dynamic Link Library
VDI	Virtual Disk Image
VDI	Virtual Desktop Infrastructure
API	Application Programming Interface
VM	Virtual Machine
ESX	Elastic Sky X
MCC	Microsoft Management Console
VSC	Virtualization Service Client
VPS	Virtualization Service Provider
RDP	Remote Desktop Protocol
PCoIP	PC-over-IP
HTML 5	HyperText Markup Language 5
TCP/IP	Transmission Control Protocol/Internet Protocol
ODBC	Open DataBase Connectivity
ICA	Independent Computing Architecture

Seznam obrázků

Obrázek 1 Virtualizace (Zdroj: [1])	2
Obrázek 2 Typy Hypervisorů (Zdroj: http://www.slideshare.net)	5
Obrázek 3 Architektura Hypervisorů (Zdroj: [4]).....	6
Obrázek 4 Architektura John Von Neumanna (Zdroj: wiki.sps-pi.cz).....	7
Obrázek 5 Plná virtualizace (Zdroj: www.datamation.com)	8
Obrázek 6 Paravirtualizace (Zdroj : www.simplex.com)	9
Obrázek 7 Virtualizace aplikací (Zdroj: www.vmware.com).....	11
Obrázek 8 Technologie VDI VMware (Zdroj: www.vmware.com)	15
Obrázek 9 Xen Rings (Zdroj: www.slideshare.net).....	19
Obrázek 10 Architektura Xen (Zdroj: wiki.xen.org).....	20
Obrázek 11 VDI-in-a-Box (Zdroj: www.oldanygroup.cz)	21
Obrázek 12 Vlastnosti XenDesktop a XenApp (Zdroj: [24]).....	22
Obrázek 13 Architektura Hyper-V (Zdroj: en.wikipedia.org)	26
Obrázek 14 Microsoft Virtualization (Zdroj: http://winblog.blob.core.windows.net)	27
Obrázek 15 Vlastní infrastruktura VMware (Zdroj: autor).....	31
Obrázek 16 Vlastní infrastruktura Hyper-V (Zdroj: autor)	34
Obrázek 17 Vlastní infrastruktura Citrix (Zdroj: autor)	36
Obrázek 18 Před ukončením skriptu (Zdroj: autor)	38
Obrázek 19 Analýza rozptylu, Bonferroniho test – Test Kopírování	54
Obrázek 20 Analýza rozptylu, Bonferroniho test – Test Microsoft Office	55
Obrázek 21 Analýza rozptylu, Bonferroniho test – Test Webový prohlížeč.....	55

Seznam tabulek

Tabulka 1 Maximální hardwarové limity (Zdroj: autor)	28
--	----

Podklad pro zadání DIPLOMOVÉ práce studenta

PŘEDKLÁDÁ:	ADRESA	OSOBNÍ ČÍSLO
Müller Marek	Gagarinova 706, Hradec Králové - Slezské Předměstí	I14760

TÉMA ČESKY:

Virtualní desktohy na platformě VMware, Hyper-V a Citrix

TÉMA ANGLICKY:

Virtual desktops on platform VMware, Hyper-V and Citrix

VEDOUcí PRÁCE:

Ing Jan Budína - KIKM

ZÁSADY PRO VYPRACOVÁNÍ:

Cíl práce:

Tato práce obsahuje a popisuje základní teoretické informace v oblasti virtualizace a virtualizačních platformách firem VMware, Microsoft a Citrix. Popisuje protokoly PCoIP, RDP a ICA, které slouží pro přenos obrazu virtuálních desktopů jednotlivých technologií. Práce dále obsahuje informace a postupy k vytváření a instalaci virtuální infrastruktury, virtuálních desktopů a porovnává hypervisory ESXI, Hyper-V a XEN. Práce porovnává tyto hypervisory na základě testů a to z hlediska výpočetního výkonu, nároků na šířku přenosového pásma a uživatelské přívětivosti.

Osnova práce:

- 1) Úvod
- 2) Základní pojmy a historie
- 3) Virtualizační technologie pro virtuální desktohy
- 4) Infrastruktura pro virtuální desktohy
- 5) Testovací metodika
- 6) Testy infrastruktury
- 7) Zpracování a shrnutí výsledků
- 8) Závěr

SEZNAM DOPORUČENÉ LITERATURY:

tištěná, elektronická

Podpis studenta: 

Datum: 11. 11. 2016

Podpis vedoucího práce: 

Datum: 11. 11. 2016