MORAVSKÁ VYSOKÁ ŠKOLA OLOMOUC
Ústav informatiky a aplikované matematiky

Jan Jakob

Cloud computing

Bakalářská práce

Vedoucí práce: Mgr. Zdeňka Krišová

Olomouc 2014

Prohlašuji, že jsem bakalářkou práci vypracoval samostatně a použil jen uvedené informační zdroje. Prohlašuji, že odevzdaná tištěná verze bakalářské práce se shoduje s elektronickou verzí vloženou do IS/STAG.

V Olomouci dne 31. 3. 2014 Podpis: .....

Poděkování

Rád bych poděkoval Mgr. Zdeňce Krišové za cenné rady, věcné připomínky a vstřícnost při konzultacích a vypracování bakalářské práce.

Zadání 2/2

Obsah

1 Úvod

Cloud computing je v současnosti velmi aktuální. V dnešní době, kdy se firmy snaží snižovat náklady a současně chtějí zvýšit svou konkurenceschopnost, je právě cloud computing tématem, o kterém se stále více hovoří. Cloud computing představuje nový způsob chápání informačních technologií, umožňuje pružně reagovat na potřeby firemního IT.

Stále více činností z oblasti informačních technologií je možné předat třetí straně (dodavateli služeb) a uvolněné prostředky (lidské zdroje, finance) zaměřit na hlavní předmět podnikání. Z výsledků průzkumu[1], který v roce 2013 publikovala poradenská firma KPMG, vyplynulo, že téměř polovina dotázaných (48 %) považuje jako hlavní důvod pro zavedení cloudu úsporu nákladů. Dalšími důvody byly: rychlost osvojení cloudu (28 %), vstup podniku na nový trh (27 %), transformace podnikových procesů (22 %) a vylepšení podpory a vztahů se zákazníky (20 %).

Cílem této práce je vytvořit modelový příklad virtuální infrastruktury v prostředí cloudu pro středně velký podnik za účelem prezentovat dostupnost cloudových služeb.

K dosažení tohoto cíle je třeba splnit níže uvedené dílčí cíle:

- Definovat pojem cloud computing a jeho základní vlastnosti.
- Popsat a provést komparaci modelů poskytování služeb.
- Analyzovat problematiku bezpečnosti a dostupnosti dat.
- Navržení metodologie vytvoření virtuální infrastruktury v cloudu.
- Provést kalkulaci provozních nákladů vytvořené virtuální infrastruktury.

K naplnění uvedených cílů budou použity výzkumné metody: analýza. komparace, interview, aplikace a experiment.

[1] KPMG INTERNATIONAL, *The cloud takes shape: Global cloud survey: the implementation challenge* [online], Dostupné z: https://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/cloud-service-providers-survey/Documents/the-cloud-takes-shapev2.pdf

2 Cloud computing

2.1 Definice

V literatuře se objevují různé definice cloud computingu. Poradenská společnost Gartner ve svém článku[2] popisuje cloud computing jako styl práce na počítači, kde prostředky IT jsou škálovatelné a flexibilní a poskytovány zákazníkům jako služba využívající technologie Internetu. V knize Cloud Computing Bible[3] je cloud definován na základě dvou základních pojmů, které jsou s ním spjaty – abstrakce a virtualizace.

- **Abstrakce**: Cloud computing abstrahuje detailní popis implementace systému. Aplikace běží na nespecifikovaném fyzické systému (hardwaru), data jsou uložena na místech, jenž nám nejsou známa, správa systému může být prostřednictvím outsourcingu předána další straně a uživatelé se k systému mohou připojit kdykoliv a odkudkoliv.

- **Virtualizace**: Prostřednictvím sdružování a sdílení zdrojů nabízí cloud computing možnost virtualizace systémů. Datová úložiště a systémy mohou být nabídnuty podle potřeby a centralizovaná infrastruktura pro ně alokuje potřebné zdroje. Náklady jsou stanoveny na základě využití zdrojů, jenž mohou být rychle rozšiřitelné.

Většina literatury uvádí odkaz na definici[4], kterou publikoval Národní úřad pro standarty a technologie Spojených států (NIST – National Institute of Standards and Technology). Ten definuje cloud computing jako model služby umožňující odkudkoliv, na vyžádání a snadno se připojit prostřednictvím sítě ke sdíleným prostředkům konfigurovatelných výpočetních zdrojů (jako jsou například servery, datová úložiště, sítě, aplikace či služby), které mohou být rychle k dispozici a stejně rychle i uvolněny s minimální potřebou řízení nebo potřeby spolupráce s poskytovatelem služby.

---

[2] Srov. CEARLEY, David W. a Kyle HILGENDORF, Cloud Computing Innovation Key Initiative Overview. In: *Technology Research — Gartner Inc.* [online], Dostupné z: https://www.gartner.com/doc/1745015/cloud-computing-innovation-key-initiative

[3] Srov. SOSINSKY, Barrie A. *Cloud Computing Bible*, s. 4.

[4] Srov. MELL, Peter a Timothy GRANCE, *The NIST Definition of Cloud Computing*, Dostupné z: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

V definici se dále uvádí, že zmíněný model cloudu se skládá z pěti základních charakteristik (on-demand self-service, broad network access, resource pooling, rapid elasticity, measured service), ze čtyř modelů nasazení (deployment models) a tří modelů služeb (service models). Jednotlivým charakteristikám a modelům se budu věnovat v dalších kapitolách.

2.2 Historie

Koncept cloud computingu se zrodil již v šedesátých letech 20. století. Americký vědec J.C.R. Licklider, jenž se zasloužil o vznik sítě ARPANET, předchůdce dnešního Internetu, představil myšlenku tzv. intergalaktické počítačové sítě. Jeho vizí bylo zpřístupnit programy a data komukoliv a odkudkoliv na světě.

Dalším vědcem, jemuž je připisován koncept cloudu, je, taktéž americký vědec, John McCarthy. Přišel s nápadem nabízet výpočetní technologie jako veřejnou službu (na vyžádání, anglicky on-demand).[5]

V sedmdesátých letech byl jeho koncept implementován firmou IBM, která uvolnila operační systém VM OS pro jejich mainframe systémy System/370. Operační systém umožnil pomocí technologie virtualizace (věnuje se jí kapitola 4.1.2) provozovat více virtuálních strojů s vlastním operačním systém na jednom fyzickém zařízení. Zdroje jako procesor, paměť či pevný disk tak mohly být sdíleny více uživateli (virtuálními stroji). Rozvoj virtualizace a cloud computingu jsou spolu úzce spjaty.[6]

Samotný pojem cloud computing byl poprvé použit až v roce 1997 a to profesorem Ramnathem K. Chellappem na jeho přednášce v rámci kongresu INFORMS v americkém Dallasu.[7]

Milníkem pro cloud computing byl nástup Salesforce.com v roce 1999. Firma se stala průkopníkem koncepce poskytování podnikových aplikací přes webové stránky. V roce 2002 přispěla k dalšímu rozvoji společnost Amazon. Představila nabídku clou-

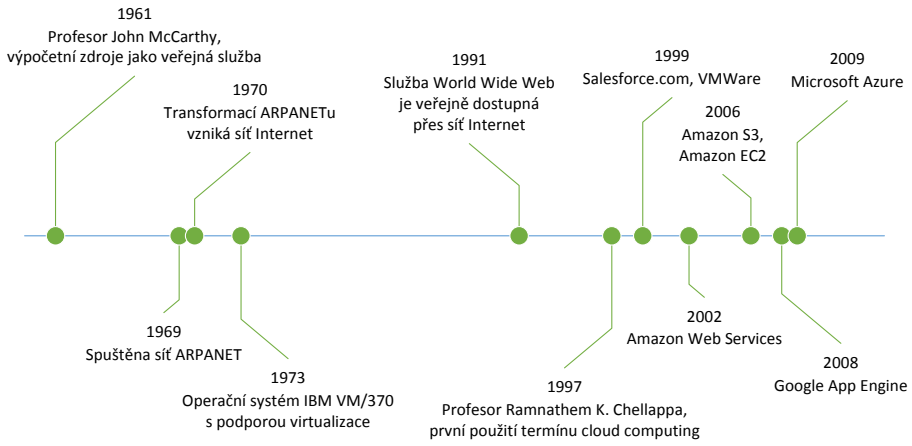
[5] Srov. MOHAMED, Arif, A history of cloud computing. In: *ComputerWeekly.com* [online], Dostupné z: http://www.computerweekly.com/feature/A-history-of-cloud-computing

[6] Srov. STEDDUM, James, A Brief History of Cloud Computing. In: *SoftLayer Blog* [online], Dostupné z: http://blog.softlayer.com/2013/virtual-magic-the-cloud

[7] Srov. Ramnath K. Chellappa, PhD, *Goizueta Business School* [online], Dostupné z: http://www.bus.emory.edu/ram/

dových služeb pod názvem Amazon Web Services (nabízející například výpočetní zdroje nebo datové úložiště). Později přišly s nabídkou snadno dostupných cloudových služeb také velké firmy jako Microsoft a Google a popularita cloud computingu začala rychle růst.[8]

Některé významné milníky v rozvoji cloud computingu, například vznik sítě Internet a nástup cloudových služeb od firem Amazon, Google nebo Microsoft, jsou znázorněny na časové ose na obrázku 1.



Obrázek 1: Historie cloud computingu[9]

2.3 Charakteristické vlastnosti

Nejprve zmíníme základní charakteristiky uvedené v definici NIST:

- **On-demand self-service**: Můžeme přeložit jako „samoobsluha na vyžádání“. Představuje možnost získání výpočetních zdrojů samostatně uživatelem bez potřeby kontaktovat poskytovatele služby. V porovnání například s klasickými servery, můžeme výrazně flexibilněji měnit parametry.

- **Broad network access** (širokopásmový přístup k síti): Připojení ke zdrojům v cloudu je k dispozici prostřednictvím sítí skrze standardní mechanismy, jenž umožňují na platformě nezávislý přístup z různých klientským zařízení (například notebook, mobilní telefon, tablet).

[8] Srov. MOHAMED, Arif, A history of cloud computing. In: *ComputerWeekly.com* [online], Dostupné z: http://www.computerweekly.com/feature/A-history-of-cloud-computing

[9] Vlastní zpracování

- **Resource pooling** (sdílení zdrojů): Poskytovatel služby nabízí k využití sdílené zdroje v rámci jednoho systému (služby) s podporou vícenásobného použití (multitenance). Podstatou tohoto konceptu je jistá úroveň abstrakce. Prostředky (procesor, paměť, datové úložiště, síť) pro virtuální systémy mohou být alokovány podle potřeby, ale neznáme jejich fyzické umístění (datacentrum, stát).

- **Rapid elasticity** (rychlá pružnost): Zdroje jsou poskytovány rychle a pružně. Systém může podle potřeby navýšit výkon (zapojením výkonnějších počítačů nebo použitím více počítačů stejně výkonných). Z pohledu zákazníka se jeví poskytované zdroje jako neomezené.

- **Measured service** (měřitelné služby): Veškeré využívané zdroje v rámci poskytovaných cloudových služeb jsou měřitelné, zákazníkům jsou poskytovány reporty a audity. Princip měřitelnosti tvoří základ ekonomického modelu služeb v cloudu. Zákazníci platí za to, co skutečně využijí – princip „pay-as-you-go“ (někdy označovaný také jako „pay-per-use“ či „charge-per-use“). Měří se například využití procesoru, paměti, množství provedených transakcí, síťový přenos.

Kromě výše uvedených vlastností by měl cloud computing splňovat i tyto další:

- **Nízká cena**: Vzhledem k tomu, že zdroje v cloud computingu jsou oproti klasické infrastruktuře využívány efektivněji, je možné dosáhnout na ceny, které vedou k úspoře nákladů za provoz informačních technologií v podniku.

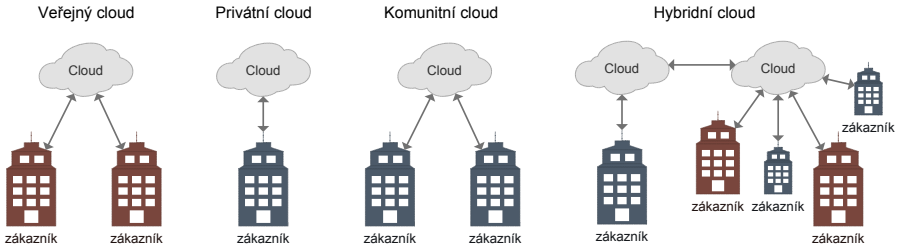
- **Jednoduché použití**: V závislosti na typu nabízené služby nemusíme potřebovat k její implementaci žádný hardware nebo softwarové licence.

- **Spolehlivost**: Velikost cloudových systémů a jejich technologie, jako je vyrovnání zátěže (load balancing) nebo vyřešení výpadku (failover) pomocí redundantních zařízení, zvyšují spolehlivost, která je tak mnohem vyšší než v případě vlastního řešení.[10]

[10]Srov. SOSINSKY, Barrie A., *Cloud Computing Bible*, s. 17.

3 Modely nasazení

Modely nasazení (anglicky deployment models) reprezentují způsob sdílení infrastruktury využívané pro poskytování cloudových služeb z pohledu zákazníka. Na obrázku 2 jsou znázorněny základní čtyři modely nasazení, jenž vychází z definice NIST.



Obrázek 2: Deployment models[11]

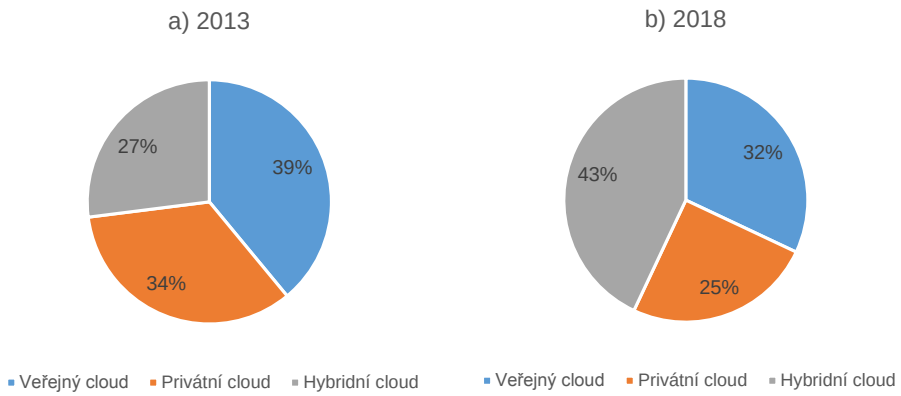
V roce 2013 provedla investiční společnost North Bridge průzkum[12] mezi firmami, které s cloudem pracují. Z průzkumu vyplynulo, že mezi modely nasazení je na prvním místě veřejný cloud s podílem 39 %, následuje privátní cloud s 34 % a hybridní cloud s 27 % (komunitní cloud nebyl v průzkumu zahrnut). Ve stejné zprávě je uveden i náhled na budoucí vývoj. Předpokládá se, že na vedoucí pozici se za pět let dostane s podílem 43 % hybridní cloud, veřejný cloud bude mít podíl 32 % a privátní 25 %.[13] Na obrázku 3 jsou výsledky průzkumu a budoucí odhad v grafické podobě.

Rozdíly mezi jednotlivými modely nasazení jsou popsány v následujících podkapitolách.

[11] Vlastní zpracování

[12] Průzkumu se zúčastnilo 855 respondentů, mezi nimiž byly jak prodejci cloudových služeb, tak také jejich zákazníci.

[13] Srov. 2013 Cloud Computing Survey. In: *North Bridge* [online], Dostupné z: http://www.northbridge.com/2013-cloud-computing-survey



Obrázek 3: Graf podílů modelů nasazení: a) rok 2013, b) výhled do roku 2018[14]

3.1 Veřejný cloud

Veřejný cloud (anglicky public cloud) je nejrozšířenější a nejdostupnější forma cloudu. Na rozsáhlé infrastruktuře jsou poskytovány veřejně služby všem zájemcům (od jednotlivců až po velké podniky). Poskytovatel veřejného cloudu služby hostuje, spravuje (instaluje, aktualizuje, ...) a prodává. Uživatelé se k veřejnému cloudu mohou vzdáleně připojit (prostřednictvím sítě Internet), užívat poskytované služby a výpočetní zdroje poskytovatele (providera). Zaplatí pouze za to, co skutečně využijí (služba, výkon, ...), což ve spojitosti s cenou je jedna z největších předností veřejného cloudu. Nevýhodou jsou naopak omezené možnosti přizpůsobení a případně i nevyhovující politika zabezpečení, kterou nemáme možnost ovlivnit.[15]

3.2 Privátní cloud

Privátní (soukromý) cloud (anglicky private cloud) je uzavřený cloud provozovaný výhradně pro určitou organizaci. Hostován a spravován může být přímo danou organizací nebo i třetí stranou (forma outsourcingu). Podobně jako u veřejného cloudu je i zde možné dosáhnout škálovatelného výkonu prostřednictvím virtualizované infrastruktury. Rozdíl je v tom, že zde zákazník platí již za celou pronajatou infrastrukturu (výpočetní zdroje) nebo v případě provozování vlastního cloudu musí podnik hradit provoz a mít dostatek finančních prostředků na pořízení celé

[14] Vlastní zpracování

[15] Srov. MAHMOOD, Zaigham a Richard HILL, *Cloud computing for enterprise architectures*, s. 6.

potřebné infrastruktury. Vlastní odpovědnost za provoz privátního cloudu přináší výhodu v možnostech většího přizpůsobení a poskytuje lepší kontrolu nad bezpečností a dodržováním stanovených vnitropodnikových předpisů a pravidel.[16]

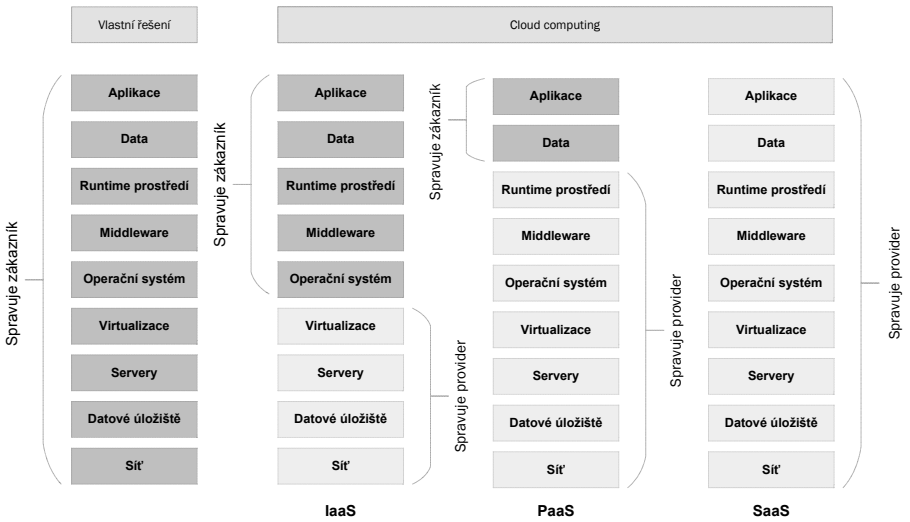
3.3 Hybridní cloud

Hybridní cloud (anglicky hybrid cloud) představuje spojení cloudu veřejného a privátního. Jednotlivé typy cloudu jsou propojeny prostřednictvím standardizovaných protokolů a vystupují navenek jako jeden celek. Vlastní zdroje (privátní cloud) mohou být snadno podle potřeby rozšířeny o ty externí (veřejný cloud). Tato kombinace vytváří infrastrukturu, kterou můžeme lépe spravovat a kontrolovat. Důležité je zde stanovení odpovědnosti za jednotlivé části cloudu (obvykle je rozdělena mezi podnik provozující privátní cloud a poskytovatele cloudu veřejného). Hybridní cloud může být pro podniky, které mají z cloudu obavu, tou nejvhodnější cestou. Citlivá data mohou být spravována podnikem v privátním cloudu, kde jsou stanoveny například vlastní bezpečnostní předpisy a pravidla, a ostatní data a aplikace mohou být převedeny do veřejného cloudu. Nevýhodou tohoto řešení je složitější implementace, jenž zajistí integraci vnitřního prostředí s vnějším (privátního a veřejného cloudu).[17]

3.4 Komunitní cloud

Posledním modelem nasazení je komunitní cloud (anglicky community cloud). Tento typ cloudu je využíván organizacemi, jež spojuje podobná činnost, bezpečnostní a jiná vnitropodniková pravidla, podléhají například stejné legislativě a využívají víceméně stejné služby. Správou cloudu je pověřena zvolená organizace nebo třetí strana. Nejčastěji je komunitní cloud využíván veřejnou správou.[18]

[16] Srov. MAHMOOD, Zaigham a Richard HILL, *Cloud computing for enterprise architectures*, s. 6.
[17] Srov. MAHMOOD, Zaigham a Richard HILL, *Cloud computing for enterprise architectures*, s. 6.
[18] Srov. SOSINSKY, Barrie A., *Cloud Computing Bible*, s. 8.



Obrázek 4: Service models[19]

4 Modely služeb

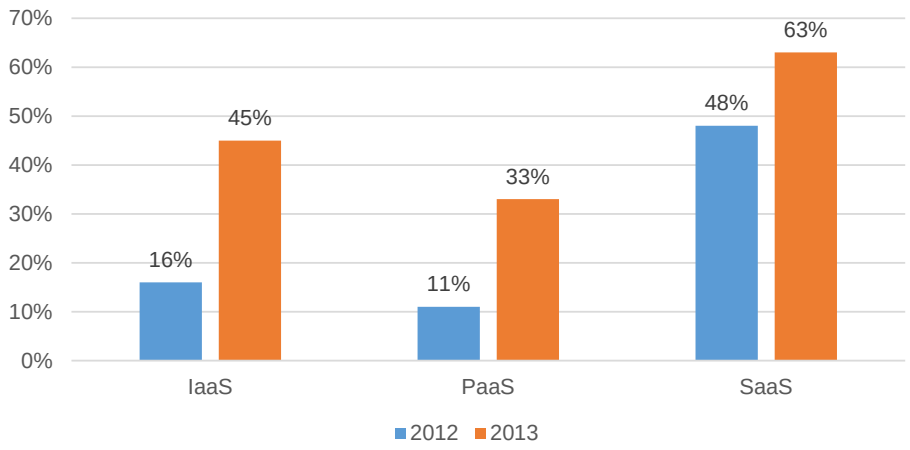
Modely služeb, někdy označované jako distribuční modely (anglicky service models), nahlíží na cloud computing z pohledu poskytovaných služeb. Podle definice NIST rozlišujeme tři základní modely – infrastruktura jako služba (Infrastructure as a Service, zkráceně IaaS), platforma jako služba (Platform as a Service, zkráceně PaaS) a software jako služba (Software as a Service, zkráceně SaaS). Z pohledu zákazníka je v cloud computingu důležité určit hranici, která rozděluje zodpovědnost za funkčnost systému (služby) mezi zákazníka a poskytovatele služby. Na obrázku 4 je znázorněn rozdíl mezi základními modely služeb spolu s rozdělením zodpovědnosti.

Podle průzkumu z roku 2013[20] používá 63 % dotázaných firem SaaS, což představuje nárůst 15 % oproti přechozímu roku 2012. 45 % uživatelů cloudových služeb využívá IaaS, v přechozím roce to bylo o 29 % méně, a PaaS používá 32 % respondentů, o 22 % více než v roce 2012 (viz obrázek 5).

V současnosti je nabízeno mnohem více služeb označovaných dovětkem „as a Service“. Může se jednat například o virtualizované desktopy (Desktop as a Service, zkráceně DaaS) nebo o službu pro správu identit (Identity as a Service, zkráceně IDaaS).

[19] Vlastní zpracování

[20] 2013 Cloud Computing Survey. In: *North Bridge* [online]. 2013 [cit. 2014-03-22]. Dostupné z: http://www.northbridge.com/2013-cloud-computing-survey



Obrázek 5: Podíly jednotlivých modelů služeb podle průzkumu mezi firmami[21]

4.1 Infrastructure as a Service

V tomto modelu má primární roli virtualizace. Poskytovatel služby Infrastructure as a Service (zkráceně IaaS) využívá své fyzické hardwarové vybavení, na němž je nám schopen nabídnout potřebné výpočetní zdroje, nejčastěji v podobě virtuálních strojů (serverů) ve spojení s datovým úložištěm, síťovou konektivitou a dalšími výpočetními zdroji. Nabízí nám tak kompletní infrastrukturu, kterou sám spravuje. Zákazník naopak zodpovídá za veškeré aspekty spojené s nasazením – instalace a správa libovolného operačního systému, middlewaru a aplikací.

Místo toho, aby podnik musel zakoupit servery, datové úložiště, síťová zařízení či software, může vše plně outsourcovat a platit za službu podle toho, co skutečně využije (pay-as-you-go). Tento princip, kdy si kupujeme výpočetní zdroje, je někdy označován jako utility computing.[22]

Obchodní model IaaS může být nabízen ve třech formách – modelech nasazení: veřejný, soukromý, hybridní. Ve veřejném cloudu jsou aplikace a služby provozovány na sdílených prostředcích, což je vhodné zejména pro méně důležité business aplikace, jednotlivé uživatele a malé a střední podniky. Na druhé straně privátní cloud je vhodný pro ty podniky, které mají speciální požadavky, jako jsou například: zabezpečení, údržba a řízení zdrojů, dodržení firemních a legislativních pravidel, atd.

[21] Vlastní zpracování

[22] Srov. MAHMOOD, Zaigham a Richard HILL, *Cloud computing for enterprise architectures*, s. 9.

Kombinací veřejného a privátního cloudu vzniká hybridní model, kde část infrastruktury je vyhrazena (privátní cloud) a zbytek je sdílen (veřejný cloud).[23]

4.1.1 Workload

V modelu nasazení IaaS je základní jednotkou virtualizovaného prostředí workload, jenž simuluje možnosti a výkon skutečného fyzického serveru. Práci vykonanou jednotkou workload lze měřit podle počtu provedených transakcí za minutu TPM (Transactions Per Second). Sledovat můžeme také další atributy, jako jsou diskové operace IOPS (Input/Output Per Second), množství vyžívané paměti RAM (v MB), síťová propustnost a latence apod.

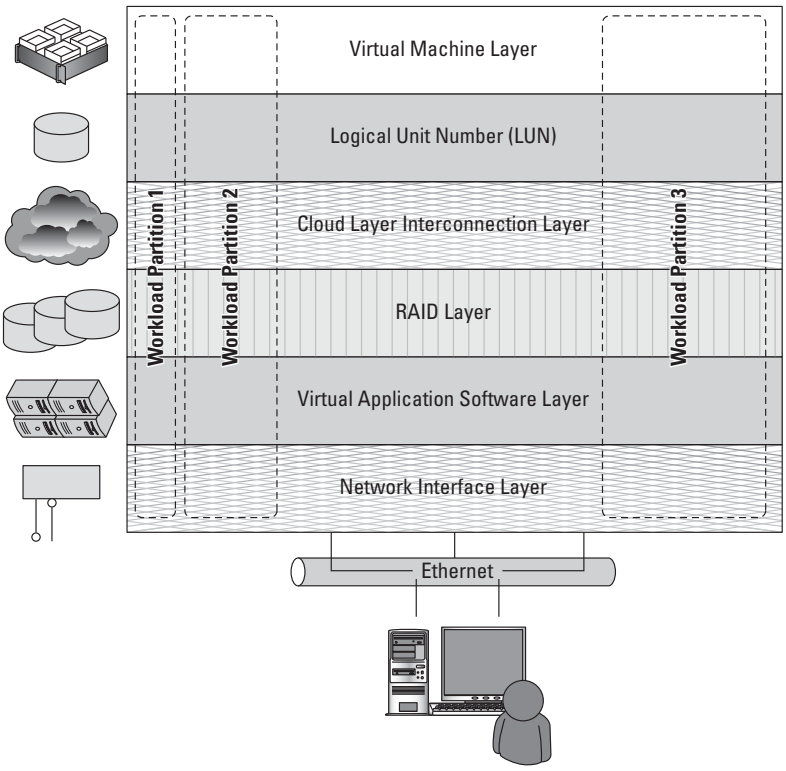
V případě hostovaného řešení, označuje se také jako hosting environment, běží aplikace na našem vlastním serveru nebo na serveru dedikovaném, jenž jsou v obou případech umístěny v datacentru poskytovatele ICT služeb. Oproti tomu v modelu cloud computingu je zákazníkovi nabídnut server jako instance s požadovaným výpočetním výkonem, jenž je možné podle potřeb zákazníka dynamicky měnit.

Na obrázku 6 jsou znázorněny tři instance virtuálních privátních serverů rozložené do zásobníku IaaS. Tři typy workload vyžadují různě velký výpočetní výkon – malý, střední, velký. Instance serverů běží na IaaS infrastruktuře tak, že čerpají z fondu virtuálních strojů, kapacity diskových polí RAID a kapacity síťového rozhraní. Tyto tři zmíněné vrstvy vyjadřují fyzické systémy, jenž jsou rozděleny na logické jednotky.

Dále si popišme jednotlivé logické vrstvy. Logical unit number (LUN) je logický kontejner pro data. Cloud interconnection layer je virtuální síťová vrstva, která přiřazuje IP adresy z rozsahu alokovaného pro IaaS síť. A virtual application software layer je virtuální aplikační vrstva obsahující software, jenž běží na fyzických zařízeních a umožňuje jejich výkon rozdělit či spojit a vytvořit tak například privátní cloud na IaaS infrastruktuře.[24]

---

[23] Srov. MAHMOOD, Zaigham a Richard HILL, *Cloud computing for enterprise architectures*, s. 50.
[24] Srov. SOSINSKY, Barrie A., *Cloud Computing Bible*, s. 67.



Obrázek 6: Virtuální privátní server v modelu IaaS[25]

4.1.2 Virtualizace

Virtualizace abstrahuje základní zdroje a zjednodušuje jejich použití, izoluje jednoho uživatele od druhého a podporuje replikaci zvyšující pružnost systému. V cloud computingu má nezanedbatelnou roli jak z pohledu poskytovatele, tak i zákazníka.

Virtualizace je úspěšně používána od konce šedesátých let 20. století. V roce 1959 byla na univerzitě v Manchesteru na počítači Atlas poprvé implementována virtuální paměť (paging), kterou využívá operační systém.[26] Princip spočívá v tom, že data jsou odkládána do bloků označovaných jako stránky (pages) a uloženy v sekundární paměti (např. pevném disku). Operační systém k datům poté přistupuje jako k primární paměti (RAM).

Virtualizace představuje simulaci rozhraní fyzického objektu jedním ze čtyř způsobů:

[25]SOSINSKY, Barrie A., *Cloud Computing Bible*, s. 68.

[26]Srov. MARINESCU, Dan *C*, Cloud *computing: theory and practice*, s. 133.

- Multiplexing: Je vytvořeno více virtuálních objektů z jedné instance objektu fyzického. Například procesor je prostřednictvím multiplexingu rozdělen mezi řadu procesů či vláken.

- Agregace: Z více fyzických objektů je vytvořen jeden objekt virtuální. Například řada fyzických pevných disků je agregována do jednoho disku RAID.

- Emulace: Z jednoho fyzického objektu je vytvořen jeden virtuální objekt simulující jiný fyzický systém. Například fyzický disk může být emulován na paměť náhodného přístupu (RAM).

- Kombinace multiplexingu a emulace: Například TCP protokol emulující spolehlivý přenos bitů a multiplexing fyzického komunikačního kanálu a procesoru.[27]

Z hlediska aplikací nebo uživatelů má virtuální stroj (virtual machine) všechny charakteristiky a atributy fyzického systému, Jedná se ale striktně o software, který fyzický stroj emuluje. Systém virtuálního stroje má přidělen vlastní adresový prostor v paměti, jsou mu přidělovány zdroje procesoru a využívá vlastní I/O zařízení s použitím vlastních ovladačů virtuálního zařízení. Některé virtuální stroje mohou být uzpůsobeny pouze pro běh jediné aplikace nebo procesu, jedná se o to tzv. process virtual machines.

Virtuální počítač je od fyzického počítače, na kterém běží, oddělen. Tato virtualizační technologie má několik výhod. Umožňuje nám spouštět více instancí s různými verzemi operačních systému, testovat aplikace v izolovaném prostředí (tzv. sandbox) a v případě cloud computingu vytvářet instance virtuálních strojů, které jsou přiřazeny k jednotkám workload.[28]

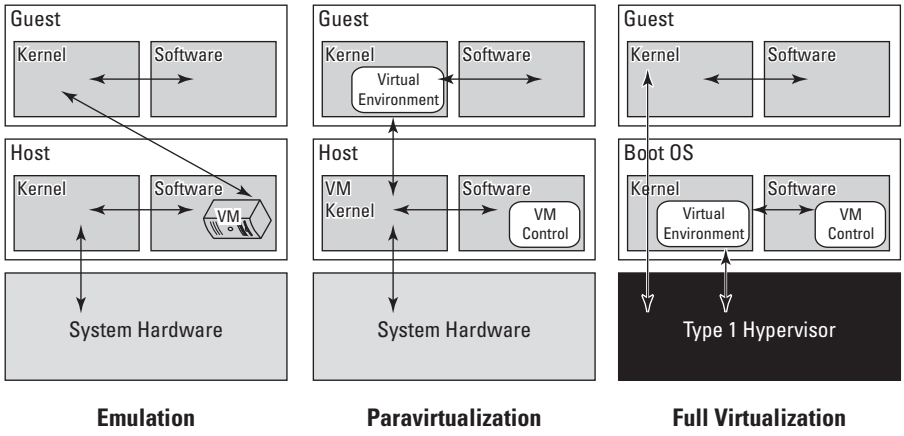
Program zajišťující virtuálním strojům přístup k systémovým zdrojům je označován jako Virtual Machine Monitor (VMM) nebo také hypervizor. VMM umožňuje běh několika operačních systémů současně na jedné hardwarové platformě, jednotlivé systémy od sebe izoluje, čímž zvyšuje bezpečnost a kontroluje, jak hostované operační systémy (guest operating system) využívají hardwarové zdroje. Dojde-li

[27] Srov. MARINESCU, Dan C., *Cloud computing: theory and practice*, s. 132.
[28] Srov. SOSINSKY, Barrie A., *Cloud Computing Bible*, s. 67.

v jednom virtuálním stroji k nečekané události, díky izolaci neovlivní žádný jiný virtuální stroj, jenž běží pod stejným hypervizorem. Rozlišujeme dva základní typy hypervizorů.[29]

První typ hypervizoru běží přímo na fyzickém stroji. Jako příklad můžeme uvést hypervizory Oracle VM, VirtualLogic VLX a VMware ESX. Druhý typ hypervizoru běží nad operačním systém nainstalovaným přímo na fyzickém stroji. Operační systém na této úrovni označujeme jako hostitelský (host operating system). Příkladem tohoto typy hypervizoru je Microsoft Hyper-V, VMware Fusion, Xen a mnoho dalších. V případě Hyper-V může být hostitelským operačním systémem například Microsoft Windows Server. Naopak Xen běží nad systémem Linux.

Na obrázku 7 je znázorněno další typové dělení virtualizace spojené s virtuálními stroji – emulace, paravirtualizace a úplná virtualizace.



Obrázek 7: Typy virtualizace počítačů[30]

Emulace simuluje hardware pro potřeby virtuálního stroje, jenž je tak nezávislý na skutečném hardwaru. Hostující operační systém tak nemusí být díky emulaci nijak upravován.

V případě paravirtualizace poskytuje hostitelský operační systém virtuálnímu strojí rozhraní, pomocí něhož hostující operační systém přistupuje přímo k hardwaru. Hostující operační systém musí být upraven, aby rozhraní hostitele podporoval.

Nakonec úplná virtualizace odpovídající prvnímu typu hypervizoru umožňuje

[29]Srov. MARINESCU, Dan C., *Cloud computing: theory and practice*, s. 136.
[30]SOSINSKY, Barrie A., *Cloud Computing Bible*, s. 102.

vytvořit virtuální stroj přímo nad skutečným hardwarem. Všechny hostující operační systémy v úplné virtualizaci komunikují přímo s hypervizorem a není potřeba je upravovat. Výkon hostujících operačních systémů (virtuálních strojů) je v porovnání s předchozími typy virtualizace nejvyšší.[31]

4.2 Platform as a Service

Model platforma jako služba (zkráceně PaaS) nabízí softwarové prostředí pro vývoj, nasazení a běh aplikací, aplikačních serverů či databází. Zahrnuje podporu pro vývoj aplikací, load balancing, škálovatelnost, multitenanci[32] a umožňuje snížit náklady na vývoj.

Platforma je založena na specifickém programovacím jazyce (může jich být současně podporováno více). Jako příklad můžeme uvést jazyky PHP, Python, Java a jazyky z rodiny .NET. Někteří poskytovatelé navíc nabízí i vlastní vývojářské nástroje. Rozhraní (GUI) aplikací je obvykle vytvářeno pomocí technologií, jako jsou HTML5, JavaScript či Silverlight. Nasazené aplikace běží v privátním či veřejném cloudu a jsou přístupné prostřednictvím sítě Internet.

Zákazník služby na bázi PaaS odpovídá za data, funkčnost nasazené aplikace a její správnou interakci s platformou. V některých případech je možné si hostované prostředí i částečně přizpůsobit. Platforma může být spravována prostřednictvím uživatelského rozhraní nebo pomocí vlastních aplikací díky poskytnutému API[33] rozhraní. Poskytovatel služby se stará o vše ostatní – od údržby fyzického hardwaru, přes konfiguraci a správu operačního systému a middlewaru až po zajištění funkčního běhové prostředí a instalaci frameworku (například .NET).

Platforma jako služba je zajímavá z hlediska nákladů. Poskytovatelé služby mohou nabídnout zajímavou cenu díky jejich snaze o maximální optimalizaci a snížení nákladů na provoz. Nemusíme investovat do nákupu hardwaru a softwarových licencí (operační systém, databáze a pod.) a platit za jejich správu. Platíme jen za nákup či vývoj nasazených cloudových aplikací a za prostředí, kde aplikace běží a to

[31] SOSINSKY, Barrie A., *Cloud Computing Bible*, s. 100-102.

[32] Multitenance je schopnost sdílet jednu aplikaci nebo výpočetní zdroje více uživateli.

[33] API je zkratka Application Programming Interface. Představuje sadu příkazů a funkcí, jenž mohou programátoři využít ve svých programech.

podle skutečného využití výpočetního výkonu a prostředků (procesor, paměť, datové úložiště, síťový provoz, ...).

Nevýhodou tohoto modelu je, že současní poskytovatelé nabízí služby na svých proprietárních řešeních, což znesnadňuje přenositelnost aplikací a dat k jinému poskytovateli.

Na globálním trhu je několik velkých poskytovatelů PaaS služeb. Jako příklad můžeme uvést služby Google App Engine, Microsoft Azure Web Sites, Amazon Web Services, Salesforce1 Platform, IBM WebSphere sMash. Většina poskytovatelů se snaží pro svou platformu získat vývojáře tak, že jim nabídne zpočátku celou platformu téměř bez nákladů.[34] Například Google App Engine nabízí 1 GB datového prostoru, dostatek výpočetního výkonu a 2 GB pro síťový přenos zcela zdarma. Pokud pro aplikaci potřebujeme vyšší limity, nezbývá než přejít na placenou variantu.[35]

4.3 Software as a Service

Posledním ze základních modelů cloudových služeb je Software as a Service (zkráceně SaaS), tedy nabídka softwaru (aplikací) jako služby v prostředí cloudu. V porovnání s předchozími modely se zákazník stará pouze o správu vložených dat (nikoliv o jejich zálohování) a správu uživatelských účtů. Poskytovatel odpovídá za všechny vrstvy zobrazené na obrázku 4 – od aplikace až po infrastrukturu.[36] To, že je software nabídnut zákazníkovi jako hotové řešení, neznamená, že by se nedal upravit. Některá řešení SaaS dávají vývojářům k dispozici rozhraní API, takže mohou své stávající aplikace s těmi v cloudu propojit nebo propojit více cloudových aplikací mezi sebou či doplnit další funkce. Příkladem služby s dostupným API rozhraním je CRM systém[37] od Salesforce.com.[38]

SaaS aplikace obvykle běží na platformě a infrastruktuře poskytovatele služby, nemusí to být ale podmínkou. Každý vývojář si může zvolit libovolnou platformu,

[34] Srov. MAHMOOD, Zaigham a Richard HILL, *Cloud computing for enterprise architectures*, s. 52.

[35] Srov. App Engine. *Google Cloud Platform* [online], Dostupné z: https://cloud.google.com/products/app-engine

[36] Srov. SOSINSKY, Barrie A., *Cloud Computing Bible*, s. 10.

[37] CRM (Customer Relationship Management) je informační systém pro správu vztahů se zákazníky.

[38] Srov. SOSINSKY, Barrie A., *Cloud Computing Bible*, s. 71.

na které svůj software bude podle modelu SaaS nabízet. Aplikace jsou poskytovány prostřednictvím rozhraní tenkého klienta, obvykle webového prohlížeče, a jsou dostupné odkudkoliv prostřednictvím sítě Internet.

Nejvíce cloudových služeb je nabízeno právě v modelu SaaS. Zákazníci si mohou vybrat z široké palety aplikací. Velké softwarové firmy, které mají příjmy i z prodeje internetové reklamy, nabízí některé služby zdarma. Jde například o webové kancelářské aplikace Google Docs nebo Office Online, cloudová datová úložiště Google Drive, OneDrive nebo DropBox a mnoho dalších služeb. Téměř každý uživatel Internetu již s nějakou cloudovou aplikací pracoval. Nejčastěji se pravděpodobně jednalo o emailovou službu (například Gmail, Outlook.com), jenž nabízí pokročilé uživatelské rozhraní a je propojena s dalšími službami, jako je kalendář nebo správce kontaktů. Díky těmto zmíněným službám a mnohým dalším mohou jednotlivci i malé firmy používat základní cloudové aplikace bez dodatečných nákladů. Dosavadně používaný software může být nahrazen a tak lze také ušetřit na nákladech za správu softwaru a nákup licencí. Větší firemní zákazníci využívají placené aplikace, jako jsou podnikové informační systémy ERP[39], zákaznické informační systémy CRM, systémy pro poskytování podpory (Help Desk) a další.

Jak se uvádí v knize Cloud Computing Bible[40], všechny aplikace nabízené jako Software as a Service, by měly mít následujících osm společných charakteristik:

1. Software je k dispozici přes Internet odkudkoliv prostřednictvím internetového prohlížeče.

2. Licence jsou poskytovány na bázi předplatného nebo podle rozsahu použití. Účtování může být měsíční nebo roční. V některých výjimečných případech je spolu s licencí účtován poplatek za údržbu/správu.

3. Nabízený software a služby jsou monitorovány a udržovány poskytovatelem bez ohledu na to, kde jednotlivé softwarové komponenty běží (klient, server).

4. Ekonomickými přínosy SaaS aplikace jsou minimální náklady pro koncové uživatele a snížené náklady na distribuci a údržbu. V porovnání se standardní

[39] ERP (Enterprise Resource Planning) je informační systém, který integruje různé podnikové procesy (učetnictví, fakturace, logistika, ...).

[40] Srov. SOSINSKY, Barrie A., *Cloud Computing Bible*, s. 72.

zakoupenou a nainstalovanou aplikací bude stejně funkční aplikace v cloudu obecně levnější.

5. Aplikace jsou aktualizovány automaticky, opravy a novinky jsou nasazovány mnohem rychleji než u klasických aplikací.

6. SaaS aplikace mají často mnohem menší bariéry pro vstup na trh než konkurenční lokálně nainstalované (klasické) aplikace. Přispívá k tomu pravidelná výše nákladů vycházející z toho, jaké služby využíváme.

7. Všichni uživatelé pracují se stejnou verzí softwaru.

8. SaaS podporuje práci více uživatelů současně a poskytuje sdílený datový model skrze jednu instanci (model multitenance).

5 Bezpečnost

O bezpečnosti cloud computingu se hovoří poměrně často, dokonce se pořádají pravidelné kongresy[41], které se tomuto tématu věnují. Pro některé podniky je právě otázka bezpečnosti cloudu hlavní překážkou pro přechod na něj.

Samotní poskytovatelé cloudových služeb si nemohou dovolit otázku bezpečnosti podcenit. Pokud by bylo odhaleno slabé místo v jejich zabezpečení a v horším případě došlo i k úniku dat některého z klientů, poškodilo by to nejen jejich jméno a důvěru u současných i potenciálních zákazníků, ale v konečném důsledku by to mohlo ohrozit i jejich podnikání.

Zodpovědní poskytovatelé cloudových služeb provádějí pravidelné bezpečnostní audity a snaží se získávat bezpečnostní certifikáty od třetích stran (například SAS 70, ISO 2077, PCI DSS). Vnikla také oborová aliance Cloud Security Alliance, která šíří osvětu v oblasti zabezpečení cloudu. Vydává publikace s popisem aktuálních bezpečnostních hrozeb, metodiky k jejich eliminaci a provozuje webový portál s přehledem bezpečnostních praktik jednotlivých poskytovatelů.[42]

V následujících podkapitolách jsou zmíněny potencionální bezpečnostní hrozby a způsob jejich řešení v prostředí cloud computingu.

5.1 Únik a ztráta citlivých údajů

Pochopitelně žádné firmě se nelíbí, že jejich data putují „ven“ z jejich firmy a nemají přehled o tom, kde jsou geograficky uložena a kdo k nim má fyzická přístup. Vznikají tak obavy z případného úniku citlivých firemních údajů.

V tomto kontextu jsou zajímavé výsledky analýzy znaleckého ústavu Apogeo Eseem zveřejněné v časopise Security World. Podle této analýzy stojí za únikem nebo ztrátou dat ve $\frac{3}{4}$ případů zaměstnanci firmy. V polovině případů se jednalo o nedbalost zaměstnance. K dalším nejčastějším příčinám patří ztráta datového nosiče (13 %) a krádež dat (12 %). Teprve potom následují útoky zvenčí na IT infrastrukturu podniku.[43]

[41] Odborná konference Bezpečnost v cloudu, http://www.bezpecnostvcloudu.cz/

[42] Srov. *Security World: Čtvrtletník o informační bezpečnosti*, 2012, č. 1., s. 5.

[43] Srov. *Security World: Čtvrtletník o informační bezpečnosti.*, 2012, č. 1., s. 3.

Poskytovatel cloudových služeb, který prošel danou bezpečnostní certifikací, má své datové centrum zabezpečené, tzn. vybavené kamerových systém, nepovolané osoby se fyzicky k datovému úložišti dostat nemohou. Ostatní osoby se identifikují pomocí čipových karet nebo pokročilého biometrického zabezpečení (otisky prstů, snímání sítnice, apod.). Veškerá data zákazníků jsou šifrována pomocí pokročilých algoritmů, například asymetrickým šifrovacím algoritmem AES-256, který používá dva klíče – soukromý a veřejný. Přenos dat mezi podnikovou sítí a cloudem probíhá přes zabezpečený kanál, v případě webového rozhraní je použito šifrované spojení pomocí aplikačního protokolu HTTPS, u hybridního cloudu může být vytvořeno šifrované spojení VPN mezi firemním směrovačem či serverem a virtuální privátní sítí v cloudu.

Ať už podnik používá privátní, veřejný nebo hybridní cloud, je důležitá správa uživatelů (identit) a jejich rolí. Nesmí být možné, aby se nepovolené osoby dostaly k citlivým datům nebo měly přístup k podnikové síti a aplikacím i po jejich odchodu ze společnosti.

Postupně roste přijímání standardizovaných řešení pro správu identit v prostředí cloudu (například SAML, OpenID, SCIM). To umožňuje provádět centrální autentizaci. Nezáleží na tom, k jaké aplikaci (on-premise, cloud) a od jakého poskytovatele se chce uživatel přihlásit, vždy je ověřen na jednom centrálním místě.[44]

Informaci o tom, kde se naše data geograficky nacházejí, bychom měli obdržet přímo od poskytovatele. Například při objednávce služeb od velkých poskytovatelů jako jsou Amazon, Microsoft nebo Google máme v závislosti na rozmístění jejich datových center po světě na výběr lokalitu pro uložení našich.

5.2 Dostupnost služeb

Důležitým kritériem při volbě dodavatele cloudových služeb je kromě zabezpečení dat i garance dostupnosti služeb. Dodavatel se zákazníkem uzavírá smlouvu SLA (Service Level Agreement), ve které se zavazuje poskytovat služby nepřetržitě s minimálním přerušením. V případě výpadku služby na dobu delší než ji povoluje smlouva SLA, musí být podle této smlouvy zákazníkovi poskytnuta kompenzace

[44]Srov. *Security World: Čtvrtletník o informační bezpečnosti*, 2013, č. 1., s. 27.

nebo odškodnění za případné ztráty vzniklé v důsledku nedostupnosti.

Při výběru poskytovatele bychom se měli zajímat také o jeho finanční kondici a sledovat reference. I když máme uzavřenou platnou smlouvu SLA, v situaci, kdy poskytovatel ukončí náhle svou činnost, se ke svým datům budeme těžko dostávat. Tento jev by mohl v současnosti nastat u malých a kapitálově slabých společností, proto je lepší dávat přednost zavedeným poskytovatelům.

Kromě smlouvy SLA s poskytovatelem služeb, je důležité mít uzavřenou obdobnou službu také s poskytovatelem internetového připojení. Stálé a kvalitní datové připojení je pro provoz aplikací v cloudu klíčové.

Pokud podnik provozuje vlastní server, dochází k výpadkům jeho služeb nejčastěji v důsledku přetížení (nárůst požadavků, nedostatečný výkon), poruchy některé z komponent nebo k útoku zvenčí (například útok DDoS, kdy je server přetížen obrovským množstvím dotazů, obvykle s ním „bojují“ webové servery). Aby bylo možné výpadkům z uvedených důvodů předejít, musel by podnik investovat nemalé prostředku do redundance klíčových komponent serveru – napájení, záložní zdroje, zálohovací zařízení, zrcadlené diskové pole, chlazení apod. Dále síť zabezpečit výkonným firewallem a směrovačem. V případě nedostatečného výkonu serveru pořídit nový. A tady se projeví hlavní přínosy cloud computingu – škálovatelnost, spolehlivost, úspora nákladů.

Podle potřeby a stanovených pravidel může virtuální server obdržet více výpočetních prostředků a navýšit tak svůj výkon. Díky funkci load balancing (viz kapitolu 6.1) jsou požadavky podle potřeby rozloženy mezí více serverových instancí. Nemusíme se starat o fyzický hardware a řešit redundanci komponent. Virtuální server běží na rozsáhlém hardwaru v datovém centru poskytovatele a díky pokročilé technologii virtualizace (viz kapitolu 4.1.2) může být v případě poruchy ihned spuštěn server záložní. Síťová infrastruktura poskytovatele by měla být natolik výkonná, aby odolala běžným pokusům o útok zvenčí.

5.3 Legislativa

Z pohledu legislativy hraje geografické umístění dat v cloudu velkou roli. Pokud jsou data uložena například na serverech ve Spojených státech amerických, podléhají legislativě dané země. Americké firmy mají v některých případech do-

konce povinnost předat federálním úřadům data zákazníků bez ohledu na to odkud pocházejí. Pro státy v Evropské unii (EU) platí směrnice 95 / 46 / ES o ochraně osobních údajů, která nepovoluje zpracovávat osobní údaje o rezidentech EU bez jejich souhlasu a navíc jejich předání do třetích zemí povoluje pouze v případě zajištění „přiměřené úrovně ochrany“. Což by výše uvedený příklad se Spojenými státy nesplňoval. V České republice je navíc nutné přihlédnout k zákonu č. 101 / 2000 Sb., o ochraně osobních údajů a k zákonu o elektronických komunikacích č. 127 / 2005 Sb. Proto je důležité důkladně zanalyzovat, jaká data a kde budou ukládána.[45]

Velcí hráči na poli cloudových služeb (Google, Microsoft, Amazon, ...) mají v Evropě vybudována svá datová centra a dávají zákazníkům na výběr, kde budou jejich data fyzicky uložena. Podobně se je rozhodla následovat i společnost Sales-Force.com, která oznámila, že v roce 2014 otevře v Evropě tři nová datová centra.[46] Uživatelé cloudových služeb tak mohou mít svá data „blíže“, navíc se na ně bude vztahovat evropská legislativa.

[45] Srov. *Security World: Čtvrtletník o informační bezpečnosti.*, 2012, č. 1., s. 3.

[46] KANARACUS, Chris. Salesforce.com to add three data centers in Europe. In: *PCWorld* [online], Dostupné z: http://www.pcworld.com/article/2103900/salesforcecom-to-add-three-data-centers-in-europe.html

6 Popis vybraných služeb

V této kapitole si popíšeme některé z celosvětově nejznámějších cloudových služeb: Amazon EC2, Google App Engine a Windows Azure Web Sites. Služba Amazon EC2 byla zvolena, protože se stala průkopníkem v poskytování služeb IaaS. Široce využívaná služba Google App Engine byla pro změnu vybrána jako reprezentant služby typu PaaS. Prostor je věnován pro porovnání i další službě typu PaaS a to Windows Azure Web Sites. Jelikož pochází z dílny softwarového giganta firmy Microsoft, nabízí úzké spojení s platformou .NET a s dalšími technologiemi od této firmy.

6.1 Amazon EC2

Amazon Elastic Compute Cloud (zkráceně Amazon EC2) je služba typu IaaS nabízející výpočetní zdroje v prostředí cloudu. Přes webové rozhraní můžeme jednoduše vybudovat virtuální infrastrukturu zahrnující virtuální servery (EC2 instance), privátní virtuální síť, datové úložiště a další. V případě virtuálního serveru si můžeme například navolit výkon procesoru, velikost paměti RAM i lokálního úložiště dat. Veškerá správa virtuálních serverů a sítí probíhá přes webové rozhraní (EC2 konzoli) nebo skrze API rozhraní.

Amazon EC2 nabízí řadu funkcí a služeb. Například funkce Auto Scaling umožňuje definovat pravidla pro automatické škálování, tzn. podle potřeby navýšit počet aktivních EC2 instancí. Další funkce Elastic Load Balancing zajistí automatické rozdělení příchozího provozu aplikací napříč více instancemi EC2. To nám umožní zvýšit odolnost našich aplikací proti chybám a přetížení. Pokud je odhalena problémová instance, Elastic Load Balancing přesměruje provoz na jinou.

Pomocí předkonfigurovaných šablon s obrazy operačních systémů, tzv. Amazon Machine Image (zkráceně AMI), můžeme jednoduše a rychle zprovoznit vlastní server. Na výběr máme mezi operačními systémy Linux (CentOS, Amazon Linux, Red Hat, Ubuntu a další) a Windows Server. Vytvořit si můžeme i vlastní obraz AMI obsahující naše data, aplikace nebo nastavení.

Amazon EC2 nabízí možnost zvolit si umístění instancí podle geografického umístění datacentra. V současné době je k dispozici devět oblastí: Jižní Virginie,

Oregon, Severní Kalifornie, Irsko, Singapur, Tokio, Sydney, Sau Paulo a GovCloud (specifický region splňující kritéria daná americkými vládními agenturami). V roce 2014 má být spuštěno nové datacentrum v Pekingu. Ve smlouvě SLA pro EC2 se Amazon zavazuje ve všech regionech zajistit 99,95 % měsíční dostupnost.

K instanci EC2 je možné připojit perzistentní datové úložiště, jenž nabízí služba Amazon Elastic Block Store (zkráceně EBS). Každý diskový svazek je automaticky replikován v rámci své zóny v daném datacentru, což zvyšuje dostupnost dat v případě selhání některé hardwarové komponenty. Diskové obrazy můžeme také kopírovat a přesouvat mezi datovými centry v různých lokalitách. Diskové svazky EBS nabízí konzistentní výkon s nízkou latencí. Podle potřeby lze kapacitu svazku během pár minut navýšit nebo snížit.

Virtuální servery lze zahrnout do virtuální privátní sítě. Prostřednictvím služby Amazon Virtual Private Cloud máme nad virtuální sítí úplnou kontrolu. Můžeme si zvolit rozsah IP adres, vytvářet podsítě, definovat pravidla pro směrování a nastavit výchozí brány. Vlastní podnikovou síť můžeme prostřednictvím zabezpečeného spojení VPN (Virtual Private Network) propojit s virtuální privátní sítí v cloudu.

U všech cloudových služeb od Amazonu platí, že platíme za to, co skutečně využíváme, například za hodinový čas běžící instance nebo za datový přenos.[47]

V současnosti má na trhu Amazon EC2 řadu konkurentů. Z těch globálních stojí za zmínku Windows Azure Virtual Machines a Google Compute Engine.

6.2 Google App Engine

Google App Engine je služba postavená na modelu PaaS. Provozuje ji společnost Google na své infrastruktuře a v komerční nabídce je od podzimu roku 2011. Na platformě App Engine můžeme snadno vytvářet, spouštět a udržovat webové aplikace. Podle potřeby zle změnit velikost datového úložiště a měnit další různé limity (například pro přenos dat). Díky poskytnuté platformě není potřeba spravovat žádný server a provádět složitou konfiguraci. Aplikace po nahrání do cloudu je hned připravena ke spuštění.

[47] Srov. Amazon EC2 Product Details. *Amazon Web Services* [online], Dostupné z: http://aws.amazon.com/ec2/details/

Google App Engine podporuje aplikace napsané v těchto programovacích jazycích: Java, Python, PHP a Go. S daty umožňuje pracovat více způsoby. Kód a statická data se ukládají do úložiště s označením Datastore. K ukládání velkých binárních souborů, jako jsou například videa a obrázky, je vymezeno úložiště Blobstore. Strukturovaná data se ukládají do databáze Google Cloud SQL, se kterou se pracuje stejně jako s databází MySQL, nabízena je ale jako samostatná služba.

App Engine zajišťuje spolehlivý běh aplikací, i když jsou silně vytížené nebo pracují s velkým množstvím dat. K tomu přispívají následující vlastnosti platformy:

- Perzistentní datové úložiště s podporou dotazování, třídění a transakcí,
- Automatická škálovatelnost a vyvažování zátěže (load balancing),
- Asynchronní fronty úkolů pro zpracování mimo rámec žádosti,
- Plánované úkoly ke spouštění akcí ve stanovený čas nebo v pravidelných intervalech,
- Integrace s dalšími cloudovými službami a rozhraními API služeb Google (například Google Analytics, Google Adwords, Google Maps).

Aplikace běží v bezpečném izolovaném a spolehlivém prostředí, v tzv. sandboxu, které je nezávislé na hardwaru, operačním systému nebo fyzickém umístění serverů. App Engine je schopen distribuovat požadavky napříč více servery a podle potřeby je škálovat.

Vývojáři aplikací mají zdarma k dispozici Software Development Kit (SDK) – sadu vývojářských nástrojů. Stáhnout si mohou verzi odpovídající zvolenému programovacímu jazyku a operačnímu systému, do nějž budou SDK instalovat. SDK obsahuje:

- Všechny knihovny a API, jež jsou podporovány v App Engine,
- Testovací prostředí emulující všechny služby App Engine na lokálním počítači,
- Nástroje pro nasazení, které umožní například nahrát aplikaci do cloudu nebo spravovat různé verze aplikace.

V lokálním prostředí se aplikace spravují pomocí SDK. U aplikací nasazených v produkčním prostředí se ke správě používá administrátorská konzole s webovým rozhraním. Umožňuje vytvářet nové aplikace, konfigurovat doménová jména a služby, zvolit verzi aplikace k nasazení, spravovat přístup k aplikaci, monitorovat chybové zprávy a mnoho dalšího.[48]

Google App Engine je možné využívat zcela zdarma, tedy pokud nepotřebujeme přesáhnout limity stanovené pro bezplatnou verzi služby (Free). Kromě omezení v podobě limitů je tato varianta služby poskytována bez smlouvy SLA. U dalších variant Paid a Premier je již smlouva SLA uzavírána a slibuje až 99,95 % měsíční dostupnost služeb.

6.3 Windows Azure Web Sites

Konkurencí pro Google App Engine je nabídka společnosti Microsoft, služba Windows Azure Web Sites z rodiny cloudových služeb Windows Azure. Poprvé byla komerčně nabídnuta v prvním čtvrtletí roku 2010.

Platforma je postavena na infrastruktuře založené na systémech Windows Server. Podporuje řadu programovacích jazyků – ASP.NET, PHP, Node.js, Python či klasické ASP. Pro práci se strukturovanými daty jsou k dispozici dva typy relačních databázových systémů – Windows SQL Azure (upravená verze databáze SQL Server pro cloud) a MySQL (populární open-source databáze). Platforma Windows Azure Web Sites je zajímá také nabídkou více než 30 open-source aplikací, frameworků a šablon (například: Wordpress, Drupal, CakePHP, Django).[49]

Začínající vývojáři na platformě Windows Azure si mohou stáhnout zdarma dostupný softwarový balík WebMatrix. Obsahuje základní nástroje pro snadný vývoj a nasazení aplikací v cloudu. Pro ty pokročilejší je k dispozici Azure SDK, které se integruje do známého vývojářského softwaru Microsoft Visual Studio. SDK umožňuje vytvářet aplikace podporující škálovatelnost zdrojů v cloudu a prostřednictvím Visual Studia dále aplikace nasazovat a spravovat.

[48] Srov. What Is Google App Engine?. *Google Developers* [online], Dostupné z: https://developers.google.com/appengine/docs/whatisgoogleappengine

[49] Srov. Web Sites. *Windows Azure* [online], Dostupné z: https://www.windowsazure.com/en-us/services/web-sites/

Jakmile je webová aplikace nasazena a spuštěna, můžeme použít webové rozhraní Windows Azure Management Portal ke sledování a konfiguraci. Na informačním panelu se zobrazí rychlý přehled o využívaných zdrojích a chybových zprávách, ke kterým došlo. V rámci možností konfigurace můžeme vybrat, jaká verze frameworku .NET nebo PHP bude použita, nastavit zabezpečené spojení pomocí certifikátů, vlastní doménu, diagnostické protokolování a provádět mnoho dalších nastavení.

Jednou z posledních přidaných funkcí v rámci Azure Web Sites je automatické škálování. Nabízeny jsou tři režimy pro provoz webových aplikací – Free, Shared, a Standard. V režimu Free a Shared se webové aplikace spouští v multitenantním prostředí a mají určeny kvóty pro výpočetní zdroje (procesor, paměť, síť), které mohou využívat. Režim Free je navíc omezen počtem webových aplikací a je poskytován bez smlouvy SLA. Jak z jeho názvu vyplývá, je zdarma, ale vzhledem k jeho omezením je vhodný zejména pro začínající vývojáře a testování bez dodatečných nákladů. Režim Shared je poskytován se smlouvou SLA, bez omezení počtu aplikací, s vyššími limity a ručně škálovatelným výkonem. Nejpokročilejší je režim Standard, jenž umožňuje běh webových aplikací na dedikovaném virtuálním stroji. Na výběr jsou tři typy instancí podle výpočetního výkonu – Small (1 jádro, 1,75 GB RAM), Medium (2 jádra, 3,5 GB RAM) a Large (4 jádra, 7 GB RAM). V případě, kdy je zapnuta funkce automatického škálování pro procesor, mohou být nastavena pravidla pro automatické škálování instancí, tzn. podle potřeby vyššího výkonu je vytvořeno více instancí. Pro režim Standard garantuje smlouva SLA 99,9 % měsíční dostupnost.[50]

V rámci Windows Azure je nabízeno velké množství služeb – SQL databáze, datová úložiště a další. Na Windows Azure Web Sites navazuje služba Windows Azure Cloud Services, která nabízí další pokročilejší možnosti pro nasazení aplikací v cloudu.

[50] Srov. TULLOCH, Mitch, *Introducing Windows Azure For IT Professionals* [online], Dostupné z: http://aka.ms/682887pdf, s. 23-27.

7 Virtuální infrastruktura v podnikové síti

V následujících kapitolách si ukážeme, jak jednoduše můžeme vytvořit virtuální infrastrukturu v prostředí cloudu pomocí služby Windows Azure od společnosti Microsoft. Důvodem výběru této služby je její přímá podpora pro platformu Windows, jenž nám umožní jednoduše nakonfigurovat virtuální síť, zprovoznit virtuální servery a vše jednoduše propojit se stávající infrastrukturou. Rozsahem nabízených služeb je cloudová služba Windows Azure podobná službě Amazon Web Service, jejíž dílčí služba Amazon EC2 byla popsána v kapitole 6.1.

Na ukázkovém příkladu budeme simulovat převedení části infrastruktury středně velkého podniku do prostředí cloudu. Nastavíme některé služby a propojíme cloud s fyzickou infrastrukturou v podniku. Na závěr se podíváme na provozní náklady takto vytvořené infrastruktury. Celý příklad vytvoření virtuální infrastruktury má za cíl demonstrovat dostupnost a jednoduchost této služby. V praktické části této práce jsou využity informace získané během studijní praxe ve středně velkém podniku z Olomouckého kraje. K získání informací byla použita metoda rozhovoru.

Veškerá správa služeb z rodiny Windows Azure probíhá přes webové rozhraní dostupné na adrese http://manage.windowsazure.com/. Abychom se mohli do administrace přihlásit, je potřeba mít vytvořený účet. Po zaregistrování můžeme po dobu 30 dní veškeré služby bezplatně otestovat, k tomuto účelu obdržíme kredit ve výši € 150.

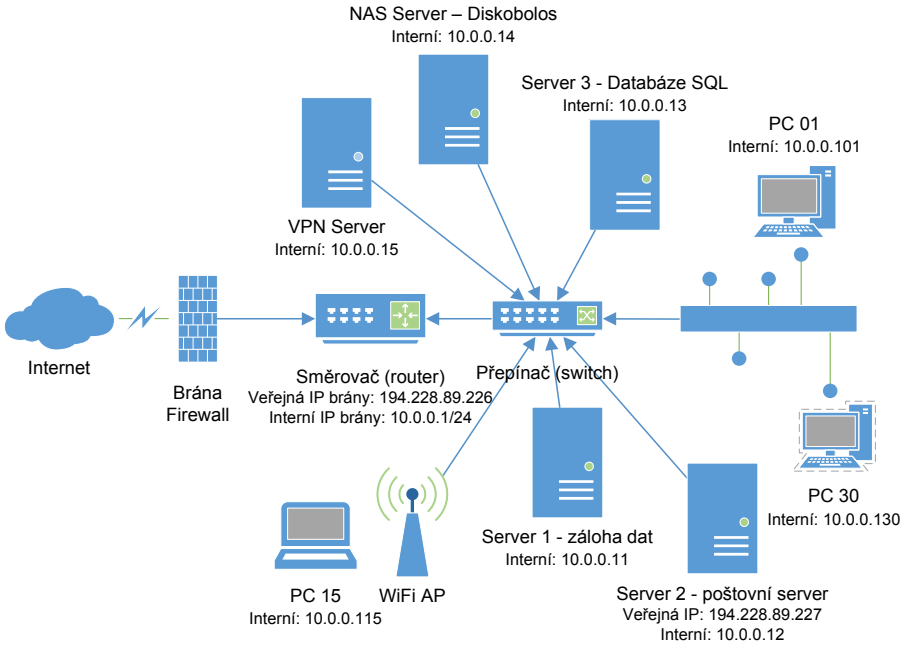
7.1 Popis fyzické infrastruktury podniku

V podniku je nyní instalováno pět fyzických serverů, jejich konfigurace a primární účel je uveden v tabulce 1. Dále je k síti připojeno diskové úložiště Discobolos určené k zálohování všech dat ze serverů, síťový směrovač, několik přepínačů (značky Bay Network, D-Link a 3Com), VPN router Nortel Networks a bezdrátový přístupový bod (WiFi Acces Point, značka Netgear).

Konektivita k síti Internet je zajištěna prostřednictvím bezdrátového point-to-point spojení v pásmu 10 GHz s garantovanou rychlostí 50 Mbit oběma směry (upload / download). Podnik má předěleny dvě veřejné IP adresy. Adresa vnitřní podnikové sítě je 10.0.0.0/24.

Typ serveru	Konfigurace	Poznámka
IBM Xeon System X3650 M3	CPU 2 x 2,67 GHz, 48 GB RAM, 3 x 146 GB + 8 x 300 GB HDD	Na serveru běží virtuální servery s databází MS SQL Server 2003 a 2008, primární server pro ukládání dat z ERP informačního systému (IS), nový server z roku 2013, pořizovací cena 107 552 Kč bez DPH (zdroj: CZC.cz)
Sun SunFire X4150	CPU 2 x 2,33 GHz, 32 GB RAM, 2 x 146 GB + 5 x 300 GB HDD	Záložní server pro ERP IS, OS Linux
IBM X Series 235	CPU 2 x 2,67 GHz, 2,5 GB RAM, 6 x 74 GB HDD	Server pro běh staré verze ERP IS (data z dceřiné společnosti), OS Linux
IBM X Series 225	CPU 2 x 2,2 GHz, 2 GB RAM, 2 x 360 GB HDD	Poštovní server s licencí Kerio Connect pro 50 uživatelů, OS Linux
Office Pro 5000	CPU 2 x 2,2 GHz, 2 GB RAM, 2 x 360 GB HDD	Technologický server, propojení výrobních zařízení

Tabulka 1: Přehled podnikových serverů[51]



Obrázek 8: Schéma podnikové sítě[52]

Na obrázku 8 je zjednodušené schéma podnikové sítě. Nejsou v něm zahrnuty všechny virtuální servery a všechny klientské stanice, kterých je v podniku celkem 30. Veškeré datové toky z a do sítě Internet prochází přes směrovač s integrovanou

[51] Vlastní zpracování

[52] Vlastní zpracování

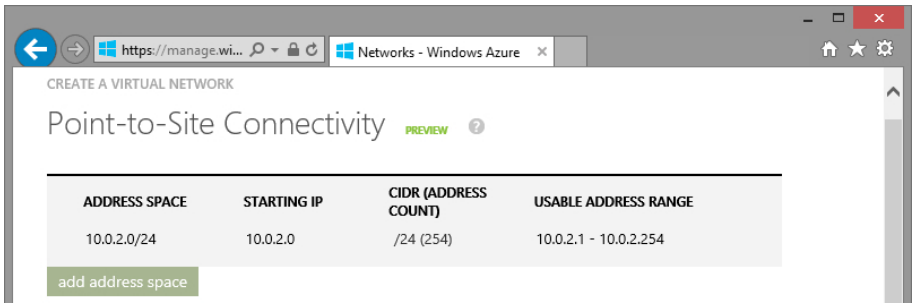
bránou firewall. Další důležitou komponentou podnikové sítě je VPN server. Má funkci síťové brány pro zabezpečený a šifrovaný přenos dat a ověřuje autentizaci a autorizaci uživatelů, kteří se chtějí do podnikové sítě přihlásit vzdáleně přes síť Internet. Na obrázku je dále znázorněn poštovní server a server pro zálohování dat (NAS). Tyto dva posledně zmíněné servery v našem příkladu převedeme do cloudu, jako ukázku možností cloudové služby Windows Azure.

7.2 Virtuální síť

Virtuální síť v cloudu nakonfigurujeme přes webovou administraci. Z nabídky vybereme *Add* → *Network Services* → *Virtual Network* → *Custom Create*. V prvním kroku zobrazeného průvodce zadáme název virtuální sítě (*olc-virtual*) a vybereme tzv. Affinity Group. Jedná se o skupinu, která říká, v jaké geografické lokalitě budou naše služby hostovány. Z rozbalovací nabídky zvolíme volbu pro vytvoření nové skupiny. Skupinu libovolně pojmenujeme (*Olomouc-Company*) a zvolíme region. V našem případě bychom měli zvolit datacentrum v Evropě. Na výběr máme mezi Europe North (Irsko) nebo Europe West (Nizozemí). Datové centrum v Evropě má výhodu v tom, že je nám geograficky blíže (dochází k menšímu zpoždění) a podléhá legislativě EU (viz kapitolu 5.3).

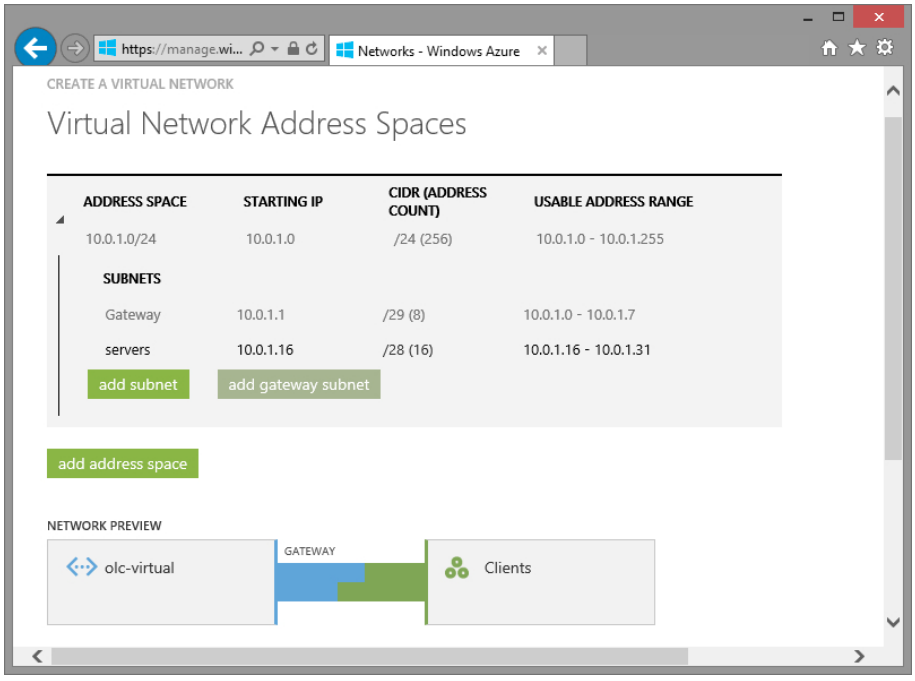
Pokračujeme krokem dva. Zde můžeme volitelně zadat název a IP adresu DNS serveru, který bude překládat doménová jména. Zatím, žádný nakonfigurován nemáme, tak tuto položku vynecháme. Budeme se věnovat možnostem konfigurace zabezpečeného VPN spojení. Na výběr máme mezi spojením *site-to-site* a *point-to-site*. V našem příkladu budeme konfigurovat spojení point-to-site pro připojení vnějších zařízení (klientů) do naší virtuální sítě. Druhý typ spojení, site-to-site, bychom použili pro propojení celé podnikové sítě s tou virtuální, jak jen znázorněno na obrázku 20. K tomu bychom potřebovali další hardwarové vybavení (například VPN server, vhodně nastavený směrovač a bránu firewall, atd.).

Označíme volbu konfigurace spojení point-to-site a pokračujeme třetím krokem, kde nastavíme rozsah IP adres vyhrazených pro vzdáleně připojená zařízení. V našem příkladu je použit rozsah adres (10.0.2.0/24) 10.0.2.1 – 10.0.2.254 (viz obrázek 9).



Obrázek 9: Nastavení rozsahu IP adres pro point-to-site VPN spojení[53]

V posledním kroku nastavíme rozsah IP adres virtuální privátní sítě, tedy té, do které budeme chtít zahrnout budoucí virtuální servery. IP adresa je virtuálnímu serveru přidělena automaticky prostřednictvím protokolu DHCP a zůstává mu napořád. Pokud bychom se pokusili nastavit IP adresu staticky, mohlo by dojít ke ztrátě spojení. Pro virtuální síť byl zvolen rozsah IP adres 10.0.1.0/24, dále byla definována podsíť 10.0.1.16/28 s názvem *servers* a automaticky vytvořená podsíť *Gateway* (viz obrázek 10). Volbou sítě a podsítě můžeme ovlivnit, z jakého rozsahu bude nově vytvořenému virtuálnímu serveru nebo službě adresa přidělena.



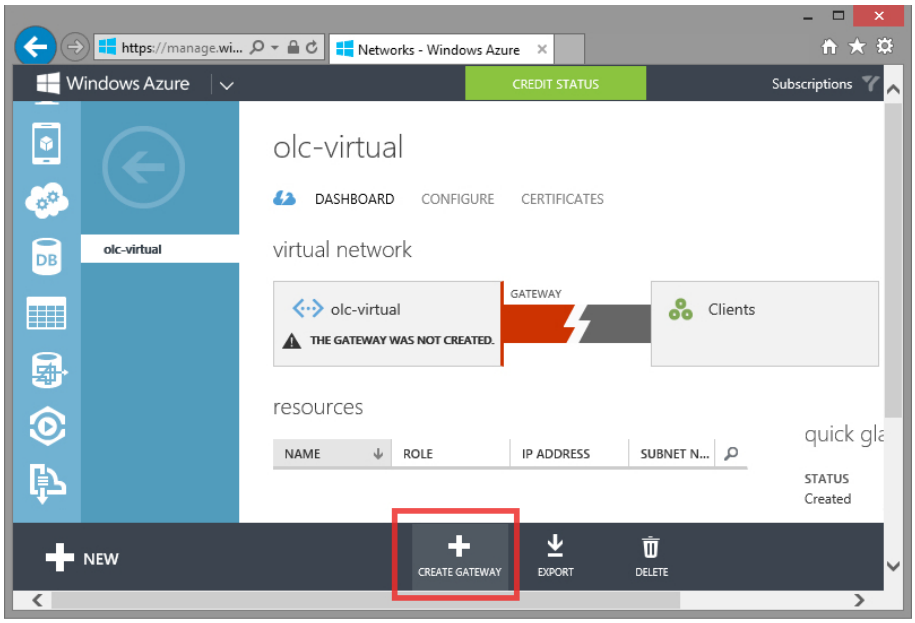
Obrázek 10: Nastavení rozsahu IP adres virtuální sítě[54]

Průvodce vytvořením nové virtuální sítě dokončíme potvrzením všech nasta-

[53] Vlastní zpracování

[54] Vlastní zpracování

vení. Jakmile bude síť připravena, můžeme vytvořit novou bránu (gateway) pro vzdálená VPN připojení. Z nabídky vybereme *Networks*→*Virtual Networks* a klikneme na naši síť (*olc-virtual*). Poté se přepneme na kartu *Dashboard*. Na této stránce máme k dispozici informace o stavu sítě – například seznam přidělených IP adres, počet klientů připojených přes VPN a další. Bránu vytvoříme kliknutím na tlačítko *Create Gateway* umístěné v zápatí této stránky (viz obrázek 11).



Obrázek 11: Vytvoření brány pro point-to-site VPN spojení[55]

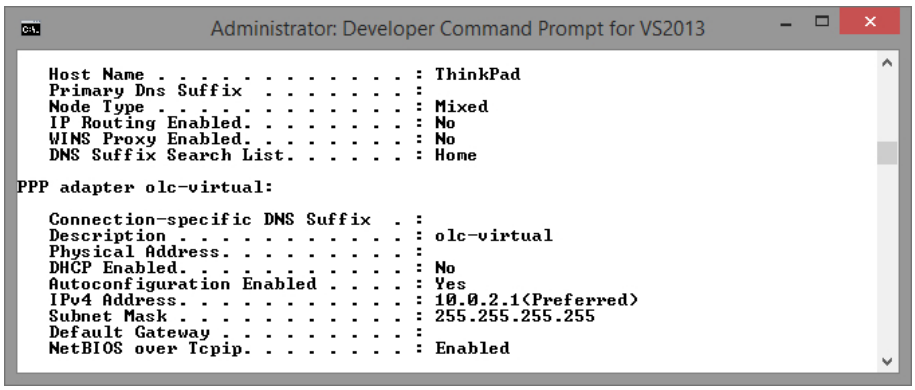
Point-to-site připojení vyžaduje po klientech ověření prostřednictvím certifikátu. Uživatel si musí vygenerovat veřejný a privátní klíč v zařízení, z kterého se bude chtít do virtuální sítě připojit. Privátní klíč by měl zůstat tajný a je vhodné si jej chránit heslem. Postup generování klíčů je již nad rámec této práce. Podrobný popis je uveden v online dokumentaci[56]. Předpokládáme, že klíče máme připravené. Z karty *Dashboard* se přepneme na *Certificates*, kde provedeme vložení veřejného certifikátu. Stejným způsobem můžeme přidat certifikáty dalších uživatelů.

Vrátíme-li se zpět na kartu *Dashboard*, nalezneme zde ke stažení malý konfigurační program, který na klientském počítači s Windows 7 nebo 8 a na serveru s Windows Server 2008 nebo 2012 nastaví vše za nás. V seznamu sítí máme po-

[55] Vlastní zpracování

[56] Configure a Point-to-Site VPN using the Management Portal Wizard. [online], Dostupné z: http://msdn.microsoft.com/en-us/library/windowsazure/dn133792.aspx

tom k dispozici VPN připojení s názvem naší virtuální sítě (*olc-virtual*). Funkčnost tohoto připojení si můžeme ověřit pomocí příkazu `ipconfig /all` zadaného v příkazovém řádku. Z výpisu informací zjistíme, zda jsme skutečně k virtuální síti připojeni a zda přidělená IP odpovídá námi definovanému rozsahu 10.0.2.1-10.0.254 (viz obrázek 12).



Obrázek 12: Ověření VPN připojení[57]

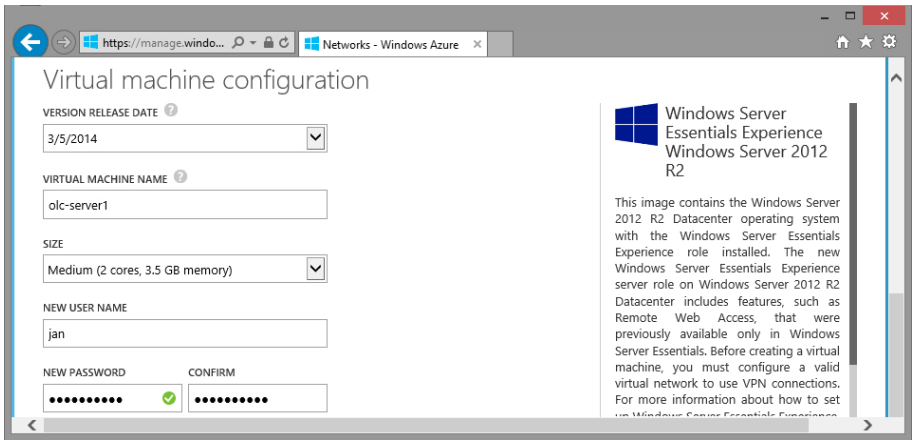
7.3 Virtuální server

Virtuální síť máme již připravenou, nyní do ní umístíme virtuální servery. Nejprve si vytvoříme virtuální server s operačním systémem Windows Server 2012. V administraci vybereme *Add*→*Compute*→*Virtual Machine*→*From gallery*. Nyní máme před sebou galerii předkonfigurovaných obrazů s operačními systémy. Na výběr máme mezi OS Windows Server, Linux (Ubuntu, CentOS, SUSE) a OS Windows Server s předkonfigurovanou instalací aplikací SQL Server, Sharepoint nebo BizTalk. Z nabídky zvolíme například instalaci Windows Server Essentials Experience (Windows Server 2012 R2) a pokračujeme dále.

Ve druhém kroku (viz obrázek 13) vybereme verzi obrazu OS. Podle data zvolíme tu nejaktuálnější (5. 3. 2014), která by měla obsahovat většinu aktualizací. Dále náš virtuální server pojmenujeme (*olc-server1*) a zadáme uživatelské jméno a heslo pro přihlášení k administrátorskému účtu na serveru. Na závěr tohoto kroku zvolíme výkonnostní konfiguraci serveru (*size*). Vybírat můžeme mezi virtuálním serverem se sdíleným procesorem a 768 MB RAM a serverem s až 8 jádry a 56 GB RAM.

[57] Vlastní zpracování

Zvolíme variantu *Medium* (CPU 2 jádra, 3,5 GB RAM). V dokumentaci je tato konfigurace doporučena pro připojení až 500 klientů k serveru. Přejdeme na krok 3.



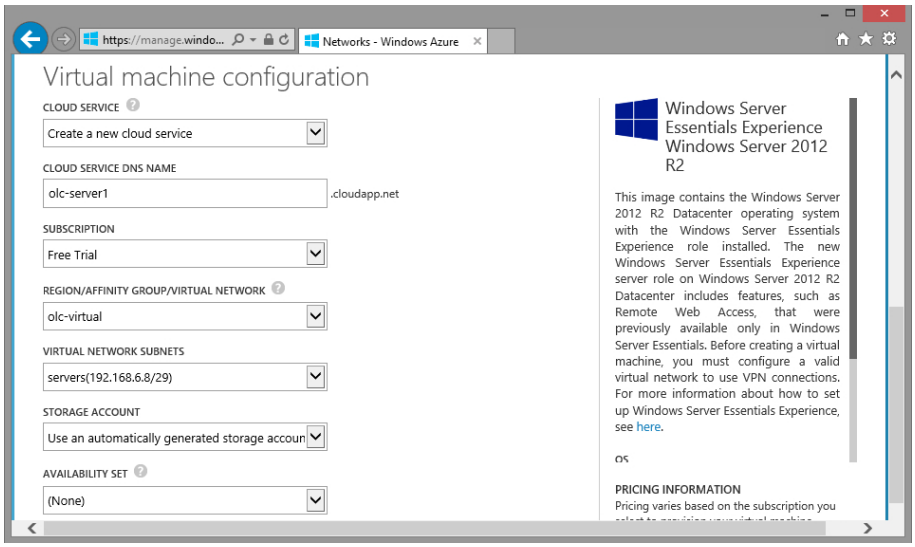
Obrázek 13: Vytvoření virtuálního serveru (krok 2)[58]

Ve třetím kroku tohoto průvodce (viz obrázek 14) nejprve nastavíme službu *Cloud Service* pro daný server. Jelikož se jedná o první server, necháme výchozí volbu *Create a new cloud service*. Cloud Service představuje kontejner, ve kterém je server umístěn. Pokud bychom později přidávali další servery, byla by k dispozici i druhá volba a to připojit nový server k některému z již existujících kontejnerů. Toto nastavení se využívá pro funkci load balancing (zmíněno v kapitole 6.1). Více serverů umístěných ve stejném kontejneru může zajistit vyšší dostupnost služeb.

Pokračujeme zadáním DNS jména kontejneru (název musí být jedinečný v doméně *.cloudapp.net*). Prostřednictvím doménového jména cloudové služby kontaktují server. Dále z nabídky *Region / Affinity Group / Virtual Network* vybereme námi vytvořenou virtuální síť (*olc-virtual*) spolu s její podsítí (*servers*). Virtuálnímu serveru bude poté přidělena IP adresa z rozsahu zvolené podsítě (10.0.1.16/28).

Nastavení *Storage Account* necháme na výchozí hodnotě, jež zajistí automatické vytvoření účtu a pod daným účtem vytvoří VHD soubor, pevný disk serveru. V rámci jednoho regionu je i pro více serverů použit vždy stejný účet. Poslední možnost nastavení v tomto kroku, *Availability Set*, necháme na výchozí hodnotě *None*. Toto nastavení slouží pro konfiguraci redundance, zajištění vyšší dostupnosti serverových služeb (například jeden server se musí restartovat kvůli aktualizaci, druhý server umístěný ve stejném kontejneru jeho roli převezme).

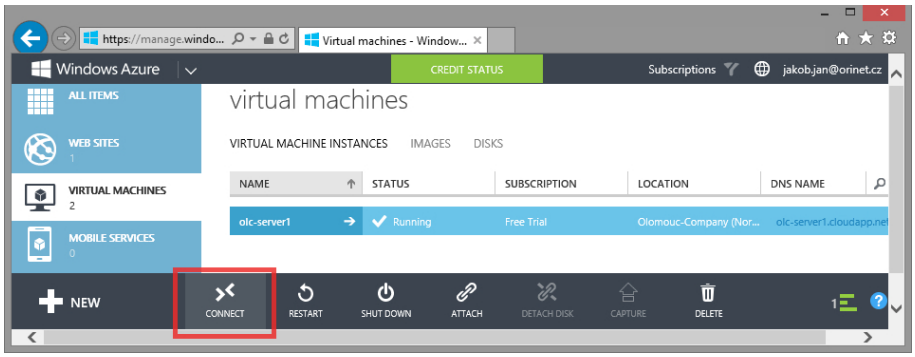
[58] Vlastní zpracování



Obrázek 14: Vytvoření virtuálního serveru (krok 3)[59]

V posledním kroku máme možnost nastavit protokoly a porty pro navázání spojení ze sítě Internet. Ponecháme výchozí nastavení. Povoleny jsou služby připojení ke vzdálené ploše a příkazový řádek PowerShell.

Průvodce vytvořením virtuálního serveru dokončíme a vyčkáme pár minut než bude server připraven. Připojení k serveru je velice jednoduché. Jakmile bude server připraven, v administraci zvolíme kategorii *Virtual Machines* a daný server vybereme. U spodního okraje okna prohlížeče se nám zobrazí základní příkazy pro práci se serverem. Server můžeme zapnout/vypnout, restartovat, připojit k němu další datové úložiště nebo se k němu vzdáleně připojit. Pro vzdálené připojení zvolíme *Connect* (viz obrázek 15).

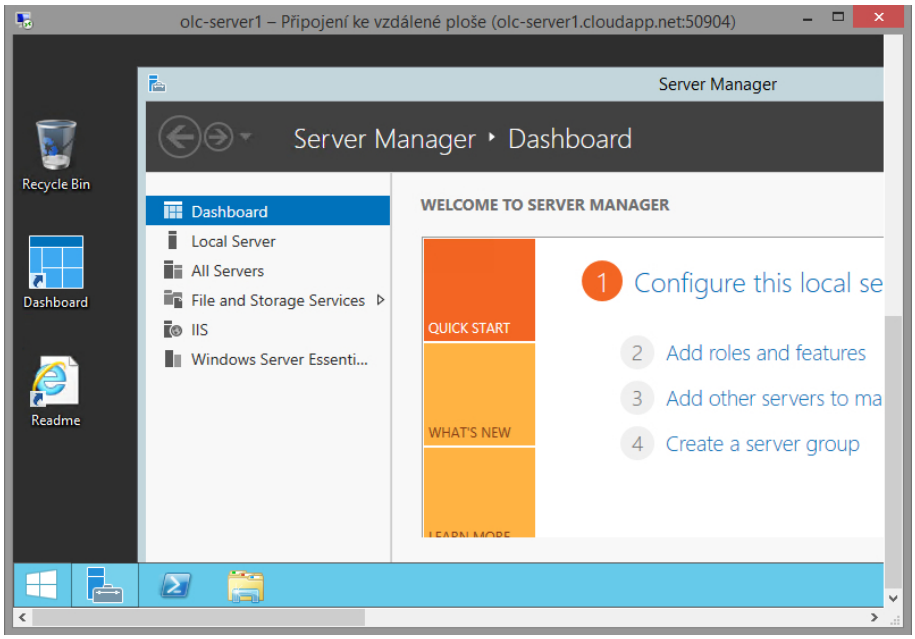


Obrázek 15: Připojení k virtuálnímu serveru[60]

[59] Vlastní zpracování

[60] Vlastní zpracování

Nabídne se nám ke stažení konfigurační soubor pro aplikaci Vzdálená plocha, soubor stačí otevřít a potvrdit nastavení zabezpečení (certifikát). Aplikace Vzdálená plocha nás vyzve k vložení přihlašovacích údajů, které jsme zadali při vytváření serveru. Po přihlášení můžeme vzdáleně server konfigurovat, například nastavit role (viz obrázek 16). Celý proces od vytvoření po přihlášení se ke spuštěnému serveru zabral jen pár minut.



Obrázek 16: Vzdálená plocha virtuálního serveru[61]

Podobným způsobem, jakým jsme vytvořili virtuální server s OS Windows Server, vytvoříme i virtuální server s OS Linux. Z galerie dostupných obrazů vybereme Ubuntu Server 12.04 LTS a zvolíme konfiguraci Small (A1) s jedním jádrem a 1,75 GB RAM. Tato konfigurace splňuje požadavky na instalaci poštovního serveru Kerio[62], který v současnosti firma sama provozuje, a je ideálním kandidátem na převedení do cloudu. Parametry zadané při vytváření serveru s OS Ubuntu Server jsou uvedeny na obrázku 17.

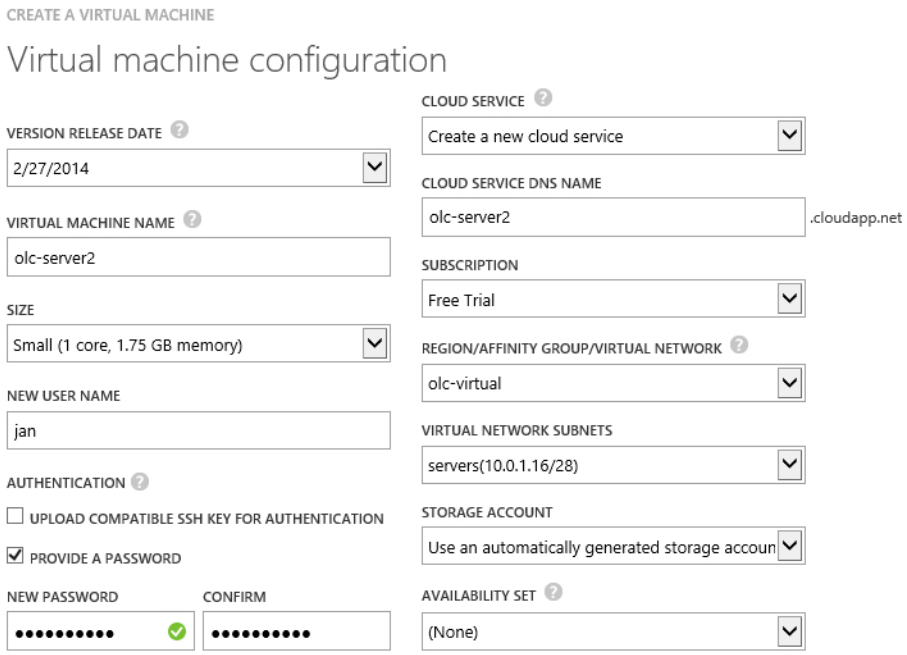
K virtuální serveru s operačním systémem Linux (Ubuntu Server) se přihlásíme pomocí zabezpečeného protokolu SSH. Pro připojení z OS Windows můžeme použít terminálovou aplikaci Putty (viz obrázek 18)[63]. V této aplikaci uvedeme pouze ad-

[61] Vlastní zpracování

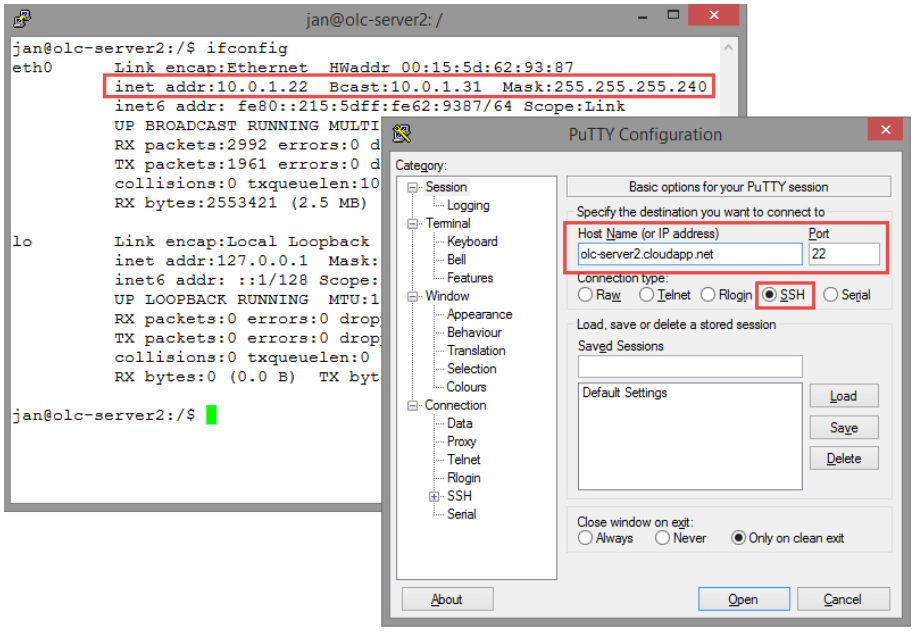
[62] Kerio Connect. [online], Dostupné z: http://www.kerio.cz/cz/connect/requirements

[63] Dostupné z: http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

resu hosta (*olc-server2.cloudapp.net*), číslo portu (*22*) a zvolíme typ připojení SSH. Adresa hosta odpovídá DNS adrese nastavené při vytváření virtuálního serveru (viz obrázek 17).



Obrázek 17: Parametry virtuálního serveru s OS Ubuntu Server[64]



Obrázek 18: Nastavení připojení k virtuálnímu serveru v programu Putty[65]

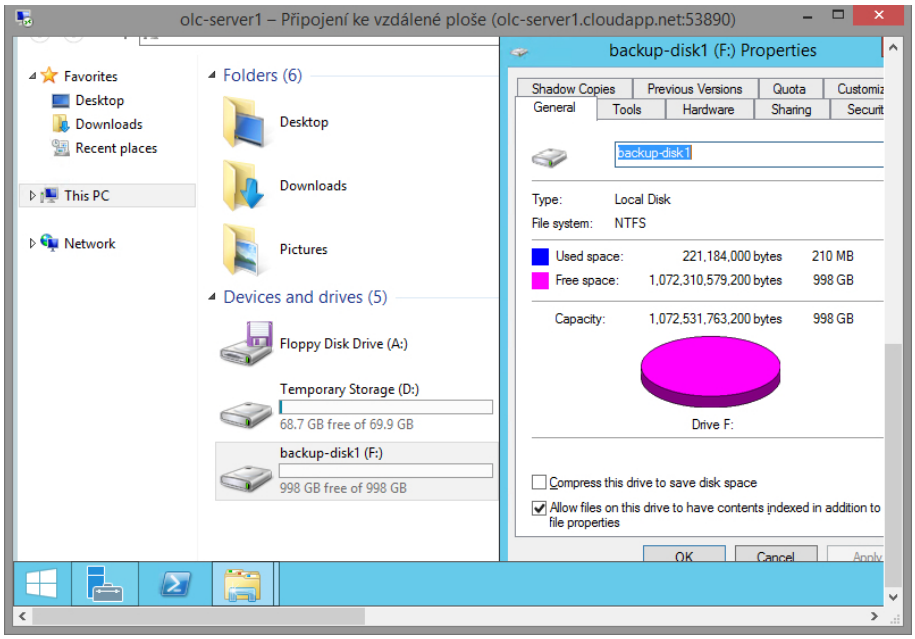
[64] Vlastní zpracování

[65] Vlastní zpracování

7.4 Datové úložiště

Windows Azure nabízí několik služeb pro práci s daty. Můžeme nastavit například úložiště pro automatické zálohování (služba Backup) nebo „klasické“ datové úložiště (služba Storage). Spolu s virtuálním serverem se vždy automaticky vytvoří soubor ve formátu VHD ve službě Storage. Ten reprezentuje pevný disk serveru, na kterém je operační systém nainstalován.

Nyní se vrátíme zpět do webové administrace služeb Windows Azure, kde k našemu serveru připojíme nové virtuální datové úložiště (soubor VHD) s kapacitou 1 TB. V rubrice *Virtual Machines* vybereme server *olc-server1*, u spodního okraje okna prohlížeče se zobrazí, nám již známý, panel s příkazy (viz obrázek 15). Nové datového úložiště vytvoříme a připojíme k serveru kliknutím na *Attach* → *Attach empty disk*. Následně zadáme požadovanou velikost v GB (1000 GB), disk si můžeme také pojmenovat (například *olc-server1-backup*). Nakonec nastavení potvrdíme a do pár minut máme k dispozici 1 TB pro ukládání dat. V systému Windows Server nový lokální disk připojíme ke stávajícím svazkům a naformátujeme.



Obrázek 19: Nový lokální disk připojený k serveru[66]

Na obrázku 19 je vidět nově vytvořený disk s kapacitou 1 TB připojený k serveru s OS Windows Server. Stejným způsobem připojíme virtuální disk k serveru

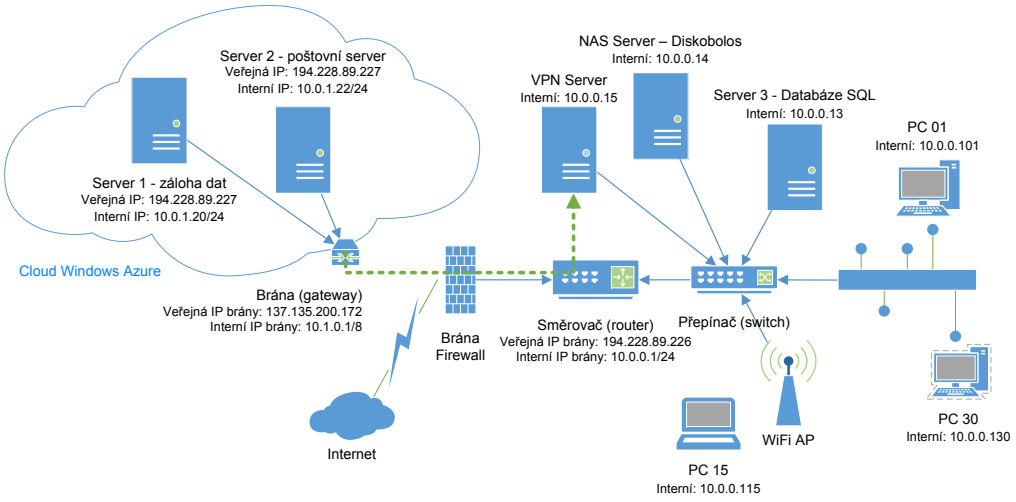
[66] Vlastní zpracování

s OS Ubuntu Server. Zvolíme kapacitu 300 GB, která by měla být dostačující pro 50 emailových schránek s kapacitou 5 GB.

7.5 Popis virtuální sítě

Pomocí postupů uvedených v předchozích kapitolách jsme vytvořili virtuální infrastrukturu umístěnou v prostředí cloudu. Zahrnuje virtuální síť, dva virtuální servery – jeden s OS Windows Server 2012 a druhý s Ubuntu Server 12.04. LTS. Virtuální síť je nakonfigurována pro připojení zařízení nacházejících se vně této sítě prostřednictvím zabezpečeného spojení VPN (point-to-site).

Veškerá nastavení a testování byla provedena pomocí jednoho notebooku (ThinkPad X220, OS Windows 8.1) s připojením k síti Internet přes linku VDSL. Pokud bychom měli fyzický přístup k firemní síti, tak bychom nastavili také VPN spojení site-to-site k propojení virtuální a fyzické sítě podniku. Schéma takto propojených sítí je na obrázku 20. Zahrnuje naše dva virtuální servery, jenž, při porovnání se schématem na obrázku 8, nahradily dva servery fyzické (poštovní a záložní server). VPN připojení je znázorněno přerušovanou zelenou linkou.



Obrázek 20: Schéma propojení virtuální sítě s fyzickou sítí v podniku[67]

[67] Vlastní zpracování

7.6 Náklady na provoz virtuální infrastruktury

V tabulce 2 jsou uvedeny celkové plánované náklady na provoz námi vytvořené infrastruktury v rámci služby Windows Azure. Předpokládá se, že oba virtuální servery budou spuštěny nepřetržitě, bude navázáno celodenní VPN spojení a využita bude celá disková kapacita. Dále je třeba započítat cenu za počet uskutečněných diskových operací (čtení / zápis) a za množství dat přenesených směrem „ven“ z našeho cloudu. Počet diskových transakcí je těžké odhadnout, ale cena za například 20 milionů transakcí je pouze $ 1. Podobně je to i s datovým přenosem. Odhad pro náš příklad je 15 GB (z toho 5 GB by připadalo na stahování poštovních zpráv). Prvních přenesených 5 GB v měsíci je vždy zdarma. Veškerá data přenesená směrem „do“ cloudu jsou zdarma.

Položka	Parametr	Cena za jednotku	Cena za měsíc
Server 1 (olc-server1)	1 x CPU, 1,75 GB RAM	$ 0,06 / hod	$ 44,64
Server 2 (olc-server2)	2 x CPU, 3,5 GB RAM	$ 0,12 / hod	$ 89,28
Datové úložiště (OS + data)	1 400 GB	$ 0,05 / GB / měsíc	$ 70,00
Operace na datovém úložišti	20 miliónů	$ 0,005 / 100 000	$ 1,00
Datový přenos z cloudu	15 GB (včetně 5 GB zdarma)	$ 0,12 / GB / měsíc	$ 1,20
VPN spojení	744 hod	$ 0,05 / hod	$ 38,00
Celkem			$ 244,12

Tabulka 2: Kalkulace měsíčních nákladů – Windows Azure[68]

Aby kalkulace odpovídala více realitě v popsaném podniku, budeme počítat s tím, že oba virtuální servery mají nainstalován operační systém Linux. Cena za virtuální server s OS Windows Server by byla vyšší, protože zahrnuje poplatek za poskytnutou licenci. Veškeré uvedené ceny jsou bez daně a v amerických dolarech. V tabulce 3 jsou pro srovnání uvedeny také ceny konkurenční služby Amazon AWS (parametry virtuálních serverů se mírně liší).

Měsíční náklady na naší modelovou infrastrukturu v rámci služby Windows Azure by činili $ 244,12 (4882,40 Kč při kurzu 20 Kč/ $ 1). Obdobný rozsah služeb od společnosti Amazon by vycházel měsíčně na $ 285,46 (5709,20 Kč). Ve srovnání s Windows Azure vychází tedy dráž. Cenový rozdíl je dán zejména vyšší hodinovou sazbou za provoz virtuálního serveru.

[68] Vlastní zpracování. Zdroj dat: Pricing Calculator. *Windows Azure* [online], Dostupné z: http://www.windowsazure.com/en-us/pricing/calculator/

Položka	Parametr	Cena za jednotku	Cena za měsíc
Server 1 (olc-server1)	1 x CPU, 1,75 GB RAM	$ 0,065 / hod	$ 48,36
Server 2 (olc-server2)	2 x CPU, 3,5 GB RAM	$ 0,171 / hod	$ 127,22
Datové úložiště (OS + data)	1 400 GB	$ 0,05 / GB / měsíc	$ 70,00
Operace na datovém úložišti	20 miliónů	$ 0,005 / 100 000	$ 1,00
Datový přenos z cloudu	15 GB	$ 0,112 / GB / měsíc	$ 1,68
VPN spojení	744 hod	$ 0,05 / hod	$ 37,20
Celkem			$ 285,46

Tabulka 3: Kalkulace měsíčních nákladů – Amazon AWS[69]

Uvedená celková kalkulace je pouze ilustrativní, neboť zahrnuje využití pouze základních služeb z nabídky Windows Azure. Cloud a princip účtování pay-as-you-go obecně nutí věnovat se více optimalizaci a zefektivnění. Například pro zálohování by bylo vhodnější použít službu Backup, kde je cena za uložený 1 GB dat v porovnání se službou Storage nižší.

[69] Vlastní zpracování. Zdroj dat: Pricing. *Amazon Web Services* [online], Dostupné z: http://aws.amazon.com/pricing/

8 Závěr

V kapitole 2 s názvem *Cloud computing* byl naplněn první dílčí cíl této práce. Uvedli jsme si zde několik definic cloud computingu, popsali jeho historický vývoj a definovali jeho hlavní charakteristické vlastnosti. Důležité je zmínit, že celá tato práce vychází z dnes široce přijímané definice cloud computingu popsané v dokumentu The NIST Definition of Cloud Computing.

Dalším dílčím cílem práce bylo popsat a porovnat modely služeb. Tento cíl byl naplněn v kapitolách 3 a 4. Kapitola 3 *Modely nasazení* se věnovala způsobům sdílení infrastruktury pro potřebu poskytování cloudových služeb z pohledu zákazníka. Rozlišeny byly čtyři modely nasazení – veřejný, soukromý, hybridní a komunitní cloud. V kapitole 4 *Modely služeb* byly zmíněny tři hlavní modely – infrastruktura jako služba (IaaS), platforma jako služba (PaaS) a software jako služba (SaaS), které rozlišují, jakou formou je cloud zákazníkovi nabízen. Pro správné pochopení principů technického řešení cloudových služeb a zejména modelu služby IaaS byl v podkapitole 4.1.2 věnován větší prostor technologii virtualizace. V kapitole 6 *Popis vybraných služeb* byly na konkrétních nabízených službách popsány principy modelu služby IaaS a PaaS.

Často skloňovaným pojmem ve spojitosti s cloud computingem je bezpečnost. Tato skutečnost byla důvodem pro stanovení dílčího cíle práce – analyzovat problematiku bezpečnosti a dostupnosti dat. Tento cíl byl naplněn v kapitole 5 *Bezpečnost*, kde byla pozornost věnována riziku úniku a ztráty dat a způsobům, jak mu předejít (šifrování dat, autorizace a autentizace uživatelů apod.). Dále byla řešena otázka dostupnosti, kde klíčovou roli hraje smlouva SLA, a na závěr byla zmíněna legislativní omezení, která se vztahují na ukládání a distribuci dat v cloudu.

V poslední kapitole práce 7 *Virtuální infrastruktura v podnikové síti* došlo k naplnění hlavního cíle práce, jenž spočíval ve vytvoření virtuální infrastruktury v prostředí cloudu za účelem demonstrovat, jak relativně jednoduché je cloud začít využívat. Na základě informací získaných během studijní praxe ve výrobním podniku v Olomouckém kraji, byl vytvořen modelový příklad virtuální infrastruktury, na němž byl daný cíl aplikován. Zahrnuté podkapitoly naplnily zbývající dva dílčí cíle – navrhnout metodologii vytvoření virtuální infrastruktury v cloudu a provést kalkulaci jejich provozních nákladů.

Před samotným vytvořením postupů, bylo potřeba si zvolit poskytovatele cloudových služeb. Volba padla na službu Windows Azure. Jak se ukázalo, je daná služba nakolik přehledně zpracovaná a jednoduchá, že díky tomu bylo možné vytvořit jak slovně, tak i graficky zpracované postupy, jenž by měly být čtenáři srozumitelné a sám by si podle nich mohl zkusit vytvořit vlastní virtuální infrastrukturu. Na tuto práci by se dalo dále navázat například tématem věnovaným tvorbě a optimalizaci aplikací v prostředí cloudu.

Aby byla ukázka dostupnosti cloudových služeb kompletní, byla provedena kalkulace měsíčních nákladů za provoz modelové infrastruktury. Pro porovnání byly doplněny také ceny konkurenční služby Amazon AWS. Měsíčně by provoz virtuální sítě se dvěma servery a téměř 1,5 TB dat vyšel na cca 4900 Kč. Pokud se někomu zdá měsíční cena vysoká, je třeba připomenout, že veškerá data uložená v cloudu jsou replikována, za celou dobu provozu nemusíme investovat ani jednu korunu do údržby hardwaru a každý měsíc ušetříme za elektrickou energii, kterou by jinak zařízení umístěna v naší firmě spotřebovala. Na téma porovnání nákladů za provoz vlastního IT a IT řešeného pomocí cloudu by mohla být napsána samostatná práce. Musela by jí ale předcházet důkladná analýza všech nákladů, které podnik na provoz vlastního IT vynaloží, sledovaných v delším časovém období.

Téma cloud computingu je tak rozsáhlé, že nebylo možné se v této práci věnovat všem jeho aspektům. Svět informačních technologií se vyvíjí velmi rychle a nepochybně za dobu, během které byla psána tato práce, byly představeny nové technologie a služby v oblasti cloud computingu.

Anotace

Jméno a příjmení autora:	Jan Jakob
Instituce:	Moravská vysoká škola Olomouc
Název práce v českém jazyce:	Cloud computing
Název práce v anglickém jazyce:	Cloud Computing
Vedoucí práce:	Mgr. Zdeňka Krišová
Počet stran:	56
Počet příloh:	0
Rok obhajoby:	2014
Klíčová slova v českém jazyce:	Cloud computing, virtualizace, infrastruktura jako služba, platforma jako služba, software jako služba, IaaS, PaaS, SaaS, Windows Azure
Klíčová slova v anglickém jazyce:	Cloud computing, virtualization, infrastructure as a service, platform as a service, software as a service, IaaS, PaaS, SaaS, Windows Azure

Tato bakalářská práce se věnuje tématu cloud computingu, novému způsobu pojetí informačních technologií, jenž se dostává do popředí zájmu firem. Cílem práce je vytvořit modelový příklad virtuální infrastruktury v prostředí cloudu pro středně velký podnik za účelem prezentovat dostupnost cloudových služeb.

This thesis is focused on the topic of the cloud computing, a new way of understanding information technology. The aim of this thesis is to create a model example of virtual infrastructure in the cloud environment for small and medium enterprises and to present the availability of cloud services.

Literatura

2013 Cloud Computing Survey. In: *North Bridge* [online]. 2013 [cit. 2014-03-22]. Dostupné z: http://www.northbridge.com/2013-cloud-computing-survey

Amazon EC2 Product Details. *Amazon Web Services* [online]. 2014 [cit. 2014-03-18]. Dostupné z: http://aws.amazon.com/ec2/details/

App Engine. *Google Cloud Platform* [online]. 2014 [cit. 2014-03-14]. Dostupné z: https://cloud.google.com/products/app-engine

CEARLEY, David W. a Kyle HILGENDORF. Cloud Computing Innovation Key Initiative Overview. In: *Technology Research — Gartner Inc.* [online]. 2011 [cit. 2014-03-01]. Dostupné z: https://www.gartner.com/doc/1745015/cloud-computing-innovation-key-initiative

Configure a Point-to-Site VPN using the Management Portal Wizard. In: *Windows Azure* [online]. 2014 [cit. 2014-03-20]. Dostupné z: http://msdn.microsoft.com/en-us/library/windowsazure/dn133792.aspx

KANARACUS, Chris. Salesforce.com to add three data centers in Europe. In: *PCWorld* [online]. 2014 [cit. 2014-03-20]. Dostupné z: http://www.pcworld.com/article/2103900/salesforcecom-to-add-three-data-centers-in-europe.html

KPMG INTERNATIONAL. *The cloud takes shape: Global cloud survey: the implementation challenge* [online]. 2013 [cit. 2014-03-20]. Dostupné z: https://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/cloud-service-providers-survey/Documents/the-cloud-takes-shapev2.pdf

MAHMOOD, Zaigham a Richard HILL. *Cloud computing for enterprise architectures*. New York: Springer-Verlag, 2011, 327 s. Computer communications and networks. ISBN 14-471-2236-4.

MARINESCU, Dan C. *Cloud computing: theory and practice*. First edition. Waltham: Elsevier, 2013, 416 s. ISBN 978-012-4046-276.

MELL, Peter a Timothy GRANCE. 800-145. *The NIST Definition of Cloud Computing*. Gaithersburg: National Institute of Standards and Technology, 2011. Dostupné z: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

MOHAMED, Arif. A history of cloud computing. In: *ComputerWeekly.com* [online]. 2009 [cit. 2014-03-16]. Dostupné z: http://www.computerweekly.com/feature/A-history-of-cloud-computing

Pricing. Amazon *Web Services* [online]. 2014 [cit. 2014-03-28]. Dostupné z: http://aws.amazon.com/pricing/

Pricing Calculator. *Windows Azure* [online]. 2014 [cit. 2014-03-28]. Dostupné z: http://www.windowsazure.com/en-us/pricing/calculator/

Ramnath K. Chellappa, PhD. *Goizueta Business School* [online]. 2014 [cit. 2014-03-17]. Dostupné z: http://www.bus.emory.edu/ram/

Security World: Čtvrtletník o informační bezpečnosti. Praha: IDG Czech Republic, 2012, č. 1. ISSN 1802-4505.

Security World: Čtvrtletník o informační bezpečnosti. Praha: IDG Czech Republic, 2013, č. 1. ISSN 1802-4505.

SOSINSKY, Barrie A. *Cloud Computing Bible*. Indianapolis: Wiley, 2011, 532 s. ISBN 978-0-470-90356-8.

STEDDUM, James. A Brief History of Cloud Computing. In: *SoftLayer Blog* [online]. 2013 [cit. 2014-03-17]. Dostupné z: http://blog.softlayer.com/2013/virtual-magic-the-cloud

The Cloud – Explained in a Picture. *The Solutions Architect* [online]. 2011 [cit. 2014-03-18]. Dostupné z: http://thesolutionsarchitect.net/the-cloud-explained-in-a-picture/

TULLOCH, Mitch. *Introducing Windows Azure For IT Professionals* [online]. Microsoft Press, 2013, [cit. 2014-03-16]. ISBN 978-073-5682-887. Dostupné z: http://aka.ms/682887pdf

Web Sites. *Windows Azure* [online]. 2014 [cit. 2014-03-15]. Dostupné z: https://www.windowsazure.com/en-us/services/web-sites/

What Is Google App Engine?. *Google Developers* [online]. 2014 [cit. 2014-03-15]. Dostupné z: https://developers.google.com/appengine/docs/whatisgoogleappengine

Seznam obrázků

Seznam tabulek