Univerzita Hradec Králové
Fakulta informatiky a managementu
Katedra informačních technologií

Návrh nasazení virtualizace a využití SharePoint pro datové úložiště

Bakalářská práce

Autor: Maroš Poliak
Studijní obor: Aplikovaná informatika

Vedoucí práce: Mgr. Josef Horálek, Ph.D.

Hradec Králové Duben 2020

Prohlášení

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně a s použitím uvedené literatury.

V Nehvizdech dne 27. 4. 2020 Maroš Poliak

Poděkování

Děkuji vedoucímu práce Mgr. Josefu Horálkovi, Ph.D za metodické a trpělivé vedení práce, za jeho čas a odborné rady, které přispěly k vypracování této práce.

Anotace

Předmětem bakalářské práce je popis nasazení cloudové platformy SharePoint v reálné společnosti. Teoretická část popisuje obecné aspekty virtualizace a její jednotlivé typy, dále obecný popis typů cloudových služeb, jejich vlastnosti a vzájemné porovnání včetně případů nasazení. Dále je popsána bezpečnost cloudových platforem na síťové úrovni, úrovni hosta a úložiště. Nakonec jsou diskutovány klady a zápory využívání cloudu a je popsána platforma Sharepoint. V praktické části jsou popsána očekávání reálné společnosti na datové uložiště, je ukázáno jak tyto požadavky plní SharePoint a jsou provedena měření dostupnosti. V závěru jsou diskutovány okolnosti, pro které je cloudová platforma vhodná.

Annotation

Title: Proposal for system virtualization and use of SharePoint as a data storage

The subject of this bachelor thesis is the description of the cloud platform implementation SharePoint in a real company. The theoretical part describes the general aspect of virtualization and its individual types, also a general description of the types of cloud services, their characteristics and their comparisons including implementation cases. Furthermore, it describes the cloud platform security on the network level, host level and storage. At the end we debate the pros and cons of cloud usage and we describe the SharePoint platform. The practical part describes the expectations of real a company of the data storage, shows how SharePoint meets these requirements and we conduct accessibility measures. At the end we discuss situations for which a cloud platform is suitable.

OBSAH

ÚVOD

V poslední dekádě prodělává IT obor revoluci. Velké a střední společnosti opouštějí model nasazení služeb uvnitř společnosti a přecházejí na modernější alternativy – cloudová řešení, microservices, různá API rozhraní. Tato práce mapuje nasazení cloudových služeb jako alternativy původních způsobů práce ve středně velké společnosti.

CÍL PRÁCE

Cílem této práce je popsat převod souborového systému a e-mailového serveru středně velké společnosti z on premise serverů do cloudového řešení – SharePoint. Nejprve jsou popsány základní charakteristiky cloudových řešení, dále požadované parametry řešení vlastního nasazení v reálné společnosti a výsledky nasazení. V závěru jsou diskutovány dopady nasazení.

TEORETICKÁ ČÁST

1 VIRTUALIZACE

Virtualizací se rozumí soubor metod a technik, které uživatelům umožňují v maximální možné míře nahradit stávající hardwarové a softwarové komponenty virtuálními, tzn. souběh několika virtuálních logických systémů v rámci jednoho fyzického, popřípadě fyzických systémů do jednoho virtuálního. Toto pomáhá vyřešit mnoho stávajících problémů včetně efektivity, bezpečnosti, vysoké dostupnosti, pružnosti, odolnosti vůči chybám, mobility a možnosti vytváření robustních systémů [1].

1.1 Vznik, důvod, obecný popis

Trendy ve virtualizaci se neustále mění. Virtualizace jako taková vznikala v druhé polovině 20. století. V 60. a 70. letech společnost IBM vyvinula tzv. Control Program/Camgridge Monitor System (CP/CMS), který se stal součástí VM/370. Tyto systémy dovolovaly uživatelům provozovat několik virtuálních prostředí izolovaně a nezávisle [2].

Kolem roku 1980 byla představena tzv. „Language-level virtualization“, která ve svém důsledku pozvedla aplikační úroveň a izolovanost. Java Virtual Machine (JVM), která byla představena v 90. letech 20. století, svůj produkt skvěle načasovala do období vzniku světové počítačové sítě (World Wide Web). JVM nabídla vývojářům možnost umístit bezpečným způsobem aktivní spustitelný obsah v rámci této sítě. Období největšího rozmachu Virtual Machine (VM) bylo přisuzováno stanfordskému výzkumnému projektu Disco, který nakonec vedl ke vzniku VMware. Ačkoli VM je nejtypičtější ukázkou virtualizace, existuje mnoho dalších příkladů, jakými jsou např. sdílení plochy, virtuální sítě, virtuální úložiště a podobně [1, 2].

V současnosti se virtualizace uplatňuje především v datových centrech, která nabízejí vysoký potenciál objemu služeb ruku v ruce s přijatelnou cenou. Primárním cílem v dnešní době je zvýšení bezpečnosti virtualizovaných prvků. Dále se virtualizace zaměřuje na personální využití v aplikacích, které se společnosti snaží stále více převádět ze stávajících forem do podoby cloudového řešení, např. balíček Microsoft Office [3].

1.2 Rozdělení

K vytvoření virtuálního prostředí je nutná kombinace hardwarových a softwarových prostředků, tyto kombinace nazýváme virtualizací platformy. Existují čtyři přístupy k provádění virtualizace:

- úplná
- paravirtualizace
- hardwarová
- softwarová

1.2.1 Úplná virtualizace

Úplná virtualizace je typická tím, že dochází k simulování (emulaci) celé platformy. Virtuální stroj simuluje významné množství hardwaru a umožňuje tak hostovanému systému běžet ve virtuálním prostředí tak, jako by byl provozován přímo na fyzickém hardwaru. Důležitým aspektem je v tomto případě sdílení prostředků. Hostovaný systém je provozován zcela izolovaně na virtuálním hardware a podstatný prvek, který zprostředkovává komunikaci mezi fyzickou a virtuální vrstvou, se nazývá hypervizor. Hypervizor zachytává činnost hostovaných systémů a přiděluje jim prostředky pro jejich fungování, alokuje paměť, čas a prioritu zpracování instrukcí, řídí přístup k fyzickým zařízením, např. síťovým prvkům, řadičům pevných disků, I/O zařízením a dalším. Tím, že mezi fyzickou vrstvou a virtuálním strojem existuje hypervizor, se stává virtuální systém zcela izolovaný a protože hypervizor zpracovává instrukce přijímané z virtuálního stroje a překládá je na fyzickou vrstvu a zpět předává virtuálnímu stroji instrukce zpracované, není schopen virtuální systém rozpoznat, že běží ve virtuální prostředí [4, 5].

Výhoda úplné virtualizace je spatřována v nezávislosti na platformě, virtuální systém je tedy možné bez problémů provozovat na zcela odlišných platformách, které nejsou kompatibilní s hostitelskou platformou. Jako příklad může sloužit provozování Linuxu na hostitelské platformě Windows. Mezi nevýhody patří náročná hardwarová režie systému plynoucí z nutného provozu hypervizoru.

1.2.2 Paravirtualizace

Paravirtualizace neboli částečná virtualizace je obdobou plné virtualizace, s tím rozdílem, že ne všechny hardwarové prostředky jsou virtualizovány. Virtuální prostředí je velmi podobné fyzickému, avšak některé instrukce jsou zpracovány přímo virtuálním strojem a tudíž nedochází ke zpracování všech instrukcí hypervizorem. V tomto případě hypervizor zpracovává pouze některé instrukce, přiděluje paměť a řídí systémové prostředky. Hostovaný stroj v případě

paravirtulizace není tedy plně izolovaný a může zjistit, že se nachází ve virtuálním prostředí. Jedním ze zásadních rozdílů je také nutnost úpravy zdrojového kódu hostovaného systému. Pro tento účel se nejvíce využívají otevřené systémy s dostupným zdrojovým kódem, tzv. open source systémy. U systémů, kde obvykle není zdrojový kód k dispozici, je možné virtualizovat alespoň některé komponenty, čehož lze dosáhnout úpravou ovladačů, proto se paravirtualizace využívá často v případě periferií, např. síťové karty apod. [5].

Výhoda paravirtualizace tkví v přenechání určité zátěže hostovanému systému, a tím pádem vede ke zvýšení výkonu a zároveň ke snížení hardwarové náročnosti hostitelského stroje a omezení zátěže hypervizoru, čímž se celý systém stává efektivnějším. Nevýhodou je nutnost úpravy zdrojových kódů hostovaných systémů pro potřeby paravirtualizace, a špatná přenositelnost a migrace systémů v rámci různých platforem.

1.2.3 Hardwarová virtualizace

Na rozdíl od předchozích dvou metod virtualizace, je hardwarová virtualizace nativně podporována hardwarovými komponentami např. procesorem, pamětí atd. Určitou část instrukcí zpracovává nativně příslušná hardwarová komponenta, čímž významně usnadňuje práci hypervizoru. Tímto se hardwarová virtualizace stává velmi efektivní a umožňuje nasazení většího množství virtuálních strojů (např. serverů) v rámci jednoho hostitelského stroje. Historicky první nativně hardwarově virtualizovanou platformou byl, již v úvodu zmiňovaný, počítač VM/370 vyrobený společností IBM v 70. letech 20. století. Hardwarová virtualizace přináší nesporné výhody, čehož si byli vědomi i výrobci hardwaru a začali integrovat tuto nativní podporu do svých produktů. Například v případě společnosti Intel byla virtualizace implementována poprvé do řady procesorů x64, přičemž se tato technologie nazývala VT-x. Vzápětí integrovala nativní podporu i společnost AMD do svých procesorů, řešení se nazývalo AMD-V [5].

V následujícím textu bude blíže popsána virtualizace procesoru, paměti a I/O zařízení.

1.2.3.1 Virtualizace procesoru

V případě podpory virtualizace procesoru se provádějí operace přímo na procesoru, což s sebou přináší zvýšení výkonu systému. Virtualizovaný stroj využívá přímo instrukční sady procesoru a systémových registrů. Aby toto bylo možné, je nezbytně nutné, aby samotná podpora byla integrována přímo v procesoru. Společnosti jako Intel a AMD tuto technologii zavedly, jak již je uvedeno výše. V této technologii je použita nová úroveň oprávnění tzv. Ring -1, kterou používá hypervizor. Ringu -1 je přiřazen nejvyšší stupeň ochrany a oprávnění, což umožňuje hostovanému systému běžet na stejné úrovni ochrany jako nativnímu. V souvislosti s tím musely být integrovány nové instrukce instrukční sady procesoru [6].

1.2.3.2 Virtualizace paměti

Paměť instalovanou ve fyzickém prostředí spravuje operační systém. Virtualizací paměti dochází k vytvoření virtuální paměti, která je běžně implementována pomocí stránkovací paměti spolu se stránkováním například na disk. Virtuální paměť může být z tohoto důvodu větší, než je kapacita paměti v systému. Procesor přistupující k paměti rozlišuje mezi virtuálními a fyzickými adresami paměti, přičemž samotný převod mezi těmito adresami je zajišťován přímo procesorem. K tomuto účelu musí být v procesoru integrována hardwarová podpora. Hardwarová podpora virtualizace paměti je daleko méně náročná na práci hypervizoru, který tak nemusí zpracovávat veškeré paměťové požadavky [7].

1.2.3.3 Virtualizace I/O zařízení

I/O zařízení (vstupně-výstupní zařízení) mohou být také virtualizována. K virtualizaci je nutná hardwarová podpora chipsetu, který zajistí přístup konkrétního hardwaru a jeho propojení a komunikaci s virtuálním strojem. Dále je zapotřebí podpora konkrétního I/O zařízení tak, aby byla umožněna funkčnost s více virtuálními stroji. Ve virtualizovaném systému jsou pak pro tato zařízení použity standardní ovladače. Výkon takto připojených zařízení je téměř shodný s výkonem přímého připojení [6].

1.2.4 Softwarová virtualizace

Charakteristické pro softwarovou virtualizaci je využití aplikací třetích stran, například produkty společností Microsoft (Hyper-V), VMware, Citrix apod. Tyto produkty podporují virtualizaci kompletních systémů např. Windows Server. Na jednom hostitelském systému je možno současně provozovat několik nezávislých virtuálních strojů v závislosti na výkonu hostitelského hardwaru. Cílem je nabídnout uživateli možnost práce a testování aplikací na několika různých platformách bez nutnosti instalace příslušného softwarového a hardwarového vybavení [8].

Velkou předností tohoto typu virtualizace je jednoduchá implementace, údržba a snadná práce s takto vytvořeným systémem. Nejširší využití nachází tato technologie především v datových centrech, kde vede k významné úspoře místa a k možnosti velmi rychlého a pružného nasazení. Jednoduchost údržby spočívá ve správě těchto systémů, kdy správce má na starosti údržbu pouze minimálního množství hardwaru. Administraci instalovaných systémů je možno provádět centralizovaně s podporou příslušné aplikace, např. v případě Microsoftu se může jednat o System Center Operations Manager (SCOM). Virtuální stroj je možno bezproblémově přesunout, jednoduše ho zálohovat pouhým zkopírováním příslušného souboru. Většina nástrojů

také umožňuje replikaci virtuálního stroje v reálném čase. Další výhodou je bezesporu finanční úspora při pořizování hardwaru a provozu hostitelského systému a energetická úspora.

1.3 Platformy pro virtualizaci

Dříve se využívala technologie přístupu více uživatelů pomocí terminálových připojení k hlavnímu serveru, což bylo velmi finančně nákladné a ne každý uživatel potřeboval ve stejnou chvíli využívat plně kapacitu a výkon, který terminálový server poskytoval. Významným omezením tohoto řešení bylo použití instalovaného systému na serveru. Oproti tomu v dnešní době umožňují různé virtualizační platformy souběžně provozovat jeden či více operačních systémů na jednom fyzickém hardwaru.

2 CLOUD

2.1 Obecný popis

Myšlenka toho, co se později stalo cloudem, vznikla na poli IT poměrně dávno. Počítačový výzkumník John McCarthy již v roce 1961 mluvil o možnosti, že se počítače a výpočetní technologie stanou „veřejnou službou“ podobně jako veřejná telefonní síť. Veřejnost začala takové veřejné služby využívat v 90. letech 20. století v podobě prvních vyhledávačů, jakými byly Yahoo! a Google, e-mailových poskytovatelů (Hotmal a Gmail) a otevřených platforem pro publikování obsahu (MySpace, Facebook a YouTube) a dalších sociálních médií (Twitter, LinkedIn). I když šlo o služby zaměřené na koncového zákazníka, hrály důležitou roli pro budoucí cloud, protože zpopularizovaly a validovaly základní myšlenky, jak jsou využívány i dnes [9].

Zpočátku se termín „Cloud“ nebo „Network Cloud“ začal používat na začátku 90. let 20. století v souvislosti s transferem dat do různých veřejných nebo částečně veřejných sítí. Šlo tedy primárně o označení přenosu dat z lokálních (soukromých) sítí do širších síťových celků (wide area network) a odtud do koncového end-pointu. Toto je důležité, protože správci sítě tento termín stále v tomto významu používají a dají se označit za „early adopters“ cloudu [9]. Moderní výraz cloud vstoupil na scénu v roce 2006, když Amazon začal nabízet službu Elastic Compute Cloud (EC2), na které si mohli zákazníci pronajmout výpočetní sílu a provozovat na ní své firemní aplikace. O tři roky později přišla společnost Google Apps se službou Google App Engine [9].

Nyní k samotné definici termínu „cloud“. Konzultační a výzkumná společnost Gartner označuje cloud jako „styl výpočtu, ve kterém jsou škálovatelné a elastické schopnosti založené na IT poskytovány jako služby externím zákazníkům pomocí technologie Internet“. Forrester Research ji podobně definoval jako „standardizovanou IT schopnost (service, software nebo

infrastruktura) poskytovanou pomocí Internetu jako pay-per-use, self-service služba“ [9]. Existují i méně technické definice, např. termín cloud popisuje entitu, která je mimo naši možnost mít s ní fyzický kontakt [10].

Standardem se stala definice Národního Institutu Standardů a Technologie (NIST): „Cloud computing je model umožňující všudypřítomný, výhodný přístup ke sdílenému poolu nastavitelných výpočetních zdrojů (sítě, servery, uložiště, aplikace a služby) na vyžádání, který je promptně zřízen a vyžaduje jen minimální údržbu a interakci s poskytovatelem. Cloud je složen z pěti základních vlastností, tří modelů služeb a čtyř deployment modelů“ [11].

Základní charakteristiky cloudu podle NIST jsou:

- **samostatné zřízení zdrojů na vyžádání** – zákazník si může jednostranně zřídit u poskytovatele výpočetní schopnost (jako je výpočetní čas na serveru nebo místo v uložišti) bez nutnosti sociální interakce na straně poskytovatele
- **široká síťová dostupnost** – schopnosti cloudu jsou přístupné přes síť pomocí standartních kanálů, a tak jsou dostupné přes různorodou směs klientů (smartphony, tablety, počítače)
- **poolování zdrojů** – zdroje poskytovatele cloudu tvoří jeden pool, který slouží více zákazníkům (multi-tenant model), a tyto zdroje jsou dynamicky přidělovány zákazníkům podle jejich potřeby; zákazník běžně nemá kontrolu nad tím, kde se zdroje nacházejí, ale může požadovat od poskytovatele lokalitu na vyšší úrovni abstrakce (stát, příp. i datové centrum); mezi takto poolované zdroje patří uložiště, výpočetní síla, paměť a připojení k internetu
- **rychlá elasticita** – zdroje a vlastnosti mohou být rychle poskytnuty i uvolněny, v některých případech automaticky, čímž je umožněno navenek rapidní škálování, ale systém se zároveň udržuje racionální; pro zákazníka se zdroje mohou jevit jako neomezené
- **měření služeb** – využití zdrojů je monitorováno, ovládáno a reportováno, což poskytuje transparentnost, a to jak poskytovateli cloudu, tak i zákazníkovi [11].

2.2 Rozdělení podle deploymentu

Definice NIST obsahuje tyto čtyři typy cloudů podle jejich umístění (deploymentu):

- **privátní** – infrastruktura cloudu je poskytována pro exkluzivní použití jedné organizaci, která zastupuje více uživatelů (business jednotek). Může být vlastněna, ovládána a řízena touto organizací, třetí osobou nebo kombinací obou a může být zřízena na území vlastněném organizací (on premises) nebo mimo ně (off premises)

- **komunitní** – infrastruktura cloudu je zřízena pro exkluzivní použití specifickou komunitou zákazníků z organizací, které mají sdílené potřeby (mise, bezpečnostní požadavky, politika a compliance). Může být vlastněna, ovládána a řízena jednou nebo vícero těmito organizacemi, třetí osobou nebo kombinací a může být on premises nebo off premises
- **veřejný** – infrastruktura cloudu je zřízena pro použití širokou veřejností. Může ji vlastnit, ovládat a řídit obchodní, vzdělávací nebo státní organizace nebo jejich kombinace. Je zřízená v infrastruktuře poskytovatele cloudu
- **hybridní** – infrastruktura cloudu je složena ze dvou nebo více oddělených cloudových infrastruktur uvedených výše, které jsou na sobě závislé určitou standardizovanou technologií, která umožňuje přesouvat data a aplikace. Příkladem může být. cloud bursting, kdy je cloud používán v privátním režimu, ale v případě, že dojde k dočasnému zvýšení využití tohoto cloudu, jsou data replikována a nabízena i z veřejného cloudu (jen po omezenou dobu a jen na tuto dobu jsou hrazeny poplatky provozovateli veřejného cloudu) [11].

2.3 Cloud jako služba, využití

Existují tři modely poskytování cloudových služeb: **Infrastructure as a Service (IaaS)**, **Platform as a Service (PaaS)** a **Software as a Service (SaaS)**. Každý z těchto tří modelů poskytuje jistou úroveň abstrakce, která snižuje úsilí, které by jinak musel vynaložit konzument služby na zřízení a udržování služby. V tradičním způsobu provozování hardwaru a softwaru přímo v datovém centru musí IT tým postavit a spravovat doslova vše, ať už jde o vlastní řešení postavené na zelené louce nebo provozování „krabicových“ řešení jiných firem. Je nutné tedy instalovat servery, operační systémy, software, zajistit správnou úroveň ochrany, patchování a mnoho dalších činností. Cloudová řešení poskytují různé úrovně automatizace, které jejich zákazníkům umožňují soustředit se na core business místo správy infrastruktury [12].

2.3.1 IaaS

Uživateli cloudu je poskytována možnost zřídit uložiště, sítě a další základní výpočetní zdroje, na které může umístit software a provozovat ho na nich, včetně operačních systémů a aplikací. Zákazník neovládá ani nespravuje infrastrukturu, ale má kontrolu nad operačním systémem, uložišti a aplikacemi, a případně také omezenou kontrolu nad některými síťovými prvky [11].

S použitím IaaS je spousta činností spojená s provozováním fyzického datového centra abstrahována a je uživateli přístupná jako kolekce služeb, která je přístupná a konfirgurovatelná

např. přes webové rozhraní. Vývojáři stále musí vymýšlet a nakódovat celé programové řešení a administrátoři musí instalovat, spravovat a patchovat programy třetích stran, ale už jako taková neexistuje žádná infrastruktura, kterou by bylo potřeba zákazníkem spravovat a řídit. Tím pádem odpadají i dlouhé objednací a dodací lhůty spojené s pořizováním nového hardwaru, které by potom zákazník musel přebírat, rozbalovat, sestavovat, instalovat a umisťovat do datového centra. S IaaP může být nová hardwarová kapacita zřízena během několika málo minut zavoláním API nebo vyžádáním z webové konzole. Podobně jako u takových komodit, jakými jsou voda a elektřina, je používání IaaS měřeno a za jeho využívání jsou účtovány poplatky. Ovšem, pokud tuto službu momentálně zákazník nevyužívá, nic ho nestojí. Tímto způsobem zpřístupňuje IaaS svým zákazníkům virtuální datacentrum a tím jim umožňuje soustředit se primárně na jejich hlavní obor podnikání a vyvíjení a údržbu programů spojených s tímto podnikáním, a přitom se jen minimálně soustředit na správu datového centra a infrastruktury [12].

Příklady využití IaaS:

- ✓ Společnost zaměřená na vývoj může vytvářet testovací prostředí, které kopíruje deployment u klienta, ale je v provozu pouze na testování. Odpadá zdlouhavé pořizování a nastavování zařízení, navíc společnost platí pouze za opravdové využití.
- ✓ Pojišťovací společnost potřebuje přepočítat čtvrtletní účetní uzávěrku. Tato úloha vyžaduje velké množství prostředků a času (v násobcích běžného provozu), ale přepočet je ve srovnání s celým rokem krátkodobá záležitost, proto se společnost raději rozhodne používat IaaS, než by nakupovala další hardware, který by zůstal většinu roku nevyužitý [13].

2.3.2 PaaS

Zákazník dostává možnost umístit do cloudové infrastruktury vlastní vytvořené aplikace nebo aplikace získané od třetích stran. Tyto aplikace jsou vytvořeny s pomocí programovacích jazyků, knihoven, služeb a nástrojů nasdílených poskytovatelem cloudu. Zákazník neovládá ani nespravuje cloudovou infrastrukturu, jako jsou sítě, servery, operační systémy nebo uložiště, ale má kontrolu nad umístěnými aplikacemi a případně nastavením prostředí, ve kterém běží [11].

PaaS je další úrovní po IaaS. Význam IaaS pro infrastrukturu je roven významu PaaS pro aplikace. PaaS je vybudovaná na základech IaaS a abstrahuje valnou část funkcionalit standardních aplikací jako službu. Vývojáři vysoce škálovatelných systémů musí často pracovat se zpracováním cachování, asynchronních zpráv a škálování databází. PaaS řešení nabízejí hotovou implementaci těchto funkcí jako služeb pro programátory, kteří se pak mohou soustředit už jen na business

logiku. PaaS je zcela k dispozici přes internet a vývojáři mají k dispozici specifickou sadu nástrojů k programování. Tímto způsobem jsou vývojáři omezeni, protože nemohou využívat jiné nástroje a zároveň se vzdávají i kontroly nad low-level aspekty programování, jako jsou správa paměti, alokace paměti a konfigurace stacku (počet vláken, velikost cache, úroveň patche systému). Kontrolu nad těmito aspekty má poskytovatel cloudu a obvykle ovlivňuje i množství výpočetní síly, ke kterému má zákazník přístup, aby zajistil rovnoměrnou škálovatelnost platformy pro jednotlivé zákazníky.

Součástí nabídky PaaS mohou být různé vývojářské stacky (např. v Amazon Web Services). Běžně jsou nabízeny integrace s produkty třetích stran, označované zpravidla jako add-ony, pluginy nebo rozšíření, které zahrnují databáze, nástroje pro logování, monitoring, cachování, vyhledávání, správu zabezpečení, e-mailů a plateb. Výběrem z většího množství integrací třetích stran dochází k zajištění odolnosti proti výpadkům, zvýšení rychlosti, zlepšení SLA, to vše bez nutnosti spravování technologií těchto třetích stran. Tímto způsobem mohou vývojáři rychle sestavit řešení čistě na základě volání API třetích stran bez nutnosti objednávání, nákupu a zprovozňování jednotlivých nástrojů. Ve srovnání s IaaS a SaaS je PaaS považováno analytiky za nejméně vyspělý model služeb, od kterého se ovšem očekává největší rozvoj [12].

2.3.3 SaaS

Nejvyšší úrovní služeb je SaaS, což je kompletní aplikace nabízená zákazníkovi jako služba. Zákazník musí pouze aplikaci nakonfigurovat a spravovat uživatele. Poskytovatel cloudu se stará o veškerou infrastrukturu, aplikační logiku, nasazení a veškeré detaily související s dostupností a poskytováním produktu nebo služby. Nejčastějším příkladem použití SaaS jsou systémy pro správu vztahů se zákazníky (Customer Relationship Management, CRM), plánování organizačních zdrojů (Enterprise Resource Planning, ERP), výplatní pásky, účetnictví, e-shopy a další běžný firemní software. SaaS systémy jsou běžné pro funkčnosti, které nepředstavují hlavní činnost organizace. Proto organizace tyto služby využívají, protože raději zaplatí pravidelný poplatek za používání služby, místo toho aby platily za provozování infrastruktury, údržbu, a lidské zdroje pro správu [12].

Zákazník získává možnost používat aplikace poskytovatele, které běží na cloudové infrastruktuře. Aplikace jsou k dispozici z různých zařízení klienta, buď jako tenký klient (např. webová e-mailová schránka), nebo jako interface programu. Zákazník neovládá ani nespravuje infrastrukturu cloudu (servery, sítě, uložiště, operační systém ani aplikace) s výjimkou nastavení specifického pro jednotlivé uživatele [11]. Vazby mezi modelem služby, jeho komponentami a odpovědnostmi jsou uvedeny v tabulce 1.

Tabulka 1: Vazby mezi poskytovatelem a zákazníkem [12]

<table>
<tr><th colspan="3">Model Služby</th><th>Cloud Stack</th><th colspan="2">Komponenty Stacku</th><th colspan="3">Zodpovědná strana</th></tr>
<tr><td rowspan="3"></td><td rowspan="5"></td><td rowspan="8"></td><td rowspan="3">Uživatel</td><td colspan="2">Přihlašování</td><td rowspan="3">Zákazník</td><td rowspan="3">Zákazník</td><td rowspan="3">Zákazník</td></tr>
<tr><td colspan="2">Registrace</td></tr>
<tr><td colspan="2">Administrace</td></tr>
<tr><td rowspan="8">SaaS</td><td rowspan="3">Aplikace</td><td>Autentizace</td><td>Autorizace</td><td rowspan="6"></td><td rowspan="3"></td><td rowspan="8">Poskytovatel Cloudu</td></tr>
<tr><td>UI</td><td>Transakce</td></tr>
<tr><td>Reporty</td><td>Dashboard</td></tr>
<tr><td rowspan="5">PaaS</td><td rowspan="3">Aplikační stack</td><td>OS</td><td>Programovací jazyk</td><td rowspan="5">Poskytovatel Cloudu</td></tr>
<tr><td>App Server</td><td>Middleware</td></tr>
<tr><td>Databáze</td><td>Monitorování</td></tr>
<tr><td rowspan="4">IaaS</td><td rowspan="4">Infrastruktura</td><td>Datacentrum</td><td>Uložiště</td><td rowspan="4">Poskytovatel Cloudu</td></tr>
<tr><td>Servery</td><td>Firewall</td></tr>
<tr><td rowspan="2">Síť</td><td rowspan="2">Load Balancer</td></tr>
<tr><td></td></tr>
</table>

2.3.4 XaaS

I když IaaS, PaaS a SaaS jsou páteří všech moderních cloudových řešení, došlo k prudkému rozmachu dalších specifických cloudových služeb, souhrnně označovaných jako XaaS. Existují tak třeba služby uložiště StaaS, Storage as a Service, například Amazon S3 [14], zálohovací služby BaaS, Back-up as a Service [15] a Sroczkowski [16] uvádí výčet dalších alternativ, které cloud nabízí jako službu: analýzy (Analytics), přihlašování (Authentication), komunikační kanály (Communications), výpočetní sílu (Computing), poskytování obsahu (Content), ukládání energie (Energy Storage), odhalování podvodů (Fraud), hardware, IT, správu a poskytování znalostí (Knowledge), databáze (MongoDB nebo Oracle), monitorování (Monitoring), platby (Payments), kontrolu kvality (Quality) a testování (Testing), obnovení (Recovery), vyhledávání (Search), zabezpečení (Security) a dokonce i Games WiFi, anebo celý Business.

2.4 Bezpečnost

Bezpečnost cloudového řešení je jedním z největších rizik, o které se uživatelé cloudových služeb zajímají. Běžní provozovatelé datových center nabízejí pouze připojení k síti a fyzické místo pro zařízení, a otázka provozování serverů, nastavení zabezpečení, firewallů, content filterů, intrusion detection systémů apod. zůstává čistě v rukou zákazníka. Zákazník musí všechny tyto aspekty vyřešit sám, ale zůstává mu absolutní přehled a kontrola nad architekturou systému, bezpečnostním designem a samotnými daty – až do té míry, že servery mohou mít i fyzickou ochranu (kovové mříže, zámky, šifrované disky) [10].

V kontextu cloudu je architektura, resource management a struktura zdrojů v backendu pro uživatele neviditelná, nedosažitelná. Ovšem tato nedosažitelnost znamená, že uživatelé cloudových služeb mohou mít přirozeně starost o úroveň zabezpečení. Na tomto místě lze použít analogii mezi ochranou dat v IT oblastí bankovnictví. V bankovní oblasti zákazník vkládá bankovky nebo převádí peněžní prostředky na účet vedený u konkrétní banky a rovněž nemá již nadále absolutní fyzickou kontrolu nad svými zdroji – zde jsou zdroje představovány penězi. Zákazník ovšem spoléhá na IT zabezpečení a profesní a finanční integritu bankovního domu, který se zavazuje převzít dohled nad nyní virtualizovanými zdroji. V podobném duchu se dá předpokládat, že uživatelé budou mít ke cloudovým řešením stále větší a větší důvěru, a budou považovat výhody spojené s užíváním virtuálních datových uložišť za adekvátní ve srovnání s riziky zbavení se absolutní kontroly nad architekturou a bezpečností. Tento přerod vyžaduje svěřování dat převážně odzkoušeným a důvěryhodným provozovatelům cloudových řešení [10].

Rozvoj zabezpečení cloudu a jeho standardizace se zvyšuje s tím, jak roste uživatelská základna, kdy je využíván efekt více zákazníků poptávajících služby u jednoho poskytovatele

cloudu, který může, bez většího dopadu na zákazníka, rozvíjet své řešení tak, aby poskytovalo aktuální zabezpečení všem zákazníkům. V tomto ohledu je potřeba zmínit rozdíl mezi komoditními a enterprise cloudy. Komoditní cloudová řešení mají za úkol primárně snižovat cenu služby pro koncového zákazníka, „komoditizovat“ infrastrukturu, kterou ve výsledku sdílí více uživatelů najednou. Komoditní řešení v mnoha přídech nejsou navržena, aby splňovala vysoké nároky na dostupnost, bezpečnost a compliance vyžadovanou velkými společnostmi, obzvláště spadají-li tyto pod nějakou formu regulace. Enterprise řešení, na druhou stranu, jsou od začátku koncipována tak, aby pro velké hráče na trhu byla zaručena vysoká dostupnost, service level agreement (SLA) a bezpečností a regulatorní požadavky. Enterprise řešení i proto bývají zpravidla výrazně dražší než komoditní řešení [12].

Zabezpečení dat se realizuje na více úrovních – síťová úroveň, úroveň hosta a aplikací [17].

2.4.1 Síťová úroveň

Data, uložená původně v soukromé síti, se v cloudu stávají přístupnými přes internet a přes sdílenou síť poskytovatele cloudu. To přirozeně vede k většímu riziku zneužití dat a navíc prakticky neexistuje možnost, jak auditovat síť poskytovatele cloudu (ať už po případném případu ztráty dat nebo on-line).

Obecně ze síťového úhlu pohledu existují tři výrazné rizikové faktory:

- **zabezpečení důvěrnosti a integrity dat při přenosu po síti** – zde je základním kamenem používání protokolu HTTPS (místo HTTP), který sám o sobě může pomoci s řešením jiných problémů na straně poskytovatele. I když případné problémy s přístupností k datům a možností je změnit v tranzitu by měly i tak být řešeny na úrovni poskytovatele cloudu, HTTPS může být další možností obrany dat
- **zabezpečení správné úrovně oprávnění** – jedním z prakticky známých případů, kdy zájmy poskytovatele mohou jít proti zájmům uživatele cloudu, je přidělování IP adres. IP adresy jsou pro poskytovatele omezeným zdrojem, takže je zpravidla hned po jejich uvolnění přiděluje jinému klientovi. To v některých případech může vést až k situaci, kdy dosud nezměněné záznamy DNS odkazují na cizí data
- **zaručení dostupnosti dat ve veřejné části cloudu** – přístupnost zdrojů může být omezena buď chybami na straně konfigurace, kdy obsah jednoduše není z internetu dostupný, nebo může být omezován nekalými živly. I v laické společnosti jsou dnes nechvalně známy DOS (Denial of Service) a DDOS (Distributed Denial of Service) útoky, kterými vnější činitel

může omezit dostupnost služby na internetu. Podobných útoků je přitom větší množství, např. DNS útoky, BGP prefix hijacking a podobně.

2.4.2 Úroveň hosta a aplikací

Jak se dá předpokládat, úroveň zabezpečení aplikací se různí podle typu cloudu:

- **IaaS** – protože zákazník si vytváří vlastní prostředí, je i zabezpečení jednotlivých součástí (stacku) i samotných aplikací v jeho režii. Na administrátora a vývojáře tak přechází nejen spolehlivost a zabezpečení aplikace, ale i úkony spojené s identity management, přihlašováním a podobně. Pro IaaS jsou pak aplikovatelné standardní pokyny pro zabezpečení virtuálních strojů a kódu
- **PaaS** – zde je možné zabezpečení rozdělit do dvou úrovní
  - zabezpečení samotné platformy
  - zabezpečení zákaznických aplikací, více méně odpovídá komentářům pro IaaS
- **SaaS** – zabezpečení, stejně jako ostatní zodpovědnosti, by měly být zcela v rukou poskytovatele cloudu

Pro zabezpečení hostů u PaaS a SaaS platí, že host je pro zákazníka neviditelný, zákazník zpravidla nemůže ani získat informace o fyzickém umístění a nastavení stroje (obojí se navíc může v čase rychle měnit).

2.4.3 Zabezpečení uložiště

Zabezpečení uložiště, ve kterém jsou v cloudu uložena klientská data, je realizováno pomocí zásad důvěrnosti, integrity a dostupnosti.

2.4.3.1 Důvěrnost

Základní otázkou většiny zákazníků vůči cloudu jistě bude, jak jsou jejich data v cloudu chráněna proti neoprávněnému přístupu. Protože programátoři jsou kreativní, existují různé přístupy – indexování, maskování, redaktování a zalamování – ovšem tyto přístupy nejsou v současnosti standardizovány, tudíž postrádají požadovaný punc oficiality. Jediný standardizovaný a uznávaný přístup je šifrování dat přímo v uložišti. V tomto ohledu se poskytovatelé cloudu opět různí. Někteří neposkytují vůbec žádné šifrování dat v cloudu, jiní ano. I pokud poskytovatel šifrování nabízí, je potřeba řešit, jaké algoritmy jsou využívány. Znovu platí, že využívány by měly být pouze šifrovací algoritmy schválené oficiální autoritou, tedy vlastnoručně vyrobené nebo "tajné" algoritmy musí byt za všech okolností zavrženy. Pro šifrování se z praktických důvodů doporučují symetrické šifry.

Pokud už zákazník řeší šifrování (na straně cloudu, nebo, v nejhorším případě, před nahráním dat do cloudu, pokud poskytovatel šifrování v cloudu nenabízí), vyvstává logicky otázka správy hesel. Zákazník by neměl, ve vlastním zájmu, nechávat otázku správy hesel na poskytovateli cloudu, ale měl by se správy hesel proaktivně chopit sám. Nelze ovšem podcenit, že správa hesel je komplexní úkon a vyžaduje kvalifikované zdroje. Jako minimum pro vlastní správu hesel se doporučuje publikace NIST 800-57 :"Část první: Obecně", "Část druhá: Best practices pro správu klíčů organizace" a "Část třetí: Doporučení pro správu klíčů pro specifické použití".

2.4.3.2 Integrita

Zatímco při přenosu dat mezi uživatelem a cloudem lze zajistit integritu dat tradičními způsoby (např. checksum), jakmile jsou data na straně cloudu, je otázka integrity dat ožehavější. Obzvláště u velkých objemů dat (řádově gigabyty) není možné přenášet všechna data k uživateli pro kontrolu, protože by znamenalo velkou zátěž pro cloud, případně velké náklady pro klienta. Přesto je pro klienta nutné, i když neví přesně, na kterých fyzických strojích jsou jeho data uložena (a tato informace se navíc v čase čile mění), aby byl schopen ověřit celkovou integritu dat, zda jsou všechna data aktuální, všechna nahrávání dat se podařila atp. Pro tento účel vznikly tzv. důkazy dosažitelnosti (proof of retrievability), což jsou matematické výpočty schopné ověřit integritu dat přímo v cloudu.

2.4.3.3 Dostupnost

V minulosti došlo k několika velkým výpadkům, například v případě S3 od Amazonu, který v roce 2008 měl dva výpadky, jeden trvající 2,5 hodiny, druhý o délce osm hodin. Kdyby tyto výpadky za rok 2008 byly jediné, znamenalo by to dostupnost služby na úrovni menší než 99.9 % (to odpovídá kumulativnímu výpadku přibližně 9 hodin za rok), zatímco zákazníci požadují ideálně dostupnost na úrovni 99,999% ("pět devítek", přibližně pět minut výpadku za rok); tuto dostupnost ovšem z velkých hráčů na trhu nikdo neposkytuje.

S dostupností souvisejí další dva problémy. Jedním je ztráta dat, kdy, například vlivem nekvalitního hardwaru, nejen že dojde k výpadku v dostupnosti, ale navíc jsou data jednou pro vždy ztracena. Druhým, možná ještě výraznějším problémem, je případné stáhnutí poskytovatele cloudu/uložiště z trhu. U každé společnosti, které svěřujeme svá data do cloudu, je potřeba vyčíslit riziko, že tato ukončí své podnikání a s tím spojené náklady s přenosem nebo i ztrátou dat a přechodu k jinému poskytovateli.

2.4.4 Správa uživatelů

I když jsou data přenesena do cloudu správně, je zaručena jejich integrita a dostupnost, problém stále není vyřešen. V mnoha společnostech je základním problémem správa identit a přístupů (Identity and Access Management). Tato oblast je velká a složitá, ale rámcově lze říct, že bez ohledu na to, jestli k autentizaci uživatele dochází přímo v cloudové platformě, nebo jestli je využívaný korporátní systém (přes SSO), pokud je používaná jen kombinace uživatelské jméno a heslo, je zabezpečení otevřené sociálním hackerským útokům a neposkytuje požadovanou ochranu.

Správně realizovaný systém IAM je mnohem složitější než prostá správa hesel a jejich složitosti, protože takový systém musí obstát před regulátory, musí pokud možno zlepšovat efektivitu, poskytovat správně možnosti autentizace a autorizace a musí být pravidelně auditovaný. Audit je přitom jedna z nejopomíjenějších součástí systémů IAM, což vede k rolím přiděleným uživatelům, kteří by je již dávno neměli mít, nebo k takovým, kteří už ve společnosti ani nejsou.

2.5 Klady a zápory využití cloudu

Cloudové služby by si nevydobyly svoje místo na slunci, kdyby neměly řadu pozitivních vlastností, jakými jsou:

- zrychlení vývojového cyklu
- odstranění pracnosti spojené se získáním, instalací a provozem infrastruktury
- standardizace
- jednoduchost získávání zdrojů a služeb [13]
- odstranění chyb z nepozornosti – vzhledem k tomu, že XaaS je jako služba vysoce používaná a pečlivě testovaná, odpadají běžné chyby, jako je zapomenutí na běžnou konfiguraci [13]
- snížení nároků na znalosti obsluhy – protože o většinu platformy se stará dodavatel, není potřeba držet tým vysoce schopných profesionálů, kteří rozumí kompletnímu stacku řešení [13]
- snížení nákladů, které by dohromady musely být využity na pořízení serverů, uložiště, síťových prvků, zálohy, disaster recovery, infrastrukturu datacenter, náklady na údržbu, obslužný personál a licence za platformu a software infrastruktury

Na druhou stranu, některým uživatelům brání k přechodu na cloudové řešení následující nesnáze:

- audit a compliance – obecně je potřeba zajistit, že data jsou uložena podle platných zákonů (vlastníka i jurisdikce lokace datacentra), je nastavena správná úroveň přístupu k datům, jejich správa a auditní stopa
- zabezpečení – zahrnuje integritu dat, zásady zachování soukromí a mlčenlivost
- výkonnost a dostupnost – existující regulatorní požadavky na dostupnost mohou být vyšší, než jsou ty nabízené poskytovatelem cloudové služby
- udržitelnost – bude cloudová platforma schopná podporovat náš business i v budoucnosti? Jaký je dopad běžných změn v platformě na náš business? [13]

Existují i negativa, kterým se lze vyhnout. Kavis [12] zmiňuje 9 základních problémů, které, pokud nejsou vzaty v potaz, mohou po zavedení cloudového řešení vést k nespokojenosti zákazníka:

- migrování aplikací do cloudu
- nepodložená očekávání
- nedostatečné informace o zabezpečení cloudu
- zvolení oblíbeného dodavatele místo správného dodavatele
- výpadky a Out-of-Business
- podceňování organizačních změn
- nedostatek znalostí
- nepochopení požadavků zákazníka
- neočekávané náklady

3 SHAREPOINT

Pro administrativu obecně jsou klíčové elektronické dokumenty. S nárůstem množství těchto dokumentů a rozšiřujícími se technickými možnostmi vznikla s postupem času potřeba dokumenty nějakým způsobem organizovat, zpřístupňovat, sdílet a případně zveřejňovat. Metoda sdílení dat a dokumentů v rámci interní sítě, jako jsou sdílené disky apod., přestala splňovat výše uvedené požadavky. Jednou z možností jak naplnit současné potřeby je využití SharePoint jako datového úložiště.

3.1 Popis produktu

SharePoint jako platforma vznikl v roce 1997. Zpočátku byl SharePoint vytvořen pouze jako IT aplikace, v dnešní době však vyžaduje interakci ze dvou stran, a to vývojáře a uživatele. Oba musí při nasazení vzájemně spolupracovat, uživatel definuje své požadavky, které následně vývojář implementuje. SharePoint je dnes pojímán jako aplikace určená pro všechny uživatele společnosti. Splňuje všechny požadavky na moderní systém datového úložiště dostupného přes internet včetně integrace s dalšími produkty společnosti Microsoft [18].

V dnešním obchodním světě, ve kterém zaměstnanci společnosti poskytují služby distribuovaným způsobem zákazníkům prakticky kdekoliv a kdykoliv, je více než kdy jindy potřeba, aby členové týmu udržovali kontakt. Efektivita spolupráce se stává vysoce důležitou, ovšem je mnohdy těžké ji docílit. Microsoft SharePoint 2013 tento problém řeší tím, že spojuje různé druhy kolaborativních a komunikačních technologií do jednoho prostředí, přístupného přes internet, které je spojeno s desktopovými aplikacemi, jako je Microsoft Office.

SharePoint 2013 zvyšuje produktivitu a efektivitu společností a business jednotek všech velikostí tím, že poskytuje sadu nástrojů pro organizaci obsahu, správu dokumentů, sdílení vědomostí, dále že vytváří velké interaktivní prostředí pro spolupráci a vyhledávání informací a lidí. Sociální rozměr SharePoint 2013 umožňuje vytvářet komunity (tj. skupiny uživatelů), sdílet myšlenky a nápady a vyhledávat zdroje a vědomosti napříč společností.

SharePoint 2013 pomáhá týmům zůstat v kontaktu a udržovat produktivitu, protože poskytuje jednotnou infrastrukturu a funkcionalitu, která dává lidem snadný přístup ke kolegům, dokumentům a informacím, které potřebují. Týmy mohou vytvářet webové stránky, na kterých dochází ke sdílení informací a které povzbuzují další spolupráci. K tomuto obsahu se uživatelé (ne nezbytně jen členové týmu) mohou dostat pomocí webového prohlížeče, pomocí softwaru, jakým je Office, a to přes různá zařízení, například PC, tablet nebo smartphone.

Webové stránky v SharePoint, neboli sites, vytvářejí místo pro zaznamenání a sdílení myšlenek, informací, komunikace a dokumentů. Funkcionalita sites umožňuje spolupráci týmů, spolupráci na dokumentech, zaznamenávání úkolů a problémů, blogování a mikroblogování (web log, forma deníku pro zápis informací s možností příspěvky komentovat) nebo vytváření znalostních bází pomocí wiki sitů (poskytují možnost rychle přidat a upravovat text, obrázky a odkazy na sitech; z havajského „wikiwiki“, což znamená „rychlý“). Dokumenty mohou být jednoduše vyžádány pro úpravu (check-out) a znovu uloženy (check-in), jednotlivé verze jsou uchovány (document version control) a předchozí verze mohou být jednoduše obnoveny. To vše ovšem na zabezpečené platformě SharePoint, která znemožňuje přístup k dokumentům neoprávněným osobám.

Každý site na SharePoint může mít několik podřízených sitů – subsitů, jejichž hierarchie připomíná stromovou strukturu adresářů v souborovém systému. Podobně, jako lze ukládat soubory na počítači do složek, lze ukládat soubory na SharePoint do sitů. Možnost spolupráce ovšem posouvá práci se soubory v SharePoint na novou úroveň – přístup k souborům je mnohem jednodušší a prostředí, zaměřené primárně na spolupráci, může drasticky zvýšit osobní i týmovou efektivitu. Soubory lze uložit jak v SharePoint, OneDrive (dříve SkyDrive), kde je vidí ne jeden uživatel, ale, v případě potřeby, všichni jeho spolupracovníci, kteří k nim mohou přistupovat na mnoha zařízeních, jak bylo uvedeno dříve (PC, tablet, smartphone). Efektivita využití je podpořena tím, že nástroje poskytované SharePoint jsou intuitivní a jednoduše použitelné, lze jednoduše vybudovat primární site pro tým, další pro organizování schůzek, další site pro wiki a třeba další pro aktuálně běžící projekt.

V SharePoint 2013 je přístup do sitů řízen pomocí systému rolí, který používá úrovně oprávnění (permission level). Úrovně oprávnění specifikují, jaká oprávnění uživatelé mají a oprávnění určují, jaké úkony mohou uživatelé provádět na situ. Ve své podstatě je každá úroveň oprávnění sadou jednotlivých oprávnění. Základní úrovně oprávnění v Sharepointu jsou Read, Contribute, Design, Full control a Limited [19].

3.2 Aplikační možnosti

Microsoft nabízí tři SharePoint 2013 řešení, která lze provozovat na serverech organizace. Každé řešení poskytuje trochu jinou skupinu funkcionalit, podle klientských přístupových licencí (Client Access License, CAL):

- SharePoint Server 2013 Enterprise CAL
- SharePoint Server 2013 Standard CAL
- SharePoint Foundation 2013

Každé z nabízených řešení umožňuje spolupráci jak uvnitř společnosti, tak s partnery a zákazníky. Ovšem každý z produktů poskytuje jiné funkčnosti.

SharePoint 2013 je balíček služeb pro Windows Server 2012 který je zároveň k volnému stažení zadarmo. SharePoint Foundation 2013 lze používat ke sdílení informací, spolupráci s ostatními uživateli, pro správu dokumentů všech typů a jako základní platformu pro aplikace pro spolupráci. Různé jazykové mutace je možné provozovat na jedné instalaci SharePoint Foundation 2013 pomocí jejích jazykových balíčků.

Obě Server řešení – Standard i Enterprise – jsou postaveny na SharePoint Foundation 2013. Proto jsou v něm přítomny všechny funkcionality Foundation. Pro společnosti ovšem nabízí navíc

funkcionality sociálních stránek, business intelligence, správy obsahu, vyhledávání, workflow a další. Standard a Enterprise mají každý ovšem vlastní funkcionality.

Při rozhodování, kterou z verzí SharePointu použít, je potřeba nejprve zjistit, které funkcionality společnost potřebuje. Rozdíly mezi všemi třemi verzemi jsou uvedeny v tabulce 2.

Tabulka 2: Schopnosti jednotlivých verzí SharePoint 2013 [19]

Funkcionality	SharePoint 2013		
	Foundation	Standard CAL	Enterprise CAL
Vyhledávání	Ne všechny možnosti	Ne všechny možnosti	Ano
Správa obsahu	Ne	Ano	Ano
ACM, Compliance	Ne	Ne	Ano
Excel Services, PowerPivot, PowerView	Ne	Ne	Ano
Scorecard a dashboardy	Ne	Ne	Ano
Access Services	Ne	Ne	Ano
Visio Services	Ne	Ne	Ano
Workflow	Ne	Ano	Ano
Business connectivity	Ano	Ano	Ano

SharePoint Online je služba provozovaná skrze web, která je hostovaná mimo společnost v cloudu, mimo server ovládané společností (off premises). Vztahují se na něj tedy všechny rysy cloudových služeb, jako je přístupnost přes web, správa třetí stranou apod. Jako služba vyžaduje SharePoint předplatné (subscription). SharePoint Online je, stejně jako Skype (dříve Lync), součástí Microsoft Office 365, na který se také vztahuje předplatné. SharePoint 2013 se dá koupit i jako samostatné předplatné.

Funkcionality SharePoint Online jsou navrženy tak, aby běžely stejným způsobem jako SharePoint 2013 on premises. Ovšem existují výjimky, například v business inteligence nebo ve správě obsahu.

Společnost se může rozhodnout pro SharePoint on premises, nebo pro SharePoint Online, nebo obojí najednou (hybridní řešení). Hybridní řešení umožňuje vyhledávání jak v cloudové části, tak v on-premise části pomocí jediného dotazu. Hybridní řešení se hodí, pokud není pro společnost možné převést veškerá data do cloudu z technických, obchodních, právních nebo jiných důvodů.

Data mohou být např. striktně hostována pouze v určité fyzické lokaci. Pomocí hybridního řešení může společnost začít okamžitě benefitovat z vlastností cloudu, a zároveň udržet on-premise kontrolu nad daty a konfigurací platformy, a nemusí se nutně rozhodovat mezi jedním nebo druhým řešením.

SharePoint je přímo integrován s aplikacemi Office do té úrovně, že produkty Office přímo obsahují příkazy pro SharePoint. K práci se SharePoint tak lze přistupovat vedle internetu i např. z Word nebo Excel. Lze tak ukládat soubory do sitů, vytvářet sity a nastavovat oprávnění přímo z aplikací Office, bez nutnosti využívat webové rozhraní SharePoint. Mimo souborů lze z Office přímo přistupovat i k událostem, kalendářům, přiděleným úkolům a blogům.

Na druhou stranu SharePoint umožňuje upravovat soubory přímo z webu – Word a Excel dokumenty se tak otevřou přímo v prohlížeči. Webová verze Office aplikací zpravidla blízce koresponduje s funkčností desktopových aplikací, i když některé funkcionality nemusejí být přítomné. Soubory lze ovšem vždy otevřít v nativních Office aplikacích (ale stále se s nimi pracuje jako se soubory uloženými v SharePoint, nikoliv lokálně), pokud tyto nativní aplikace jsou na zařízením, přes které uživatel přistupuje k SharePoint, nainstalovány. Produkty Microsoft Office XP poskytují alespoň základní integraci se SharePointem, od verze Microsoft Office 2007 je toto propojení výrazně lepší, a každá další verze přináší nové a užší spojení (např. Backstage v Office 2010).

Pro úplnost se sluší dodat, že i když je SharePoint cloudový nástroj, díky zmíněné integraci s MS Office lze pracovat se soubory i offline. Soubory uložené v offline režimu jsou synchronizovány s verzí v cloudu při dalším připojení k síti [19].

3.3 Klady a zápory využití Sharepointu

SharePoint urazil od svého vzniku dlouhou cestu a stal se nástrojem pro ulehčení správy intranetu, místo neohrabané pomůcky vedoucí k zoufalství uživatelů. Přesto, některé slabé stránky SharePoint 2013 ukazují, že je stále kam se vyvíjet. Gaile [20] udává 6 kladů a 6 záporů SharePoint:

3.3.1 Klady

- **je přístupný přes internet** – přístupnost přes internet zajišťuje vysokou úroveň spolupráce. Soubory mohou být do cloudu nahrány přes internetový portál, zpřístupněny autorizovaným uživatelům, upravovány a znovu uloženy, pokud je potřeba. Zároveň dochází ke snížení počtu fyzických dokumentů

- **je přístupný přes mobilní zařízení** – umožňuje uživatelům přístup k datům uloženým v intranetu (SharePoint) odkudkoliv, s využitím mobilního zařízení (smartphone, tablet). Tato schopnost je výrazně lepší v SharePoint 2013, než byla v SharePoint 2010
- **umožňuje vytvářet sociální sítě** – v předchozích verzích SharePoint možnost vytvářet sociální sítě prakticky neexistovala. V SharePoint 2013 lze spojovat skupiny, týmy i jednotlivce navzájem skrze internet, takže lze rychleji přenášet zprávy, dokumenty nebo potřeby.
- **umí se integrovat s MS Office** – mnoho společností dnes používá produkty řady MS Office pro většinu administrativy. Na rozdíl od jiných platforem pro firemní intranet, soubory vytvořené v MS Office jsou k dispozici okamžitě a lze je upravovat i přímo v SharePoint
- **lze jednodušše převést do brandu společnosti** – i když Microsoft varuje před některými změnami v platformě, brandovat stránky (tj. nastavit firmní logo, nadpisy, barvy) je relativně jednoduché. To zpříjemní vzhled intranetu a pomůže uživatelům lépe akceptovat tento nástro jako součást firemního toolsetu
- **má dobré zabezpečení** – Microsoft rozvinul autorizační a autentikační protokoly SharePoint do té míry, že uživatelé mohou přistupovat ke službě zcela individuálně. To tedy znamená, že pracovníci mohou mít přístup ke všem oblastem intranetu, kam přístup potřebují, a do žádných míst, kam přístup nepotřebují. I pro uživatele, kteří často mění svoji úroveň přístupu, bude složité dostat se/udržet si přístup k informacím, ke kterým přístup mít nemají.

3.3.2 Zápory

- **úpravy řešení nejsou doporučeny** – SharePoint mohl společnostem přinést možnosti, jak přidávat vlastní funkčnosti svému intranetovému systému, ale Microsoft od tohoto přístup odrazuje. Vzhledem k tomu, že tato praktika není doporučována, může její (nad)užívání vést k chybám, pokud se Microsoft v budoucnosti rozhodne změnit možnosti nastavení.
- **nastavení vyhledávání vyžaduje mnoho úprav** – většina uživatelů bude zklamaná vyhledáváním v SharePoint. Ve srovnání s tím, jak snadno lze najít zatoulaný soubor na počítači, vyhledávání přes internet je, při nejmenším, složité. Interní IT pracovníci musí strávit hodně času, aby platformu nastavili tak, aby vyhledávání bylo účinné, což často představuje nepředvídané náklady. Pokud společnost tyto odborníky nemá a musí je najímat externě, tyto náklady mohou být velmi vysoké

- **sociální sítě nejsou spojeny se zbytkem intranetu** – aby mohli uživatelé sdílet nebo dostávat upozornění, musí se nejdřív dostat mimo hlavní intranetové stránky. Uživatelský zážitek (user experience) je v tomto ohledu špatný a vede ke zvýšeným nárokům na školení běžného uživatele, který bez nich nedokáže využívat sociální funkčnosti SharePoint. Zde je prostor pro velké zlepšení
- **veřejné stránky již nejsou podporovány** – před zákazníky, kteří uvažují o přechodu na SharePoint, stojí unikátní výzva. SharePoint už neumožňuje vytvořit veřejné stránky (přístupné i z vnějšku společnosti), které by byly postaveny na datech v intranetu. Pokud tedy zákazník tuto funkčnost potřebuje, musí se obrátit na třetí stranu, jejíž kvalita může být různá. Pro obzvláště menší zákazníky může tento aspekt snadno způsobit, že SharePoint nebude ve společnosti zaveden
- **dostupné aplikace nejsou jednoduše použitelné a často nejsou spravovatelné** – v mnoha ohledech se zdá, že k dodání aplikací do SharePoint došlo až na poslední chvíli, snad ve snaze držet krok s ostatními cloudovými službami, které aplikace také podporují. Výsledkem je, že je velice složité přidat do platformy o něco více než velmi základní funkcionality
- **nelze ho provozovat v malé síti** – Pokud disponuje firma jen malým intranetovým prostředím, je zcela jisté, že nebude moci využít všechny funkčnosti SharePoint. Jsou totiž potřeba separátní workflow server a OWA server, aby byl odemčen plný potenciál platformy. Pokud jsou tedy fáze sběru požadavků a plánování před nasazením platformy podceněny, dojde k zanedbání požadavků na další hardware a snížení užitných vlastností SharePoint.

PRAKTICKÁ ČÁST

4 NASAZENÍ V REÁLNÉ SPOLEČNOSTI

4.1 Popis výchozího stavu

Společnost, ve které došlo k nasazení SharePoint, dále jen společnost, byla založena v Praze v roce 2004, kde má zároveň sídlo ve starší budově. Důležitost stáří budovy bude popsáno níže. Společnost se specializuje na přípravu a realizaci krátkodobých akademicko-poznávacích zájezdů (experiential learning) připravovaných výhradně na zakázku pro zahraniční univerzity, konkrétně pro jejich studenty v programech MBA a Executive MBA.

Zájezdy jsou plánovány na 3 – 21 denní pobyty, kde hlavní náplní jsou akademický program a logistické služby. Zákazníky jsou univerzity a obchodní školy z USA, Velké Británie, Austrálie a Mexika – pro ČR nejsou služby vůbec poskytovány. Počet cestujících se u jednoho zájezdu se pohybuje mezi 10 až 120. Destinace společnosti jsou na 6 kontinentech (Evropa, Asie, Latinská Amerika, Severní Amerika, Austrálie a Afrika), s tím, že všechny aktivity jsou organizovány z jediné pobočky v Praze.

Mezi hlavní cílové lokality patří Čína, Vietnam, Jižní Afrika, Česká Republika, Německo a Maďarsko. Společnost je schopná zařídit celý zájezd; kompletně se stará o celou skupinu cestujících a obstarává pro ně veškeré logistické služby, mezi které patří ubytování, stravování, autobusová doprava v místě pobytu, průvodce a kulturní program. Ovšem hlavní náplní zájezdu je akademický program, který je připraven na základě požadavků klienta. Jedná se zpravidla o přednášky na odborná témata, návštěvy společností a setkání s top managementem firem, panelové diskuze s odborníky atp. Celý program je koncipován tak, aby jednotliví cestující – studenti univerzit – získali odborné znalosti v rámci oboru jejich studia.

V současné době má společnost dvě kanceláře, v Praze a v Hongkongu. Důležitým faktorem je ovšem pracovní náplň, která spočívá v poskytování studijních pobytů po celém světě, část zaměstnanců je tedy neustále mimo kanceláře a potřebuje vzdálený přístup k datové infrastruktuře společnosti.

V původní konfiguraci byl nasazen operační systém Windows Server 2008, který poskytoval virtuální prostředí pro další služby. Hlavní ze služeb, která byla provozována v tomto prostředí, byla Windows SBS Server 2003 se službou Exchange 2003 s následujícími parametry: využitelná disková kapacita 35GB pro uživatelské složky a dalších 45GB pro sdílené složky, dále služby Forefront Security, Antigen, NTBackups a File Server s maximální kapacitou 500GB.

Všechny softwarové servery byly provozovány pouze v jedné lokalitě společnosti (Praha) na fyzickém serveru Hewlett-Packard. V popsané konfiguraci ovšem žádný z těchto systémů nebyl zabezpečen pro případ selhání HW či SW; například disky nebyly zařazeny v diskovém poli, tj. výpadek kteréhokoliv z disků by znamenal ztrátu přístupu k výše zmíněným provozovaným službám, a z toho vyplývající ztráty dat.

V rozporu s principy zabezpečení a zálohování dat byla data v původním řešení zálohována na jeden externí disk, který byl umístěn ve stejné fyzické lokalitě (stejná serverová místnost a stejný rack). Tyto zálohy nebyly schopné, kvůli nedostatku kapacity disku, pojmout celý objem zálohovaných dat, a tedy docházelo k pravidelným selháním zálohovacího procesu. Navíc denní zálohování, z časového hlediska, zabralo více než jeden den, což značně omezovalo výkon systémů a tím i uživatelský komfort, a reálná frekvence záloh tím pádem byla víceméně náhodná, delší, než jeden den.

Dále je potřeba zmínit, že v budově byli zaměstnanci společnosti (uživatelé) rozmístěni ve dvou patrech a zároveň v různých částech budovy. Vzhledem k těmto mezením, která klade historická budova, nebylo možné vybudovat adekvátní síťovou infrastrukturu; např. obě patra byla propojena pouze jedním síťovým kabelem, což výrazně omezovalo propustnost sítě. Dalším aspektem, který značně omezoval dostupnost služeb z prostředí mimo společnost, bylo připojení k internetu, které v dané lokalitě a s dostupnými ISP dosahovalo maximálních teoretických hodnot 10/8Mbit.

4.1.1 Souhrn stávajících nedostatků

Uživateli a manažery byly identifikovány následující provozní nedostatky a slabá místa:

1. příliš pomalé přístupy k systémům skrze VPN ze všech míst mimo lokální síť (například z Hongkongu a Číny)
2. možnost využití VPN je blokovaná v některých státech (na hotelech, na veřejných WiFi i v internetových kavárnách)
3. omezení přístupu na e-mailový server z hotelů, kde je zablokovaný standardní port; uživatelé se musí připojovat např. pomocí webové služby přes prohlížeč, což je pomalé a neefektivní
4. na sdílení pracovních informací šlo prakticky využít jen veřejné sdílené e-mailové složky. To je neefektivní a je potřeba jiné, lepší řešení pro sdílení informací vč. e-mailů mezi uživateli
5. existuje standardizovaná adresářová struktura, ale je zastaralá a tudíž bude potřeba ji revidovat

6. jedinečná lokalizace dat v sídle společnosti představuje riziko v případě katastrofálního selhání systému, případně živelné události (např. požár) – neexistují žádné dodatečné externí zálohy, současné zálohy by byly během požáru zničeny spolu se zbytkem infrastruktury

Tato zjištění byla rozdělena do tří tematických celků, konkrétně:

- **Access** (Přístup ke službě): nálezy 1. až 3.
- **Sharing** (Sdílení informací ve společnosti): nálezy 4. a 5.
- **Back-up** (Řešení záloh dat a e-mailů): nález 6.

  Nad tento rámec jsou součástí parametrů řešení ještě dvě skupiny požadavků:
- **Security** (Bezpečnost)
- **Operational** (Funkční a užitné vlastnosti systému)

4.2 Identifikace požadavků na změnu

V návaznosti na identifikovaná zjištění byly formulovány tyto požadavky na nové řešení. Požadavky jsou formulovány zvlášť pro e-mailové řešení a pro datové uložiště. V závorkách je vždy uvedeno téma, kterého se daný požadavek dotýká.

4.2.1 Požadavky na e-mailové řešení

- snadný 24/7 přístup k e-mailům společnosti bez potřeby VPN odkudkoliv na světě (Access)
- přístup k e-mailům musí být rychlý ze všech typů připojení (hotel, veřejná WiFi) (Access)
- zajištěný support pro nově pořízený systém, např. Outlook-on-the-Web (Access)
- e-mailové řešení je kompatibilní s Outlookem jako s hlavní aplikací, je přístupné ze všech OS (Windows, Mac) a přes všechny smartphony (Android, WM, iOS) (Access)
- možnost vytvářet neomezené množství sdílených (veřejných) doručovacích složek. (Access, Sharing)
- e-mail sdílený ve *Veřejné* složce Outlooku bude k dispozici všem zaměstnanců bez ohledu na lokalitu a typ připojení, a to včetně bezproblémového přístupu k přílohám (Access, Sharing)
- každý e-mail lze obnovit ze záloh během jednoho pracovního dne s minimální historií 14 dnů, zálohy jsou prováděny denně (Back-up)
- zabezpečení uživatelských účtů a dat (Security)

- možnost běžné správy všech účtů (zřizování, blokování, mazání, změna hesla, přesměrování, vytváření skupin apod.) z jedné lokality (Operational)
- snadné nastavení nového účtu – na základě jména, hesla a mailového serveru by měla být ihned vygenerována nová schránka (Operational)
- přístupová práva jsou rozdělena minimálně na úrovně uživatel a administrátor (Operational)
- možnost vytvářet skupiny – maillisty a skupiny pro správu zabezpečení (Operational)
- možnost vytvářet aliasy (Operational) přesměrování zpráv po odchodu zaměstnance
- snadná migrace bez dopadu na dostupnost služby během migrace (Operational)
- podpora sdílených a veřejných kalendářů (Operational)

4.2.2 Požadavky na datové uložiště

- snadný 24/7 přístup k datům společnosti odkudkoliv na světě (Access)
- garantovaná dostupnost za všech okolností – zároveň i mimo pracovní dobu a o víkendech (Access)
- přístup k datům je možný ze všech běžných OS (Windows, Mac, aj.) (Access)
- dokumenty, které mají pod 5 MB, bude možné stáhnout, otevřít nebo modifikovat za méně než 20 vteřin. (Access)
- vytvoření transparentní a sjednocené struktury pro sdílení dat společnosti; datová struktura by měla být navržena tak, aby eliminovala vznik datových duplicit a umožnila identifikaci starých a nepoužívaných dat pro případné smazaní (Sharing)
- k dokumentům, které jsou uloženy ve sdílených složkách, lze přistupovat z lokalit na celém světě a s použitím libovolného internetového připojení. (Sharing)
- více uživatelů může upravovat jeden soubor (Sharing)
- systém podporuje verzování souborů, a umožňuje obnovení dat/přístup k datům i v případě selhání některé z firemních lokalit či neoprávněného zásahu jiného uživatele (Back-up)
- systém je považován za zabezpečený z pohledu obecně uznávaných standardů zabezpečení citlivých údajů osob a společností (Security)
- možnost obnovit jednotlivé soubory ze zálohy až do 14 dnů administrátorem (Back-up)
- garantovaný maximální čas pro obnovu dat i mimo pracovní dobu a víkendy (Back-up)
- možnost běžné správy dat z jedné lokality (Operational)
- přístup k souborům je rozdělen minimálně na úrovně uživatel a administrátor (Operational), viz výše

- support s garantovaným časem odezvy (Operational)
- vyhledávání (Operational)

4.2.3 Další požadavky

Vedle základních požadavků na uložiště a e-mail společnost, v rámci výběru nového řešení, brala v potaz ještě dvě funkčnosti, jejichž potřeba byla s růstem společnosti stále palčivější. Šlo o účetní systém a docházkový systém. Ani jeden ze systémů do té doby neexistoval. Na tyto služby nejsou kladeny požadavky na vzdálený přístup nebo odezvy.

4.3 Změna do cílového stavu

4.3.1 Výběr řešení

V době rozhodování byla managementem společnosti uvažována různá řešení. Nakonec byl na základě interního průzkumu možností vybrán MS Office 365. Ten nabízí základní Office funkcionality, které společnost využívá (MS Word, MS Excel), navíc má v cloudu Exchange Server jak e-mailové řešení a SharePoint + OneDrive pro pokrytí potřeb sdílení dat. U docházkového a účetního systému byla zvolena varianta provozu z vlastněného fyzického serveru, takže do rozhodování o využití cloudu pro data a e-maily logicky nevstupovaly.

Pro přechod ze stávajícího řešení na Sharepoint byly osloveny 3 externí společnosti, které měly připravit migrační plán na základě předchozích zkušeností s migracemi do Sharepoint/Cloudu. Jedna z těchto společností, která vyhrála výběrové řízení, ve výsledku připravila model a migrační plán. Samotná migrace byla realizována interně zaměstnanci společnosti.

4.3.2 Cílový stav

V rámci přesunu do cílového stavu byly do cloudu přesunuty soubory a e-maily. MS Office 365 nabízí pro ukládání souborů 2 základní platformy – OneDrive a SharePoint. Na úrovni managementu společnosti bylo rozhodnuto, že cílem pro soubory se stane SharePoint. OneDrive je dodnes využíván sporadicky, hlavně při transferu objemnějších souborů.

Pro e-mailové řešení se využil Exchange server ze sady MS Office 365. Dále jsou dodnes využívány služby CRM Microsoft Dynamics a některé aplikace na míru.

Na druhou stranu do cloudu, ani s řešením obsahující celé MS Office 365, nešly převést všechny funkcionality potřebné pro provoz společnosti. Součástí přechodu na SharePoint tak bylo, původně neplánované, pořízení nového serveru včetně příslušných licencí v následující konfiguraci:

HW server HP ProLiant DL380 gen9

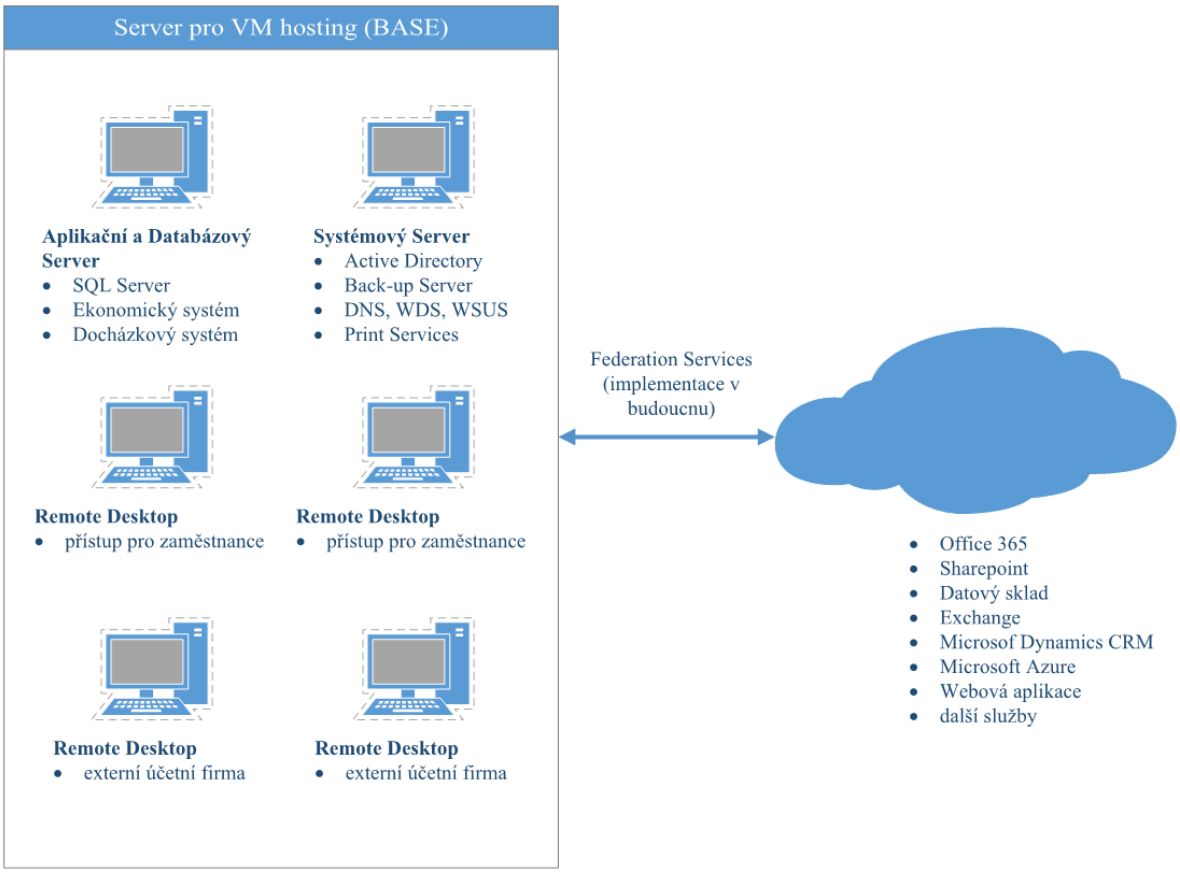
- 2x Intel(R) Xeon(R) CPU E5-2620 v3 @ 2.40GHz, 6 Cores, 12 Logical Processors
- 64GB RAM
- celková disková kapacita o velikosti 7TB konfigurovaná v RAID 1+0
- operační systém Windows Server 2016std

Na tomto serveru jsou nadále provozovány 2(3) virtuální servery a 4 virtuální PC:

- Active Directory server pro správu uživatelských účtů, DNS, dále služby File Services, Update Server, Deployment Services, Print Services, které jsou potřebné pro běžný chod kanceláře a správu uživatelských stanic
- server pro provoz starých firemních aplikací
- aplikační server, na kterém jsou převážně provozovány nové aplikace spojené s růstem firmy – účetní systém a docházkový systém (obojí krabicové řešení) – a služby potřebné pro jejich provoz, jmenovitě SQL Server
- 4 virtuální PC jsou určená pro umožnění práce externím zaměstnancům (účetní), případně pro vzdálený přístup kmenových zaměstnanců. Virtualizována jsou právě 4, protože tento počet ještě odpovídá výkonnostním možnostem fyzického serveru

Jak je vidět z celkového popisu (viz obr. 1), ve společnosti jsou momentálně dvě Active Directories, které spolu ovšem nejsou synchronizované. To znamená, že např. založení nového uživatelského účtu je nutno udělat dvakrát, v každém Active Directory zvlášť. Rozhodnutí ponechat Active Directory i ve společnosti je motivováno vlastnostmi její cloudové varianty – v AD v cloudu je dražší, složitěji se spravuje a neobsahuje Group Policies, které jsou pro rostoucí společnost nezbytností. Nepříjemnost správy dvou AD by v budoucnosti mohlo odstranit použití Federation Services, o kterém se v současnosti uvažuje.

Obrázek 1: Konfigurace on premise a v cloudu po migraci do SharePoint



4.3.3 Vlastní realizace řešení

Migrace dat uživatelů, e-mailů a složek, byla rozdělena do dvou částí:

1. soubory byly kopírovány ze serverových disků ve společnosti do SharePoint ručně; tato činnost zabrala dohromady několik týdnů
2. exchange e-mail byl migrován pomocí připravených skriptů. Migrace zabrala jeden víkend, přes který uživatelé nesměli ke svým e-mailovým účtům přistupovat. V pondělí pak došlo k převodu jejich účtů na nový Exchange server

Pro úspěšné provedení migrace bylo potřeba nejprve identifikovat soubory pro migraci, odstranit nepotřebné soubory, odstranit duplicity a vytvořit novou strukturu souborů pro použití v SharePoint, která by umožňovala rychlou orientaci a dohledání potřebných dat. Tato činnost zabrala delší dobu (týdny) a samozřejmě nebylo možné ověřovat pro každý soubor u všech zaměstnanců, jestli je, nebo není i nadále potřebný. I tak ale nebyly po migraci do SharePoint hlášeny žádné ztráty dat.

V rámci samotné migrace se zjistilo, že SharePoint má omezení pro velké soubory (v době migrace 20 MB) – tento limit byl zásadní hlavně pro marketingové soubory (videa, prezentace, záznamy) a bylo proto nutné zřídit on premise dedikovaný souborový disk.

5 MĚŘENÍ A VÝSLEDKY

Jak je popsáno výše, původní soubory a e-maily byly migrovány do SharePoint. SharePoint splnil všechny požadavky na e-mailový server a uložiště souborů, jak jsou identifikovány v kapitole „Identifikace požadavků na změnu“, předně 24/7 dostupnost, správu a zálohování. Když jsou tyto požadavky splněny, je potřeba přistoupit k měření uživatelského komfortu, spokojeností s novým řešením. Rovněž je možné provést měření zaměřené na odezvu SharePoint pro uživatele.

5.1 Zpětná vazba uživatelů

Vazbu na výsledek převodu e-mailů a souborů, vnímané dopady a případné problémy poskytli jak řadoví zaměstnanci, tak manažeři.

Uživatelé zmiňovali především:

- nemožnost pracovat s velkými soubory – hlavně marketingová data (videa)
- přístup k datům lokálně byl subjektivně rychlejší, dokud soubory byly v lokální síti – toto tvrzení bude posuzováno dále
- po nasazení se ukázalo, že SharePoint funguje správně pouze s Internet Explorer, na Chrome a Edge dochází k problémům
- uživatelé jsou při přístupu z vně společnosti už od začátku spokojeni se SharePoint, připojení k němu je výrazně jednodušší a rychlejší než práce s VPN

Problémy se ztrátou souborů nebyly zaznamenány. To je potřeba přisoudit především řádné přípravě souborů a přípravě struktury před samotnou migrací. Tato příprava nesouvisí přímo s vybranou cílovou platformou, ať už by byla v cloudu, či nikoli. Takovou přípravu je obecně potřeba doporučit obecně pro veškeré migrace dat.

Management

- oceňuje integraci s Office 365
- považuje Sharepoint za bezpečný
- zjistil problémy s rozsáhlým verzováním souborů – hlídání např. 20 verzí jednoho souboru plus jeho pod-verzí znamená výrazný nárůst místa, který tento soubor v cloudu zabírá
- předpokládal vyšší využití funkcí dostupných v SharePoint, např. sdílení odkazů a využívání dotazníků, ale tyto byly shledány příliš těžkopádnými a neintuitivními a tudíž se nevyužívají
- vidí přínos ve škálovatelnosti, zvlášť v krizových situacích
- vidí úsporu v nákladech, které by jinak stálo udržování vlastních serverů, aplikací a lidské síly potřebné na jejich nepřetržitou podporu

5.2 Měření odezev

Uživatelé měli po přechodu na cloud dojem, že responsivita je horší. U dat a e-mailů skladovaných on-premise se dá, při přístupu z intranetu, předpokládat prakticky nulová latence a nedochází ke ztrátám packetů.

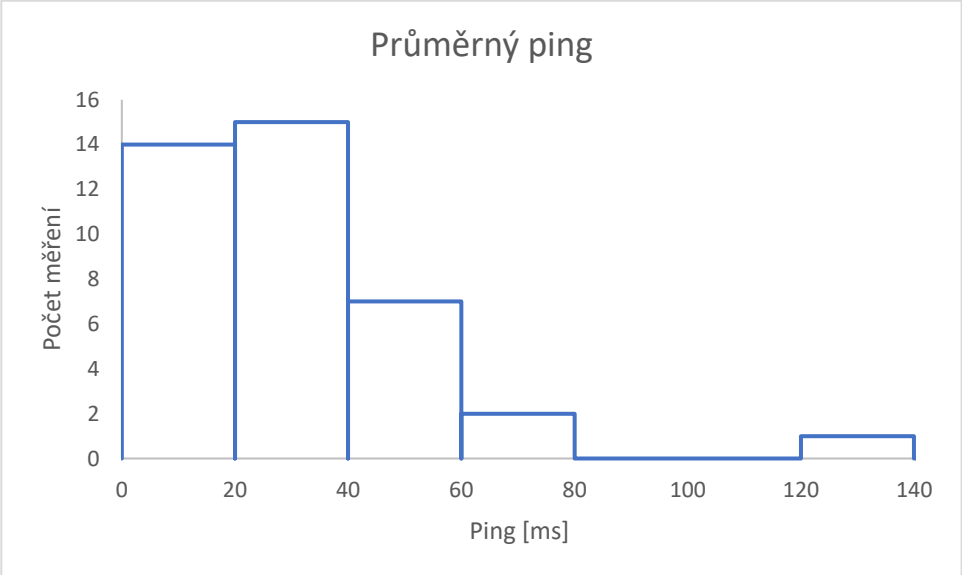
Pro měření odezvy byl z různých uživatelských stanic testován přístup na server SharePoint. Byla zkoumána doba odezvy a jitter, přitom všichni uživatelé byli v době měření mimo kancelář společnosti a tedy přistupovali přes různé sítě, poskytovatele a z různých částí světa.

Parametry testu byly:

- 1500 dotazů na SharePoint během 30 minut
- měřena doba odezvy a jitter
- zapojeno 39 zaměstnanců

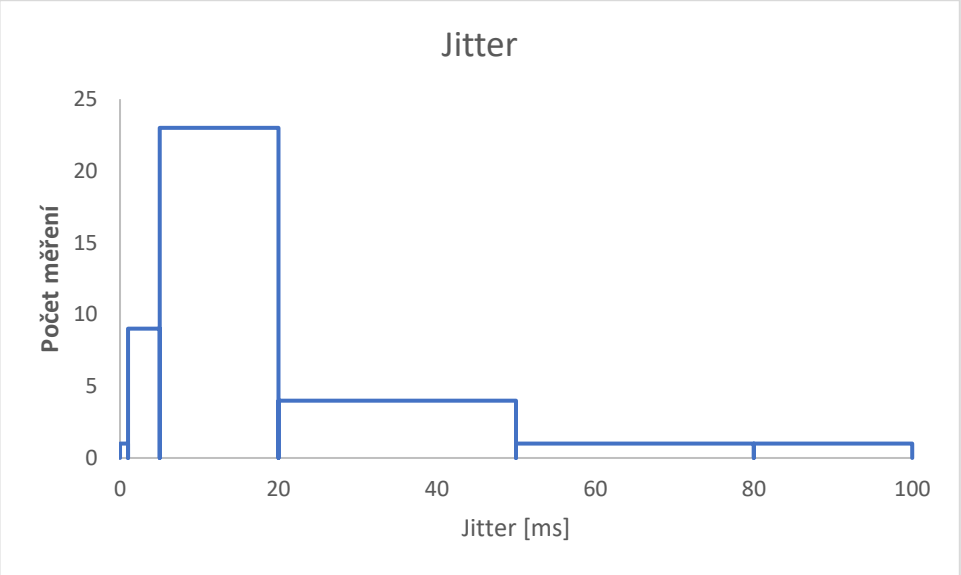
Měřením bylo ověřeno, že uživatelé ze SharePoint obdrží odpověď v průměru za 32 milisekund. Rozdělení odezev není normální, ale je výrazně vychýleno směrem k nižším hodnotám, jak je vidět na obr. 2.

Obrázek 2: Průměrný ping



Průměrný jitter byl stanoven na 13 milisekund. Rozdělení jitterů bylo znázorněno na obr. 3, aby odpovídalo klasifikaci podle 3rd Echelon [21].

Obrázek 3: Konfigurace on premise a v cloudu po migraci do SharePoint, jitter



Z tohoto rozdělení je patrné (viz tab. 3), že většina uživatelů, z pohledu cloudu, spadá do kategorie „velmi dobré“ (very good).

Tabulka 3: Konfigurace on premise a v cloudu po migraci do Sharepoint

Jitter menší než [ms]	Klasifikace	Počet uživatelů
1	Excellent	1
5	Extremely Good	9
20	Very Good	23
50	Good	4
80	Good to Fair	1
100	Fair	1

6 ZÁVĚR

Bylo popsáno nasazení SharePoint do středně velké společnosti. Hlavním cílem bylo zpřístupnit soubory a e-maily pro zaměstnance pracující jak v centrále společnosti, tak v různých lokalitách po celém světě.

Všechny věcné záměry spojené s nasazením byly splněny. SharePoint nahradil původní řešení fungující přes VPN a zpřístupnil data uživatelům prakticky bez omezení, data dostupnosti dokládají, že uživatelé nemají problémy s přístupem k datům, která potřebují k práci a management oceňuje výhody cloudu, mezi které řadí škálovatelnost, bezpečnost, dostupnost a omezení nákladů spojených s provozem hardwaru vlastními silami.

Úspěch nasazení byl ovšem podmíněn řádnou přípravou – data byla shromážděna, vyčištěna, byla vytvořena nová struktura dat – s čímž cloud jako takový přímo nesouvisí a tento krok je nutným předpokladem jakékoliv úspěšné migrace dat.

SharePoint je úspěšně využíván pro menší soubory používané v rámci Office 365, využití dalších funkcionalit bylo blokováno technickými problémy. Jmenovitě velké soubory, využívané například pro marketing, nejsou SharePoint dobře podporovány. SharePoint nefungoval zcela správně na všech typech prohlížečů. U těchto obtíží lze očekávat, že budou časem odstraněny, nebo že se situace minimálně zlepší, ale momentálně mohou představovat limitující faktory pro nasazení v jiných společnostech.

Další funkcionality, účetní systém a docházkový systém, SharePoint neposkytuje vůbec, a minimálně z důvodu provozu těchto služeb musí ve společnosti zůstat dedikovaný fyzický server.

Celkově vzato může cloudová integrace, v tomto případě SharePoint, snížit náklady společnosti, snížit počet serverů provozovaných společností samotnou, ale prozatím cloudové služby nemohou nahradit portfolio všech služeb, které společnost používá.

7 SEZNAM POUŽITÉ LITERATURY

[1] DOUGLIS, Fred a Orran KRIEGER. Virtualization. *IEEE Internet Computing*. 2013, **17**(2), 6-9. DOI: 10.1109/MIC.2013.42. ISSN 1089-7801. Dostupné také z: http://ieeexplore.ieee.org/document/6488669/

[2] SCROGGINS, Richard. Virtualization Technology Literature Review. *Global Journal of Computer Science and Technology*. 2013, **13**(1), 1-6. ISSN 0975-4172.

[3] KIRSCH, Brian. Server virtualization trends and predictions for 2015. *TechTarget* [online]. 2014. [cit. 2015-10-27]. Dostupné z: http://searchservervirtualization.techtarget.com/feature/Server-virtualization-trends-and-predictions-for-2015

[4] PEREZ, Ronald, Leendert VAN DOORN a Reiner SAILER. Virtualization and Hardware-Based Security. *IEEE Internet Computing*. 2008, **6**(5), 24-31. DOI: 10.1109/MSP.2008.135. ISSN 1540-7993. Dostupné také z: http://ieeexplore.ieee.org/document/4639019/

[5] GOLDEN, Bernard. *Virtualization for dummies (R)*. Hoboken (NJ): John Wiley & Sons, 2008. ISBN 9780470148310.

[6] GOUDA, K C, Anurag PATRO, Dines DWIVEDI a Nagaraj BHAT. Virtualization Approaches in Cloud Computing. *International Journal of Computer Trends and Technology*. 2014, **12**(4), 161-166. DOI: 10.14445/22312803/IJCTT-V12P132. ISSN 22312803. Dostupné také z: http://www.ijcttjournal.org/archives/ijctt-v12p132

[7] RUEST, Danielle a Nelson RUEST. *Virtualizace: podrobný průvodce*. Brno: Computer Press, 2010. ISBN 978-80-251-2676-9.

[8] KELBLEY, John a Mike STERLING. *Microsoft Windows Server 2008 R2 Hyper-V: podrobný průvodce administrátora*. Brno: Computer Press, 2011. ISBN 978-80-251-3286-9.

[9] ERL, Thomas, Zaigham MAHMOOD a Ricardo PUTTINI. *Cloud Computing: Concepts, Technology & Architecture*. Upper Saddle River (NJ): Prentice Hall, 2013. ISBN 9780133387568.

[10] FURHT, Borko a Armando ESCALANTE. *Handbook of Cloud Computing*. New York City (NY): Springer Publishing, 2010. ISBN 978-1-4419-6523-3.

[11] MELL, Peter a Timothy GRANCE. *The NIST Definition of Cloud Computing*. National Institute of Standards and Technology, 2011. Dostupné z https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

[12] KAVIS, Michael. *Architecting the Cloud*. Hoboken (NJ): John Wiley & Sons, 2014. ISBN 978-1-118-61761-8.

[13] HURWITZ Judith, Marcia KAUFMAN a Fern HALPER. *Cloud Services for Dummies*. Hoboken (NJ): John Wiley & Sons, 2012. ISBN 978-1-118-33891-9.

[14] KULKARNI, Gurudatt, Ramesh SUTAR a Jayant GAMBHIR. Cloud Computing-Storage as Service. *International Journal of Engineering Research and Applications* 2012, **2**(1), 945-950. ISSN: 2248-9622.

[15] SHARMA, Kruti a Kavita SINGH. Online Data Back-up and Disaster Recovery Techniques in Cloud Computing: A Review. *International Journal of Engineering and Innovative Technology*. 2012, **5**(2), 249-254.

[16] SROCZKOWSKI, Piotr. *Cloud: IaaS vs PaaS vs SaaS vs DaaS vs FaaS vs DBaaS* [online]. 2018. Dostupné z https://brainhub.eu/blog/cloud-architecture-saas-faas-xaas/

[17] MATHER, Tim, Subra KUMARASWAMY a Shahed LATIF. *Cloud Security and Privacy*. Sebastopol (CA): O'Reilly Books, 2009. ISBN: 978-0-596-80276-9.

[18] WELDON, L. S. J. Knowledge Sharing Through MS SharePoint. *Collaborative Librarianship*. 2012, **4**(1), 23-30. Dostupné také z https://digitalcommons.du.edu/cgi/viewcontent.cgi?article=1185&context=collaborativelibrarianship

[19] LONDER, Olga M. a Penelope COVENTRY. *Microsoft SharePoint 2013 Step by Step*. London: Microsoft Press, 2013. ISBN 978-0-7356-6703-7.

[20] GAILE, Brandon. *12 Sharepoint Pros and Cons* [online], 2015. Dostupné z https://brandongaille.com/12-sharepoint-pros-and-cons/

[21] 3rd ECHELON. Jitter calculator. Dostupné z http://www.3rdechelon.net/jittercalc.asp

8 SEZNAM POUŽITÝCH TABULEK A OBRÁZKŮ

9 SEZNAM POUŽITÝCH ZKRATEK

AD	Active Directory
API	Application Programming Interface
BaaS	Backend as a Service
BGP	Border Gateway Protocol
CAL	Client Access Licenses
CP/CMS	Control Program/Camgridge Monitor System
CRM	Customer Relationship Management
DDOS	Distributed Denial of Service
DNS	Domain Name System
DOS	Denial of Service
ERP	Enterprise Resource Planning
I/O	Input/Output
IaaS	Infrastructure as a Service
IAM	Identity Access Management
JVM	Java Virtual Machine
NIST	National Institute of Standards and Technology
OWA	Outlook Web Access
PaaS	Platform as a Service
SaaS	Software as a Service
SBS	Small Business Server
SCOM	System Center Operations Manager
SLA	Service Level Agreement
SSO	Single sign on
StaaS	Storage as a Service
VM	Virtual Machine
VPN	Virtual Private Network