Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Třívrstvá architektura a migrace aplikací v rámci veřejného cloudu

Bc. Glib Kushnir

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Glib Kushnir

Systémové inženýrství a informatika
Informatika

Název práce

Třívrstvá architektura a migrace aplikací v rámci veřejného cloudu

Název anglicky

Three-tier architecture and application migration to the public cloud

---

Cíle práce

Hlavním cílem je demonstrovat a ověřit možnosti migrace aplikací s třívrstvou architekturou do veřejného cloudu.

Dílčí cíle:
• Představit charakteristiky třívrstvové architektury
• Definovat charakteristiky Cloud computing
• Porovnat existující cloudové platformy
• Představit migrační modely do cloudu
• Demonstrace migrace na reálném prostředí
• Závěrem uvést doporučení při migrace

Metodika

Metodika teoretického hlediska diplomové práce je založena na sběru, studiu a analýze odborných zdrojů. V teoretické časti jsou představené charakteristiky vícevrstvové architektury a cloud computingu, které slouží základem pro praktickou část. Dále práce obsahuje metodiku vytvořeni pravidel pro hodnoceni cloudových platforem a migračních modelů. V praktické časti je demonstrována migrace zvolené aplikace na reálném prostředí u vybraného poskytovatele cloudových služeb. V závěrečné části na podkladě dosažených výsledků jsou formulované doporučeni vyplývající ze zpracované diplomové práce.

Doporučený rozsah práce

60 – 80 stran

Klíčová slova

Cloud computing, vícevrstvová architektura, migrace, veřejný cloud, migrační náklady, infrastruktura

Doporučené zdroje informací

EEL, T.; PUTTINI, R.; MAHMOOD, Z.: Cloud Computing: Concepts, Technology & Architecture, 2013. ISBN 978-01-333-8752-0.

LASZEWSKI T.: Cloud Native Architectures: Design high-availability and cost-effective applications for the cloud, 2018. ISBN 978-1-78728-054-0.

MANJUNATH G.; SITARAM D.: Moving to the Cloud Developing Apps in the New World of Cloud Computing, 2012. ISBN 978-1-59749-725-1.

ROUTREE D.; CASTRILLO I.: The Basics of Cloud Computing: Understanding the Fundamentals of Cloud Computing in Theory and Practice, 2013. ISBN 978-01-240-5932-0.

Předběžný termín obhajoby

2019/20 LS – PEF

Vedoucí práce

Ing. Jiří Vaněk, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 8. 5. 2019

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 14. 10. 2019

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 05. 04. 2020

Čestné prohlášení

Prohlašuji, že svou diplomovou práci „Třívrstvá architektura a migrace aplikací v rámci veřejného cloudu" jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 05.04.2020 _____

Poděkování

Rád bych touto cestou poděkoval Ing. Jiřímu Vaňkovi, Ph.D., za odborné rady při zpracování této diplomové práce.

Třívrstvá architektura a migrace aplikací v rámci veřejného cloudu

Abstrakt

Předmětem této diplomové práce je demonstrace a ověření možnosti migrace v rámci veřejného cloudu na příkladu jednoduché aplikace, která má třívrstvou architekturu. Práce se skládá ze dvou částí. V první, teoretické části jsou představeny charakteristiky vícevrstvé architektury, uvedeny základní principy, na kterých jsou postavené mikroslužby (microservises) a popsán je koncept cloud computingu, které dále slouží jako základ pro praktickou část. Druhá část práce obsahuje metodiku vytvoření pravidel pro hodnocení cloudových platforem a migračních modelů. V praktické části je demonstrována migrace zvolené aplikace na reálném prostředí u vybraného poskytovatele cloudových služeb. V závěrečné části jsou na podkladě dosažených výsledků formulovaná doporučení vyplývající ze zpracované diplomové práce.

Klíčová slova: Cloud computing, vícevrstvá architektura, migrace, veřejný cloud, migrační náklady, infrastruktura

Three-tier architecture and application migration to the public cloud

Abstract

The aim of this thesis is to demonstrate and verify the possibility of migration within the public cloud based on a simple application that has a three-layer architecture. The thesis consists of two parts. The first theoretical part introduced characteristics of multilayer architecture, basic principles for microservises and described a concept of cloud computing, which further serves as a basis for the practical part. The second part contains the methodology of creating rules for evaluating cloud platforms and migration models. The practical part demonstrates the migration of the selected application in a real environment at a selected cloud service provider. In the final part based on the achieved results there are formulated results and recommendations from the processed diploma thesis.

Keywords: Cloud computing, multitier architecture, migration, public cloud, migration costs, infrastructure

Obsah

Seznam obrázků

Seznam tabulek

1 Úvod

Cloud už dávno není pouze módní slovo, ale mění základy podnikání. Podniky všech velikostí chtějí použít cloud jako prostředek k růstu jednoduchým, ale nákladově efektivním způsobem. Pro udržení stávajících zákazníků a získání nových je zásadní, aby podniky připravovaly své nové aplikace přímo v cloudu, ale otázkou je, jak správně převést již existující.

Mnoho vedoucích pracovníků v oblasti IT se pokouší o migraci do veřejného cloudu v nepřítomnosti prověřené cloudové strategie nebo bez splnění důležitých předpokladů, které vedou k suboptimálním výsledkům nebo přímému selhání. Přestože existují osvědčené postupy pro plánování a provádění veřejných cloudových migrací, každý use-case musí být optimalizován pro každou konkrétní migraci, aby ta proběhla úspěšné.

Cloud má mnoho potenciálních výhod a cloudové infrastruktury sdílejí mnoho, ale ne všechny. Totéž platí o potenciálních výzvách. Navíc vzhledem k rychlému vzniku cloudu během posledního desetiletí existují různé názory na potenciální výzvy a přínosy.

Schopnost určit vhodnost cloudové infrastruktury pro klíčové cíle organizace je zvýšena jasnou definicí a formulací výhod a výzev během migrace do veřejného cloudu. Pravděpodobnost úspěšného využití výhod cloudové infrastruktury se zvyšuje, když byl obchodní případ adekvátně určen a konkrétní výhody byly jasně definovaný.

Zásady využití cloudu by měly doplňovat cloudovou strategii. Mělo by to pomoct podniku rozhodnout, co dělat a proč. Úkolem této diplomové práce je připravit cloudovou strategii pro podnik, který se zvýšením počtů zákazníků trpí problém škálovatelnosti své infrastruktury. Podnik potřebuje spravovat zdroje tak, aby splňovaly požadavky spotřebitelů v průběhu růstu jejich počtů. Kvalitní cloudová strategie znamená důkladné znalosti o již existující infrastruktuře a i implementovaných aplikacích. Podnik musí považovat změny v průběhu migrace jak na straně infrastruktury, tak i na straně samotné aplikace s cílem optimalizace nákladů během migrace. Praktická část této diplomové práce bude obsahovat příklad zhodnocení všech potřebných informací pro přípravu cloudové strategie, která pak poskytne kvalitní metodiku při migraci aplikací do veřejného cloudu.

2 Cíl práce a metodika

2.1 Cíl práce

Hlavním cílem je demonstrovat a ověřit možnosti migrace aplikací s třívrstvou architekturou do veřejného cloudu.

Dílčí cíle:

- Představit charakteristiky třívrstvé architektury;
- Definovat charakteristiky cloud computingu;
- Porovnat existující cloudové platformy;
- Představit migrační modely do cloudu;
- Demonstrace migrace na reálném prostředí;
- Závěrem uvést doporučení pro migraci?

2.2 Metodika

Metodika teoretického hlediska diplomové práce je založena na sběru, studiu a analýze odborných zdrojů. V teoretické části jsou představeny charakteristiky vícevrstvé architektury a cloud computing, které slouží jako základ pro praktickou část. Dále práce obsahuje metodiku vytvoření pravidel pro hodnocení cloudových platforem a migračních modelů. V praktické části je demonstrována migrace zvolené aplikace na reálném prostředí u vybraného poskytovatele cloudových služeb. V závěrečné části jsou na podkladě dosažených výsledků formulovaná doporučení vyplývající ze zpracované diplomové práce.

3 Teoretická východiska

3.1 Cloud computing

Cloud computing představuje výhodnou nabídku, která se liší od tradičních podnikových IT prostředí. Pomocí současných technologií, jako jsou virtualizace, aplikační kontejnery a serverless computing[1], které agregují a sdílejí výpočetní prostředky, může cloud computing nabídnout úspory z rozsahu, které by jinak nebyly dostupné. Díky minimální počáteční investici umožňuje cloud computing globální dosah služeb a informací prostřednictvím elastického prostředí výpočetní techniky, které podporuje škálovatelnost na vyžádání. Cloudy také přebírají otevřené standardy, škálovatelné schéma a architekturu orientovanou na služby (SOA) a také představují flexibilní řešení na vyžádání flexibilním nebo finančním způsobem.

Podle Amerického národního institutu pro standardy a technologie je cloud computing model umožňující všudypřítomný, pohodlný přístup vyžádání ke sdíleným, konfigurovatelným výpočetním zdrojům (např. sítě, servery, úložiště, aplikace a služby), které lze rychle zajistit a odstranit s minimálním úsilím a bez interakce poskytovatele [1]. Tento cloudový model se skládá z pěti základních charakteristik, tří modelů služeb a čtyř modelů nasazení.

Mezi 5 charakteristik patří:

Samoobslužné služby na vyžádání

Spotřebitel výpočetních zdrojů může jednostranně spravovat výpočetní funkce, jako je čas serveru a síťové úložiště, podle potřeby automaticky nebo s minimální interakcí poskytovatelem cloudových služeb. Zaměření této vlastnosti je, že cloud computing nabízí uživatelům relativní snížení nákladů, času a úsilí potřebného k provedení akce, protože poskytuje uživateli schopnost dělat to, co potřebují, kdykoli to potřebují, aniž by to vyžadovalo další uživatelské interakce nebo režie.

[1] Serverless computing – je model provádění cloudových výpočtů, ve kterém poskytovatel cloudu provozuje server a dynamicky řídí přidělování strojních prostředků.

Přístup přes internet

Funkce, kde jsou fyzické a virtuální zdroje dostupné prostřednictvím sítě a jsou přístupné prostřednictvím standardních mechanismů, které podporují použití heterogenními klientskými platformami [1]. Tato klíčová charakteristika je zaměřena na to, že cloud computing nabízí zvýšenou úroveň pohodlí v tom, že uživatelé mohou přistupovat k fyzickým a virtuálním zdrojům odkudkoli, pokud je stroj přístupný z internetu, a používají širokou škálu klientů včetně zařízení, jako jsou mobilní telefony, tablety a notebooky.

Multitenancy

To je funkce, při které jsou fyzické nebo virtuální zdroje přidělovány tak, že uživatelé a jejich výpočty a data jsou od sebe izolované a navzájem nepřístupné. Skupina uživatelů cloudových služeb, kteří tvoří nájemce, obvykle patří do stejné organizace zákazníků cloudových služeb. Mohou nastat případy, kdy skupina uživatelů cloudových služeb zahrnuje uživatele z více různých zákazníků cloudových služeb, zejména v případě veřejného cloudového a komunitního cloudového nasazení. Avšak daná zákaznická organizace cloudových služeb může mít mnoho různých vztahů s jediným poskytovatelem cloudových služeb zastupujícím různé skupiny v organizaci.

Škálovatelnost a elasticita

Funkce cloudu, kde lze fyzické a virtuální zdroje rychle a pružně upravit, v některých případech automaticky, za účelem rychlého zvýšení nebo snížení počtů zdrojů. Pro zákazníka cloudových služeb jsou fyzické nebo virtuální zdroje k dispozici většinou v neomezeném počtu a lze je kdykoli zakoupit v jakémkoli množství automaticky, bez žádných smluvních omezení. Zaměření této klíčové vlastnosti je, že zákazníci se nemusí starat o plánování kapacit a omezení výpočetních prostředků.

Shromažďování zdrojů

Funkce, kde fyzické nebo virtuální zdroje jsou použité jedním nebo více zákazníky cloudových služeb. Tato klíčová charakteristika je zaměřena na to, že poskytovatelé cloudových služeb mohou podporovat multitenancy a zároveň pomocí abstrakce maskovat před zákazníkem složitost procesu. Zákazníci pouze vědí, že služba funguje a obecně nemají žádnou kontrolu ani znalosti o tom, jak jsou zdroje poskytovány nebo

kde jsou tyto zdroje umístěny. Tím se zbaví část původního pracovního zatížení zákazníka, například náklady na údržbu. I při této úrovni abstrakce by mělo být zdůrazněno, že uživatelé stále mohou určit polohu na vyšší úrovni abstrakce (např. země, stát nebo datové centrum).

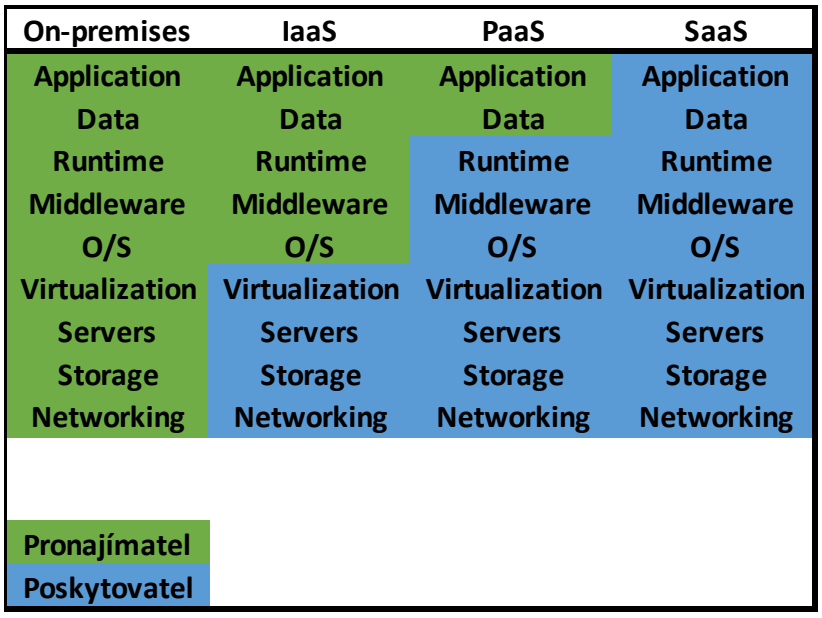
Měřená služba

To je vlastnost, při které využití zdrojů lze sledovat, kontrolovat, vykazovat a fakturovat. Toto je důležitá funkce potřebná k optimalizaci a ověření doručené cloudové služby. Zaměření této klíčové vlastnosti je, že zákazník může platit pouze za zdroje, které používá. Z pohledu zákazníka umožňuje cloud computing přechod od obchodního modelu s nízkou účinností a neefektivním využitím výpočetních zdrojů k vysoce efektivnímu modelu.

3.1.1 Distribuční modely

Existují 3 modely cloudových služeb, často označované jako „SPI model“, tj. software, platforma nebo infrastruktura jako služba. SPI model popisuje rozdělení zodpovědnosti během poskytování služeb mezi poskytovatelem cloudových služeb (CSP) a zákazníkem.

Obrázek 1 Rozdělení odpovědnosti v cloudu



Zdroj: vlastní zpracování

3.1.1.1 Infrastructure as a Service (IaaS)

Systém IaaS umožňuje zákazníkům získat prostředky bez skutečného nákupu hardwaru. Tento přístup má potenciál eliminovat kapitálové výdaje. Tržiště IaaS rychle dozrálo a desítky poskytovatelů zvládnou téměř jakoukoliv potřebu. Poskytuje online zpracování nebo kapacitu pro ukládání dat. Tato cloudová služba je ideální pro podniky zvažující velké, jednorázové zpracovatelské projekty nebo občasné, extrémně velké požadavky na ukládání dat (tj. testovací prostředí). IaaS nabízí schopnost poskytovat zpracování, úložiště, sítě a další základní výpočetní zdroje, což zákazníkovi umožňuje nasazení a provoz libovolného softwaru, který může zahrnovat OS a aplikace.

Zatímco mnoho organizací dnes používá virtualizaci ke konsolidaci svých IT infrastruktur, hardwarová konsolidace je pouze jednou výhodou virtualizace. Organizace, které se přesouvají na virtualizaci pomocí funkcí IaaS, mohou mít významné výhody:

- Snížení provozních nákladů IT a kapitálových nákladů zlepšením využití zdrojů a poměrů mezi správci a servery.
- Rychlejší uvedení produktu na trh díky vyšší účinnosti a automatizaci standardizovaných řešení.
- Zjednodušená, integrovaná správa, včetně monitorování v reálném čase.
- Větší viditelnost obchodních procesů a výkonu systému za účelem identifikace propouštění.
- Škálované operace, které mohou splňovat dynamiku trhu a obchodní strategii.

3.1.1.2 Platform as a Service (PaaS)

Model PaaS mohou využívat organizace, které chtějí vyvíjet nové softwarové aplikace, aniž by museli pořizovat a instalovat hardware a operační systém. Poskytuje také přístup k různým novým a inovativním službám, jako jsou rozpoznávání obličeje, internet věcí a umělá inteligence.

Poskytuje prostředí pro vývoj aplikací v cloudu. PaaS poskytuje schopnost nasazovat aplikace vytvořené zákazníkem nebo získané na základě vývojových jazyků a nástrojů nabízených poskytovatelem. CSP nabízí vývojářům organizací elementární architekturu orientovanou na služby (SOA) pro konfiguraci nové obchodní aplikace. Vlastní vývoj vyžaduje vývojové, testovací a akceptační platformy uživatelů, všechny oddělené

od produkčního prostředí. Prostřednictvím PaaS si mohou vývojáři organizací pronajmout své vývojové prostředí kompletní se sadou nástrojů SOA a jsou účtovány pouze za dobu, kdy jsou nástroje a prostředí používány [2].

Pobídky organizace k přechodu do prostředí PaaS se liší v závislosti na velikosti a IT zralosti organizace. Pro velké organizace je klíčovou motivací ke zvažování PaaS schopnost rychle a levně vyvíjet a nasazovat nové aplikace. Velké organizace mají další pobídky k tomu, aby zvážili přechod na PaaS:

- Vysoce standardizované a automatizované zajišťování předdefinovaných pracovních zatížení.
- Integrovaná vývojová a runtime platforma pro konkrétní pracovní vytížení.
- Konzistentní nasazení založená na vzorech pro nejběžnější pracovní zatížení.
- Silná podpora cloudových nativních aplikací, včetně technologií, jako jsou kontejnery, serverless computing a microservices.

3.1.1.3 Software as a Service (SaaS)

SaaS je nejčastěji používanou cloudovou službou. Se SaaS společnosti platí za hotové aplikace na základě předplatného. SaaS nabízí zákazníkům použití aplikací běžících na cloudové infrastruktuře vytvořené poskytovatelem cloudových služeb (CSP). Služby jsou dostupné z různých klientských zařízení, jako je webový prohlížeč (např. webový e-mail) nebo programové rozhraní. Příklady populárních zákaznických aplikací SaaS jsou Facebook, g-mail, uživatelské aplikace Yahoo, Google Documets a Microsoft Office 365.

Spotřebitelé nemusí spravovat ani řídit základní cloudovou infrastrukturu, včetně sítě, serverů, operačních systémů, úložiště nebo dokonce jednotlivých funkcí aplikace, s možnou výjimkou omezených nastavení konfigurace aplikací specifických pro uživatele [2].

SaaS poskytuje podnikům úplnou svobodu v řízení IT infrastruktury a celého softwarového balíčku, který jim umožňuje soustředit se na využívání funkcí služby k dosažení jejich obchodních cílů. Obchodní řešení implementovaná jako cloudové služby poskytují zákazníkům flexibilitu při výběru přístupu, který je pro jejich společnost

nejlepší, a umožňují tak v cloudu spotřebovat a provádět obchodní procesy, analýzy a aplikace.

SaaS má následující klíčové vlastnosti:

- Nabídky SaaS jsou přístupné přes internet, což velmi usnadňuje jejich zveřejnění v co nejkratší době velkému publiku.
- SaaS pracuje na cenovém modelu založeném na využití, který umožňuje podnikům předplatit pouze ty služby, které potřebuje, a pro požadovaný počet uživatelů.
- SaaS obvykle nabízí standardní sadu funkcí, která umožňuje určitou úroveň konfigurace pro jednotlivé zákazníky, ale obvykle žádné přizpůsobení.
- Organizace mohou snížit své kapitálové výdaje (CapEx) na pořízení softwarových licencí přijetím nabídek SaaS na základě předplatného.

3.1.2 **Způsoby nasazení**

Modely nasazení obecně charakterizují dispozice výpočetních zdrojů pro poskytování služeb spotřebitelům, jakož i rozlišení mezi třídami spotřebitelů. Existují tři běžně používané modely nasazení cloudu: soukromé, veřejné a hybridní. Dalším modelem je komunitní cloud, který se používá méně často, ale třeba je velmi populární v Číně, kde jsou přísná pravidla na přenos dat uvnitř zemí.

3.1.2.1 Veřejný cloud (Public cloud)

Představuje nabídku od jednoho CSP pro mnoho klientů, kteří sdílejí výkon cloudového zpracování současně. Veřejní cloudoví klienti sdílejí aplikace, výpočetní výkon a prostor pro ukládání dat. Klientská data se mísí, ale segregace je zajištěna pomocí metaznaček [2].

Gartner definuje veřejný cloud computing jako styl výpočetní techniky, kde jsou škálovatelné a elastické funkce podporované IT poskytovány jako služba externím zákazníkům využívajícím internetové technologie [3]. Veřejný cloud využívá technologie k podpoře zákazníků, kteří jsou externí vůči organizaci poskytovatele. Používání veřejných cloudových služeb generuje typy úspor z rozsahu a sdílení zdrojů, které mohou snížit náklady a zvýšit výběr technologií. Z pohledu vládní organizace znamená použití veřejných cloudových služeb, že jakákoliv organizace (v jakémkoli průmyslovém odvětví

a jurisdikci) může používat stejné služby (např. infrastruktura, platforma nebo software) bez záruk, kde by byla data umístěna a uložena.

Ve veřejných cloudech se zdroje nabízí jako služba. Uživatelé mohou měnit své potřeby na požádání a nemusí kvůli tomu nakupovat hardware. Poskytovatelé veřejného cloudu spravují infrastrukturu a rozdělují ji podle kapacitních požadavků uživatelů.

U veřejného modelu mají zákazníci omezenou viditelnost a kontrolu nad informacemi o bezpečnosti. Podrobnosti o fungování systému poskytovatele jsou obvykle považovány za proprietární a nejsou k dispozici ke kontrole zákazníky. Certifikace cloudových služeb může zákazníkům poskytnout jistotu.

3.1.2.2 Soukromý cloud (Private cloud)

Uživatelem je pouze jeden podnik. Může být zastoupeno několik různých oddělení nebo divizí, ale všechny existují ve stejném podniku. Soukromé cloudové systémy často využívají virtualizaci na stávajících počítačových serverech podniku, aby se zlepšilo využití počítače. Soukromý cloud obvykle zahrnuje také zajišťování a měření komponent, umožňující rychlé nasazení a případné zpětné zúčtování. Tento model úzce souvisí s existujícími modely outsourcingu IT na trhu, ale může se jednat také o model interní dodávky podniku [2].

Soukromý cloud je vhodný pro kritické aplikace a služby citlivé na dodržování předpisů, nezbytných pro kontinuitu podnikání. Dostupnost kritických dat je klíčem k rozhodnutí, zda zachovat pracovní vytížení na místě.

U modelu soukromého nasazení může instalace a správa cloudového softwaru způsobit značné náklady na cloudový software, i když v rámci spotřebitelské organizace existuje nepřidělený hardware. Výdaje mohou být zmírněny, pokud organizace přijala prostředí architektury orientované na služby a přesune se do vzorce výdajů pro interní oddělení.

U privátních cloudů jsou k dispozici omezené zdroje, protože výpočetní a úložná kapacita je pevná a byla přizpůsobena očekávaným pracovním zatížením a omezením nákladů. Pokud je organizace dostatečně velká, může být schopna poskytnout zákazníkům dostatečnou pružnost v rámci spotřebitelské organizace.

U privátních cloudů mají spotřebitelé možnost implementovat vhodně silnou bezpečnost, aby chránili zdroje před vnějšími hrozbami na stejné úrovni zabezpečení, jaké lze dosáhnout u jiných zdrojů než cloud.

3.1.2.3 Hybridní cloud (Hybrid cloud)

Kombinace dvou nebo více výše uvedených modelů rozmístění. Každý ze tří modelů nasazení cloudu má oproti ostatním modelům nasazení specifické výhody a nevýhody. Hybridní cloud využívá výhody ostatních cloudových modelů a poskytuje tak optimální uživatelský dojem.

Architektura hybridního cloudu vyžaduje mít cloudovou infrastrukturu přímo v prostorách organizace a zároveň servery umístěné jinde. Je možné ji implementovat různými způsoby. Organizace může mít například data a aplikace umístěné v cloudu, který zachovává kontrolu nad topologií sítě organizace a její vnitřní politikou. Zároveň si může zachovat existující fyzickou infrastrukturu (ačkoli ta se nedá dynamicky měnit) a půjčovat si další zdroje podle potřeby.

Hybridní nasazení pomáhají využívat funkce veřejného cloudu pro určité nekritické pracovní zátěže a současně zachovávají podnikově důležitá data a aplikace. Příkladem je prasknutí klíčových obchodních kapacit na místě během sezónního nárůstu; replikace vybraných informací o zákaznících do lehké cloudové databáze pro rychlejší přístup mobilními aplikacemi je další.

Organizace využívající hybridní nasazení se mohou rozhodnout omezit druh dat/služeb, které jsou vystaveny veřejnosti, a pomáhat tak zmírňovat hrozby.

3.1.2.4 Komunitní cloud (Community cloud)

Soukromý a veřejný cloud jsou řešení pro uživatele, kteří mají společné připojení nebo přidružení, jako jsou obchodní sdružení, stejné odvětví nebo společná lokalita. Obchodní model umožňuje CSP poskytovat cloudové nástroje a aplikace specifické pro potřeby komunity.

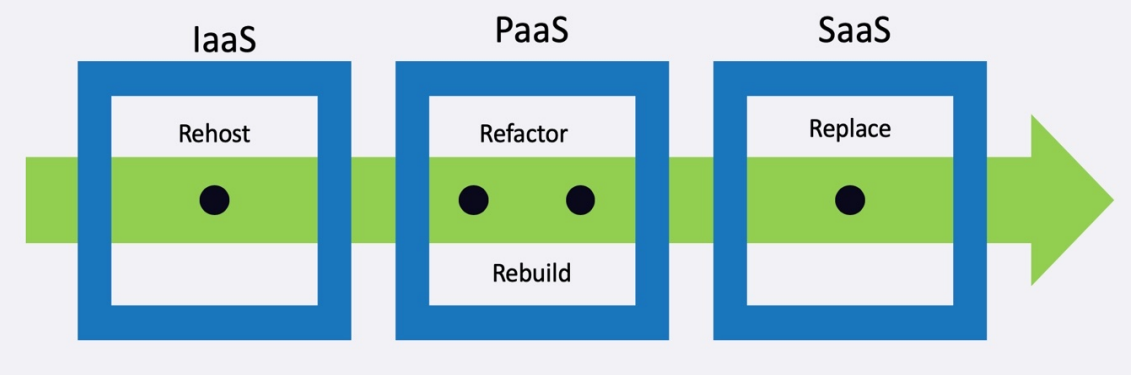
Náklady jsou rozloženy mezi menší počet uživatelů než u veřejného cloudu (ale větší než u privátního cloudu). Potenciál úspor nákladů tedy není tak vysoký. Cloud mohou spravovat přímo organizace nebo třetí strana a umístěn může být v prostorách organizace nebo mimo ni.

Výhody bezpečnosti v prostředí komunitního cloudu využívají například vládní, zdravotnické nebo telekomunikační komunity organizací, ale též regulované soukromé podniky. Místo pouhého využívání prostoru ve veřejném cloudu mohou organizace testovat a pracovat v cloudové platformě, která je bezpečná, vyhrazená pouze pro ně, a dokonce splňuje specifické předpisy.

3.1.3 **Cloudové migrační strategie**

Dobře promyšlená migrační strategie se schopností poskytovat efektivní cloudová řešení je pro organizaci velmi důležitá. „5R cloudové migrace“ od společnosti Gartner jsou skvělým místem pro začátek při zvažování všech možností migrace aplikací do cloudu.

Obrázek 2 Migrační strategie



Zdroj: vlastní zpracování

3.1.3.1 Rehost

Rehosting je proces přesunu stávajících fyzických a virtuálních serverů do řešení založeného na infrastruktuře jako služba (IaaS). Klíčovou výhodou tohoto přístupu, který se také nazývá „Lift and shift“ („výtah a posun“), je, že systémy lze rychle migrovat beze změny jejich architektury. To je často cesta, kterou společnosti podniknou, když jsou v cloud computingu nové. Při rehostingu s cloudem v zásadě zacházíte jako s jiným datovým centrem, což znamená, že z dostupných cloudových služeb nevyužíváte maximum.

3.1.3.2 Refactor

Toto je proces spouštění aplikací na infrastruktuře poskytovatele cloudu, také nazývaný platforma jako služba (PaaS). PaaS znamená, že vývojáři jsou schopni znovu použít rámce, jazyky a kontejnery, do nichž již investovali. U aplikací nebo pracovních zátěží, které lze refaktorovat za účelem využití cloudových schopností, budete moci využít některé funkce nativního cloudu nabízené infrastrukturou PaaS za snížené náklady a zvýšenou škálovatelnost. Největší nevýhody této možnosti však zahrnují přechodné riziko, chybějící schopnosti a zablokování rámce. Jedním z běžných problémů, se kterým se vývojáři potýkají, je to, že mnoho možností PaaS používá pomíjivé úložiště. To obvykle vyžaduje změnu kódové základny pro použití cloudového úložiště namísto místního systému souborů pro uložené soubory.

3.1.3.3 Rearchitect

Některé aplikace budou muset být více upraveny, aby byly migrovány do cloudu. Některé budou vyžadovat přidanou funkčnost, zatímco jiné možná budou muset být kompletně přepracované, než budou moci být rehostovány nebo přepracovány a nakonec nasazeny do cloudu.

To může být obtížná volba, protože úprava velké kódové základny tak, aby se stala více domorodcem v cloudu, může být časově náročná a nákladná. Příkladem by bylo vzít komplexní monolitickou aplikaci založenou na Pythonu a přenést ji do Google App Engine. Návrh aplikace určí množství změn, které budou implementované. Existuje možnost, že pak bude potřeba je rozdělit do více aplikací a vyměnit některé komponenty.

3.1.3.4 Rebuild

V tomto scénáři se aplikace přeprogramuje, původní kódování se zahodí a znovu se vytvoří na infrastruktuře PaaS. Opětovné sestavení aplikace umožní využít pokročilejších a inovativních funkcí od poskytovatele cloudu a vylepšit tak existující aplikaci. Hlavní nevýhodou této možnosti je lock-in (uzamčení) dodavatele.

Pokud například poskytovatel provede technickou změnu nebo změnu cen, kterou zákazník nemůže přijmout, nebo která poruší dohodu o úrovni služeb (SLA), může být zákazník nucen přejít zpět k předchozí aplikaci a potenciálně ztratit některé, nebo všechny své aplikační prostředky.

3.1.3.5 Replace

V tomto scénáři zcela nahrazuje existující aplikace aplikací dodávaným jako služba (SaaS). Výhodou modelu nahrazení je to, že umožňuje vyhnout se nákladům na vývoj IT. Můžeme se však setkat s problémy s přístupem k datům, s nepředvídatelnou sémantikou dat a s uzamčením dodavatele.

3.1.4 **Poskytovatele**

Dnes existuje celá řada poskytovatelů cloudových služeb a rozhodující je i výběr správných služeb pro technické a obchodní potřeby organizace. Někteří odborníci tvrdí, že cloud je komodita a že cena je jediným významným faktorem. Ostatní jsou silně proti této myšlence a zjišťují, že funkce a konfigurace služeb se velmi liší, a to i mezi předními poskytovateli na trhu. Například různí poskytovatelé nabízejí mnoho druhů konfigurací zabezpečení a správy a často tíhnou ke kompatibilitě s určitými softwarovými platformami místního prostředí pro hybridní cloudové aktivace. Takové sklony poskytovatele mohou přilákat různé skupiny zákazníků. Paritní služba by se však nikdy neměla předpokládat. Proto bude pro organizace koncových uživatelů zásadní, aby identifikovaly své kritické požadavky a zmapovaly je na schopnosti potenciálních poskytovatelů.

Cloud computing IaaS představuje největší segment trhu cloudu (širší trh IaaS zahrnuje také cloudové úložiště). Společnost Gartner každý rok připravuje takzvané Magic Quadranty, který hodnotí různé oblasti IT, a zároveň existuje Magic Quadrant poskytovatelů služeb IaaS. Tento magický Magic Quadrant pokrývá všechny běžné případy použití cloudových IaaS, včetně vývojářství a testování, produkční prostředí (včetně těch, která podporují kritickou pracovní zátěž) pro interní aplikace i aplikace orientované na zákazníka, dávkové výpočty (včetně vysoce výkonných počítačových [HPC]) a Disaster Recovery[2]. Zahrnuje nejen hostování jednorázových pracovních zátěží, ale také nahrazení tradičních podnikových datových center cloudovými prostředími, která mohou podporovat velmi různorodou škálu pracovních zátěží. Zahrnuje vhodnost pro širokou škálu vzorů návrhů aplikací, včetně cloudových nativních aplikací, webových aplikací a starších podnikových aplikací. Tento Magic Quadrant vyhodnocuje všechna cloudová řešení IaaS u všech typu nasazení.

[2] Disaster recovery – postupy pro zajištění obnovy IT služeb po živelných pohromách a jiných zásadních událostech.

Obrázek 3 Magic Quadrant pro IaaS

Zdroj: Gartner ©

Popis všech hráčů na trhu není cílem této práce, proto dále budou charakterizovány pouze poskytovatele, které patří do skupiny „Leaders“.

3.1.4.1 Microsoft Azure

Microsoft je velký a diverzifikovaný dodavatel technologií, který se stále více zaměřuje na poskytování svých softwarových možností prostřednictvím cloudových služeb. Její podnikání v Azure bylo zpočátku přísně PaaS, ale Microsoft vstoupil na cloudový IaaS trh spuštěním Azure Virtual Machines v červnu 2012 (s běžnou dostupností v dubnu 2013).

Možnosti Microsoft Azure se staly inovativnějšími a otevřenějšími, se zlepšenou podporou pro Linux a open-source aplikační balíčky. Kromě toho mnoho zákazníků, kteří

sledují multicloud strategii, bude používat Azure pro některé ze svých pracovních vytížení a software Azure Stack pro on-premise může potenciálně přilákat zákazníky hledající hybridní řešení.

Azure nemá nejlepší spolehlivost ve své třídě, ačkoli se spolehlivost neustále zlepšuje a společnost Microsoft nadále investuje do snižování rušivé údržby. Zákazníci naznačují, že většina problémů spolehlivostí souvisí s virtuálními sítěmi. Většina takových problémů ovlivňuje jednotlivé zákazníky, nikoli region jako celek. Dopad na zákazníka lze snížit pečlivým sledováním a použitím vysoce dostupné architektury.

3.1.4.2 Amazon Web Services

Amazon Web Services (AWS), dceřiná společnost Amazonu, je poskytovatelem cloudových služeb. V roce 2006 byl průkopníkem trhu cloudových služeb IaaS. AWS je dominantním lídrem na trhu a IT leaderem po více než 10 let, a to nejen v IaaS, ale také v integrovaných IaaS + PaaS s výnosem z konce roku 2017 více než 20 miliard USD [4]. Prostřednictvím nových služeb a akvizic pokračuje v agresivní expanzi na nové trhy IT, čímž se přidává k již bohatému portfoliu služeb. Rovněž pokračuje v rozšiřování stávajících služeb o nové funkce se zvláštním důrazem na správu a integraci.

AWS je nejvyspělejším podnikovým poskytovatelem s nejsilnějším záznamem o úspěchu zákazníka a nejužitečnějším partnerským ekosystémem. Je to tedy poskytovatel, který si zákazníci nejen vyberou, a které oceňují inovace a realizují digitální obchodní projekty, ale také preferují zákazníci, kteří migrují tradiční datová centra do cloudu IaaS. Může snadno podporovat kritické produkční aplikace a implementaci vysoce bezpečných a kompatibilních řešení. Implementaci, migraci a správu výrazně usnadňuje ekosystém AWS s více než 2 000 poradenskými partnery, kteří nabízejí řízené a profesionální služby. Společnost AWS má nejširší ekosystém poskytovatelů služeb ISV v cloudu, který zajišťuje, že zákazníci jsou schopni získat podporu a licence pro většinu komerčního softwaru a také získat softwarová a SaaS řešení, která jsou předběžně integrována do AWS.

AWS se stále přizpůsobuje vzniku konkurentů – nejen poskytovatelů cloudových služeb, ale také zavedených konkurentů na nových trzích, na něž vstupuje se službami, které vytlačují stávající řešení. Protože společnost AWS zavádí více služeb kompatibilních s otevřeným zdrojovým kódem, stále více potřebovala pracovat s open-source komunitami vzájemně prospěšným způsobem a začala odpovídajícím způsobem

měnit svůj přístup. Budoucí technologické volby zákazníků budou pravděpodobně ovlivněny ekosystémovými vztahy AWS.

3.1.4.3 Google cloud provider

Google je internetový poskytovatel technologií a služeb. Společnost Google poskytuje nabídku PaaS od roku 2008, ale na trh cloudových služeb IaaS vstoupila až poté, co byl v červnu 2012 spuštěn program Google Compute Engine (s běžnou dostupností v prosinci 2013).

Strategie společnosti Google pro GCP se zaměřuje na komercializaci interních inovativních technologických funkcí, které Google vyvinul pro provozování svého spotřebitelského podnikání v měřítku, a na jejich zpřístupnění jako služby, kterou mohou ostatní společnosti koupit. Plán možností společnosti Google se stále více zaměřuje na zákazníky s tradičními pracovními zátěžemi a procesy IT a také s cloudovými nativními aplikacemi. Google se umístil jako „otevřený“ poskytovatel s důrazem na přenositelnost, který je zaměřen na ekosystémy s otevřeným zdrojovým kódem. Stejně jako jeho konkurenti však Google přináší hodnotu prostřednictvím automatizace operací v měřítku a tyto vlastní výhody neposkytuje open source.

Společnost GCP se sama o sobě řadí do pozice lídra nákladů na trhu, její nejhlubší sjednané slevy jsou však obvykle omezeny na jednoletou smlouvu. Zákazníci, kteří hodnotí konkurenční náklady, by měli oddělit standardní slevy (závazné a trvalé použití) od sjednaných podnikových slev a měli by si být vědomi, že slevy GCP jsou spíše za službu než za celkovou smlouvu. Google je často rigidní při vyjednávání smluv, s výjimkou největších zákazníků, kteří mohou získat mimořádnou flexibilitu. Její prodejní síla, i když je technicky zběhlá, má často omezené zkušenosti s organizací pro zadávání zakázek.

3.2 Modely aplikační architektury

Aplikační architektury se neustále vyvíjejí, přizpůsobují se novým požadavkům a využívají nové technologie. Nejprůhlednější modely jsou modely klient/server a n-tier, které odkazují na to, jak aplikace využívají funkční prvky komunikační výměny. Model klient/server se ve skutečnosti vyvinul na n-tierový model, který většina prodejců podnikových softwarových aplikací v poslední době používají nejvíce v aplikačních

architekturách. Během dalších několika let se model třívrstvé architektury stal přímou evolucí z dnešního pohledu již koncepčně zastaralé dvouvrstvé architektury.

Během posledních dvou let se objevil nový přístup k architektuře aplikací: mikroslužby (microservices). Microservice Architecture je vzor pro implementaci obchodní logiky v organizaci pomocí malých jednoúčelových služeb. Tento přístup poskytuje kontrast k tradiční metodě budování monolitických služeb.

Existuje několik důvodů, proč zvolit jeden přístup místo druhého, ale žádný není absolutně lepší, nebo horší než druhý. Tato část představuje modely třívrstvé architektury a vývojové kroky od modelu n-tier k mikroslužbám.

3.2.1 **Vícevrstvá architektura**

Tradiční nebo monolitická aplikace neodděluje uživatelské rozhraní od jeho funkčnosti nebo dat. Obvykle jsou tyto aplikace spravované ručně a fungují jako jeden kus. Díly nejsou zaměnitelné a úpravy jsou často náročné a potřebuje to hodně času. Analogie by byla v době před zaměnitelnými součástmi, kdy byla většina věcí vytvořena ručně. Pokud se část rozbila, musel člověk najít řemeslníka, který by mohl ručně vyrobit jedinečnou náhradu. To způsobilo výrazný odpor v produktivitě. Nástup zaměnitelných součástek způsobil explozivní nárůst průmyslové produktivity.

Aplikace postavené na dvouvrstvé architektuře nemají tendenci se dobře škálovat. Obvykle vyžadují složité zpracování, velké objemy transakcí a častou údržbu.

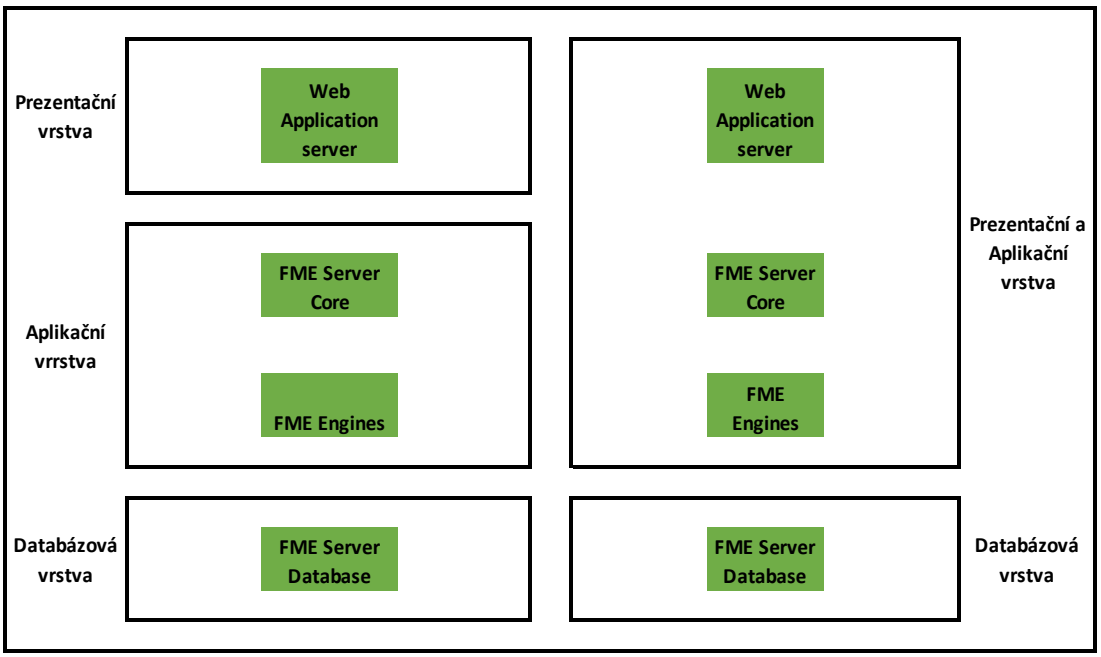
Ke složitosti aplikace se vztahují také složité algoritmy, velké množství objektů nebo velké množství funkcí. Ve většině dvouvrstvých aplikací jsou logika uživatelského rozhraní, logika aplikace a logika přístupu k databázi vzájemně propojeny, nejsou oddělené a modulární. Potenciál pro opakované použití kódu, který poskytuje víceúrovňový objektově orientovaný systém, je do značné míry eliminován a s rostoucí složitostí a velikostí aplikace roste i obtížnost udržovat ji bez chyb.

3.2.1.1 Třívrstvá architektura

Nejzásadnější změny v modelu dvouvrstvé architektury se začaly při webových aplikacích. Webové aplikace se spoléhají na standardnější rozhraní a formáty zpráv, ve kterých je sdílení aplikací snadnější. Přechod z klasického klienta/serveru na webovou architekturu vyžaduje použití tenkých klientů (webových prohlížečů), webových serverů, aplikačních serverů a databázové servery. Webový prohlížeč spolupracuje s webovými

servery a aplikačními servery a webové servery interagují s aplikačními servery a databázovými servery. Tyto odlišné funkce podporované servery jsou označovány jako úrovně, které se kromě úrovně klienta vztahují k modelu n-úrovně (n-tier).

Obrázek 4 Dvou – a třívrstvé architektury



Zdroj: vlastní zpracování

Model n-tier se spoléhá na standardní webovou architekturu, kde webový prohlížeč formátuje a prezentuje informace přijaté z webového serveru. Strana serveru ve webové architektuře se skládá z více a odlišných serverů, které jsou funkčně oddělené. Model n-tier může být klient a webový server; nebo klient, webový server a aplikační server; nebo klientský, webový, aplikační a databázový server. Tento model je škálovatelnější a ovladatelnější, a přestože je složitější než klasický model klient/server, umožňuje aplikačním prostředím vyvíjet se směrem k distribuovaným výpočetním prostředím.

Model n-tier představuje významný krok ve vývoji distribuovaného zpracování dat z klasického modelu klient/server. Model n-tier poskytuje mechanismus ke zvýšení výkonu a udržovatelnosti aplikací typu klient/server při zjednodušené kontrole a správě kódu aplikace.

3.2.2 **Architektura orientovaná na služby**

Architektura zaměřená na služby (Service oriented architecture – SOA) je hlavně o vývoji podnikových procesů, aplikací a služeb a plynulé integrace různorodých aplikací do světa propojených podniků, přizpůsobení rychlé reakce na změny a využití obrovské míry podnikové automatizace. Jedná se o soubor obecných zásad návrhu, které organizacím umožňují měnit obchodní procesy velmi rychle a reagovat na měnící se požadavky podnikání způsobem, který by byl nepraktický nebo nákladově omezující pomocí konvenčního vývoje aplikací a přidělování zdrojů [10].

Na SOA lze pohlížet jako na výpočetní metodologii nebo na přístup k budování IT systémů, v nichž jsou obchodní služby, tj. služby poskytované organizací klientům, jsou klíčovými organizačními principy používanými pro sladění IT systémů s potřebami podnikání. Dřívější přístupy používané při vytváření IT systémů se zaměřovaly na přímé použití specifických implementačních prostředí, jako je objektová orientace nebo procedurální orientace k řešení obchodních problémů. Tyto přístupy vedly k systémům, které jsou často spojeny s vlastnostmi a funkcemi konkrétní technologie prostředí provádění. Z výše uvedeného popisu architektury orientované na služby jasně plyne, že služba je klíčovou součástí. Lze ji považovat za prostředek, s jehož pomocí jsou potřeby spotřebitele spojeny s možnostmi poskytovatele služeb [10].

Služby v rámci organizačního kontextu mohou být buď poháněny potřebami spotřebitele a jsou rozepsané na úrovni systému (shora dolů), nebo s ohledem na systémové schopnosti poskytovatele služeb a budování služeb, které mohou být vystavené vyšším vrstvám v architektuře (zdola nahoru). Ale dnes jsou služby postaveny spíše z pohledu inženýrů nebo dodavatelů než z pohledu uživatelů.

3.2.2.1 Mikroslužby

Mikroslužby (microservices) jsou variantou SOA, která strukturuje aplikaci jako soubor volně spojených služeb. Aplikace je rozdělena do funkčních služeb: každá z nich má vysokou soudržnost a je ve většině případů relativně malá (odtud název – microservice). Rozdělením logických modulů do samostatných služeb je pak snadné zjistit, který tým vlastní část projektu, protože vlastní celou samostatnou službu. Týmy mohou řídit, včetně nasazení, monitorování, v jakém jazyce je napsáno atd.

Protože jsou mikroservisy malé, je jednodušší je složit a záleží mnohem méně na tom, jaký je váš implementační jazyk. Mikroslužby mohou být ve skutečnosti zcela

na jedno použití, protože přepisování funkcí nevyžaduje tolik práce. Mikroservisy komunikují po síti pomocí zpráv. Pro architekturu microservice je nepodstatné, jaký datový formát zprávy používají, nebo protokoly, kterými jsou přenášeny. Mikroslužby jsou zcela definovány zprávami, jež přijímají, a zprávami, jež vysílají. Z pohledu jednotlivých instancí mikroprocesorů a z pohledu vývojáře, který tento mikroservis píše, přicházejí pouze zprávy a zprávy k odeslání. Při nasazení může být tato instance mikroprocesoru účastníkem konfigurace požadavek/ odpověď nebo konfigurace publikování/přihlášení nebo libovolného počtu variant. Způsob, jakým jsou zprávy distribuovány, není definující charakteristikou architektury Microservice. Všechny distribuční strategie jsou vítány bez předsudků [12].

Síť mikroservisů může své principy splňovat tím, že splňuje malou sadu architektonických omezení. Jedná se o nezávislost na dopravě a pattern matching[3]. Dopravní nezávislost je schopnost přesouvat zprávy z jednoho mikroservisu do druhého, aniž by bylo nutné, aby mikroservice o sobě navzájem věděly. Když jeden mikroservice potřebuje vědět o jiném mikroservice, aby mu mohla poslat zprávu, je to fatální chyba. Poruší princip výsady, protože příjemce je z pohledu odesílatele privilegován. Již nemůžete skládat další mikroservisy přes přijímač, aniž byste měnili odesílatele. Patter matching je schopnost směrovat zprávy na základě dat uvnitř zprávy. Toto je funkce, která umožňuje dynamicky definovat síť. To umožní přidávat a odebírat během provozu mikroslužby, a to bez ovlivnění existujících zpráv nebo ostatních služeb.

Microslužby mohou věrohodně řešit potřeby vlastního podnikového softwaru. Díky užšímu sladění softwarové architektury systému se skutečným záměrem podnikání mohou mít softwarové projekty mnohem úspěšnější výsledky. Skutečná obchodní hodnota může být dodána rychleji. Systémy microslužeb přistupují k minimálnímu životaschopnému stavu produktu rychleji, a proto mohou být uvedeny do výroby dříve. Jakmile jsou ve výrobě, udržují krok s měnícími se požadavky jednoduššími způsoby.

[3] Pattern matching – metoda analýzy a zpracování datových struktur v programovacích jazycích, založená na provádění určitých instrukcí v závislosti na shodě studované hodnoty s jedním nebo druhým vzorkem.

4 Vlastní práce

Diplomová práce je reálným projektem, který má autor ve společnosti LUKAPO s.r.o. Tento projekt je zaměřen na migraci aplikace do cloudu vyvinuté zákazníkem firmy LUKAPO – společnosti Extraweb[4]. Autor diplomové práce je zde hlavním architektem nové infrastruktury a je zodpovědný za celý proces migrace. Aktuálně je projekt úspěšně dokončen a výsledky a postup jsou představeny v této části.

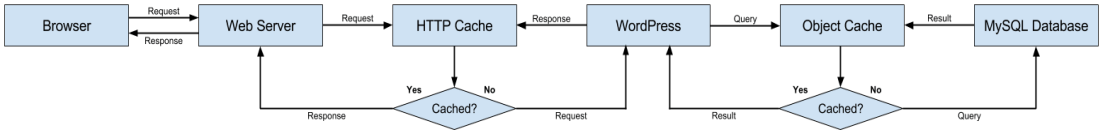
4.1 Charakteristika společnosti Extraweb

Podle mezinárodního provozovatele hostingů Kinsta, nejoblíbenější a nejpoužívanější systém pro správu obsahu web stránek je WordPress, který se používá u 35,2 % všech webů ve světě [5]. Je to velký trh také kvůli tomu, že WordPress nabízí možnost vytváření vlastních pluginů a pomůcek, které jsou většinou placené, i když samotný WordPress je licencován pod GPLv2[5]. Jednou takovou společností je Extraweb, která v době psaní této diplomové práce byla velmi zajímavá pro české zákazníky a měla kolem 8000 uživatelů. Extraweb rozšiřoval své služby a potřeboval profesionální expertizu své infrastruktury, aby zajistil bezproblémový přístup ke svému produktu odkudkoliv ze světa a byl schopný obsloužit více než 20 tisíc nových zákazníků. Proto se společnost LUKAPO s.r.o. obrátila právě na Extraweb.

4.1.1 Aktivity společnosti Extraweb

Mezi hlavní aktivity společnosti můžeme zařadit prodej svého vlastního pluginu pro WordPress, který usnadňuje vytváření webových stránek. Není potřeba přesně znát, jakým způsobem funguje ten plugin, protože to je pouze rozšíření pro WordPress, jehož architektura je více důležitá pro vytvoření nové infrastruktury.

Obrázek 5 WordPress architektura



Zdroj: vlastní zpracování

[4] Jméno společnosti bylo změněno
[5] Používat a upravovat může kdokoli.

Diagram výše poskytuje dobrý přehled o tom, jak vypadá informační tok při používání WordPress. Tento informační tok můžeme rozdělit do tří oblastí:

- Cyklus požadavků a odpovědí mezi prohlížečem a WordPress.
- WordPress (vykonává PHP skripty).
- Cyklus dotaz – výsledek mezi WordPress a MySQL databází.

Jako samotná webová aplikace je WordPress perfektním příkladem vícevrstvé architektury:

- Prezentační vrstva používá základní CSS, HTML (s některými tématy se nyní používá i HTML5), jQuery a Backbone.js pro řídící portál.
- Aplikační vrstva – která se považuje za WordPress – je napsána v PHP a zpracovává mnoho základních operací pro čtení a zápis do datového úložiště a zároveň poskytuje API pro vývojáře, aby ji mohli dále využívat.
- Databázová vrstva je databáze MySQL.

Společnost Extraweb prodává vlastní plugin, který patří do aplikační vrstvy. Je to PHP skript, který umožňuje uživatelům rozšířit funkce svého webu. Pro lepší podporu uživatelů Extraweb spravuje celý WordPress a při nákupu VIP balíčku poskytuje i hostingové služby.

4.1.2 **Požadavky společnosti Extraweb**

Spokojenost uživatelů je prioritou v Extraweb, proto tato firma chce zavést Service-level agreement (SLA) – smlouva mezi poskytovatelem služby a jejím uživatelem, která zajistí 99,99 % dostupnosti webu – celkový čas výpadku nesmí přesahovat 4,22 minuty měsíčně. Aby poskytovatel služeb byl připraven k tomuto SLA, je potřeba zajistit vysokou dostupnost infrastruktury. Extraweb připravuje obrovskou marketingovou kampaň, která by měla přivést více než deset tisíc nových zákazníků. To znamená, že by infrastruktura měla být připravena k takovému zvýšení počtu zákazníků a k vyššímu výkonu serverů.

4.1.3 **Infrastruktura společnosti Extraweb**

Pro poskytnutí svých služeb využívá společnost Extraweb 30 serverů, které se nachází u třech providerů: VULTR, Digital Ocean a Linode. I když jsou to všechno cloudoví provideři, Extraweb nevyužívá jejich cloudové možnosti, ale používá servery jenom pro hostingové cíle. Každý z těchto serverů je zálohován a všechny zálohy se nachází v AWS, kde je pro každý server na zálohování vytvořen vlastní S3 bucket[6]. V okamžiku, kdy bylo rozhodnuto o migraci infrastruktury do jednoho poskytovatele cloudových služeb, společnost měla 6433 uživatelů.

Tabulka 1 Měsíční náklady na provoz infrastruktury (včetně DPH)

Poskytovatel	Služby	Měsíční náklady
VULTR	20 serverů	$ 1330
LINODE	3 servery	$ 625
DO	7 serverů	$ 160
AWS	zálohování	$ 475
Celkem		$ 2590
Cena za 1 uživatele		$ 0.40

Zdroj: vlastní zpracování

Mezi hlavní příčiny migrace infrastruktury můžeme zařadit:

- Jeden z poskytovatelů má časté výpadky[7].
- Existující řešení neobsahuje vysoké dostupnosti. Jakmile jeden ze serverů spadne, všechny weby na něm nefungují.
- Špatné využití serverů. Na nový server se vždy přidává určitý počet hostingů a musí zbýt volné místo. Jakmile zákazníci nahrávají do webu obsah, místo dochází. Pak je třeba přesouvat weby na jiné servery (má-li doménu ve správě zákazník, tak to není možné), nebo servery navyšovat. Vždy tedy dochází k neúplnému využití a plýtvání.

[6] Amazon Simple Storage Service (Amazon S3) je služba ukládání objektů, která nabízí škálovatelnost, dostupnost dat, zabezpečení a výkon.
[7] Aby se zachovalo dobré jméno společnosti, název nebude poskytnut.

- Staré servery se nedají snadno smazat, protože je potřeba znát jejich IP. Pokud má zákazník správu domény u Extraweb, jde to nastavit. Má-li zákazník doménu ve své správě, neexistuje možnost to změnit a nelze web přesunout jinam. To je důvod, proč i když je výpadek u jednoho z poskytovatelů, nedá se hromadně přejít k jinému cloudovému poskytovateli.
- Servery lze pouze zvětšovat, ne zmenšovat. Kvůli disku je potřeba zvětšovat celý server a nejde zvětšit jen disk. Pak nastává moment, kde společnost vlastní zbytečně moc CPU a RAM, které nejsou využívané a přináší další náklady. Po analýze stávající infrastruktury bylo zjištěno, že 30 % existující kapacity není využíváno.
- Přidání nového hostingového serveru znamená hodně ruční práce.

4.2 Volba poskytovatele cloudu

Společnost Extraweb nevlastní servery, ale používá kapacity cloudových providerů. Žádné extra servisy, které vlastní pouze konkrétní poskytovatel, společnost nevyužívá. Zároveň Extraweb má vlastní operační tým, který přidává nové hostingové servery a má znalosti v architektuře své aplikace, proto aby se vyřešily existující problémy a splnily požadavky společnosti, byl vybrán IaaS distribuční model. Extraweb nemá potřebu vybudovat vyhrazené datacentrum, nemá citlivá data uživatelů, která by podle zákona měla hostit pouze v privátním cloudu a chce použít flexibilitu a škálovatelnost veřejného cloudu. Společnost má globální dosah a chce se spojit se zákazníky v různých lokalitách s minimálním úsilím, proto jako způsob nasazení byl vybrán veřejný cloud.

IaaS model je standardizovaná, vysoce automatizovaná nabídka výpočetních prostředků doplněných úložnými a síťovými funkcemi a jsou vlastnictvím poskytovatele služeb a nabízení zákazníkovi na vyžádání. Zdroje jsou škálovatelné a elastické v téměř reálném čase a jsou měřeny podle použití, co je hlavním důvodem použití tohoto distribučního modelu.

4.2.1 Hodnocení kritických schopností při výběru poskytovatele

Veřejný cloud IaaS je třeba vyhodnotit z hlediska jeho technické vhodnosti pro potřeby pracovního vytížení a potřeb organizace. Tato část zkoumá osm širokých

oblastí kritických schopností, které musíme zvážit při hodnocení nabídek veřejné cloudové služby IaaS:

- Možnosti související s výpočty.
- Možnosti související s úložištěm.
- Možnosti související se sítí.
- Možnosti související se zabezpečením.
- Funkce související se správou.
- Možnosti související s vývojem.
- Soulad a dokumentace.

Na základě těchto oblastí budou zhodnoceny produkty/služby každého poskytovatele na kritické schopnosti.

4.2.2 **Základní kritéria při hodnocení poskytovatelů**

I když služby cloudových providerů se liší, následující kritéria jsou základní možností, která se považuje za součást každého cloudového poskytovatele IaaS na trhu. Tento seznam představuje minimální požadavky, které musí poskytovatel splňovat, aby byl považován za cloudového poskytovatele IaaS. Tento seznam může být užitečný při rozlišování, zda je poskytovatel spravovaný poskytovatelem hostingu nebo poskytovatelem cloudového IaaS:

- Plně automatizované poskytování samoobslužných zdrojů infrastruktury na vyžádání.
- Samoobslužná rozhraní vystavená přímo zákazníkovi, včetně webového uživatelského rozhraní a API.
- Samoobslužné nástroje příkazového řádku pro systémy Linux i Windows.
- Přímý přístup k samosprávě infrastruktury.
- Škálovatelnost a pružnost zdrojů infrastruktury v reálném čase.
- Modely placení za použití služeb (např. za hodinu a za GB/měsíc).
- Vývojové centrum, které zahrnuje dokumentaci k API.

4.2.2.1 Možnosti související s výpočty

Požadované

Rozptyl datových center: Poskytovatelé musí mít nejméně tři datová centra, která jsou od sebe vzdálena minimálně 200 kilometrů. Tato datová centra musí být na různých energetických sítích. Nabízení více datových center s touto úrovní rozptylu umožňuje podnikovým zákazníkům vyvinout možnosti dostupnosti, které mohou udržet problémy způsobující místní výpadky, jako jsou bouře

Více kontinentů a datových center: Poskytovatelé musí zahrnovat nabídky služeb, aby uspokojili vysokou dostupnost (HA) a zotavení po katastrofě (DR) na více kontinentech a pro nadnárodní zákazníky. Poskytovatel musí mít minimálně dvě nabídky v Evropě a dvě nabídky ve Spojených státech.

Rychlé, samoobslužné poskytování: Cloudová služba musí nabízet samoobslužné poskytování instancí buď prostřednictvím konzoly pro správu, nebo prostřednictvím programového rozhraní. Poskytování musí být simultánní, nikoli postupné – samoobslužná rozhraní a řídicí rovina poskytovatele musí být schopny poskytovat velký počet instancí pro více zákazníků současně, bez závislostí mezi těmito zajišťovacími úlohami. Konečně musí být zajišťovací schopnost rychlá.

Podpora velkých instancí: Poskytovatelé musí nabídnout instance s velkým počtem procesorových jader a velkým množstvím paměti pro případy použití náročného na procesor, nebo paměť. Poskytovatel musí být schopen poskytovat instance, které podporují alespoň 16 CPU a 128 GB RAM.

Žádné upřednostňování zdrojů u nájemců: Ve standardní službě není přijatelné vyhladovovat případy jednoho zákazníka za účelem vyvážit, nebo zlepšit výkon ostatních, pokud zákazník jasně nepředplatí takovou úroveň služeb s proměnlivým výkonem.

Údržba hostitele zachovávajícího VM: Poskytovatel musí být schopen provádět údržbu na výpočetním hostiteli, aniž by to narušovalo běh virtuálních počítačů na tomto hostiteli. Taková údržba může zahrnovat provedení aktualizace jádra nebo aktualizace hypervisoru.

Dynamické horizontální automatické měřítko: Cloudová služba musí poskytovat funkce pro automatické škálování VM horizontálně na základě spouštěčů.

Dynamické vertikální automatické měřítko: Cloudová služba musí poskytovat funkce pro automatickou změnu velikosti CPU a RAM na stávajících virtuálních počítačích na základě spouštěčů.

Preferované

Explicitní afinita k hostiteli: V některých případech použití je třeba, aby se dva nebo více virtuálních počítačů explicitně zdržely na stejném hostiteli. Toto ujištění je užitečné pro organizace, které potřebují zlepšit výkon, minimalizovat latenci nebo maximalizovat zabezpečení (např. mezi aplikačním serverem a databázovým serverem). Proto musí cloudová služba podporovat samoobslužné rozhraní, kde klienti mohou určit, které instance musí sdílet fyzického hostitele

VM s jediným nájemcem: VM s jediným nájemcem zajišťují, aby instance byly umístěny na fyzickém hostiteli, který není sdílen s žádným jiným zákazníkem. U této konkrétní nabídky mohou být úložiště a síť sdíleny nebo izolovány.

Základní výpočetní výkon: Výkonnostní standardy v celém odvětví IaaS nejsou dobře definovány ani standardizovány. Podnikoví zákazníci však potřebují vědět, co je „očekávané“ nebo „normální“, pokud jde o základní výpočetní výkon u jejich poskytovatele. Poskytovatelé musí každoročně publikovat dokumentovaný scénář/skript testování výkonu proti třem nebo více nejoblíbenějším velikostem instance a napříč standardní konfigurací systému Linux i standardní konfigurací systému Windows.

Poskytování za minutu: Alespoň jedna verze instance systému Linux musí být schopna se spustit a uvést do provozu za méně než jednu minutu. Tento image musí mít následující minimální specifikace: 1 CPU, 2 GB RAM a 40 GB úložiště.

Služba zálohování: Poskytovatel musí nabídnout službu zálohování, která usnadňuje zálohování a obnovu následující VM a disků připojených k současným VM.

Docker[8] kontejnerová služba: Poskytovatelé musí nabídnout spravovanou kontejnerovou službu založenou na Docker, která zahrnuje škálovatelnou, vysoce dostupnou a monitorovanou infrastrukturu správy kontejnerů.

Kontejnerová služba Kubernetes[9]: Platforma musí nabízet kontejnerovou službu založenou na Kubernetes. Hlavní uzel Kubernetes musí být minimálně spravován automaticky. Je však přijatelné požadovat, aby zákazník prováděl obnovení pracovních uzlů.

Volitelné

Nabídka HPC: Mnoho organizací v oblasti vědeckých a finančních služeb se stále více snaží využívat nabídky IaaS pro vysoce výkonné počítačové projekty (HPC). Hlavní poskytovatelé proto musí do svých platforem zahrnout nabídku těchto instancí.

Export obrazu VM: Cloudová služba musí podporovat schopnost exportovat existující běžící VM nebo kopii VM do obrazového formátu VMDK, OVF nebo VHD.

Poskytování bare-metal serveru: Cloudová služba musí nabízet možnost využití fyzického serveru jako služby – která se nespouští na platformách virtualizace serverů. Nabídka fyzického serveru musí být plně automatizovaná.

Instance optimalizované pro ML: Poskytovatel musí nabídnout konfiguraci instance pro výpočet, která je optimalizována pro strojové učení (ML).

4.2.2.2 Možnosti související s úložištěm

Požadované

Hromadný import/export dat se šifrováním: Je obtížné migrovat velké množství dat na externí hostitelské místo prostřednictvím sítě. Výzva je z velké části omezena šířkou pásma, latencí sítě, celkovou spolehlivostí a poplatky za páteřní internet. Poskytovatelé proto musí nabídnout službu hromadného importu a exportu dat se šifrováním pro přesun velkého množství dat do cloudové služby i mimo ni.

[8] Docker je projekt, jehož cílem je poskytnout jednotné rozhraní pro izolaci aplikací do kontejnerů v prostředí macOS, Linuxu i Windows.
[9] Kubernetes je systém pro orchestraci virtualizace na úrovni operačního systému.

Replikace napříč geografií: Pro služby úložiště objektů a datové úložiště musí poskytovatel nabídnout službu replikace, která překračuje regionální hranice. Tato nabídka musí být službou, ke které se zákazníci mohou přihlásit pro ochranu dat, a zákazník musí mít kontrolu nad umístěním v konkrétní zemi. Vzhledem k vzdálenosti mezi regionálními hranicemi by tato replikace měla být asynchronní.

Snapshot[10] úložiště: Cloudová služba musí podporovat momentální kopii úložiště, tzv. „snapshot“. Zákazníci musí být schopni vytvořit snapshot jakéhokoli úložiště pomocí samoobslužných prostředků. Kromě toho musí být zákazníci schopni používat snímky jako obrazy k samoobslužnému poskytování nových výpočetních instancí.

Řada úložiště: Poskytovatel musí nabídnout různou řadu datového úložiště zaměřeného na různé úrovně výkonu a ceny. Alespoň jedna z úrovní musí obsahovat SSD a musí poskytovat vyšší vstup/výstup (I/O) než úrovně bez SSD. Cíl řady a procentuální zlepšení oproti standardní nabídce jiné než SSD musí být zdokumentovány.

Škálovatelná služba ukládání objektů: Poskytovatel musí nabídnout distribuovanou službu ukládání objektů s více datovými centry, kde lze objekty (individuální soubory) ukládat a získávat prostřednictvím API[11] webových služeb.

Replikace úložiště objektů: Poskytovatel musí automaticky replikovat objekty napříč více datovými centry. Tato replikace nesmí přesahovat hranice zemí (nebo zákazník musí mít schopnost tomu zabránit). Alternativně musí být replikace řízena z hlediska umístění v zemi.

Šifrovací služby s povoleným poskytovatelem: Služba ukládání objektů musí zákazníkům umožnit použít serverem podporované šifrování na straně serveru (SSE). Zákazníci by si měli uvědomit, že mohou vždy před vlastním nahráním a uložením v rámci veřejného cloudového úložiště spravovat své vlastní šifrovací klíče a šifrovat svá vlastní data.

Verzování objektu: Služba ukládání objektů musí zákazníkovi nabídnout možnost verzování objektu. Tato funkce automaticky udržuje předchozí verze objektu, čímž chrání před náhodnou ztrátou dat v důsledku přepsání nebo vymazání objektu. Příliš mnoho verzí však vede k rozrůstání úložiště.

[10] Snapshot je obrazem dat na diskovém oddílu.
[11] API – Application Programming Interface – rozhraní pro programování aplikací.

Preferované

Připojení k více instancím: Zákazníci mohou být ochotni využít datové úložiště na více výpočetních instancích. Je přijatelné, aby disky byly v režimu jen pro čtení.

Šifrovatelný spouštěcí disk: Zákazník musí být schopen šifrovat spouštěcí disk jakékoli instance napříč jakýmkoli typem instance. Šifrování musí být jednoduchou samoobslužnou možností, kterou si zákazníci mohou vybrat při zajišťování instance.

Zásady správy životního cyklu objektů: Zákazník musí být schopen nastavit časové zásady týkající se objektů, které umožňují automatické provádění akcí podle stáří objektů. Tato funkce musí minimálně podporovat automatické mazání objektů, které jsou starší určité doby.

Volitelné

Služba úložiště pro jednoho nájemce: Poskytovatelé musí zákazníkům umožnit vytvořit pevný disk pro jednoho nájemce. Tento disk pro jednoho nájemce lze použít ve spojení s libovolnými výpočetními instancemi, které by jinak využívaly datové úložiště.

Podpora statického webhostingu: Zákazníci musí být schopni implementovat plně funkční web pomocí služby úložiště objektů a přidružených kontejnerů objektů. Díky této funkci mohou zákazníci snadno nahrávat statický webový obsah a publikovat weby, aniž by museli konfigurovat webové servery výpočetních instancí.

4.2.2.3 Možnosti související se sítí

Požadované

Hierarchická topologie LAN definovaná zákazníkem: Zákazníci požadují schopnost navrhnout hierarchickou síťovou infrastrukturu u poskytovatele a zvolit si své schéma adresování IP bez závislosti na tom, zda mají instance u poskytovatele. Před nasazením jakékoli výpočetní instance musí být zákazníci schopni navrhnout následující síťové komponenty a rozvržení:

- Firewally a ACL;
- Podsítě nebo virtuální sítě LAN (VLAN);
- Směrování;

- VPN;
- Překlad síťových adres (NAT);
- Vyrovnávání zatížení

Multisegmentové sítě a více podsítí na virtuální síť: Jeden zákazník musí mít možnost mít více segmentů virtuální sítě (přibližně ekvivalentních s VLAN), aniž by k vytváření překryvů musel používat software třetích stran. Platforma musí navíc umožnit zákazníkovi vytvořit více podsítí na virtuální síť.

Izolované virtuální sítě a soukromé IP adresy: Poskytovatelé musí nabízet virtuální sítě, které jsou plně izolované a externě nedostupné. Dále musí existovat konfigurace instancí, které mohou být umístěny pouze v těchto izolovaných virtuálních sítích
a bez veřejné IP adresy nebo internetového směrování.

Statické adresy IP: Aby bylo možné říct, že poskytovatel podporuje statické IP adresy, musí poskytovat několik funkcí. Zaprvé, pokud je výpočetní instanci dynamicky přiřazena IP adresa, musí tato adresa zůstat po celou dobu fungování instance stejná (pokud ji zákazník nechce změnit). Zadruhé, zákazník musí být schopen získat IP adresu, včetně veřejné IP adresy, která může být přiřazena k výpočetní instanci.

Připojení k zákazníkům VPN: Poskytovatelé musí zákazníkům umožnit přístup ke cloudové službě prostřednictvím tunelu IPsec VPN nebo tunelu SSL (Secure Sockets Layer) (SSL) / TLS (Transport Layer Security) přes veřejný internet. Musí to být samoobslužná funkce ze strany poskytovatele, i když zákazníci budou muset provést konfiguraci na jejich konci.

Virtuální sítě s více datovými centry: Poskytovatel musí zákazníkovi umožnit používat virtuální sítě, které pokrývají dvě nebo více datových center.

Preferované

Vyrovnávání zatížení na základě směrování obsahu: Platforma musí být schopna směrovat požadavek na službu na základě obsahu žádosti. Služba musí podporovat následující:

- Směrování založené na URI: Místní služba vyrovnávání zátěže vrstvy 7 podporuje směrování požadavků na základě vzorů identifikátoru unifikovaného

zdroje (URI). To zákazníkovi umožňuje vytvářet skupiny výpočetních instancí vyrovnávajících zatížení, která reagují na konkrétní vzory URI definované zákazníkem.

- Směrování založené na záhlaví: Místní služba vyrovnávání zátěže vrstvy 7 podporuje směrování požadavků na základě HTTP hlaviček. To zákazníkovi umožňuje vytvářet skupiny výpočetních instancí vyrovnávajících zatížení, která reagují na vzory definované zákazníkem v obsahu konkrétní HTTP hlavičky. Tato kategorie zahrnuje možnost směrování požadavků na základě souborů cookie.
- Směrování založené na parametrech: Místní služba vyrovnávání zatížení vrstvy 7 podporuje směrování požadavků na základě parametrů zadaných požadavků HTTP. To umožňuje zákazníkovi vytvořit skupiny vyrovnávání zatížení výpočetních instancí, které reagují na vzory definované v požadavcích zákazníka (například na základě dat v požadavku POST).

Volitelné

Podpora IPv6: Poskytovatelé musí podporovat IPv6 na bráně (např. vyrovnávač zatížení) nebo na úrovni instance a vystavovat tuto funkci zákazníkům.

Přineste si své veřejné IP adresy: Zákazníci musí mít možnost přinést si vlastní autonomní systémová čísla (ASN) a veřejně směrovatelné IP adresy. Platforma musí zákazníkům umožnit poskytovat jejich infrastrukturu pomocí IP adres v tomto netblocku. Platforma musí také být schopna správně směrovat adresy. Kromě toho musí platforma umožnit zákazníkům prostřednictvím samoobslužných služeb automaticky poskytovat tyto IP adresy.

4.2.2.4 Možnosti související se zabezpečením

Požadované

Stavový síťový firewall: Poskytovatel musí zákazníkům umožnit nastavit firewall pravidla, která jsou přidružena k virtuální síti nebo podsíti, která slouží jako stavový firewall pro příchozí a odchozí provoz bez ohledu na to, zda přenos pochází z platformy nebo na ni. Zákazník musí být dále schopen nastavit pravidla, která jsou spojena s virtuálními stroji. Kromě toho musí být aktualizovaná pravidla okamžitě použita

ve všech instancích. Změny pravidel nesmí vyžadovat restartování nebo zastavení jakýchkoli služeb.

Počáteční pověření pro administrativní přístup: Výchozí administrativní přístup pro každou nasazenou instanci v cloudové službě musí být automaticky vygenerován nebo vybrán v okamžiku poskytnutí zákazníkem.

Zabezpečené SSL/TLS API společné identifikátory: Společné identifikátory API platformy orientované na zákazníka musí být zabezpečeny pomocí SSL/TLS. Certifikát SSL/TLS musí být podepsán běžně důvěryhodnou certifikační autoritou (CA). Nesmí to být certifikát s vlastním podpisem, pouze pokud poskytovatel je také důvěryhodnou certifikační autoritou.

Zmírnění DDoS: Poskytovatelé musí nabídnout službu snižování distribuovaného odepření služby (DDoS). Útoky DDoS, které pocházejí z internetu, musí být automaticky detekovány a zmírněny pro všechny zákazníky na celé platformě.

Řízení přístupu pro správu MFA: Poskytovatelé musí zákazníkům umožnit řídit přístup uživatelů ke cloudové službě prostřednictvím multifaktorového ověřování (MFA). MFA nemusí být výchozí konfigurace, ale poskytovatelé musí zákazníkům nabídnout zabezpečení uživatelských účtů.

Oprávnění založené na rolích a skupinách: Poskytovatelé musí povolit autorizaci na základě rolí, která povolí přístup pouze k předem definovaným produktům a službám.

Preferované

Hierarchie pravidel firewall brány: Zákazníci musí být schopni implementovat pravidla firewall brány na různých úrovních. To je užitečné při implementaci pravidel omezujících firewall, která ostatní správci nemohou přepsat.

Přiřazení více firewall pravidel: Zákazníci musí mít možnost přiřadit tři nebo více firewall pravidel samostatné instanci nebo skupině instancí.

WAF: Platforma musí poskytovat webový aplikační firewall (WAF) jako službu. WAF je určen k ochraně aplikací, které jsou přístupné přes HTTP a HTTPS před útokem.

Ověřování pomocí SSO se SAML: Poskytovatelé musí nabídnout Single Sign-On (SSO) přihlašovací přístup do konzoly pro správu GUI a prostřednictvím Security

Assertion Markup Language (SAML). Platforma musí umožňovat integraci s jednou nebo více službami SSO třetích stran.

Volitelné

Pracovní postup schvalování: Poskytovatelé musí zákazníkům nabídnout samoobslužný pracovní postup schvalování. Zákazníci někdy chtějí možnost přidat k funkcím cloudové služby schvalovací krok, zejména ty, které akumulují náklady. Pracovní postup schvalování znamená, že když uživatel podá žádost o přístup k službě, musí vlastník účtu (nebo nějaký jiný pověřený správce) žádost schválit, nebo zamítnout a žádost je automaticky provedena, pokud je schválena.

4.2.2.5 Funkce související se správou

Požadované

GUI konzole pro správu: Poskytovatelé musí nabídnout bohatou konfigurovatelnou webovou konzoli pro správu pro interakci s cloudovou službou. Poskytovatelé musí prokázat, že nejdůležitější funkce cloudových služeb jsou zastoupeny v konzole a že všechny nové služby jsou zastoupeny v konzole do 180 dnů od jejich vydání. Nakonec musí webová konzola GUI podporovat aktuální verze prohlížečů Chrome, Edge, Firefox, Internet Explorer a Safari a mobilní prohlížeče v předních tabletech Android a iOS (např. mobilní Safari a WebKit).

Samoobslužný systém protokolování incidentů: Poskytovatelé musí nabídnout systém správy incidentů pro identifikaci, odesílání a sledování incidentů cloudové služby. Systém musí být dostupný online a musí být přístupný přes API platícím zákazníkům. Musí také zahrnovat schopnost odesílat incidenty a sledovat stavy a aktualizace incidentů.

Samoobslužné šablony: Poskytovatelé musí zákazníkům umožnit vytváření šablon infrastruktury. Šablona v tomto scénáři je plán, který umožňuje shromáždit různé zdroje společně. Tyto prostředky mohou zahrnovat výpočetní instance, svazky úložiště, síťové prvky, konfigurace monitorování a konfigurace zabezpečení. Zákazník musí být schopen vytvářet, ukládat a zajišťovat šablony vytvořené v cloudové službě. Šablona není jen kombinace velikosti výpočetní instance a konkrétního obrazu. Je to sestavení manifestu, který poskytuje více prvků, a musí udělat více, než jen specifikovat, jak poskytnout jednu, nebo více výpočetních instancí.

Služba sledování výkonu v reálném čase: Poskytovatelé musí nabídnout službu sledování výkonu v reálném čase. Musí být přístupná ze servisního rozhraní nebo z konzole a nesmí vyžadovat, aby si zákazníci vytvořili vlastní desky pro sledování výkonu. Musí podporovat:

- Výpočetní metriky (například využití procesoru, využití paměti).
- Metriky úložiště (například využití délky fronty a operace vstupu/výstupu za sekundu [IOPS]).

Kontroly, prahové hodnoty a oznámení týkající se výkonu v reálném čase: Poskytovatelé musí zákazníkům umožnit sledovat celkový stav jejich výpočetních, úložných a síťových infrastruktur v případě selhání a v případě selhání obdržet upozornění. Poskytovatelé musí zákazníkům umožnit přijímat oznámení na základě monitorování výkonu a výstrahy musí být generovány do jedné minuty od spouštěné prahové hodnoty.

Protokolování konfigurace zabezpečení: Poskytovatelé musí nabídnout protokolování konfigurací zabezpečení, včetně změn síťových zásad a změn v konfiguracích brány firewall. Zákazníci musí mít přístup k těmto protokolům prostřednictvím samoobslužných rozhraní. Protokoly by měly být standardně poskytovány po dobu nejméně tří měsíců a zákazníci by měli být schopni tyto protokoly exportovat pro delší uchovávání.

Vlastní metriky monitorování: Platforma musí nabízet metodu, s jejíž pomocí mohou zákazníci zasílat vlastní metriky monitorovací službě, která vytvoří výstrahu stejně jako u jakékoli jiné metriky. Poskytovatelé mohou požadovat, aby byl monitorovaný agent nainstalován na sledovaných prostředcích.

Preferované

Knihovna SDK: Poskytovatelé musí nabídnout bohatou sadu knihoven SDK pro tři nebo více programovacích jazyků: Java, .NET, Node.js, Perl, PHP, PowerShell, Python a Ruby. Tyto sady SDK by měly přinejmenším poskytovat podporu pro základní služby: výpočet, ukládání a vytváření sítí. Soupravy SDK musí zahrnovat také dokumentaci

a ukázky kódu. Je přijatelné, aby poskytovatel podporoval knihovnu s otevřeným zdrojovým kódem namísto jejího vytváření nezávisle.

Cenové API: Poskytovatelé musí nabídnout API pro cenová data, která zákazníci nebo třetí strany mohou dotazovat/získat přístup, aby získali cenové body v reálném čase pro jakékoli aktivum, které poskytovatel cloudu nabízí.

Nástroj pro optimalizaci nákladů: Poskytovatelé musí zákazníkům nabídnout službu, která doporučuje konfigurace pro optimalizaci finančních výdajů. Služba musí poskytovat doporučení specifická pro zákazníka a založena na současných nebo historických vzorcích u poskytovatele. Nesmí to být generické pro zákazníka. Doporučení musí být proveditelná, vázaná na konkrétní aktiva a musí být doloženo, že mají určitou výši finančních úspor. Tato služba musí být nabízena přímo poskytovatelem a nesmí vyžadovat, aby zákazník vyhledával partnery třetích stran.

Prognóza nákladů: Platforma musí poskytovat službu předpovídání nákladů, která zákazníkovi umožní použít jeho vlastní historické údaje o nákladech k projektování budoucích nákladů. Tato služba musí zákazníkovi umožnit projektovat vyšší, nebo nižší využití než dříve a určit účinky měnících se zdrojů a služeb (například přechod z mnoha malých výpočetních instancí na méně velkých výpočetních instancí).

Volitelné

Export síťové architektury pomocí GUI: Poskytovatelé musí zákazníkům umožnit exportovat grafické znázornění architektury jejich infrastruktury, včetně všech serverů, úložišť a sítí. Zákazníci musí být schopni exportovat tuto vizualizaci do obrazového souboru (například JPG nebo BMP), PDF, formátu Microsoft Visio nebo Microsoft PowerPoint

Mobilní aplikace pro konzolu pro správu: Poskytovatelé musí zákazníkům nabídnout mobilní aplikaci, která pracuje na jedné ze tří nejlepších mobilních platforem (Android, iOS a Windows). Tato mobilní aplikace musí být schopna sledovat, hlásit a upozorňovat na všechny obecně dostupné služby.

Výpočet bez serveru (serverless): Poskytovatel musí nabídnout službu serverless, která abstraktuje základní infrastrukturu. Zákazník by neměl potřebovat správu operačního systému nebo zdraví infrastruktury. Poskytovatel však může nabídnout přímý

přístup do virtuálních strojů nebo kontejnerů. Tato služba je určena pro univerzální aplikační logiku a musí podporovat webové aplikace, ale nesmí být zaměňována s funkčními platformami (spouštěnými událostmi).

4.2.2.6 Možnosti související s vývojem

Požadované

Relační DBaaS: Poskytovatel musí nabídnout relační databázi jako službu poskytovanou jako plně automatizovaná samoobslužná nabídka. V této službě by zákazník neměl mít přístup k základní instanci a údržbu databáze musí provádět výhradně poskytovatel.

NoSQL DBaaS: Databáze NoSQL jsou stále populárnější pro rozsáhlé škály aplikačních architektur. Poskytovatel musí nabídnout plně automatizovanou samoobslužnou nabídku NoSQL DBaaS, která je přístupná ze zbytku cloudové nabídky IaaS.

Jazyky SDK: Poskytovatel musí podporovat soupravy pro vývoj softwaru (SDK), které zabalují své API do nejméně dvou různých programovacích jazyků.

Podpora CLI: Poskytovatel musí podporovat CLI pro interaktivní správu a skriptování platformy. CLI může být založeno na libovolném počtu jazyků, jako jsou Python nebo PowerShell.

Preferované

CDN: Sítě pro doručování obsahu (CDN) jsou globální mezipaměťové, nebo akcelerační sítě, které se snaží zlepšit výkon přístupu koncových uživatelů po celém světě.

Ukládání do mezipaměti: Ukládání do mezipaměti umožňuje zákazníkům optimalizovat výkon pro operace čtení a také udržovat důležité informace o dostupnosti, jako je příbuznost relace a stav.

Asynchronní služba zasílání zpráv: Poskytovatel musí nabízet spolehlivou službu asynchronního zasílání zpráv s mnoha čísly. Služba by měla zahrnovat fronty i témata a musí podporovat jak vzory zpráv point-to-point, tak publikování–předplatné.

Volitelné

Hadoop jako služba: Poskytovatelé musí dodávat prostředí Hadoop jako plně automatizované a samoobslužné. Musí to být úplná služba, nikoli pouze „instalace jedním kliknutím“ společnosti Hadoop.

Služba řízení zdroje: Poskytovatel musí nabídnout soukromou službu řízení verzí pro zdrojový kód zákazníka (např. soukromé úložiště zdrojového kódu kompatibilní s Git).

4.2.3 Microsoft Azure

Microsoft Azure je vhodný pro širokou škálu případů použití, které běží dobře pod virtualizací. Ačkoli není tak vyspělý nebo na funkce bohatý jako AWS, má širší schopnosti než kterýkoli z jeho konkurentů a má svůj vlastní odlišný soubor diferencovaných a inovativních služeb. Zákazníci pravděpodobně zváží Microsoft Azure pro hostování aplikací společnosti Microsoft, jako je SharePoint, a také pro případy použití, kdy je aplikace založená na systému Windows, napsaná v .NET, vyvinutá týmem pomocí vývojářských nástrojů společnosti Microsoft, jako je Visual Studio, nebo závislá na middlewaru společnosti Microsoft. Microsoft však stále více zacílí na aplikace, které běží na Linuxu. Pracovní zatížení Linuxu je nejrychleji rostoucí částí portfolia Azure a tvoří 40 % Azure VM. Vývojářská zkušenost společnosti Microsoft je vylepšená těsnou integrací s Visual Studio. Většina zákazníků se však rozhodne používat portál nebo CLI a nespravuje se pomocí filozofie DevOps.

Možnosti související s výpočty

Hyper-V-virtualizovaný, široká škála různých virtuálních strojů s možností změny velikosti. Maximální velikost VM 416 CPU x 11400 GiB. Možnosti HPC, které zahrnují vysoce výkonná síťová propojení. Zákazníci mohou případně použít výpočetní službu založenou na PaaS VM (role Cloud Services Web a Worker) nebo App Service. Docker je představen jako kontejnerová služba (Azure Container Service) s výběrem orchestrátorů (Docker Swarm, Kubernetes a Azure Container Instance).

Možnosti související s úložištěm

Efektivní lokální úložiště, blokové úložiště nezávislé na VS (Disk) a úložiště objektů (Blobs) s integrovaným CDN, úložiště souborů s omezenou podporou protokolů (Files) a archivní úložiště (Archive). Vyšší výkon a úložiště založené na SSD (Premium Storage) je k dispozici jako místní úložiště pro konkrétní typy VS a blokové úložiště Managed Disks.

Možnosti související se sítí

SDN (virtuální sítě). Funkce vyrovnávání zatížení (Load balancer) zahrnuje směrování obsahu. Globální služba vyrovnávání zatížení. Připojení třetích stran prostřednictvím partnerských burz (ExpressRoute).

Možnosti související se zabezpečením

Může splňovat nejběžnější audity a běžné požadavky na dodržování předpisů, včetně SOC 1, SOC 2, ISO 27001, FedRAMP, PCI, HIPAA a GxP (farmaceutický průmysl). Granulární RBAC. Služba Active Directory a integrace. Služba správy klíčů.

Funkce související se správou

Řídicí portál je neustále k dispozici. Žádná okna údržby. Sledování. Plánovací služba. Šablony (správce zdrojů). Automatizační a konfigurační služby (Azure Automation). Významné tržiště.

Možnosti související s vývojem

Rozsáhlé pokrytí API. RESTful rozhraní se širokou sadou jazykových vazeb (především od Microsoftu s některými příspěvky komunity). CLI pokrývá širokou škálu funkcí se silnou podporou pro Windows PowerShell. Integrace IDE, včetně vývojářských služeb integrovaných do Visual Studio Team Services.

4.2.4 **Amazon Web Services**

AWS je komplexní platforma se stále rostoucí nabídkou služeb a možností. Může snadno začít používat základní funkce, ale implementace osvědčených postupů je obtížná. Obzvláště obtížný je proces architektury a správy aplikací, které podporují model zóny dostupnosti AWS z důvodu naprosté složitosti budování distribuovaného systému s ohledem na model zóny dostupnosti. Zákazníci musí také věnovat pozornost doporučeným postupům v oblasti výkonu a zabezpečení.

AWS je obzvláště silnou volbou pro digitální podnikání a další nové aplikace, včetně aplikací orientovaných na zákazníka, big data, backend pro mobilní aplikace a IoT. Jeho rozsáhlá sada služeb je užitečná pro zvýšení produktivity vývojářů a zjednodušení operací a zákazníci obvykle používají směs IaaS a PaaS AWS. Je nejvhodnější pro styl operací DevOps, ale jsou také životaschopné tradiční operační postupy.

Možnosti související s výpočty

Většinou virtualizované Xen, omezené možnosti KVM, široká škála různých virtuálních strojů s možností změny velikosti. Maximální velikost VS 448 CPU × 24576 GiB. Možnost jediného nájemce VS (vyhrazené instance a vyhrazení hostitelé). Volba HPC, která zahrnuje GPU, a vysoce výkonná síťová propojení. Instance FPGA. Volba pro burstable-CPU, menší VS. Měření za sekundu. Docker jako kontejnerová služba integrovaná do EC2 (ECS) fungující jako služba, která počítá s celou řadou spouštěčů událostí.

Možnosti související s úložištěm

Efektivní lokální úložiště (Non-volatile memory express (NVMe) s některými výpočetními instancemi), blokové úložiště nezávislé na virtuálním stroji (Elastic Block Store [EBS]), vrstvené úložiště objektů s integrovaným CDN (S3 s CloudFront), úložiště souborů s omezenou podporou protokolu (EFS) a archivní úložiště (Glacier). Volitelné šifrování. Volitelné zajištění IOPS pro EBS poskytují záruky kvality služeb pro výkon úložiště.

Možnosti související se sítí

Vysoce dostupné a sofistikované SDN (Amazon VPC). Možnosti vyrovnávání zatížení (Load balancer) zahrnují směrování obsahu. DNS (Route 53) zahrnuje globální službu vyrovnávání zatížení. Připojení třetích stran prostřednictvím partnerských burz (Direct Connect).

Možnosti související se zabezpečením

Splňuje téměř všechny běžné audity a společné požadavky na compliance, včetně GDPR, SOC 1, SOC 2, SOC 3, ISO 27001, FedRAMP, PCI, HIPAA a GxP (farmaceutický průmysl). Šifrování je k dispozici pro většinu datových úložišť. Velmi podrobný RBAC (správa identit a přístupu [IAM]), včetně RBAC napříč více účty. MFA také zahrnuje API. Integrace služby Active Directory. Služba správy klíčů, včetně hardwarových bezpečnostních modulů. WAF, včetně integrovaných anti-DDoS.

Funkce související se správou

Řídicí konzole je neustále k dispozici. Žádná okna údržby. Více zón datových center. Široká škála nativních funkcí, včetně monitorování (CloudWatch), dynamického autoscalingu, šablonizace (CloudFormation), správy konfigurace (Cong, OpsWorks), katalogu služeb a správy faktur. Rozsáhlé tržiště.

Možnosti související s vývojem

Rozsáhlé pokrytí API s rozhraním RESTful, se širokou škálou jazykových vazeb a sad SDK od AWS a komunity, včetně zabezpečeného mobilního API. Nástroj CLI a Windows PowerShell pokrývají širokou škálu funkcí. Integrace IDE. Vývojářské služby (CodeStar a další).

4.2.5 Google Cloud Provider

Možnosti GCP přitahují vývojáře vytvářející cloudové nativní aplikace, zejména aplikace s architekturou založenou na kontejnerech. GCP má bohatou sadu dobře navržených, inovativních schopností a je vhodný pro širokou škálu případů použití, které

fungují dobře ve virtualizovaném prostředí. Má dobře navržené uživatelské rozhraní, které vyvažuje snadné použití pro jednoduché i složité úkoly. GCP dále využívá nejjednodušší přístup pro nové uživatele ve svých výpočetních službách, pokud jde o vzdálený přístup, ve srovnání s jinými předními poskytovateli hyperscale.

Možnosti související s výpočty

Virtualizovaný na KVM se širokou škálou přizpůsobitelných velikostí VS. Maximální velikost VS 416 CPU x 11776 GB. V nabídce mají instance optimalizované pro TensorFlow (Cloud TPU). Volba pro burstable-CPU, menší VS. Měření za sekundu. Kontejnerová služba Docker založená na Kubernetes integrovaná s Google Container Engine (GCE). Funkce jako služba s velmi omezeným spouštěním událostí.

Možnosti související s úložištěm

Efektivní a trvalé lokální úložiště (NVMe s většinou výpočetních instancí). Blokové úložiště nezávislé na VS. Úložiště objektů s integrovaným CDN. Všechna data jsou standardně šifrována (Encryption at rest) a v pohybu. Zákazníci si mohou poskytnout své vlastní klíče.

Možnosti související se sítí

Vysoce výkonný, k dispozici SDN. Šifrování LAN a WAN. Integrované lokální a globální vyvažování zátěže včetně směrování obsahu pomocí AnyCast spíše než služby Cloud DNS. Připojení třetích stran prostřednictvím partnerských burz (Cloud Interconnect).

Možnosti související se zabezpečením

Audit GDPR, SOC 1, SOC 2, SOC 3 a ISO 27001. Bude podporovat PCI a HIPAA s BAA. WAF (beta). Granulární RBAC.

Funkce související se správou

Řídicí konzole je neustále k dispozici. Žádná okna údržby. Monitorování (Stackdriver), hlášení chyb a ladění. Hlášení výkonu. Šablony (Cloud Deployment Manager). Tržiště (Orbitera).

Možnosti související s vývojem

Rozsáhlé pokrytí API. RESTful rozhraní se širokou sadou jazykových vazeb. CLI a Windows PowerShell podporují širokou škálu funkcí. Integrace IDE.

4.2.6 Výsledky hodnocení kritických schopností

Hodnocení je provedeno pomocí vícekriteriální analýzy variant, na základě nominální informace o službách poskytovatelů, kde kritériem hodnoceni je kvantitativní veličina – počet povinných, preferovaných a volitelných služeb v konkrétní oblasti a kritéria jsou v maximalizačním typu. Za každou službu z oblasti povinné dostává poskytovatel 1 bod, za služby z oblasti preferované – 0,5 bodu, volitelné – 0,2 bodu. Celkový počet bodů je představen v následující tabulce. Služba, která je nabízena uživatelům méně než 1 rok, se v úvahu nebere.

Tabulka 2 Hodnocení kritických schopností

Kritické schopnosti	AWS	Azure	GCP
Výpočetní pevnost	12,3	12,3	12,1
Úložiště a šifrování	9,9	9,9	9,9
Síťová flexibilita architektury	7,4	3,4	4,2
Zabezpečení a dodržování	6,7	6,2	3,2
Správa uživatelů	9	6,2	8
Vývojářské služby	4,9	5,9	5,7
Průměr	50,20	43,90	43,10

Zdroj: vlastní zpracování

Na základě provedeného hodnocení a celkové informace o cloudových providerech, společnost Extraweb rozhodla provést migrace do veřejného AWS cloudu.

4.3 Návrh infrastruktury

Při hodnocení připravenosti aplikace pro cloudovou infrastrukturu existuje řada možností, které je třeba zvážit. Například pouhým rehostingem aplikace nemusí dojít k výrazným úsporám nákladů. Opačně může přestavba nabídnout velkou výhodu v cloudu, ale s velkým úsilím a náklady. Snad nejjednodušší jsou situace, ve kterých lze funkčnost jednoduše nahradit, například přechod na alternativu založenou na SaaS. Pro dosažení cíle bylo zapotřebí zvážit různé možnosti migrace jak z hlediska úsilí, tak i z hlediska výhod při migraci do AWS.

4.3.1 Model infrastruktury

Pro uspokojování požadavků zákazníka bylo zapotřebí připravit nejrychlejší způsob migrace do AWS a variantu s nejlevnější budoucí infrastrukturou. Jako nejrychlejší způsob vždy je Rehost – migrační strategie, která obvykle používá nástroje pro migraci k celkové replikaci aplikace v cloudovém prostředí. Nejlevnější infrastruktura požaduje adaptace cloudových rámců a úpravy přímo ve zdrojovém kódu – přechod na microservisní architekturu a migrace způsobem refactoring. Dále jsou představené návrhy infrastruktur pomocí různých metod s využitím následujících služeb od AWS:

- VPC – Virtual Private Cloud – Poskytuje logicky izolovanou část cloudu AWS, kde můžete spustit prostředky AWS ve virtuální síti, kterou definujete.
- Subnet – podsíť, je částí VPC.
- Internet Gateway – Internetová brána, která je horizontálně škálovatelná a vysoce dostupná součást VPC, umožňující komunikaci mezi instancemi ve VPC a internetu.
- NAT Gateway – Network adress translation gateway – brána, která umožňuje instancím v soukromé podsíti připojení k internetu nebo jiným službám AWS, ale brání internetu v navázání spojení s těmito instancemi.
- EC2 – Elastic Cloud Compute – služba, která poskytuje bezpečnou výpočetní kapacitu s možností změny velikosti v cloudu. Je navržena tak, aby vývojářům usnadnila cloud computing ve webovém měřítku.
- Autoscaling group – pomáhá udržovat dostupnost aplikace a umožňuje automaticky přidávat, nebo odebírat instance EC2 podle podmínek, které definujete.

- S3 – Simple Storage Service – služba ukládání objektů, která nabízí špičkovou škálovatelnost, dostupnost dat, zabezpečení a výkon.
- Redis – Remote Dictionary Server – je rychlé, open-source[12] datové úložiště s klíčovou hodnotou v paměti, které lze použít jako databázi, mezipaměť, zprostředkovatele zpráv a front.
- RDS – Relational Database Service – usnadňuje nastavení, provozování a škálování relační databáze v cloudu. Poskytuje nákladově efektivní a obnovitelnou kapacitu při automatizaci časově náročných administrativních úkolů, jako jsou poskytování hardwaru, nastavení databáze, záplatování

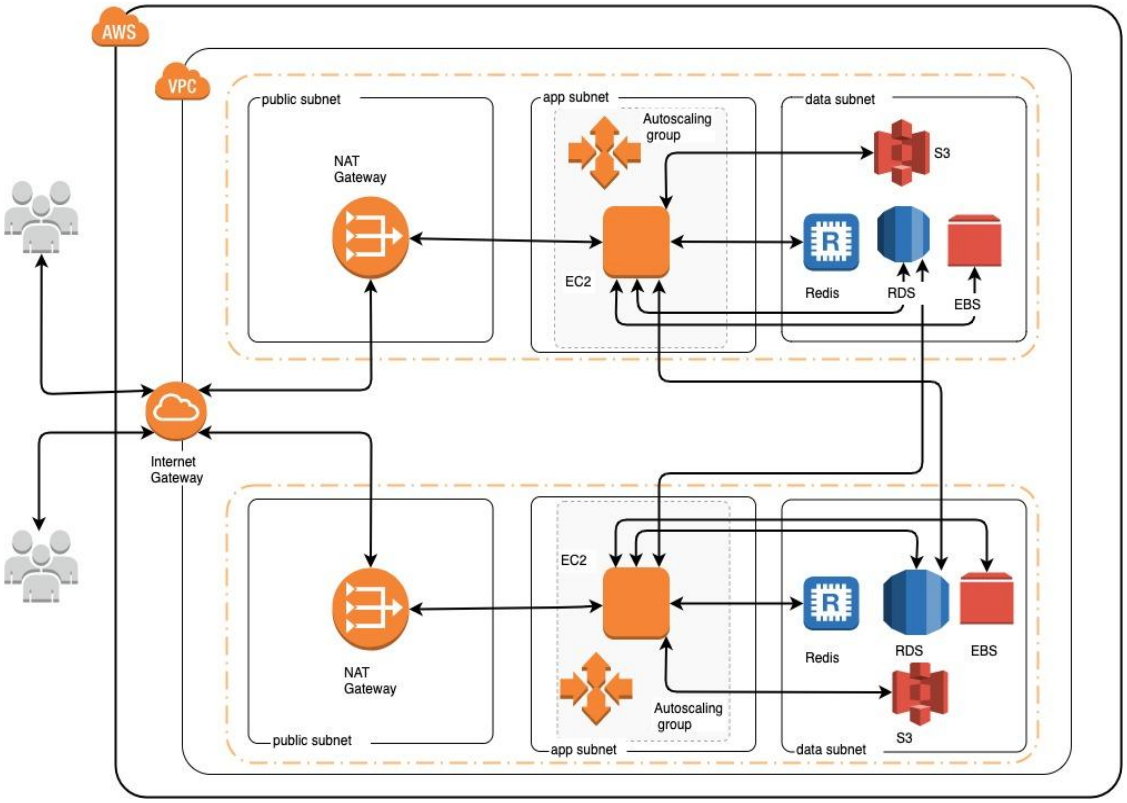
- a zálohování.
- EBS – Elastic Block Storage – poskytuje datové úložiště pro použití s instancemi Amazon EC2 v cloudu AWS.
- Dynamo DB – Databáze typu klíč-hodnota, která poskytuje milisekundový výkon v libovolném měřítku.
- Network load balancer – vyrovnávač zatížení sítě, který automaticky distribuuje příchozí provoz do více cílů.
- ECS – Elastic Container Service – umožňuje spouštět kontejnery, aniž byste museli řídit jejich organizaci.
- ECS task – pro spuštění kontejnerů v Amazon ECS je vyžadována definice úlohy. Některé z parametrů, které můžete určit v definici úlohy, zahrnují:
- Docker image[13], který se má použít s každým kontejnerem ve vaší úloze.
- Kolik CPU a paměti se mají použít s každou úlohou nebo s každým kontejnerem v rámci úlohy.
- OFS – Objectvie FS – sdílený souborový systém, který se přizpůsobuje automaticky, s neomezeným úložištěm a vysokým výkonem.
- CloudFront CDN – služba rychlého doručování obsahu (CDN), která bezpečně dodává data, videa, aplikace a API zákazníkům po celém světě s nízkou latencí a vysokými přenosovými rychlostmi.

[12] Open-source software je typ počítačového softwaru, ve kterém je zdrojový kód uvolňován na základě licence, v níž držitel autorských práv uděluje uživatelům práva ke studiu, změně a distribuci softwaru komukoli a pro jakýkoli účel.
[13] Docker image – šablona (pouze pro čtení) k vytváření kontejnerů. Image se používají k ukládání a odesílání aplikací.

4.3.1.1 Migrace způsobem rehost – Lift and Shift

Na obrázku níže je vidět návrh infrastruktury metodou rehost, kde jsou všechny webové stránky zákazníka umístěny na stejné virtuální instanci.

Obrázek 6 Migrace způsobem Rehost – Lift and Shift



Zdroj: vlastní zpracování

Náklady na budoucí infrastrukturu

I když metoda rehost znamená jednoduché kopírování infrastruktury bez jakýchkoliv změn, existuje možnost přidání Wordpress pluginu, který dovoluje nahradit vestavené databázové funkce Wordpress a změnit model databáze z SQL na NoSQL bez změny kódu, což sníží budoucí náklady. Další možnost ušetření je rezervování výpočetních kapacit na 3 roky.

Tabulka 3 Náklady na služby pro migraci rehost – Lift and Shift (včetně DPH)

Služba	Měsíční splátka
NAT Gateway	$ 37,44
EC2 (m5a.2xlarge – 32 GiB, 8 vCPU)	$ 299,52
EC2 (m5a.2xlarge – reserved instance)	$ 213,12
Redis (cache.t2.medium 2vCPU 3.22 GiB)	$ 56,16
RDS (db.r4.large – 2 vCPU, 15.25GiB)	$ 325,00
EBS (per 100 GB)	$ 11,90
S3 (per 100 GB)	$ 3,69
Dynamo DB	$ 8,42
Data	$ 14,80

Zdroj: vlastní zpracování

Tabulka 4 Náklady na infrastrukturu rehost – Lift and Shift (včetně DPH)

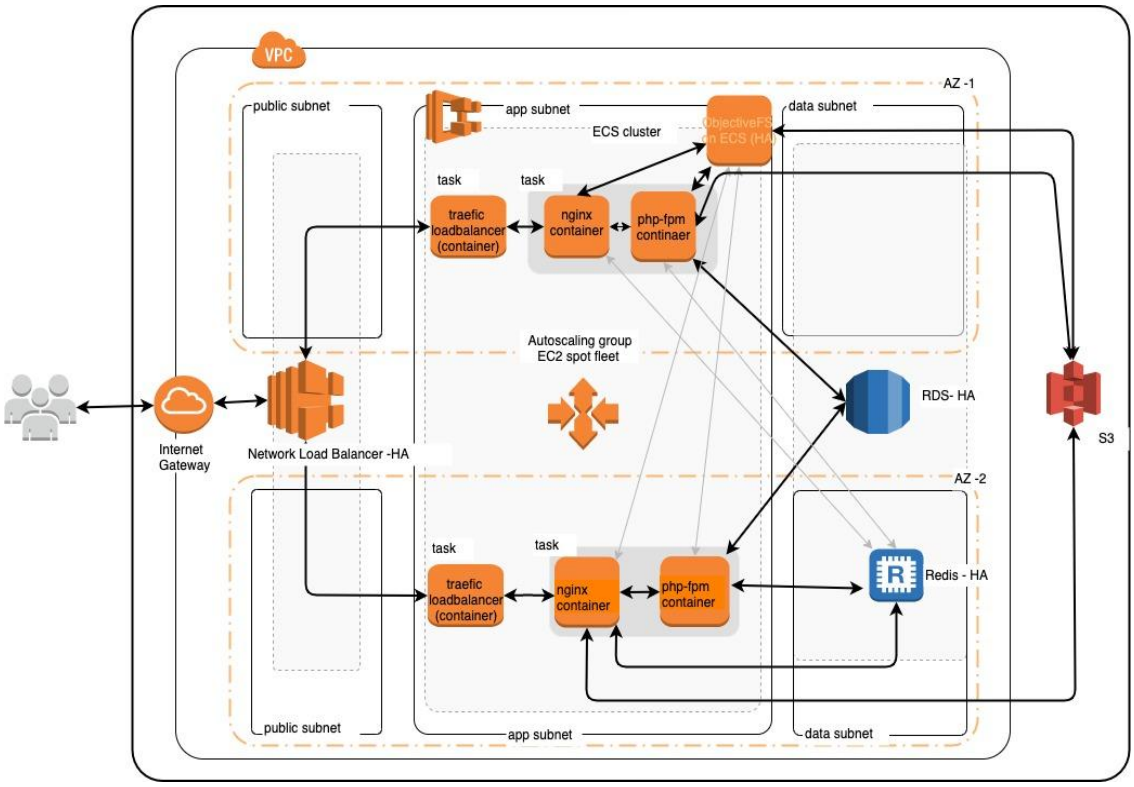
Služba	Lift and Shift	Lift and Shift – reserved
2 NAT Gateway	$ 74,88	$ 74,88
17 EC2: m5a.2xlarge	$ 5091,84	
17 EC2: m5a.2xlarge – reserved		$ 3623,04
Redis: cache.t2.medium	$ 325	$ 325
RDS: db.r4.large	$ 56,16	
EBS (2 TB)	$ 238	$ 238
S3	$ 430	$ 73,8
Dynamo DB		$ 8,42
Data	$ 299,52	$ 299,52
Celkem	**$ 6515,4**	**$ 4998,86**

Zdroj: vlastní zpracování

4.3.1.2 Migrace způsobem refactoring – microservice

Na obrázku níže je vidět návrh infrastruktury metodou refactoring, kde jsou webové stránky zákazníka rozděleny a seskupeny do malých kontejnerů.

Obrázek 7 Migrace způsobem refactoring – microservice



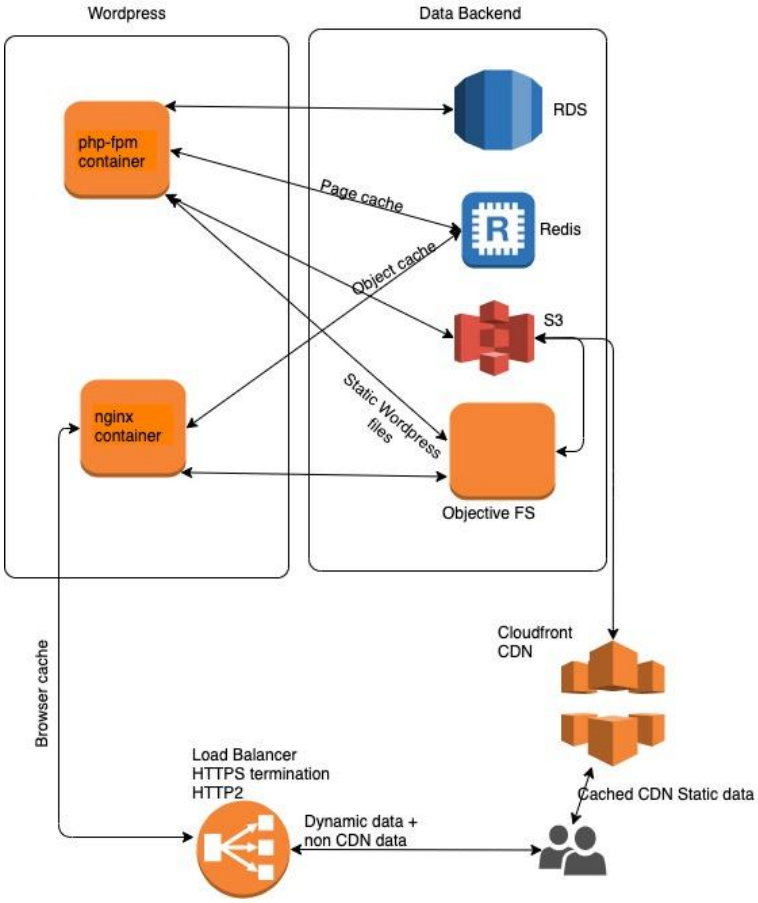
Zdroj: vlastní zpracování

Přehled mikroservisů

Základní myšlenkou adaptace mikroservisní architektury je rozdělení jednotlivých procesů do samostatných kontejnerů. Ve WordPress se dá oddělit PHP-FPM[14] a Nginx[15] do různých kontejnerů a nový způsob informačního toku WordPress je dále představen na obrázku.

[14] FastCGI Process Manager – odpovídá za spuštění PHP skriptů
[15] Webserver

Obrázek 8 Nový způsob informačního toku WordPress



Zdroj: vlastní zpracování

Náklady na budoucí infrastrukturu

Jedna z možností ušetření stejně jako i v předchozím příkladě je rezervování výpočetních kapacit na 3 roky – sloupec „Microservices – reserved¨. ECS, který používáme pro kontejnerizace aplikace, nabízí možnost využití spotových instancí – nepoužitá instance EC2, která je k dispozici za nižší cenu, než je cena na vyžádání. Spot instance běží, kdykoli je k dispozici kapacita a naše stanovená maximální cena za hodinu je větší než spot cena.

Tabulka 5 Náklady na služby pro migraci refactoring – microservices (včetně DPH)

Služba	Měsíční splátka
Network Load balancer	$ 19,71
EC2 (m5a.large – 8 GiB, 2 vCPU)	$ 299,52
EC2 (m5a.large – reserved instance)	$ 213,12
EC2 (m5a.large – spot instance)	$ 100,22
Redis (cache.t2.medium 2vCPU 3.22 GiB)	$ 56,16
RDS (db.r4.large – 2 vCPU, 15.25GiB)	$ 325,00
OFS (10 licenci)	$ 300
S3 (per 100 GB)	$ 3,69
Data	$ 14,80

Zdroj: vlastní zpracování

Tabulka 6 Náklady na služby pro migraci refactoring – microservices (včetně DPH)

Služba	Základna infrastruktury – Microservices	Microservice – reserved	Microservice – spot
3 Load Balancers	$ 74,88	$ 74,88	$ 74,88
12 EC2: m5a.2xlarge	$ 3 594,24		
12 EC2: m5a.2xlarge –reserved		$ 2 557,44	
12 EC2: m5a.2xlarge – spot			$ 1 202,64
1 Redis: cache.t2.medium	$ 56,16	$ 56,16	$ 56,16
2 RDS: db.r4.large	$ 650,00	$ 650,00	$ 650,00
0FS (10 licenci)	$ 300,00	$ 300,00	$ 300,00
S3	$ 1 000,00	$ 1 000,00	$ 1 000,00
Data	$ 299,52	$ 299,52	$ 299,52
Celkem	$ 5 974,80	$ 4 938,00	$ 3 583,20

Zdroj: vlastní zpracování

Náklady na jednoho uživatele

Kvůli úsporám z rozsahu očekáváme se zvýšením počtu uživatelů snížení nákladů na infrastrukturu. Náklady na infrastrukturu jsou představeny ve variantě základní infrastruktura – microservices a vypočtení kapacity v této variantě je zcela dostačující k obsluze 20 tisíc uživatelů. Předpokládáme, že díky nesledující optimalizaci se dostaneme na cenu o cca 25–30 % nižší, než je zde uvedeno, ale není možné to přesně odhadnout.

Tabulka 7 Náklady na jednoho uživatele (včetně DPH)

Počet uživatelů	Náklady na infrastrukturu	Náklady na správu	Celkové náklady na 1 uživatele	Celkem
2000	$ 2,99	$ 1,30	$ 4,29	$ 8 574,80
5000	$ 1,19	$ 1,30	$ 2,49	$ 12 474,80
10000	$ 0,60	$ 1,30	$ 1,90	$ 18 974,80
20000	$ 0,30	$ 1,30	$ 1,60	$ 31 974,80

Zdroj: vlastní zpracování

5 Výsledky a diskuze

Hlavním cílem diplomové práce bylo provést migraci aplikace s třívrstvou architekturou do cloudu. Před samotnou migrací bylo potřeba provést analýzu současné architektury aplikace s možností návrhu na zlepšení a posoudit na trhu existující nabídky od cloudových providerů.

Provedená práce se skládala ze čtyř částí. První část představovala rozhodnutí o způsobu nasazení cloudu – na základě provedené analýzy byla vybrána migrace do veřejného cloudu. Dalším krokem bylo posouzení distribučního modelu budoucí infrastruktury – IaaS byl vybrán jako nejvíce odpovídající. Dále následovalo porovnání IaaS nabídek od tří největších cloudových poskytovatelů a Amazon Web Services měl největší průměr při hodnocení kritických schopností. V poslední části byly navrženy 2 způsoby migrace a uvedené odpovídající budoucí náklady na novou infrastrukturu.

5.1 Zhodnocení a výběr infrastruktury

Zákazník předem stanovil určité požadavky na infrastrukturu, dle kterých je potřebné ocenit provedenou práce:

- Nejsou časté výpadky u poskytovatele cloudových služeb.
- Vysoká dostupnost.
- Plné využití serverů.
- Jednoduché spravování serverů.
- Schopnost snižovat servery.

5.1.1 Lift and Shift

Nejsou časté výpadky u poskytovatele cloudových služeb

Řešení je založené na stabilních službách AWS, v roce 2019 byl pouze jeden velký výpadek EC2[16].

Vysoká dostupnost

Migrace typu Lift and Shift neobsahuje řešení pro vysokou dostupnost. Není možné v případě potřeby zvýšit výpočetní kapacity pouze pro jeden web, ale pouze pro celý virtuální stroj.

Plné využití serverů

Při potřebě dodatečného místa je možnost přidat navíc EBS úložiště bez navýšení velikosti serveru, ale vždy je toto dodatečné množství větší, než je potřeba, což neřeší problém úplně. To samé se týká i samotných serverů, že se zvětšením počtu CPU a RAM vždy budou výpočetní kapacity, které nejsou využívané a přináší další náklady.

Jednoduché spravování serverů

AWS poskytuje centralizovanou kontrolu přístupu k instancím EC2 na úrovni uživatele a instance. Zásady a principy IAM odstraňují potřebu sdílení a správy klíčů SSH. Mezi automatizaci v této infrastruktuře můžeme zařadit autoscaling (automatická škálovatelnost) serverů a databáze.

Schopnost snižovat servery

AWS poskytuje možnost snižovat velikost serveru během pár minut.

5.1.2 Microservices

Nejsou časté výpadky u poskytovatele cloudových služeb

Jak už bylo řečeno v předchozí kapitole, řešení je založené na stabilních službách AWS.

[16] Summary of the Amazon EC2 and Amazon EBS Service Event in the Tokyo (AP-NORTHEAST-1) Region, August 23, 2019: https://aws.amazon.com/ru/premiumsupport/technology/pes/

Vysoká dostupnost

Kvůli tomu, že každá web stránka má svoje vlastní kontejnery, je jednoduché nastavit podmínky navýšení výpočetní kapacity pro určitý web bez vlivu na ostatní hostingy.

Plné využití serverů

Při mikroservisní architektuře při potřebě dodatečného místa využíváme jednoduše škálovatelnou službu Objective FS pro statické soubory a pro zvětšení počtu CPU a RAM přidáváme další kontejnery, což nám poskytne možnost využít pouze potřebné výpočetní kapacity.

Jednoduché spravování serverů

AWS poskytuje centralizovanou kontrolu přístupu ke kontejnerům ECS pomocí konzole a příkazového řádku.

Schopnost snižovat servery

AWS poskytuje možnost snižovat počet kontejnerů jak na základě automatické škálovatelnosti, tak i ručně.

5.1.3 Cena nové infrastruktury

Níže je uveden přehled cen pro různé typy migrací do cloudu.

Tabulka 8 Náklady na budoucí infrastrukturu (včetně DPH)

	Cena za jednoho uživatele	Měsíční cena	20 tisíc uživatelů
Současná infrastruktura	$ 0,40	$ 2590	$ 8000
Lift and Shift	$ 1,01	$ 6515,4	$ 20200
Lift and Shift – reserved	$ 0,77	$ 4998,9	$ 15400
Microservices	$ 0,75	$ 5974,8	$ 15000
Microservices – reserved	$ 0,62	$ 4938	$ 12400
Microservices – spot	$ 0,45	$ 3583,2	$ 9000

Zdroj: vlastní zpracování

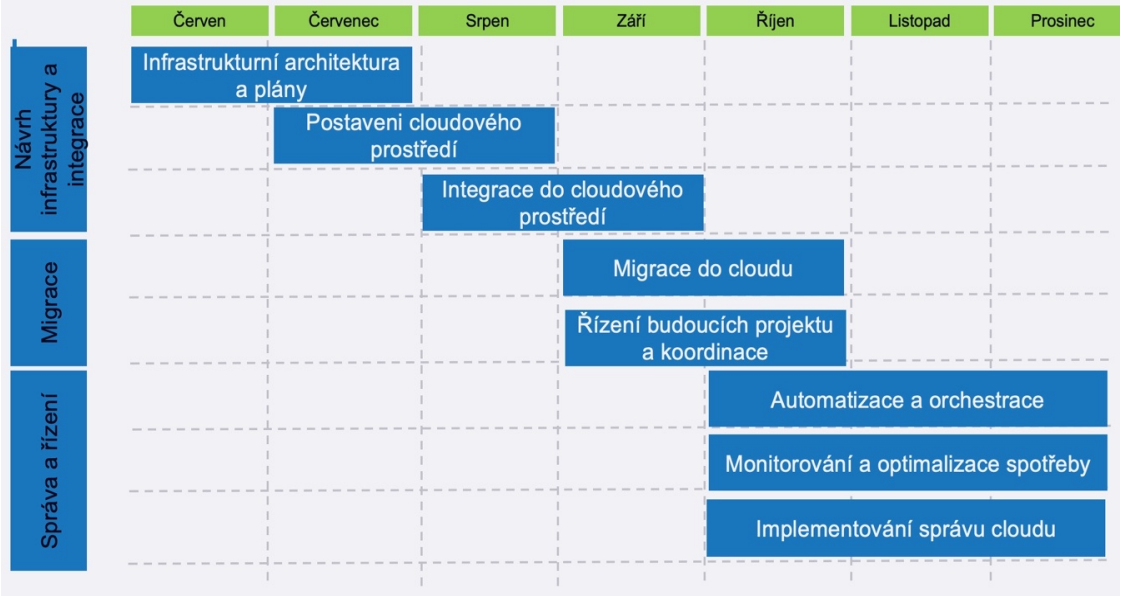
5.1.4 Shrnutí výběru a návrh migrační mapy

Na základě poskytnuté informace ohledně způsobu migrace, budoucí infrastruktuře a cenách na tuto infrastrukturu se zákazník rozhodl pokračovat s metodou microservices – spot. I když celkové náklady jsou o 11,1 % vyšší v porovnání s již

existující infrastrukturou, prioritou u společnosti Extraweb je vysoká dostupnost zákaznických webů a možnost obsloužení dalších zákazníků bez jakýchkoliv omezení a při plném využití již zakoupené výpočetní kapacity.

Dalším krokem bylo požádání Extrawebu o migrační mapu, kde budou přesně definované konečné termíny každého dílu migrace. Tato mapa byla výsledkem plánování budoucích prací a základem pro odevzdávání nové infrastruktury Extrawebu.

Obrázek 9 Migrační mapa



Zdroj: vlastní zpracování

Celková migrace se skládala ze tří částí:

- Návrh infrastruktury a integrace (červen–září):
  - Infrastrukturní architektura a plány,
  - postavení cloudového prostředí,
  - integrace do cloudového prostředí.
- Migrace (září–říjen):
  - Migrace do cloudu,
  - řízení budoucích projektů a koordinace.
- Správa a řízení (říjen–prosinec):
  - Automatizace a orchestrace,
  - monitorování a optimalizace spotřeby,
  - implementace správy cloudu.

Za úspěšnost projektu bylo považováno rozmístěni webů nových zákazníků na nové infrastruktuře. Projekt byl odevzdán na konci prosince roku 2019 a je považován za úspěšný jak ze strany Extraweb, tak i ze strany LUKAPO s.r.o.

6 Závěr

Cílem práce byla demonstrace migrace do veřejného cloudu aplikace s třívrstvou architekturou, s možností refaktoringu kódu a předělání aplikací do mikroservisní architektury. Zároveň bylo cílem porovnat nabídku existujících cloudových providerů a představení migračních modelů do cloudu i s následnou ukázkou budoucí infrastruktury

Teoretická část představuje pět základních charakteristik cloud computing a popisuje SPI model, který se skládá ze tří distribučních modelů: Software, Platforma a Infrastruktura. Pro každý z modelů jsou sepsané výhody, které organizaci přinesou při využití konkrétního modelu a odpovídajících služeb. Dále jsou v teoretickém východisku představené základní způsoby nasazení, které obecně charakterizují dispozice cloudových výpočetních zdrojů pro spotřebitele. Pro jednoduchou a úspěšnou migraci spotřebitel potřebuje předem stanovit cloudovou migrační strategii, která je představena v této části, a zároveň si vybrat vhodného poskytovatele služby, který bude nejvíce uspokojovat potřeby zákazníka.

Druhá část teoretického východiska popisuje různé architektury aplikací: tradiční dvouvrstvou a třívrstvou architekturu a architekturu zaměřenou na služby (Service oriented architecture – SOA). Mezi SOA patří architektura postavená na mikroservisech, které jsou v současnosti velmi populární. Microservisy mohou věrohodně řešit potřeby vlastního podnikového softwaru a urychlit proces vývoje a testování nových aplikaci.

Vlastní práce se skládá ze tří částí. První představuje charakteristiku společnosti, popisuje její aktivity a architekturu hlavní aplikace, kterou chce podnik migrovat do cloudu. Dále jsou popsané požadavky společnosti a aktuální infrastruktura. Po provedené analýze byly sepsané hlavní příčiny migrace do cloudu a rozpracované měsíční náklady na provoz.

Druhá část je zaměřena na volbu poskytovatelů cloudových služeb. Nejdřív byla stanovena hodnoticí kritéria při výběru poskytovatelů a dále byla na jejich základě provedena analýza. Microsoft Azure, Amazon Web Services a Google Cloud Provider patří mezi největší hráče na trhu, proto hodnocení bylo provedeno pouze u těchto tří poskytovatelů. Každý z nich dostal určitý počet bodů za existenci služeb odpovídajících kriteriím a nejvíce bodů bylo u AWS. Proto následující infrastruktura byla předložena na základě služeb AWS.

Třetí část je věnovaná návrhu infrastruktury pro zákazníka. Byly představeny dva modely migrace – Lift and Shift a refactoring. Každý model obsahuje návrh infrastruktury a propočet budoucí nákladů. U nákladů je ještě vždy představen způsob jejich snížení například pomocí rezervace výpočetních kapacit. Tato část ještě obsahuje náklady na hosting pro lepší porovnání při výběru způsobu migrace.

Pátá část je zaměřena na popis výsledků provedené migrace do veřejného cloudu. Zhodnocení a výběr infrastruktury byly provedeny na základě předem stanovených požadavků od zákazníka a poté byla představena migrační mapa s popisem jednotlivých kroků.

Výstupem této práce není příklad migrace pro určitou společnost, ale představení postupu při migrace do cloudu s podrobným popisem jednotlivých kroků. Principy použité v této práci se dají použít při návrhu infrastruktury ve všech distribučních modelech a při všech způsobech nasazení.

7 Seznam použitých zdrojů

Elektronické

1. Mell, P.; Grance T.: The NIST Definition of Cloud Computing, 2011, National Institute of Standards and Technology Special Publication 800-145. [online]. [cit. 2019-08-05]. Dostupné z: https://csrc.nist.gov/publications/detail/sp/800-145/final
2. ISACA (Information Systems Audit and Control Association), IT control objectives for cloud computing: controls and assurance in the cloud, ISACA, 2011. [online]. [cit. 2019-08-06]. Dostupné z: https://www.isaca.org/chapters2/kampala/newsandannouncements/Documents/IT%20contro%20bjectives%20for%20Cloud%20computing.pdf
3. Public Cloud Computing, Gartner. Gartner.com. 2019. [online]. [cit. 2019-08-20]. Dostupné z: https://www.gartner.com/it-glossary/public-cloud-computing/
4. Gartner, Inc.: Magic Quadrant for Cloud Infastructure as a Service, Worldwide, 2018. [online]. [cit. 2019-08-24]. Dostupné z: https://www.gartner.com/en/documents/3875999
5. Wild and Interesting WordPress Statistics and Facts (2020). [online]. [cit. 2019-08-20]. Dostupné z: https://kinsta.com/blog/wordpress-statistics/

Bibliografické

6. NEWCOMER E., LOMOW G. Understanding SOA with Web Services, 2005. ISBN 978-0321180865.
7. EEL, T.; PUTTINI, R.; MAHMOOD, Z.: Cloud Computing: Concepts, Technology & Architecture, 2013. ISBN 978-01-333-8752-0.
8. HUNTER T., Advanced Microservices: A Hands-on Approach to Microservice Infrastructure and Tooling, 2017. ISBN 978-1-4842-2886-9
9. JAKSON K. L.: Architecting Cloud Computing Solutions: Build cloud strategies that align technology and economics while effectively managing risk, 2018. ISBN 978-1-78847-245-2.
10. LASZEWSKI T.: Cloud Native Architectures: Design high-availability and cost-effective applications for the cloud, 2018. ISBN 978-1-78728-054-0.

11. MANJUNATH G.; SITARAM D.: Moving to the Cloud Developing Apps in the New World of Cloud Computing, 2012. ISBN 978-1-59749-725-1.
12. ROUTREE D.; CASTRILLO I.: The Basics of Cloud Computing: Understanding the Fundamentals of Cloud Computing in Theory and Practice, 2013. ISBN 978-01-240-5932-0.