

Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií



Bakalářská práce

Virtualizace a privátní cloud v moderním IT

Jan Bílek

© 2015 ČZU v Praze

ZADÁNÍ

BAKALÁŘSKÉ

PRÁCE

Jan Bílek

INFOK

Virtualizace a privátní cloud v moderním IT

Virtualization and private cloud in modern IT

Rozsah práce:

40 - 50 stran

Klíčová slova:

virtualizace, VMware, Hyper-V, Microsoft, Cloud

Cíl práce:

Cílem práce je charakterizovat řešení privátního cloudu a jeho nasazení v současných podmínkách IT pomocí nástrojů společností Microsoft a VMware a to v prostředí s vysokým stupněm automatizace. Dílčími cíli jsou porovnat řešení obou dodavatelů na příkladu z praxe - řešení samoobslužného portálu pro vývojáře a finanční zhodnocení řešení obou dodavatelů na praktickém příkladu (privátní cloud – samoobslužný portál pro vývojáře).

Metodika:

Metodika řešené problematiky bakalářské práce je založena na studiu informačních zdrojů, analýze řešení jednotlivých dodavatelů, což představuje charakterizaci platformem a dílčích produktů. Praktická část je založena na implementaci řešení obou dodavatelů v laboratorním prostředí a dále na finančním rozboru. Na základě získaných dat a poznatků bude formulován závěr bakalářské práce.

Harmonogram:

Studium odborných informačních zdrojů, stanovení dílčích cílů a postupu řešení: 06/2014

Zpracování přehledu řešené problematiky: 07/2014 – 08/2014

Vypracování vlastního řešení, diskuse, doporučení a závěry: 09/2014 - 02/2015

Tvorba finálního dokumentu práce: 02/2015 – 03/2015

Odevzdání práce a tezí: 03/2015

Literatura:

Amaris Chris; Rand Morimoto; Pete Handley; David Ross - **Microsoft® System Center 2012 Unleashed**, Sams, ISBN-10: 0-672-33612-X

Marshall Nick, Scott D. Lowe, Forbes Guthrie, Matt Liebowitz, Josh Atwell - **Mastering VMware vSphere 5.5**, SMBX, ISBN: 978-1-118-66114-7

Tulloch Mitch - **Optimizing and Troubleshooting Hyper-V Networking**, Microsoft Press, ISBN:978-0-7356-7900-9

Tulloch Mitch - **Optimizing and Troubleshooting Hyper-V Storage**, Microsoft Press, ISBN:978-0-7356-7898-9

Internetové zdroje:

Performance Best Practices for VMware vSphere® 5.5,
http://www.vmware.com/pdf/Perf_Best_Practices_vSphere5.5.pdf

VMware, Inc., 3401 Hillview Ave. Palo Alto, CA 94304

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Virtualizace a privátní cloud v moderním IT" jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 11. 3. 2015

Poděkování

Rád bych touto cestou poděkoval Ing. Jiřímu Vaňkovi, Ph.D. za jeho konzultace a vedení mé práce, dále potom zástupcům českých poboček společností VMware a Microsoft za poskytnutí užitečných rad. Dále také rodině a všem, kteří mi poskytli podporu při psaní této práce.

Virtualizace a privátní cloud v moderním IT

Virtualization and private cloud in modern IT

Souhrn

Bakalářská práce „Virtualizace a privátní cloud v moderním IT“ analyzuje nový trend v oblasti informačních technologií – cloud computing a jeho využití v moderní IT infrastruktuře. První kapitola vysvětluje virtualizaci - technologii úzce spjatou s cloudem a dále reflektuje obecně přijímané definice cloudu a zavádí členění dle modelů nasazení a distribučních modelů.

Další kapitoly bakalářské práce řeší nasazení privátního cloudu pro firemního zákazníka na příkladu z praxe, a porovnávají řešení dvou největších dodavatelů dané technologie, dostupných na současném trhu.

Závěrečná část poskytuje shrnutí, vyzdvihuje obecné přínosy řešení privátního cloudu pro zákazníka na konkrétním výše uvedeném příkladu, poukazuje na rozdíly řešení obou dodavatelů a prezentuje ekonomickou rozvahu řešení obou dodavatelů.

Klíčová slova: virtualizace, privátní cloud, VMware, Microsoft, Hyper-V, IaaS, SaaS, PaaS

Summary

Bachelor thesis "Virtualization and private cloud in the modern IT" analyzes the new trend in information technology - cloud computing and its use in modern IT infrastructure. The first chapter explains the historical context and virtualization - technology closely related to the cloud, reflects the general definition of „cloud“ and introduces a classification according to deployment and distribution models. In subsequent chapters, deals with private cloud deployment for business customer on example of best practice solution and compares solution provided by two largest suppliers of this technology on market today. The final section provides a summary, highlights the general benefits of private cloud on specific example mentioned above, highlights the differences of solutions of both suppliers and presenting economic balance of both vendors.

Keywords: virtualization, private cloud, VMware, Microsoft, Hyper-V, IaaS, SaaS, PaaS

Obsah

1	Úvod.....	11
2	Cíl práce a metodika	13
2.1	Cíl práce.....	13
2.2	Metodika	13
3	Teoretická východiska	14
3.1	Virtualizace.....	14
3.1.1	Virtualizace hardwaru.....	15
3.1.2	Hardwarové rozšíření CPU pro podporu virtualizace.....	19
3.1.3	Hypervizory podle Microsoftu a VMware.....	20
3.1.4	Výhody virtualizace	23
3.1.5	Nevýhody virtualizace	23
3.2	Cloud.....	24
3.2.1	Definice Cloudu podle NIST	24
3.2.2	Výhody privátního cloudu	27
3.2.3	Nevýhody privátního cloudu	31
4	Vlastní práce	32
4.1	Microsoft.....	32
4.1.1	Komponenty.....	32
4.1.2	Instalace a konfigurace prostředí	35
4.2	VMware	49
4.2.1	Komponenty.....	49
4.2.2	Instalace a konfigurace prostředí	51
5	Zhodnocení výsledků.....	72
5.1	Technické srovnání	72
5.2	Ekonomické porovnání	72
5.2.1	Microsoft.....	73
5.2.2	VMware	74
6	Závěr	75
7	Seznam použitých zdrojů.....	76

Seznam obrázků

Obrázek 1- Gartner magic quadrant for virtualization 2014.....	12
Obrázek 2- konsolidace serverů pomocí virtualizace	15
Obrázek 3- režimy privilegií architektury x86 bez virtualizace	15
Obrázek 4- režimy privilegií architektury x86 - plná virtualizace s binárním překladem...	17
Obrázek 5- porovnání Type 1 a Type 2 hypervisorů.....	18
Obrázek 6- režimy privilegií architektury x86 - paravirtualizace.....	19
Obrázek 7- režimy privilegií architektury x86 –virtualizace s HW podporou CPU	20
Obrázek 8- Monolitický hypervisor	21
Obrázek 9- Mikrokernel hypervisor	22
Obrázek 10- Model služeb podle NIST	26
Obrázek 11- Microsoft Private Cloud.....	33
Obrázek 12- Instalátor SCVMM.....	36
Obrázek 13- System Center Virtual Machine Manager - Konzole.....	37
Obrázek 14- SCVMM konzole - zobrazení Cloudu	38
Obrázek 15- SCVMM, vytvoření služby - vzor	39
Obrázek 16- SCVMM - vytvoření služby - Service Template Designer.....	40
Obrázek 17- Instalace App Controller	41
Obrázek 18- App Controller - portál.....	42
Obrázek 19- App Controller - připojení k SCVMM.....	43
Obrázek 20- App Controller - portál.....	44
Obrázek 21- App Controller - portál, přehled.....	45
Obrázek 22- App Controller - Vytvoření služby	46
Obrázek 23- App Controller - služba.....	47
Obrázek 24- App Controller - nasazená služba	48
Obrázek 25- VMware vCloud suite	49
Obrázek 26- vCenter - Deploy OVF Template.....	52
Obrázek 27- Deploy OVF Template - volba zdroje	53
Obrázek 28- Deploy OVF Template - OVF Detaily.....	54
Obrázek 29- vCenter server instalace konzole	55
Obrázek 30- vCenter web client	56
Obrázek 31- VMware Identity Appliance – nasazení přes web client	57

Obrázek 32- VMware Identity Appliance - webové rozhraní	57
Obrázek 33- VMware Identity Appliance - připojení do domény	58
Obrázek 34- vCloud Automation Center - instalace OVF.....	58
Obrázek 35- vCAC - konzole	59
Obrázek 36- vCAC - konfigurace SSO.....	60
Obrázek 37- vCAC web klient - ověření	60
Obrázek 38- vCAC web klient – administrátor přihlášen.....	61
Obrázek 39- vCAC IaaS - Instalace.....	62
Obrázek 40- vCAC IaaS Instalátor	63
Obrázek 41- vCAC IaaS - konfigurace SSO	64
Obrázek 42- vCAC - instalace dokončena.....	65
Obrázek 43- vCAC - Identity Store	66
Obrázek 44- vCAC - konfigurace blueprint	67
Obrázek 45- vCAC - nastavení služby	68
Obrázek 46- vCAC - žádost o službu	69
Obrázek 47- vCAC - žádost podána	70
Obrázek 48- vCAC - Requests.....	70
Obrázek 49- vCAC - žádost úspěšně dokončena.....	71
Obrázek 50- vCenter server - vytvořena služba.....	71

Seznam tabulek

Tabulka 1- Licence Microsoft.....	73
Tabulka 2- Licence VMware	74

Seznam použitých zkratk a pojmů

OVF – Open Virtualization Framework

OVA – Open Virtual Appliance

SCVMM – System Center Virtual Machine Manager

SCAC – System Center App Controller

SSO – Single Sign On

VCAC – vCloud Automation Center

VMM - Virtual Machine Monitor

1 Úvod

K výběru tohoto tématu autora motivovuje jeho vztah k informačním technologiím a hlavně virtualizaci operačních systémů, kterou se autor zabývá již od vstupu této technologie na trh. Tehdy se jednalo o dnes již notně zastaralý systém VMware ESX, který ale umožňoval tehdy nevídanou a neobvyklou (alespoň co se IT v tehdejších společnostech týká) možnost provozovat současně několik operačních systémů na jednom fyzickém hardwaru.

V následujících letech společnost VMware představila technologii VMotion, která umožňovala virtuální stroj za chodu přesunout z jednoho fyzického stroje na druhý, bez výpadku, bez přerušení chodu a naprosto transparentně pro operační systém a aplikace na něm běžící. Tato funkcionality, a virtualizace obecně, předpověděla budoucnost v IT a obecně směr, jakým se firemní IT a IT v datacentrech bude ubírat. V té době se, tak jak je to obvyklé, jednalo o technologii dostupnou jen velkým firmám, a to ještě navíc jen těm, které mohly sáhnout hlouběji do rozpočtu.

Časem ale, jak se virtualizační technologie rozšiřovaly a zlevňovaly, začaly být dostupné pro širší spektrum zákazníků a dnes tvoří virtualizované servery, podle analytické společnosti Gartner, více než 50 % instalovaných serverů (1) a předpokládá se, že toto číslo v roce 2016 vystoupá až na 86 %.

Virtualizace se tedy stala jakýmsi průmyslovým standardem. Virtualizuje se jak ve velkých nadnárodních společnostech, tak v menších firmách. Virtualizují se souborové servery, print servery, terminálové servery, databáze, ale také koncové stanice a pracovní plochy pro uživatele.

S rozšířením virtualizace do všech zákoutí IT, přišly další výzvy v podobě správy rozsáhlé virtuální infrastruktury. Spravovat infrastrukturu, obsahující několik tisíců virtuálních strojů, vyžaduje zcela odlišný přístup, vedoucí ke snaze co nejvíce administrativních úkolů automatizovat. Pryč jsou doby, kdy pro nasazení nového serveru bylo nutné koupit nový hardware, nainstalovat ho do racku, připojit ho do sítě, nakonfigurovat, nainstalovat operační systém, nainstalovat záplaty, nainstalovat aplikace atd. Dnes, s využitím virtualizačních nástrojů a nástrojů pro automatizaci, stačí jen přes webový prohlížeč vyplnit formulář na samoobslužném portálu a software se postará o zbytek, například vytvoří virtuální stroj, nastaví mu IP adresu, nainstaluje do něj potřebné aplikace, nainstaluje aktualizace, vytvoří potřebné uživatelské účty a až je vše hotovo, odešle žadateli email s přístupovými údaji.

To umožňuje „privátní cloud“, jež není to samé co virtualizace, ačkoliv mnohdy se tyto dva pojmy zaměňují. Několik virtualizovaných serverů ještě netvoří cloud. Společnými jmenovateli cloudu jsou témata jako automatizace, IT služby, nebo samoobslužnost. Virtualizace zde ovšem hraje hlavní roli a je základním stavebním kamenem privátního cloudu.

Podrobně se virtualizací zabývá kapitola „Teoretická východiska“, která mimo jiné popisuje historii virtualizace a postupný přechod k modernímu „cloudu“ včetně důvodů, které k tomu vedly.

Další kapitola porovnává řešení dvou vybraných dodavatelů technologie pro privátní cloud na vybraném modelu z praxe – testovací prostředí pro vývojáře, fungující jako samoobslužný portál. Porovnání probíhá formou kompletní implementace řešení obou dodavatelů v laboratorním prostředí a následném hodnocení řešení z pohledu náročnosti instalace, jednoduchosti ovládnutí pro uživatele a administrátora. Součástí je i ekonomická rozvaha náročnosti jednotlivých řešení. Porovnávány jsou produkty společností VMware a Microsoft, jež jsou stabilně označovány za leadery ve virtualizačním průmyslu.

Obrázek 1- Gartner magic quadrant for virtualization 2014



Zdroj: DataCenterPost.com (1)

2 Cíl práce a metodika

2.1 Cíl práce

Cílem práce je charakterizovat řešení privátního cloudu a jeho nasazení v současných podmínkách IT pomocí nástrojů společností Microsoft a VMware a to v prostředí s vysokým stupněm automatizace. Dílčími cíli jsou porovnání řešení obou dodavatelů na příkladu z praxe - řešení samoobslužného portálu pro vývojáře a finanční zhodnocení řešení obou dodavatelů na praktickém příkladu (privátní cloud – samoobslužný portál pro vývojáře).

2.2 Metodika

Metodika řešené problematiky bakalářské práce je založena na studiu informačních zdrojů, analýze řešení jednotlivých dodavatelů, což představuje charakterizaci platformy a dílčích produktů. Praktická část bakalářské práce je založena na implementaci řešení obou dodavatelů v laboratorním prostředí a dále na finančním rozboru. Na základě získaných dat a poznatků bude formulován závěr bakalářské práce.

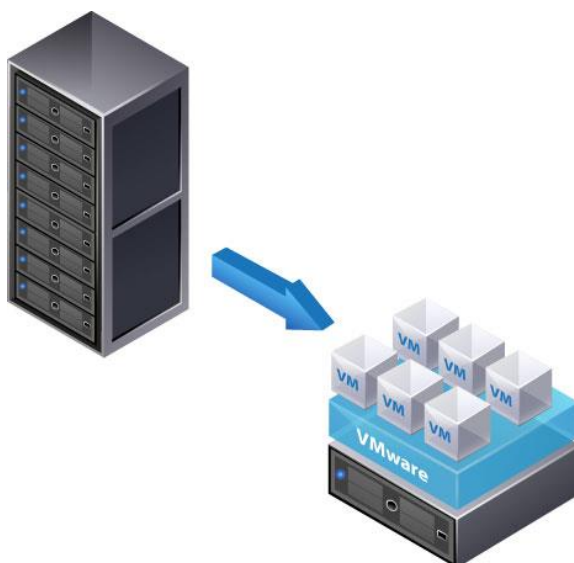
3 Teoretická východiska

3.1 Virtualizace

Historie termínu „virtualizace“ sahá až do šedesátých let dvacátého století. Tehdy byl termín „virtualizace“ použit v souvislosti s logickým rozdělením zdrojů sálového počítače pro různé aplikace (2). Od té doby se význam pojmu posunul a rozšířil a dnes rozlišujeme několik rozdílných typů virtualizace, mezi příklady patří virtualizace aplikací (application virtualization), pracovních ploch (desktop virtualization), uživatelská virtualizace (user virtualization), virtualizace sítě (network virtualization) a v neposlední řadě také virtualizace hardwaru, případně serverů (hardware/server virtualization), která je úzce spjatá s cloudovými službami a proto jí je věnována pozornost podrobně v následujících odstavcích.

Motivací pro rozvoj současných virtualizačních platform, byla situace vzniklá v devadesátých letech po rozšíření klient-server řešení a masivnímu nasazování serverových operačních systémů Linux a Windows. Typicky, z důvodů vzájemné nekompatibility aplikací a bezpečnosti, se nasazovaly dedikované servery pro jednu aplikaci tak, aby případný výpadek jednoho serveru nezpůsobil pád několika aplikací. Takové servery běžely velmi často s nízkým zatížením (řádově 10 - 40 %), avšak z výše uvedených důvodů nebylo možné aplikace konsolidovat na jeden fyzický server a snížit tak množství fyzických serverů a s ním související spotřebu elektrické energie, produkci tepla, potřebu chlazení atd. Řešení v roce 1999 uvedla na trh jako první společnost VMware s produktem, který umožňoval virtualizaci počítačů na platformě x86.

Obrázek 2- konsolidace serverů pomocí virtualizace

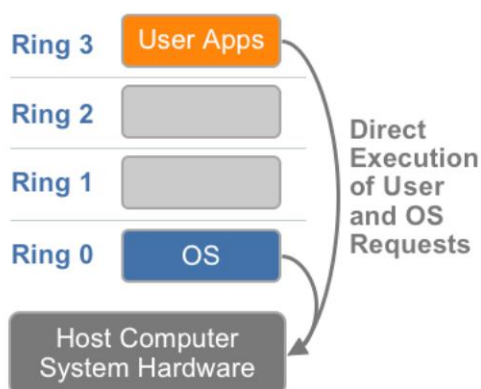


Zdroj: VMware (3)

3.1.1 Virtualizace hardwaru

Stejně jako většina ostatních platform, je i x86 navržena pro provoz současně pouze jednoho operačního systému. Platforma x86 používá pro provádění instrukcí čtyři režimy privilegií, nazývané ring 0 až ring 3. V části označené ring 0 (privilegovaná úroveň, úroveň jádra – angl. privilege level/root level) je spuštěno jádro OS, které má právo spouštět privilegované instrukce. V části označené jako ring 3 (neprivilegovaná úroveň, uživatelská úroveň – angl. least privilege level/user mode) se spouští aplikace. Ring 1 a 2 se v běžných OS nepoužívá (4).

Obrázek 3- režimy privilegií architektury x86 bez virtualizace



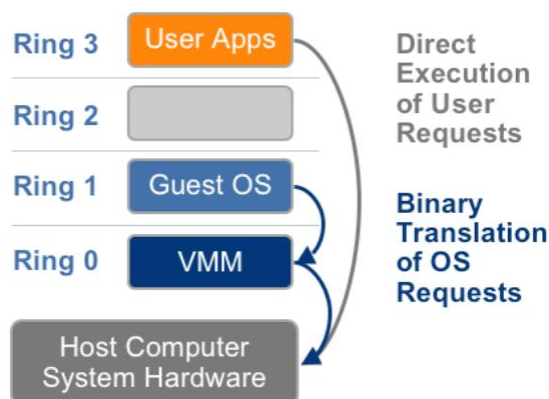
Zdroj VMware (5)

Virtualizace hardwaru spoléhá na vytvoření virtuálního počítače. Virtuální počítač se chová stejně jako skutečný – fyzický počítač s operačním systémem. Společně s virtualizací hardwaru, zavádíme pojmy „host“ nebo „virtuální stroj“ (anglicky: guest) a hostitel (anglicky host). Tyto pojmy zavádíme z důvodu odlišení softwaru běžícího na fyzickém počítači a softwaru běžícím na virtuálním počítači. Kód, který se provede na virtuálním počítači, je oddělen od hardwaru, na kterém běží hostitel. Software, který běží přímo na fyzickém hardwaru a spravuje virtuální stroje, se nazývá „hypervizor“ (někdy také VMM-Virtual Machine Monitor). Rozlišujeme 3 základní typy virtualizace hardwaru (5).

Plná virtualizace

Termín plná virtualizace (Full Virtualization) označuje způsob virtualizace, při kterém je virtuální stroj, pomocí vrstvy hypervizoru, plně oddělen od fyzického stroje na kterém běží. Neví, že je virtualizován a pro chod v tomto prostředí nejsou vyžadovány žádné úpravy jádra. Hypervizor v tomto případě poskytuje virtuálnímu stroji všechny služby jako na fyzickém systému – virtuální správu paměti, BIOS, zařízení atd. S plnou virtualizací se nekritické instrukce (ty, které nekontrolují napřímo hardware a neohrožují bezpečnost systému) spouští přímo na hardwaru, zatímco kritické instrukce (kontrolující hardware přímo) jsou emulovány pomocí binárního překladu (angl. Binary Translation). Důvod tohoto rozdělení je ten, že binární překlad vyžaduje výkonovou režii. Rozdělení na nekritické a kritické instrukce a jejich provádění odlišnými způsoby proto pomáhá zvýšit výkon, ale také zajistit bezpečnost systému. Proto plná virtualizace kombinuje binární překlad a přímé provádění kódu. Virtuální operační systém je zcela oddělen od základního hardwaru a v důsledku toho OS virtuálního stroje neví, že je právě virtualizován, což zajišťuje bezpečnost a jeho snadnou přenositelnost.

Obrázek 4- režimy privilegií architektury x86 - plná virtualizace s binárním překladem



Zdroj: VMware (5)

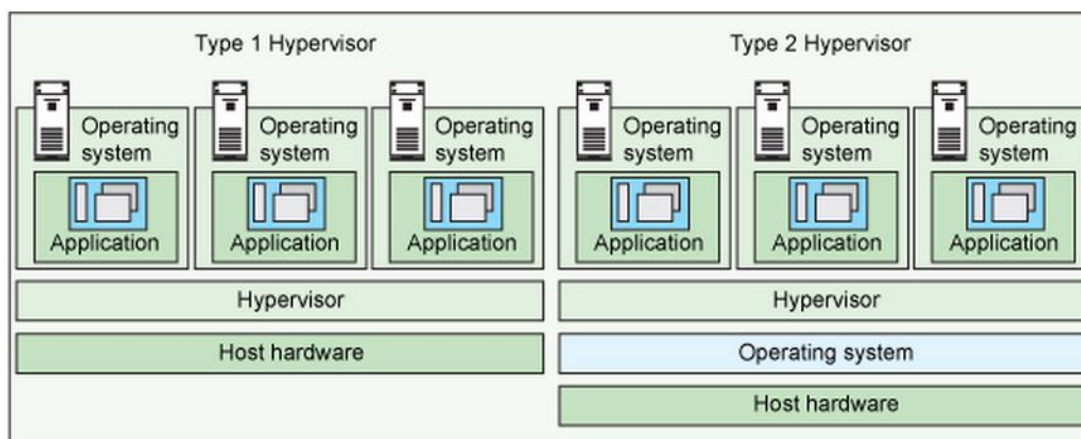
Výkon plné virtualizace nemusí být ideální, protože zahrnuje binární překlad, který je poměrně náročný. Výkon plné virtualizace na architektuře x86 je obvykle 80 – 97 % výkonu, dosažitelného na hardwaru hostitelského počítače. Výrobci CPU proto vyvinuli technologie pro podporu tzv. hardwarově asistované virtualizace, která nabízí obecně lepší výkon – podrobněji se tomuto tématu věnuje kapitola 3.1.2. „Hardwarové rozšíření CPU pro podporu virtualizace“.

Plná virtualizace je technika, která je dnes běžně využívána společnostmi VMware (v produktu ESXi) a Microsoft (v produktu Hyper-V).

Host-based virtualizace

Alternativně lze provozovat virtualizaci také nad úrovní hosta a jeho operačního systému. V tomto případě se hypervizorem stává virtualizační aplikace (např. VirtualBox, VMware Workstation). Hostitelský operační systém je stále zodpovědný za zprostředkování kontaktu s hardwarem a můžou na něm běžet – a obvykle běží – i další aplikace. Vzhledem k další úrovni překladu instrukcí, vykazuje host-based virtualizace nižší výkon než ostatní typy. Tento typ hypervizoru se někdy nazývá také Layer 2, Type 2, nebo hosted hypervizor. Zatímco produkty VMware ESXi, případně Microsoft Hyper-V jsou řazeny do skupiny Layer 1 hypervizorů (nebo Type 1, native, bare metal).

Obrázek 5- porovnání Type 1 a Type 2 hypervizorů



Zdroj: IBM (6)

Mezi výhody host-based virtualizace patří jednoduchost instalace bez nutnosti provádění změn v hostitelském systému a také fakt, že o ovladače a komunikaci s hardwarem se stará hostitelský systém a virtualizační software již toto nemusí řešit.

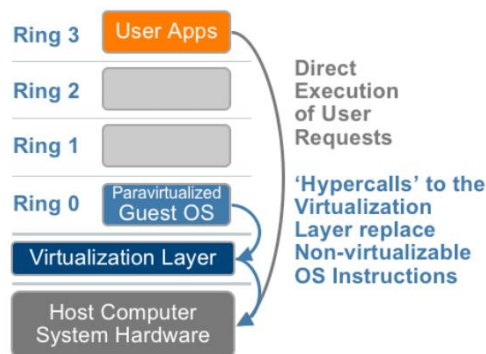
Nevýhodou je snížení výkonu oproti adekvátnímu řešení na bázi layer 1 hypervizoru. Proto se host-based virtualizace nepoužívá pro kritické aplikace, které vyžadují vysoký výkon.

Tento typ virtualizace je typický pro klientské stroje a testování, kdy je možné simulovat běh aplikace v jiném operačním systému v rámci jednoho klientského počítače. Typickým příkladem použití je vývojář aplikací, který chce otestovat, jak jeho aplikace funguje na jiném operačním systému. Nejjednodušším způsobem je instalace virtuálního stroje s požadovaným OS pomocí jednoho z výše zmiňovaných nástrojů host-based virtualizace.

Paravirtualizace

Paravirtualizace je založena na komunikaci virtuálního stroje s hypervizorem za účelem zlepšení výkonu a efektivity. Na rozdíl od ostatních typů, u paravirtualizace je nutný zásah do virtualizovaného systému. V rámci tohoto zásahu jsou některé instrukce v jádře virtualizovaného systému, které by se jinak překládaly pomocí náročného binárního překladu, nahrazeny „voláními hypervizora“ (angl. hypercalls), pomocí kterých komunikuje operační systém virtuálního stroje přímo s hypervizorem.

Obrázek 6- režimy privilegií architektury x86 - paravirtualizace



Zdroj: VMware (5)

Paravirtualizace se tím liší od plné virtualizace, kde operační systém virtuálního stroje nemusí být modifikován a neví, že je virtualizován, chová se stejně jako by virtualizován nebyl a volání jsou zachycena hypervizorem a provedena pomocí binárního překladu.

Jako výhodou paravirtualizace je označována snížená režie hypervizoru v porovnání s plnou virtualizací. Toto ale velmi záleží na typu zátěže, která je na daném systému provozována.

Mezi nevýhody patří nemožnost provozování proprietárních systémů, které neumožňují úpravu jádra (Microsoft Windows).

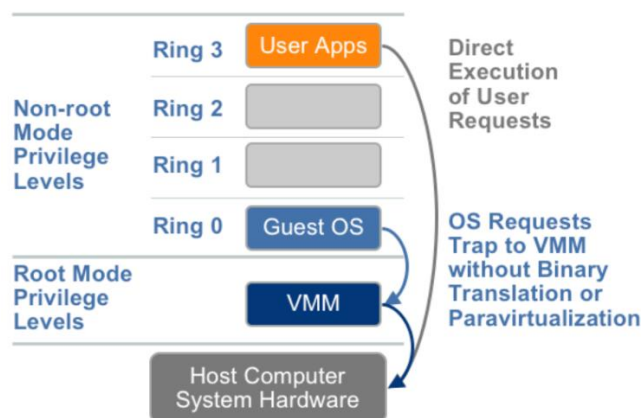
Příkladem hypervizoru, který využívá paravirtualizaci pro CPU a operační paměť, je open-source projekt XEN, který využívá modifikované linuxové jádro.

Častěji, než při virtualizování instrukcí CPU, je paravirtualizace využívána ve spojení s I/O zařízeními a to dodatečnou instalací paravirtualizovaných ovladačů do hostovaného systému. V případě společnosti VMware se jedná o instalaci tzv. „VMware tools“ a v případě produktů společnosti Microsoft se do operačního systému virtuálního stroje instalují „Hyper-V integration components“ jež zahrnují například ovladače pro síťovou kartu, které komunikují přímo s hypervizorem, což velmi výrazně zvyšuje výkon a snižuje zatížení CPU.

3.1.2 Hardwarové rozšíření CPU pro podporu virtualizace

Výrobci CPU Intel a AMD vyvinuli způsob, jakým lze hypervizor spustit v režimu vyšších privilegií než Ring 0. Technologie nese název VT-x pro Intel a AMD-V pro AMD. Přidává k existujícím ještě Ring -1 (Super Privilege Mode), ve kterém běží hypervizor a umožňuje virtuálním strojům používat nativně jak Ring 0 tak Ring 3, zatímco hypervizor běží v novém modu bez nutnosti použít binární překlad instrukcí, což snižuje režii hypervizoru.

Obrázek 7- režimy privilegií architektury x86 –virtualizace s HW podporou CPU



Zdroj: VMware (5)

CPU se za běhu dokáže přepínat mezi režimy (Ring 0 a Ring -1), tento proces se nazývá VMX přechod (VMX transition). Tyto přechody existují dva. VM-Entry, který přechází z Ring -1 do Ring 0 a VM-Exit, který opouští Ring 0 a vrací se do Ringu -1. Pro správu přechodů mezi jednotlivými režimy byla zavedená datová struktura VMCS (Virtual Machine Control Structure). Virtuální stroj v tomto případě běží v Ring 0, a neví o tom, že je virtualizován a že pod ním běží hypervizor. Pokud se virtuální stroj pokusí použít privilegované instrukce, tyto instrukce nejsou provedeny přímo na CPU, ale místo toho jsou odchyceny a přesměrovány do Ringu -1, kde běží hypervizor který danou instrukci provede a výsledek odešle zpět do virtuálního stroje. Tato změna v architektuře CPU dovolila použít hypervizory, používající mikrokernl (např. Hyper-V – více v kapitole Hypervizory podle Microsoftu a VMware) (4).

3.1.3 Hypervizory podle Microsoftu a VMware

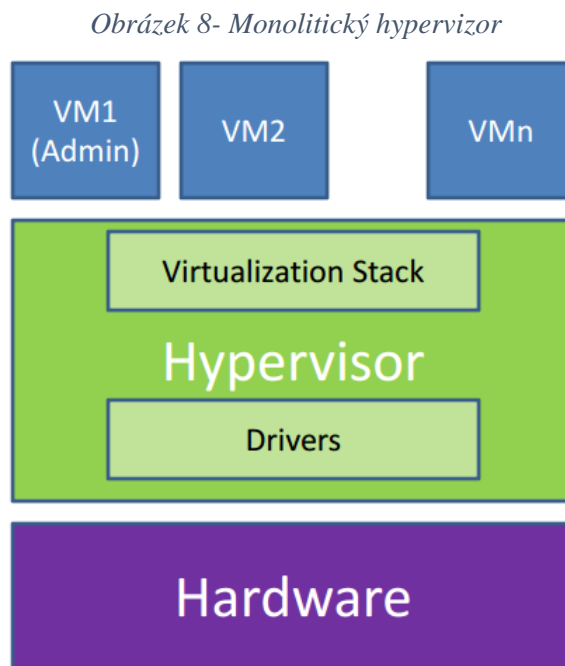
Následující kapitola se zabývá charakteristikou a rozdíly mezi hypervizory společností Microsoft a VMware. V obou případech se jedná o hypervizory typu 1, které běží přímo na hardwaru a nahrazují operační systém.

VMware

Společnost VMware používá ve svém produktu ESXi tzv. monolitický hypervizor. Jedná se o hypervizor, který obsahuje veškeré ovladače pro hardware, ke kterému přistupuje. Jedná se například o síťová zařízení, úložiště, vstupní zařízení atd. První virtuální stroj, který se vytvoří po nainstalování hypervizoru, se nazývá parent partition a slouží pro účely správy hypervizoru (na obrázku označen VM1).

Výhodou je možnost použití hypervizoru ve spojení s procesorem, který hardwarově nepodporuje virtualizaci (více v kapitole „Hardwarové rozšíření CPU pro podporu virtualizace“).

Mezi nevýhody patří velikost hypervizoru a také větší prostor pro případný útok na hypervizor a také omezená podpora zařízení.

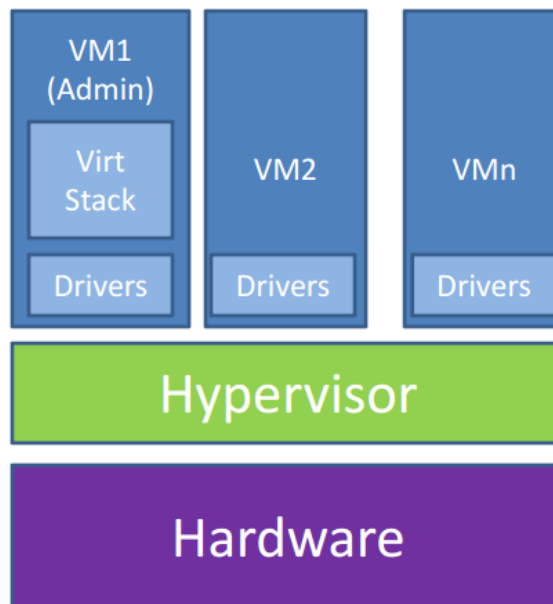


Zdroj Computer Science University of Toronto (7)

Microsoft

Společnost Microsoft používá ve svém virtualizačním produktu Hyper-V tzv. mikrokernel. Jedná se o malý hypervizor, který obsahuje jen nejnútnější služby pro správu CPU a paměti, které se nemění. Zbytek zajišťuje parent partition (VM1 na obrázku 9). Virtuální stroje přistupují k hardwaru dvěma způsoby, které závisí na konkrétním virtuálním stroji. Pokud je ve virtuálním stroji nainstalován balíček „Hyper-V integration components“, přistupuje tento stroj k hardwaru pomocí rychlé sběrnice VMBus. Pokud na virtuálním stroji nejsou nainstalovány „Hyper-V integration components“, přistupuje stroj k hardwaru pomocí parent partition. Ovladače v tomto případě nejsou součástí hypervizoru, jako v případě monolitického hypervizoru, ale jsou součástí virtuálních strojů (včetně parent partition). Hypervizor na bázi mikrokernelu vyžaduje CPU s hardwarovou podporou virtualizace.

Obrázek 9- Mikrokernel hypervizor



Zdroj Computer Science University of Toronto (7)

3.1.4 Výhody virtualizace

- Lze provozovat více serverů na jednom fyzickém hardwaru, z čehož plyne výhoda menších nároků na prostor, nižší spotřeba elektrické energie, nižší tvorba zbytkového tepla a následně nižší spotřeba elektrické energie potřebné pro chlazení.
- Virtuální stroj je uložen formou několika souborů na diskovém subsystému. Stejně jako jiné soubory, může být virtuální stroj kopírován nebo přenášen na jiné místo a to do konce za běhu (live migration). Tato vlastnost zlepšuje možnosti správy virtuálních strojů a zjednodušuje jejich zálohování.
- Virtuální stroj umožňuje běh vzájemně nekompatibilních aplikací na jednom fyzickém hardwaru.
- Virtuální stroj vytváří určitou bezpečnostní hranici. Při chybě v aplikaci v jednom virtuálním stroji je afektován pouze tento jeden stroj. Chyba neovlivní chod ostatních virtuálních strojů.
- Běh několika operačních systémů na jednom fyzickém stroji zjednodušuje vývoj aplikací a jejich následné testování.

3.1.5 Nevýhody virtualizace

- Zvýšená komplexita systémů. Virtualizace přidává další článek řetězce, který je nutno nainstalovat, nakonfigurovat a následně spravovat. Virtualizační vrstva, případně hostitelský stroj, se v závislosti na zvoleném typu virtualizace stává dalším bodem v řetězci, který může selhat a způsobit tím nedostupnost systémů na něm závislých.
- Nižší výkon. Virtualizace poskytuje obecně nižší výkon než při spuštění stejné aplikace na ekvivalentním fyzickém serveru. Režie hypervizoru se liší v závislosti na typu zátěže, obecně se u moderních hypervizorů uvádí výkonnostní pokles v rámci jednotek procent v porovnání s fyzickým serverem.
- Množství dodavatelů. Na trhu se vyskytuje mnoho dodavatelů virtualizačních produktů a pro správný výběr je nutná hluboká znalost produktů a příslušného IT prostředí.

3.2 Cloud

Co je to cloud? Magické slovo, které se objevilo v IT oblasti jako blesk z čistého nebe. „Cloud“ má dnes tolik definic, včetně několika extrémních, říkajících, že „cloud je všechno“, až po takové, říkající, že „cloud není nic“. Která je ta správná, záleží na úhlu pohledu. Pokud dnes někdo používá slovo „cloud“, může stejnými slovy říkat několik různých informací, podle toho jakou definici „cloudu“ zrovna vyznává.

Poradenská společnost Gartner, definuje cloud jako „...*style of computing in which scalable and elastic IT-enabled capabilities are delivered as a service using Internet technologies*“ (8).

Což volně přeloženo znamená: Způsob použití počítačů, ve kterém jsou rozšiřitelné a pružné IT funkce doručovány ve formě služeb prostřednictvím internetu“. Do této definice může spadat všechno, ale také nic, záleží na tom, co ještě je „pružné“ a „rozšiřitelné“ a co již ne. Národní institut standardů a technologie (National Institute of Standards and Technology, NIST), publikoval v září 2011, po několika letech práce a patnácti vydaných konceptech, dokument (9) The NIST Definition of Cloud Computing (10). Tento dvoustránkový dokument obsahuje jednoduchý popis cloudu. Tento popis se ujal jako definice cloudu a používá ho mnoho firem fungujících na cloudovém trhu.

3.2.1 Definice Cloudu podle NIST

V následující části je definován Cloud podle NIST, z dokumentu „The NIST Definition of Cloud Computing“ (9).

Základní charakteristiky

Jedná se o popis základních charakteristik, které by měl cloud podle NIST splňovat.

Samoobslužnost

Zákazník, ať už interní nebo externí, má možnost požádat o službu, jako například serverový čas nebo síťové úložiště samostatně, automaticky, bez potřeby lidské interakce s poskytovatelem služeb.

Přístup přes síť

Dodávané služby jsou dostupné přes síť a přístupné prostřednictvím standardních mechanismů, které podporují používání služeb heterogenními tenkými nebo tlustými klienty (například mobilní telefony, tablety, notebooky a pracovní stanice).

Sdílené zdroje

Zdroje privátního cloudu jsou sdílené s několika zákazníky. Zdroje poskytovatele, ať už fyzické nebo virtuální, mohou být dynamicky přiřazovány a odebírány na základě požadavků zákazníků. Je zde náznak nezávislosti na lokalitě v tom smyslu, že zákazník nemá kontrolu nebo vědomí o přesné lokaci přidělených zdrojů, ale může mít možnost specifikovat umístění na vyšší úrovni abstrakce (například kontinent, stát). Příkladem zdrojů může být úložiště, výpočetní výkon, operační paměť a síťová propustnost.

Flexibilita

Cloud je flexibilní, dokáže pružně reagovat na velikost poptávky. Zvýšení výkonu cloudu je jednoduché a bez výpadku. Pro zákazníka se cloudová služba jeví jako neomezená.

Měření služeb – pay-per-use

Jedním z atributů cloudu je také měření služeb. To v praxi znamená, že zákazník platí jen za to, co doopravdy využije. Ať už je to procesorový čas, místo na diskovém systému, případně síťová konektivita. Cloudové řešení by mělo obsahovat nástroje, pomocí kterých můžeme tyto metriky vyhodnocovat a říct, kolik by který zákazník měl za služby zaplatit. Tyto údaje by měly být transparentní pro poskytovatele i pro zákazníka.

Model služeb dle NIST

Jedná se o popis modelů služeb dle NIST, z dokumentu „The NIST Definition of Cloud Computing“ (9).

Software as a Service (SaaS)

Službou poskytovanou zákazníkovi je použití aplikace běžící na cloudové infrastruktuře poskytovatele. Cloudová infrastruktura dle NIST je soubor hardwaru a softwaru, který umožňuje splnit pět základních předpokladů cloud computingu. Za cloudovou infrastrukturu lze považovat jak fyzickou tak abstraktní úroveň. Fyzická úroveň obsahuje veškeré hardwarové prostředky, nutné k běhu poskytovaných cloudových služeb a typicky obsahuje servery, úložiště a síťové vybavení. Abstraktní úroveň se skládá ze softwaru provozovaného nad fyzickou úrovní a udává základní vlastnosti cloudu. Konceptně je abstraktní vrstva umístěna nad fyzickou vrstvou.

Platform as a Service (PaaS)

Službou poskytovanou zákazníkovi je nasazení aplikace vyvinuté, nebo jinak získané zákazníkem. Aplikace by měla být vyvinuta použitím programovacích jazyků, knihoven,

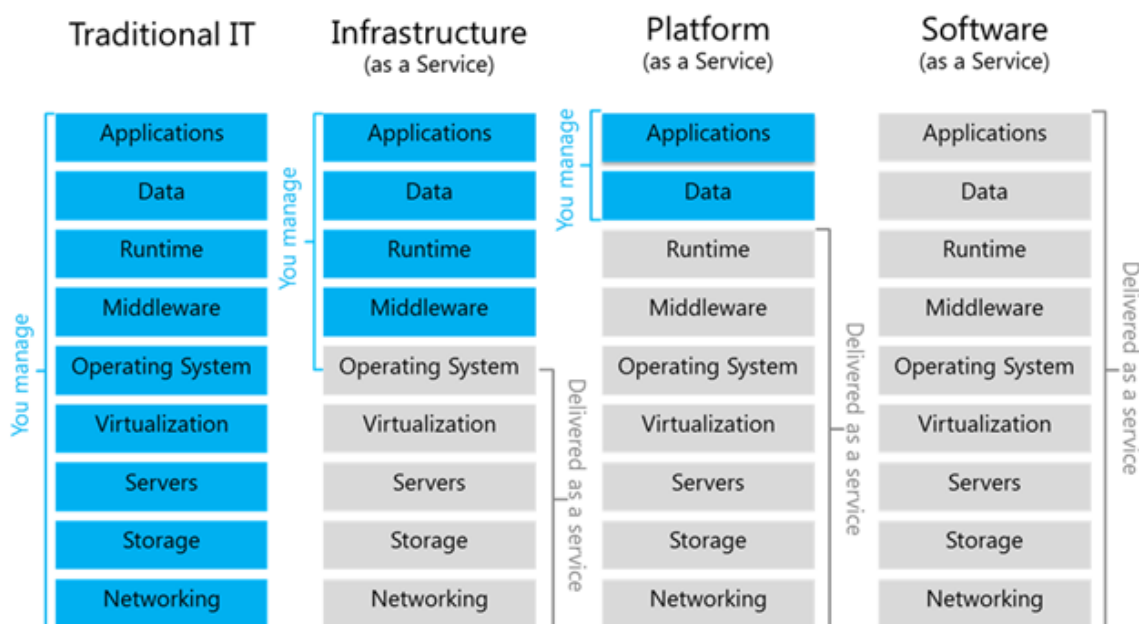
služeb a nástrojů, podporované poskytovatelem, ale nevyklučuje se ani použití kompatibilních programovacích jazyků, knihoven, služeb a nástrojů z jiných zdrojů.

Zákazník nemá kontrolu nad cloudovou infrastrukturou (zahrnující síť, servery, operační systémy, úložiště), nad níž služba běží. Ale má kontrolu nad nasazenými aplikacemi a případným nastavením prostředí, které tuto aplikaci provozuje.

Infrastructure as a Service (IaaS)

Službou poskytovanou zákazníkovi je poskytnutí výpočetního výkonu, úložiště, sítě a dalších nezbytných výpočetních zdrojů, tak aby spotřebitel měl možnost spustit libovolný software, který může zahrnovat operační systém a aplikaci. Zákazník nespravuje cloudovou infrastrukturu, ale spravuje operační systém, úložiště a nasazené aplikace. Zákazník může s omezením mít pod správou také síťová zařízení – například firewall.

Obrázek 10- Model služeb podle NIST



Zdroj MSDN Blog (11)

Modely nasazení podle NIST

Jedná se o popis modelů nasazení dle NIST, z dokumentu „The NIST Definition of Cloud Computing“ (9).

- **Privátní cloud**

Cloudová infrastruktura, která je zavedena pro použití výlučně jedinou organizací. Organizace může zahrnovat více spotřebitelů – interních zákazníků – například oddělení

v rámci organizace. Tato infrastruktura může být vlastněna, spravována a provozována organizací, která jí využívá, ale také třetí stranou, případně libovolnou kombinací – například může být vlastněna třetí stranou, ale spravována organizací. Tato infrastruktura může být umístěna v prostorách organizace, nebo může být pronajata.

- **Komunitní cloud**

Cloudová infrastruktura, zavedená pro výhradní použití určitého společenství zákazníků z organizací, které mají společné požadavky (např. bezpečnostní). Tato infrastruktura může být vlastněna, spravována a provozována jedním nebo více zákazníky v rámci daného společenství, případně třetí stranou, nebo nějakou jejich kombinací. Tato infrastruktura může být umístěna uvnitř nebo mimo prostory organizace.

- **Veřejný cloud**

Cloudová infrastruktura, zavedená pro použití širokou veřejností. Tato infrastruktura může být vlastněna, spravována a provozována komerčním, akademickým, nebo vládním subjektem nebo nějakou jejich kombinací. Tato infrastruktura je umístěna v prostorách poskytovatele cloudu.

- **Hybridní cloud**

Cloudová infrastruktura, složená ze dvou, nebo více odlišných cloudových infrastruktur (privátní, komunitní nebo veřejný cloud), které zůstávají samostatné, ale jsou spolu propojeny standardizovanou nebo proprietární technologií, která umožňuje přenositelnost dat a aplikací – například rozložení zátěže mezi cloudy.

3.2.2 Výhody privátního cloudu

Následující kapitola se věnuje výhodám privátního cloudu, v porovnání s veřejným cloudem, případně s prostou virtualizací. Prostou virtualizací je označováno prostředí, které používá serverovou virtualizaci, ale nepoužívá nástroje pro automatizaci a samoobslužnost. Srovnání s prostou virtualizací se nabízí hned z několika důvodů. Předně se virtualizace považuje za předchůdce a zároveň základní stavební kámen pro privátní cloud, ale také z důvodu, že v současné době existuje mnoho společností, které používají virtualizaci, jsou s ní spokojeni a řeší otázku, jestli nasadit nebo nenasadit řešení na bázi privátního cloudu. Privátní cloud je porovnáván i s veřejným cloudem, který obvykle nabízí porovnatelné služby. Srovnání se zabývá odlišnostmi obou řešení.

Spolehlivost

Privátní cloud, na rozdíl od veřejného cloudu, obvykle nabízí lepší a lépe předvídatelnou dostupnost služeb pro uživatele. U veřejného cloudu je dostupnost a údržba serverů daná SLA (Service Level Agreement) – smlouvou o úrovni služeb, která obsahuje definici „údržby“ a „dostupnosti“ a také informaci o procentuální dostupnosti služeb pro zákazníka. Například úroveň SLA 99,9 %, při měsíční kalkulaci SLA, nám říká, že poskytovaná služba bude dostupná 99,9 % času, což při měsíční kalkulaci znamená, že služba může být nedostupná maximálně 44 minut / měsíc. Pokud je SLA vypočítáváno ročně (což je specifikováno ve smlouvě), znamenala by úroveň 99,9 % možnost výpadku až 525 minut ročně. Do této doby se ale obvykle nezahrnuje plánovaná údržba. Podmínky, za kterých lze údržbu považovat za plánovanou, diktuje smlouva. Obvykle musí být tento úkon ohlášen zákazníkovi v dostatečném předstihu, bohužel provedení údržby není běžně možné nijak ovlivnit. Pokud sjednaná úroveň SLA není dodržena ze strany dodavatele, je ve smlouvě uvedeno, jakým způsobem dojde ke kompenzaci. Obvyklá je sleva z měsíční ceny za dodávané služby. Ačkoliv se zdají být takto dlouhé výpadky nemyslitelné pro velké společnosti a kritické aplikace, při pohledu malé firmy je situace jiná. Malá firma obvykle nemá prostředky na zajištění takové dostupnosti, jakou nabídne poskytovatel veřejného cloudu. Měsíční poplatek za takovou službu si ale malá firma již dovolit může.

Privátní cloud nabízí vyšší spolehlivost i ve srovnání s prostou virtualizací. Nástroje pro správu privátního cloudu umožňují jeho propojení s veřejným cloudem (více v odstavci „Možnost rozšíření do public cloudu“) a jeho použití při automatizované obnově po havárii (disaster recovery), kdy je možné systém, který standardně běží na infrastruktuře zákazníka v jeho vlastní serverovně, pravidelně replikovat do veřejného cloudu a v případě katastrofy, způsobující nedostupnost primární lokace (požár, záplavy, pád meteoritu ...), spustit tento systém v záložní lokaci – veřejném cloudu.

Fyzické umístění dat

Privátní cloud obvykle nabízí větší úroveň bezpečnosti dat, než řešení v Public cloudu, a to toho z důvodů, že veškerá firemní data jsou umístěna na serverech, které jsou pod přímou správou společnosti a nejsou sdílené s žádnou jinou společností. Tyto servery mohou být umístěné v rámci interní sítě zákazníka a spravovány interním IT oddělením. Případně mohou být umístěny v datovém centru poskytovatele služeb, spravovány poskytovatelem, zatímco firma, jakožto uživatel cloudu, se k němu připojuje přes zabezpečenou linku.

Společnosti podnikající v oborech s vysokými nároky na bezpečnost dat, například bankovníctví nebo zdravotnictví, budou pravděpodobně z tohoto důvodu upřednostňovat privátní cloud před veřejným cloudem.

V případě privátního cloudu si zákazník může zvolit kde přesně, na jakých serverech, v jakém datacentru a v jaké zemi se budou jeho data nacházet. Což obecně nelze říct o službách veřejného cloudu a může to s sebou nést legislativní problémy. U public cloudových služeb obvykle nelze ovlivnit, kde přesně se data nachází, nebo lze jen vybrat region – například Evropa, nebo Asie.

Například Německo je velmi striktní v otázce ukládání dat v cizích státech. Společnosti v Německu ze zákona nesmí ukládat některá svá data v zahraničí (12). Což s sebou nese řadu problémů v souvislosti s nasazením cloudových služeb, které jsou ze své podstaty centralizované do velkých datacenter. Německá legislativa donutila mnoho poskytovatelů veřejných cloudových služeb k vytvoření datacenter přímo v Německu.

Fyzická bezpečnost dat

Jako argument se často používá úroveň fyzické bezpečnosti dat. Zatímco v případě privátního cloudu, nasazeného interně v prostorech společnosti, je fyzické zabezpečení serverů, záležitostí a odpovědností společnosti využívající privátní cloud. V případě využití služeb public cloudu se společnost musí spolehnout na úroveň zabezpečení dodavatele, do které většinou nelze zasahovat. Společnost například nemůže požadovat vyšší zabezpečení, než nabízí dodavatel, jedinou možností je akceptace úrovně zabezpečení, kterou nabízí dodavatel, případně volba interně nasazeného privátního cloudu.

V případě volby hostovaného privátního cloudu v datacentru poskytovatele je situace o trochu lepší, protože se obvykle jedná o řešení na míru a poskytovatel má větší prostor pro nastavení úrovně bezpečnosti. I tak je zde ale méně možností než v případě privátního cloudu nasazeného interně.

Fyzická bezpečnost se dá označit jako výhoda, ale také jako nevýhoda privátního cloudu. Záleží na úhlu pohledu. Pro velké společnosti provozující interní privátní cloudy většinou není problém dosáhnout na velmi vysokou úroveň fyzické bezpečnosti serverů převyšující možnosti, které nabízejí poskytovatelé public cloudů, případně private cloudů hostovaných v datacentrech poskytovatele. Menší firmy ale obvykle nemají prostředky na dosažení takto vysoké úrovně zabezpečení a proto se velmi často uchylují ke kompromisům a řešením, které snižují fyzické zabezpečení pod úroveň dosahovanou poskytovateli public cloudů. Jedním

dechem je však nutno dodat, že fyzická bezpečnost datacenter poskytovatelů public cloudu je obecně na velmi vysoké úrovni, jedná se o důležitý argument případných zájemců o tento typ služby. Proto berou dodavatelé těchto služeb problematiku bezpečnosti velmi vážně a nechávají se často auditovat a certifikovat, čímž dokládají úroveň bezpečnosti případným zájemcům. Investice do datových center poskytovatelů jsou velmi vysoké (např. 15 miliard dolarů v případě investice do datacenter společnosti Microsoft (13)) a tak každá pochybnost, nebo případný úspěšný pokus o prolomení bezpečnosti, znamená odliv zákazníků a znehodnocení této investice. Volba služeb public cloudu je často odůvodnitelná, hlavně pokud zákazník nedokáže (ať už finančně nebo technologicky) zajistit adekvátní úroveň bezpečnosti při implementaci privátního cloudu, nebo pracuje s daty, která nevyžadují vysokou úroveň bezpečnosti.

Možnost rozšíření do public cloudu

Nástroje privátního cloudu obvykle nabízí funkcionalitu umožňující propojení privátního cloudu, provozovaného na serverech a infrastruktuře zákazníka, s public cloudem provozovaným dodavatelem a toto řešení ovládat z jednoho místa – jedné administrátorské konzole. Rozšířením privátního cloudu do veřejného cloudu vzniká hybridní cloud.

Možnost libovolné konfigurace

Privátní cloud nabízí také svobodu volby konfigurace poskytovaných služeb. Například v případě virtuálních strojů můžeme, u komerčně dostupných služeb veřejného cloudu, vybírat jen z několika konfigurací, které pokrývají běžnou poptávku většiny zákazníků. Pokud si ale z nabídky připravených konfigurací zákazník nevybere, není možné tuto konfiguraci připravit „na míru“ tak jako to lze v případě privátního cloudu.

Rozložení nákladů

Pomocí obslužných nástrojů řešení privátního cloudu, lze zajistit dělení nákladů za provoz IT služeb mezi odběratele služeb. Obslužné nástroje pomáhají měřit využití infrastruktury jednotlivými odběrateli. Následně je možné interně fakturovat využití sdílené infrastruktury, případně dále s těmito daty pracovat.

Snížení zátěže IT pracovníků

Některé úkony, které IT pracovníci provádějí rutinně, lze automatizovat. V krajních případech je možné, po implementaci řešení Privátního cloudu, i snížení počtu IT pracovníků.

3.2.3 Nevýhody privátního cloudu

Počáteční investice

Počáteční investice je větší než v případě použití veřejného cloudu, z důvodu nutnosti nákupu potřebné infrastruktury. Na druhou stranu, eliminuje riziko navýšení poplatků oproti využití služeb veřejného cloudu.

Náročnost implementace

Nasazení privátního cloudu je velice náročný úkol, který nevyžaduje pouze technické znalosti a zkušenosti, ale také znalost procesů v organizaci. Zejména definice IT služeb vyžaduje kooperaci nejen IT oddělení, ale také odběratelů IT služeb – interních IT oddělení, s jejichž pomocí se definují služby poskytované privátním cloudem a způsob jejich měření.

Síťová konektivita

V případě privátního cloudu, umístěného v jiné lokaci než klienti, kteří se k němu připojují a využívají jeho služby, může být problémem s kapacitou sítě. Vzhledem k umístění datacentra cloud providera, může docházet ke zvýšení latence, což může být problém při využívání některých aplikací.

4 Vlastní práce

Vlastní práce je založena na implementaci privátního cloudu dle fiktivního zadání. V následující kapitole bude popsána instalace a zprovoznění privátního cloudu od každého vybraného dodavatele – společnosti Microsoft a VMware, se zaměřením na rozdíly jak v provedení konfigurace a implementace řešení, tak na rozdíly v konceptech dodavatelů – porovnání konceptů virtuálních appliance, v případě společnosti VMware, proti instalaci a konfiguraci produktů rodiny SystemCenter v případě společnosti Microsoft.

Zadání

Privátní cloud, poskytující jedinou službu a to virtuální prostředí, pro vývojáře B2B řešení, obsluhovaný přes webové rozhraní, přes které si vývojář zažádá o vytvoření vývojářského prostředí, které je následně zcela automatizovaně vytvořeno v prostředí privátního cloudu.

Řešení

Řešení obou dodavatelů jsou implementována v laboratorním prostředí sestávajícího ze dvou fyzických serverů, každý osazen dvěma šestnáctijádrovými procesory AMD Opteron 6272 a 64GB RAM.

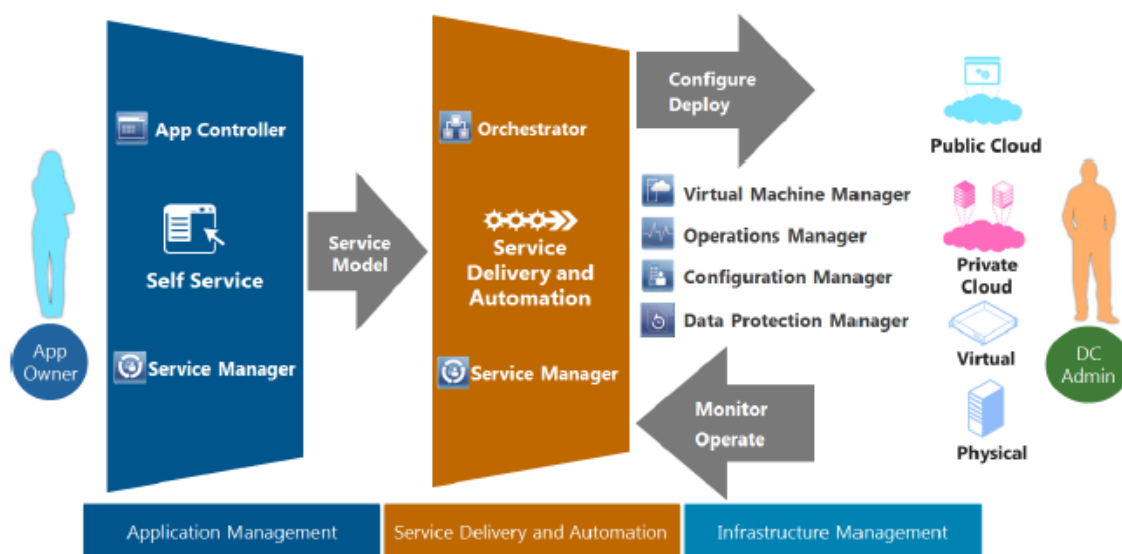
4.1 Microsoft

Řešení privátního cloudu společnosti Microsoft je založeno na Windows Serveru s technologií Hyper-V a produktů z rodiny System Center. Oba tyto produkty jsou dostupné ve dvou edicích. Standard, pro menší implementace a prostředí s nižší úrovní virtualizace a Datacenter, pro větší prostředí s vyšším nasazením virtualizace. Obě edice používají stejný licenční model, založený na licenci, která pokrývá dva fyzické procesory v serveru. Obě edice jsou také funkčně zcela shodné. Jediným rozdílem mezi edicemi je počet virtuálních instancí, které je možno nasadit. Každá Standard licence opravňuje k nasazení 2 virtuálních instancí licencovaného softwaru, zatímco edice Datacenter opravňuje k nasazení neomezeného počtu virtuálních instancí, běžících na licencovaném serveru.

4.1.1 Komponenty

Následující obrázek stručně popisuje úlohu a rozvržení jednotlivých komponent privátního cloudu na platformě Microsoft (14).

Obrázek 11- Microsoft Private Cloud



Zdroj: Microsoft (14)

Hypervizor Microsoft Hyper-V

Hypervizor Microsoft Hyper-V je instalován buď samostatně, jako produkt Microsoft Hyper-V Server, případně jako instalovatelná role Microsoft Windows Serveru. Hypervizor využívá mikrokernél, jak již bylo popsáno v kapitole 3.1.3.2. Hypervizor je klíčová součást jak virtualizace, tak i následné implementace privátního cloudu, o kterém pojednává tato práce.

System Center Virtual Machine Manager

System Center Virtual Machine Manager je nástroj pro správu virtualizovaných datacenter. Umožňuje konfigurovat jednotlivé hypervizory, síťové prostředky a úložiště. Umožňuje také vytvářet virtuální počítače a služby v privátních cloudech. Ačkoliv se jedná o produkt společnosti Microsoft, je s ním možné spravovat i hypervizory jiných dodavatelů. Stejně jako hypervizor, je i tato součást klíčová pro nasazení privátního cloudu.

System Center App Controller

Nástroj System Center AppController slouží jako samoobslužný portál pro uživatele cloudu. Jeho pomocí lze spravovat existující, případně žádat o nové služby poskytované cloudem. Zajišťuje portál pro správu virtuálních strojů, aplikací a služeb v rámci privátního cloudu nebo cloudu na bázi Windows Azure. System Center App Controller je nástupce Self-Service portal role, instalovatelné společně s minulou verzí System Center Virtual Machine

Manageru, ve verzi 2012 se jedná o samostatný produkt. Na rozdíl od předchůdce, rozšiřuje možnosti správy v cloudovém prostředí. V případě zadaného scénáře, je portál této aplikace místo, ze kterého je možné objednat službu zákazníkem. V našem případě je zákazníkem vývojář, který žádá o službu vývojářské prostředí.

System Center Service Manager

Nástroj pro incident management, problem management, event management a správu IT služeb. Nabízí správu incidentů, správu dodržování SLA, asset management s možností fulltextového vyhledávání atd. Tento nástroj, ačkoliv souvisí s moderním trendem dnešního IT, není bezpodmínečně nutný pro nasazení v privátním cloudu, proto je mu v této práci věnována jen nezbytná pozornost pro pochopení souvislostí.

System Center Orchestrator

Nástroj pro tvorbu technologických procesů - orchestrací a runbooků. Používá se pro automatizaci procesů a je možné ho použít pro automatizaci libovolného technologického IT procesu napříč heterogenním prostředím. Pro Orchestrator existují integrační balíčky pro různé technologie, takže se nejedná o technologii jen pro produkty společnosti Microsoft, ale je možné integrovat různé technologie. Například zautomatizovat proces, ve kterém se automaticky vytvoří další virtuální webserver, pokud farma webserverů nestíhá obsluhovat požadavky – například před Vánoci. Následující nový webový server nemusí být provozován na platformě Microsoft, ale pomocí integračního balíčku může být vytvořen i na jiné platformě.

System Center Operations Manager

Nástroj zajišťující monitoring kompletní infrastruktury a to nejen infrastruktury na platformě Microsoftu. Pro Operations Manager jsou k dispozici management packy umožňující monitoring například síťové infrastruktury, případně monitoring hardwaru serverů pomocí management packů jednotlivých dodavatelů.

System Center Data Protection Manager

System Center Data Protection Manager je nástroj pro zálohu a obnovení. Umožňuje zálohovat jak lokálně, na síťové úložiště, tak případně na pásky. Dokáže zálohovat SQL Server, Exchange Server, SharePoint, virtuální servery, souborové servery, ale také stolní počítače a laptopy využívající systém Windows. Tento produkt není nutný pro implementaci privátního cloudu, ale je uveden jako součást licence produktů System Center.

4.1.2 Instalace a konfigurace prostředí

Tato část popisuje laboratorní prostředí a dále instalaci a konfiguraci jednotlivých komponent. Laboratorní prostředí obsahuje následující servery:

- doménový řadič domény bilek.local s adresou l2-dc.bilek.local, použitý taktéž jako DNS server;
- členský server domény bilek.local, s adresou l2-scvm.bilek.local, s nainstalovanou aplikací Microsoft System Center Virtual Machine Manager ve verzi 2012 R2;
- členský server domény bilek.local, s adresou l2-sql.bilek.local, s nainstalovanou aplikací SQL Server 2012, použitý jako databázový stroj pro podporu dalších aplikací;
- členský server domény bilek.local, použitý pro instalaci aplikace Microsoft System Center 2012 R2 – App Controller;
- členský server domény bilek.local, s adresou l2-hvhost.bilek.local, použitý jako hypervizor Hyper-V;
- všechny servery používají operační systém Windows Server 2012 R2.

Instalace a konfigurace hypervizoru

Instalace hypervizoru, v případě produktu společnosti Microsoft, je možná několika způsoby. Je možné nainstalovat samotný hypervizor bez obslužných služeb ve formě produktu Microsoft Hyper-V Server, který je zdarma ke stažení na stránkách společnosti Microsoft a sám o sobě nevyžaduje žádnou licenci. Další možností je instalace operačního systému Microsoft Windows Server 2012 R2 a využití role Hyper-V server. Samotný OS Windows Server je možné nainstalovat jak v klasické verzi s grafickým uživatelským rozhraním, nebo nově (od verze 2008) také bez grafického uživatelského rozhraní – v daném případě je server ovládán prostřednictvím funkce příkazové řádky. Absence grafického rozhraní má výhodu v nižším počtu instalovaných komponent, což snižuje exponovaný povrch pro potenciální útok na tento server a také snižuje počet komponent, vyžadujících údržbu a aktualizace. Nevýhodou je omezená možnost správy a nemožnost využití běžných správcovských nástrojů lokálně. Pro účely implementace laboratorního prostředí byla zvolena plná verze Windows Serveru 2012 R2.

Instalace a konfigurace SQL serveru a doménového řadiče

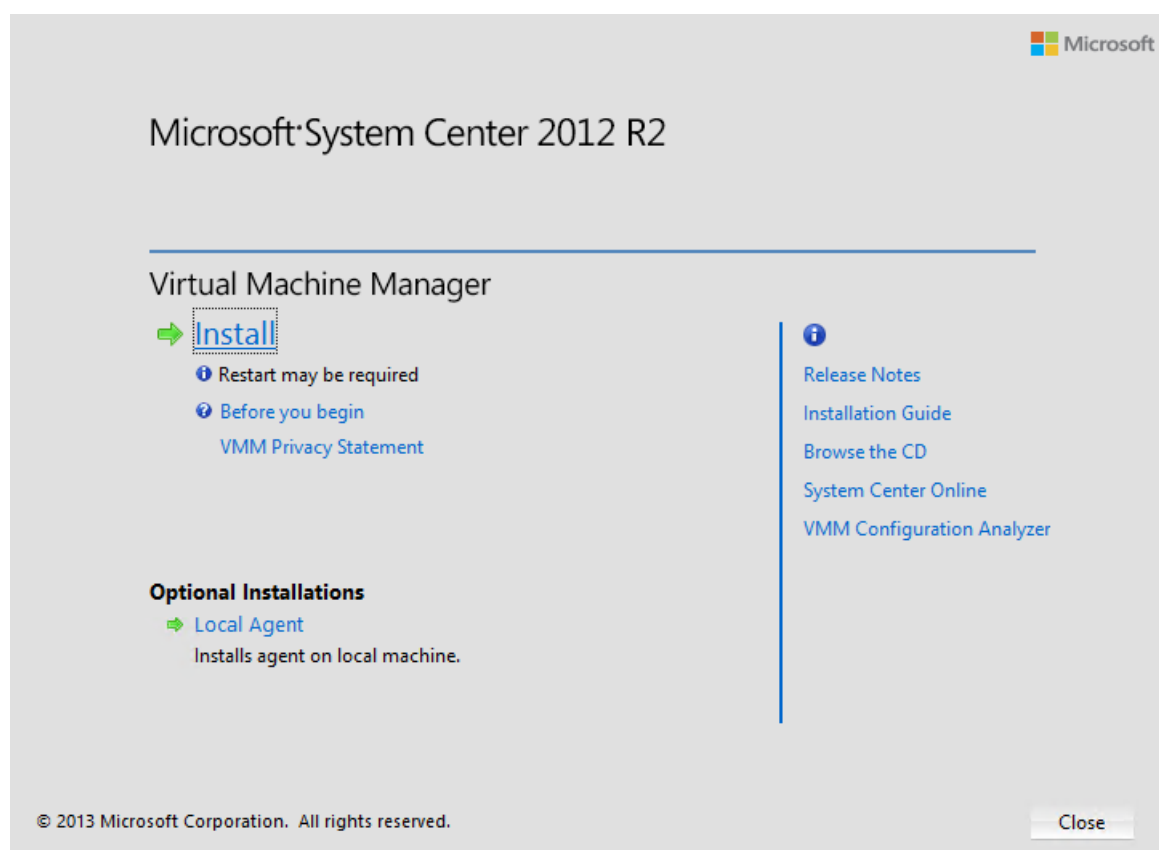
V laboratorní implementaci jsou dále přítomny instance databázového serveru SQL 2012 (L2-SQL.bilek.local), který zajišťuje provoz databází nutných pro provoz dalších obslužných aplikací privátního cloudu (Virtual Machine Manager).

Doménový řadič (v tomto případě L2-DC.bilek.local) zajišťuje služby ověřování v rámci lokální domény prostřednictvím protokolu Kerberos.

Instalace a konfigurace System Center Virtual Machine Manageru

Instalace SCVMM proběhla na virtuální server s nainstalovaným OS Windows Server 2012 R2. Instalace vyžaduje přístup k instanci SQL serveru, při instalaci instalátor vytvoří potřebné databáze. Je proto nutné ověřit síťovou dostupnost SQL serveru. Dále jsou vytvořeny sdílené složky pro knihovnu používanou v SCVMM. Následující obrázek 12 je úvodní při instalaci SCVMM 2012R2.

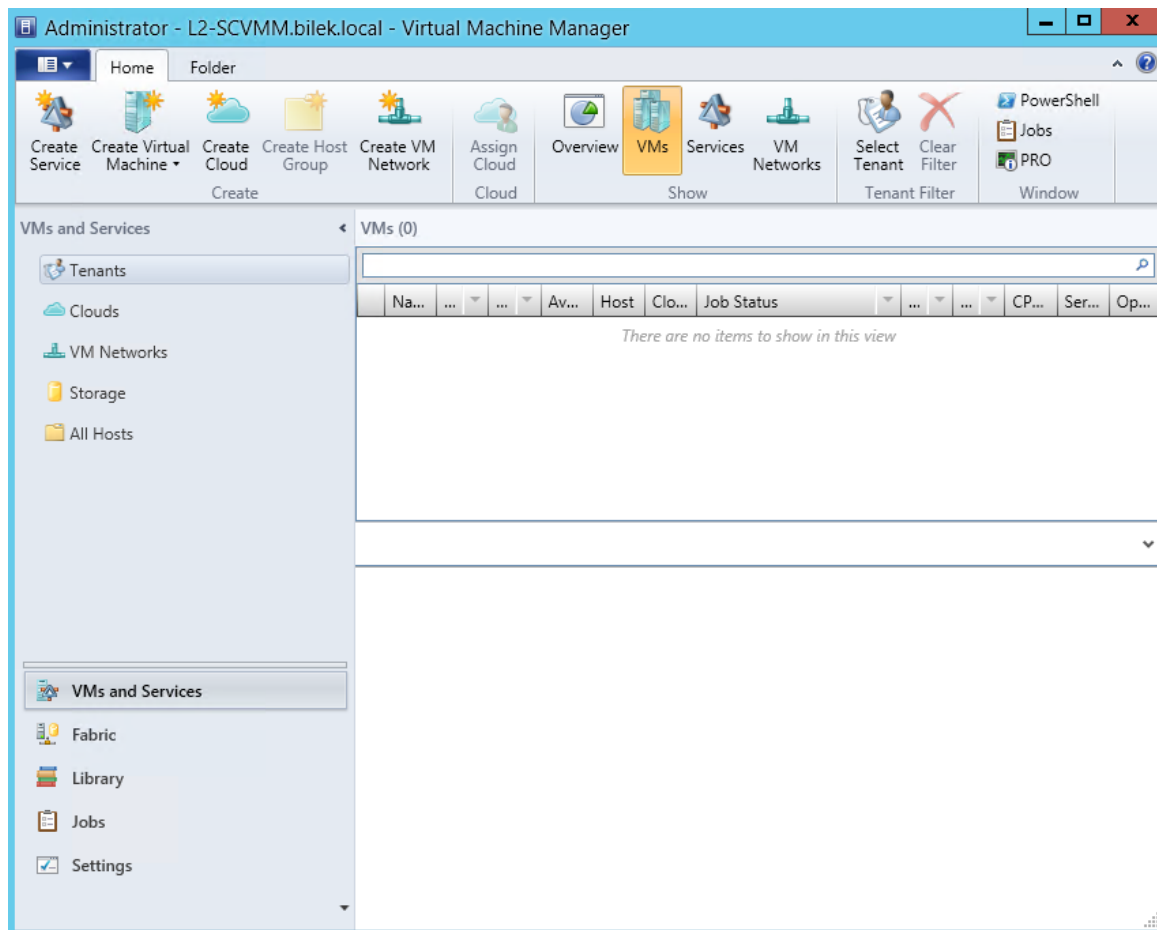
Obrázek 12- Instalátor SCVMM



Zdroj: vlastní zpracování

Po instalaci je možné spustit konzoli SCVMM, jak je znázorněno na následujícím obrázku 13.

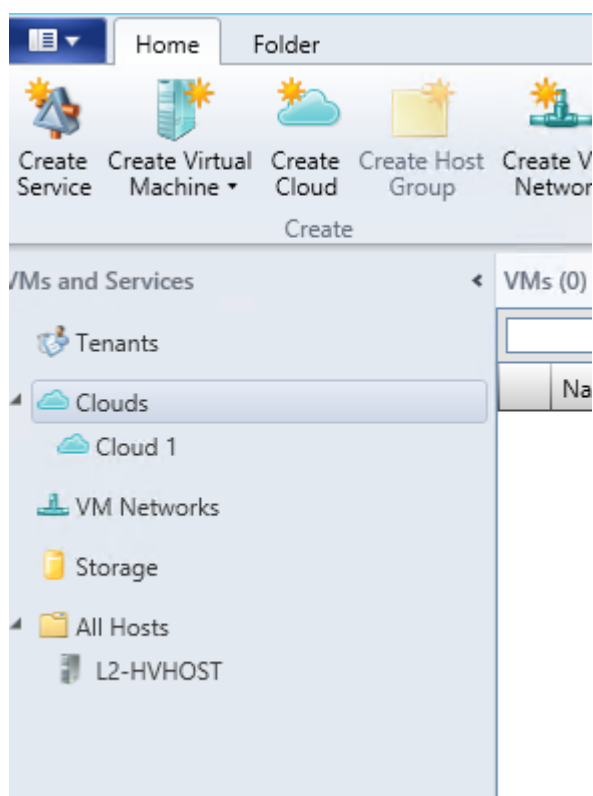
Obrázek 13- System Center Virtual Machine Manager - Konzole



Zdroj: vlastní zpracování

Při následné konfiguraci jsou nakonfigurovány účty, které SCVMM využívá pro správu hypervizorů a spouštění úkolů. Dále je SCVMM připojen k hypervizoru (L2-HVHOST.bilek.local). Po připojení k hypervizoru je již možné pomocí průvodce vytvořit cloud, do kterého je zahrnut již zmíněný hypervizor l2-hvhost.bilek.local. Nový cloud, jak je vidět z obrázku 14, se zobrazí v seznamu cloudů v konzoli SCVMM.

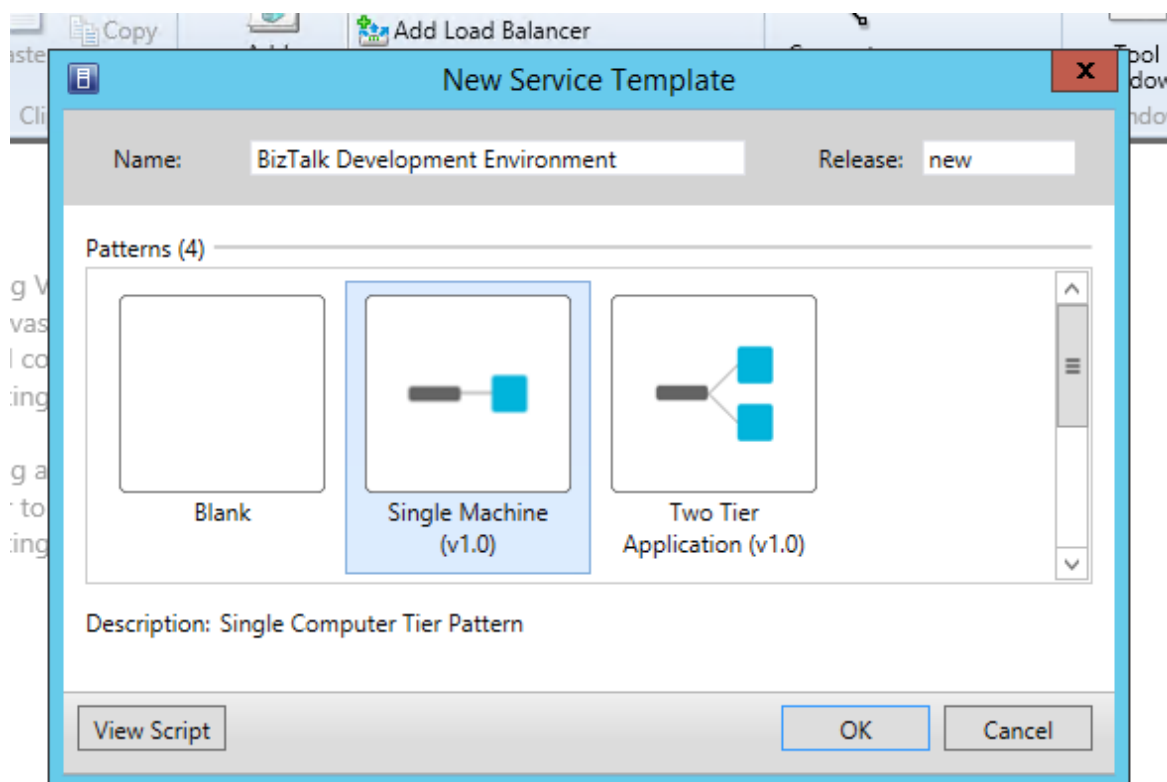
Obrázek 14- SCVMM konzole - zobrazení Cloudu



Zdroj: vlastní zpracování

Po vytvoření cloudu je vytvořena vzorová instance virtuálního stroje, do kterého je nainstalováno vývojářské prostředí dle zadání. Následně je na základě tohoto předinstalovaného stroje vytvořen vzorový virtuální stroj (VM Template). Tento VM Template je v následujícím kroku použit při definici nové služby (Service), která bude poskytována nově vytvořeným cloudem (v tomto případě „Cloud 1“). Pro vytvoření služby slouží průvodce dostupný z hlavního menu konzole SCVMM. V průběhu vytváření služby je zadán typ služby – jak je vidět z následujícího obrázku 15.

Obrázek 15- SCVMM, vytvoření služby - vzor

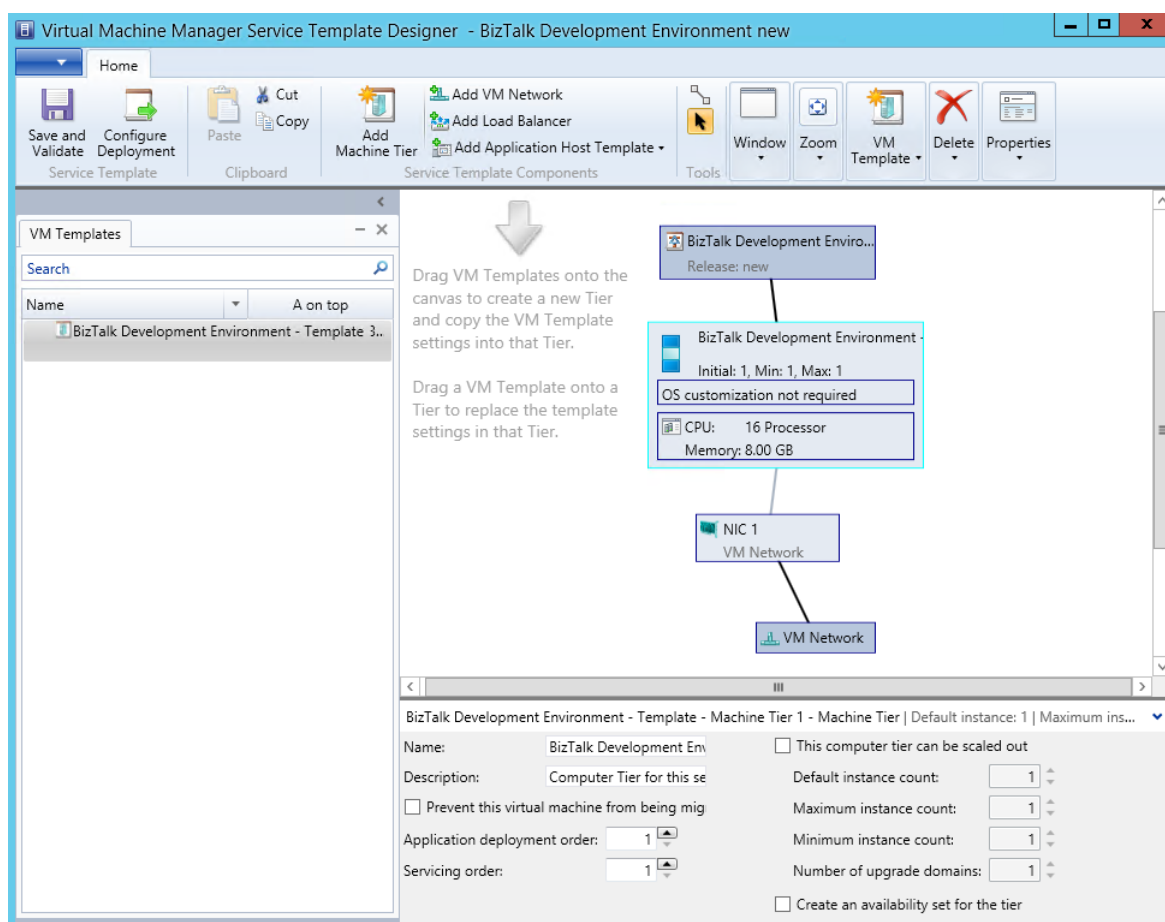


Zdroj: vlastní zpracování

V následujícím kroku je možné nastavit až třístupňovou aplikaci, která může obsahovat například databázový stroj, aplikační server a webový server pro front-end. Všechny servery jsou následně vytvořeny jako součást vytvářené služby a nemusí se vytvářet samostatně. V tomto případě je zvolena možnost jednotlivého stroje.

Následující krok zahrnuje konfiguraci nově vytvářené služby, pomocí nástroje Virtual Machine Manager Service Template Designer, který se spustí jako součást průvodce vytvořením nové služby a slouží pro specifikaci parametrů služby, jako je konfigurace strojů, použité VM templates, připojení strojů ke konkrétní síti atd. Template Designer je znázorněn na obrázku 16.

Obrázek 16- SCVMM - vytvoření služby - Service Template Designer



Zdroj: vlastní zpracování

Po uložení vzoru služby je služba vytvořena. Nyní je vytvořena uživatelská role podle zadání. Uživatelská role je pojmenována „Developers“ a obsahuje jediný uživatelský účet „BILEK\Developer“. Dané roli jsou následně přiřazena práva vytvářet instance služby „BizTalk Development Environment“, která byla vytvořena v předchozích krocích a také zdroje cloudu (výpočetní výkon, RAM paměť, prostor na úložišti atd.), které mohou být Developerem použity.

Instalace a konfigurace System Center AppControler

Instalace SCAC byla provedena na samostatný virtuální server tak, jak je to doporučeno společností Microsoft. Druhou možností je instalace na stejný server společně s SCVMM, z důvodu výkonu je ale preferována instalace na samostatný server. Instalace probíhá podobným instalátorem jako SCVMM – viz obrázek 17.

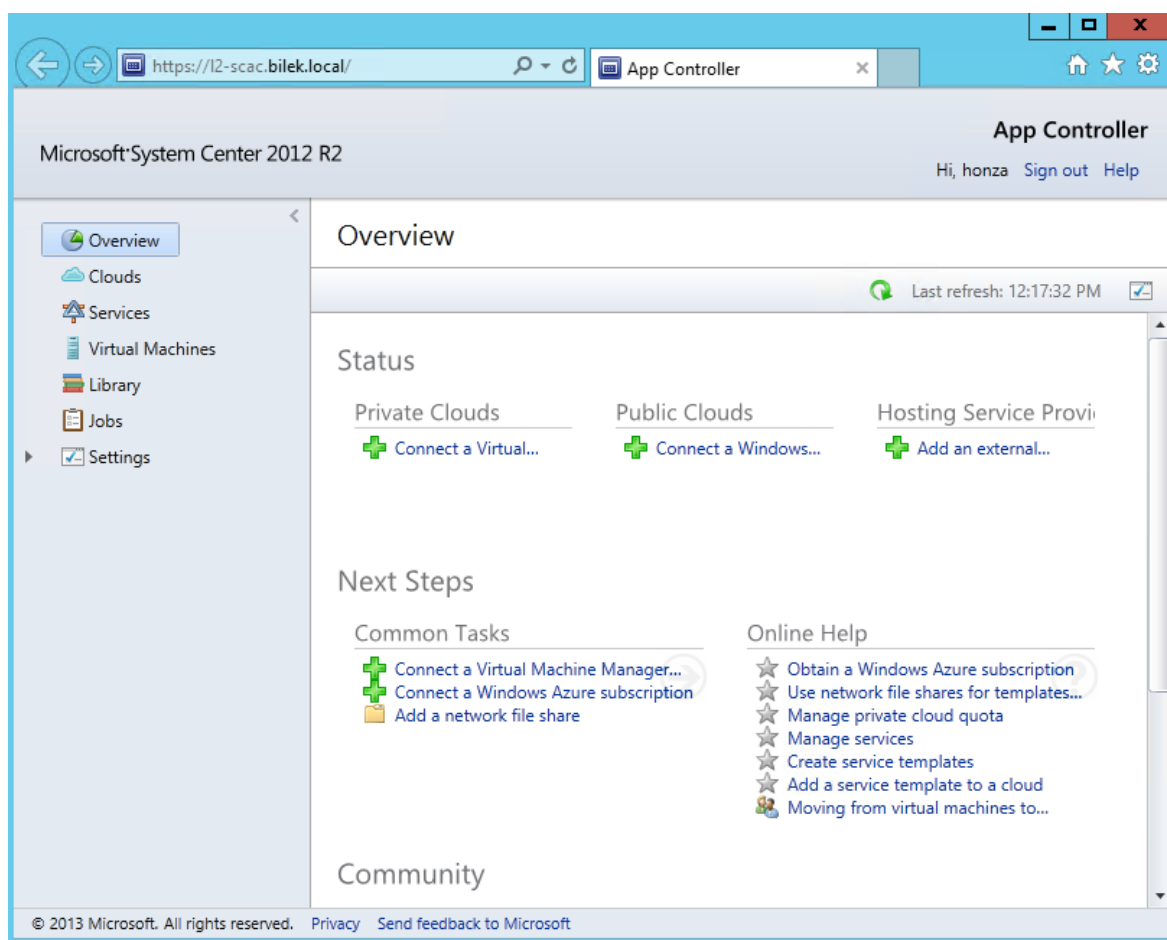
Obrázek 17- Instalace App Controller



Zdroj: vlastní zpracování

V průběhu instalace je vytvořena databáze, potřebná pro běh App Controlleru, a také webový server, který slouží pro provoz webové stránky portálu. Po dokončení instalace je možné se přihlásit k vytvořenému portálu, který je znázorněn na obrázku 18.

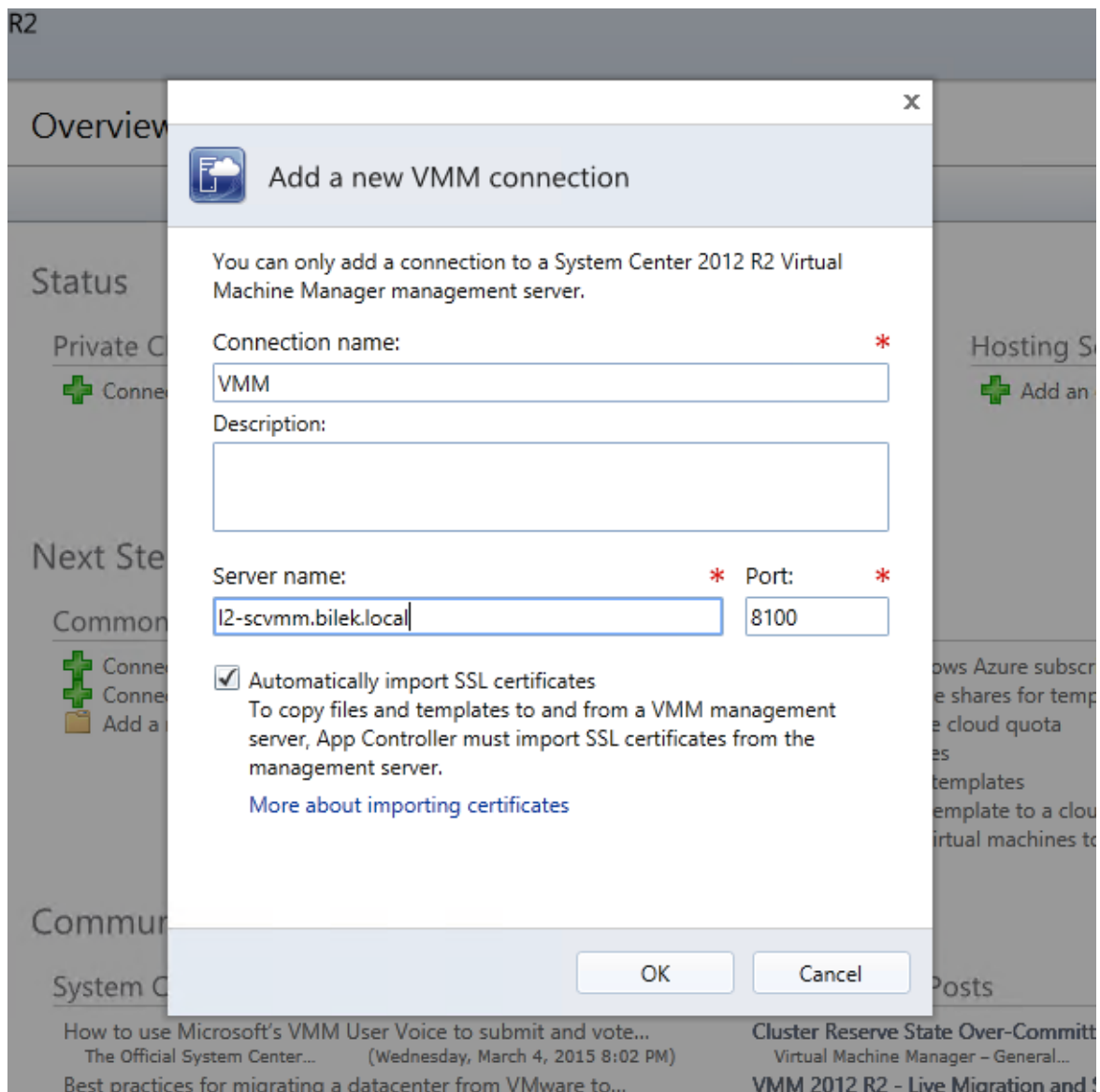
Obrázek 18- App Controller - portál



Zdroj: vlastní zpracování

Připojení App Controlleru k instanci Virtual Machine Manageru, po přihlášení administrátorským účtem, je znázorněno na obrázku 19.

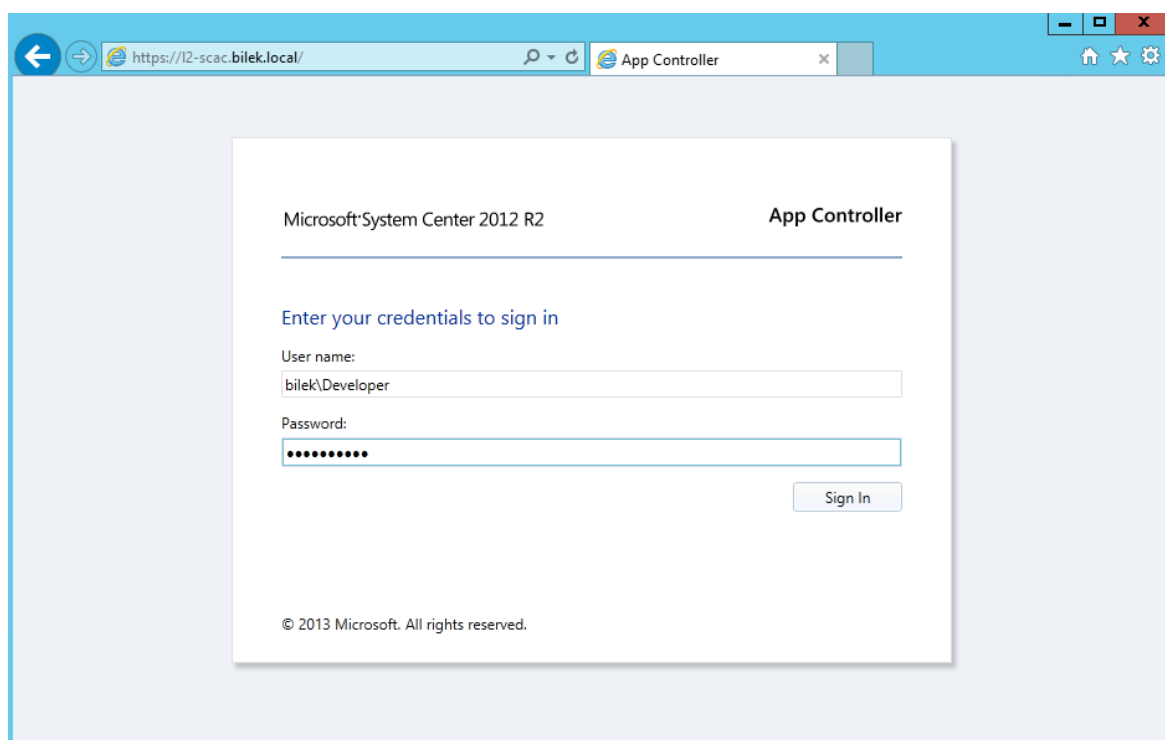
Obrázek 19- App Controller - připojení k SCVMM



Zdroj: vlastní zpracování

Toto je již veškerá nutná konfigurace. Nyní je možné přihlásit se účtem Developera, kterému bylo v minulých krocích uděleno právo k vytvoření služby. Vstupní dialog je znázorněn na následujícím obrázku 20.

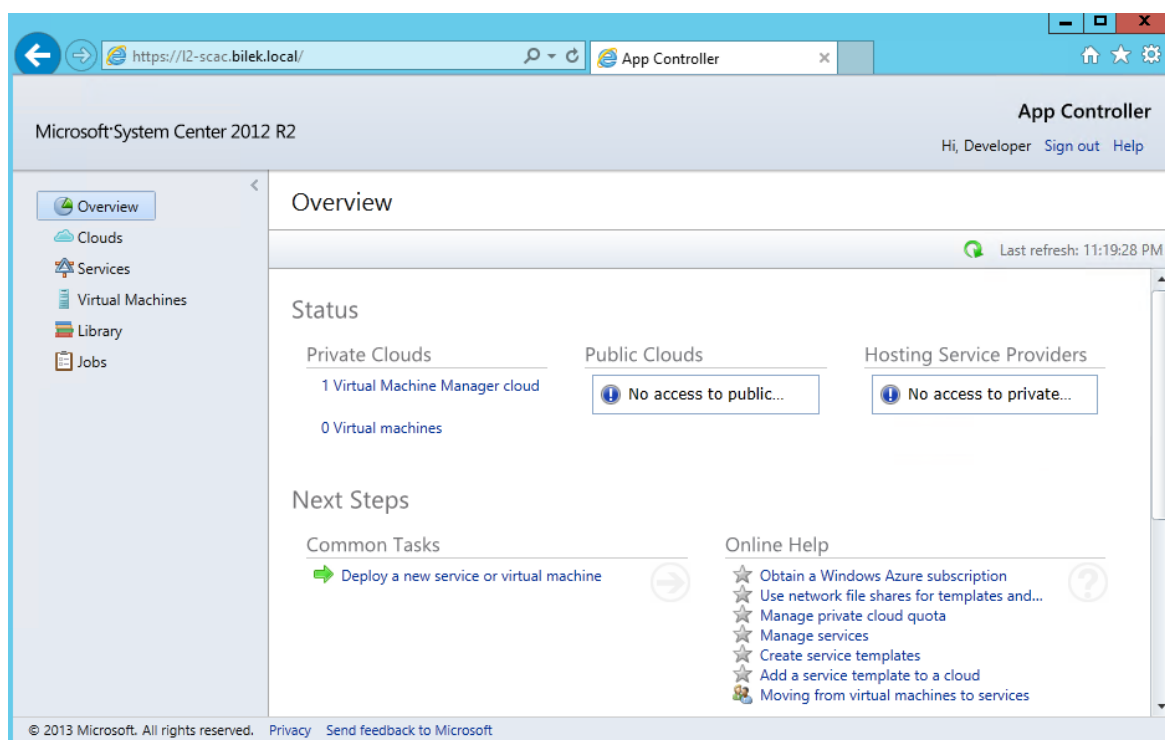
Obrázek 20- App Controller - portál



Zdroj: vlastní zpracování

Po přihlášení je zobrazen přehled na obrázku 21, na kterém je patrné, že je k dispozici jeden cloud (v předchozích krocích vytvořený „Cloud 1“) a nejsou k dispozici žádné veřejné cloudy ani hostované služby.

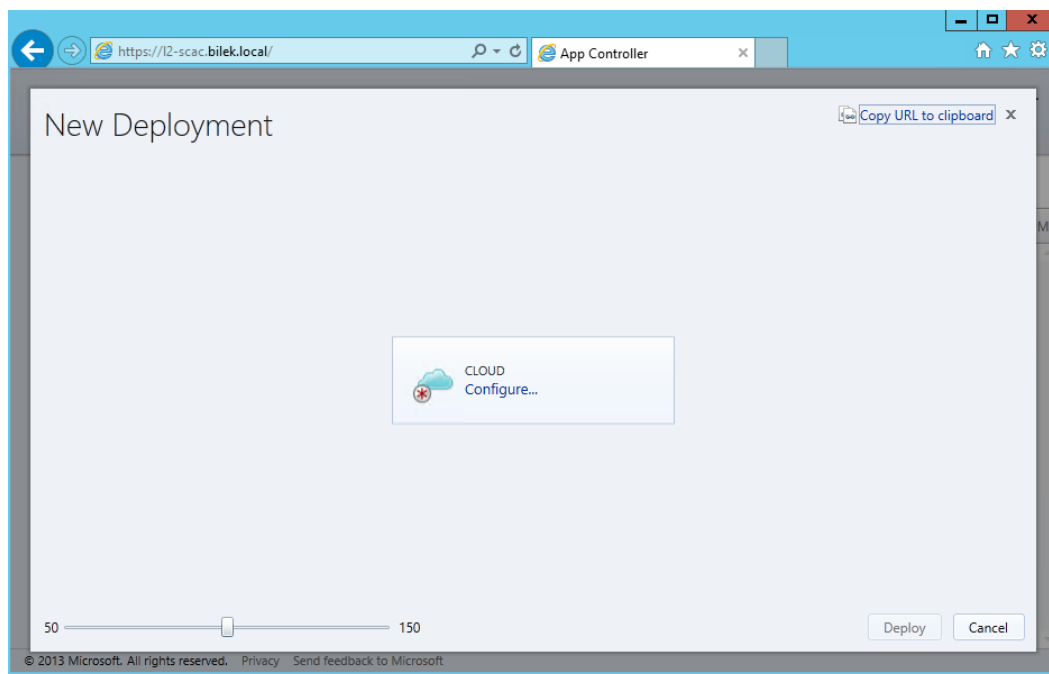
Obrázek 21- App Controller - portál, přehled



Zdroj: vlastní zpracování

Přes portál je možné požádat o vytvoření instance předdefinované služby. Poté se spustí průvodce, který je znázorněn obrázkem 22.

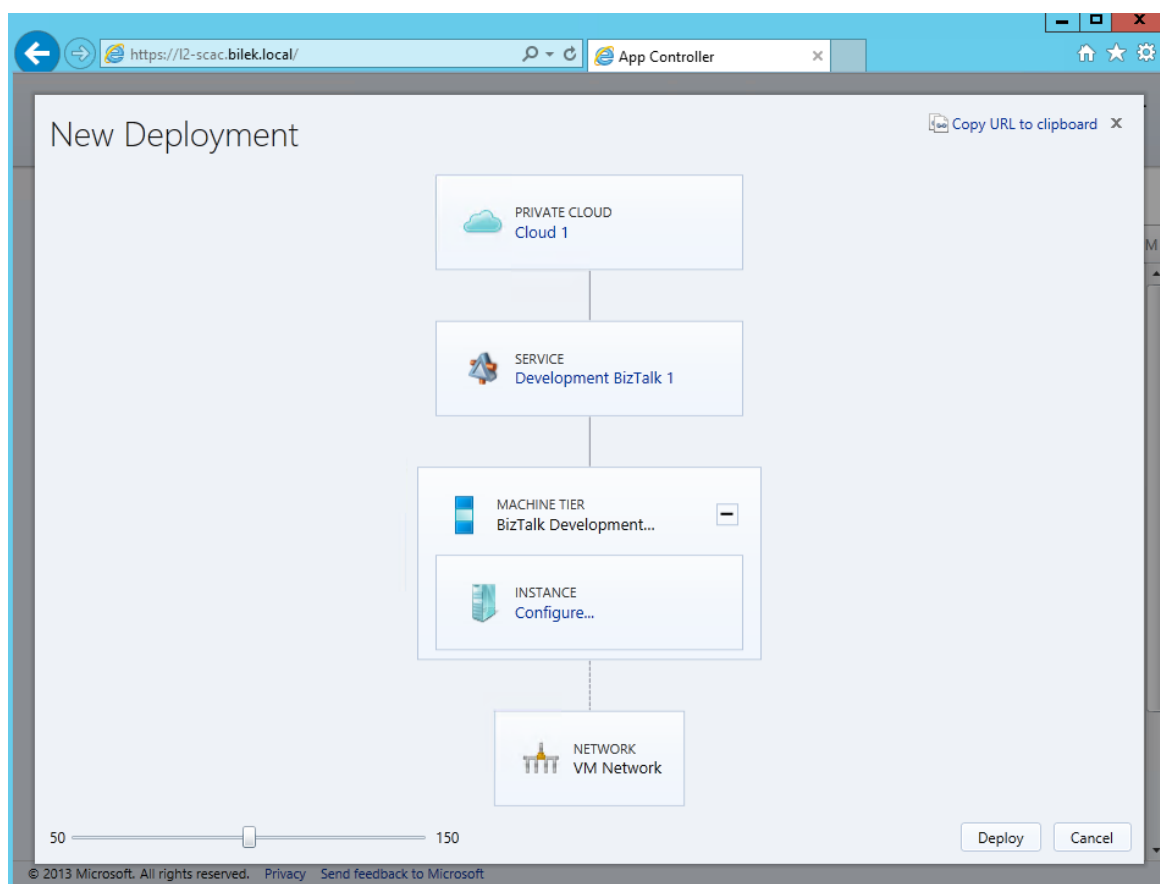
Obrázek 22- App Controller - Vytvoření služby



Zdroj: vlastní zpraocvání

Následně je uživatel vyzván ke specifikování cloudu, ve kterém má být požadovaná služba vytvořena. Po zadání jsou načteny aktuálně dostupné služby pro tento cloud a uživatel vybírá službu. Na dalším obrázku je zobrazena nasazovaná služba.

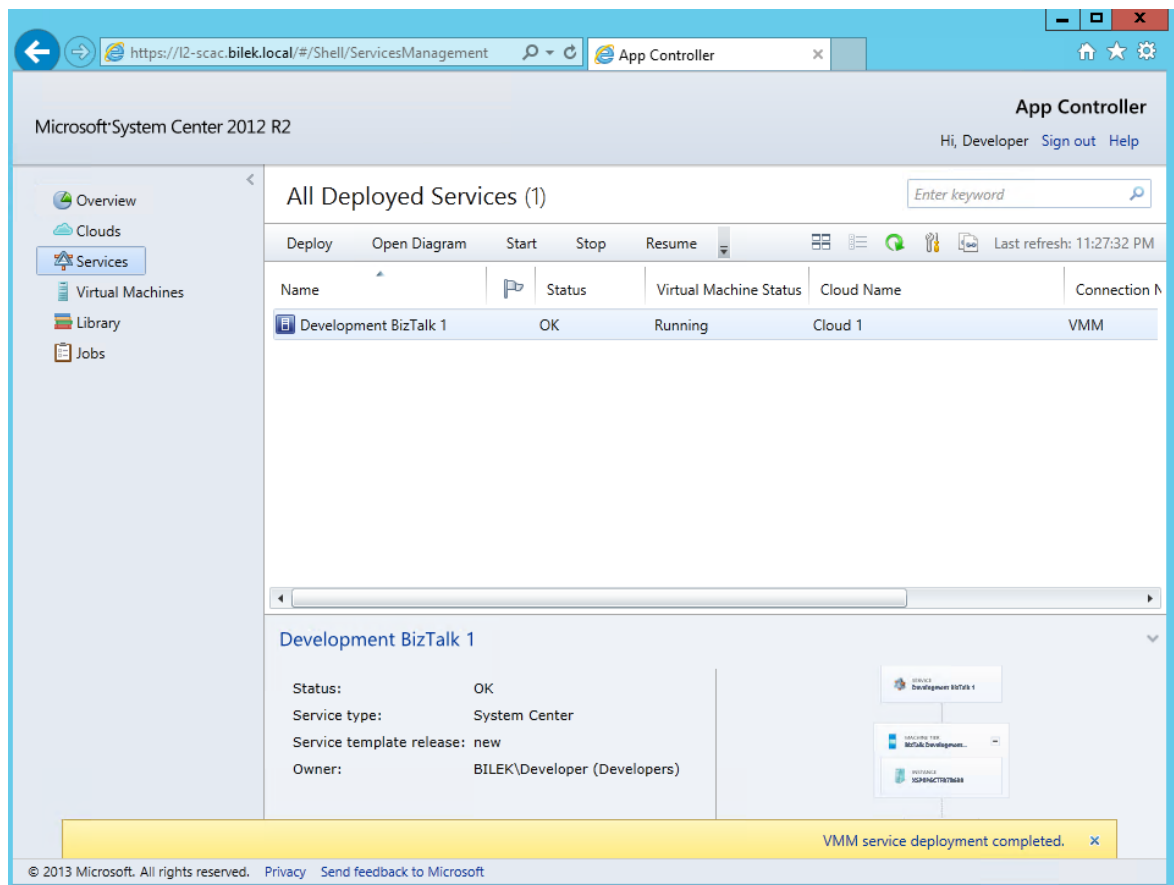
Obrázek 23- App Controller - služba



Zdroj: vlastní zpracování

Po stisknutí tlačítka „Deploy“ je zažádáno o vytvoření služby. Po vytvoření služby je uživatel notifikován a služba se objeví v portále.

Obrázek 24- App Controller - nasazená služba



Zdroj: vlastní zpracování

V seznamu virtuálních strojů se dále zobrazí vytvořené virtuální stroje, ze kterých se skládá vytvořená služba. Se službou je možné i nadále manipulovat. Je možné ji upravovat, zrušit, nebo požádat o novou, tak jak je to specifikováno ve vlastnostech jeho uživatelské role.

Tímto byl vytvořen a otestován privátní cloud, obsluhovaný přes samoobslužný portál a poskytující službu vývojářského prostředí.

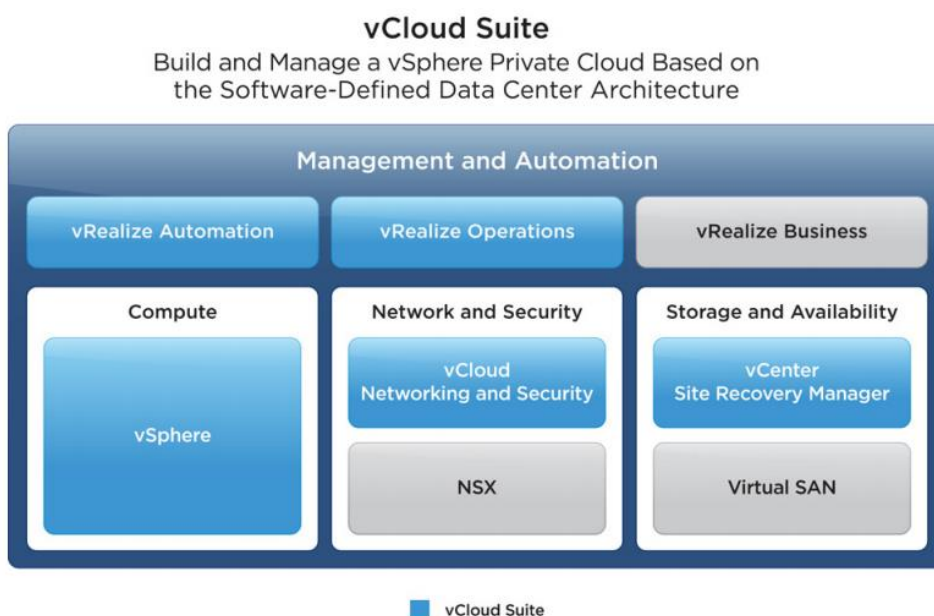
4.2 VMware

Řešení privátního cloudu společnosti VMware, je založené na balíku produktů vCloud suite, zahrnující hypervizor ESXi, platformu vSphere, komponenty pro automatizaci vCloud Automation Center.

4.2.1 Komponenty

Následující obrázek – 25 znázorňuje okruhy použití jednotlivých komponent vCloud suite.

Obrázek 25- VMware vCloud suite



Zdroj: VMware (15)

vSphere

VMware vSphere je název platformy a skupiny produktů společnosti VMware, zajišťující virtualizaci a vše s ní související. Dříve byla platforma vSphere známa jako VMware Infrastructure. Platforma vSphere obsahuje například:

- vSphere Virtual Machine File System – VMFS - souborový systém používaný pro ukládání virtuálních strojů na platformě vSphere;
- vSphere Virtual SMP – technologie umožňující jednomu virtuálnímu stroji použít více fyzických procesorů najednou;
- vSphere vMotion – technologie zajišťující živou migraci – migraci virtuálních strojů z jednoho hostitele na druhého, bez jejich vypnutí;

- vSphere Storage vMotion – umožňuje přenos datových souborů virtuálního stroje na jiného fyzického hostitele bez nutnosti vypnutí virtuálního stroje;
- vSphere High Availability (HA) – Technologie zvyšující dostupnost virtuálních strojů. V případě havárie fyzického stroje umožňuje automaticky restartovat virtuální stroje, které běžely na havarovaném serveru, na jiném fyzickém serveru;
- vSphere Distributed Resource Scheduler (DRS) – Technologie zlepšující využití výpočetního výkonu napříč datacentrem. Umožňuje přemigrovat virtuální stroje, které vyžadují vysoký výkon na fyzické stroje, které nejsou tolik vytížené;
- vSphere Storage Distributed Resource Scheduler (Storage DRS) – Technologie podobná DRS, týkající se úložiště. Umožňuje migrovat úložiště virtuálních strojů na fyzické hostitele s menším vytížením a tím i lepším výkonem;
- vSphere Fault Tolerance – Technologie společnosti VMware, umožňující vysokou dostupnost virtuálního stroje. Využívá zrcadlení operační paměti na dvou fyzických hostech technologií vLockstep. V případě náhlého výpadku jednoho z fyzických hostitelů, virtuální stroj běží nadále bez výpadku na druhém stroji. Rozdíl oproti vSphere High Availability spočívá v téměř nulovém výpadku – není nutno virtuální stroj znovu startovat – vše se provede transparentně pro běžící virtuální stroj;
- vSphere Distributed Switch (VDS) – Umožňuje provoz virtuálních strojů se stejným síťovým nastavením na různých fyzických hostech;
- Pro účely naplnění testovacího scénáře, jsou použity komponenty VMware vSphere Client a VMware vSphere Web Client.

vCenter Site Recovery Manager

Nástroj pro automatizaci disaster recovery scénářů a failover testování virtualizovaných aplikací. Tento nástroj, ačkoli je součástí vCloud suite, není součástí nasazovaného řešení.

VMware Identity Appliance

Nástroj pro správu identit a propojení s Active Directory

vCenter Operations (nově vRealize Operations)

Nástroj pro měření výkonu, monitoring, plánování kapacity ve vSphere prostředí. Tento nástroj, ačkoli je součástí vCloud suite, není součástí nasazovaného řešení.

vCloud Automation Centre (nově vRealize Automation)

Nástroj umožňující samoobslužnost ve vSphere prostředí. Jedná se o klíčovou součást implementace cloudu. Je tvořen virtuální appliance a dále infrastrukturní částí, která musí být instalována na serveru běžícím na Windows Serveru.

4.2.2 Instalace a konfigurace prostředí

Tato část popisuje laboratorní prostředí a dále instalaci a konfiguraci jednotlivých komponent. Laboratorní prostředí obsahuje následující servery:

- doménový řadič domény janbilek.local s adresou janbilek-dc1.janbilek.local, použitý taktéž jako DNS server, běžící na Windows 2012 R2;
- server s adresou vcac-appliance.janbilek.local, nasazený jako virtuální appliance vCloud Automation Center;
- server s adresou vcac-identity.janbilek.local, nasazený jako virtuální appliance vCloud Automation Center Identity Appliance;
- členský server domény janbilek.local, s adresou vcac-iaas.janbilek.local, s nainstalovanou aplikací SQL Server 2012, a vCloud Automation Center IAAS Components;
- hypervizor ESXi s adresou esxi1.janbilek.local.

Instalace hypervizoru

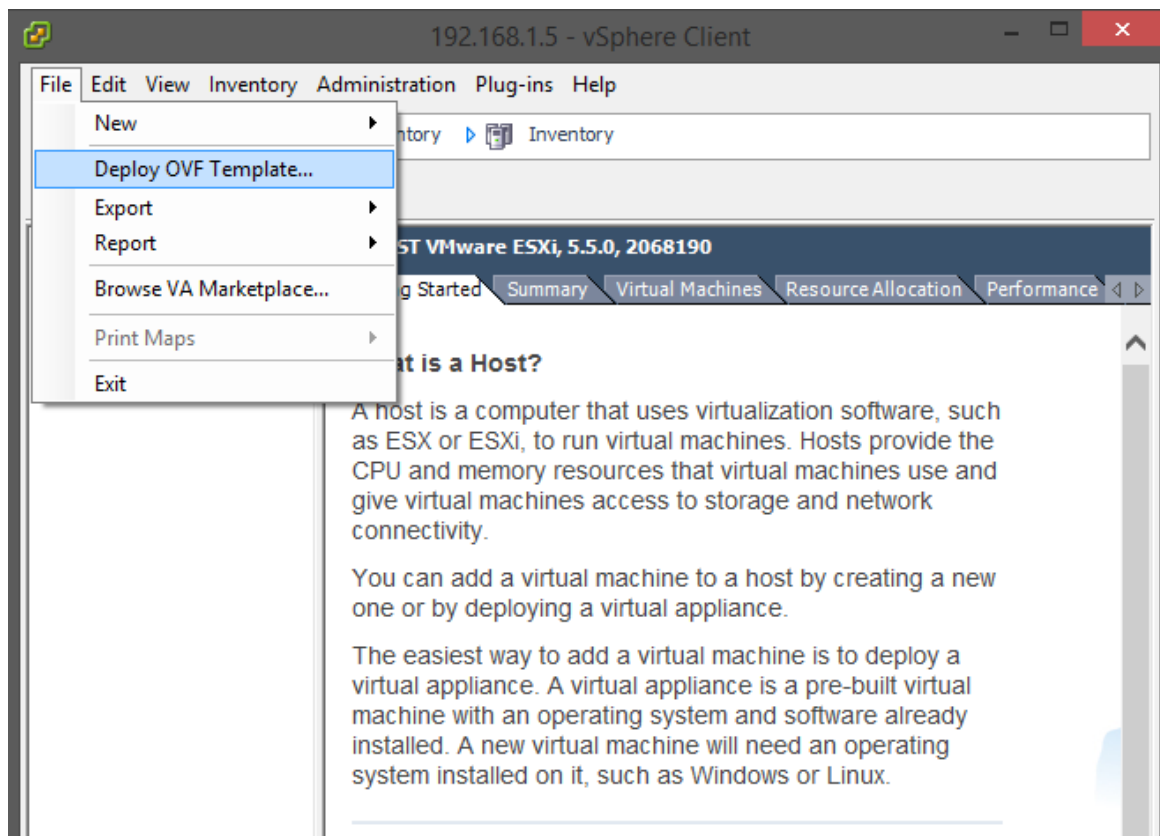
Instalace ESXi hypervizoru byla proveda vložení instalačního media do mechaniky serveru a následováním pokynů instalátoru. Po dokončení instalace je možné se k ESXi serveru připojit pomocí vSphere klienta. Jedná se o aplikaci pro MS Windows, s jejíž pomocí lze spravovat ESXi server.

Instalace vCenter serveru

Pro instalaci vCenter serveru bylo v předchozích verzích nutné instalovat virtuální stroj na bázi Microsoft Windows, do kterého se následně nainstalovala aplikace vCenter server od společnosti VMware. V aktuálních verzích ale společnost VMware postupně odstupuje od tohoto způsobu a používá koncept virtuálních „Appliance“. Virtuální appliance je předpřipravený obraz virtuálního serveru – v tomto případě na bázi linuxu, který se naimportuje do virtuálního prostředí a nakonfiguruje obvykle přes webové rozhraní. Mezi výhody tohoto řešení patří rychlá a jednoduchá instalace a také nezávislost na platformě Windows.

Samotná instalace appliance produktu vCenter byla provedena pomocí vSphere Clienta, po připojení k hypervizoru ESXi, je zvolením možnosti File->Deploy OVF Template spuštěn průvodce importem virtuální appliance, která je reprezentována OVF (Open Virtualization Format), případně (Open Virtual Appliance) souborem.

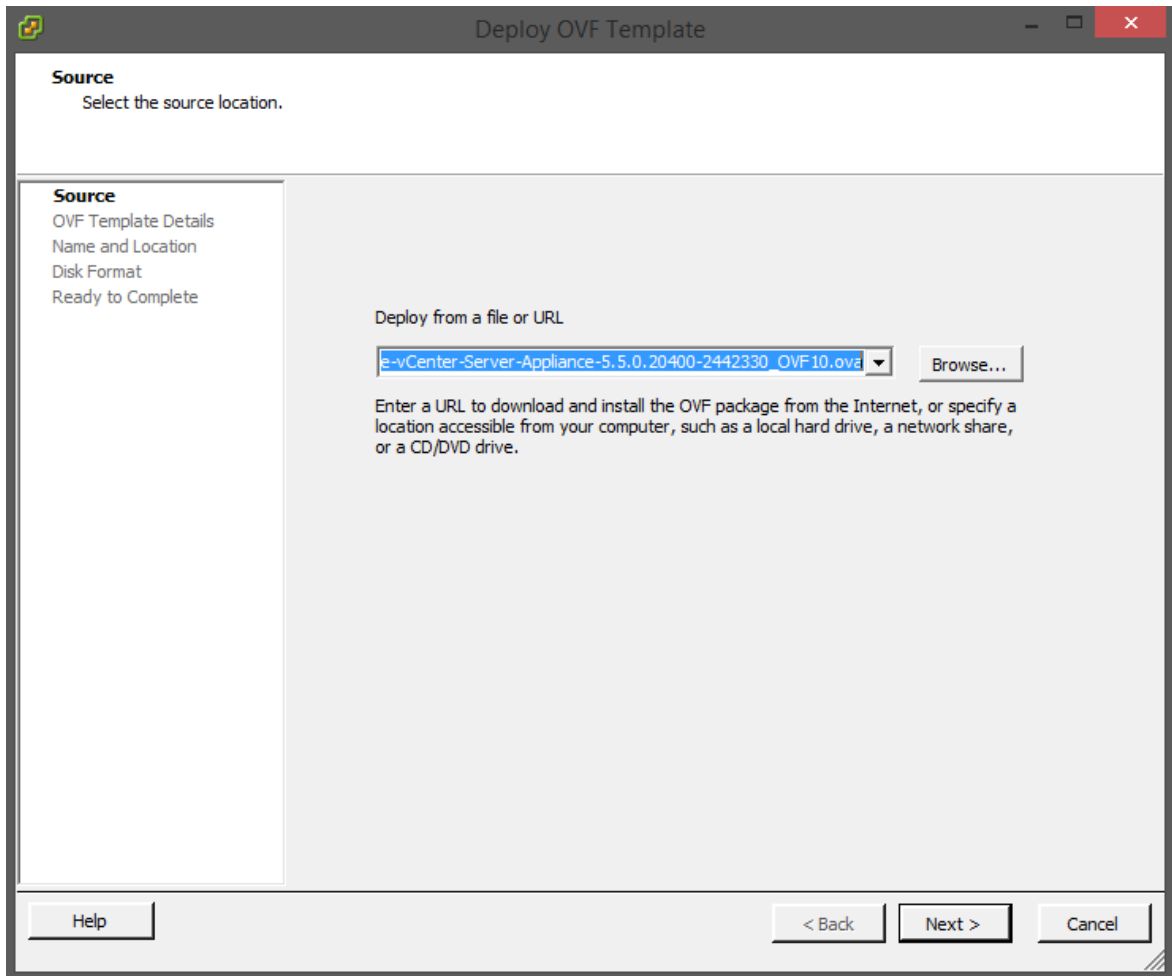
Obrázek 26- vCenter - Deploy OVF Template



Zdroj: vlastní zpracování

V následujícím kroku je zadána cesta k OVA souboru, který obsahuje virtuální appliance.

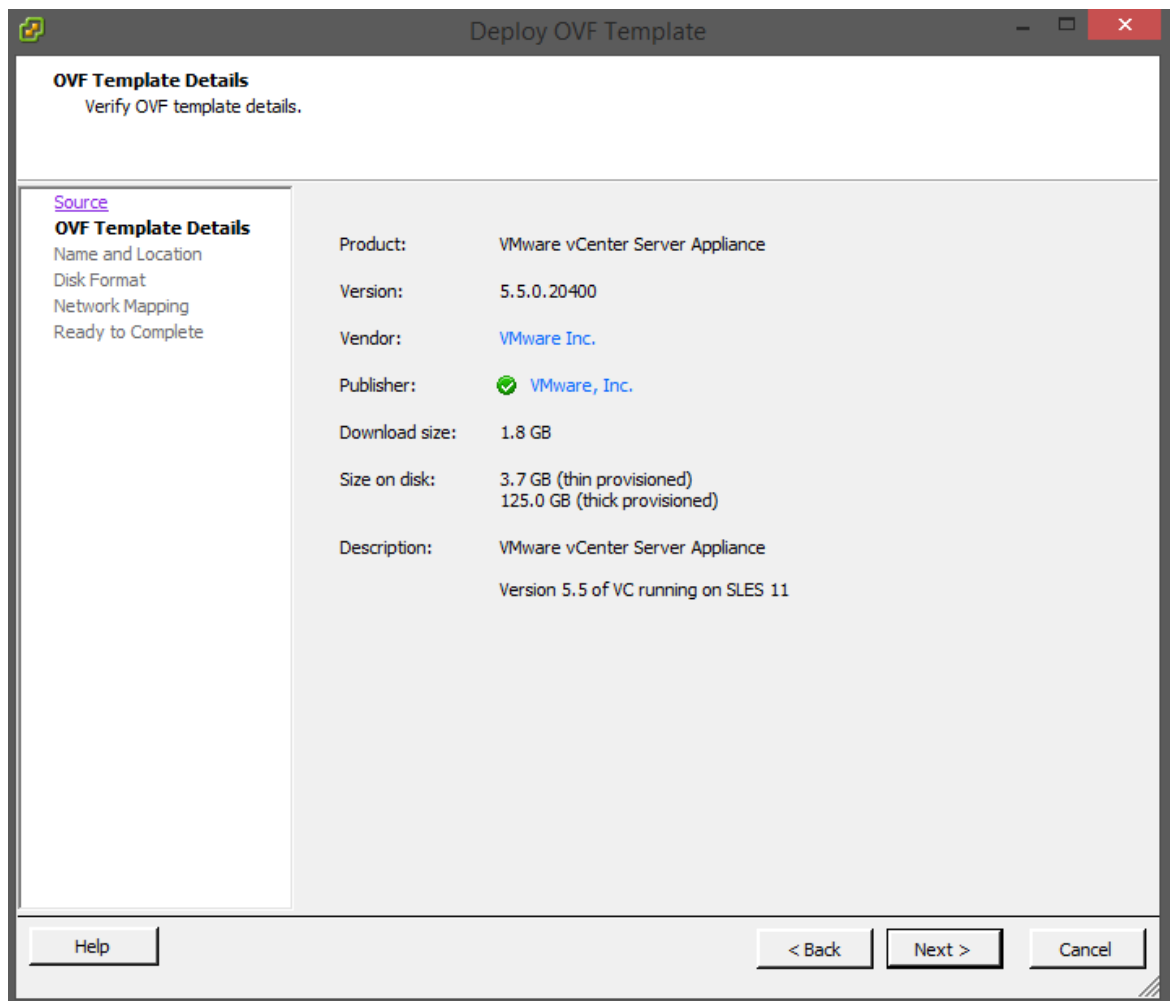
Obrázek 27- Deploy OVF Template - volba zdroje



Zdroj: vlastní zpracování

Po načtení souboru jsou zobrazena data o importované appliance.

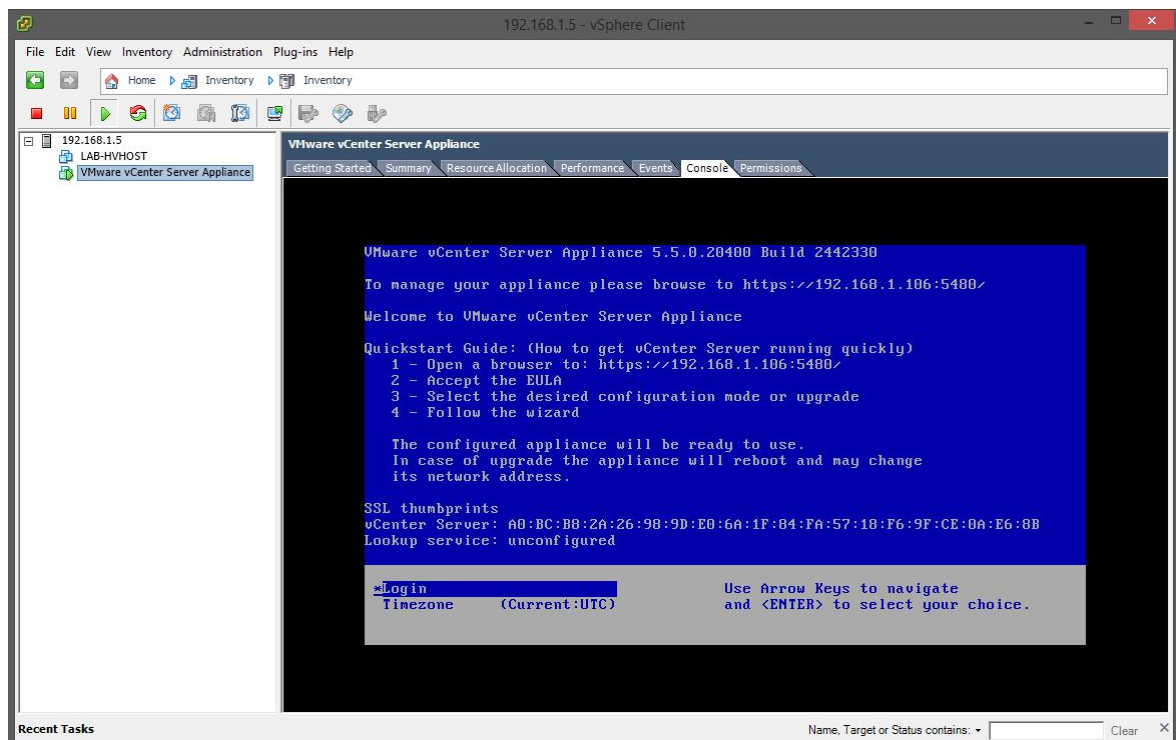
Obrázek 28- Deploy OVF Template - OVF Detaily



Zdroj: vlastní zpracování

Dále je zadáno jméno instance, a další detaily. Po dokončení importu a spuštění appliance se provede úvodní nastavení zakončené obrazovkou na obrázku 29.

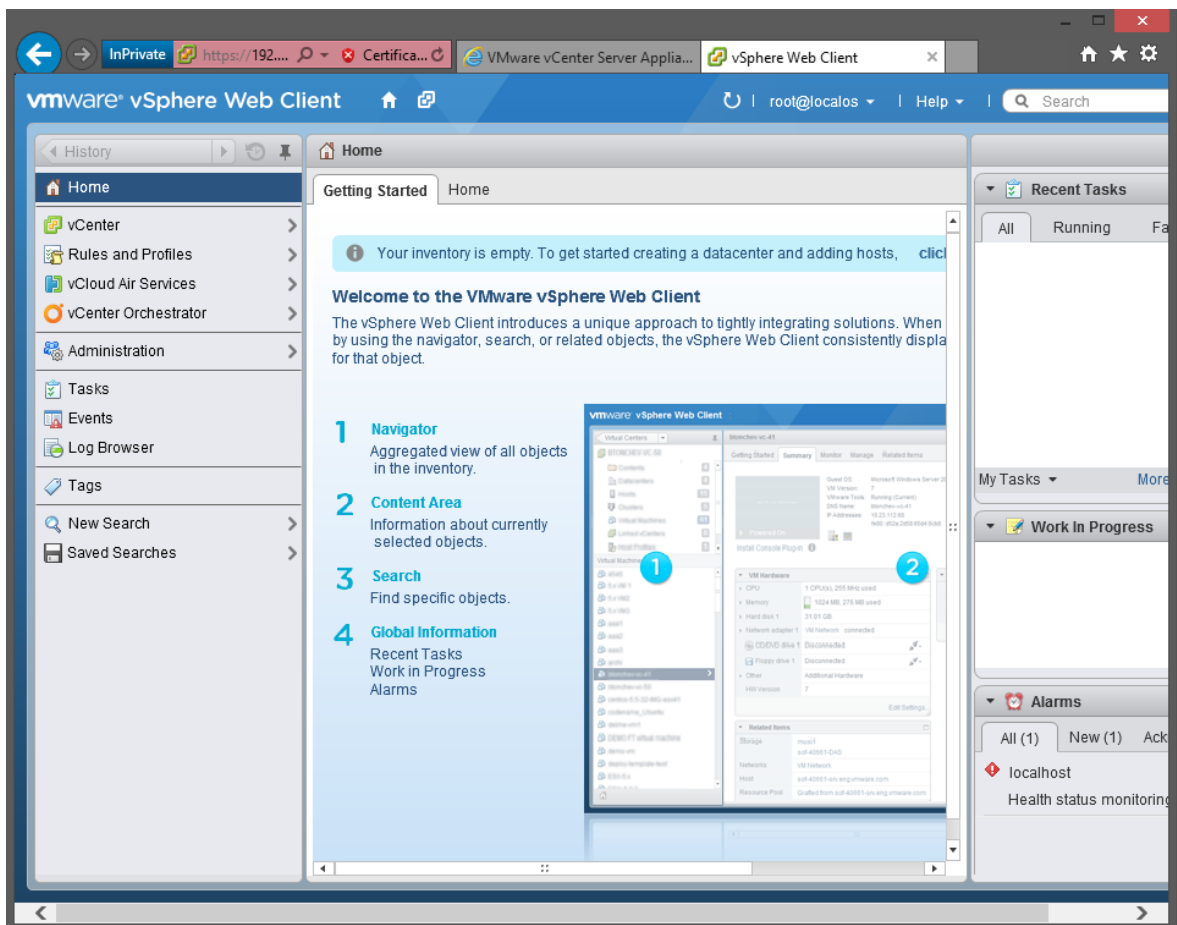
Obrázek 29- vCenter server instalace konzole



Zdroj: vlastní zpracování

Instalace dále pokračuje přes webové rozhraní, kde dojde k odsouhlasení smluvních podmínek a dokončení nastavení. Po tomto kroku je již možné využívat webový klient.

Obrázek 30- vCenter web client

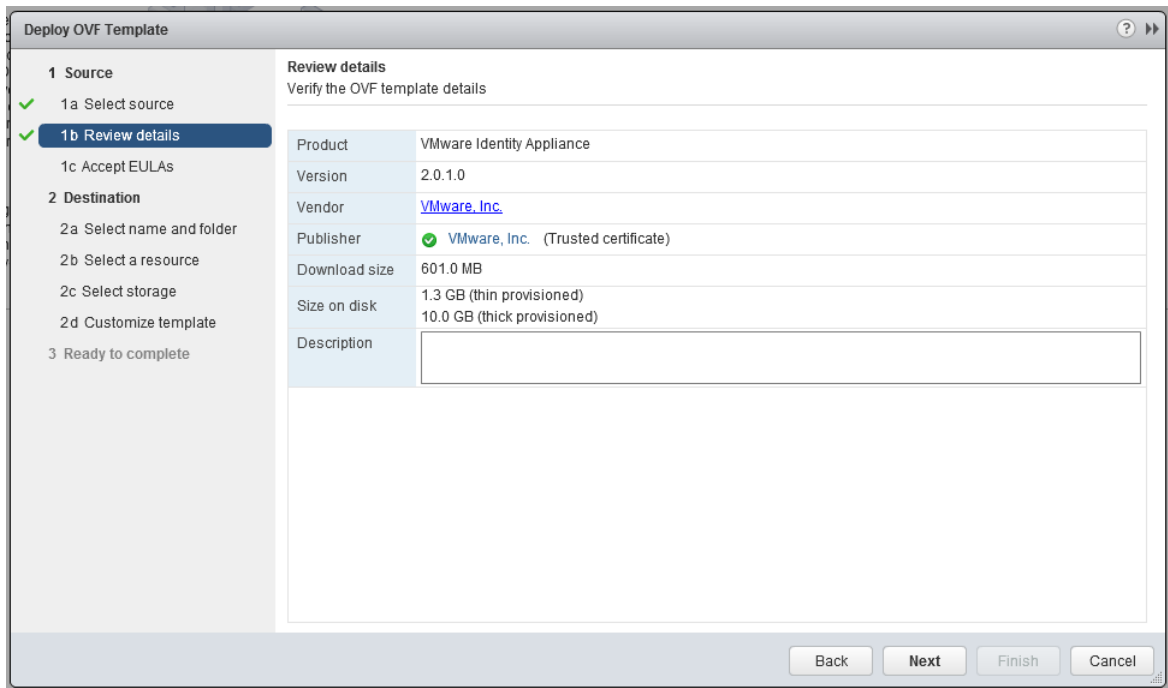


Zdroj: vlastní zpracování

Instalace VMware Identity Appliance

Instalace VMware Identity Appliance probíhá podobně jako instalace vCenter appliance, nyní je však použit webový klient, přes který je appliance importována.

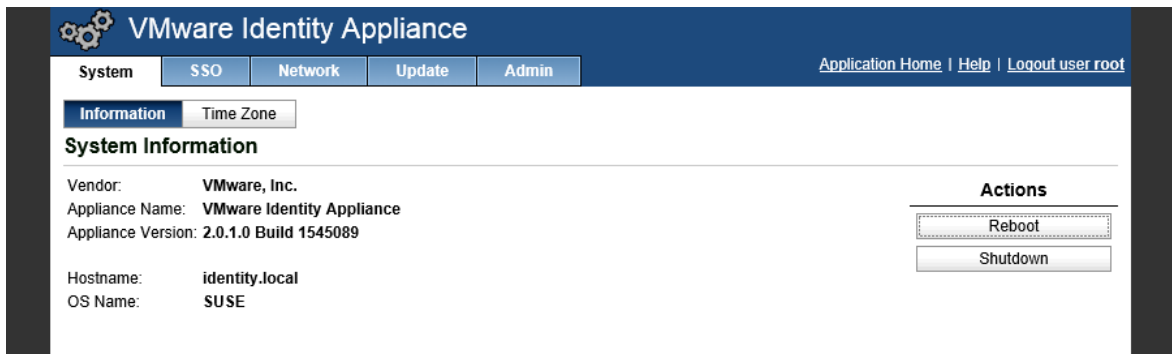
Obrázek 31- VMware Identity Appliance – nasazení přes web client



Zdroj: vlastní zpracování

Po dokončení importu appliance je instalace dokončena přes webové rozhraní.

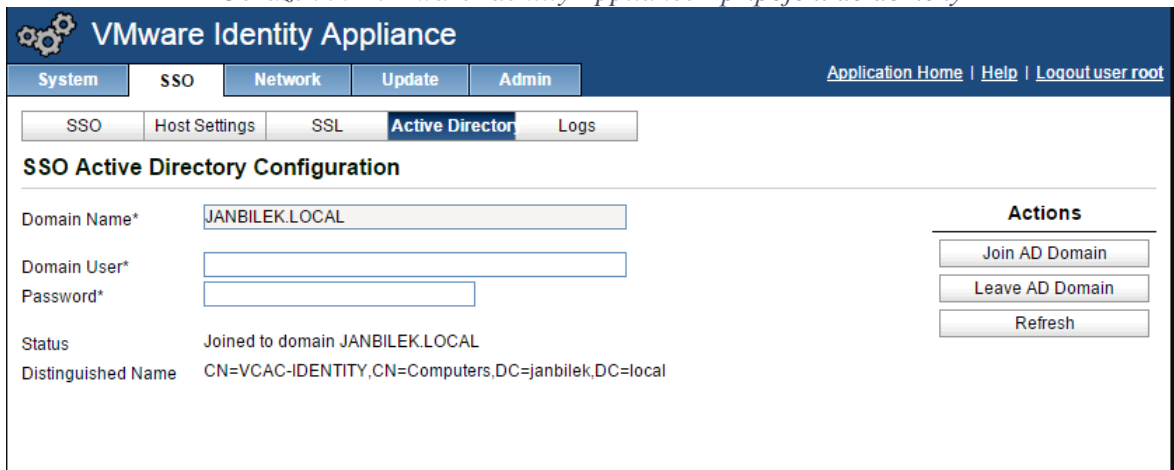
Obrázek 32- VMware Identity Appliance - webové rozhraní



Zdroj: vlastní zpracování

Přes webové rozhraní VMware Identity Appliance, je dále appliance spojena s doménou janbilek.local.

Obrázek 33- VMware Identity Appliance - připojení do domény

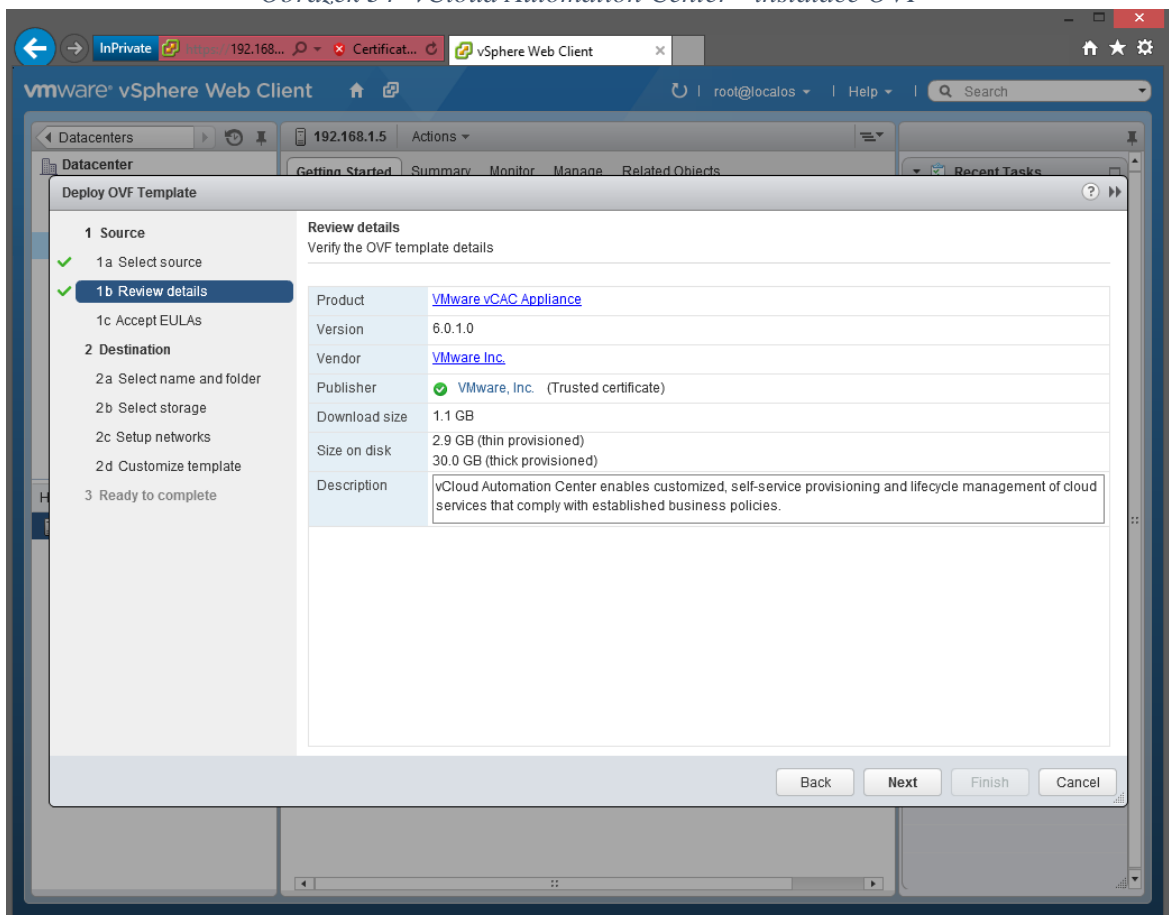


Zdroj: vlastní zpracování

Instalace vCloud Automation Center

Instalace vCloud Automation Center je provedena importem virtuální appliance přes vSphere web klient.

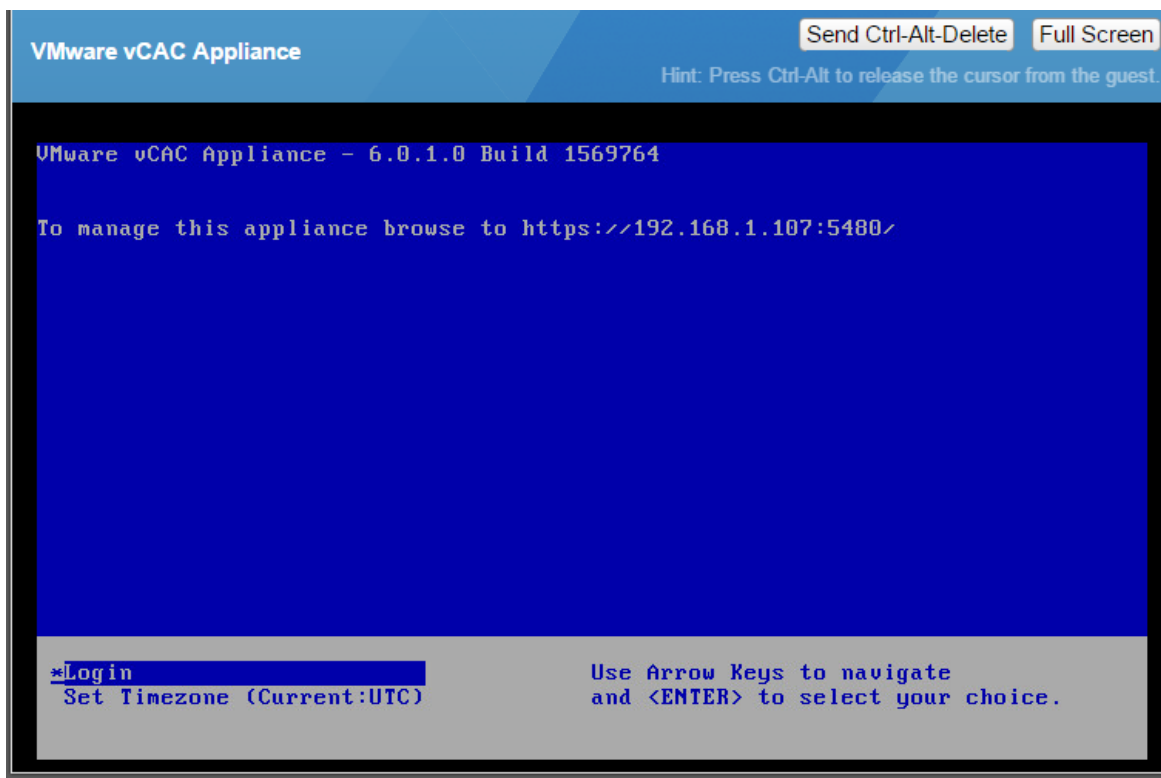
Obrázek 34- vCloud Automation Center - instalace OVF



Zdroj: vlastní zpracování

Po dokončení importu a startu vCloud Automation Center, je možné se přihlásit do administračního webového rozhraní. Pokud je při instalaci zvolena možnost získat IP adresu z DHCP serveru, tuto adresu zjistíme přihlášením na konzole virtuální appliance.

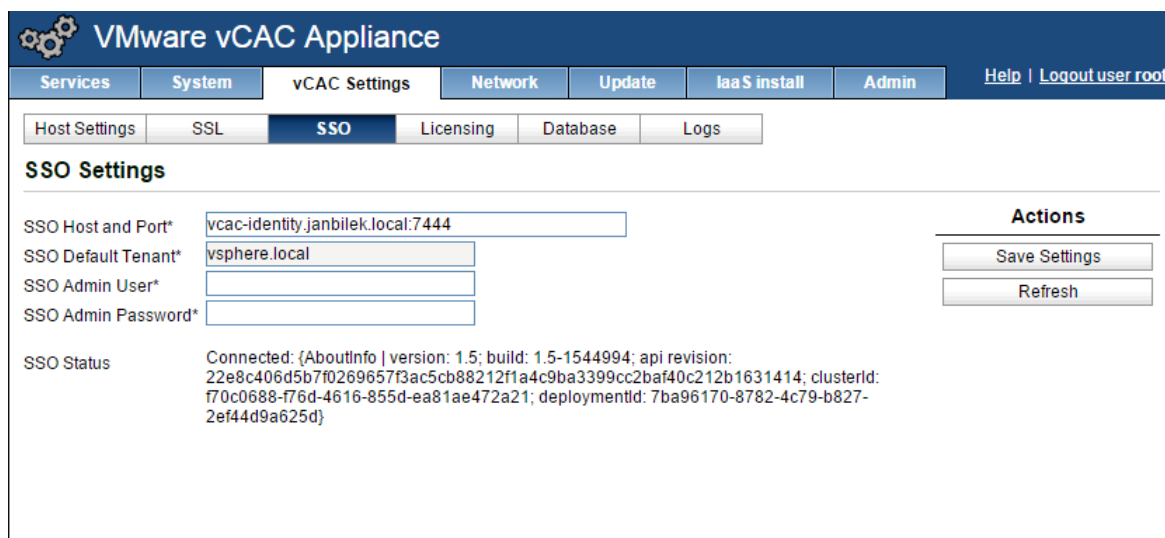
Obrázek 35- vCAC - konzole



Zdroj: vlastní zpracování

Další kroky konfigurace přes webové rozhraní zahrnují konfiguraci doménového jména, certifikátu zabezpečení webového rozhraní a také připojení na vcac-identity appliance, která zajišťuje SSO (Single Sign On) funkcionalitu.

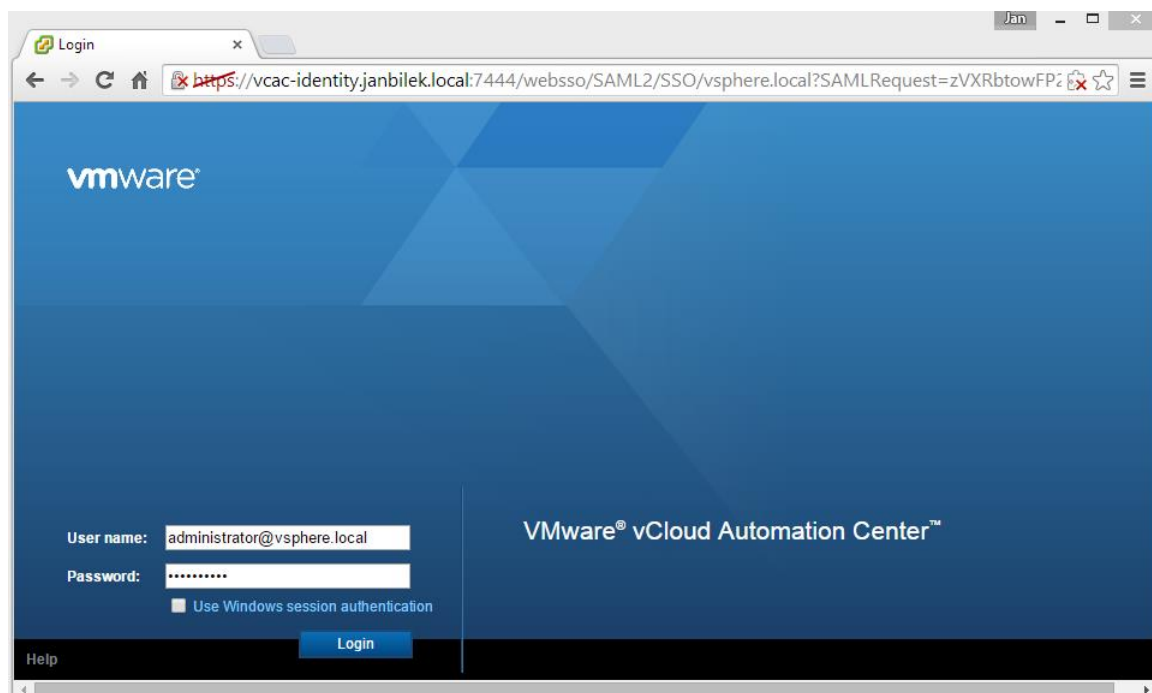
Obrázek 36- vCAC - konfigurace SSO



Zdroj: vlastní zpracování

Po nastavení SSO je možné se přihlásit do webového klienta VMware vCloud Automation Center pomocí účtu administrátora VMware identity. Webový klient vCAC se v tomto případě nachází na adrese <https://vcac-appliance.janbilek.local/shell-ui-app>. Při přihlašování je přihlašovací dialog přeměřován na vcac-identity.janbilek.cz (patrně z následujícího obrázku), kde je požadavek ověřen a předán zpět vCAC klientovi.

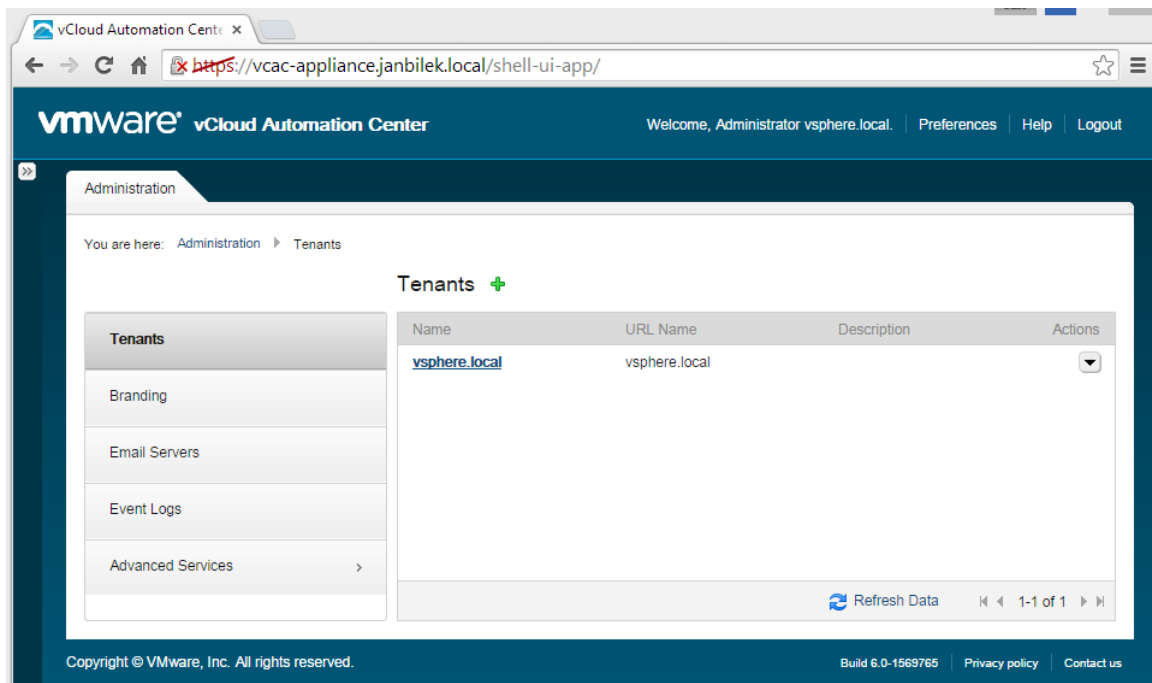
Obrázek 37- vCAC web klient - ověření



Zdroj: vlastní zpracování

Po ověření je uživatel přihlášen do vCAC web klienta - viz obrázek 38. Tímto je ověřena funkčnost ověřování přes VMware identity appliance.

Obrázek 38- vCAC web klient – administrátor přihlášen

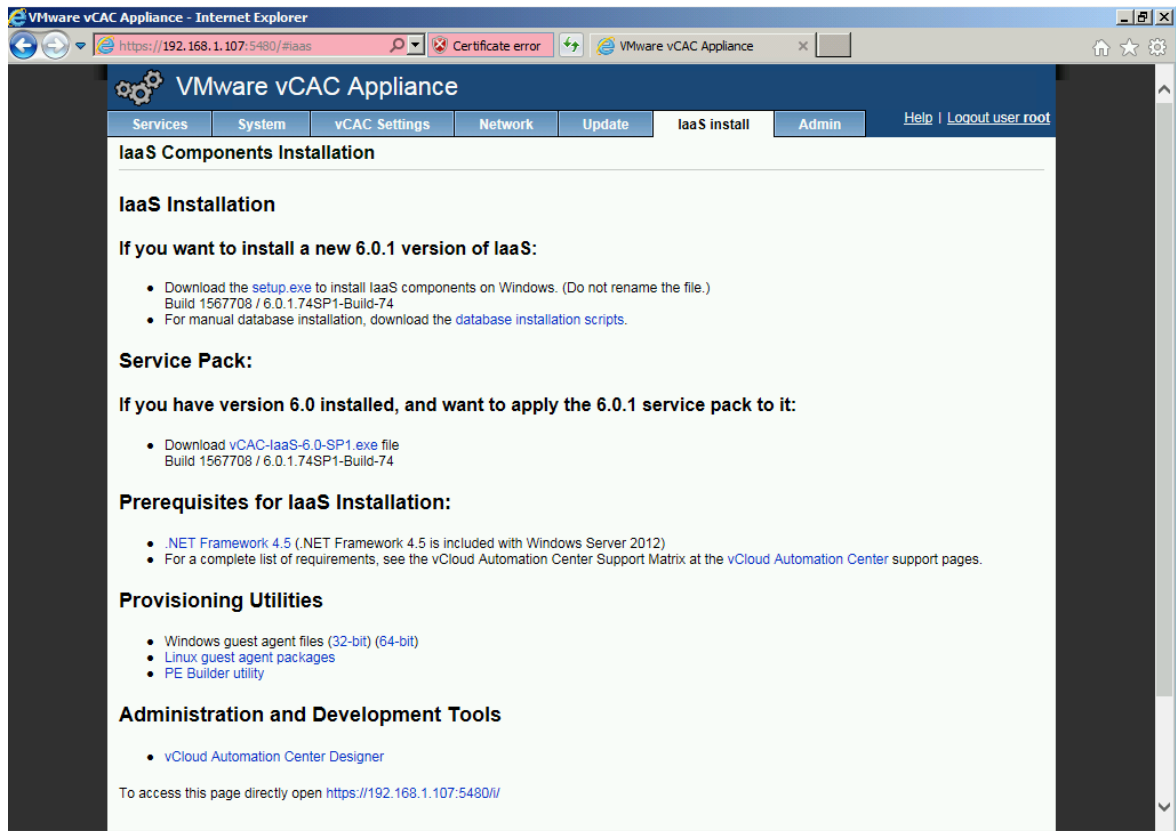


Zdroj: vlastní zpracování

Instalace vCloud Automation Center – IaaS components

Instalaci vCAC – IaaS je nutné provést na stroj, který běží na operačním systému Windows. Instalace vCAC využívá SQL server jako databázový stroj, je tedy nutné mít k dispozici instanci SQL serveru, na kterém jsou v průběhu instalace vytvořeny požadované databáze. Z tohoto stroje je následně stažen instalační balíček z vCAC Appliance administračního rozhraní – sekce IaaS Install.

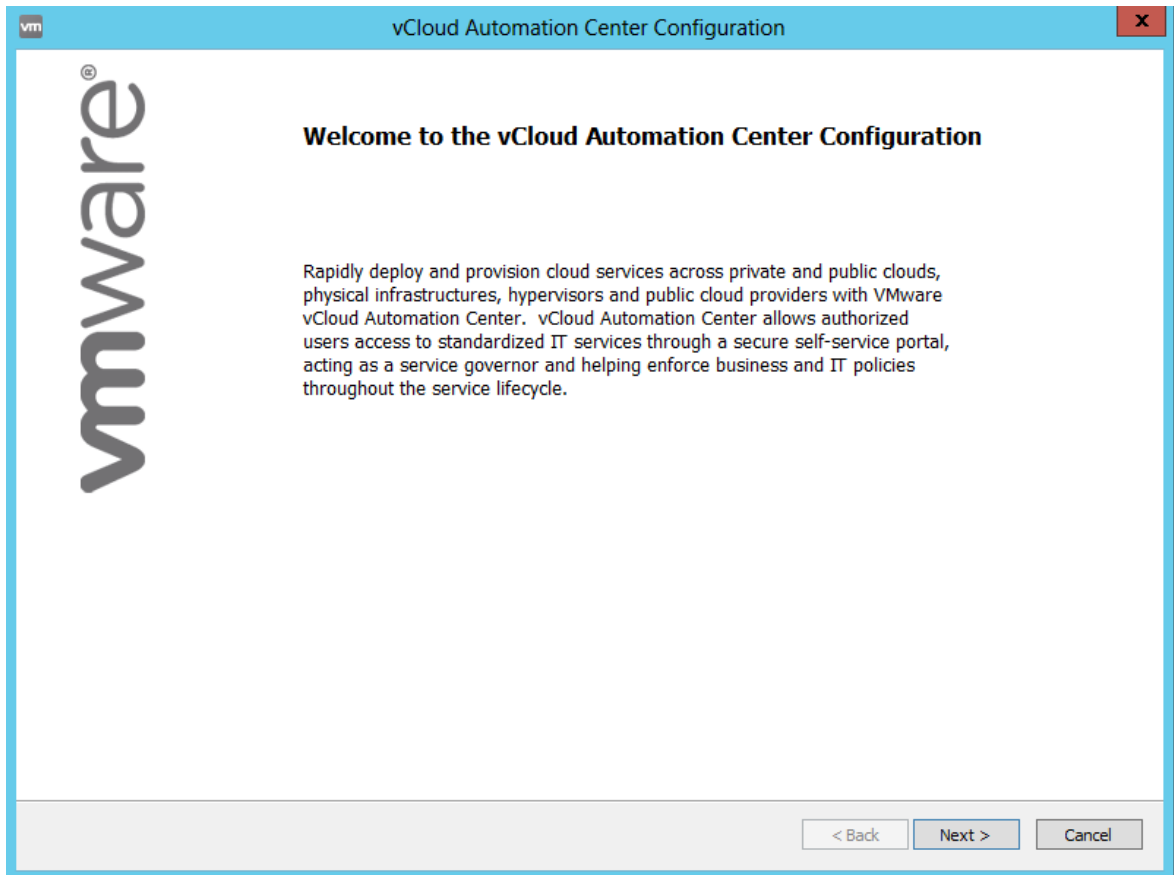
Obrázek 39- vCAC IaaS - Instalace



Zdroj: vlastní zpracování

Po stažení souboru setup.exe je spuštěn instalátor. Tento soubor je jedinečný pro každou instalovanou instanci vCAC appliance a obsahuje údaje o této jednotlivé appliance. Není tedy možné použít tento soubor z jiného prostředí, kde je nasazena vCAC appliance. Následující obrázek znázorňuje instalátor IaaS Components

Obrázek 40- vCAC IaaS Instalátor



Zdroj: vlastní zpracování

V průběhu instalace je ověřena přítomnost pre-rekvizit nutných pro instalaci, dále specifikována lokace SQL serveru, uživatelské účty, pod kterými poběží služby potřebné pro provoz IaaS komponent, přihlašovací údaje root uživatele pro vcac-appliance a také údaje nutné pro připojení komponent ke službě SSO běžící na VMware identity appliance – jak ukazuje následující obrázek.

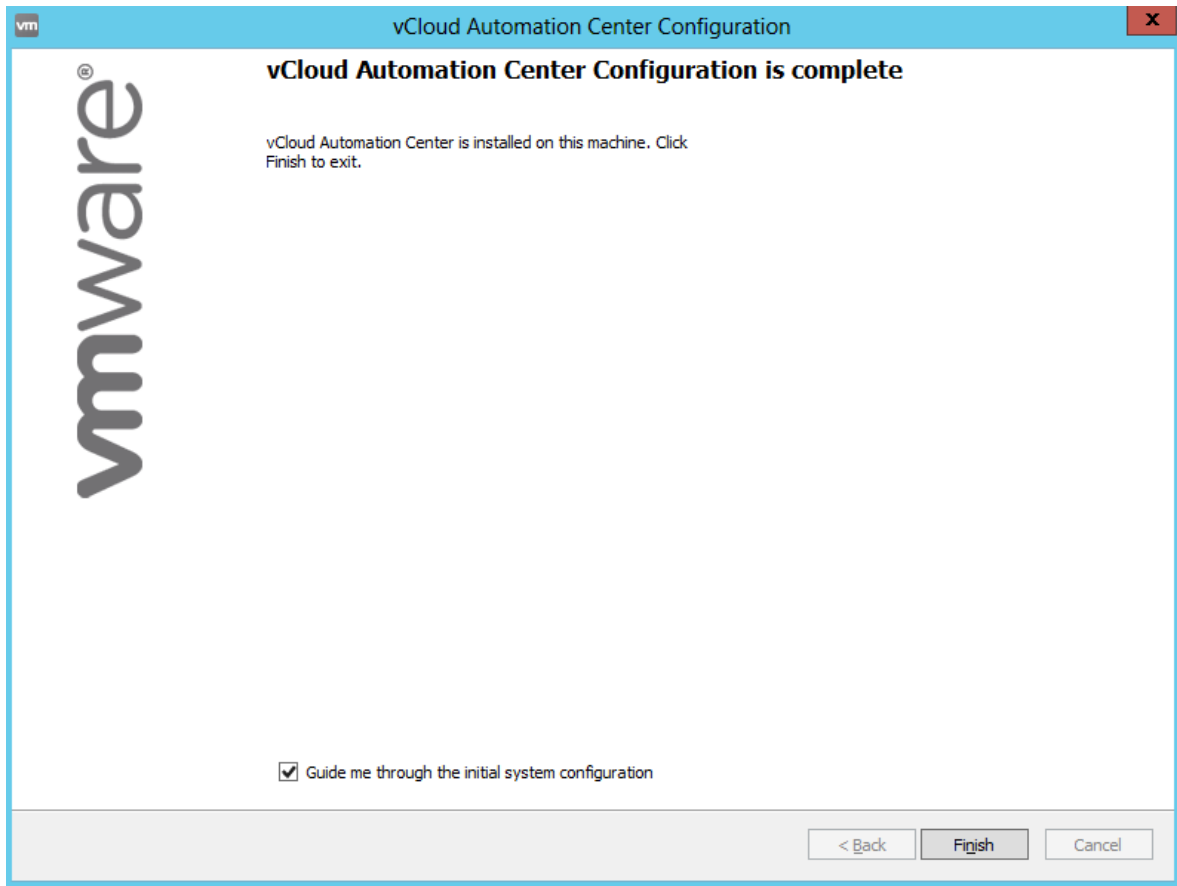
Obrázek 41- vCAC IaaS - konfigurace SSO

The screenshot shows the 'vCloud Automation Center Configuration' window. The main title is 'Component Registry' with the instruction 'Specify the information to register the IaaS components with vCloud Automation Center.' The window is divided into three sections: 'Component Registry', 'SSO Administrator Credentials', and 'IaaS'. In the 'Component Registry' section, the 'Server' field contains 'vcac-appliance.janbilek.local'. The 'SSO Default Tenant' field contains 'vsphere.local' with a 'Load' button. The 'Certificate' field contains 'CN=vcac-appliance.janbilek.local, OU=local, O=janbilek, C=cz' with a 'Download' button. Below the certificate field, there is a link 'View Certificate' and a checked checkbox 'Accept Certificate'. The 'SSO Administrator Credentials' section has a 'User name' field with 'administrator@vsphere.local' and a 'Test' button. The 'Password' and 'Confirm' fields are masked with asterisks. The 'IaaS' section has an 'IaaS Server' field with 'vcac-new' and a 'Test' button. Below this field is the instruction 'Enter the host name or IP address of the local machine.' At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Zdroj: vlastní zpracování

Po tomto nastavení jsou vytvořeny potřebné databáze a služby, což je potvrzeno informací o dokončení instalace. Dalším krokem je konfigurace cloudu přes vCAC appliance.

Obrázek 42- vCAC - instalace dokončena



Zdroj: vlastní zpracování

Konfigurace cloudu

V předchozích krocích byly nainstalovány všechny potřebné komponenty. Dále je provedena konfigurace cloudu a jeho uživatelů. Prvním krokem je nastavení odběratele cloudových služeb (Tenant) a jeho připojení k Identity Storu, který v tomto případě je Active Directory doména janbilek.local. Tímto nastavením je zajištěno, že se uživatel může přihlásit svým uživatelským jménem a heslem, které používá v doméně a nemusí používat další uživatelské jméno a heslo jenom pro připojování ke cloudu. Na následující obrázku je zobrazen formulář konfigurace Identity Store ve vCloud Automation Center.

Obrázek 43- vCAC - Identity Store

The screenshot shows the 'Add Identity Store' configuration page in the VMware vCloud Automation Center. The page has a dark blue header with the VMware logo and 'vCloud Automation Center' text. On the right side of the header, there is a welcome message 'Welcome, Administrator vsphere.local.' and links for 'Preferences', 'Help', and 'Logout'. The main content area is titled 'Add Identity Store' and contains a form with the following fields:

- Name:** Development
- Type:** Active Directory (dropdown menu)
- URL:** ldap://janbilek-dc1.janbilek.local:389
- Domain:** janbilek.local
- Domain alias:** (empty field)
- Login user DN:** CN=vcacuser,CN=Users,DC=janbilek,DC=local
- Password:** (masked with dots)
- Group search base DN:** OU=Development,DC=janbilek,DC=local
- User search base DN:** (empty field)

A green checkmark icon and the text 'Connection is available.' are displayed at the top left of the form. At the bottom right of the form, there are three buttons: 'Test Connection', 'Add', and 'Cancel'.

Zdroj: vlastní zpracování

Dále je vytvořen Endpoint, v tomto případě je endpointem vCenter server. Je ale možné vytvořit jako endpoint i Hyper-V, XenServer a jiné. Po vytvoření endpointu jsou načteny zdroje, které má daný endpoint k dispozici. Tyto zdroje jsou použity v dalším kroku, ve kterém je vytvořena skupina uživatelů – Developerů, kterým jsou zdroje přiřazeny. Po přiřazení zdrojů skupině uživatelů, je možné vytvořit tzv. blueprint, což je vzor virtuálního stroje, případně služby. V tomto případě je zvolena možnost klonování vzorového stroje, který je již přednastaven. Je možné ale zvolit sofistikovanější workflow, které vytvoří například vícestupňovou aplikaci.

Obrázek 44- vCAC - konfigurace blueprint

vmware vCloud Automation Center

Welcome, dev-vcac. Preferences Help Logout

Home Catalog Items Requests Inbox Administration Infrastructure

You are here: Home > Infrastructure > Blueprints > Blueprints

Edit Blueprint - vSphere (vCenter)

Modify the blueprint by making changes below.

Blueprint Information Build Information Properties Actions

Blueprint type: Server
Action: Clone
* Provisioning workflow: CloneWorkflow
* Clone from: BizTalk Development Template
Customization spec:

Machine Resources

* Minimum Maximum

CPUs: 8
Memory (MB): 8096
Storage (GB): 50
Lease (days):
(Leave blank for no expiration date)

* Storage volumes: Volumes (1)

#	Capacity (GB)	Drive Letter / Mount Path	Label	Storage Reservation Policy
0	50			

Allow user to see and change storage reservation policies

Maximum volumes: 15
Maximum network adapters: Unlimited

OK Cancel

Zdroj: vlastní zpracování

Po vytvoření blueprintu je dále nastavena a publikována služba, která bude využívat tento blueprint. Skupině Developerů jsou přiřazena práva pro využití této služby a také akce, které mohou provádět.

Obrázek 45- vCAC - nastavení služby

Add Entitlement

Details | Items & Approvals

Entitled Services +

Search

Name	Approval Policy
BizTalk Devel...	(none) ▼

Entitled Catalog Items +

Search

Name	Approval Policy
BT2010	(none) ▼

Entitled Actions +

Search

Name	Approval Policy
Add Compon...	(none) ▼
Associate Flo...	(none) ▼
Cancel Reco...	(none) ▼
Change Leas...	(none) ▼
Connect Usin...	(none) ▼
Connect Usin...	(none) ▼
Connect Usin...	(none) ▼
Connect Usin...	(none) ▼

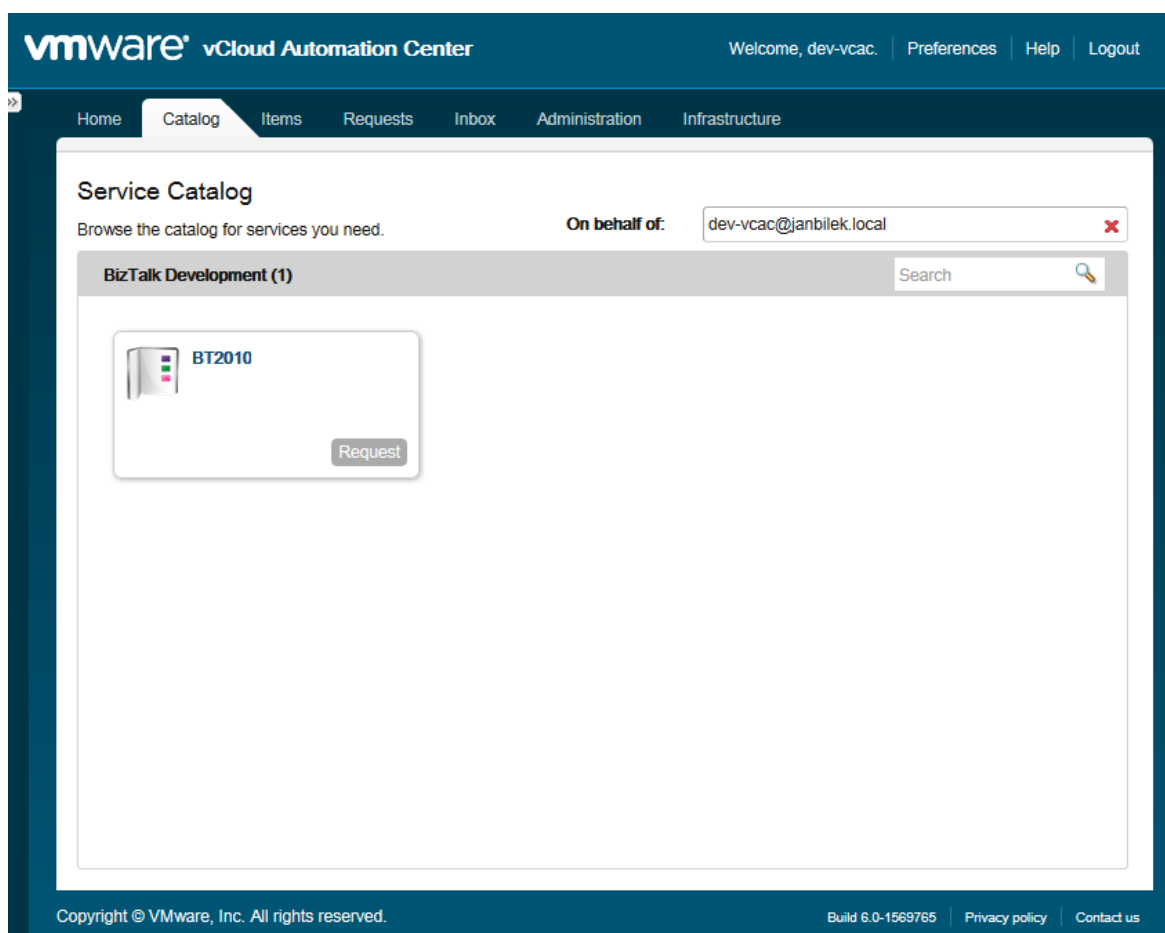
< >

< Back Add Cancel

Zdroj: vlastní zpracování

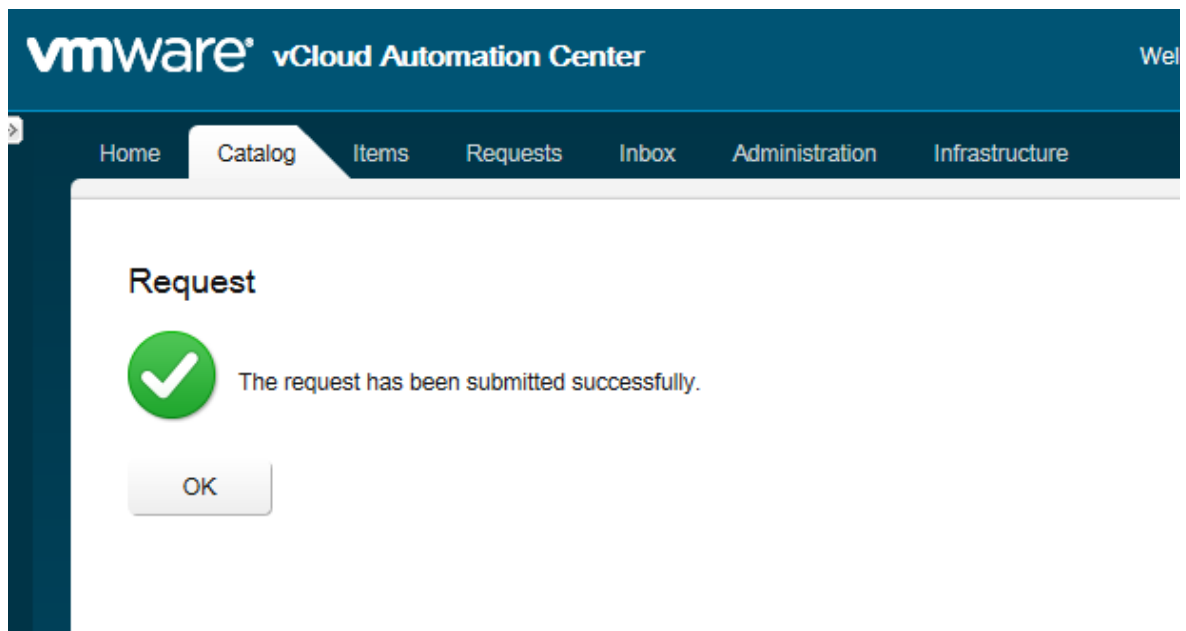
Po nastavení služby je nastavení dokončeno a zákazník může požádat o vytvoření služby. Služba je dostupná přes vCAC Automation Center.

Obrázek 46- vCAC - žádost o službu



Zdroj: vlastní zpracování

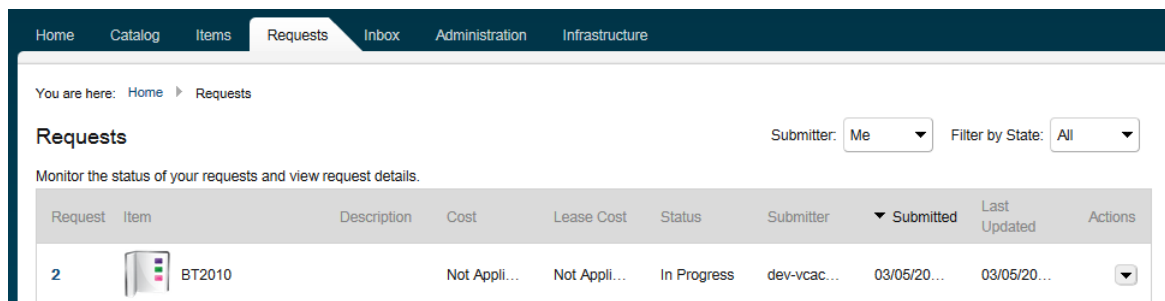
Obrázek 47- vCAC - žádost podána



Zdroj: vlastní zpracování

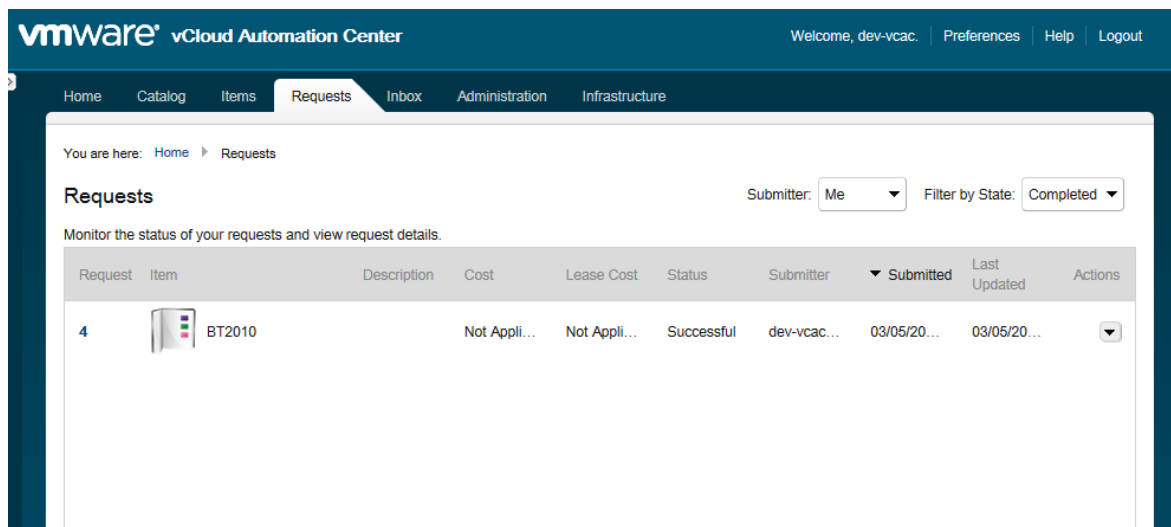
Po podání žádosti o službu je požadavek předán vCenter serveru, uživatel může stav požadavku sledovat v záložce Requests.

Obrázek 48- vCAC - Requests



Zdroj: vlastní zpracování

Obrázek 49- vCAC - žádost úspěšně dokončena



Zdroj: vlastní

Tímto je služba vytvořena a připravena pro použití zákazníkem. Vytvoření služby je možné ověřit také z logu vCenter serveru, který bude obsahovat následující informace.

Obrázek 50- vCenter server - vytvořena služba

Name	Target	Status	Details	Initiated by	Requested start time	Start time	Completed time
Power On virtual mach...	dev004	Completed		vpxuser	3/5/2015 5:27:26 AM	3/5/2015 5:27:26 AM	3/5/2015 5:27:28 AM
Create virtual machine	192.168.1.5	Completed		vpxuser	3/5/2015 5:26:14 AM	3/5/2015 5:26:14 AM	3/5/2015 5:26:17 AM

Zdroj: vlastní zpracování

5 Zhodnocení výsledků

V předchozí kapitole byly implementovány jednotlivé produkty, které tvoří řešení privátního cloudu v podání jednotlivých dodavatelů – společností Microsoft a VMware. Tato kapitola obsahuje shrnutí poznatků získaných při práci s těmito produkty a dále nabízí ekonomické srovnání na uvedeném příkladu portálu pro vývojáře.

5.1 Technické srovnání

Oba dodavatelé nabízí produkty, které splňují požadavky na privátní cloud, avšak každý dodavatel k řešení přistupuje odlišně. Zatímco společnost VMware spoléhá na technologii virtuálních appliance, konkurenční společnost Microsoft razí cestu instalací jednotlivých produktů na servery s OS MS Windows. Během implementace laboratorního řešení se ukázalo jako problematictější řešení s virtuálními appliance, které trpěly různými neočekávanými chybami a několik funkcí nefungovalo napoprvé tak, jak mělo. Mezi největší problémy patřilo propojení serveru s nainstalovanými IaaS komponentami se serverem s vCAC appliance. Problém se ale nakonec podařilo vyřešit a celé řešení zprovoznit. Instalace řešení společnosti Microsoft proběhla v pořádku.

Na druhou stranu nutno podotknout, že řešení společnosti VMware jako celek působí výrazně komplexnějším dojmem a nabízí širší možnosti nastavení. Na produktech společnosti VMware, zejména na hypervizoru ESXi, jsou znatelné roky vývoje a ladění. Trh s virtualizačními produkty se ale posouvá od hypervizorů směrem k souvisejícím produktům a službám. Jinými slovy hypervizory přestávají přinášet zisk. Každý dodavatel dnes dodává svůj hypervizor zdarma k použití a zisk následně přinášejí až související aplikace a služby. A právě v souvisejících aplikacích (vCAC, vCAC IaaS) je znatelný prostor pro zlepšení, který se ještě násobí po přihlédnutí k ekonomické stránce věci.

5.2 Ekonomické porovnání

Následující kapitola zahrnuje porovnání nákladů na licence, odpovídající zadání výše uvedené implementace. Jedná se o licence na dva fyzické servery. Každý je osazen dvěma procesory. Jako zdroj cen byly použity internetové prezentace dodavatelů a ceny jsou uvedeny jako ceníkové, bez zohlednění jakýchkoliv slev. Každý z dodavatelů poskytuje na dodávané licence slevy, jejich výše se ale mění v závislosti na mnoha faktorech, proto pro účely porovnání jsou použity pouze ceníkové ceny, ačkoliv v případě reálné objednávky budou konečné ceny pravděpodobně nižší.

5.2.1 Microsoft

V případě řešení společnosti Microsoft je třeba licencovat dva produkty. Prvním je samotný operační systém Windows Server 2012 R2 v edici Datacenter, která umožní licenčně pokrýt neomezený počet virtuálních instancí Windows Serveru. Dalším produktem je balík System Center 2012R2, taktéž v edici Datacenter, který opět umožní pokrýt neomezený počet virtuálních instancí a to bez dodatečných nákladů.

Oba produkty mají shodné licencování. Jedna licence pokrývá maximálně 2 fyzické procesory. Pro 2 fyzické servery jsou tedy potřeba 2 licence od každého produktu.

Velká výhoda licencování společnosti Microsoft je v tom, že v ceně licencí je zahrnuta licence na operační systém pro virtuální stroje. Pokud tedy potenciální zájemce o private cloud řešení provozuje v současné době prostředí s převahou serverů s operačním systémem od Microsoft, může být tato nabídka velmi zajímavá.

Tabulka 1- Licence Microsoft

Produkt	Počet licencí	Cena za 1 licenci	Cena celkem
Windows Server 2012 R2 Datacenter	2	6155 USD (16)	12310 USD
System Center 2012R2 Datacenter	2	3607 USD (17)	7214 USD
Celková cena			19524 USD

Zdroj: vlastní zpracování

5.2.2 VMware

Cena za VMware řešení obsahuje jen cenu za licence nástrojů, které umožní Private Cloud vybudovat a provozovat, neobsahuje žádné licence pro operační systémy virtuálních strojů. Proto v případě provozu Windows Serverů na tomto cloudu je třeba připočítat ještě cenu za jejich licence a podle počtu serverů je nutné zvolit odpovídající počet licencí edice Standard, popřípadě pokrýt servery licencemi edice Datacenter. Licence vCloud suite jsou prodávány podle počtu osazených procesorů, v tomto případě dva fyzické servery, každý se dvěma procesory, dohromady 4 licence. V cenové kalkulaci je počítáno s licencí vCloud Enterprise.

Tabulka 2- Licence VMware

Produkt	Počet licencí	Cena za 1 licenci	Cena celkem
vCloud Suite Enterprise	4	11495 USD (18)	45980 USD
Celková cena			45980 USD

Zdroj: vlastní zpracování

6 Závěr

Problematika privátního cloudu je důsledkem přirozeného vývoje informačních technologií. Do popředí se dostávají stále sofistikovanější systémy, které i díky rostoucímu výpočetnímu výkonu a kapacitám výpočetních systémů umožňují realizovat nové koncepty. Před několika lety se stejně tak hovořilo o virtualizaci, jejíž nástup byl označován jako nástup moderního IT. Dnes je virtualizace používána jako komponenta privátního cloudu a jako moderní jsou označovány systémy, které umožňují úkony co nejvíce automatizovat a zjednodušit.

Těmito systémy se zabývá tato bakalářská práce, která charakterizuje řešení privátního cloudu a v kapitole 3. Teoretická východiska, popisuje virtualizaci a privátní cloud v souvislostech a širším kontextu a zavádí definice cloudu podle NIST.

Přínosem k této problematice je kapitola 4. Vlastní práce, která je založená na vytvoření kompletního prostředí privátního cloudu v laboratorním prostředí, za použití komponent dvou nejdůležitějších dodavatelů na trhu. Model využívá charakteristik cloudu zavedených v kapitole 3. Teoretická východiska.

Praktickým zjištěním je skutečnost, že vhodným výběrem dodavatele řešení privátního cloudu, může společnost ušetřit významnou část nákladů.

7 Seznam použitých zdrojů

1. LAPLANTE, Tim. Virtualization has surpassed 50 percent of all server workloads. *DataCenterPost.com*. [Online] 20. 3 2014. [Citace: 1. 9 2014.] <http://datacenterpost.com/2014/03/virtualization-surpassed-50-percent-server-workloads.html>.
2. AMREHN, Erich. 45 (40)Years of Mainframe Virtualization: CP-67/CMS and VM/370 to z/VM. [Online] [Citace: 20. 8 2014.] [https://www-950.ibm.com/events/wwe/grp/grp019.nsf/vLookupPDFs/7%20-%20VM-45-JahreHistory-EA-J-Elliott%20%5BKompatibilit%C3%A4tsmodus%5D/\\$file/7%20-%20VM-45-JahreHistory-EA-J-Elliott%20%5BKompatibilit%C3%A4tsmodus%5D.pdf](https://www-950.ibm.com/events/wwe/grp/grp019.nsf/vLookupPDFs/7%20-%20VM-45-JahreHistory-EA-J-Elliott%20%5BKompatibilit%C3%A4tsmodus%5D/$file/7%20-%20VM-45-JahreHistory-EA-J-Elliott%20%5BKompatibilit%C3%A4tsmodus%5D.pdf).
3. VMware - Server Consolidation. *VMware*. [Online] VMware, 2015. [Citace: 20. 1 2015.] <http://www.vmware.com/consolidation/consolidate>.
4. *International Journal of Advanced Research in Computer Science & Technology (IJARCST 2014)*. S. Suresh, Dr. M.Kannan. 2, 2014, Sv. A Study on System Virtualization Techniques. ISSN : 2347 - 8446.
5. VMware, Inc. 3401 Hillview Ave, Palo Alto. Understanding Full Virtualization, Paravirtualization, and Hardware Assist. [Online] http://www.vmware.com/files/pdf/VMware_paravirtualization.pdf.
6. THOLETI, BHANU P. Hypervisors, virtualization, and the cloud: Learn about. *IBM developerWorks*. [Online] 23. 09 2011. [Citace: 20. 1 2015.] <http://www.ibm.com/developerworks/cloud/library/cl-hypervisorcompare/cl-hypervisorcompare-pdf.pdf>.
7. Tutorial 1 - CSC469. [Online] <http://www.cdf.toronto.edu/~csc469h/fall/tutorials/t1/Tutorial1.pdf>.
8. Gartner, Inc. Gartner IT Glossary. *Gartner*. [Online] [Citace: 30. 8 2014.] <http://www.gartner.com/it-glossary/cloud-computing/>.
9. BROWN, Evelyn. Final Version of NIST Cloud Computing Definition Published. *NIST*. [Online] 25. 10 2011. [Citace: 2. 9 2014.] <http://www.nist.gov/itl/csd/cloud-102511.cfm>.
10. Mell, Peter a Grance, Timothy. The NIST Definition of Cloud. *NIST*. [Online] 9 2011. [Citace: 2. 9 2014.] <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>.

11. CHOU, David C. Rise of the Cloud Ecosystems. *Technet Blog*. [Online] Microsoft, 16. 3 2011. [Citace: 20. 1 2015.] <http://blogs.msdn.com/b/dachou/archive/2011/03/16/rise-of-the-cloud-ecosystems.aspx>.
12. VERGE Jason. DataCenterKnowledge. *AWS Adds Second European Cloud Region in Germany*. [Online] 10. 23 2014. [Citace: 1. 12 2015.] <http://www.datacenterknowledge.com/archives/2014/10/23/aws-launches-cloud-data-center-in-germany/>.
13. Microsoft. Microsoft Datacentres. [Online] [Citace: 17. 1 2015.] <http://azure.microsoft.com/en-us/regions/>.
14. Microsoft Private Cloud - A Comparative Look at Functionality, Benefits and Economics. [Online] 2012.
15. VMware. VMware vCloud Suite Datasheet. [Online] <http://www.vmware.com/files/pdf/products/vCloud/VMware-vCloud-Suite-Datasheet.pdf>.
16. Microsoft. Windows Server 2012 R2 Datasheet. *Microsoft Volume Licensing*. [Online] 2014. <http://www.microsoft.com/licensing/about-licensing/windowsserver2012-r2.aspx>.
17. Microsoft. System Center 2012 R2 Licensing Datasheet. *Volume Licensing*. [Online] 2014. <http://www.microsoft.com/licensing/about-licensing/SystemCenter2012-R2.aspx>.
18. VMware. vCloud suite pricing. *VMware*. [Online] VMware, 2014. <http://www.vmware.com/products/vcloud-suite/pricing>.
19. MALÝ, Martin. Co je a není cloud. *LUPA.CZ*. [Online] [Citace: 30. 8 2014.] <http://www.lupa.cz/clanky/co-je-a-co-neni-cloud/>.