

Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií



Diplomová práce

Rozšíření datového centra o Microsoft Azure Stack Hub

Šimon BENEŠ

© 2022 ČZU v Praze

ZADÁNÍ DIPLOMOVÉ PRÁCE

Šimon Beneš

Systémové inženýrství a informatika
Informatika

Název práce

Rozšíření datového centra o Microsoft Azure Stack Hub

Název anglicky

Data center extension with Microsoft Azure Stack Hub

Cíle práce

Diplomová práce je zaměřena na problematiku rozšíření datového centra vybrané firmy o technologii Microsoft Azure Stack Hub. Hlavním cílem této práce je analyzovat zapojení do stávající infrastruktury s ohledem na poskytované služby.

Dílní cíle práce jsou:

- představení Microsoft Azure Stack Hub
- porovnání administrace stávajících technologií s rozšířením nové technologie
- zhodnocení přínosu pro zákazníky
- porovnání ekonomické výhodnosti
- shrnutí získaných poznatků a výsledků

Metodika

Metodika řešené problematiky diplomové práce vychází ze studia a analýzy odborných informačních zdrojů. V první části diplomové práce je představena technologie Microsoft Azure Stack Hub. Dále je uvedena problematika zapojení do běžné firemní sítě. Poté se teoretická část věnuje otázce ekonomické výhodnosti.

Praktická část se zabývá zejména analýzou integrace Microsoft Azure Stack Hub do datového centra zvolené firmy a rozdíly mezi běžnou firmou a zvoleným datovým centrem. Je zde představena infrastruktura a použité technologie zvoleného prostředí. Na základě analýzy prostředí a získaných poznatků je provedeno zhodnocení rozšíření stávajícího datového centra o technologii Microsoft Azure Stack Hub nejen pro firmu, ale i pro zákazníky. Pomocí syntézy teoretické a praktické části jsou formulovány závěry diplomové práce.

Doporučený rozsah práce

50 – 60 stran

Klíčová slova

Microsoft Azure Stack Hub, hyperkonvergované řešení, Azure Stack Hub TCO analýza, hybridní scénáře, privátní cloud

Doporučené zdroje informací

<https://docs.microsoft.com>

<https://docs.microsoft.com/en-us/azure-stack/operator>

<https://docs.microsoft.com/en-us/azure-stack/operator/azure-stack-overview>

<https://docs.vmware.com/>

KLEIN, M. – ROESNER, S. Building Hybrid Clouds with Azure Stack. Birmingham: Packt Publishing Ltd., 2017. ISBN 978-1-78646-629-7

LEE, J. – LEONARDO, G. – MILGRAM, J. – RENDÓN, D. Azure Strategy and Implementation Guide : The Essential Handbook to Cloud Transformation with Azure, 4th Edition. Birmingham: Packt Publishing Ltd., 2021. ISBN 978-1-80107-797-2

SAVILL, J. Microsoft Azure Infrastructure Services for Architects : Designing Cloud Solutions. Indianapolis: John Wiley & Sons, Inc., 2019. ISBN 978-1-119-59657-8, 978-1-119-59653-0, 978-1-119-59660-8

TOROMAN, M. Azure Networking Cookbook : Practical Recipes to Manage Network Traffic in Azure, Optimize Performance, and Secure Azure Resources. Birmingham: Packt Publishing Ltd., 2019. ISBN 978-1-78980-022-7

Předběžný termín obhajoby

2021/22 LS – PEF

Vedoucí práce

doc. Ing. Jiří Vaněk, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 2. 7. 2021

doc. Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 19. 10. 2021

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 23. 02. 2022

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Rozšíření datového centra o Microsoft Azure Stack Hub" 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 30.3.2022

Poděkování

Rád bych touto cestou poděkoval vedoucímu práce doc. Ing. Jiřímu Vaňkovi, Ph.D. za vedení mé práce, manželce Martině za její trpělivost s mým studiem a celému implementačnímu týmu za odpovědi na všetečné otázky.

Rozšíření datového centra o Microsoft Azure Stack Hub

Abstrakt

Tato diplomová práce se zabývá technologií Microsoft Azure Stack Hub. V teoretické části se věnuje představení technologie, možnostmi nasazení a administrace ve firemním prostředí. Součástí je také shrnutí přínosů nejen pro zákazníka, ale i pro poskytovatele služeb. Dále jsou prozkoumány možnosti zapojení do běžného firemního prostředí a také ekonomická stránka této technologie v porovnání s provozovanými technologiemi. Praktická část se věnuje integraci do stávajícího prostředí datového centra s ohledem na poskytované služby zákazníkům. Detailně představuje proces nasazení i vnitřní architekturu a zapojení. V praktickém porovnání se zaměřuje na administraci prostředí v porovnání s technologiemi vmware. Věnuje se i získávání dat o využití pro následné vyúčtování služeb.

Klíčová slova: Microsoft Azure Stack Hub, hyperkonvergované řešení, Azure Stack Hub TCO analýza, hybridní scénáře, privátní cloud

Data center extension with Microsoft Azure Stack Hub

Abstract

This diploma thesis deals with Microsoft Azure Stack Hub technology. The theoretical part deals with the introduction of technology, deployment options and administration in the corporate environment. It also includes a summary of benefits not only for the customer, but also for service providers. Furthermore, the possibilities of involvement in a common corporate environment and also the economic side of this technology in comparison with the operated technologies are explored. The practical part deals with the integration into the existing data center environment with regard to the services provided to customers. It presents in detail the deployment process as well as the internal architecture and wiring. In practical comparison, it focuses on the administration of the environment in comparison with vmware technologies. It also deals with obtaining usage data for the subsequent billing of services.

Keywords: Microsoft Azure Stack Hub, hyperkonverged solution, Azure Stack Hub TCO analysis, hybrid scenarios, private cloud

Obsah

1 Úvod.....	9
2 Cíl práce a metodika	10
2.1 Cíl práce	10
2.2 Metodika	10
3 Teoretická východiska	11
3.1 Představení Azure Stack Hub.....	11
3.2 Možnosti nasazení	12
3.3 Možnosti správy systému	15
3.4 Administrace Azure Stack Hub.....	16
3.5 Přínos pro zákazníky	19
3.6 Ekonomická výhodnost.....	21
3.7 Zapojení do běžné firemní sítě.....	27
4 Vlastní práce	32
4.1 Integrace do prostředí datového centra	32
4.2 Proces nasazení	33
4.3 Post Deployment	41
4.4 Porovnání administrace	42
4.5 Billing & Usage.....	57
5 Výsledky a diskuse	62
6 Závěr.....	64
7 Seznam použitých zdrojů	65
8 Seznam obrázků	67
9 Seznam tabulek	68
10 Seznam použitých zkratk.....	69

1 Úvod

V posledních letech je provoz IT stále více orientován na cloudové služby. Už dávno to není jen o virtuálních serverech a infrastruktuře (IaaS), ale do popředí se začínají dostávat platformní služby (PaaS) a software jako služba (SaaS). To ale neznamená, že by se tradiční IT provozované především v datových centrech vytratilo, naopak se využije spojení s cloudem nebo dokonce s více cloudy.

Cloud lze rozdělit do tří skupin, veřejný cloud, privátní cloud a hybridní cloud. Veřejný cloud sdílí prostředky a nabízí služby veřejnosti přes internet, privátní cloud, který není sdílený a nabízí služby přes privátní interní síť obvykle hostovanou místně a hybridní cloud, který sdílí služby mezi veřejným a privátním cloudem v závislosti na jejich účelu. (1) Některé zdroje uvádějí ještě čtvrtou kategorii, kterou je komunitní cloud, ke kterému má přístup pouze určitá komunita uživatelů, ale domnívám se, že komunitní cloud je podmnožinou privátního cloudu.

Při používání cloudových služeb vznikají obavy, že data uložená v cloudu mohou být ztracena nebo, a to hlavně, zneužita. Proto vznikají různá legislativní nařízení, zejména pro státní podniky, která ukládají, jaká data smí být v jaké lokalitě uložena. Odpovědí na tyto obavy může být technologie společnosti Microsoft Azure Stack Hub, která přináší výhody privátního a hybridního cloudu a zároveň splňuje přísné legislativní požadavky. Obsah této práce je zaměřena na tuto technologii – Microsoft Azure Stack Hub.

V úvodní části práce je představena technologie Microsoft Azure Stack Hub a je porovnávána se stávajícími provozovanými technologiemi nejen z pohledu hardware, ale i z pohledu správy. Dále jsou zmíněny výhody pro zákazníky, integrace do firemního prostředí a též ekonomický pohled na toto řešení.

Prostředí datového centra se nedá považovat za běžné firemní prostředí, proto se vlastní práce zaměřuje na integraci do datového centra. Jsou zde zmíněna i různá úskalí, která byla potřeba překonat, nebo na která je si třeba dát pozor.

V závěru práce jsou shrnuta důležitá zjištění a doporučení, která vycházejí ze znalostí a zkušeností autora.

2 Cíl práce a metodika

2.1 Cíl práce

Diplomová práce je zaměřena na problematiku rozšíření datového centra vybrané firmy o technologii Microsoft Azure Stack Hub. Hlavním cílem této práce je analyzovat zapojení do stávající infrastruktury s ohledem na poskytované služby.

Dílčí cíle práce jsou:

- představení Microsoft Azure Stack Hub
- porovnání administrace stávajících technologií s rozšířením nové technologie
- zhodnocení přínosu pro zákazníky
- porovnání ekonomické výhodnosti
- shrnutí získaných poznatků a výsledků

2.2 Metodika

Metodika řešené problematiky diplomové práce vychází ze studia a analýzy odborných informačních zdrojů. V první části diplomové práce je představena technologie Microsoft Azure Stack Hub. Dále je uvedena problematika zapojení do běžné firemní sítě. Poté se teoretická část věnuje otázce ekonomické výhodnosti.

Praktická část se zabývá zejména analýzou integrace Microsoft Azure Stack Hub do datového centra zvolené firmy a rozdíly mezi běžnou firmou a zvoleným datovým centrem. Je zde představena infrastruktura a použité technologie zvoleného prostředí. Na základě analýzy prostředí a získaných poznatků je provedeno zhodnocení rozšíření stávajícího datového centra o technologii Microsoft Azure Stack nejen pro firmu, ale i pro zákazníky. Pomocí syntézy teoretické a praktické části jsou formulovány závěry diplomové práce.

3 Teoretická východiska

3.1 Představení Azure Stack Hub

Azure Stack Hub je rozšíření Azure, které poskytuje způsob, jak spouštět aplikace v místním prostředí a doručovat služby Azure v prostředí datacentra. Díky konzistentní cloudové platformě mohou organizace bez problémů provádět technologická rozhodnutí na základě obchodních požadavků, nikoli na základě obchodních rozhodnutí založených na technologických omezeních. (2) Takto představuje svůj produkt Azure Stack Hub Microsoft.

Z této definice ale nelze usoudit, zda se jedná o softwarový produkt, hardware, či něco jiného. Co to tedy je? Azure Stack Hub patří do rodiny Azure Stack, která se dělí na Azure Stack Edge, Azure Stack HCI a Azure Stack Hub.

Azure Stack Edge, dříve Azure Data Box, je účelový hardware, který je propojený s cloudem Microsoft Azure a umožňuje spouštět úlohy v prostředí zákazníka. Správa tohoto zařízení probíhá přímo z cloudu. Využívá se především tam, kde je potřeba nízké latence a potřeba rychlé odezvy, jako jsou například IoT zařízení, nebo hardwarová akcelerace grafických čipů.

Azure Stack HCI je druhý produkt z rodiny Azure Stack. Jedná se o hyperkonvergované řešení určené pro škálovatelnou virtualizaci s využitím hybridního cloudu. Další použití je pro virtualizované desktopy, vysoce výkonné SQL servery, nebo použití Azure Kubernetes služeb.

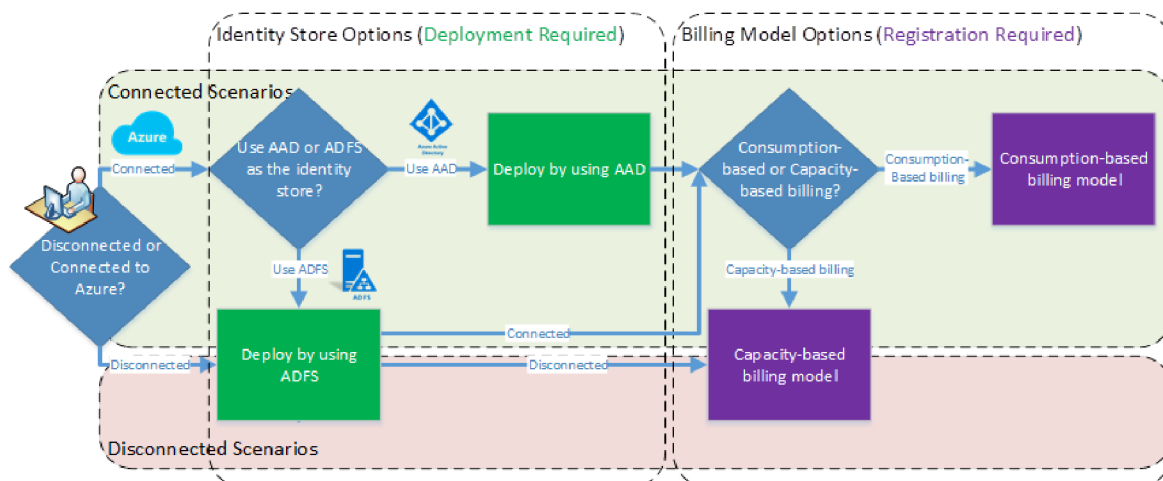
Azure Stack Hub, dříve jen Azure Stack, je posledním produktem z rodiny Azure Stack. Jedná se o řešení kombinující hyperkonvergovaný hardware společně se softwarem pro správu od společnosti Microsoft. Aby byla zajištěna správná funkce softwaru, tak nelze použít libovolný hardware, ale pouze certifikovaný. V současné době mají certifikaci tyto partneři Microsoftu: Cisco, Hewlett Packard Enterprise, Lenovo, Dell EMC a Avanade. Stěžejní funkcí je ale poskytování Azure služeb v on-premise prostředí zákazníka.

Celá rodina Azure Stack je úzce svázána s veřejným cloudem Microsoft Azure. Cloudová platforma Azure zahrnuje více než 200 produktů a služeb navržených tak, aby pomáhaly s realizací nových řešení pro aktuální úlohy dneška a s utvářením budoucnosti. (3) Najdeme zde služby z různých kategorií, jako například identita, analýza, IoT, zabezpečení,

databáze, kontejnery a další. A část těchto služeb můžeme mít i v lokálním prostředí datového centra za pomoci nasazení Azure Stack Hub.

3.2 Možnosti nasazení

Řešení Azure Stack Hub lze provozovat ve dvou modelech připojení systému k internetu a ke cloudové službě Azure. Jedním je connected model a druhým disconnected model. Tento model po nasazení nelze změnit, je proto potřeba se vhodně rozhodnout, který model zvolit. Pro rozhodování je klíčové si vhodně zvolit poskytovatele identit (AAD/ADFS) a licenční model. Možné rozhodovací cesty, který model zvolit, ukazuje Obrázek 1: Connected/disconnected cesty.



Obrázek 1: Connected/disconnected cesty

V režimu online/connected se jedná o režim, kdy lokální zařízení plně komunikuje s veřejným cloudem Microsoft Azure a díky tomu může fungovat v hybridním režimu a využívat cloudové ověřování včetně multifaktorového ověřování. Zde je možné použít zdroj identit Azure Active Directory (AAD), nebo Active Directory Federation Services (ADFS). Tento connected model je výchozí volbou, protože nejvíce využívá výhod hybridních scénářů v prostředí Azure a Azure Stack Hub. Licenční model je možné v connected režimu zvolit mezi pay-as-you-use, tedy modelem, kdy se platí pouze za využití služby, nebo capacity-based, kdy se jednorázově zaplatí za kapacitu celého Azure Stack Hub.

Volba úložiště identity pro správu nemá žádný vliv na nasazované virtuální počítače v rámci poskytované služby uvnitř Azure Stack Hub, u kterých je možné zvolit zdroj identity samostatně. Lze mít jeden virtuální počítač, který bude používat identitu pracovní skupiny, druhý se zdrojem identit v Active Directory a třetí se zdrojem identit v Azure Active Directory. Tato volba nijak nesouvisí s výběrem identity pro samotný Azure Stack Hub.

Licenční modely, či billing – modely fakturace – jsou platba za využívání služeb nebo platba za kapacitu. Při modelu využívání služeb se poplatky za využívání účtují v rámci předplatného Azure. Platby jsou pouze za použité zdroje Azure Stack Hub. Fakturace na základě kapacity je jednorázová platba vázaná na počet jader v Azure Stack Hub a licenčně pokrývá všechny zdroje bez ohledu, zda se používají. Kapacitní model fakturace vyžaduje Enterprise Agreement (EA), aby mohla být nastavena dostupnost položek v Marketplace.

Druhý režim disconnected je odpojený režim, kde není potřeba internetového připojení. Použití může být vhodné například na zaoceánských lodích nebo v dolech, kde je připojení k internetu často nemožné, nebo v prostředích se zvýšeným důrazem na oddělení sítí z bezpečnostních důvodů. V tomto režimu je omezení pouze na ADFS zdroj identit a pouze licenční model na základě kapacity. Protože vícetenantní prostředí vyžaduje ke své funkcionalitě použití Azure Active Directory (AAD), tak není možné v tomto modelu využívat více tenantů.

Důvody pro zvolení disconnected režimu mohou být následující:

- bezpečnostní nebo jiná omezení, která ukládají nepřipojení k internetu,
- blokování posílání dat do Azure, včetně dat o využití,
- použití Azure Stack Hub čistě jako privátní cloud nasazený v prostředí podnikového intranetu, které nemá hybridní scénáře. (4)

Disconnected režim, který se v některých případech též označuje jako submarine scenario, má jisté dopady do použití funkcí Azure Stack Hub. Tyto dopady jsou buď omezení některých funkcí, nebo jejich úplná nedostupnost.

Nedostupné služby jsou:

- odkazy na online dokumentaci, rychlý start a další, které používají internetové odkazy z portálu Azure Stack Hub,
- upozornění na nápravu (remediation) a zmírnění (mitigation), které používají internetové odkazy z portálu Azure Stack Hub,
- použití federačních účtů Azure AD (AAD) ke správě nasazení Azure Stack Hub,
- telemetrická data pro Azure Stack Hub a všechny balíčky třetích stran, které jsou závislé na telemetrických datech,
- služby seznamu odvolaných certifikátů (CRL) a protokolu OSCP (Online Certificate Status Protocol).

Služby s omezenou funkcí jsou:

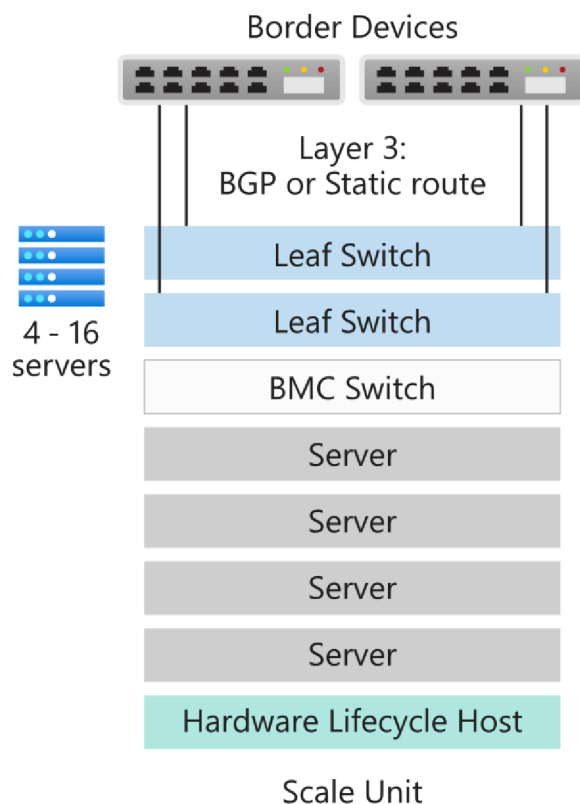
- nasazení virtuálních počítačů s rozšířením DSC (Desire State Configuration) pro konfiguraci virtuálního počítače – DSC rozšíření hledá nejnovější WMF (Windows Management Framework) na internetu,
- nasazení virtuálních počítačů s rozšířením Docker pro spouštění příkazů – Docker kontroluje nejnovější verze na internetu,
- Marketplace – v disconnected režimu nelze stahovat položky Marketplace v portálu Azure Stack Hub, lze však položky stahovat pomocí nástroje Marketplace syndication tool na zařízení s internetovou konektivitou a následně přenést do prostředí Azure Stack Hub,
- služby App Service jako je WebApps vyžadují připojení k internetu pro aktualizaci obsahu,
- Rozhraní příkazového řádku (Command Line Interface – CLI) má omezenou funkčnost pro autentizaci a zřizování objektů služeb,
- funkce Cloud Discovery z nástroje Visual Studio může objevit rozdílné cloudy, nebo nemusí fungovat vůbec,
- ověřování ADFS podporují pouze Visual Studio Enterprise a Visual Studio Code,
- běžné použití Key Vault je mít za běhu tajné kódy pro aplikaci, v Azure AD mohou běžní uživatelé (bez administrátorských práv) přidávat service principals, v ADFS musejí mít administrátorská práva.

3.3 Možnosti správy systému

Řešení je možné pořídit buď jako systém, který si vlastník spravuje sám, nebo jako spravovanou službu. V první variantě si vlastník pořídí hardware od dodavatele, řídí si správu i provoz a se žádostmi na podporu se obrací na Microsoft. Většinou je pak zařízení v místním prostředí. Ve variantě spravované služby se nekupuje hardware, nespravuje se místními administrátory a obvykle je zařízení u poskytovatele. Se žádostmi o podporu se uživatel obrací na poskytovatele. Není-li výlučně uvedeno, jedná se v celé práci o connected režim s vlastní správou a provozem.

Celé řešení se skládá ze 4 až 16 serverů, dvou leaf switchů, management serveru a management switchte. Konfigurace až do 16 serverů je umístěna v rámci jedné rackové skříně a je označována jako scale unit. Ta má i svůj vlastní region. Je-li potřeba rozšířit kapacitu nad tuto hranici, pak hovoříme o další scale unit, která má stejné zapojení a funkcionalitu jako uvedené řešení. V současné době není možné provozovat dvě a více scale unit z prostředí jednoho portálu, ale v budoucnu by se tato možnost měla objevit. Portál tak má v možnosti výběru vždy jen jeden region, který určuje danou scale unitu.

V řešení od společnosti Cisco přebírá funkci management serveru Fabric Interconnect, který je v řešení zastoupen dvakrát z důvodu vysoké dostupnosti. Celé řešení od společnosti Cisco neobsahuje SPoF (Single Point of Failure), přestože výpadek management serveru neovlivní provoz jednotlivých zdrojů a nebylo by nutné mít tento server redundantně. Management server se v dokumentaci označuje jako Hardware Lifecycle Host. Škálování v rámci scale unit je možné od 4 serverů s přírůstkem po jednom. Někteří vendori mají v nabídce pouze vlastní možnosti škálování – 4, 8, 12 a 16 serverů. Na Obrázek 2: Příklad scale unity je zachycena minimální konfigurace se čtyřmi servery.



Obrázek 2: Příklad scale unity

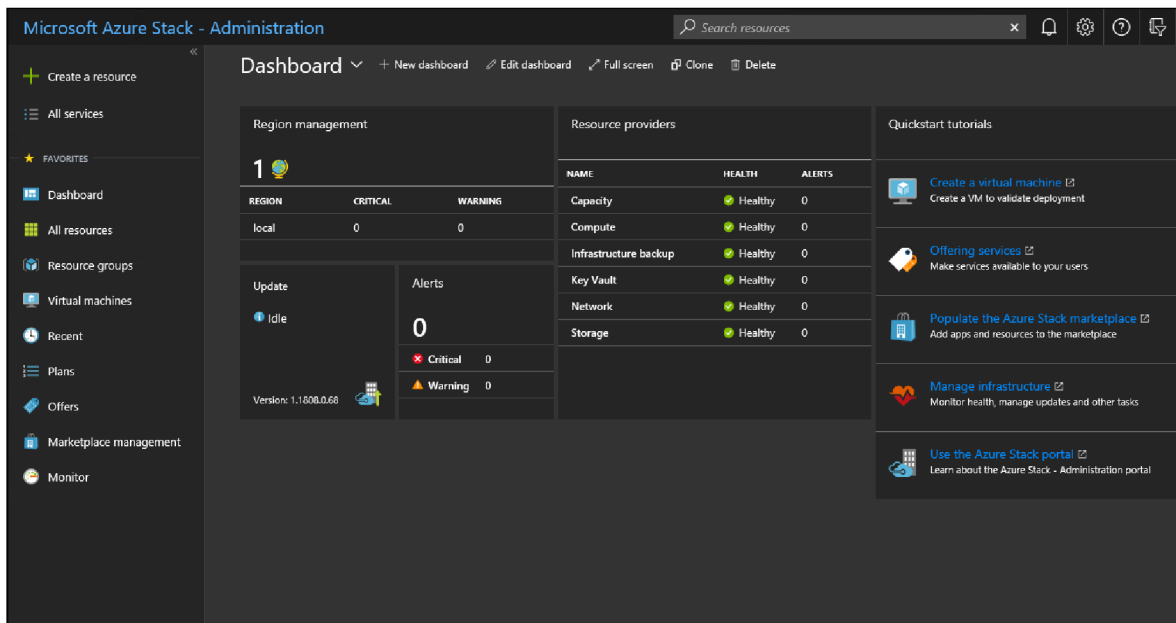
3.4 Administrace Azure Stack Hub

Administrace Azure Stack Hub se provádí z prohlížeče přes webové rozhraní. Tato rozhraní jsou dvě – portál a admin portál. To je dané tím, že Azure Stack Hub je multitenantní systém. Lze tedy provozovat několik naprosto oddělených prostředí, která se vzájemně neovlivňují.

V admin portálu se spravují všechny konfigurační položky, které jsou společné pro všechny tenanty. Tato administrace je zákazníkům skryta a je určena pro administrátory poskytovatele služeb Azure Stack Hub. Lze zde provádět například tyto akce:

- registrace Azure Stack Hub s Azure
- naplnění Marketplace
- vytváření plánů, nabídek a předplatných pro jednotlivé tenanty
- spravovat aktualizace

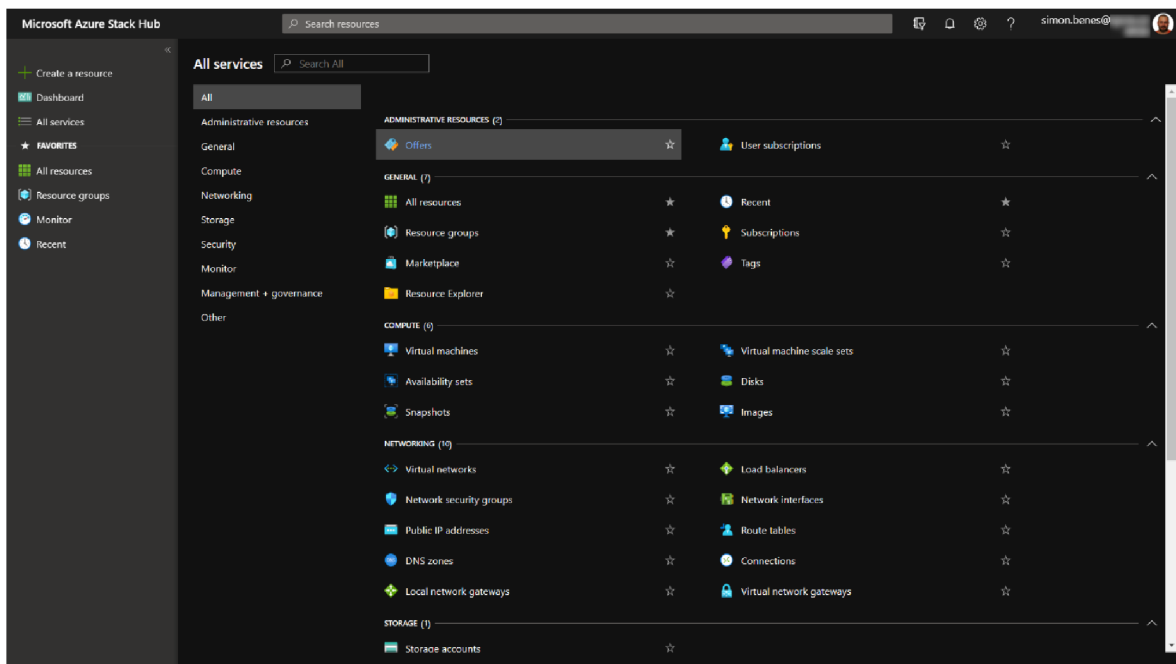
Pohled na admin portál je zobrazen na Obrázek 3: Admin portál.



Obrázek 3: Admin portál

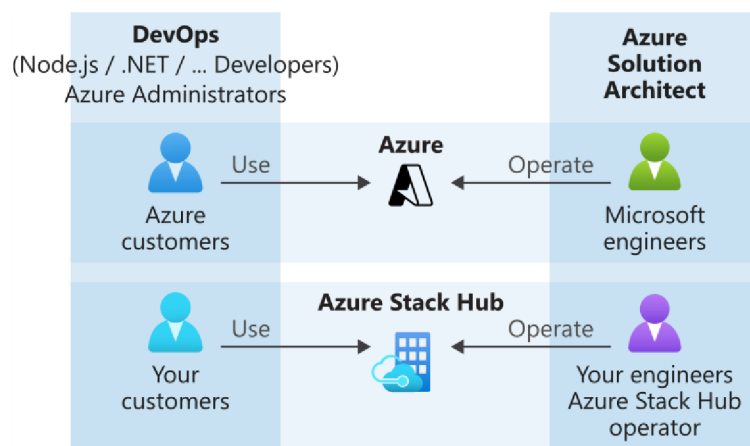
Druhým portálem je uživatelský portál. Je určen pro samotné využívání zdrojů ať uživateli podniku nebo jeho zákazníky. Zde je možné si vytvořit a použít zdroje z Marketplace, které správce umožnil použít – např. virtuální servery, virtuální sítě, databázi a další. Portál je určen pro administrátory zákazníka využívající služeb Azure Stack Hub. Samostatné prostředí je ohraničené subskripcí. Použité zdroje mohou být stejné v několika subskripcích, ale vzájemně jsou odděleny. Subskripce je vždy pro jednoho zákazníka, ale jeden zákazník může mít více subskripcí. Může tak provozovat nesouvisející projekty každý ve vlastním prostředí.

Portál je podobný portálu veřejného cloudu Azure. Ovládání je shodné, jen v Azure Stack Hub nenajdeme všechny služby, je zde pouze podмноžina služeb, které lze použít v místním prostředí. Na Obrázek 4: Portál Azure Stack Hub je zobrazen uživatelský portál.



Obrázek 4: Portál Azure Stack Hub

Jak již bylo zmíněno, admin portál určuje možnosti využití služeb a portál nastavuje samotné využívání povolených služeb. V porovnání s veřejným cloudem Azure můžeme konstatovat, že portál Azure Stack Hub je ekvivalentem portálu Azure, zatímco admin portál nemá v Azure veřejně dostupný ekvivalent. O admin portál v Azure se stará tým Microsoft inženýrů a o admin portál Azure Stack Hub se stará tým inženýrů poskytovatele. Rozdíl je zachycen na Obrázek 5: Job role.



Obrázek 5: Job role

3.5 Přínos pro zákazníky

Azure Stack Hub je rozšířením Azure, které přináší flexibilitu a inovace cloud computingu do místního prostředí. (5) Azure Stack Hub používá stejné technologie jako Azure, které zahrnují základní součásti infrastruktury jako služby (IaaS), software jako služby (SaaS) a platformních služeb (PaaS). Mezi tyto možnosti patří:

- virtuální počítače Azure pro Windows a Linux
- Azure Web Apps a Azure Functions
- Azure Key Vault
- Azure Resource Manager
- Azure Marketplace
- kontejnery
- nástroje pro správu (plány, nabídky, RBAC, atd.)

Zákazníci si mohou pohodlně z prostředí portálu sami vytvořit službu, kterou zrovna potřebují, nebo ji zrušit v okamžiku, kdy ji nepotřebují. Poskytování těchto služeb je na současných technologiích používaných ve vybrané firmě nereálné. Současné poskytování služeb je na základě požadavků zákazníka, kterým tým administrátorů vytvoří a spravuje jejich zákaznické prostředí. Jakákoliv změna v poskytované službě znamená změnový požadavek, který trvá nějakou dobu, proto je velkým přínosem zejména agilita v poskytování služeb.

Azure Stack Hub poskytuje zákazníkům několik možností. Klasická dodávka služby, která funguje v současném prostředí, kdy na základě požadavků vytvoří administrátoři poskytovatele celé prostředí a spravují je. Realizace je tedy plně ve správě poskytovatele a pro zákazníka nemá žádnou přidanou hodnotu, nicméně přínosem pro poskytovatele je rychlejší nasazení některých služeb.

Někteří zákazníci mají své administrátory, kteří by si rádi alespoň některé projekty řídili a spravovali sami. To současné technologie sledované firmy neumožňují, ale právě technologie Azure Stack Hub umožní poskytovat i tyto služby, protože je od základu navržen jako multitenantní prostředí. Zákazník dostane své vlastní prostředí, které si ovládá dle svého

uvážení. Díky virtualizované síti si může zvolit síťové prostředí dle svých potřeb a neovlivní provoz v jiném prostředí.

Další možností poskytnutí služby je kombinace předešlých dvou. Zákazník má svoje prostředí a konfiguruje si své prostředí sám, ale zároveň přiřadí práva poskytovateli, aby za něj prováděl složitější úlohy. To může být vhodné pro zákazníky, kteří si sice chtějí prostředí spravovat sami, ale ještě nemají dostatečné znalosti.

Komunikace mimo prostředí Azure Stack Hub probíhají přes veřejné adresy. Volné veřejné adresy jsou umístěny v poolu veřejných adres a při použití jsou z poolu vyjmuty a přiřazeny konkrétnímu prostředí. Pokud už zdroj není použit, tak je veřejná adresa vrácena zpět do poolu a může ji použít jiný zákazník. Přiřazení těchto adres probíhá dynamicky a nelze tento proces ovlivnit (nelze si nechat přiřadit konkrétní adresu).

Jeden z požadavků zákazníka může být propojení s jeho lokálním prostředím, nebo s prostředím v cloudu. I tento požadavek lze technologií Azure Stack Hub vyřešit, a to pomocí Virtual Network Gateway. Jedná se VPN koncentrátor, kterému je přiřazena veřejná adresa (opět z poolu veřejných adres) a pomocí Local Network Gateway, která definuje druhou stranu tunelu, a Connection se spojí oba konce do VPN tunelu. Při propojení je nutné mít na paměti síťovou adresaci, aby nedošlo ke kolizi adresních rozsahů.

Přínosem pro zákazníka je také možnost nasazovat zdroje pomocí ARM a Bicep šablon. Tím je možné mít infrastrukturu popsanou jako kód. Takto připravená infrastruktura slouží zároveň jako záloha pro případ havárie a zároveň, díky relativně čitelnému kódu, jako dokumentace.

Protože Azure Stack Hub není jen virtualizace, tak se zákazník nemusí omezovat pouze na virtuální servery, ale je možné využít podмноžinu PaaS služeb Azure, jako například velmi oblíbený kubernetes cluster, nebo App Service. Použití služeb urychlí nasazení, protože není nutné nasazovat virtuální servery a na nich ručně nasazovat potřebné aplikace pro běh služby.

Tradiční poskytování IT služeb je ve sledované firmě poskytováno formou měsíčního paušálu, většinou v dlouhodobějším období. V tomto modelu není prostor pro jakoukoliv změnu, není možné vytvořit o jeden server víc, nebo naopak méně. Vzhledem k možnostem účtování Azure Stack Hub je toto jeho další výhodou. Zákazník může využívat model pay-as-you-go, tedy platba pouze za využití služby. To může být vhodné například při testování,

kdy je možné v průběhu testování měnit velikosti zdrojů, nebo při požadavku na zvýšený výkon v určitém čase (např. při měsíční uzávěrce).

3.6 Ekonomická výhodnost

Ekonomické porovnání bylo provedeno na platformách vmware a Azure Stack Hub. Zčásti lze říct, že tyto varianty nelze porovnat, protože v případě vmware nemáme k dispozici PaaS služby. Proto je porovnání provedeno na společných možnostech, pro jednoduchost jen virtuální servery. Hardware je pro obě varianty stejný, proto náklady na pořízení nebudeme uvažovat. Také činnosti, které budou nákladově stejné v obou variantách, nejsou uvažovány. Nejedná se tak o ekonomickou výhodnost pomocí TCO.

Porovnání je provedeno na konfiguraci s osmi fyzickými servery, kde každý má dva procesory, každý procesor s dvaceti jádry, 1,5 TB operační paměti a 92 TB raw úložiště. Pro účely licencování jde celkem o 16 procesorů s 320 fyzickými jádry. Velikost operační paměti je irelevantní, protože nevstupuje do licenčního modelu.

Virtualizace se využívá hlavně pro možnost využít přidělené a nevyužité zdroje virtuálního serveru jinému. V případě procesorů se běžně používá přetěžování až 1:5 (fyzické jádro:virtuální jádro), v níže uvedeném porovnání je tento poměr po odečtení režie zvolen 1:3. Přetížení lze využít i u fyzické/virtuální paměti, ale zde je již režie na tuto změnu tak vysoká, že se běžně nepoužívá. Naopak u úložiště to funguje obráceně. Aby se zachovala vysoká dostupnost, tak jsou data uložena interně na třech místech. To znamená, že využitelná kapacita úložiště je třikrát menší, než je součet kapacit jednotlivých disků.

S přihlédnutím k výše uvedenému a po odečtení zdrojů pro režii budeme v porovnání uvažovat 16 procesorů, 320 fyzických jader, 960 virtuálních procesorů a 163 TB úložiště. Pro eliminaci rozdílu, kdy vmware má některé vstupní náklady jednorázové a Azure Stack Hub se může licencovat za dobu používání, je uvažována doba provozu pět let. Pro přesnější porovnání z hlediska využívání jsou zvoleny varianty 10/50/90% všech zdrojů, tedy 96 vCPU a 16,3 TB úložiště pro 10%, 480 vCPU a 81,5 TB úložiště pro 50% a 864 vCPU a 146,7 TB úložiště pro 90% zdrojů.

Platforma Azure Stack Hub je zdarma (pořizovací cena softwaru je nulová), platby jsou účtovány podle licenčního modelu. V kapacitním modelu jsou platby v ročních obdobích za fyzická jádra. V tomto modelu se prodávají ve dvou balíčcích IaaS a App Service. Prvním

balíčkem je pokryta celá infrastruktura bez aplikačních služeb a platba je ve výši \$144 za fyzické jádro a rok. Druhý balíček má navíc aplikační služby a platba je ve výši \$400 za fyzické jádro a rok. Doplnkovým balíčkem je Event Hubs, kde je cena stanovena na \$2400 za jádro a rok s minimálním počtem 10 jader. Přehled je v Tabulka 1: Kapacitní model licencování. (6)

Tabulka 1: Kapacitní model licencování

balíček	core	roků	cena / core / rok	cena / 5let	kurz	cena celkem Kč
IaaS package	320	5	\$ 144	\$ 230 400	21,615	4 980 096 Kč
App Service	320	5	\$ 400	\$ 640 000	21,615	13 833 600 Kč
Event Hub	10	5	\$2 400	\$ 120 000	21,615	2 593 800 Kč

Licenční model pay-as-you-use je pouze za použité zdroje. Mezi tyto zpoplatněné zdroje se řadí vCPU (virtuální procesor), úložiště a licence Windows Server za každé vCPU. U licence Windows Server můžeme zvolit i variantu nákupu licencí pro všechny procesory bez ohledu na jejich využití, tak jak se běžně licencují servery v datacentrech. Dále jsou zpoplatněny další služby, které v našem porovnání neuvažujeme, protože je nelze provozovat na platformě vmware. Náklady za využití vCPU jsou kalkulovány v Tabulka 2: Cena za využití vCPU.

Tabulka 2: Cena za využití vCPU

využití	# vCPU	měsíců	cena vCPU /měsíc	cena vCPU / 5let	kurz	cena celkem Kč
10%	96	60	\$ 6	\$ 34 560	21,615	747 014 Kč
50%	480	60	\$ 6	\$ 172 800	21,615	3 735 072 Kč
90%	864	60	\$ 6	\$ 311 040	21,615	6 723 130 Kč

Náklady za využití úložiště jsou v Tabulka 3: Cena za využití vHDD.

Tabulka 3: Cena za využití vHDD

využití	# vHDD	měsíců	cena vHDD /měsíc	cena vHDD / 5 let	kurz	cena celkem Kč
10%	16,3	60	\$ 10	\$ 10 015	21,615	216 468 Kč
50%	81,5	60	\$ 10	\$ 50 074	21,615	1 082 341 Kč
90%	146,7	60	\$ 10	\$ 90 132	21,615	1 948 214 Kč

Celková cena za využití Azure Stack Hub je součtem ceny za vCPU a vHDD a je uvedena v Tabulka 4: Cena za využití Azure Stack Hub. Náklady na provoz jsou lineární s používanými zdroji.

Tabulka 4: Cena za využití Azure Stack Hub

využití	cena vCPU	cena vHDD	cena celkem Kč
10%	747 014 Kč	216 468 Kč	963 483 Kč
50%	3 735 072 Kč	1 082 341 Kč	4 817 413 Kč
90%	6 723 130 Kč	1 948 214 Kč	8 671 343 Kč

Ve sledované firmě probíhá plánování kapacit pro nákup hardwaru tak, že existuje nějaké aktuální využití zdrojů, ke kterému se připočte plánované využití zdrojů z plánovaných projektů a rezerva pro budoucí projekty, které zatím plánované nejsou. To znamená, že při nákupu hardwaru je využita přibližně polovina kapacity celého nově pořízeného hardware. Maximální využitá kapacita zdrojů po pěti letech životnosti se pohybuje kolem 90%, proto je v předchozích tabulkách uvedena tato hodnota.

Produkty vmware jsou licencovány na fyzický procesor. Licence je složena ze dvou částí. První je licence na samotný produkt, která je jednorázová a platí neomezenou dobu. Druhá část je licence za podporu, která má roční poplatek. Jedná se o produkty a licence na vmware vSphere – virtualizace výpočetního výkonu, vmware vSAN – virtualizace diskového úložiště a vmware NSX – virtualizace sítě. Posledním produktem je vmware vCenter, který slouží jako společný orchestrátor a je jako jediný licencovaný na instanci. V případě používání Windows Server jsou potřeba ještě licence na tento operační systém. Žádné další poplatky nejsou na této platformě uplatněny.

Licence vmware produktů (7) ukazuje Tabulka 5: Cena za využití vmware. Pro přepočtení ceny z amerického dolaru na české koruny byl použit kurz 21,615 (1.2.2022) (8). Náklady na licencování vmware za pětileté období jsou 15 541 509 Kč bez ohledu na využívané zdroje.

Tabulka 5: Cena za využití vmware

Produkt Vmware	cena/licence	# licencí	celkem	kurz	celkem Kč	celkem za 5 let
vCenter Server	\$ 6 175	1	\$ 6 175	21,615	133 473	133 473 Kč
Support vCenter Server	\$ 1 544	1	\$ 1 544	21,615	33 374	166 868 Kč
vSphere Enterprise Plus	\$ 3 595	16	\$ 57 520	21,615	1 243 295	1 243 295 Kč
Production Support vSphere	\$ 899	16	\$ 14 384	21,615	310 910	1 554 551 Kč
vSAN Enterprise Plus	\$ 7 495	16	\$119 920	21,615	2 592 071	2 592 071 Kč
Support for vSAN	\$ 1 874	16	\$ 29 984	21,615	648 104	3 240 521 Kč
NSX Data Center Enterprise Plus	\$ 8 495	16	\$135 920	21,615	2 937 911	2 937 911 Kč
Support for NSX	\$ 2 124	16	\$ 33 984	21,615	734 564	3 672 821 Kč
Celkem						15 541 509 Kč

Porovnání technologií v provozování virtuálních serverů shrnuje Tabulka 6: Porovnání provozu virtuálních serverů. Do tohoto přehledu jsou zahrnuty oba licenční modely včetně obou variant kapacitního modelu. Balíček IaaS je z pohledu porovnání funkcionalit blíže platformě vmware, protože ani ta neobsahuje možnost platformních služeb. V tomto porovnání vychází lépe Azure Stack Hub ve všech jeho licenčních možnostech. Pro detailnější porovnání jsou uvedeny i procentuální poměry se základy jednotlivých variant.

Tabulka 6: Porovnání provozu virtuálních serverů

AzS IaaS	vs.	Azure Stack Hub	vs.	AzS App Service	vs.	Vmware
4 980 096 Kč		8 671 343 Kč		13 833 600 Kč		15 541 509 Kč
100%	<	174%	<	278%	<	312%
57%		100%		160%		179%
36%		63%		100%		112%
32%		56%		89%		100%

Výše uvedené platí pro provoz virtuálních serverů, které nevyžadují licenci operačního systému. Pro používání virtuálních serverů s operačním systémem Windows Server je nutné mít ještě licenci na tento operační systém. Na platformě vmware je pouze varianta pořízení licence na základě počtu fyzických jader. Na platformě Azure Stack Hub jsou možnosti dvě. První možnost je stejná jako u platformy vmware, tedy pořízení licence na základě počtu fyzických jader a druhá varianta platby za využití, kde se platí měsíční poplatek za běžící server.

Při porovnání licencí Windows Server je virtualizace vmware licencována na 320 jádrech. Jedna licence pokrývá dvě jádra, proto je potřeba 160 licencí na operační systém. Dále je potřeba licence software assurance, která v sobě obsahuje License mobility nutné pro provoz ve virtualizovaném prostředí. Zároveň obsahuje New Versions Rights, která zajišťuje možnost použití nových verzí. (9) Použitím tohoto modelu jsou pokryty všechny instance virtuálních serverů Windows Server bez ohledu na jejich počet.

Licencování pro Windows Server je na platformě Azure Stack Hub možné využít ve dvou modelech. Prvním je, stejně jako na platformě vmware, licencování na základě fyzických jader procesoru. Druhým modelem licencování je nákup licence zároveň s běžícím virtuálním serverem, kdy je měsíční poplatek účtován zároveň s provozem virtuálního serveru. Platba je pouze za dobu běhu tohoto serveru. V případě vypnutí nebo smazání serveru se již dále neúčtuje. To může být výhodné pro testovací prostředí, nebo pro využívání jen v některých částech roku. Tyto dva modely nelze kombinovat.

Přehled licenčních nákladů na první model, tedy licencování na základě počtu jader, je v Tabulka 7: Licence Windows Server per core. (10) (11)

Tabulka 7: Licence Windows Server per core

Produkt Microsoft	cena/licence/rok	# licencí	celkem	kurz	celkem Kč	celkem za 5 let
Windows Server Datacenter	\$ 758	160	\$121 280	21,615	2 621 467	2 621 467 Kč
Software Assurance	\$ 190	160	\$ 30 400	21,615	657 096	3 285 480 Kč
Celkem						5 906 947 Kč

V Tabulka 8: Licence Windows server – pay-as-you-go jsou náklady na licencování Windows Serveru podle druhého modelu. Výpočty uvažují virtuální servery, které běží 24 hodin denně po dobu pěti let.

Tabulka 8: Licence Windows server – pay-as-you-go

využití	# vCPU	měsíců	cena vCPU /měsíc	cena vCPU / 5let	kurz	cena celkem Kč
10%	96	60	\$ 28	\$ 161 280	21,615	3 486 067 Kč
50%	480	60	\$ 28	\$ 806 400	21,615	17 430 336 Kč
90%	864	60	\$ 28	\$1 451 520	21,615	31 374 605 Kč

Už na první pohled je vidět, že i pouhé využití 20% výpočetního výkonu má větší náklady než licencování prvním modelem. Přesná hranice, kde se výhodnost jednotlivých modelů licencování mění, je 163 vCPU, resp. 17% celkových zdrojů s Windows Server operačním systémem běžících 5 let:

$$5\,906\,947 / 21,615 / 60 / 28 \approx 163$$

(cena licencí per core / kurz / měsíců / cena za vCPU v \$)

Pro zvolení správného licencování Windows Server operačního systému velmi záleží na počtu jader běžících serverů. Pokud uvažujeme servery, které jsou v provozu 24 hodin denně po dobu pěti let, tak hranice výhodnosti je na 163 virtuálních procesorech. Pod touto hranicí je výhodnější licencování pay-as-you-use, nad touto hranicí to je licencování na základě počtu jader. Shrnutí je v Tabulka 9: Provnání nákladů na licencování Windows

Tabulka 9: Provnání nákladů na licencování Windows

pay-as-you-use		vs.	per core
10%	3 486 067 Kč	<	5 906 947 Kč
50%	17 430 336 Kč	>	5 906 947 Kč
90%	31 374 605 Kč		5 906 947 Kč

3.7 Zapojení do běžné firemní sítě

Proces integrace Azure Stack Hub do firemní sítě se dá definovat posloupností následujících kroků:

- plánování
- objednávka
- kroky před nasazením
- doručení hardware
- nasazení v lokalitě
- kroky po nasazení

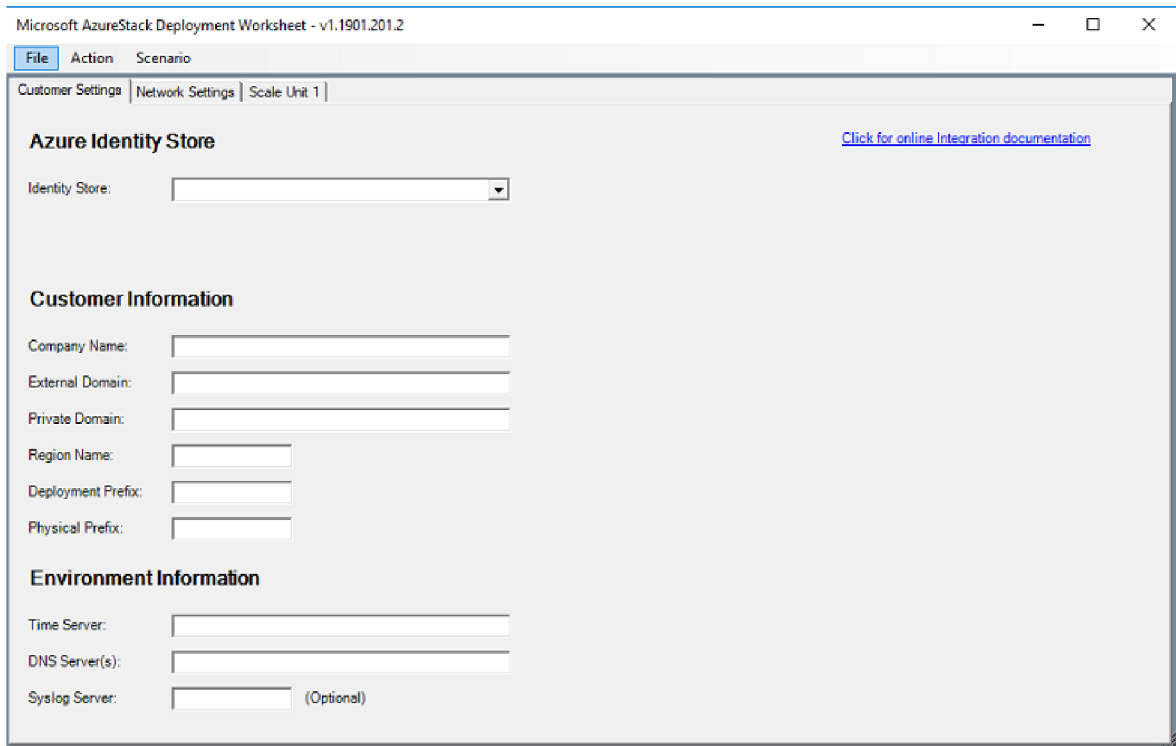
Krok plánování je velice důležitým krokem, protože nesprávný návrh kapacity může způsobit nedostatečné zdroje, nebo naopak příliš mnoho volných kapacit. V tomto kroku je potřeba mít na paměti, že pořízený hardware se nedá jednoduše rozšířit. Nelze přidat operační paměť, nelze přidat diskovou kapacitu do jednotlivých serverů, ale lze přidat celý nový server, pouze musí být ve stejné konfiguraci, jako jsou stávající servery. Počet serverů je možné rozšiřovat až do naplnění celé scale unity. Pokud se Azure Stack Hub pořizuje pro předem známé požadavky, tak je situace jednodušší, ale vždy je potřeba počítat i s určitou rezervou.

Azure Stack Hub se objednává u partnera, který má požadované zkušenosti a potřebné techniky, většinou certifikované výrobcem. Objednávka se příliš neliší od objednávky na obyčejný hardware. Hardware pro Azure Stack Hub musí být certifikovaný Microsoftem, proto jsou možnosti výběru užší.

Před samotnou dodávkou hardwaru je nutné si ujasnit a sepsat rozhodnutí o:

- modelu připojení a zprostředkovatele identity
- licenčním modelu
- integraci sítě
- integraci brány firewall
- požadavcích na certifikáty

Microsoft pro tyto účely připravil List nasazení Azure Stack Hub, což je Windows Forms aplikace, která agreguje všechny potřebné informace o nasazení a rozhodnutí na jednom místě. (12) Na Obrázek 6: List nasazení je zachycen náhled na aplikaci List nasazení.

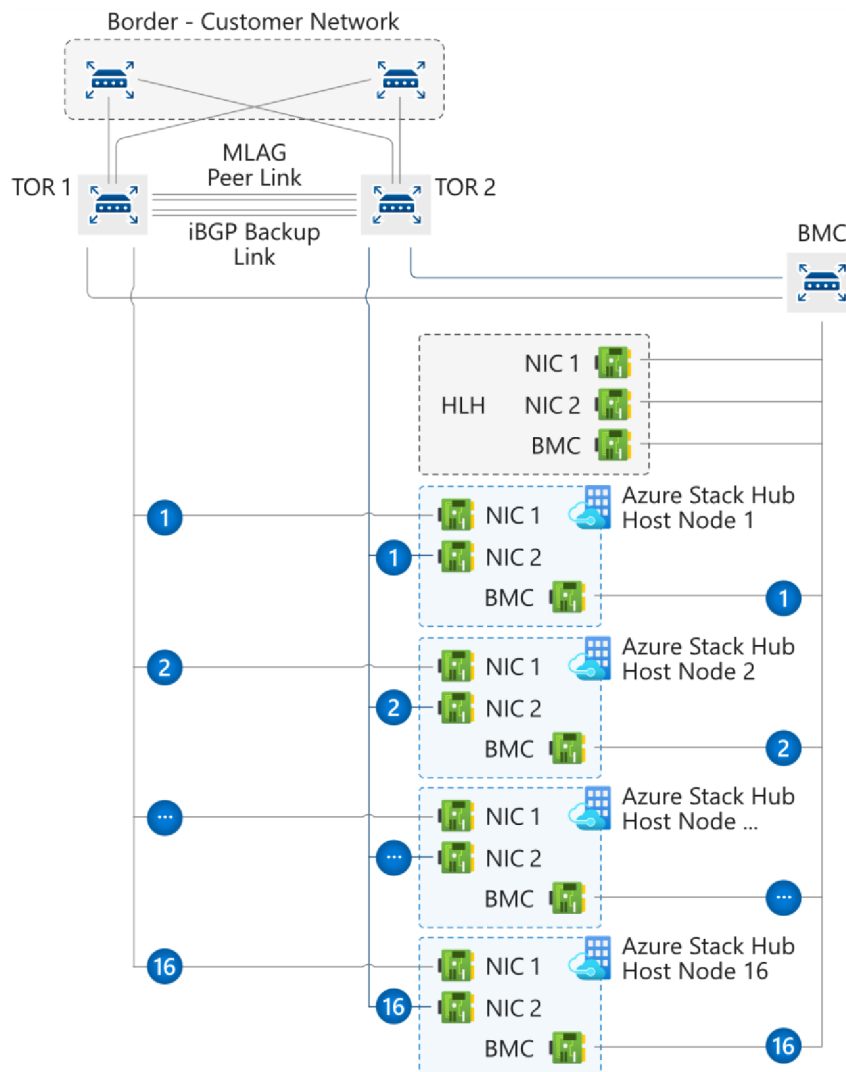


The screenshot shows a window titled "Microsoft AzureStack Deployment Worksheet - v1.1901.2012". The application has a menu bar with "File", "Action", and "Scenario". Below the menu bar are tabs for "Customer Settings", "Network Settings", and "Scale Unit 1". The main content area is divided into three sections:

- Azure Identity Store**: Includes a dropdown menu for "Identity Store:" and a link for "Click for online Integration documentation".
- Customer Information**: Includes input fields for "Company Name:", "External Domain:", "Private Domain:", "Region Name:", "Deployment Prefix:", and "Physical Prefix:".
- Environment Information**: Includes input fields for "Time Server:", "DNS Server(s):", and "Syslog Server:" (with an "(Optional)" label).

Obrázek 6: List nasazení

Integrace sítě je velmi důležitým krokem pro nasazení, provoz a správu. Zapojení v rámci rackové skříně Azure Stack Hub je zachyceno na Obrázek 7: Síťové zapojení. Zapojení je ve vysoké dostupnosti, tedy každý server je zapojen do dvou Top of Rack (TOR) switchů. Aby tato vysoká dostupnost byla zachována, tak je z každého TOR switche propojení do dvou border zařízení zákazníka. Border zařízení je nejbližší switch nebo router zákazníka. (13)



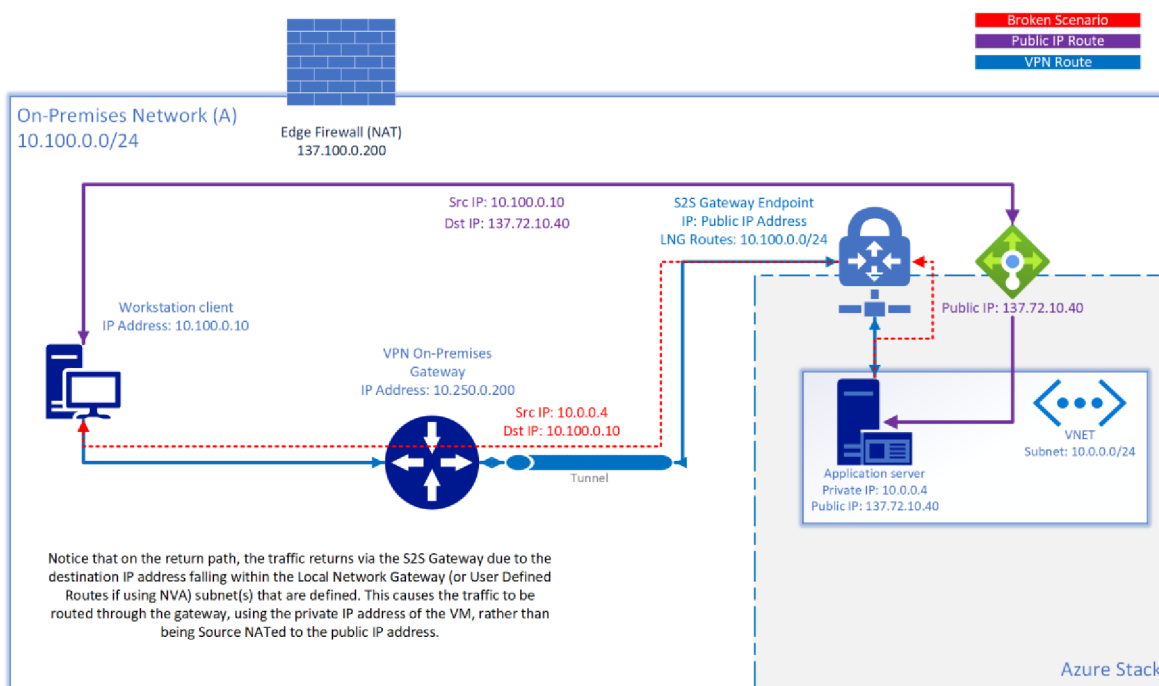
Obrázek 7: Síťové zapojení

Logické sítě reprezentují abstrakci nad fyzickou vrstvou síťové infrastruktury. Při plánování je potřeba vzít v potaz následující sítě a jejich velikosti:

- Public VIP – /26 (62 IP) až /22 (1022 IP) – doporučeno /24
- Switch infrastructure – /26 – síť pro vnitřní komunikaci switchů
- Infrastructure – /24 – síť pro interní komunikaci jednotlivých komponent
- Private – /20 – síť pro storage, privátní VIP, infrastrukturní kontejnery a ostatní interní funkce
- BMC – /26 – síť pro management komunikaci

Public VIP je síť, která komunikuje mimo Azure Stack Hub. Nemusí to být nutně veřejné adresy. Tyto adresy se použijí, pokud je v administraci požadavek na veřejnou adresu. Na ní budou vy publikované a dostupné vytvořené služby. Azure Stack Hub rezervuje 31 adres z tohoto rozsahu. Ty jsou určeny pro vnitřní služby, App Service, SQL resource providers a budoucí využití.

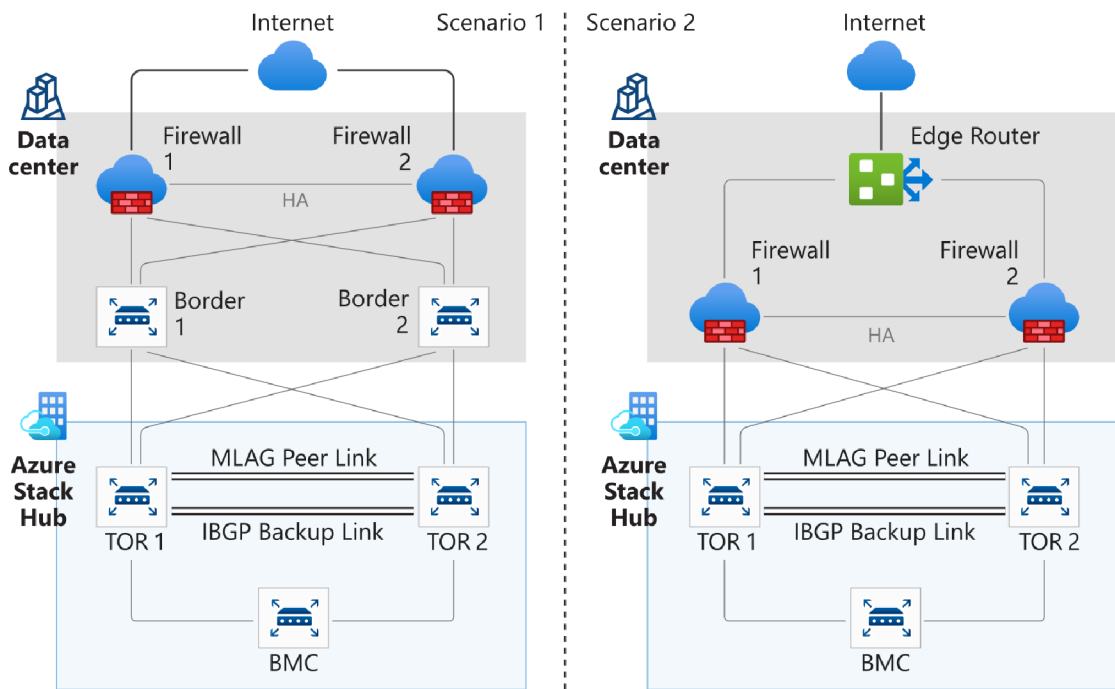
Komunikace s vnitřní sítí zákazníka lze uskutečnit dvěma způsoby. Prvním je použití Public VIP a druhým je použití Virtual Network Gateway a vytvoření S2S tunelu. Může existovat scénář, který je zachycen na Obrázek 8: PVIP a S2S. Pokud je navázán S2S tunel, tak může dojít k potížím, pokud se zdroj (zde stanice s IP 10.100.0.10) pokusí komunikovat s cílem na jeho PVIP (zde 137.72.10.40), protože se cíl pokusí poslat odpověď zdroji do S2S tunelu. V tomto případě je nutné vybrat jednu z možností připojení.



Obrázek 8: PVIP a S2S

K zajištění zabezpečení Azure Stack Hub se doporučuje použití zařízení s bránou firewall. Brány firewall mohou pomoci bránit se například proti útokům distribuovaného odmítnutí služby (DDoS), detekci narušení a kontrole obsahu. Mohou se však také stát překážkou propustnosti pro služby úložiště Azure, jako jsou objekty blob, table a queue. (14)

Na Obrázek 9: Firewall jsou znázorněny dva scénáře, jak je možné integrovat bránu firewall.



Obrázek 9: Firewall

4 Vlastní práce

4.1 Integrace do prostředí datového centra

Každá firma má nějakou svoji interní síť, ať už se jedná o jeden počítač připojený k internetu, nebo o několik různých síťových segmentů pro různé účely. Datové centrum je typickým příkladem, kde existuje několik různých podsítí, ať už z důvodu rozdělení provozu, bezpečnostních důvodů, či segmentace zákazníků. Převážně z těchto důvodů je potřeba proces integrace řádně promyslet a naplánovat. Při nevhodném návrhu integrace Azure Stack Hub je nutné začít s integrací znovu od začátku přeinstalací systému, nedá se zde použít metoda opravy, případně „přiohnutí“.

Azure Stack Hub je jako celek samostatné datové centrum, obsahuje výpočetní výkon, úložiště, síť a další komponenty, které se vyskytují v běžném datovém centru. Při konfiguraci se zadává pool public IP adres, přes které probíhá komunikace mezi vnitřním prostředím a vnějším prostředím. Základní otázkou je, zda se integruje Azure Stack Hub jako samostatné datové centrum vedle stávajícího již běžícího, nebo zda se integruje do nějaké části stávajícího datového centra. Každá z těchto variant má své klady a své zápory.

Zapojení Azure Stack Hub jako samostatně běžící datové centrum je z pohledu integrace snadnější proces. Do poolu veřejných adres se přidají skutečné veřejné adresy (dostupné z internetu), DNS systém překládá interní jména k těmto veřejným adresám, takže není problém s vytvořením zdroje, který je dostupný přes své jméno hned po svém vytvoření i z internetu. Nevýhodou je, že nelze využít existující site-to-site VPN spojení navázané do stávajícího datového centra od zákazníků a je potřeba realizovat nové.

Druhá varianta znamená, že se externím rozhraním připojí samostatná podsíť datového centra. Pool veřejných adres v Azure Stack Hub jsou ve skutečnosti privátní adresy z rozsahu přiděleného pro tuto podsíť. Výhodou je, že zdroj či služba publikovaná z Azure Stack Hub může být dostupná i ze vzdáleného prostředí zákazníka přes již existující VPN spojení do datového centra vhodným směrováním síťového provozu. Mezi nevýhody se řadí nutnost mapovat skutečnou veřejnou adresu dostupnou z internetu na veřejnou adresu Azure Stack Hub a již zmíněný problém s DNS záznamy.

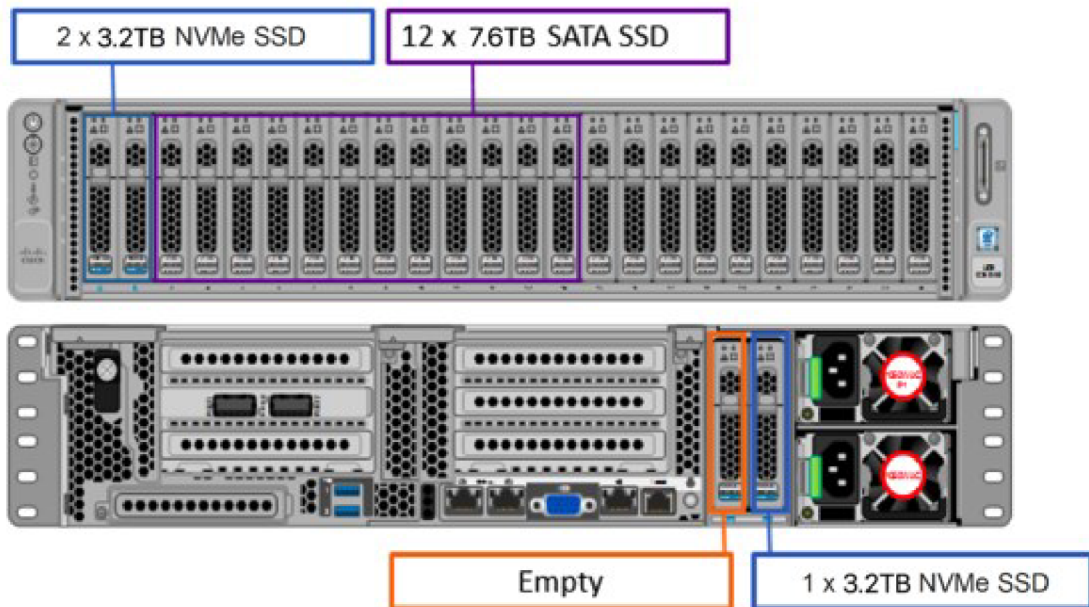
Při implementaci Azure Stack Hub ve zvolené firmě byla vybrána druhá možnost. První zmíněná nevýhoda je, že Azure Stack Hub mapuje vnitřní síť na nějakou adresu z poolu veřejných adres, které předpokládá, že jsou veřejné. Aby byly dostupné z internetu, tak je nutné provoz směřovat skrz vnitřní síť datového centra a do internetu je mapovat na skutečné veřejné adresy.

Manuální udržování tabulky záznamů dvojic veřejné adresy Azure Stack Hub a skutečné veřejné adresy je velmi náchylné na chyby a značnou mírou snižuje agilitu pro zákazníky. Z těchto důvodů byla navržena a implementována aplikace, která přes API rozhraní Azure Stack Hub z něj vyčítá informace o veřejné IP adrese a nastavuje síťová zařízení v datovém centru. Aplikace si udržuje informaci i o zákazníkovi a dovolí pouze takové změny, na které má zákazník oprávnění.

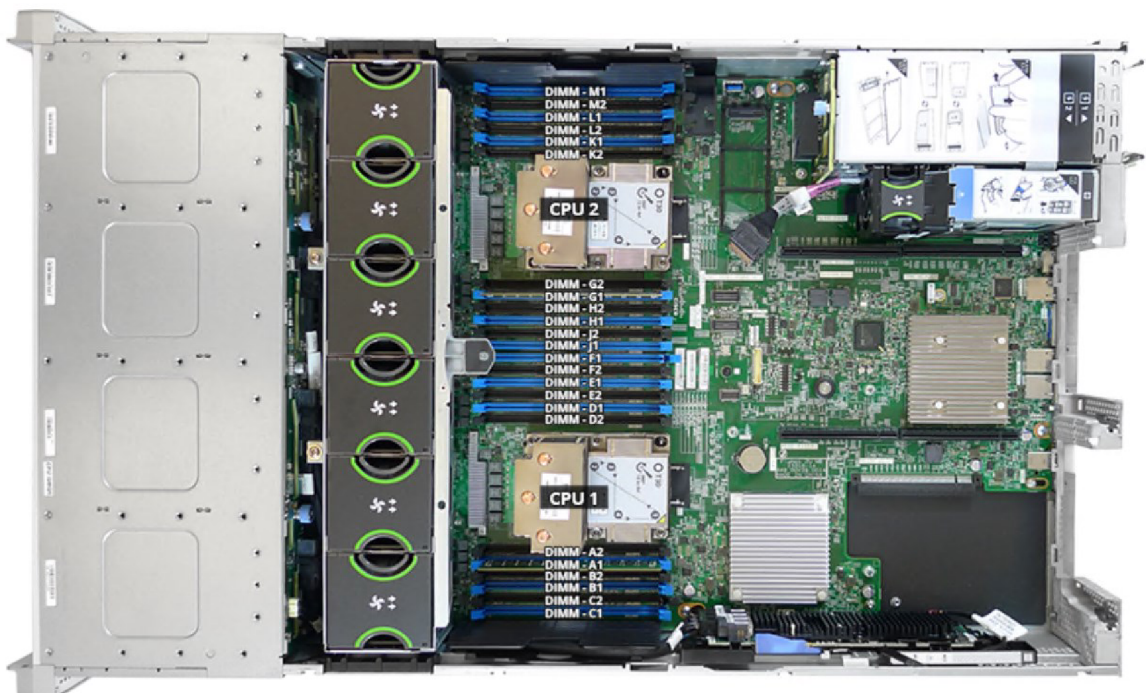
Druhou zmíněnou nevýhodou je překlad DNS jmen. Azure Stack Hub má svůj vlastní systém doménových jmen, kde si udržuje překlady mezi jmény a IP adresami z poolu veřejných adres. Zatímco realizace překladu IP adres je realizována přes NAT, tak u jmen je potřeba udržovat externí DNS. Do finalizace této práce nebyla tato problematika vyřešena, tak zde není ani detailně rozebrána.

4.2 Proces nasazení

Nasazované řešení se skládá z osmi dvouprocesorových serverů Cisco UCS C240 M5SX osazených procesory Intel Xeon Gold 6248, 1,5TB operační paměti a 12 SSD disků s kapacitou 91,2 TB. Dále jsou zde 3 NVMe SSD disky, které slouží jako cache. Pohled na server zepředu a zezadu je znázorněn na Obrázek 10: Server. Na Obrázek 11: Server – vnitřní pohled je znázorněn vnitřní pohled na server.



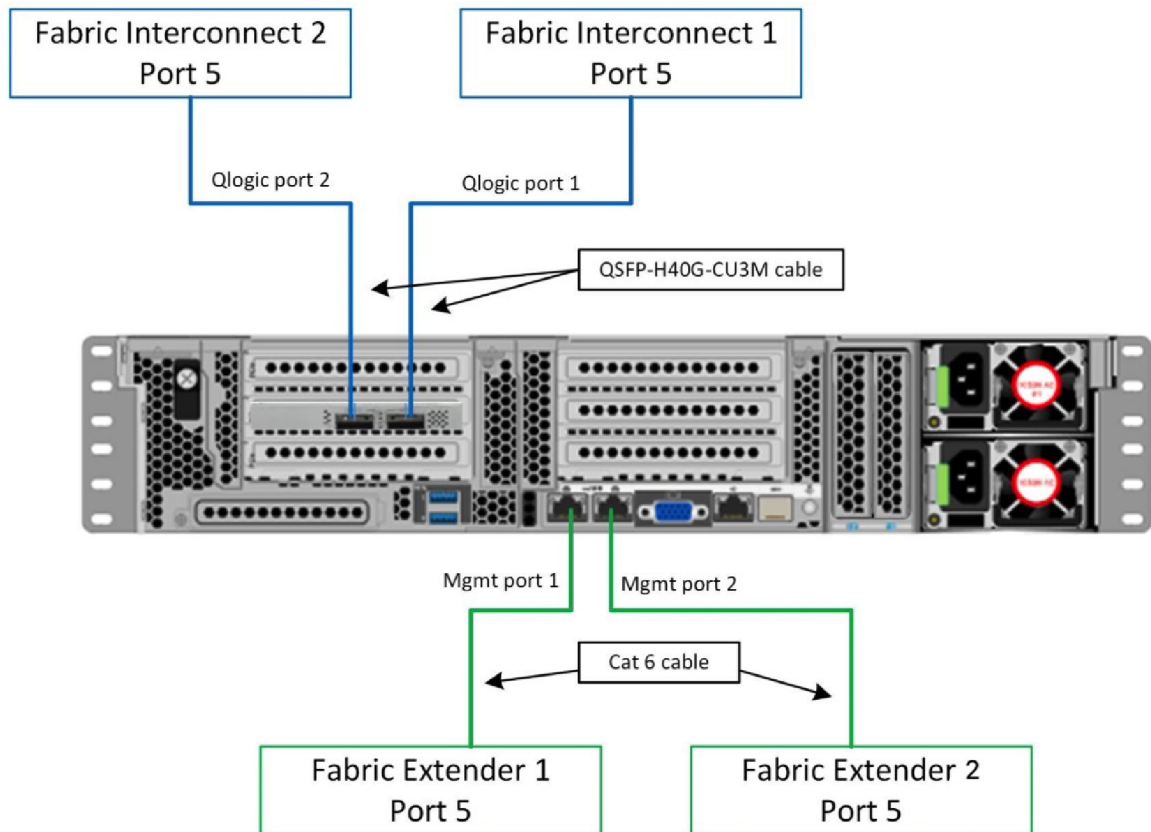
Obrázek 10: Server – vnější pohled



Obrázek 11: Server – vnitřní pohled

Každý z těchto serverů má zapojenu dvojici management rozhraní vždy do dvojice Fabric Extender (FEX) Cisco 2348UPQ a dvojici provozních/datových rozhraní do dvojice

Fabric Interconnect (FI) Cisco UCS 6332. Na následujících obrázcích je pohled na síťové prvky serveru, FEX, FI a celkové schéma na zapojení jednoho serveru ke jmenovaným zařízením.



Obrázek 12: Server – síťová rozhraní

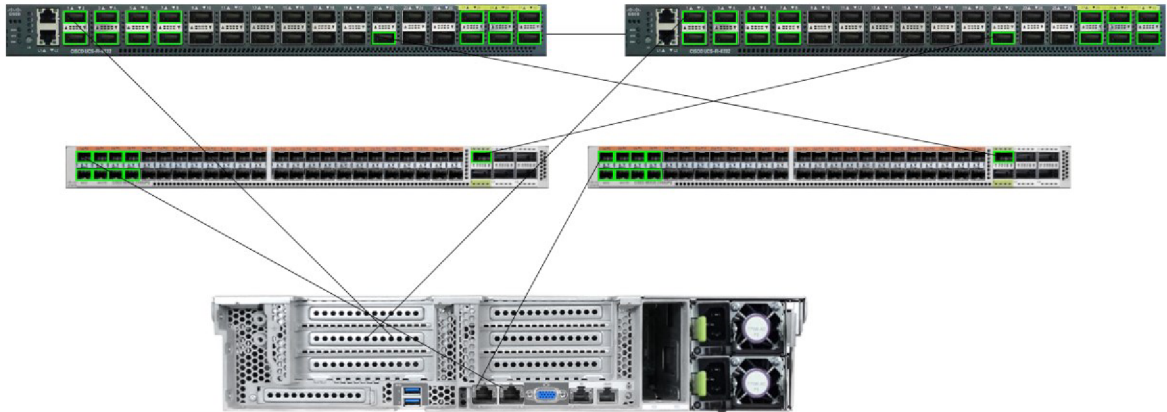
Physical Display



Obrázek 13: Fabric Extender (FEX)



Obrázek 14: Fabric Interconnect (FI)

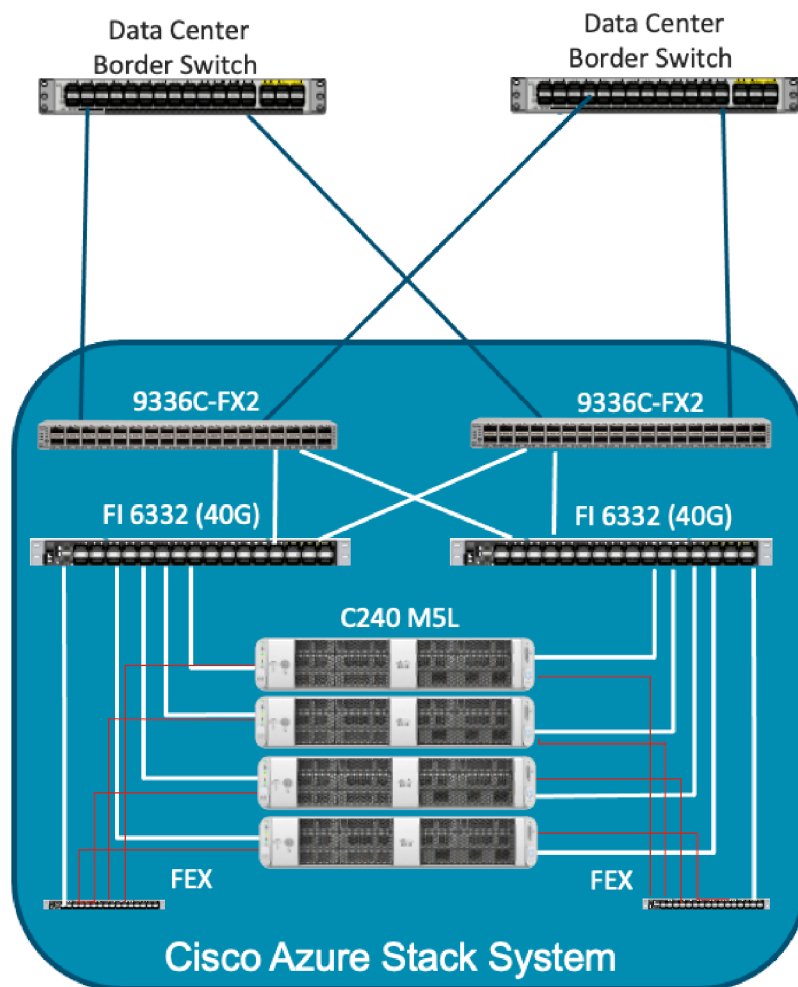


Obrázek 15: Zapojení serveru do FEX a FI

Prvních osm portů ve FEX je připojeno k osmi serverům – management. Fabric port (vpravo) je zapojen do nadřazeného Fabric Interconnectu.

Prvních osm portů ve FI je opět zapojeno k osmi serverům – data. Port 22 je připojen k FEX. Porty 27-32 jsou vždy po třech zapojeny do top of rack switchů (TOR) Cisco 9336C.

High level design je zachycen na Obrázek 16: Azure Stack Hub HLD.



Obrázek 16: Azure Stack Hub HLD

Po dodání hardwaru je nutné všechny komponenty zapojit a zkonfigurovat. Zapojení provádí dodavatel, kontrolu zapojení a konfiguraci provádí technik vendora. Před příjezdem techniků je nezbytné mít splněny následující předpoklady:

- všechny certifikáty musejí být zakoupeny a připraveny,
- musí být rozhodnuto o názvu oblasti/regionu,
- nebyly změněny parametry uvedené v listu nasazení. (15)

V průběhu plánování byl jeden z cílů rozhodnout o pojmenování Azure Stack Hub z pohledu domény. Ta se skládá z vyšších řádu vlastněné domény. Systém pojmenování je vymyšlený tak, že celý Azure Stack Hub má jméno domény třetího řádu. Pokud vlastníme

doménu druhého řádu firma.cz a zvolili jsme si jméno pro Azure Stack Hub „azs“, pak FQDN je azs.firma.cz. Doménou čtvrtého řádu je region. Region je název oblasti, kde je Azure Stack Hub umístěn a používá se pro rozlišení více scale unit. V případě použití více scale unit zatím portál neumožňuje měnit region přímo v jeho rozhraní, ale plánuje se tato funkcionality v budoucnu. Pro zařízení v Praze můžeme mít jméno praha.azs.firma.cz. Přístup na portál pak bude na adrese <https://portal.praha.azs.firma.cz>.

Protokol https je určen pro šifrovanou komunikaci a využívá certifikátů. Certifikáty pro Azure Stack Hub mohou být vydány veřejnou certifikační autoritou i interní certifikační autoritou, ale nejsou povoleny self-signed certifikáty. Pokud se používá veřejná certifikační autorita, tak musí být obsažena v rámci Microsoft Trusted Root Authority programu. Azure Stack Hub musí mít síťový přístup k seznamu odvolaných certifikátů (CRL), který je dostupný na protokolu http.

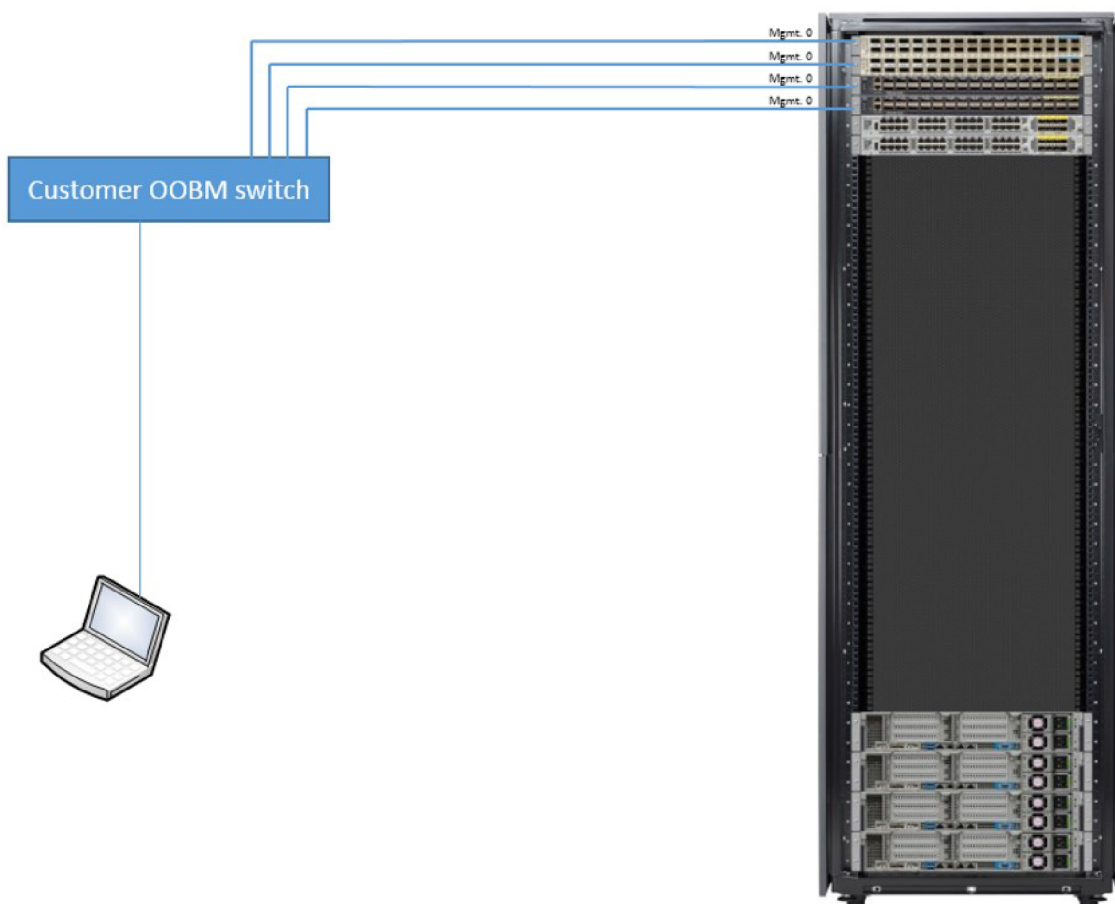
Pro nasazení v Azure Stack Hub jsou nutné tyto certifikáty:

- portal.praha.azs.firma.cz – certifikát, kterým se prokazuje zákaznický portál,
- adminportal.praha.azs.firma.cz – certifikát, kterým se prokazuje administrátorský portál,
- management.praha.azs.firma.cz – certifikát pro komunikaci při nasazování zdrojů pomocí ARM,
- adminmanagement.praha.azs.firma.cz – certifikát pro komunikaci při nasazování zdrojů pomocí ARM šablon v administrátorském prostředí,
- *.blob.praha.azs.firma.cz (wildcard) – certifikát pro bezpečný přístup k úložišti typu blob,
- *.table.praha.azs.firma.cz (wildcard) – certifikát pro bezpečný přístup k úložišti typu table,
- *.queue.praha.azs.firma.cz (wildcard) – certifikát pro bezpečný přístup k úložišti typu queue,
- *.vault.praha.azs.firma.cz (wildcard) – certifikát pro bezpečný přístup k trezoru klíčů,
- *.adminvault.praha.azs.firma.cz (wildcard) – certifikát pro bezpečný přístup k trezoru klíčů v administrátorském prostředí,

- *.adminhosting.praha.azs.firma.cz (wildcard) – certifikát pro hostování rozšíření v administrátorském prostředí,
- *.hosting.praha.azs.firma.cz (wildcard) – certifikát pro hostování rozšíření.

Hvězdičkové (wildcard) certifikáty používají vytvářené zdroje v zákaznických subskripcích pro zabezpečenou komunikaci. Z toho plyne i podmínka jedinečnosti názvů těchto vytvářených zdrojů. Nelze mít dva zdroje se stejným jménem. Tato podmínka je při vytváření zdroje validována a pokud již jméno existuje, tak nedovolí zdroj vytvořit.

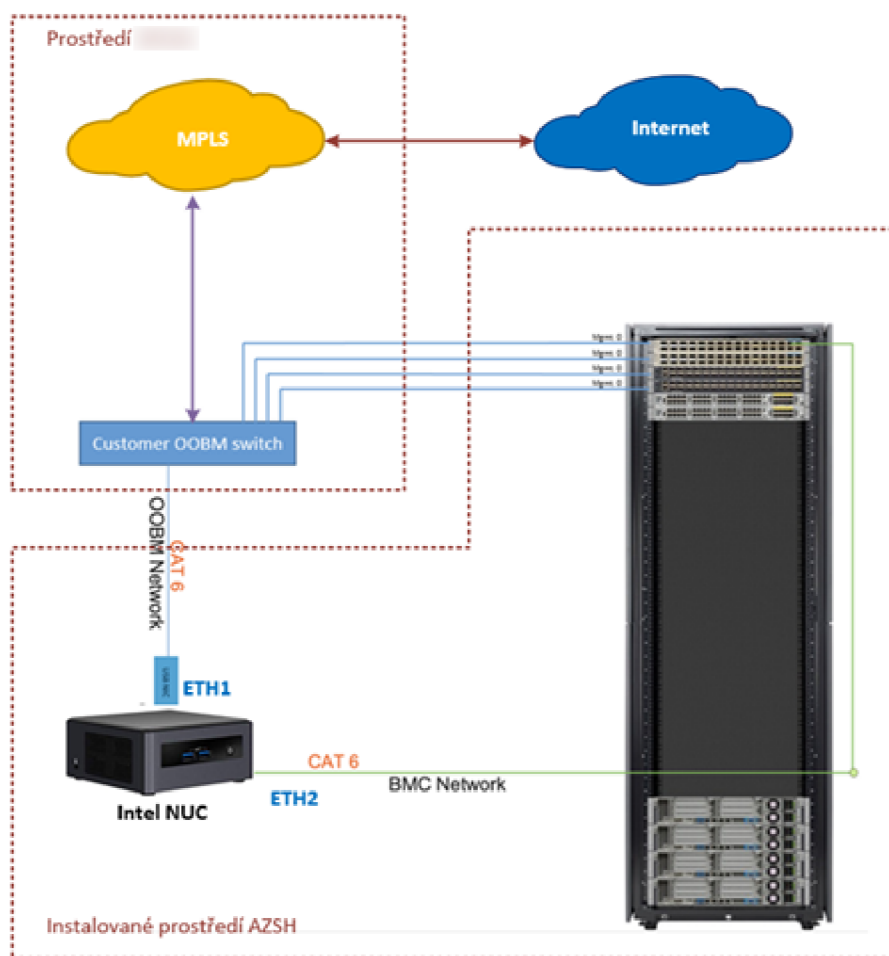
Technik, po kontrole zapojení, připojuje své zařízení k OOBM síti s přístupem na management zařízení tak, jak je zobrazeno na Obrázek 17: Deployment.



Obrázek 17: Deployment

Z důvodu cestovních omezení v rámci epidemie COVID-19 bylo realizováno alternativní řešení, kdy se, místo zařízení technika, použilo předkonfigurované zařízení Intel

NUC, které se zapojilo jedním rozhraním k OOBM switchi a druhým rozhraním k síti s připojením k internetu. Technikovi byl zřízen VPN přístup k tomuto zařízení a z něj se prováděla instalace. Zapojení je zobrazeno na Obrázek 18: Alternativa deploymentu.



Obrázek 18: Alternativa deploymentu

Po kontrole zapojení a připojení k zařízení se provede konfigurace síťových zařízení tak, aby všechny komponenty byly síťově dostupné. Poté následuje instalace samotného systému Azure Stack Hub, která trvá několik hodin. Instalační i ověřovací proces probíhá formou PowerShell příkazů.

4.3 Post Deployment

Po samotné instalaci následuje její kontrola pomocí příkazu `Test-AzureStack`. Tento příkaz zkontroluje stav celého Azure Stack Hub a pokud je zařízení v pořádku, tak vrátí hodnotu `$true`. Pokud ověření stavu selže, tak je vrácena hodnota `$false`. Tento příkaz se spouští z privilegovaného endpointu a je vhodné ho použít kdykoliv je potřeba ověřit stav, v provozu, zejména před aktualizací systému.

Po úspěšné validaci stavu je nutné zaregistrovat Azure Stack Hub do Azure, aby bylo možné stahovat položky z Marketplace a spárovat využívané zdroje s příslušnou smlouvou, ze které budou čerpány poplatky za využívání. Registrace se provádí příkazem `Set-AzsRegistration` do určité subskripce a je potřeba zadat její ID. Registraci je potřeba provést účtem, který je vlastníkem příslušné subskripce. Pro některé operace jsou potřeba práva global admin, např. pro instalační skripty pro resource provider. Obnovení nebo změna registrace se provádí odebráním registrace (`Remove-AzsRegistration`) a novou registrací. (16) Důvody pro přeregistraci jsou převážně pro licenční model na základě kapacity a jsou to tyto:

- obnovení roční subskripce
- změna licenčního modelu
- při změně škálování (přidání/odebrání fyzických serverů)

Azure Stack Hub má integrovaný monitoring vnitřní infrastruktury přístupný z admin portálu. Každá komponenta má položky `Health` a `Alerts`. `Health` určuje zdravotní stav komponenty a `Alerts` počet výstrah, které jsou v severitách `Warning`, který indikuje nestandardní stav komponenty a většinou nemá dopad do běžících služeb, a `Critical`, kdy už je komponenta ve vážném zdravotním stavu. Tento interní monitoring je vhodné zaintegrovat do centrálního monitoringu datového centra. To lze posíláním událostí do Event Hubu, který je možné integrovat se systémy třetích stran.

Jedním z dalších kroků je nastavení zálohování, které má Azure Stack Hub také integrované a také dostupné z admin portálu. Jedná se pouze o zálohu a obnovu infrastruktury, zálohování jednotlivých uživatelských subskripcí je nutné řešit samostatně. Zálohuje se do umístění zadané UNC cestou, není podporován NFS protokol. Zálohy jsou šifrované veřejným klíčem certifikátu.

4.4 Porovnání administrace

Sledovaná firma používá virtualizační platformu vmware vSphere v místním prostředí a Microsoft Azure v cloudovém prostředí, proto je porovnání provedeno na těchto třech technologických prostředích – vmware, Azure a Azure Stack Hub. Porovnání je provedeno od samotné instalace a konfigurace daného prostředí až po vytvoření virtuálního serveru.

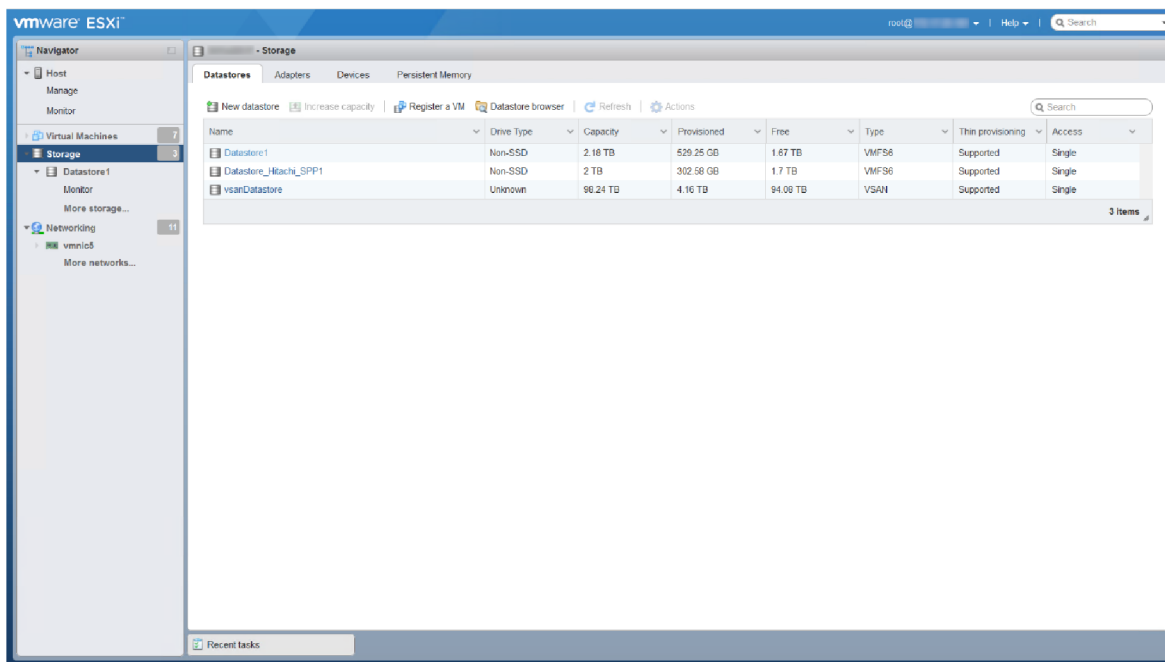
Instalace virtualizovaného prostředí vmware začíná instalací operačního systému na pořízený hardware. Operačním systémem vmware je vlastní linux-based systém Photon, který zprostředkovává produkt vmware vSphere. Po instalaci operačního systému na všechny fyzické servery (ESXi hosty) je možné je ovládat, ale pouze každý samostatně. Aby bylo možné je spravovat přes jednotné rozhraní, tak je potřeba nainstalovat produkt vmware vCenter. Není to jen společné prostředí, ale zároveň zajišťuje vysokou dostupnost na úrovni hardwaru. Aby se mohly využít lokální disky jako společné úložiště, tak je potřeba nainstalovat další produkt vmware vSAN. Tento produkt zajišťuje dostupnost dat i v případě výpadku jednoho ze serverů. Pro virtualizované sítě je potřeba produkt vmware NSX. Sledovaná firma nepoužívá lokální disky pro společné úložiště, ani virtualizované sítě. Pro společné úložiště je použita SAN síť. Sítě jsou přivedeny k virtualizaci klasickým nevirtualizovaným způsobem.

Microsoft Azure je cloudové prostředí, které není potřeba instalovat vlastními zdroji, instalaci provádí technici poskytovatele služby. Zákazník dostane připravené prostředí, ve kterém si instaluje potřebné virtuální servery a ostatní služby potřebné pro konkrétní využití. Tato instalace probíhá v rámci prostředí převážně pomocí průvodce, případně pomocí připravených skriptů.

Obdobně je na tom Azure Stack Hub, protože instalaci v lokálním prostředí provádí technici dodavatele. Tato instalace je součástí dodávky hardware a není povolena instalace zákazníkem. Instalace jedné lokality trvá většinou jeden den včetně následné konfigurace.

Po instalaci operačních systémů a podpůrných produktů je potřeba systém zkonfigurovat, aby plnil požadovanou funkčnost. V prostředí vmware se jedná o konfiguraci samotných ESXi hostů, konfiguraci vCenter, konfiguraci vSAN a konfiguraci NSX. Síťová konfigurace ESXi hostů probíhá již v rámci instalace operačního systému, ostatní konfigurace probíhají přes webový prohlížeč ESXi hosta nebo vCenter. Všechny

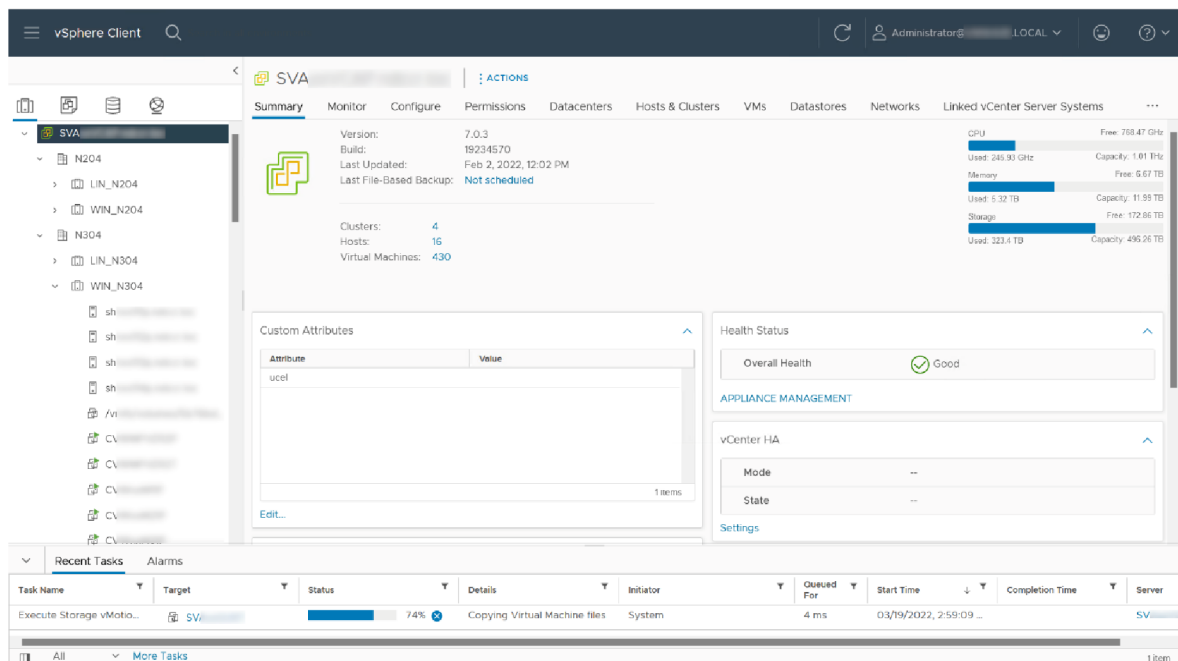
konfigurace v rozhraní ESXi se vztahují pouze ke konkrétnímu ESXi, proto je vhodné provádět celou konfiguraci přes vCenter, kde je možné provést změny na všech serverech. Na Obrázek 19: ESXi rozhraní je zachyceno ESXi rozhraní s pohledem na konfiguraci diskového úložiště.



Obrázek 19: ESXi rozhraní

Rozhraní vmware vCenter je centrem konfigurace pro všechny použité produkty. Základní obrazovka je rozdělena na tři části, první je levý panel, kde se přepínají pohledy na zobrazení jednotlivých fyzických serverů v clusterech, logických datacentrech, zobrazení podle logického uspořádání do složek a podsložek, zobrazení datových úložišť a pohled na síťové prostředí. Druhá část je panel ve spodní části okna, kde se zobrazují aktuální úkoly a výstrahy. Poslední část je pravý (největší) panel, kde jsou záložky, které přepínají pohledy na konkrétní zdroj vybraný v levém panelu.

Na Obrázek 20: vCenter rozhraní je vybrán objekt vCenter (v levém panelu) a v pravém panelu zobrazen pohled na souhrnné informace. Ve spodním panelu je vidět, že právě probíhá úkol Storage vMotion, který přesouvá úložiště virtuálního serveru z jednoho na druhé.



Obrázek 20: vCenter rozhraní

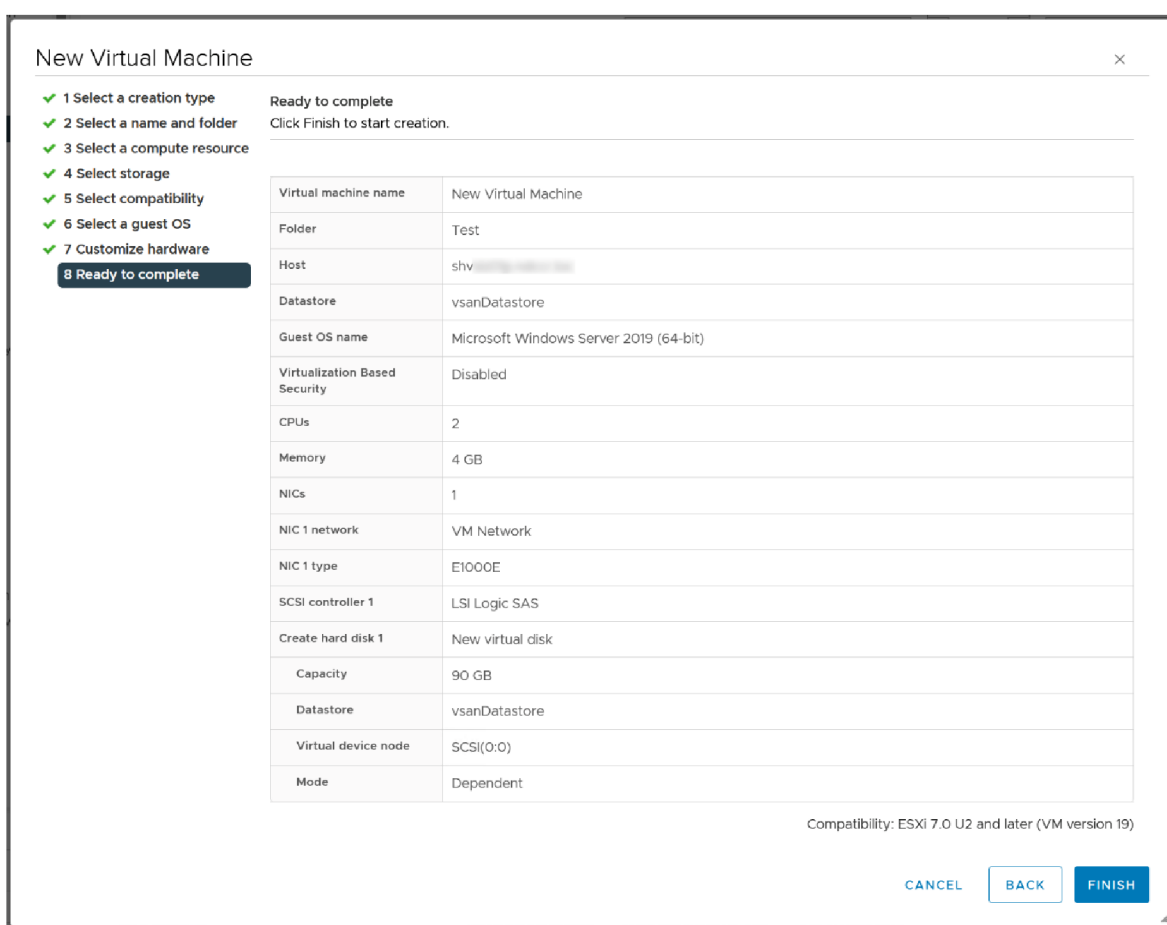
Konfigurace diskového úložiště technologií vSAN se provádí aktivací na clusteru na záložce Configure. Po aktivaci služby se zobrazí prostředí pro konfiguraci diskových skupin, ze kterých se následně vytváří společné úložiště pro všechny servery v clusteru. Virtualizace sítě technologií NSX vyžaduje instalaci pomocných virtuálních serverů a konfigurace probíhá přes samostatné webové rozhraní.

Oproti konfiguraci vmware je konfigurace prostředí Microsoft Azure je nulová. V okamžiku zpřístupnění prostředí, tedy po uzavření smlouvy a vytvoření subskripce, je prostředí plně zkonfigurované a možné okamžitě používat. Není nutné připojovat diskové úložiště, ani není nutné konfigurovat síť. Konfigurace sítě a potřebné diskové úložiště pro virtuální servery se provádí přímo při vytváření tohoto virtuálního serveru.

Podobně je tomu i u Azure Stack Hub. Konfigurace probíhá po instalaci techniky dodavatele. Předáním řešení je prostředí plně připraveno na používání. Nutno podotknout, že v rámci tohoto řešení nelze přidávat úložiště pomocí sítě SAN. To je zároveň nevýhodou Azure Stack Hub, protože pokud dojde k vyčerpání kapacity úložiště, tak jedinou možností rozšíření je přidání dalšího fyzického serveru.

Vytváření virtuálního serveru je na všech třech platformách obdobný a realizuje se pomocí průvodce. V prostředí vmware je možné nový virtuální server vytvořit od základu,

nebo nasadit pomocí existující šablony. Při vytváření nového serveru vyzve průvodce postupně k názvu serveru a umístění do složky, určení fyzického serveru, na kterém má tento virtuální server běžet, výběr úložiště, kompatibilitu se staršími verzemi hostitele, výběr operačního systému pro správnou nabídku vmware tools, nastavení zdrojů jako jsou procesor, paměť, řadič a velikost disku, výběr z existujících sítí a na závěr shrnutí zadaných parametrů. Na Obrázek 21: Průvodce vytvoření serveru – vmware je zobrazena finální obrazovka průvodce se souhrnem zadaných parametrů.



Obrázek 21: Průvodce vytvoření serveru – vmware

Po vytvoření serveru je připraven virtuální hardware, ale je nutné nainstalovat operační systém. Při vytváření serveru ze šablony se udělá klon disku šablony a průvodce nabídne, v případě operačního systému Windows, i sysprep disku, aby se vygenerovaly nové identifikátory systému a nedošlo ke kolizi v doménovém prostředí. Průvodce též umožňuje připojit server do domény Active Directory.

V prostředí Azure se virtuální servery vždy nasazují ze šablony, která se vybírá v rámci Marketplace. Na Obrázek 22: Průvodce vytvoření serveru – Azure je úvodní stránka vytvoření serveru.

Microsoft Azure

Dashboard > rg-vm > Create a resource > Marketplace >

Create a virtual machine

Basics Disks Networking Management Advanced Tags Review + create

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. [Learn more](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *

Resource group * [Create new](#)

Instance details

Virtual machine name *

Region *

Availability options

Security type

Image * [See all images](#) [Configure VM generation](#)

Azure Spot instance

Size * [See all sizes](#)

Administrator account

Username *

Password *

Confirm password *

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * None Allow selected ports

Select inbound ports *

Warning: This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

Licensing

Save up to 49% with a license you already own using Azure Hybrid Benefit. [Learn more](#)

[Review + create](#) < Previous Next : Disks >

Obrázek 22: Průvodce vytvoření serveru – Azure

Úvodní stránka sbírá informace o logickém i fyzickém umístění, názvu, velikosti a administrátorských údajích virtuálního serveru. Na další kartě Disks se přiřazují disky a určuje jejich redundance a šifrování. Pod záložkou Networking najdeme konfigurační položky týkající se sítě. Lze zde síť nejen vybrat, ale pokud neexistují, tak zároveň i vytvořit. V Managementu je možnost zapnout diagnostiku při startu, připojit identitu Azure AD, nastavení automatického vypnutí, nebo orchestraci aktualizací. Před vytvořením serveru zkontroluje průvodce správnost všech zadaných dat a pokud je validace úspěšná, tak server vytvoří.

Další možností vytvoření serveru v Azure jsou ARM šablony. Jedná se o šablonu ve formátu JSON, která popisuje celý zdroj a lze popsat celé prostředí. Dynamičnost v použití šablon přinášení parameters a variables. Parameters jsou proměnné zadávané z vnějšku šablony, zatímco variables jsou používány pouze uvnitř šablony. Vytvoření stejného serveru jako v předchozím případě je možné použít následující ARM šablonu.

```
{
  "$schema": "http://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {
    "location": {
      "type": "string"
    },
    "networkInterfaceName": {
      "type": "string"
    },
    "enableAcceleratedNetworking": {
      "type": "bool"
    },
    "networkSecurityGroupName": {
      "type": "string"
    },
    "networkSecurityGroupRules": {
      "type": "array"
    },
    "subnetName": {
      "type": "string"
    },
    "virtualNetworkName": {
      "type": "string"
    },
    "addressPrefixes": {
      "type": "array"
    }
  }
}
```

```
},
"subnets": {
  "type": "array"
},
"publicIpAddressName": {
  "type": "string"
},
"publicIpAddressType": {
  "type": "string"
},
"publicIpAddressSku": {
  "type": "string"
},
"pipDeleteOption": {
  "type": "string"
},
"virtualMachineName": {
  "type": "string"
},
"virtualMachineComputerName": {
  "type": "string"
},
"virtualMachineRG": {
  "type": "string"
},
"osDiskType": {
  "type": "string"
},
"osDiskDeleteOption": {
  "type": "string"
},
"virtualMachineSize": {
  "type": "string"
},
"nicDeleteOption": {
  "type": "string"
},
"adminUsername": {
  "type": "string"
},
"adminPassword": {
  "type": "secureString"
},
"patchMode": {
  "type": "string"
},
},
```



```

    "enableHotpatching": {
      "type": "bool"
    }
  },
  "variables": {
    "nsgId": "[resourceId(resourceGroup().name, 'Microsoft.Network/networkSecurityGroups',
parameters('networkSecurityGroupName'))]",
    "vnetName": "[parameters('virtualNetworkName')]",
    "vnetId": "[resourceId(resourceGroup().name, 'Microsoft.Network/virtualNetworks',
parameters('virtualNetworkName'))]",
    "subnetRef": "[concat(variables('vnetId'), '/subnets/', parameters('subnetName'))]"
  },
  "resources": [
    {
      "name": "[parameters('networkInterfaceName')]",
      "type": "Microsoft.Network/networkInterfaces",
      "apiVersion": "2021-03-01",
      "location": "[parameters('location')]",
      "dependsOn": [
        "[concat('Microsoft.Network/networkSecurityGroups/',
parameters('networkSecurityGroupName'))]",
        "[concat('Microsoft.Network/virtualNetworks/', parameters('virtualNetworkName'))]",
        "[concat('Microsoft.Network/publicIpAddresses/',
parameters('publicIpAddressName'))]"
      ],
      "properties": {
        "ipConfigurations": [
          {
            "name": "ipconfig1",
            "properties": {
              "subnet": {
                "id": "[variables('subnetRef')]"
              },
              "privateIPAllocationMethod": "Dynamic",
              "publicIpAddress": {
                "id": "[resourceId(resourceGroup().name,
'Microsoft.Network/publicIpAddresses', parameters('publicIpAddressName'))]",
                "properties": {
                  "deleteOption": "[parameters('pipDeleteOption')]"
                }
              }
            }
          }
        ]
      },
      "enableAcceleratedNetworking": "[parameters('enableAcceleratedNetworking')]",
      "networkSecurityGroup": {

```

```

        "id": "[variables('nsgId')]"
    }
}
},
{
    "name": "[parameters('networkSecurityGroupName')]",
    "type": "Microsoft.Network/networkSecurityGroups",
    "apiVersion": "2019-02-01",
    "location": "[parameters('location')]",
    "properties": {
        "securityRules": "[parameters('networkSecurityGroupRules')]"
    }
},
{
    "name": "[parameters('virtualNetworkName')]",
    "type": "Microsoft.Network/virtualNetworks",
    "apiVersion": "2020-11-01",
    "location": "[parameters('location')]",
    "properties": {
        "addressSpace": {
            "addressPrefixes": "[parameters('addressPrefixes')]"
        },
        "subnets": "[parameters('subnets')]"
    }
},
{
    "name": "[parameters('publicIpAddressName')]",
    "type": "Microsoft.Network/publicIpAddresses",
    "apiVersion": "2019-02-01",
    "location": "[parameters('location')]",
    "properties": {
        "publicIpAllocationMethod": "[parameters('publicIpAddressType')]"
    },
    "sku": {
        "name": "[parameters('publicIpAddressSku')]"
    }
},
{
    "name": "[parameters('virtualMachineName')]",
    "type": "Microsoft.Compute/virtualMachines",
    "apiVersion": "2021-07-01",
    "location": "[parameters('location')]",
    "dependsOn": [
        "[concat('Microsoft.Network/networkInterfaces/',
parameters('networkInterfaceName'))]"
    ],

```

```

"properties": {
  "hardwareProfile": {
    "vmSize": "[parameters('virtualMachineSize')]"
  },
  "storageProfile": {
    "osDisk": {
      "createOption": "fromImage",
      "managedDisk": {
        "storageAccountType": "[parameters('osDiskType')]"
      },
      "deleteOption": "[parameters('osDiskDeleteOption')]"
    },
    "imageReference": {
      "publisher": "MicrosoftWindowsServer",
      "offer": "WindowsServer",
      "sku": "2022-datacenter-g2",
      "version": "latest"
    }
  },
  "networkProfile": {
    "networkInterfaces": [
      {
        "id": "[resourceId('Microsoft.Network/networkInterfaces',
parameters('networkInterfaceName'))]",
        "properties": {
          "deleteOption": "[parameters('nicDeleteOption')]"
        }
      }
    ]
  },
  "osProfile": {
    "computerName": "[parameters('virtualMachineComputerName')]",
    "adminUsername": "[parameters('adminUsername')]",
    "adminPassword": "[parameters('adminPassword')]",
    "windowsConfiguration": {
      "enableAutomaticUpdates": true,
      "provisionVmAgent": true,
      "patchSettings": {
        "enableHotpatching": "[parameters('enableHotpatching')]",
        "patchMode": "[parameters('patchMode')]"
      }
    }
  },
  "diagnosticsProfile": {
    "bootDiagnostics": {
      "enabled": true
    }
  }
}

```

```

        }
    }
}
],
"outputs": {
    "adminUsername": {
        "type": "string",
        "value": "[parameters('adminUsername')]"
    }
}
}
}

```

ARM šablony mohou působit příliš krkolomně, dost možná kvůli formátu JSON. Proto existuje i možnost šablon v jazyce Bicep. (17) Tento jazyk jednoduchým způsobem popisuje zdroje v Azure opět pomocí parametrů a proměnných. Pro porovnání je níže uvedena Bicep šablona úplně stejného virtuálního serveru jako výše.

```

param location string
param networkInterfaceName string
param enableAcceleratedNetworking bool
param networkSecurityGroupName string
param networkSecurityGroupRules array
param subnetName string
param virtualNetworkName string
param addressPrefixes array
param subnets array
param publicIpAddressName string
param publicIpAddressType string
param publicIpAddressSku string
param pipDeleteOption string
param virtualMachineName string
param virtualMachineComputerName string
param virtualMachineRG string
param osDiskType string
param osDiskDeleteOption string
param virtualMachineSize string
param nicDeleteOption string
param adminUsername string

@secure()
param adminPassword string
param patchMode string
param enableHotpatching bool

```

```

var nsgId = resourceId(resourceGroup().name, 'Microsoft.Network/networkSecurityGroups',
networkSecurityGroupName)
var vnetName = virtualNetworkName
var vnetId = resourceId(resourceGroup().name, 'Microsoft.Network/virtualNetworks',
virtualNetworkName)
var subnetRef = '${vnetId}/subnets/${subnetName}'

resource networkInterfaceName_resource 'Microsoft.Network/networkInterfaces@2021-03-01' = {
  name: networkInterfaceName
  location: location
  properties: {
    ipConfigurations: [
      {
        name: 'ipconfig1'
        properties: {
          subnet: {
            id: subnetRef
          }
          privateIPAllocationMethod: 'Dynamic'
          publicIPAddress: {
            id: resourceId(resourceGroup().name, 'Microsoft.Network/publicIpAddresses',
publicIpAddressName)
            properties: {
              deleteOption: pipDeleteOption
            }
          }
        }
      }
    ]
    enableAcceleratedNetworking: enableAcceleratedNetworking
    networkSecurityGroup: {
      id: nsgId
    }
  }
  dependsOn: [
    networkSecurityGroupName_resource
    virtualNetworkName_resource
    publicIpAddressName_resource
  ]
}

resource networkSecurityGroupName_resource 'Microsoft.Network/networkSecurityGroups@2019-02-01' = {
  name: networkSecurityGroupName
  location: location
  properties: {
    securityRules: networkSecurityGroupRules
  }
}

```

```

    }
  }

resource virtualNetworkName_resource 'Microsoft.Network/virtualNetworks@2020-11-01' = {
  name: virtualNetworkName
  location: location
  properties: {
    addressSpace: {
      addressPrefixes: addressPrefixes
    }
    subnets: subnets
  }
}

resource publicIpAddressName_resource 'Microsoft.Network/publicIpAddresses@2019-02-01' = {
  name: publicIpAddressName
  location: location
  properties: {
    publicIPAllocationMethod: publicIpAddressType
  }
  sku: {
    name: publicIpAddressSku
  }
}

resource virtualMachineName_resource 'Microsoft.Compute/virtualMachines@2021-07-01' = {
  name: virtualMachineName
  location: location
  properties: {
    hardwareProfile: {
      vmSize: virtualMachineSize
    }
    storageProfile: {
      osDisk: {
        createOption: 'FromImage'
        managedDisk: {
          storageAccountType: osDiskType
        }
        deleteOption: osDiskDeleteOption
      }
      imageReference: {
        publisher: 'MicrosoftWindowsServer'
        offer: 'WindowsServer'
        sku: '2022-datacenter-g2'
        version: 'latest'
      }
    }
  }
}

```

```

}
networkProfile: {
  networkInterfaces: [
    {
      id: networkInterfaceName_resource.id
      properties: {
        deleteOption: nicDeleteOption
      }
    }
  ]
}
osProfile: {
  computerName: virtualMachineComputerName
  adminUsername: adminUsername
  adminPassword: adminPassword
  windowsConfiguration: {
    enableAutomaticUpdates: true
    provisionVMAgent: true
    patchSettings: {
      enableHotpatching: enableHotpatching
      patchMode: patchMode
    }
  }
}
diagnosticsProfile: {
  bootDiagnostics: {
    enabled: true
  }
}
}
}

```

```
output adminUsername string = adminUsername
```

V prostředí Azure Stack Hub je vytváření velmi podobné, téměř stejné. Drobné odlišnosti jsou dané zejména tím, že vývoj Azure probíhá rychleji a nové funkcionality jsou na Azure Stack Hub nasazovány po ověření v prostředí Azure až s odstupem času. Na Obrázek 23: Průvodce vytvoření serveru – Azure Stack Hub je vidět, že změny oproti Azure nejsou patrné.

Microsoft Azure Stack Hub

Dashboard > Subscriptions > SBTesting > rg-vm > Marketplace > Windows Server 2022 Datacenter - Pay as you go >

Create a virtual machine

Basics | Disks | Networking | Management | Advanced | Tags | Review + create

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. [Learn more](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *

Resource group * [Create new](#)

Instance details

Virtual machine name *

Region *

Availability options

Image * [Browse all public and private images](#)

Size * **Standard DS1 v2**
1 vcpu, 3.5 GiB memory
[Change size](#)

Administrator account

Username *

Password *

Confirm password *

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * None Allow selected ports

Select inbound ports *

⚠ This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

[Review + create](#) [< Previous](#) [Next : Disks >](#)

Obrázek 23: Průvodce vytvoření serveru – Azure Stack Hub

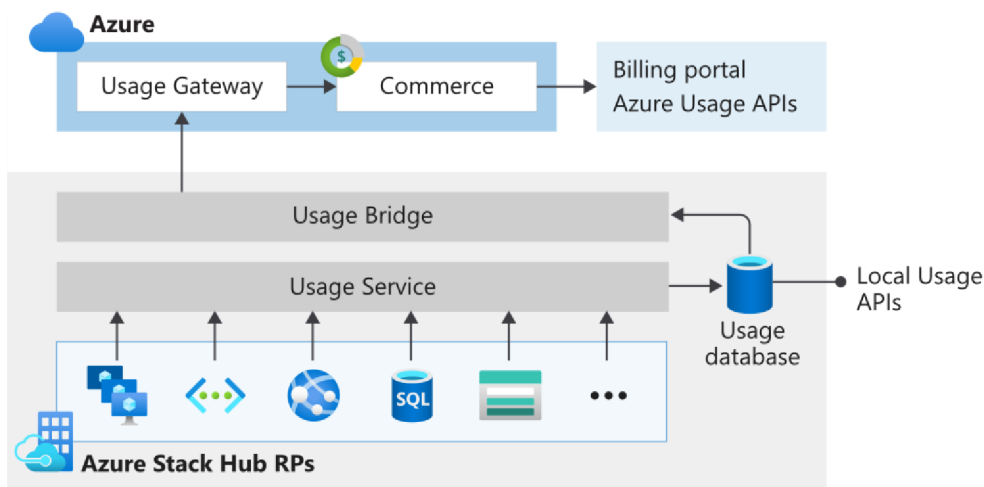
Šablony připravené pro prostředí Azure jsou použitelné i pro Azure Stack Hub, to je velká výhoda pro organizace využívající Azure a Azure Stack Hub. Je zde vidět, že oba produkty pocházejí z dílny jednoho producenta.

4.5 Billing & Usage

Pro každého provozovatele infrastruktury je důležité vědět, který systém spotřebuje kolik zdrojů a v případě, že tyto zdroje jsou nakupovány jako služba, tak i cenu těchto zdrojů. Znamená to, že je potřeba znát využití zdrojů (kolik hodin běžel virtuální počítač, jak velké úložiště zabírá apod.) a cenu za tyto zdroje. Cena a množství spotřebovaných jednotek má přímou úměrnost a lze říci, že se jedná o přepočtení podle předem známého ceníku.

Azure Stack Hub poskytuje informace o využívání služeb, neposkytuje informace o spotřebované ceně. Spotřebovaná cena je k dispozici v prostředí Azure. To je také jeden z důvodů, proč je potřeba v connected režimu zaregistrovat Azure Stack Hub do subskripce Azure. V disconnected režimu, kdy se platí za kapacitu dopředu, nedává tato informace smysl a už principu nepřipojení k Azure není k dispozici.

Na Obrázek 24: Billing je zobrazeno schéma toku informací o používání. Je vidět, že všechny využívané zdroje posílají informace o používání přes službu do databáze. Zároveň jsou data odesílána do Azure a poskytnuta přes API rozhraní. V Azure se udělá přepočtení na cenu a ta je opět k dispozici přes API rozhraní.



Obrázek 24: Billing

Azure Stack Hub generuje data o využívání v hodinových intervalech s minutovou granularitou pro každou subskripci. K dispozici jsou informace o použitých zdrojích jako jméno zdroje, umístění v subskripci a počet spotřebovaných jednotek. Každý zdroj má své specifické předem dané MeterID, jméno zdroje, množstevní jednotka a poznámka. Pro IP adresy jsou informace následující:

Statická IP adresa:

Meter ID: F271A8A388C44D93956A063E1D2FA80B

Meter name: Static IP Address Usage

Unit: IP addresses

Notes: Count of IP addresses used. If you call the usage API with a daily granularity, the meter returns IP address multiplied by the number of hours.

Dynamická IP adresa:

Meter ID: 9E2739BA86744796B465F64674B822BA

Meter name: Dynamic IP Address Usage

Unit: IP addresses

Notes: Count of IP addresses used. If you call the usage API with a daily granularity, the meter returns IP address multiplied by the number of hours.

Z výše uvedeného je patrné, že Meter ID je položka pro strojové zpracování a položka Meter name je položka čitelná pro lidské oko. Seznam všech položek je dostupný na odkazu <https://docs.microsoft.com/en-us/azure-stack/operator/azure-stack-usage-related-faq?view=azs-2108>.

Přístup k API rozhraní využívání zdrojů Azure Stack Hub je možné buď pomocí PowerShellu nebo REST API. Přistupovat k těmto zdrojům může operátor Azure Stack Hub nebo uživatel prostředí. Operátor má přístup ke všem datům o užívání všech uživatelských subskripcí, zatímco uživatel může přistupovat pouze ke své vlastní subskripci.

Další pohled přístupu je, zda se přistupuje přímo k rozhraní Azure Stack Hub, nebo přes Azure portál. Data získaná z rozhraní Azure Stack Hub jsou pouze o využívání zdrojů, zatímco data získaná z portálu Azure jsou transformována jako podklad pro vyúčtování.

Pomocí PowerShellu probíhá získání dat o využití následujícími kroky:

- instalace potřebných modulů

```
Install-Module -Name Az.BootStrapper -Force
Install-Module PowerShellGet -MinimumVersion 2.2.3 -Force
Install-AzProfile -Profile 2020-09-01-hybrid -Force
Install-Module -Name AzureStack -RequiredVersion 2.2.0
```

- příprava prostředí

```
$AADTenantName = "firma.onmicrosoft.com"
Add-AzEnvironment -Name "AzureStackAdminDC" `
  -ArmEndpoint "https://adminmanagement.dc.azs.firma.cz" `
  -AzureKeyVaultDnsSuffix adminvault.dc.azs.firma.cz `
  -AzureKeyVaultServiceEndpointResourceId https://adminvault.dc.azs.firma.cz
$AuthEndpoint = (Get-AzEnvironment -Name `
  "AzureStackAdminDC").ActiveDirectoryAuthority.TrimEnd('/')
$TenantId = (invoke-restmethod "$($AuthEndpoint)/$($AADTenantName)/.well-known/openid-
configuration").issuer.TrimEnd('/').Split('/')[1]
```

- připojení k Azure Stack Hub

```
Connect-AzAccount -EnvironmentName "AzureStackAdminDC" -TenantId $TenantId
```

- získání dat

```
Get-AzsSubscriberUsage -ReportedStartTime "2022-03-11" -ReportedEndTime "2022-03-12"
```

Tímto se získá report využití všech služeb v časovém rozmezí uvedených parametrů pro všechny použité zdroje. Vhodným filtrováním dat lze dostat potřebné údaje pro konkrétní subskripci, pro konkrétní zdroj.

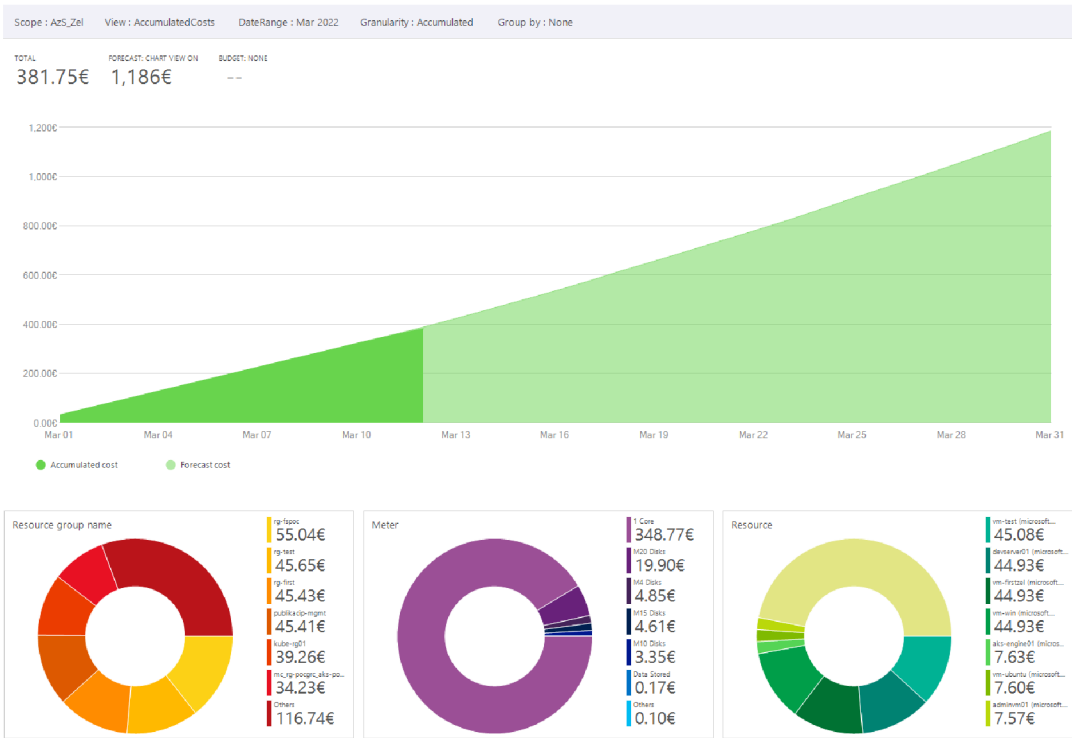
Další možností získání dat o využívání je použití REST API. Základním rozdílem proti použití PowerShell přístupu je ten, že API volání je vždy zaměřeno na konkrétní subskripci. Nelze tedy jedním voláním získat data za všechny použité zdroje ze všech subskripcí, ale je nutné zavolat API vícekrát.

Volání probíhá metodou GET na

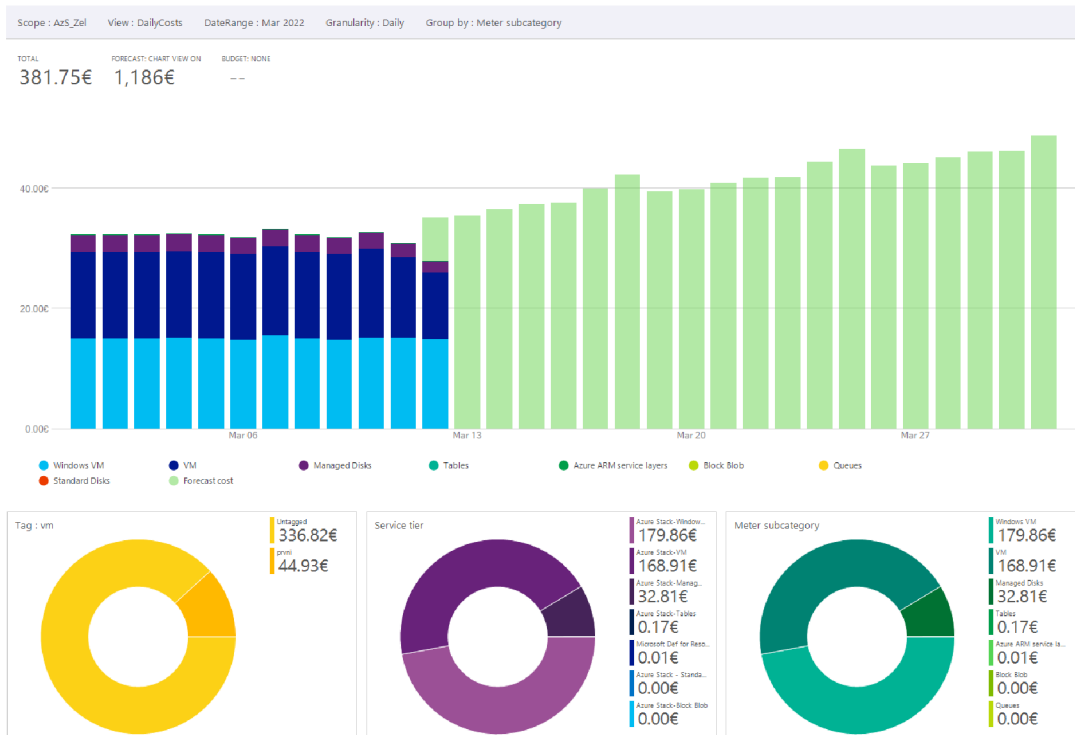
`https://{armendpoint}/subscriptions/{subId}/providers/Microsoft.Commerce.Admin/subscriberUsageAggregates?reportedStartTime={reportedStartTime}&reportedEndTime={reportedEndTime}&aggregationGranularity={granularity}&subscriberId={sub1.1}&api-version=2015-06-01-preview&continuationToken={token-value}`, kde:

- `armendpoint` – je Azure Resource Manager koncový bod Azure Stack Hub našeho prostředí. Tento bod je ve formátu `adminmanagement.{doménové jméno}`
- `subId` – je id subskripce uživatele, který provádí volání
- `reportedStartTime` – je čas začátku časového období
- `reportedEndTime` – je čas konce časového období
- `granularity` – je granularita, s jakou chceme mít data k dispozici. Jsou k dispozici dvě hodnoty – měsíční a denní. Tento parametr je volitelný a výchozí členění je nastaveno na jako denní.
- `sub1.1` – je id subskripce, na kterou filtrujeme data. Toto je nepovinný parametr, který najde uplatnění, pokud má vlastník více subskripcí a potřebuje využití pro každou zvlášť. (18)

Zatímco přístup k lokálnímu rozhraní Azure Stack Hub je převážně pro strojní zpracování a získání dat o využití, tak získání dat z portálu Azure je spíše pro přehledy o spotřebovaných zdrojích v podobě peněz. Na Obrázek 25: Billing v Azure 1 a Obrázek 26: Billing v Azure 2 jsou dva různé pohledy na interaktivní graf se stejnými daty, pouze s jiným pohledem.



Obrázek 25: Billing v Azure 1



Obrázek 26: Billing v Azure 2

5 Výsledky a diskuse

Azure Stack Hub není technologie, která by se dala vyzkoušet, zda vyhovuje požadavkům na provoz a zda majiteli bude vyhovovat. Proto je potřeba nejprve určit požadavky a rozhodnout se o případném nákupu až po jejich zvážení. Jedna z prvních otázek by měla být, zda je možné a vhodné použít zdroj identit Azure Active Directory. Pokud je odpověď na tuto otázku negativní, tak zůstává jen možnost ověřování přes ADFS, která nám určuje jediný možný model připojení, a to model disconnected. Režim připojení disconnected má jen jeden licenční/účtovací model a tím je licencování dle kapacity.

Při zvolení zdroje identit AAD je kapacitní model licencování k dispozici také, ale lze si vybrat i model licencování jen za použité zdroje. Nabízí se zde další otázka, jaký způsob používání výpočetních zdrojů se očekává. Pokud jsou předem určeny využití zdroje, které budou v provozu bez výpadku po celou dobu životnosti a neuvažuje se o vytváření/rušení další zdrojů, tak může být kapacitní model vhodnější volbou i při použití identit z AAD.

Další otázkou může být, kdo bude Azure Stack Hub spravovat. Lze využít služeb poskytovatelů a zařízení nemusí být umístěné ani v lokalitě koncového uživatele. V takovém případě se nejspíš neuvažuje varianta disconnected modelu, protože nedává příliš smysl. Při této otázce je potřeba zvážit dostatek lidských zdrojů a jejich znalosti. Otázka lidských zdrojů a jejich znalostí je vlastně samostatnou otázkou. Jiný pohled bude mít firma s administrátory vmware bez znalosti cloudových služeb Microsoft a jiný firma s administrátory Azure. Firma disponující znalostmi vmware bude mít nižší provozní náklady na virtualizaci vmware a dražší na Azure Stack Hub. A obráceně, firma s dostatečnou znalostí Azure bude mít provozní náklady na vmware vyšší. Pro jednu firmu může být Azure Stack Hub přínos, pro druhou zbytečně drahá investice.

Další vhodnou otázkou je, zda je možné pomocí Azure Stack Hub poskytnout zákazníkům lepší služby, případně úplně nové zatím neposkytované služby. Málodky je zákazníkům poskytována možnost vytvářet si v dedikovaném prostředí své vlastní síťové konfigurace, které lze v relativně krátkém čase měnit, nebo služby bezpečného úložiště, jakým je Key Vault. Opět zde závisí na konkrétní firmě a jejich poskytovaných službách, ale Azure Stack Hub určitě přinese minimálně agilitu, s jakou je možné poskytované služby doručit. Co je ale výhodou, je možnost použít automatizace, ať už pomocí ARM šablon, nebo šablon Bicep. Tato možnost na současných technologiích pro zákazníky chyběla.

Pokud firma provozuje virtualizaci na platformě vmware, tak zásadní bude i otázka, jak vypadá porovnání těchto dvou platform z finančního hlediska. Toto porovnání je rozděleno na dvě části, podle licencování běhu virtuálních serverů a podle licencování operačního systému Windows Server. Důvod tohoto rozdělení je, že každé firemní prostředí obsahuje různé množství těchto operačních systémů a prostý součet by zbytečně zkresloval výsledky tohoto porovnání.

V licencování na základě běžících virtuálních serverů je nejvýhodnější balíček IaaS z kapacitního licencování, následován o 74% dražším modelem licencování pay-as-you-use. Dalším v pořadí se umístil balíček App Service z kapacitního licencování, který je 2,78 krát dražší než balíček IaaS. Nejdražším licencováním je z tohoto pohledu platforma vmware. Pokud bychom porovnávali v delším časovém horizontu, tak by se pořadí určitě změnilo, ale s ohledem na morální zastarávání a větší náchylnost na chyby hardwaru nedává delší období smysl. Výběr správného licenčního modelu závisí na plánovaném využívání služeb.

Z pohledu licencování operačního systému byly uvažovány dva modely, již zmíněný pay-as-you-use a licencování na základě fyzických jader. Protože první model závisí na běžících serverech, tak byly zvoleny varianty 10%, 50% a 90% běžících Windows Server operačních systémů. Výsledek porovnání není jednoznačný, při běhu serverů s méně než 163 vCPU je výhodnější model licencování pay-as-you-use, nad touto hranicí už je výhodnější použít model licencování na jádra fyzického procesoru.

Slučovat tato dvě porovnání do jednoho společného nedává smysl, protože každá firma používá různé množství různých operačních systémů. Jiné licencované operační systémy zde nejsou uvedeny a je vhodné si udělat jejich porovnání. Pro jednoznačný závěr jsou potřeba konkrétní dodatečné vstupní informace.

Jednou z dalších otázek by mohlo být, jak „to“ celé zapojit. Existují dvě hlavní možnosti, celé jako samostatné datové centrum na veřejných IP adresách, nebo jako datové centrum uvnitř datového centra na privátních adresách. Každá z těchto variant má své výhody a také nevýhody a omezení. Zapojení s veřejnými adresami je z pohledu provozu jednodušší volba. Při zapojení s privátními adresami je dobré mít rozmyšleno, jakým způsobem se budou adresy překládat na veřejné a jakým způsobem se budou překládat DNS jména.

6 Závěr

Diplomová práce byla zaměřena na problematiku rozšíření datového centra o technologii Microsoft Azure Stack Hub.

V teoretické části byla představena technologie Azure Stack Hub a uvedeny možnosti nasazení do firemního prostředí, včetně představení administrace. Tato technologie byla porovnána se stávajícími provozovanými technologiemi nejen z pohledu technického, ale také ekonomického. Byly uvedeny výhody nejen pro zákazníky, ale i pro poskytovatele. Ekonomická výhodnost porovnávala všechny možnosti licenčních modelů se stávajícími technologiemi vmware a licencování operačního systému Windows Server.

Praktická část se věnovala integraci do prostředí datového centra. Detailně byl rozebrán proces nasazení, včetně vnitřního uspořádání nejen v rackové skříni, ale i zapojení jednotlivých komponent. V praktickém porovnání se srovnávala administrace stávajících technologií vmware s technologií Azure Stack Hub. Závěr praktické části se věnoval získávání dat o využívání, které jsou podkladem pro vyúčtování služeb.

Azure Stack Hub je platforma celého datového centra, která není určena pro každého. Tím samozřejmě není myšleno, že si jí nemůže kdokoliv pořídit, ale to, že není pro každého vhodná. Existují případy, kdy je vyloženě nevhodná, např. kvůli nemožnosti rozšíření o SAN úložiště. Na druhé straně jsou případy, kdy je platforma vyloženě výhodná, např. ve velmi proměnném testovací prostředí. Pro usnadnění rozhodování o pořízení této technologie byly v závěru zhodnoceny výsledky celé diplomové práce.

7 Seznam použitých zdrojů

- (1) MICROSOFT. *Co je cloud?* [online]. [cit. 2021-08-14]. Dostupné z: <https://azure.microsoft.com/cs-cz/overview/what-is-the-cloud/>
- (2) MICROSOFT. *Přehled o službě Azure Stack Hub* [online]. [cit. 2021-08-14]. Dostupné z: <https://docs.microsoft.com/cs-cz/azure-stack/operator/azure-stack-overview?view=azs-2102>
- (3) MICROSOFT. *Co je Azure* [online]. [cit. 2021-08-14]. Dostupné z: <https://azure.microsoft.com/cs-cz/overview/what-is-azure/>
- (4) MICROSOFT. *Disconnected deployment* [online]. [cit. 2022-03-05]. Dostupné z: <https://docs.microsoft.com/cs-cz/azure-stack/operator/azure-stack-disconnected-deployment?view=azs-2108>
- (5) MICROSOFT. *Comparing the Azure ecosystem* [online]. [cit. 2021-08-15]. Dostupné z: <https://docs.microsoft.com/en-us/azure-stack/operator/compare-azure-azure-stack?view=azs-2102>
- (6) MICROSOFT. *Azure Stack Hub Licensing, Packaging & Pricing Guide*. 2021. Dostupné také z: <https://azure.microsoft.com/mediahandler/files/resourcefiles/azure-stack-hub-licensing-packaging-pricing-guide/Azure%20Stack%20Hub%20Licensing%20Packaging%20and%20Pricing%20Guide.pdf>
- (7) ITPRICE. *VMware License* [online]. [cit. 2022-02-01]. Dostupné z: <https://itprice.com/vmware/license--perpetual---term---subscription-4>
- (8) ČESKÁ NÁRODNÍ BANKA. *Kurzy devizového trhu* [online]. [cit. 2022-02-01]. Dostupné z: <https://www.cnb.cz/cs/financni-trhy/devizovy-trh/kurzy-devizoveho-trhu/kurzy-devizoveho-trhu/index.html?date=01.02.2022>
- (9) MICROSOFT. *Microsoft Volume Licensing* [online]. [cit. 2022-03-24]. Dostupné z: <https://www.microsoft.com/en-us/licensing/licensing-programs/software-assurance-default>

- (10) CDW. Microsoft Windows Server Datacenter edition. *License & software assurance* [online]. [cit. 2022-02-01]. Dostupné z: <https://www.cdw.com/product/microsoft-windows-server-datacenter-edition-license-software-assurance/4325221>
- (11) CDW. Microsoft Windows Server Datacenter Edition. *Software assurance* [online]. [cit. 2022-02-01]. Dostupné z: <https://www.cdw.com/product/microsoft-windows-server-datacenter-edition-software-assurance-2-cores/4325222?pfm=srh>
- (12) MICROSOFT. *List nasazení pro Azure Stack Hub* [online]. [cit. 2021-08-15]. Dostupné z: <https://docs.microsoft.com/cs-cz/azure-stack/operator/azure-stack-deployment-worksheet?view=azs-2102>
- (13) MICROSOFT. *Network integration* [online]. [cit. 2021-08-15]. Dostupné z: <https://docs.microsoft.com/en-us/azure-stack/operator/azure-stack-network?view=azs-2102>
- (14) MICROSOFT. *Integrate a firewall with your Azure Stack Hub* [online]. [cit. 2021-08-15]. Dostupné z: <https://docs.microsoft.com/en-us/azure-stack/operator/azure-stack-firewall?view=azs-2102>
- (15) MICROSOFT. *Integrate datacentra* [online]. 2012 [cit. 2022-02-22]. Dostupné z: <https://docs.microsoft.com/cs-cz/azure-stack/operator/azure-stack-customer-journey?view=azs-2108&tabs=customer>
- (16) MICROSOFT. *Register Azure Stack Hub with Azure* [online]. [cit. 2022-03-26]. Dostupné z: <https://docs.microsoft.com/en-us/azure-stack/operator/azure-stack-registration>
- (17) MICROSOFT. *Bicep documentation* [online]. [cit. 2022-03-20]. Dostupné z: <https://docs.microsoft.com/en-us/azure/azure-resource-manager/bicep/>
- (18) MICROSOFT. *Azure Stack Hub API využití prostředků poskytovatele prostředků* [online]. [cit. 2022-03-13]. Dostupné z: <https://docs.microsoft.com/cs-cz/azure-stack/operator/azure-stack-provider-resource-api?view=azs-2108>

8 Seznam obrázků

Obrázek 1: Connected/disconnected cesty	12
Obrázek 2: Příklad scale unity	16
Obrázek 3: Admin portál	17
Obrázek 4: Portál Azure Stack Hub	18
Obrázek 5: Job role	18
Obrázek 6: List nasazení	28
Obrázek 7: Síťové zapojení	29
Obrázek 8: PVIP a S2S	30
Obrázek 9: Fiwall	31
Obrázek 10: Server – vnější pohled	34
Obrázek 11: Server – vnitřní pohled	34
Obrázek 12: Server – síťová rozhraní	35
Obrázek 13: Fabric Extender (FEX)	35
Obrázek 14: Fabric Interconnect (FI)	36
Obrázek 15: Zapojení serveru do FEX a FI	36
Obrázek 16: Azure Stack Hub HLD	37
Obrázek 17: Deployment	39
Obrázek 18: Alternativa deploymentu	40
Obrázek 19: ESXi rozhraní	43
Obrázek 20: vCenter rozhraní	44
Obrázek 21: Průvodce vytvoření serveru – vmware	45
Obrázek 22: Průvodce vytvoření serveru – Azure	46
Obrázek 23: Průvodce vytvoření serveru – Azure Stack Hub	56
Obrázek 24: Billing	57
Obrázek 25: Billing v Azure 1	61
Obrázek 26: Billing v Azure 2	61

9 Seznam tabulek

Tabulka 1: Kapacitní model licencování	22
Tabulka 2: Cena za využití vCPU.....	22
Tabulka 3: Cena za využití vHDD.....	23
Tabulka 4: Cena za využití Azure Stack Hub	23
Tabulka 5: Cena za využití vmware	24
Tabulka 6: Porovnání provozu virtuálních serverů.....	24
Tabulka 7: Licence Windows Server per core.....	25
Tabulka 8: Licence Windows server – pay-as-you-go	26
Tabulka 9: Provnání nákladů na licencování Windows.....	26

10 Seznam použitých zkratek

AAD – Azure Active Directory
ADFS – Active Directory Federation Services
API – Application Programming Interface
ARM – Azure Resource Manager
CRL – Certificate Revocation List
DDoS – Distributed Denial of Service
DNS – Domain Name System
EA – Enterprise Agreement
FEX – Fabric Extender
FI – Fabric Interconnect
FQDN – Fully Qualified Domain Name
IaaS – Infrastructure as a Service
NAT – Network Address Translation
OOBM – Out-of-band Management
PaaS – Platform as a Service
RBAC – Role-Based Access Control
SaaS – Software as a Service
TCO – Total Cost of Ownership
vCPU – virtuální procesor
vHDD – virtuální diskové úložiště
VPN – Virtual Private Network