

Virtualizace v Azure cloudu: Analýza Azure Virtual Machine a Azure Virtual Desktop

Radek Kratochvíl



Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

Ústav informatiky a umělé inteligence

Akademický rok: 2024/2025

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení: Radek Kratochvíl
Osobní číslo: A21604
Studijní program: B0613A140020 Softwarové inženýrství
Forma studia: Kombinovaná
Téma práce: Virtualizace v Azure cloudu: Analýza Azure Virtual Machine a Azure Virtual Desktop
Téma práce anglicky: Virtualization in Azure Cloud: Comparative Analysis of Azure Virtual Machine and Azure Virtual Desktop

Zásady pro vypracování

- Zpracujte literární rešerši na téma virtualizace a cloud computing.
- Popište cloudovou platformu Microsoft Azure.
- Shrňte rozdíly mezi Azure Virtual Machine a Azure Virtual Desktop.
- Implementujte a spravujte Azure Virtual Machine a podrobněji Azure Virtual Desktop.
- Srovnajte výkon, náklady, vhodnost nasazení, flexibilitu, bezpečnost a compliance aspekty Azure.
- Proveďte diskusi poznatků a doporučte využití pro různé scénáře.

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. MANGAN, Ryan. *Mastering Azure Virtual Desktop: A Practical Guide to Designing, Implementing, and Managing Azure Virtual Desktop Environments*. 2nd ed. Packt Publishing, 2024. ISBN 978-1835884140.
2. STEFANOVIC, Vladimir a Milos KATINSKI. *Pro Azure Administration and Automation*. Amsterdam: APress, 2021. ISBN 978-1-4842-7324-1.
3. SABALE, Arun a Balu N. ILAG. *Microsoft Azure Virtual Desktop Guide: Configuring and Operating Microsoft Azure Virtual Desktop (Exam AZ-140)*. Springer, 2022. ISBN 978-1-4842-8063-8.
4. MICROSOFT. *Azure Virtual Machines* [online]. © 2024. Dostupné z: <https://learn.microsoft.com/cs-cz/azure/virtual-machines/overview> [cit. 2024-10-21]
5. MICROSOFT. *Azure Virtual Desktop* [online]. © 2024. Dostupné z: <https://learn.microsoft.com/cs-cz/azure/virtual-desktop/overview> [cit. 2024-10-21]

Vedoucí bakalářské práce: **doc. Ing. Martin Sysel, Ph.D.**
Ústav počítačových a komunikačních systémů

Datum zadání bakalářské práce: **27. října 2024**
Termín odevzdání bakalářské práce: **2. června 2025**



L.S.

doc. Ing. Jiří Vojtěšek, Ph.D. v.r.
děkan

prof. Mgr. Roman Jašek, Ph.D., DBA v.r.
ředitel ústavu

Ve Zlíně dne 17. listopadu 2024

PROHLÁŠENÍ AUTORA BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že

- odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb., v platném znění bez ohledu na výsledek obhajoby;
- bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému a bude dostupná k nahlédnutí;
- jedno vyhotovení bakalářské práce v listinné podobě bude ponecháno Univerzitě Tomáše Bati ve Zlíně k uložení;
- na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 mohu užít své dílo – bakalářskou práci – nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá; neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji, že

- jsem na bakalářské práci pracoval(a) samostatně a použitou literaturu jsem řádně citoval(a); v případě publikace výsledků budu uveden(a) jako spoluautor;
- odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

Ve Zlíně, dne

.....
podpis autora

ABSTRAKT

Tato bakalářská práce se zaměřuje na analýzu a praktické aspekty virtualizačních řešení v cloudovém prostředí Microsoft Azure, se specifickým důrazem na služby Azure Virtual Desktop (AVD) a Azure Virtual Machine (AVM).

Teoretická část práce představuje základní koncepty cloud computingu a virtualizace, včetně jejich vývoje, principů a typů. Dále se zabývá modely nasazení cloudu dle definice NIST a seznamuje s hlavními virtualizačními platformami. Podrobněji je pak představena platforma Microsoft Azure a její klíčové služby AVD, AVM a Intune.

Praktická část práce popisuje proces nasazení a správy Azure Virtual Desktop, včetně plánování, konfigurace, nastavení přístupových práv a správy uživatelských profilů pomocí FSLogix. Dále se věnuje důležitým aspektům jako je licencování, zabezpečení a nástroje pro efektivní správu v prostředí Azure, mezi které patří PowerShell, Azure Portal a automatizační nástroje. Značná pozornost je věnována také evaluaci a srovnání služeb Azure Virtual Desktop a Azure Virtual Machine z hlediska výkonu, nákladů, flexibility, bezpečnosti a vhodnosti nasazení pro různé podnikové scénáře. Závěrem jsou formulována doporučení pro optimální využití těchto technologií.

Součástí práce je rovněž příloha s PowerShell skripty, které jsou navrženy jako funkce pro usnadnění správy a automatizace v prostředí Azure.

Klíčová slova: Azure, virtualizace, cloud computing, Azure Virtual Machine, Azure Virtual Desktop

ABSTRACT

This bachelor's thesis focuses on the analysis and practical aspects of virtualization solutions within the Microsoft Azure cloud environment, with a specific emphasis on Azure Virtual Desktop (AVD) and Azure Virtual Machine (AVM) services.

The theoretical part of the thesis introduces the fundamental concepts of cloud computing and virtualization, including their evolution, principles, and types. It further discusses cloud deployment models as defined by NIST and presents major virtualization platforms. The Microsoft Azure platform and its key services, AVD, AVM, and Intune, are then introduced in more detail.

The practical part of the thesis describes the process of deploying and managing Azure Virtual Desktop, including planning, configuration, access rights setup, and user profile management using FSLogix. It also addresses crucial aspects such as licensing, security, and tools for efficient management in the Azure environment, which include PowerShell, Azure Portal, and automation tools. Significant attention is given to the evaluation and comprehensive comparison of Azure Virtual Desktop and Azure Virtual Machine services in terms of performance, costs, flexibility, security, and suitability for deployment in various business scenarios. Finally, recommendations for the optimal utilization of these technologies are formulated.

The thesis also includes an appendix with PowerShell scripts, designed as functions to facilitate management and automation within the Azure environment.

Keywords: Azure, virtualization, cloud computing, Azure Virtual Machine, Azure Virtual Desktop

Na tomto místě bych chtěl poděkovat vedoucímu své bakalářské práce doc. Ing. Martinu Syslovi, Ph.D., za veškerou podporu a pomoc, cenné rady a připomínky, za odborné vedení práce i za podporu a trpělivost při jejím vytváření.

Mé poděkování patří rovněž mé rodině a kolegům z práce, kteří mě v době kombinovaného vysokoškolského studia a při zpracování bakalářské práce podporovali.

OBSAH

ÚVOD.....	13
I TEORETICKÁ ČÁST	14
1 VIRTUALIZACE.....	15
2 VÝVOJ A PRINCIP VIRTUALIZACE	16
3 TYPY VIRTUALIZACE	17
4 ROZHODNUTÍ VIRTUALIZOVAT	18
4.1 VÝHODY VIRTUALIZACE	18
4.1.1 Zvýšení flexibility	18
4.1.2 Dostupnost.....	19
4.1.3 Bezpečnost	19
4.2 NEVÝHODY VIRTUALIZACE	20
4.2.1 Složitá správa systému a cena	20
4.2.2 Sdílené systémové prostředky	20
5 VIRTUALIZAČNÍ PLATFORMY	21
5.1 VMWARE	21
5.2 HYPER-V.....	21
5.3 WINDOWS SANDBOX.....	21
5.4 KVM (LINUX).....	22
6 CLOUDOVÁ ŘEŠENÍ.....	23
6.1 ZÁKLADNÍ MODEL Y CLOUD COMPUTINGU PODLE DEFINICE NIST	23
6.1.1 Software as a Service (SaaS).....	23
6.1.2 Platform as a Service (PaaS).....	24
6.1.3 Infrastructure as a Service (IaaS)	24
6.2 MODEL Y NAsAZENÍ.....	25
6.2.1 Veřejný cloud	25
6.2.2 Privátní cloud	25
6.2.3 Hybridní cloud	26
6.3 HLAVNÍ POSKYTOVATELÉ CLOUDOVÝCH SLUŽEB.....	26
7 MICROSOFT AZURE	28
7.1 AZURE VIRTUAL DESKTOP (AVD).....	28
7.2 AZURE VIRTUAL MACHINE (VM)	29
7.3 INTUNE.....	29
II PRAKTICKÁ ČÁST.....	31
8 NAsAZENÍ AZURE VIRTUAL DESKTOP.....	33
8.1 PLÁNOVÁNÍ NAsAZENÍ	34
8.2 KONFIGURACE.....	35

8.3	PŘIHLÁŠENÍ DO AZURE PORTÁLU	36
8.4	VYTVOŘENÍ A SPRÁVA PŘEDPLATNÉHO (SUBSCRIPTION).....	36
8.5	NASTAVENÍ PŘÍSTUPOVÝCH PRÁV (ACCESS CONTROL – IAM)	37
8.6	HOST POOL.....	38
8.7	SESSION HOST	40
8.8	ZPŮSOB PŘIPOJENÍ UŽIVATELŮ K AZURE VIRTUAL DESKTOP	41
8.9	UŽIVATELSKÉ PROFILY	42
8.10	LICENCOVÁNÍ.....	42
9	NÁSTROJE PRO SPRÁVU	44
9.1	AUTOMATIZACE POMOCÍ POWERSHELLU	44
9.2	AZURE <i>PORTAL</i>	44
9.3	AUTOMATION ACCOUNTS.....	45
9.4	AZURE CLI (COMMAND-LINE INTERFACE)	46
10	PROVOZNÍ ŘÍZENÍ A METODY PRO SPRÁVU	48
10.1	ŠKÁLOVÁNÍ	48
10.2	AKTUALIZACE SOFTWARE	48
11	EVALUACE A SROVNÁNÍ AVD A AVM	50
11.1	VÝKON	50
11.2	NÁKLADY	51
11.3	VHODNOST NASAZENÍ	53
11.4	FLEXIBILITA	53
11.5	BEZPEČNOST	54
11.6	COMPLIANCE	54
11.7	POROVNÁNÍ NÁKLADŮ DLE JEDNOTLIVÝCH PŘÍPADŮ.....	55
11.7.1	Cloudové řešení s užitím AVD	55
11.7.2	Hybridní řešení s Citrix Virtual Apps and Virtual Desktops	57
12	POZNATKY Z NASAZENÍ A DOPORUČENÍ PRO SPRÁVU	60
13	ZÁVĚR	61
	SEZNAM POUŽITÉ LITERATURY	63
	SEZNAM OBRÁZKŮ	66
	SEZNAM TABULEK.....	67
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK	68
	SEZNAM PŘÍLOH.....	69

ÚVOD

V současnosti je stále patrnější trend, kdy organizace hledají efektivnější způsoby, jak spravovat svou IT infrastrukturu, přičemž se vyhýbají nutnosti vlastnit a provozovat vlastní datová centra. Tento posun je do značné míry způsoben rostoucí poptávkou po externích cloudových službách, které organizacím umožňují využívat výpočetní, úložné a síťové zdroje bez potřeby investovat do vlastního hardwaru a jeho správy.

Důvodem pro tento přechod je snaha o zvýšení flexibility, škálovatelnosti a dostupnosti technologických prostředků, zatímco zároveň snižují náklady na provoz infrastruktury a zajištění její bezpečnosti. Jedním z přístupů, který umožňuje tento přechod, je cloud computing. Tento model nabízí přístup k potřebným zdrojům prostřednictvím internetu a nahrazuje lokálně hostované servery a datová centra.

Práce se zaměří na konkrétní nástroje a služby, jako jsou Azure Virtual Machine a Azure Virtual Desktop, a zhodnotí jejich vliv na efektivitu a konkurenceschopnost organizací.

I TEORETICKÁ ČÁST

1 VIRTUALIZACE

Virtualizace je zásadním milníkem v oblasti informačních technologií, která výrazně zvyšuje efektivitu využívání hardwarových zdrojů a usnadňuje správu IT infrastruktury. Tato technologie umožňuje abstrakci fyzického hardwaru a tvorbu virtuálních instancí operačních systémů, aplikací a síťových zdrojů. Díky virtualizaci je možné na jednom fyzickém serveru provozovat více virtuálních strojů, což vede k lepšímu využití dostupných kapacit, snižuje náklady na hardwarové vybavení a usnadňuje jeho správu.[3]

Virtualizace se používá v různých oblastech, od serverových prostředí až po desktopová řešení, a to jak v tradičních datových centrech, tak i v cloudových platformách. Cloud computing, jako inovativní přístup k poskytování IT zdrojů, se na virtualizaci zakládá. Mnohé cloudové platformy, jako Microsoft Azure, využívají virtualizaci pro optimalizaci poskytovaných služeb a zdrojů na požádání.[3]

2 VÝVOJ A PRINCIP VIRTUALIZACE

Virtualizace představuje technologii, která umožňuje provoz více logických výpočetních prostředí (virtuálních strojů) na jednom fyzickém zařízení. Využívá se převážně zejména v serverové infrastruktuře, kde přináší vyšší efektivitu, flexibilitu a snížení nákladů na hardware.

Podle odborné literatury vznikla myšlenka virtualizace již v 60. letech 20. století v souvislosti s vývojem mainframe systémů společnosti IBM. Moderní virtualizace je nejčastěji realizována pomocí tzv. hypervizoru, který zajišťuje oddělení fyzického hardwaru od virtuálních strojů. [1]

Existují dva hlavní typy hypervizorů, které se liší způsobem svého nasazení a interakcí s hardwarem. [1], [2]

Hypervizory typu 1, často označované jako „bare-metal“, běží přímo na fyzickém hardwaru bez potřeby hostitelského operačního systému. Tato přímá interakce s hardwarem umožňuje efektivnější využití systémových prostředků a vyšší výkon virtuálních strojů. Příkladem takových hypervizorů jsou Microsoft Hyper-V, VMware ESXi nebo Xen. [1], [2]

Na druhé straně hypervizory typu 2, známé jako „hostované“, fungují jako aplikace nad existujícím operačním systémem. Tento přístup je běžný v desktopových prostředích, kde uživatelé potřebují provozovat více operačních systémů na jednom zařízení. Mezi zástupce tohoto typu patří VirtualBox nebo VMware Workstation. [1], [2]

3 TYPY VIRTUALIZACE

Virtualizace není omezena pouze na servery; odborná literatura rozlišuje několik hlavních oblastí, mezi které patří serverová, desktopová, aplikační a síťová a virtualizace úložiště.

Serverová virtualizace je proces, při kterém je fyzický server rozdělen na více virtuálních strojů (VM), z nichž každý může běžet na jiném operačním systému. Tento přístup umožňuje konsolidaci serverů, což vede ke snížení nákladů na hardware a zjednodušení správy IT prostředí. Serverová virtualizace je široce využívána v datových centrech a cloudových službách.[3]

Desktopová virtualizace umožňuje uživatelům přístup k virtuálním desktopům běžícím na vzdálených serverech. Tento model přináší výhody v podobě centralizované správy, bezpečnosti a flexibility, protože uživatelé mohou přistupovat ke svým pracovním prostředím z různých zařízení a míst.[3]

Aplikační virtualizace spočívá v oddělení aplikace od operačního systému, na kterém běží. Aplikace jsou spuštěny v izolovaných prostředích, což zajišťuje jejich bezproblémový běh a snadnou správu. Tento přístup je užitečný při nasazování aplikací v prostředích s různými operačními systémy nebo verzemi.[3]

Síťová virtualizace zahrnuje abstrakci fyzické síťové infrastruktury do virtuálních sítí, které mohou být konfigurovány a spravovány nezávisle na fyzické struktuře. Tento přístup umožňuje efektivnější správu sítí, zlepšuje jejich flexibilitu a zjednodušuje nasazování nových služeb.[3]

Virtualizace úložiště se zaměřuje na abstrakci fyzických úložných zařízení do jednotného virtuálního úložného prostoru. Tento model umožňuje efektivní správu dat, zvyšuje dostupnost a zjednodušuje zálohování a obnovu dat.[3]

4 ROZHODNUTÍ VIRTUALIZOVAT

Hlavním důvodem pro nasazení virtualizace je ekonomická efektivita. Virtualizace umožňuje maximálně využít dostupný výkon fyzického hardwaru tím, že efektivně rozdělí jeho kapacity mezi více virtuálních strojů. To přináší nejen úsporu nákladů na hardware, ale i snížení nákladů na správu a údržbu infrastruktury. Dalším důvodem je zjednodušení správy IT prostředí, protože mnoho virtualizačních platform je dodáváno jako hotová řešení, která lze snadno implementovat a konfigurovat s minimálními programátorskými dovednostmi správce. Tyto platformy často nabízejí integrované nástroje pro správu, monitoring a údržbu, což značně usnadňuje každodenní operace.[3], [4], [5]

Virtualizace také umožňuje flexibilitu při migraci mezi fyzickými a virtualizovanými prostředím, díky čemuž je snadné přenášet existující aplikace na novou infrastrukturu. Nástroje pro migraci dat a virtuálních strojů mezi různými platformami usnadňují přechod na nové technologie a umožňují rychlou adaptaci na změny v potřebách organizace. Další výhodou je možnost vzdálené správy, která výrazně zjednodušuje údržbu a monitoring i u geograficky oddělených systémů.[3]

4.1 Výhody virtualizace

Virtualizace také přináší výhody v oblasti správy osobních stanic. Může například umožnit běh různých operačních systémů na stejné pracovní stanici nebo vytvoření testovacích prostředí pro vývoj a ladění aplikací. Tímto způsobem mohou vývojáři pracovat bezpečněji, protože testovací prostředí je izolováno od podkladního operačního systému, což minimalizuje riziko jeho narušení. Virtualizace rovněž umožňuje simulaci hardwaru, který ještě neexistuje v reálné podobě, což může být užitečné například při testování nových aplikací před jejich nasazením na skutečném hardware.[3]

4.1.1 Zvýšení flexibility

V době před virtualizací bylo pořízení každého fyzického serveru časově náročné a vyžadovalo pečlivý výběr, schválení a dodávku hardware. Tento proces, který mohl trvat týdny až měsíce, je v dnešním rychle se měnícím a agilním prostředí velmi neefektivní. Virtualizace umožňuje těmto zpožděním předejít, neboť vytváření virtuálních instancí pro konkrétní funkce je možné provést doslova během několika minut. Tento proces je silně automatizován a může být řízen centrálním managementem prostřednictvím jednoduchých

příkazů. Jediným omezením zůstává kapacita podkladního hardware nebo licenční ujednání, které mohou omezit množství virtuálních strojů, které lze provozovat na jednom fyzickém serveru.[3]

4.1.2 Dostupnost

Pro zajištění vysoké dostupnosti virtuálních serverů je nezbytné využívat load balancery, které mohou mít softwarovou nebo hardwarovou podobu. Při návrhu virtualizačního prostředí je důležité myslet na geografickou dostupnost, aby se minimalizovala rizika spojená s výpadky. Díky technologiím, které umožňují migraci virtuálních strojů mezi servery, je možné obnovit provoz nebo jej přesměrovat s minimálním výpadkem.[3]

Další výhodou je jednoduchá správa zálohování a obnovy. Možnost dynamicky přidávat a odstraňovat virtuální nody a provádět jejich migraci mezi servery bez výpadků přispívá k vysoké redundanci systému. Pokud dojde k výpadku jednoho geograficky odděleného datacentra, lze provoz rychle obnovit ze záloh v jiném datacentru, čímž je zajištěna kontinuita služeb a minimalizován dopad na uživatele.[3]

4.1.3 Bezpečnost

Větší organizace často zavádějí rozdělení odpovědnosti mezi různé oblasti virtualizační platformy, čímž dochází k rozdělení rolí a úkolů mezi jednotlivé administrátory. Tento přístup má za cíl minimalizovat riziko, že by jeden administrátor měl plný přístup ke všem konfiguracím, což by mohlo vést k nežádoucím změnám nebo dokonce k havárii systému. Rozdělení pravomocí zajišťuje větší kontrolu a zvyšuje úroveň bezpečnosti.[23], [3]

Kromě definování rolí nabízí různé virtualizační platformy i možnost dodatečného ověření pomocí druhého faktoru, například pomocí potvrzení na mobilním zařízení nebo použití hardwarového klíče. Tato metoda poskytuje další vrstvu ochrany, která výrazně zvyšuje bezpečnostní standardy a pomáhá předcházet neoprávněnému přístupu k citlivým datům nebo konfiguracím.[23]

4.2 Nevýhody virtualizace

I když virtualizace přináší mnoho výhod, jako je efektivní využívání hardwarových zdrojů, flexibilita a zjednodušená správa, není bez svých nevýhod. Existují i oblasti, ve kterých může virtualizace narazit na určité problémy. V této sekci se zaměříme na komplikace, které mohou nastat při implementaci a používání virtualizovaných prostředí, a na výzvy, které s těmito technologiemi souvisejí.[3]

4.2.1 Složitá správa systému a cena

Různorodost virtualizačních platforem, které nabízí různí výrobci, může značně zvýšit nároky na zaškolení personálu. Každá platforma má své specifické požadavky a nástroje, což může znamenat dodatečné školení a časové investice. Kromě toho mohou licence a technická podpora potřebná pro provoz příliš komplexních virtualizovaných prostředí být finančně náročná.[3], [20]

Pokud není implementována jasná strategie pro tvorbu a správu virtuálních strojů, může docházet k jejich nekontrolovanému a neefektivnímu využívání. Tato situace je obzvláště problematická, pokud jsou zdroje dostupné i pro neproškolené uživatele, což může vést k neoptimálnímu rozdělení systémových prostředků. Z tohoto důvodu je doporučeno zavést monitoring, který by umožnil efektivní kontrolu nad využíváním zdrojů. Tento monitoring však opět zvyšuje náklady a vyžaduje personál s adekvátními dovednostmi pro jeho správu[20]

4.2.2 Sdílené systémové prostředky

Jedním z hlavních argumentů pro virtualizaci je možnost sdílení zdrojů mezi více virtuálními stroji, což může přinést významné úspory. Tento přístup však může mít i své nevýhody, zejména pokud systém není schopen efektivně rozdělovat dostupné prostředky mezi jednotlivé instance. V případě, že některý z virtuálních strojů začne nadměrně využívat dostupné zdroje, může to mít negativní dopad na výkon celého systému.[4]

Neefektivní nebo nadměrné využívání systémových prostředků, například při instalaci velkých aktualizací balíčků, může způsobit přetížení hostitelského systému a zpomalit dynamiku prostředí. Takové problémy mohou výrazně snížit efektivitu virtualizovaného prostředí a vést k výpadkům nebo zpomalení výkonu, což je v kontrastu s očekávanými výhodami virtualizace.[4], [5], [6]

5 VIRTUALIZAČNÍ PLATFORMY

Existuje široké spektrum virtualizačních nástrojů, které nabízejí různé úrovně virtualizace. Tyto nástroje umožňují efektivní správu a využívání virtuálních prostředků v závislosti na konkrétním využití ať už pro osobní, komerční, nebo podnikové účely. Některé nástroje jsou určeny pro správu jednoho, jiní zase pro desítky podkladních systémů. Níže jsou uvedeny některé z nejznámějších a nejběžněji používaných virtualizačních nástrojů.

5.1 VMware

VMware ESXi je robustní virtualizační nástroj, který funguje jako samostatný operační systém určený výhradně pro virtualizaci. Tento nástroj je známý pro svou stabilitu a vysoký výkon, ale vzhledem k těmto požadavkům má omezený seznam podporovaných zařízení, která musí splňovat specifické certifikační požadavky pro použití s tímto produktem. VMware ESX je určen pro podnikové prostředí, kde je vyžadována vysoká dostupnost, efektivní správa a spolehlivost.[7]

5.2 Hyper-V

Hyper-V je virtualizační nástroj vyvinutý společností Microsoft, který byl poprvé vydán v roce 2008. Hyper-V je určen pro systémovou virtualizaci na platformě x86 a byl původně dostupný jako volitelná součást operačního systému Windows Server 2008. Tento nástroj umožňuje vytvářet a spravovat virtuální stroje na serverech, což přispívá k vyšší efektivitě a flexibilitě při správě infrastruktury. V současnosti je Hyper-V integrovaný přímo do Windows Serveru i některých verzí operačního systému Windows 10, což zjednodušuje nasazení a používání tohoto nástroje i pro menší organizace.[8]

5.3 Windows Sandbox

Windows Sandbox je virtualizační nástroj, který byl do operačního systému Windows 10 integrován v roce 2018 a později se objevil i v systému Windows 11. Tento nástroj je dostupný pouze v edicích Windows 10 Pro, Enterprise a Education. [9]

Windows Sandbox využívá technologii hardwarové virtualizace, která odděluje hostitelský operační systém od virtuální instance. Na rozdíl od jiných virtualizačních nástrojů nevyžaduje složité nastavení, protože funguje jako jednoduše konfigurovaná kopie hostitelského systému. Ačkoliv je tento nástroj závislý na hostitelském operačním systému,

zajišťuje dostatečnou oddělenost systémových souborů, což jej činí ideálním pro bezpečné testování aplikací nebo souborů, které by mohly být rizikové pro hlavní operační systém. [9]

5.4 KVM (Linux)

KVM (Kernel-based Virtual Machine) představuje virtualizační technologii pro operační systém Linux, která umožňuje běh více virtuálních strojů na jednom fyzickém serveru. Jedná se o řešení integrované přímo do linuxového jádra, díky čemuž je považováno za stabilní, bezpečné a výkonné. KVM proměňuje běžný Linux na plnohodnotný hypervizor a umožňuje spouštění hostovaných systémů, jako jsou například Windows, různé distribuce Linuxu nebo další operační systémy. Virtualizační vrstvy jsou spravovány pomocí nástrojů jako libvirt nebo QEMU, které poskytují další možnosti konfigurace a řízení. Velkou výhodou KVM je otevřený kód a silná komunita, což přináší široké možnosti přizpůsobení a integrace například do cloudových řešení, včetně OpenStack. Díky své flexibilitě a absenci licenčních poplatků je KVM častou volbou v prostředích, kde se klade důraz na otevřené technologie a nákladovou efektivitu. [10]

6 CLOUDOVÁ ŘEŠENÍ

Cloudová řešení představují soubor síťově propojených datacenter, která jsou rozmístěná v různých geografických lokalitách a společně vytvářejí virtuální infrastrukturu, nazývanou cloud. Tento přístup umožňuje poskytování flexibilních a škálovatelných IT služeb na základě požadavků uživatelů.[6], [11]

Moderní cloud computing staví na základech položených v éře sálových počítačů a systémů sdílení výpočetního času, které představovaly rané formy centralizovaného poskytování výpočetních zdrojů. V počátcích schématického znázorňování komplexních propojení infrastrukturních komponent se často používala metafora oblak (anglicky cloud), symbolizující abstrakci a propojenost těchto vzdálených a sdílených zdrojů, jejichž interní detaily byly uživateli skryty. [6], [11]

V dnešní době označuje termín cloud za servery připojené k internetu, které jsou dostupné z veřejné sítě a poskytují uživatelům různé služby na základě placeného pronájmu. Cloudová řešení mohou nabízet širokou škálu služeb od pronájmu konkrétních aplikací, jako jsou e-mailové nebo webové servery, až po komplexní poskytování celé IT infrastruktury. To zahrnuje například pronájem operačních systémů, virtualizovaných prostředků nebo dokonce celé servery, vše odpovídajícími licencemi a konfiguracemi. [6], [12]

6.1 Základní modely cloud computingu podle definice NIST

Cloud computing představuje model výpočetních služeb, který umožňuje vzdálený přístup k výpočetním zdrojům prostřednictvím sítě, obvykle internetu. Tento přístup je charakteristický vysokou mírou automatizace, flexibilitou při alokaci zdrojů a modely účtování založenými na skutečné spotřebě. Jedním z nejcitovanějších rámců pro klasifikaci cloudových služeb je definice poskytnutá americkým Národním institutem pro standardy a technologie (NIST), který rozlišuje tři základní modely poskytování služeb: Software as a Service (SaaS), Platform as a Service (PaaS) a Infrastructure as a Service (IaaS).[3], [11]

6.1.1 Software as a Service (SaaS)

SaaS je model, ve kterém poskytovatel cloudových služeb zajišťuje plně funkční aplikace, které jsou dostupné uživatelům přes internet. Tento model je zaměřen na koncové uživatele, kteří mají přístup k aplikacím prostřednictvím webového rozhraní, bez nutnosti instalace na

vlastních zařízeních. Uživatelé tak nemusejí řešit správu a údržbu aplikace, protože vše je zajištěno poskytovatelem služby.[12]

SaaS aplikace jsou často založeny na modelu předplatného, což znamená, že organizace platí pouze za skutečně využívané služby. Mezi nejběžnější příklady SaaS patří nástroje jako Google Workspace, Microsoft 365, Salesforce nebo Dropbox. Tyto aplikace umožňují organizacím a jednotlivcům zaměřit se na samotnou práci, aniž by museli investovat do správy a údržby IT infrastruktury. [12]

Tento model je vhodný zejména pro aplikace, které nevyžadují rozsáhlou customizaci a jsou standardizované pro širokou uživatelskou základnu. SaaS je ideální pro organizace, které chtějí rychle nasadit aplikace bez nutnosti investovat do vlastní infrastruktury. [12]

6.1.2 Platform as a Service (PaaS)

PaaS je model, který poskytuje vývojářům kompletní platformu pro vývoj, testování a nasazování aplikací, aniž by se museli starat o správu infrastruktury. Tento model poskytuje prostředí pro vývoj software, což zahrnuje operační systémy, databáze, vývojové nástroje, middleware a další komponenty, které jsou potřebné k tomu, aby mohl být software plně funkční. Výhodou PaaS je, že poskytovatel cloudových služeb spravuje celou základní infrastrukturu, zatímco vývojáři se soustředí na aplikace a jejich kód. [12]

PaaS platformy jsou ideální pro organizace, které chtějí vyvíjet a nasazovat aplikace, ale nemají zájem o správu serverů a dalších částí infrastruktury. Tento model je výhodný zejména pro vývojáře, kteří potřebují flexibilní a rychlé prostředí pro nasazení aplikací. Platformy jako Microsoft Azure App Services, Google App Engine nebo Heroku jsou příklady PaaS, které poskytují širokou škálu nástrojů pro vývojáře. [12]

6.1.3 Infrastructure as a Service (IaaS)

IaaS je model, který poskytuje uživatelům kompletní infrastrukturu, která zahrnuje virtualizované servery, úložiště a síťové komponenty. Tento model dává organizacím a jednotlivcům plnou kontrolu nad operačními systémy, aplikacemi a daty, které běží na

cloudové infrastruktury, zatímco samotnou fyzickou infrastrukturu spravuje poskytovatel cloudových služeb. [12]

IaaS je vhodný pro organizace, které potřebují větší úroveň kontroly nad svým prostředím, ale zároveň nechtějí investovat do fyzických serverů a hardwaru. Tento model nabízí flexibilitu a možnost rychlého škálování, což je ideální pro dynamicky se měnící pracovní zatížení, například pro vývojová prostředí, testování nebo provoz aplikací s vysokými nároky na výkon. [12]

Mezi největší poskytovatele IaaS patří Amazon Web Services (AWS), Microsoft Azure a Google Cloud Platform. Tyto platformy umožňují organizacím vytvářet, spravovat a škálovat vlastní IT infrastrukturu bez nutnosti vlastnit fyzické servery.[11], [12], [13]

6.2 Modely nasazení

Způsoby nasazení cloudových řešení představují různé přístupy k distribuci a správě výpočetních prostředí. Jejich výběr je podmíněn organizačními potřebami, požadavky na bezpečnost, regulačním rámcem a ekonomickými faktory. Mezi nejčastěji rozlišované modely nasazení patří veřejný, privátní a hybridní cloud, přičemž každý z nich nabízí specifické výhody i omezení.[6], [11]

6.2.1 Veřejný cloud

Veřejný cloud je model, kdy poskytovatel cloudových služeb pronajímá infrastrukturu, platformu nebo aplikace širokému okruhu uživatelů prostřednictvím veřejného internetu. Všechny prostředky (servery, úložiště, síťové komponenty) jsou spravovány třetí stranou, která zajišťuje jejich dostupnost, bezpečnost a údržbu. Uživatelé mají k těmto prostředkům přístup na základě předplacených služeb, obvykle podle modelu „pay-as-you-go“, což znamená, že platí pouze za využívané prostředky.[6], [12]

6.2.2 Privátní cloud

Privátní cloud je cloudová infrastruktura, která je určena pro využívání pouze jednou organizací. Tento model může být nasazen buď ve vlastních prostorách organizace, nebo může být hostován třetí stranou. Hlavní výhodou privátního cloudu je, že poskytuje vyšší úroveň kontroly nad daty, konfiguracemi a zabezpečením, což je ideální pro organizace, které mají specifické požadavky na ochranu citlivých informací nebo regulace, jako jsou

například banky nebo zdravotnické instituce. Mezi často využívané technologie pro budování privátního cloudu patří například OpenStack, VMware vSphere či Microsoft Azure Stack.[6], [7], [11]

6.2.3 Hybridní cloud

Hybridní cloud je kombinací veřejného a privátního cloudu, která umožňuje organizacím využívat nejlepší vlastnosti obou modelů. Uživatelé mohou například provozovat citlivé aplikace a data v privátním cloudu, zatímco méně citlivé aplikace mohou běžet ve veřejném cloudu. Vhodně navržená hybridní architektura umožňuje dynamicky přesouvat pracovní zátěž mezi jednotlivými prostředím v závislosti na aktuálních potřebách, bezpečnostních požadavcích nebo nákladech. Hybridní přístup se tak stává preferovaným řešením pro organizace usilující o rovnováhu mezi výkonem, flexibilitou a dodržováním bezpečnostních standardů. [6], [12]

6.3 Hlavní poskytovatelé cloudových služeb

Globální trh cloudových služeb je ovládán několika klíčovými poskytovateli, jejichž nabídka pokrývá široké spektrum služeb od základní infrastruktury po pokročilé analytické a vývojové nástroje. Mezi nejvýznamnější aktéry patří společnosti Amazon Web Services (AWS), Microsoft Azure a Google Cloud Platform (GCP), které společně zaujímají dominantní podíl na trhu veřejného cloudu.[12], [13], [14], [15]

Amazon Web Services je obecně považován za průkopníka v oblasti cloud computingu a dlouhodobě si udržuje vedoucí pozici zejména v segmentu IaaS. Jeho rozsáhlé portfolio služeb a flexibilita přístupu z něj činí preferovanou volbu nejen pro startupy a vývojářské týmy, ale také pro rozsáhlé korporace a organizace využívající open-source technologie.[13]

Google Cloud Platform se naopak profiluje jako poskytovatel zaměřený na data-driven řešení, strojové učení a vývoj aplikací. Nabízí pokročilé analytické nástroje, jako je BigQuery, a služby v oblasti umělé inteligence, které jej činí oblíbeným mezi datovými inženýry, vědci a vývojáři využívající moderní vývojové paradigma.[14]

Microsoft Azure si vybudoval silnou pozici díky hluboké integraci s produkty Microsoft, jako jsou Active Directory, Microsoft 365 či Windows Server, což jej činí atraktivním řešením zejména pro podnikové prostředí. Azure je rovněž lídrem v oblasti hybridních cloudových scénářů, kde umožňuje efektivní propojení on-premise prostředí s cloudovou infrastrukturou prostřednictvím nástrojů jako je Azure Arc nebo Azure Stack.[15]

Podle finančních výsledků za čtvrté čtvrtletí roku 2024 generoval Amazon Web Services roční výnos přesahující 115 miliard USD, čímž si udržel pozici lídra na trhu. Microsoft, který v rámci divize Intelligent Cloud zahrnuje Azure i další cloudové služby, dosáhl ročního běhu příjmů ve výši 102 miliard USD, což potvrzuje jeho roli silného konkurenta AWS. Google Cloud pak uzavřel čtvrtletí s výnosem 12 miliard USD, což odpovídá ročnímu běhu ve výši 48 miliard USD. Tyto hodnoty ukazují na výrazné tempo růstu cloudových služeb a potvrzují dominantní postavení Microsoftu mezi podniky, zejména díky jeho integraci do širších infrastrukturních a softwarových ekosystémů. [14], [15], [16], [16]

7 MICROSOFT AZURE

Po popisu základních principů virtualizace a jeho různých modelů je nyní vhodné zaměřit se na konkrétní poskytovatele cloudových služeb. Jedním z nejrozšířenějších poskytovatelů je Microsoft Azure, který nabízí širokou škálu služeb pro správu IT infrastruktury. Azure poskytuje řešení pro firemní i individuální uživatele a zahrnuje širokou nabídku nástrojů pro virtualizaci, správu serverů, databází a dalších komponentů.[15]

Azure se vyznačuje flexibilitou, škálovatelností a integrací s dalšími produkty od Microsoftu, což usnadňuje přechod a implementaci pro organizace, které již využívají Microsoft technologie. Umožňuje vytvářet a spravovat virtuální počítače budovat síťovou infrastrukturu, nasazovat databáze, konfigurovat bezpečnostní prvky a automatizovat správu celého prostředí. Platforma je přístupná přes webové rozhraní, CLI nástroje i REST API, což výrazně rozšiřuje možnosti správy a integrace. [15]

Pro potřeby této práce je Azure využíván především jako prostředí pro nasazení služby Azure Virtual Desktop (AVD) a jako základ pro vytvoření a správu Azure Virtual Machines. Díky propojení jednotlivých komponent v rámci jedné platformy je možné efektivně sledovat náklady, optimalizovat výkon a udržovat bezpečnostní standardy.[15]

7.1 Azure Virtual Desktop (AVD)

Služba zaměřená na poskytování virtuálních strojů pro koncové uživatele. AVD umožňuje organizacím poskytovat pracovní prostředí na dálku, což je ideální pro scénáře, kde je potřeba centralizovat správu pracovních stanic a přístup k desktopovým aplikacím z jakéhokoli zařízení.[17]

Díky tomu lze snadno provádět údržbu, aktualizace softwaru a správu bezpečnostních politik bez nutnosti zásahů do jednotlivých zařízení. Bezpečnostní opatření v rámci AVD zahrnují pokročilé nástroje, jako je šifrování dat, multifaktorová autentizace a možnost správy bezpečnostních politik, což zajišťuje ochranu citlivých informací. [17]

AVD je také plně integrovaný s Intune, což organizacím umožňuje bezpečný a kontrolovatelný přístup nad uživatelskou základnou k aplikacím a celým desktopům. Provázanost s ekosystémem Microsoftu přináší i přehledné licencování v rámci Office365.

Proto je ideálním řešením pro organizace, které hledají bezpečné, škálovatelné a flexibilní pracovní prostředí. [17], [18]

7.2 Azure Virtual Machine (VM)

Azure Virtual Machine je služba poskytující virtuální stroje v cloudu. Tyto virtuální stroje mohou sloužit jako servery, ale také jako desktopy, a můžou běžet na různých operačních systémech, jako je Windows, Linux a další. Služba umožňuje vytvářet a spravovat virtuální stroje na infrastruktuře Azure bez nutnosti vlastního hardwaru. Uživatelé si mohou vybírat z různých konfigurací podle svých potřeb, ať už jde o výkon procesoru, velikost operační paměti nebo kapacitu úložiště. Tato variabilita umožňuje nasazení virtuálních strojů pro širokou škálu využití, od vývoje a testování až po provoz náročných podnikových aplikací.[15], [18]

Podpora různých operačních systémů, včetně Windows a Linux distribucí umožňuje snadnou integraci do stávajících IT prostředí. Další výhodou je možnost dynamického škálování výkonu, díky čemuž lze pružně reagovat na aktuální potřeby aplikací a optimalizovat náklady na provoz.[15]

Virtuální stroje v Azure lze snadno propojit s dalšími cloudovými službami, jako jsou Azure Storage, Azure Networking či nástroje pro monitoring. Tato provázanost umožňuje vytvořit stabilní a bezpečné prostředí, které usnadňuje správu infrastruktury a zvyšuje její efektivitu. Azure Virtual Machine je vhodná pro scénáře, kdy organizace potřebují plnou kontrolu nad virtuálními servery a mají specifické požadavky na konfiguraci operačních systémů a aplikací. [20]

7.3 Intune

Cloudová služba Microsoft Intune slouží ke správě mobilní zařízení (MDM) a správu mobilních aplikací (MAM). Podmnožinou mobilních zařízení je možné si představit veškeré zařízení v podobě fyzických a virtuálních počítačů či mobilních telefonů. Veškeré tyto zařízení, předpisy a správa se souhrnně označuje jako end-user computing (EUC). Integrace s Azure nebo přímo s Microsoft Entra ID je vzhledem k faktu, že jsou tyto nástroje ze stejné rodiny od Microsoftu plně propojené. Narozdíl ale od dnes již staršího, avšak stále hojně využívaného hybridního řešení s pomocí on-premise Active Directory, Intune nelimituje žádné zařízení na základě operačního systému. Pomocí Intune a jeho nástrojů i v podobě

podpory skriptování je možné nasazovat a do jisté míry efektivně spravovat aplikace, zásady dodržování předpisů a primárně řídit celý životní cyklus všech registrovaných zařízení.[19]

Intune je plně spravován přes webové rozhraní, avšak pro detailnější a efektivnější práci je doporučeno využít nástroje jako je PowerShell, Azure CLI, Terraform nebo Azure Resource Manager templates. Po nainstalování a importování správných modulů, lze díky konzistenci jazyka powershellu Intune instantně spravovat. [19]

II PRAKTICKÁ ČÁST

Praktická část této práce se zaměřuje na nasazení a správu služby AVD v prostředí cloudové platformy Microsoft Azure. Cílem je detailně demonstrovat možnosti implementace této technologie, způsoby její správy a vyhodnotit její vhodnost pro různá IT prostředí s důrazem na efektivitu a automatizaci.

V rámci praktické části je popsán proces nasazení AVD, včetně konfigurace jednotlivých komponent, jako jsou hostitelské servery (s ohledem na optimální konfiguraci z hlediska efektivity týmu a potenciálního využití nástrojů pro automatizaci a orchestraci), uživatelské profily a bezpečnostní nastavení. Je analyzována správa AVD, včetně nástrojů a dostupných možností automatizace administrativních úloh s cílem minimalizovat nároky na velikost správcovského týmu u rozsáhlých instancí. V kontextu AVD je rovněž popsána správa virtuálních strojů v Azure s ohledem na jejich roli v host poolu (například jako multi-session Windows 11).

Významnou součástí práce je evaluace výkonu, nákladů a flexibility AVD. Je provedeno posouzení bezpečnostních aspektů a souladu s regulačními požadavky (compliance). Na základě získaných poznatků jsou formulována doporučení pro ideální nasazení a konfiguraci AVD v rámci efektivně fungujícího týmu, včetně návrhu na využití dalších nástrojů, které nad tímto řešením operují a umožňují snížit personální nároky na správu rozsáhlých prostředí. Srovnání se samostatnými virtuálními stroji (VM) je provedeno s ohledem na jejich specifické využití v rámci AVD host poolu.

8 NASAZENÍ AZURE VIRTUAL DESKTOP

Architektura služby je tvořena několika vrstvami, které zajišťují jak samotnou virtualizaci prostředí, tak směrování a správu uživatelských připojení. Na Obrázku č. 1 je znázorněno typické propojení komponent v rámci Azure, jak jsou propojeny a jakým způsobem dochází k navázání relace mezi uživatelem a dostupným prostředím.

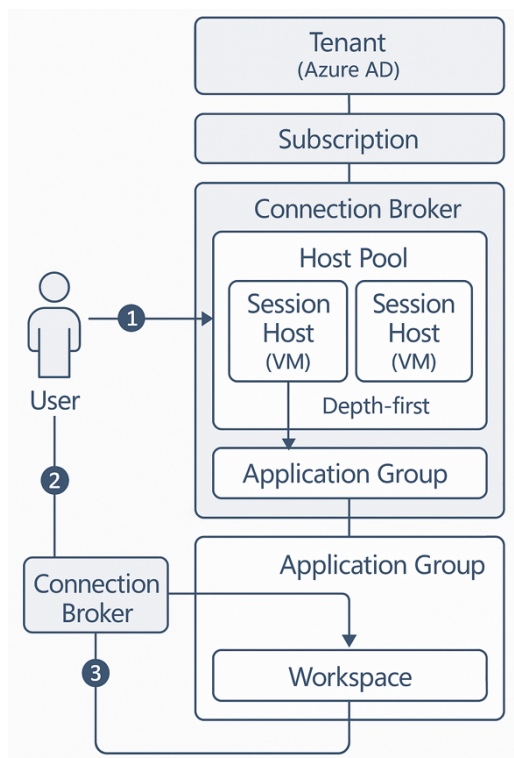
Na nejvyšší úrovni se nachází tenant, který představuje prostředí spravované prostřednictvím Azure Active Directory. V rámci něj je definována subscription, která umožňuje vytvářet a spravovat jednotlivé prostředky, mezi nimiž se nachází také logická skupina komponent AVD.

Prvkem pro směrování připojení je Connection Broker, jenž rozhoduje, na který z dostupných session hostů bude uživatel připojen. Tyto session hosty jsou organizovány do host poolu, kde každý jednotlivý stroj (virtuální počítač) může obsloužit více relací v závislosti na nastavení. V tomto případě je využit algoritmus typu depth-first, který upřednostňuje využití jednoho stroje naplno před přidělením dalšího. Tím dochází k efektivnímu využívání výpočetních prostředků.

Další komponentou je application group, která definuje, jaké aplikace nebo plochy jsou dostupné jednotlivým uživatelům. Tyto aplikace jsou následně prezentovány prostřednictvím workspace, kde si uživatel vybírá, ke které službě se připojí. Celý proces je zprostředkován přes Connection Broker, bez nutnosti přímého spojení mezi uživatelem a session hostem.

Ve výchozím nastavení prochází uživatelská komunikace přes infrastrukturu Microsoftu, což zajišťuje zabezpečení i dostupnost připojení. Pro specifické scénáře může být využita technologie ShortPath, která umožňuje přímé spojení mezi uživatelem a session hostem pomocí UDP protokolu, čímž výrazně zkracuje latenci a zlepšuje odezvu při práci. Tato funkce však vyžaduje odpovídající síťové podmínky, a není vždy k dispozici, pokud není splněna podpora pro přímé propojení.

Architektura jako celek zajišťuje oddělení jednotlivých rolí v rámci systému – autentizace, přístupová oprávnění, směrování, samotná virtualizace – a umožňuje škálovat výkon dle potřeby provozu. Tímto způsobem lze AVD efektivně nasadit jak pro malé týmy, tak pro rozsáhlé podnikové prostředí.[17], [18], [21], [22]



Obrázek 1 Architektura služby AVD a logika připojení uživatele (Depth-first)

(Zdroj: vlastní)

8.1 Plánování nasazení

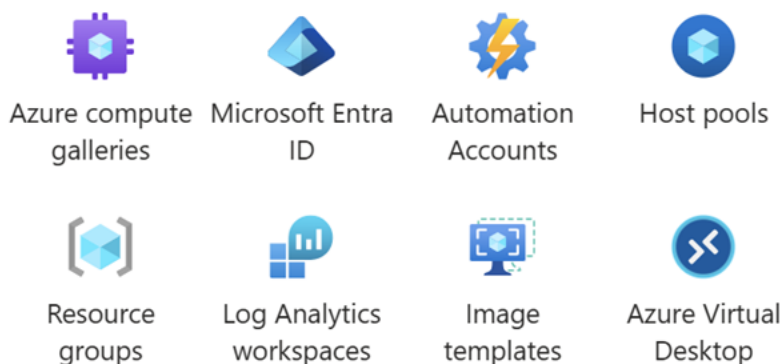
Prvním krokem při zavádění služby AVD v podniku je důkladná analýza potřeb organizace. Je nutné určit počet aplikací, které budou v rámci AVD provozovány, protože to přímo ovlivňuje výběr hardwaru a konfiguraci infrastruktury. Stejně tak je důležité znát očekávaný počet uživatelů, kteří budou AVD aktivně využívat. Neméně důležitým jsou bezpečnostní požadavky a samozřejmostí je dostupný rozpočet na plánované řešení.

Následuje příprava prostředí v rámci Microsoft Azure, kde budou služby provozovány.

To zahrnuje:

- Plně funkční doménu: Může se jednat o Microsoft Entra ID (Azure AD) nebo vlastní doménový řadič v hybridním propojení, které umožňuje správu přístupů a identit.
- Virtuální síť (VNet): Slouží pro izolaci a zabezpečení prostředí. V některých případech může být vhodné doplnit síť o VPN pro bezpečné propojení s on-premises infrastrukturou.

Správně nastavené prostředí zajistí hladký průběh implementace AVD a všech souvisejících komponent, jako jsou host pooly a session hosty.[17], [24], [25]



Obrázek 2 Výčet komponent pro správu AVD

(Zdroj: vlastní z portálu Azure)

8.2 Konfigurace

Po dokončení fáze plánování je dalším krokem samotná konfigurace prostředí Azure Virtual Desktop. Ta zahrnuje vytvoření a propojení komponent v rámci předem připravené infrastruktury.

Základní kroky konfigurace:

1. Výběr vhodného image operačního systému:

Microsoft nabízí několik předpřipravených image pro AVD, včetně verzí Windows 10 Enterprise multi-session a Windows 11 Enterprise multi-session, které umožňují více uživatelům sdílet jeden virtuální desktop. Je možné vytvořit i vlastní image s předinstalovaným softwarem dle potřeb organizace.

2. Založení a správa Host Poolu:

Host pool představuje skupinu jednoho nebo více Session hostů, ke kterým se připojují uživatelé. Při jeho vytváření se volí typ připojení:

Pooled – více uživatelů sdílí Session hosty (efektivní využití zdrojů),

Personal – jeden uživatel má přidělený vlastní virtuální stroj.

3. Nastavení aplikačních skupin (Application Groups):

Slouží k definici, které aplikace nebo celé desktopy budou konkrétním uživatelům zpřístupněny. Typy:

RemoteApp – zpřístupnění konkrétních aplikací,

Desktop – zpřístupnění celého vzdáleného desktopu.

4. Přiřazení uživatelů:

Pomocí Azure AD nebo hybridního připojení k tradičnímu AD se určují oprávnění jednotlivých uživatelů a jejich přístup k aplikačním skupinám.

5. Konfigurace síťového přístupu a zabezpečení:

Nasazení NSG (Network Security Groups) pro omezení provozu, případně Azure Firewall nebo VPN Gateway pro zajištění bezpečného přístupu z externí sítě.

Konfigurace by měla být vždy dokumentována a testována na pilotní skupině uživatelů, aby bylo možné včas odhalit a odstranit případné nedostatky v návrhu nebo výkonu prostředí.

[17], [21], [26]

8.3 Přihlášení do Azure portálu

Za předpokladu, že jsou splněny všechny nezbytné požadavky, jako je vytvoření účtu v prostředí Azure a přiřazení odpovídajících oprávnění, lze přistoupit k přihlášení do portálu na adrese <https://portal.azure.com>. Tento portál představuje hlavní nástroj pro správu a konfiguraci všech služeb a zdrojů v Azure. Po úspěšném přihlášení je uživateli zpřístupněno grafické rozhraní, ve kterém lze provádět implementaci i správu všech komponent souvisejících s Azure Virtual Desktop nebo samostatnými virtuálními stroji.

Portál je možné rozšířit o pokročilejší správu pomocí nástrojů jako Azure CLI, PowerShell nebo ARM šablon. PowerShell vyžaduje předchozí instalaci a konfiguraci příslušných modulů, které umožňují autentizaci vůči Azure a správu prostředků z příkazové řádky.

Přesto pro většinu běžných operací při nasazení a správě Azure Virtual Desktop plně postačuje přehledné grafické rozhraní webového portálu.

8.4 Vytvoření a správa předplatného (Subscription)

V prostředí Microsoft Azure neoznačuje pojem subscription pouze jednoduchý model pravidelné platby, jak ho známe například ze streamovacích služeb. V Azure jde o zásadní logický rámec, ve kterém jsou pod resource group seskupeny veškeré cloudové prostředky,

kterými jsou například virtuální počítače, databáze, úložiště nebo síťové komponenty. Každý nově vytvořený prostředek je vždy navázán na konkrétní předplatné, které určuje, kdo k němu má přístup, jak se účtuje jeho provoz, a kam patří z organizačního hlediska.

Azure nabízí více typů předplatných podle konkrétních potřeb uživatelů. Nejrozšířenější je model Pay-As-You-Go, ve kterém uživatel platí pouze za skutečně spotřebované prostředky – bez závazků a s vysokou flexibilitou. Pro velké podniky je vhodnější Enterprise Agreement, který přináší výhodnější ceny, centralizovanou správu více předplatných a možnost konsolidovaného účtování. Speciálním typem je Dev a Test subscription, které je určeno pro vývojové a testovací účely s omezením produkčního nasazení a s nižšími náklady.

Bezpečnost předplatného je zásadní pro zajištění integrity celého prostředí. K tomu slouží například Role Based Access Control (RBAC), který přesně určuje, kdo má přístup, ke kterým prostředkům a jaké operace může provádět. Mezi doporučené bezpečnostní praktiky patří také pravidelné audity, využití nástroje Azure Security Center pro monitoring hrozeb a správná konfigurace sítě včetně šifrování přenosu a firewallů. Azure navíc splňuje řadu mezinárodních bezpečnostních a legislativních standardů, což je důležité zejména pro podniky působící v regulovaných odvětvích.

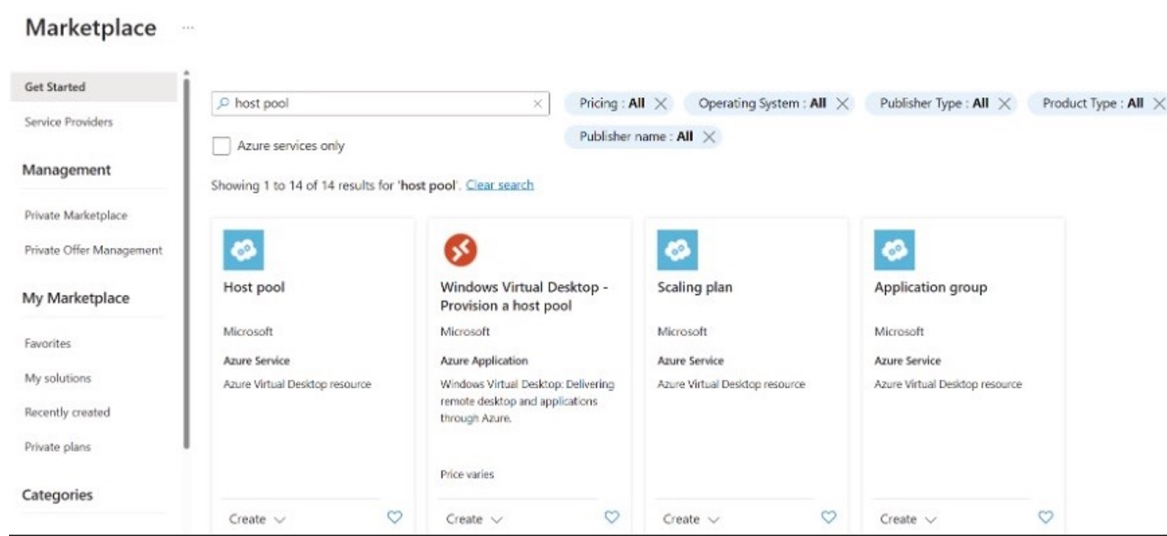
Součástí přípravy prostředí pro nasazení Azure Virtual Desktop je správné nastavení předplatného. Toto předplatné tvoří základní rámec pro správu a organizaci všech zdrojů v Azure. Umožňuje efektivně oddělit prostředky podle jednotlivých projektů, organizačních jednotek nebo geografických oblastí. [15], [22]

8.5 Nastavení přístupových práv (Access control – IAM)

Po vytvoření předplatného následuje konfigurace přístupových práv prostřednictvím funkce Access Control. Microsoft Azure využívá systém řízení přístupu založený na rolích, který umožňuje přesné přiřazení oprávnění jednotlivým uživatelům nebo skupinám v závislosti na jejich pracovních rolích a odpovědnostech.

Oprávnění lze definovat na různých úrovních – od celé úrovně předplatného, přes skupiny prostředků až po jednotlivé konkrétní prostředky. Při přiřazení role na vyšší úrovni, například na úrovni předplatného, se oprávnění automaticky dědí i na všechny podřízené části, pokud není toto dědění výslovně přepsáno. Tento přístup výrazně zjednodušuje správu oprávnění, zejména ve složitějších a rozsáhlejších prostředích.

Například role „Owner“ (vlastník) umožňuje plný přístup ke všem zdrojům v rámci dané úrovně včetně možnosti přiřazovat oprávnění dalším uživatelům. Naopak role „Virtual Machine Contributor“ umožňuje spravovat virtuální stroje, ale bez možnosti spravovat síťové komponenty nebo přístupová práva. Uživatel, kterému je přiřazena role pro Azure Virtual Desktop (např. AVD User), může pouze přistupovat ke vzdálenému desktopu, ale nemá oprávnění měnit jeho konfiguraci. Tímto způsobem lze přístup v prostředí Azure velmi detailně přizpůsobit potřebám jednotlivých týmů a současně omezit riziko nechtěných nebo neoprávněných zásahů do produkčních systémů.[17], [21], [23]



Obrázek 3: Rozhraní Marketplace.

(Zdroj: vlastní z portálu Azure)

8.6 Host Pool

Host pool tvoří základní vrstvu infrastruktury při nasazení Azure Virtual Desktop. Jeho hlavní funkcí je sdružování a správné řízení session hostů, tedy virtuálních strojů, které poskytují uživatelům přístup ke vzdálenému prostředí – ať už ve formě desktopu, nebo jednotlivých aplikací. V praxi to znamená, že host pool určuje, na jaký session host bude konkrétní uživatel připojen, jak bude fungovat přidělování relací a jakým způsobem se bude dané prostředí chovat z pohledu výkonu a dostupnosti.

Součástí konfigurace host poolu je i volba provozního režimu. Azure umožňuje dvě základní varianty. První z nich je režim pooled, ve kterém mohou jednotlivé virtuální stroje obsluhovat více uživatelů současně. Tento přístup je efektivní zejména z hlediska nákladů a provozu, a hodí se do prostředí, kde uživatelé nepotřebují vyhrazené pracovní stanice. Druhou možností je režim personal, kde má každý uživatel přiřazen svůj vlastní virtuální

stroj. Tento model nachází uplatnění především tam, kde je vyžadováno trvalé pracovní prostředí s individuálním nastavením, vyšší výpočetní výkon, nebo specifické bezpečnostní požadavky.

Vytvoření host poolu probíhá prostřednictvím služby Azure Marketplace, která slouží jako rozhraní pro nasazování jednotlivých komponent a služeb v prostředí Azure. Pomocí vyhledávacího pole lze najít příslušnou komponentu, a po kliknutí na možnost vytvoření je administrátor přeměrován do průvodce konfigurací. Zde se postupně vyplňují všechny nezbytné parametry.

Mezi základní požadavky při vytváření host poolu patří výběr předplatného, přiřazení do existující nebo nové resource group a volba geografické oblasti (location), ve které budou jednotlivé zdroje vytvořeny. Dále je potřeba zadat název host poolu, který musí být v rámci prostředí unikátní. Jedním z důležitých kroků je také výběr typu aplikační skupiny, označovaný jako preferred app group type. Tato volba určuje, zda bude host pool určen pro publikování kompletního vzdáleného desktopu, nebo pouze jednotlivých aplikací. V případě publikace aplikací běží každá z nich v kontextu uživatelského profilu na session hostu, ale uživatel ji vnímá jako samostatné okno na svém lokálním zařízení.[17], [18], [21]

Home > Marketplace >

Create a host pool

Basics Session hosts Workspace Advanced Tags Review + create

Project details

A host pool is a collection of one or more identical virtual machines within an Azure Virtual Desktop environment. Here you can give details to create Azure virtual machines for your host pool now, or you can create and add them later, for example if you plan to add virtual machines from Azure Local. [Learn more](#)

Subscription * ⓘ

Resource group * ⓘ

Host pool name *

Location * ⓘ

Validation environment ⓘ

Preferred app group type * ⓘ

Host pool details

Define how session hosts in this host pool will be created, managed, and assigned.

Host pool type *

East US

Metadata will be stored in Azure geography associated with (US) East US. [Learn more](#)

☒ No ☐ Yes

Desktop

Desktop

RemoteApp

Select a type

i If you select pooled, users can maintain their personalization and user data with FSLogix. [Learn more](#)

Obrázek 4: Rozhraní vytvoření Host pool.

(Zdroj: vlastní z portálu Azure)

8.7 Session Host

Session host představuje výpočetní prostředek, který v rámci služby Azure Virtual Desktop zajišťuje samotné poskytování vzdáleného prostředí pro koncové uživatele. Jde o standardní virtuální stroj běžící v Azure, který je přiřazen do předem vytvořeného host poolu. Po připojení uživatele prostřednictvím AVD klienta dochází k navázání relace právě na jeden z těchto virtuálních strojů.

V závislosti na konfiguraci host poolu může session host zprostředkovat buď plnohodnotné vzdálené prostředí s přístupem k desktopu, nebo zpřístupnit pouze vybrané aplikace pomocí režimu RemoteApp. To, jakým způsobem jsou uživatelé na jednotlivé session hosty směřováni, určuje nastavení vyvažování zátěže, přičemž Host Pool umožňuje různé strategie přidělování – například rovnoměrné rozložení relací napříč všemi dostupnými stroji nebo preferování určitého stroje na základě zátěže.

Při nasazení většího počtu session hostů se v praxi využívají automatizační nástroje jako ARM šablony, skripty v Bicep, PowerShell nebo Azure CLI. Tyto nástroje umožňují rychlejší a opakovatelné nasazení, udržení jednotné konfigurace napříč všemi stroji a zajišťují snadnou škálovatelnost celého řešení.

Stejně důležitou roli hraje i výběr vhodného image, ze kterého jsou session hosty nasazovány. Lze využít buď standardní obrazy poskytované Microsoftem (např. Windows 11 Enterprise Multisession s Microsoft 365 aplikacemi), nebo vlastní image přizpůsobený konkrétním potřebám organizace – například s předinstalovanými aplikacemi, úpravami registrů nebo specifickým zabezpečením.

Session hosty musí být připojeny k Azure Active Directory, případně k hybridnímu prostředí s on-premises doménou. Uživatelé k nim přistupují pomocí přihlašovacích údajů, přičemž jejich pracovní prostředí je zpravidla uloženo odděleně pomocí řešení FSLogix. Tento nástroj umožňuje připojení uživatelského profilu jako samostatného kontejneru, což výrazně usnadňuje přechod mezi různými stroji a zachování konzistentního prostředí pro uživatele.

Z hlediska provozu je možné session hosty škálovat podle aktuální potřeby. Azure Virtual Desktop nabízí možnost automatického škálování, které na základě definovaných pravidel přidává nebo odebírá jednotlivé instance v závislosti na zatížení. To umožňuje efektivnější využití prostředků a současně optimalizaci provozních nákladů. Principy a metody efektivního škálování a správy provozních nákladů jsou podrobněji vysvětleny v kapitole 10.1. [21], [22], [23]

8.8 Způsob připojení uživatelů k Azure Virtual Desktop

Způsob připojení koncových uživatelů k AVD se v praxi odvíjí především od toho, jak má daná organizace navrženou a nakonfigurovanou síťovou infrastrukturu. Mezi nejčastěji používané scénáře patří připojení přes VPN, ExpressRoute nebo přímé připojení přes internet s využitím identity spravované pomocí Entra ID (dříve Azure AD). Každé z těchto řešení má své výhody i omezení, ale z pohledu koncového uživatele je výsledný zážitek prakticky stejný. Technické detaily jako typ spojení nebo způsob směrování provozu zůstávají zcela v pozadí.

Běžný uživatel jednoduše spustí příslušnou klientskou aplikaci, zadá své přihlašovací údaje a podle přiřazených oprávnění se mu zobrazí nabídka dostupných prostředí. Může jít buď o celý vzdálený desktop, nebo o konkrétní aplikace publikované pomocí služby RemoteApp. Samotná infrastruktura AVD pak na základě aktuální dostupnosti a vytížení automaticky rozhodne, na který session host bude uživatel připojen. Díky této automatizaci není potřeba, aby se uživatel aktivně rozhodoval, na jaký stroj se připojuje.

V minulosti uživatelé k připojení využívali zejména aplikaci Microsoft Remote Desktop, která byla dostupná napříč platformami – pro Windows, macOS, Android i iOS. Přihlášení probíhá pomocí účtu, který je buď přímo vytvořený v Entra ID, nebo do něj synchronizovaný z lokálního Active Directory. Následně se uživateli zpřístupní konkrétní „workspace“, tedy kontejner s aplikacemi nebo desktopem, který mu byl přidělen IT oddělením. Workspaces bývají často rozdělené logicky, například podle organizační struktury nebo geografického regionu.

V současnosti Microsoft postupně nahrazuje Remote Desktop novou aplikací Windows App, která nabízí modernější rozhraní, lepší podporu více účtů a vyšší míru integrace s Windows 11. Windows App je dostupná ke stažení na oficiálním odkazu <https://aka.ms/WindowsApp> a stává se výchozí volbou pro připojení k AVD, zejména v nových nasazeních.

Z hlediska konzistence uživatelského profilu umožňuje FSLogix připojit uživatelský profil nezávisle na tom, na jaký konkrétní session host se uživatel přihlásí. Díky tomu má každý uživatel při každém připojení k dispozici své nastavení, data i prostředí přesně tak, jak ho opustil naposledy, což výrazně zvyšuje komfort a snižuje nároky na podporu ze strany IT.

Celý systém AVD je tedy navržen tak, aby uživatelům co nejvíce usnadnil práci – připojení je rychlé, bezpečné a především konzistentní. Veškerá složitost běží na pozadí, ať už jde o směrování relací, správu přístupů nebo zajištění dostupnosti jednotlivých služeb. [21], [23]

8.9 Uživatelské profily

Efektivní řešení této problematiky je nezbytné pro zajištění konzistentního a dostupného uživatelského prostředí bez ohledu na konkrétní virtuální stroj, ke kterému se uživatel v daný moment připojí. Pro tyto účely je v prostředí Azure Virtual Desktopu primárně doporučeno využívat technologii FSLogix. Tato technologie umožňuje oddělit uživatelská data a konfigurační nastavení od samotného operačního systému.

Prvním krokem při konfiguraci prostředí pro ukládání profilových kontejnerů je vytvoření Storage Accountu v Azure Portal. Při zakládání je nutné zvolit typ účtu, který podporuje protokol SMB, protože FSLogix komunikuje se síťovým úložištěm prostřednictvím tohoto protokolu. Doporučuje se využít variantu Azure Files Premium, která zajišťuje nízkou latenci a vyšší výkon, což je obzvláště kritické u velkých nebo výkonnostně náročných nasazení, kde latence profilů má významný dopad na uživatelský zážitek.

Po úspěšném vytvoření úložiště je třeba vytvořit nový sdílený adresář (File Share), kam se budou profilové kontejnery ukládat. Tento sdílený prostor může nést například název profileshare. Velikost File Share je třeba přizpůsobit předpokládanému objemu dat v uživatelských profilech a počtu uživatelů.

Následně je nutné povolit ověřování přístupu prostřednictvím Azure AD Kerberos, které umožňuje bezpečnou autentizaci uživatelů v rámci Azure Active Directory bez nutnosti přímé integrace se službou AD DS v on-premises prostředí. Tato možnost výrazně usnadňuje nasazení v čistě cloudových nebo hybridních scénářích.

Posledním krokem je správné nastavení oprávnění k nově vytvořenému File Share. Uživatelé, případně skupiny zabezpečení, musí mít nakonfigurovaná oprávnění jak na úrovni sdílení (share-level permissions), tak i v rámci NTFS oprávnění přímo ve struktuře úložiště. Nejčastější konfigurace zahrnuje přidání skupiny „FSLogix Users“ s oprávněními Modify na NTFS úrovni a Contributor nebo Storage File Data SMB Share Contributor na úrovni sdílení v Azure.[26]

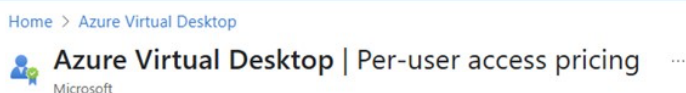
8.10 Licencování

Pro přístup k prostředí AVD musí mít každý uživatel odpovídající licenci. Microsoft využívá uživatelsky založený licenční model, což znamená, že nárok na využívání služby je vázán na konkrétního uživatele, nikoliv na zařízení nebo relaci. Přístup k AVD je zahrnut v následujících předplatných:

- Microsoft 365 E3 / E5
- Microsoft 365 Business Premium
- Windows 10/11 Enterprise E3 / E5

Tyto licence zahrnují také nárok na Windows 10/11 Enterprise Multisession, což je verze OS dostupná výhradně v Azure a umožňující přístup více uživatelům současně na jednom session hostu.

Microsoft také nabízí alternativní způsob licencování, který umožňuje zpřístupnit prostředí i uživatelům bez předchozího nároku vyplývajícího z vlastních licencí. Tento model spočívá v možnosti licencovat přístup na základě konkrétního uživatele za měsíční poplatek. V praxi to znamená, že organizace může zpřístupnit virtuální desktopové prostředí i těm pracovníkům, pro které nejsou dostupné rozsáhlejší licenční plány. Licencování je možné rozdělit podle cílového operačního systému, přičemž přístup k relacím hostovaným na Windows Serveru je cenově výhodnější než přístup k instancím operačních systémů Windows 10 nebo Windows 11 v režimu víceuživatelského nasazení. Tento způsob licencování zajišťuje flexibilitu v případech, kdy je potřeba rychle a efektivně zpřístupnit vzdálené pracovní prostředí bez nutnosti komplexní licenční infrastruktury.[29]



Obrázek 5: Rozhraní přímého uživatelského licencování.

(Zdroj: vlastní z portálu Azure)

9 NÁSTROJE PRO SPRÁVU

9.1 Automatizace pomocí Powershellu

Jedním z nejpoužívanějších nástrojů pro automatizovanou správu prostředí pomocí kódu je Microsoft PowerShell. Umožňuje správu operačních systémů Windows i cloudových služeb prostřednictvím příkazové řádky a integrovaného vývojového prostředí (IDE), jako je například Visual Studio Code. Jeho hlavní výhodou je jednoduchost v kombinaci s vysokou modularitou, což z něj činí ideální prostředek pro automatizaci úloh ve firemním prostředí i v cloudových řešeních jako je Azure.

Pro správu Azure Virtual Desktop je používán modul Az.Accounts, který je součástí širší sady modulů Az PowerShell. Pomocí těchto modulů lze kompletně spravovat prostředky v Azure – od vytváření a konfigurace resource group, přes nasazení host poolů a session hostů, až po správu přístupových práv, diagnostiku a monitoring.

V rámci automatizace nasazování a následné správy cloudových prostředků v prostředí Microsoft Azure hrají významnou roli tzv. tagy. Jedná se o jednoduché páry klíč–hodnota, které lze přiřadit téměř ke všem typům zdrojů v rámci předplatného (Subscription). Tagy slouží především k lepší organizaci, přehlednosti a zpětné identifikaci jednotlivých prostředků.

Díky správně nastaveným tagům lze vytvářet detailní reporty o využití prostředků napříč různými odděleními, projekty nebo geografickými oblastmi. Tagy rovněž umožňují přesnější sledování nákladů a následnou optimalizaci provozu, jelikož je možné přesně určit, které zdroje generují největší náklady a za jakým účelem byly nasazeny. Tímto způsobem lze efektivněji řídit rozpočet i interní vyúčtování v rámci organizace.[20]

9.2 Azure Portal

Webové rozhraní Azure Portal představuje centrální bod pro správu všech komponent cloudového prostředí Microsoft Azure. Umožňuje spravovat široké spektrum služeb – od identit a oprávnění uživatelů, přes infrastrukturu a nasazení aplikací, až po konkrétní služby jako je Azure Virtual Desktop, Azure Virtual Machine nebo RemoteApp.

Významnou předností portálu je jeho okamžitá dostupnost z různých zařízení bez nutnosti instalace jakéhokoli klienta tedy přes běžný webový prohlížeč. To umožňuje

administrátorům provádět správu prakticky odkudkoli, včetně mobilních zařízení, což výrazně zvyšuje flexibilitu a reakce schopnost v provozu.

Azure Portál však zdaleka neslouží pouze k ruční konfiguraci. Ve spojení s nástroji jako je Azure DevOps a systémem pro správu verzí (Git) je možné prostřednictvím portálu sledovat i nasazování prostředků a infrastruktury jako kódu. Tato integrace zároveň otevírá prostor pro použití automatizačních nástrojů například PowerShell DSC (Desired State Configuration) nebo Azure CLI, které umožňují efektivní vzdálenou správu a nasazení.

V kontextu správy Azure Virtual Desktop slouží Azure Portal jako intuitivní rozhraní pro nasazování a správu Host Poolů, Session Hostů a dalších prvků této služby. Kromě samotného provozu nabízí i přístup ke službám jako je Azure Monitor nebo Service Health, které umožňují podrobné sledování stavu systému, výkonu i případných výpadků.

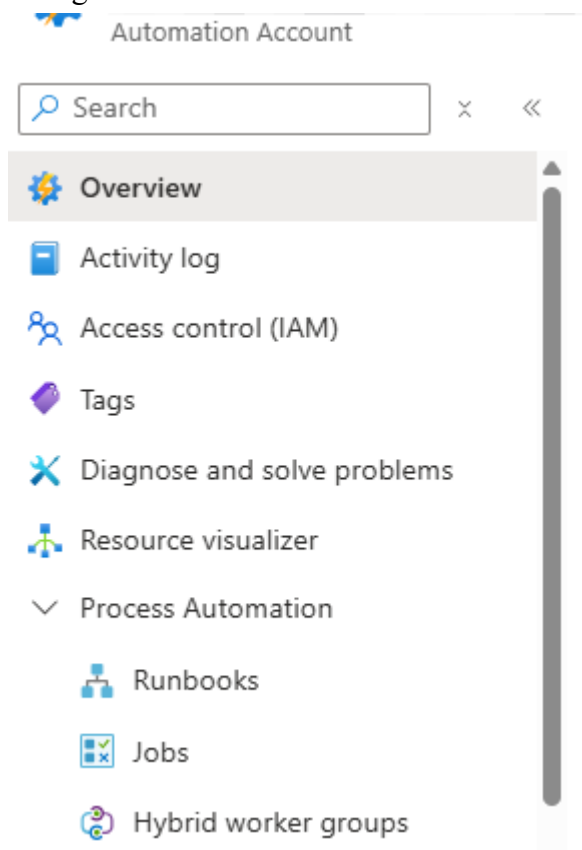
Samozřejmostí je také možnost správy Azure Virtual Machines, které představují základní výpočetní jednotky využívané jak samostatně, tak jako součást infrastruktury AVD. Portál umožňuje vytvářet nové virtuální stroje, upravovat jejich parametry, spravovat přístupová oprávnění, disky i síťová rozhraní. Tím se Azure Portál stává zásadním nástrojem nejen pro správu desktopového prostředí, ale také pro celkovou správu virtualizace v Azure, což odpovídá zaměření této práce.

9.3 Automation Accounts

Součástí prostředí Azure Portal je nástroj Automation Accounts, který poskytuje prostředky pro správu automatizačních procesů v cloudovém prostředí. Tyto prostředky jsou nazývané runbooks, tedy předpisy nebo skripty, pod kterými jsou definované opakované operace. Runbooks mohou pokrývat různé oblasti správy prostředků, jako je například nasazování, konfigurace nebo plánovaná údržba virtuálních strojů a dalších služeb.

Runbooky lze vytvářet v několika podobách, přičemž systém podporuje skriptovací jazyky PowerShell a Python. Kromě toho je možné využít také grafický editor přímo v prostředí Azure Portal, který umožňuje vizuální návrh a úpravy bez nutnosti psaní kódu. Tento přístup je vhodný zejména v případech, kdy je požadována vyšší přehlednost nebo spolupráce více správců s různou úrovní technických znalostí.

Automatizace pomocí runbooks přináší úsporu provozních nákladů, eliminuje rutinní manuální zásahy a zároveň zvyšuje spolehlivost a konzistenci v prováděných úkonech. Díky možnostem plánovaného spouštění nebo napojení na konkrétní události je možné provoz prostředí Azure Virtual Desktop i Azure Virtual Machines efektivně řídit a přizpůsobit specifickým požadavkům organizace.



Obrázek 6: Rozhraní automation account.

(Zdroj: vlastní z portálu Azure)

9.4 Azure CLI (Command-Line Interface)

Azure CLI představuje nástroj pro správu cloudových prostředí Microsoft Azure prostřednictvím příkazového řádku. Tento nástroj je dostupný přímo ve webovém rozhraní Azure Portal, kde lze spustit Cloud Shell, prostředí, které umožňuje okamžité provádění příkazů bez nutnosti instalace na lokální zařízení.

Pro správné fungování Cloud Shellu je nezbytné mít vytvořený a aktivovaný příslušný SA(Storage Account), který slouží k uchovávání prostředí a dat potřebných pro běh shellu. Po jeho aktivaci je možné začít využívat plnou funkcionalitu Azure CLI přímo v prohlížeči.

Syntaxe příkazů v Azure CLI se do určité míry podobá PowerShellu, avšak jedná se o samostatný nástroj s odlišnou strukturou příkazů i modulárním systémem. Azure CLI je postavené na architektuře příkazů ve stylu Unix/Linux a pracuje se sadou vlastních příkazů začínajících prefixem `az`, např. `az vm create`, `az group list` apod. Na rozdíl od PowerShellu nepoužívá tzv. `cmdlets`, ale pracuje s jednodušší strukturou příkazů, často využívanou v automatizačních skriptech a DevOps scénářích.

Díky multiplatformnímu charakteru lze Azure CLI provozovat na různých operačních systémech včetně Windows, macOS i Linux. Nabízí možnost správy celé infrastruktury – od vytváření `resource group`, přes nasazování virtuálních strojů a `host poolů`, až po správu síťových rozhraní a přístupových politik. Vzhledem ke své přehlednosti a podpoře integrace do CI/CD nástrojů je Azure CLI často voleno jako nástroj pro automatizaci správy cloudových prostředí. [18], [20]

10 PROVOZNÍ ŘÍZENÍ A METODY PRO SPRÁVU

10.1 Škálování

Jedním z nejdůležitějších nástrojů pro plně automatizovaný provoz session hostů v rámci AVD je scaling plan česky plán škálování. Tento prvek, který lze konfigurovat ve vyhrazené části rozhraní host poolu, slouží k efektivnímu řízení počtu aktivních instancí. Tímto způsobem je možné optimalizovat provozní náklady a předejít zbytečnému využívání prostředků v době, kdy nejsou aktivně využívány.

Pro každý host pool může být scaling plan nakonfigurován individuálně, což umožňuje vytvořit flexibilní řešení odpovídající konkrétním provozním potřebám. Dále je možné systém nastavit tak, aby při připojení prvního uživatele došlo k automatickému spuštění první instance, i když jsou všechny session hosty aktuálně ve vypnutém stavu. Díky tomu nemusí být v daném okamžiku aktivní žádná běžící virtuální instance.

Tento přístup má však i svá rizika. V případě, že jsou všechny session hosty vypnuté ve stavu deallocated, nejsou k nim přiřazeny žádné výpočetní prostředky ani jiné hardwarové komponenty, které by bylo možné v daný moment rezervovat. Z důvodu že, tyto prostředky jsou přiděleny až v okamžiku spuštění. A protože konfigurace každého stroje definuje konkrétní velikost instance, může nastat situace, kdy daný typ prostředků není v dané chvíli v lokaci poskytovatele dostupný. V takovém případě je nutné provést realokaci na jiný dostupný typ virtuálního stroje.

Tato změna však může mít dopad na náklady, a proto je vhodné zvážit založení technického požadavku (Microsoft Support case) s žádostí o kompenzaci. Realokaci je možné provést prostřednictvím rozhraní Azure na profilu VM v sekci size. V případě, že je potřeba přesunout větší množství instancí (např. desítky až stovky), je efektivní využít automatizovaný skript.[35], [33]

10.2 Aktualizace software

Výzva při správě rozsáhlé infrastruktury s větším počtem session hostů a host poolů je pravidelná aktualizace softwaru. Tato problematika se netýká pouze podkladního operačního systému, ale zahrnuje i jednotlivé aplikace a komponenty využívané koncovými uživateli.

Společnost Microsoft vydává bezpečnostní a funkční aktualizace operačních systémů v rámci tzv. „Patch Tuesday“, který připadá na druhé úterý v měsíci. Pomocí

automatizovaných procesů, jako jsou runbooky, je možné efektivně udržovat aktuální stav většího množství session hostů bez nutnosti ručních zásahů. Tento přístup výrazně zjednodušuje správu a umožňuje rychlé nasazení bezpečnostních oprav v celé infrastruktuře.

Pro distribuci aktualizovaných verzí operačního systému a aplikací napříč geografickými oblastmi se využívá služba Azure Compute Gallery. Díky ní lze spravovat jednu hlavní (tzv. „gold“) image, která se následně replikuje do jednotlivých regionů. Tímto způsobem se výrazně snižuje časová a administrativní náročnost aktualizací a zároveň se zajišťuje jednotné prostředí napříč celou infrastrukturou.

V případech, kdy je potřeba distribuovat specifický software pouze do určité oblasti, je možné vytvořit regionální kopii hlavní image a upravit ji podle konkrétních požadavků. Tento přístup umožňuje cílenou konfiguraci bez negativního dopadu na ostatní části prostředí.

K instalaci lokálních programů a přizpůsobení nastavení slouží předem připravené shell skripty. Tyto skripty zjednodušují správu, umožňují rychlé změny a výrazně snižují riziko chyb při manuálním zásahu. Automatizované nasazení navíc usnadňuje škálování prostředí a zajišťuje konzistentní konfiguraci nových instancí.

Využitím těchto metod je možné dosáhnout efektivní a flexibilní správy aktualizací softwaru v celé infrastruktuře. Pro organizace s rozšířenou infrastrukturou nebo specifickými požadavky na správu může být vhodné využít řešení třetích stran, která nabízejí dodatečné funkcionality a optimalizaci provozu. Mezi tato řešení patří například platforma Nerdio, která poskytuje nástroje pro automatizaci a správu Azure Virtual Desktop. Nerdio umožňuje efektivní nasazení a konfiguraci AVD prostřednictvím předdefinovaných šablon, optimalizaci nákladů dynamickým škálováním a rozšířený monitoring výkonnostních parametrů.[18], [22]

11 EVALUACE A SROVNÁNÍ AVD A AVM

Obě možnosti staví na infrastruktuře Azure, ale liší se přístupem k poskytování prostředí koncovým uživatelům i způsobem správy. Zatímco běžná virtuální mašina nabízí izolovaný provoz jednotlivého zařízení, AVD přináší centralizovaný víceuživatelský přístup v rámci jednoho host systému. Právě kvůli častému překrývání v praxi a možnosti zvolit pro stejný účel jednu nebo druhou variantu má smysl obě služby podrobně porovnat z pohledu výkonu, nákladů, vhodnosti nasazení, flexibility, bezpečnosti a souladu s firemními pravidly (compliance). Toto porovnání může napomoci při rozhodování, jaký přístup zvolit pro konkrétní potřeby organizace.

11.1 Výkon

Diskové úložiště hraje zásadní roli při spouštění operačního systému, práci s uživatelskými profily a načítání aplikací. Microsoft Azure nabízí několik variant diskových služeb, které se liší latencí, rychlostí přenosu dat (IOPS), perzistencí dat a cenou.

Tabulka 1: Porovnání výkonu dle použití typu disků.

Typ disku	Latence	IOPS	Vhodné použití
Standard HDD	Vysoká	Nízké	Testování, nenáročné scénáře
Standard SSD	Střední	Průměrné	Běžné produkční nasazení
Premium SSD	Nízká	Vysoké	Víceuživateleské, vyšší zatížení
Ephemeral OS Disk	Extrémně nízká	Vysoké	Pouze pro AVD, bez perzistence

(zdroj: vlastní)

Standard HDD je cenově nejdostupnější varianta, založená na klasickém magnetickém disku. Vzhledem ke své vysoké latenci a nízkému IOPS je vhodná zejména pro testovací prostředí nebo málo využívané systémy, kde výkon není prioritou.

Standard SSD využívá flash paměť s lepší odezvou než HDD, ale stále patří mezi levnější varianty. Vhodná je pro běžná produkční prostředí, kde se očekává průměrné zatížení.

Premium SSD přináší nízkou latenci a vysoký výkon, čímž je ideální pro aplikace s nároky na rychlou odezvu například víceuživatelské AVD prostředí, databázové systémy nebo webové aplikace s intenzivními operacemi nad diskem.

Ephemeral OS disk se ukázal jako nejrychlejší varianta pro AVD. Vzhledem k tomu, že se data neukládají trvale (neexistuje persistentní OS disk), je start relace znatelně rychlejší – přibližně o 30–50 % ve srovnání se Standard SSD. Tento typ disku je ideální pro scénáře,

kde je požadována rychlost a zároveň se využívá FSLogix pro správu uživatelských profilů, protože FSLogix ukládá profily na externí úložiště a nezávisí na perzistenci OS disku.

Pro dosažení vysokého výkonu je zásadní výběr správné size virtuálního stroje. Microsoft nabízí širokou škálu výpočetních instancí, které lze přizpůsobit podle požadavků konkrétního scénáře. Pro náročnější grafické aplikace lze využít například:

- NV-series: GPU akcelerované VM s NVIDIA Tesla M60, vhodné pro vizualizace, CAD a virtualizaci desktopů.
- NC-series: Výpočetně náročné úlohy, strojové učení, simulace. Obsahují GPU Tesla K80 nebo V100.
- NVadsA10 v5-series: Moderní grafické akcelerátory NVIDIA A10, optimalizované pro AVD, s možností konfigurace podle počtu virtuálních GPU (vGPU).

AVD podporuje i zapnutí GPU akcelerace (GPU-accelerated rendering), která výrazně zlepšuje uživatelský zážitek v aplikacích s grafickým rozhraním. Pro použití je nutné nainstalovat odpovídající ovladače a použít podporované VM typy.[33], [36]

11.2 Náklady

Jedním z rozhodujících faktorů při výběru mezi AVD a klasickými VM je ekonomická náročnost jejich provozu. I když se obě varianty opírají o stejnou infrastrukturu Azure, jejich nákladové modely se liší nejen způsobem účtování, ale i efektivitou využití prostředků.

Azure VM funguje na modelu IaaS což znamená, že každý virtuální stroj je provozován samostatně a zákazník platí za alokované prostředky, a to konkrétně za výpočetní výkon (vCPU, RAM), úložiště a případně i síťový provoz. V praxi to znamená, že pokud chce organizace poskytnout pracovní prostředí deseti uživatelům, musí vytvořit deset samostatných VM instancí, což je nákladné jak na provoz, tak na správu.

Oproti tomu AVD, které spadá do modelu DaaS umožňuje víceuživatelský přístup multisession. Jeden výkonnější virtuální stroj může současně obsluhovat několik uživatelů. Pokud vezmeme reálný příklad, pro deset uživatelů lze vystačit se dvěma instancemi VM typu D4as v5 (každá se 4 vCPU a 16 GB RAM), které jsou zapojeny jako session hosty do jednoho AVD host poolu. Cena jedné takové VM instance se pohybuje kolem 3 200 Kč měsíčně (při standardním „Pay-As-You-Go“ modelu bez rezervací), celkem tedy cca 6 400

Kč měsíčně. Naproti tomu nasazení deseti individuálních VM by znamenalo náklad v rozmezí 30–35 tisíc Kč měsíčně, v závislosti na velikosti instance, typu disku a regionu.

Dalším klíčovým rozdílem je licencování. U AVD lze využít stávající licence Microsoft 365 (např. E3/E5 nebo Business Premium), které v sobě již obsahují nárok na využití AVD prostředí. Není tak nutné pořizovat další specifické licence pro operační systém. Naproti tomu samostatné VM vyžadují buď vlastní Windows Server licenci, nebo aktivaci prostřednictvím tzv. Azure Hybrid Benefit – což sice může snížit náklady, ale vyžaduje, aby organizace měla k dispozici odpovídající on-premises licence.

Specifickou kapitolou jsou náklady na úložiště. AVD typicky využívá Azure Files Premium pro ukládání uživatelských profilů prostřednictvím technologie FSLogix. Tento centralizovaný přístup umožňuje snížit datovou redundanci, zjednodušit zálohování a zrychlit přihlašování uživatelů napříč různými relacemi. Náklady na prémiové sdílené úložiště o velikosti 200 GB (dostatečné pro desítky uživatelů) se pohybují kolem 1 000 Kč měsíčně.

Je důležité zmínit i skryté náklady, jako je monitoring, bezpečnostní audit nebo zálohování. Obě varianty tedy AVD i VM mohou využívat služby jako Azure Monitor, Log Analytics nebo Defender for Cloud, jejichž náklady se pohybují podle objemu přenesených dat a četnosti dotazů. Pro běžné nasazení je však třeba počítat s rezervou kolem 300–500 Kč měsíčně.

Přestože účtování není přímo na uživatele, v praxi lze odhadnout průměrné náklady na uživatele na základě celkových nákladů a počtu uživatelů. Například:

V jednom reálném scénáři s přibližně 250 uživateli činily měsíční náklady na základní logy a služby kolem 10 £, což odpovídá přibližně 300 Kč měsíčně.

V jiném případě s 100 zařízeními a různými logovacími službami byly měsíční náklady kolem 25 £, tedy přibližně 750 Kč

Celkově lze říct, že při nasazení pro více uživatelů je AVD výrazně ekonomičtější, a to nejen v oblasti výpočetních prostředků, ale také v oblasti správy a licencování. VM naopak zůstává vhodnější pro individuální a specifické scénáře, kde je třeba naprostá izolace, specifická konfigurace nebo trvalý přístup. [27]

11.3 Vhodnost nasazení

AVD je vhodný především pro organizace, které potřebují centralizované a víceuživatelské prostředí s možností sdílení výpočetních zdrojů. Díky multisession architektuře umožňuje efektivní využití hardwarových prostředků a tím snižuje náklady na provoz. Tento přístup je vhodný zejména pro scénáře, kde uživatelé využívají podobné aplikace a pracovní postupy, například kancelářské aplikace, vzdálený přístup k podnikovým systémům či školicí prostředí.

Naopak VM poskytují izolované a dedikované prostředí, které je vhodné pro specifické případy, kdy je nutné mít plnou kontrolu nad konfigurací operačního systému a aplikací. VM jsou preferovanou volbou pro náročné aplikace, které vyžadují unikátní nastavení, či pro provoz prostředí s vysokými bezpečnostními požadavky, kde izolace jednotlivých instancí hraje klíčovou roli. VM rovněž lépe vyhovují scénářům, kde je potřeba provozovat aplikace neslučitelné s víceuživatelským přístupem AVD.

Celkově je tedy vhodnost nasazení obou řešení závislá na konkrétních požadavcích organizace, počtu uživatelů, typu aplikací a požadované úrovni kontroly nad systémem.

11.4 Flexibilita

Flexibilita spočívá především ve schopnosti efektivně škálovat počet uživatelů a přizpůsobovat výkon hostitelských strojů dle aktuální potřeby. Multisession přístup umožňuje na jednom fyzickém nebo virtuálním stroji provozovat více uživatelských relací, což zvyšuje efektivitu využití zdrojů. Správa AVD prostředí je centralizovaná, což usnadňuje nasazení aktualizací a správu uživatelských profilů prostřednictvím nástrojů jako FSLogix.

Na druhé straně Azure Virtual Machines nabízejí vysokou míru přizpůsobení na úrovni operačního systému, softwaru a síťových konfigurací. Každá VM je samostatná instance, kterou lze konfigurovat individuálně, což umožňuje nasazení specifických řešení a testovacích prostředí. Nevýhodou je větší náročnost na správu a škálování, protože každá VM vyžaduje samostatnou údržbu a monitorování.

Z hlediska flexibility tedy AVD poskytuje jednodušší škálovatelnost a centralizovanou správu vhodnou pro standardizovaná prostředí, zatímco VM umožňují detailní konfigurace vhodné pro náročné a individuální scénáře. [17]

11.5 Bezpečnost

Bezpečnostní model Azure Virtual Desktop je založen na centralizaci dat a řízení přístupu. Data jsou uložena v cloudu, nikoli na koncových zařízeních uživatelů, což snižuje riziko jejich ztráty nebo odcizení. AVD podporuje vícefaktorovou autentizaci, integraci s Azure Active Directory a možnost aplikovat bezpečnostní politiky na úrovni hostitelských serverů i uživatelských relací. Microsoft rovněž pravidelně aktualizuje služby a infrastrukturu, čímž minimalizuje bezpečnostní rizika.

Azure Virtual Machines poskytují plnou kontrolu nad bezpečnostní konfigurací systému, což umožňuje detailní nastavení firewallů, antivirových řešení a dalších bezpečnostních opatření. Ovšem tato odpovědnost leží zcela na správci VM, který musí zajistit správnou aktualizaci a monitoring bezpečnostních událostí. Izolace jednotlivých VM může být výhodou v prostředích vyžadujících vysokou míru bezpečnostní segregace.

V kontextu bezpečnosti tedy AVD nabízí výhodu centralizace a jednoduchosti správy, zatímco VM umožňují větší kontrolu a přizpůsobení bezpečnostních opatření. [22]

11.6 Compliance

V prostředí Azure Virtual Desktop hraje otázka souladu s předpisy důležitou roli. Díky tomu, že AVD běží v rámci cloudového prostředí Microsoft Azure, je možné využít jednotný způsob řízení bezpečnosti a přístupu, který je ve většině případů mnohem jednodušší a efektivnější než v klasické on-premise infrastruktuře.

Azure nabízí nástroje, které pomáhají organizacím naplňovat požadavky různých legislativ, jako je například GDPR, HIPAA nebo normy typu ISO 27001. Microsoft pravidelně prochází audity a publikuje certifikace, které potvrzují soulad jeho služeb s mezinárodními standardy. Součástí prostředí jsou také nástroje pro sledování a řízení souladu, které umožňují IT týmu včas identifikovat nedostatky a reagovat na ně.

Velkou výhodou je možnost nastavit podmínky, za jakých se může uživatel připojit do prostředí – a to jak z hlediska zařízení, které používá, tak i s ohledem na to, odkud se připojuje a zda splňuje nastavené bezpečnostní požadavky. K tomu slouží tzv. Conditional Access Policies, které umožňují vynutit například dvoufázové ověření, zakázat přístup z nedůvěryhodných lokalit, nebo povolit přístup jen z firemních zařízení. Tyto podmínky tak výrazně omezují možnosti zneužití přístupu a zároveň pomáhají naplňovat požadavky na bezpečnost dat.

Dalším nástrojem, který podporuje řízení souladu, je Azure Policy. Umožňuje vytvářet pravidla, která definují, co může nebo nesmí být v rámci infrastruktury nasazeno. Omezení na konkrétní geografickou oblast u datových úložišť nebo automatické šifrování disků. Pravidla se navíc dají aplikovat plošně napříč prostředím a spravovat centrálně, což usnadňuje dohled nad jejich dodržováním.

Zatímco u AVD jsou tyto nástroje přirozenou součástí celého řešení, v případě klasických virtuálních strojů si musí organizace většinu věcí nastavovat a hlídat sama. To zahrnuje nejen šifrování disků nebo auditování přístupů, ale i ruční nastavení pravidel připojení a bezpečnostních politik. Takový přístup je často náročnější na čas i odborné znalosti a může vést k chybám nebo opomenutím. I proto bývá AVD z pohledu souladu s předpisy v mnoha situacích praktičtější variantou.

11.7 Porovnání nákladů dle jednotlivých případů

Odhadování celkových nákladů spojených s provozem cloudových řešení, jako jsou AVD nebo Citrix, je komplexní úkol, který vyžaduje zohlednění celé řady faktorů. Nejde pouze o přímé náklady na výpočetní výkon nebo úložiště, ale i o méně zřejmé položky, jako jsou náklady na síťový provoz v rámci Azure (např. výstupní data), zálohování, monitoring, alerting nebo licencování doplňkových služeb. Tyto aspekty se mohou výrazně promítnout do celkového TCO (Total Cost of Ownership). Proto je důležité při kalkulaci nákladů uvažovat v širším kontextu, nejen z pohledu technického, ale také provozního a bezpečnostního.

11.7.1 Cloudové řešení s užitím AVD

Uvažujme modelovou firmu o 10 zaměstnancích, která se rozhodla zcela využívat své pracovní prostředí pouze v cloudu pomocí služby AVD. Firma neprovozuje žádnou vlastní serverovou infrastrukturu a upřednostňuje model bez vstupních investic do hardware či licencí pro on-premises systémy tedy plně založený na OPEX (operating expense).

Hlavním požadavkem firmy je poskytnout zaměstnancům bezpečný, flexibilní a výkonný vzdálený přístup ke sdílenému desktopovému prostředí, které bude využíváno pro běžné kancelářské aplikace (M365 aplikace) a klienta podnikového informačního systému (SAP, s databázovým serverem běžícím mimo AVD hosty). Toto prostředí má být dostupné odkudkoliv (bez závislosti na firemní síti či VPN). Firma požaduje možnost centrální správy,

zálohování profilů a monitoring výkonu systému. Všichni zaměstnanci již využívají licenci Microsoft 365 Business Premium, která obsahuje i potřebné právo na využívání AVD.

Pro odhad výkonu a počtu session hostů je klíčová hustota uživatelů na virtuální stroj, která se liší dle intenzity a typu používaných aplikací. Pro uvedené aplikace (Excel, Outlook, klient SAP) a předpokládanou střední uživatelskou zátěž je vhodný poměr přibližně 1,5 až 2 vCPU a 4 GB RAM na uživatele. Pro zajištění lepšího výkonu a stability dvě VM typu D8as v5 (8vCPU, 32 GB RAM). To zajistí dostatečný výkon i při vyšší souběžné zátěži a poskytne prostor pro růst. [27]

Tabulka 2: Základní náklady na provoz AVD.

Komponenta	Popis	Cena (měsíčně)
Microsoft 365 Business Premium	10 uživatelů	4 335
2 × D8as v5 (8vCPU, 32 GB RAM)	S Session hosty, 2 VM (včetně OS disku, předpoklad 24/7 provozu bez optimalizace)	10 000
Azure Files Premium (FSLogix)	200 GB úložiště pro profily (cca 0,20 €/GB)	1 020
Monitoring + Log Analytics	Základní diagnostika	383
Celkem (odhad)	Bez rezervací a bez Hybrid Benefit	15 738 Kč / měs.

(zdroj: vlastní)

Tabulka 3: Roční odhad nákladů.

Typ nákladu	Roční výše (Kč)
OPEX (provozní)	≈ 188 856

(zdroj: vlastní)

Je důležité podotknout, že uvedená cena za virtuální stroje předpokládá jejich běh 24/7. V reálném nasazení Azure Virtual Desktopu lze náklady na session hosty výrazně snížit (často o 50–70 %) implementací autoscalingu. Ten vypíná nebo snižuje počet session hostů mimo pracovní dobu nebo při nízké zátěži, čímž optimalizuje využití prostředků a minimalizuje náklady. Cloudové nasazení pomocí AVD je ideálním řešením pro malé a střední firmy, které chtějí flexibilitu, jednoduchost a dostupnost moderního prostředí bez investic do fyzické infrastruktury. Přestože přináší určitou míru závislosti na cloudové konektivitě a

ukládání dat mimo firmu, tyto nevýhody jsou často kompenzovány vysokou mírou zabezpečení, škálovatelnosti a provozní efektivity. V prostředí, kde není vyžadováno udržení dat výhradně on-premises, jde o technologicky i finančně výhodné řešení. [27], [29]

11.7.2 Hybridní řešení s Citrix Virtual Apps and Virtual Desktops

Alternativou k plně cloudové infrastruktuře, jako je Azure Virtual Desktop, je nasazení virtuálního desktopového prostředí formou hybridního modelu s využitím platformy Citrix Virtual Apps and Desktops. Tento přístup kombinuje provoz vybraných částí infrastruktury v prostředí vlastní organizace (on-premise) s hostováním aplikačních serverů nebo desktopových session hostů v prostředí Microsoft Azure. Výsledkem je řešení, které umožňuje firmám zachovat větší míru kontroly nad komponentami systému, přičemž zároveň využívají výhod škálovatelnosti a dostupnosti veřejného cloudu.

Z pohledu architektury je v tomto scénáři provozována většina řídicích komponent Citrix infrastruktury v datovém centru organizace. Jedná se zejména o Delivery Controller, který zajišťuje správu připojování uživatelů a přiřazování zdrojů, dále o StoreFront, sloužící jako rozhraní pro přístup uživatelů k dostupným aplikacím a desktopům, a o Citrix Director, nástroj pro monitoring a správu výkonu celé infrastruktury. V některých případech je do on-premises části zařazena i licenční služba Citrix, případně Profile Management, pokud není zajištěn prostřednictvím jiné technologie.

Pro samotné poskytování aplikačního nebo desktopového prostředí uživatelům jsou využívány virtuální stroje hostované v Azure, které fungují jako session hosty. Tyto stroje jsou součástí delivery grup definovaných v Citrix Studio, kde administrátor nastavuje logiku přiřazení uživatelů a přístup k jednotlivým zdrojům. Komunikace mezi on-premises komponentami a cloudovými session hosty je zajištěna buď prostřednictvím VPN tunelu nebo pomocí služby Azure ExpressRoute, která nabízí garantovanou latenci a vyšší bezpečnost propojení oproti běžnému veřejnému internetu.

Z hlediska licencování je nutné zajistit několik samostatných oblastí. V první řadě je nutné zakoupit Citrix Virtual Apps and Desktops licence, typicky v modelu Concurrent nebo User/Device. V prostředí menší firmy o 10 zaměstnancích se jeví jako nejvýhodnější model per user, kde je každému uživateli přiřazena licence pro neomezený přístup k desktopům a aplikacím. Tyto licence se pořizují v ročním předplatném nebo formou trvalých licencí s možností předplatného pro aktualizace a podporu. Cena se pohybuje přibližně od 4 000 do

5 000 Kč za uživatele a rok, v závislosti na úrovni edice (Standard, Advanced nebo Premium).

Dále je třeba zohlednit náklady na provoz fyzické infrastruktury. V organizaci je nutné vyhradit alespoň dva redundantní servery pro běh Citrix DDC a StoreFront komponent. Tyto servery lze provozovat na existující virtualizační platformě (např. VMware vSphere nebo Microsoft Hyper-V), nebo nasadit dedikovaná zařízení. Celková investice do této části infrastruktury se pohybuje kolem 150 000 Kč, zahrnující základní hardware, potřebné licence a operační systémy.

K propojení on-premises infrastruktury s prostředím Azure je nutné zajistit odpovídající síťové rozhraní. Může se jednat o běžné VPN napojení, které je relativně levné na pořízení i provoz, nicméně má omezenou propustnost a nelze garantovat stabilní latenci. Pro náročnější provoz je vhodné využít ExpressRoute, které nabízí garantované SLA a nižší latence, ovšem za výrazně vyšší měsíční poplatky, které se pohybují od 10 000 Kč měsíčně a výše, v závislosti na konfiguraci a poskytovateli konektivity.

Pro samotné session hosty nasazené v Azure je počítáno s využitím strojů řady D4as v5, které disponují čtyřmi virtuálními jádry a 16 GB RAM. Pro deset uživatelů postačí dva tyto stroje v režimu vyvažování zátěže. Každý stroj představuje náklad přibližně 4 500 Kč měsíčně, doplněný o náklady na datové disky, zálohování a monitoring, které činí zhruba 1 000 až 1 500 Kč měsíčně na stroj.

Tento hybridní model přináší několik výhod. Organizace má plnou kontrolu nad autentizací, správou přístupů i vlastními politikami. Zároveň je možné flexibilně škálovat aplikační servery podle aktuálních potřeb. Veškerá data, identity i řídicí logika zůstávají v interním prostředí organizace, což je důležité pro firmy s přísnými bezpečnostními požadavky nebo regulacemi na ochranu dat. Citrix navíc nabízí bohatou sadu funkcí pro správu a diagnostiku, které mohou přesahovat možnosti standardního AVD.

Na druhou stranu je třeba počítat s vyšší komplexitou celého řešení. Administrace hybridní infrastruktury vyžaduje pokročilé znalosti nejen v oblasti Citrix technologií, ale i ve správě sítí, Azure prostředí a bezpečnostních politik. Oproti AVD je zde rovněž vyšší vstupní investice do infrastruktury a licencí. Správa dvou rozdílných prostředí (on-premises a cloud) klade větší nároky na koordinaci a konzistenci nastavení. Tato varianta je tak vhodná spíše pro firmy s vlastním IT oddělením nebo s externím partnerem, který zajišťuje dlouhodobou správu.[31], [32]

Tabulka 4: Kombinované náklady na provoz AVM a Citrix.

Citrix licence (User)	10 uživatelů × 4 500 Kč / rok	OPEX	45 000 / rok
Azure D4as v5 VM (2 ks)	Session hosty v Azure (4vCPU, 16 GB RAM), 2 VM × 4 500 Kč / měs.	OPEX	9 000 / měs.
Disky, zálohy, monitoring (2 VM)	Odhad 1 250 Kč / VM	OPEX	2 500 / měs.
VPN Gateway / ExpressRoute	Připojení k on-premises síti (ExpressRoute min.)	OPEX	10 000 / měs.
Fyzická infrastruktura (on-prem)	2 redundantní servery + OS a virtualizační SW	CAPEX	150 000
Citrix řídicí komponenty (on-prem)	DDC, StoreFront, Director, License server (běh na vlastním HW)	CAPEX	v ceně výše
Síťová infrastruktura	Základní síťové vybavení, UPS, záloha	CAPEX	cca 30 000
Správa a monitoring (interní/externí)	IT podpora (odhad pro SMB firmu – 1 FTE/externí partner)	OPEX	15 000 / měs.

(zdroj: vlastní)

Tabulka 5: Roční odhad nákladů (OPEX + CAPEX)

Typ nákladu	Roční výše (Kč)
OPEX (provozní)	≈ 950 000
CAPEX (investice)	≈ 180 000

(zdroj: vlastní)

12 POZNATKY Z NASAZENÍ A DOPORUČENÍ PRO SPRÁVU

Postupné budování infrastruktury a propojení jednotlivých komponent ukazuje, jak AVD funguje v reálném provozu, jaké jsou vazby mezi jeho prvky a kde mohou vzniknout technické komplikace. Hlavním přínosem této služby je možnost zpřístupnit pracovní prostředí a aplikace centrálně, nezávisle na zařízení uživatele a jeho fyzickém umístění.

V porovnání s klasickým provozem založeným na jednotlivých virtuálních strojích přináší AVD jednodušší správu víceuživatelských relací a snadnější integraci s dalšími službami Azure, například automatizačními nástroji nebo bezpečnostními zásadami. Přesto je důležité věnovat pozornost několika oblastem, které mohou v praxi způsobovat problémy.

V praxi se ale ukazuje, že některé části nasazení vyžadují zvýšenou pozornost. Častým problémem bývá nesprávná registrace zařízení v Entra ID nebo Intune, což může způsobit ztrátu uživatelského profilu nebo přístupových oprávnění. Také změny v prostředí, které se mohou na první pohled jevit jako drobné, ale mohou způsobit výpadky služby nebo problémy s přihlášením.

Správné škálování prostředí hraje důležitou roli nejen z pohledu výkonu, ale i nákladů. Nepřesně nastavený autoscaling může vést k neefektivnímu využívání prostředků, což se následně projeví ve vyšších provozních nákladech.

Další častou příčinou komplikací je nesprávně nakonfigurovaná síťová infrastruktura, zejména v případě, kdy jsou AVD relace v hybridním prostředí (připojení k on-premises AD). Zanedbaná správa přístupových práv nebo špatně nastavené NSG pravidla mohou vést ke ztrátě konektivity nebo bezpečnostním incidentům.

Při správě AVD je důležité průběžně sledovat změny v dokumentaci Microsoftu a sledovat novinky, protože prostředí se rychle vyvíjí. Užitečným zdrojem praktických poznatků bývají odborná fóra, diskusní skupiny nebo zkušenosti ostatních správců, sdílené například na Reddit, Stack Overflow nebo platformě X.

Užitečným pomocníkem může být také umělá inteligence při hledání konkrétních skriptů, ladění chyb nebo navrhování alternativních postupů. Je však nutné k výstupům přistupovat s kritickým myšlením. AI je pouze nástroj, který nenese odpovědnost za funkčnost řešení a správce musí vždy rozumět tomu, co konkrétní nastavení provádí, a ideálně ho před nasazením otestovat.

13 ZÁVĚR

V této bakalářské práci se věnuji tématu virtualizace a cloud computingu, přičemž hlavní důraz kladu na cloudovou platformu Microsoft Azure a její službu Azure Virtual Desktop. V úvodních kapitolách popisují vývoj a principy virtualizace, přechod ke cloudovým technologiím a jednotlivé modely poskytování a nasazení služeb, které jsou základem pro další části práce.

Na to navazuje přehled cloudové platformy Microsoft Azure, kde popisují její architekturu, možnosti integrace, nástroje pro správu a nejčastější scénáře využití. Dále se zaměřuji na porovnání dvou konkrétních služeb Azure Virtual Machine a Azure Virtual Desktop. Rozebírám jejich rozdíly v oblasti správy, výkonu, nákladů, škálovatelnosti a vhodnosti pro různé typy organizací.

V praktické části se věnuji nasazení a správě těchto služeb, přičemž detailněji zpracovávám Azure Virtual Desktop včetně jeho technického pozadí, možností automatizace a zapojení do širší infrastruktury. Cílem není pouze ukázat, jak službu nasadit, ale i jak ji smysluplně provozovat v kontextu každodenního IT provozu. Zohledňuji také bezpečnostní a compliance aspekty, které jsou v dnešní době stále důležitější.

V závěrečné části provádím porovnání obou řešení a navrhuji vhodné scénáře nasazení. Azure Virtual Desktop se ukazuje jako efektivní nástroj zejména pro prostředí, kde je potřeba centrálně spravovat více uživatelů a zařízení, zatímco Azure Virtual Machine je vhodnější pro individuálně přizpůsobené nebo specifické úlohy.

Domnívám se, že práce naplňuje cíle zadané v úvodu, a to jak od literární rešerše přes technický popis a praktickou implementaci až po srovnání a návrh využití pro různé situace. Výsledný text nabízí jak teoretický přehled, tak praktický náhled do fungování moderních cloudových řešení s důrazem na využití v reálném provozu.

SEZNAM POUŽITÉ LITERATURY

- [1] BRODKIN, Jon. With long history of virtualization behind it, IBM looks to the future [online]. Network World, 2009-04-30. Dostupné z: <https://www.networkworld.com/article/780523/virtualization-with-long-history-of-virtualization-behind-it-ibm-looks-to-the-future.html> [cit. 2025-04-25]
- [2] PURE STORAGE. Type 1 vs. Type 2 Hypervisor [online]. Dostupné z: <https://blog.purestorage.com/purely-educational/type-1-vs-type-2-hypervisor/> [cit. 2025-04-16].
- [3] RUEST, Danielle a Nelson RUEST. Virtualizace: podrobný průvodce. Vyd. 1. Brno: Computer Press, 2010. ISBN 978-80-251-2676-9.
- [4] SINGH, Amar. Advantages and Disadvantages of Virtualization in Cloud Computing [online]. UniNets, 21. 4. 2025 Dostupné z: <https://www.uninets.com/blog/virtualization-advantages-and-disadvantages> [cit. 2025-05-26].
- [5] TAYLOR, Kelsey. *Virtualization In Cloud Computing: Pros & Cons of Virtual Platform* [online]. HiTechNectar, 2020 Dostupné z: <https://hitechnectar.com/blogs/pros-cons-virtualization-in-cloud-computing/> [cit. 2025-05-26].
- [6] RUPARELIA, Nayan B. Cloud Computing. Revised and updated ed. MIT Press Ltd, 2023. ISBN 978-0262376228.
- [7] PATRÃO, Luciano. *VMware vSphere Essentials: A Practical Approach to vSphere Deployment and Management*. 1st ed. Berkeley, CA: Apress, 2024. ISBN 979-8-8688-0207-2.
- [8] MICROSOFT. Hyper-V: Přehled technologie [online]. © 2025. Dostupné z: <https://learn.microsoft.com/cs-cz/windows-server/virtualization/hyper-v/hyper-v-overview> [cit. 2025-03-12].
- [9] MICROSOFT. Windows Sandbox [online]. © 2025. Dostupné z: <https://learn.microsoft.com/cs-cz/windows/security/application-security/application-isolation/windows-sandbox/> [cit. 2025-05-26].
- [10] RED HAT. What is KVM? [online]. Red Hat, [cit. 2025-04-20]. Dostupné z: <https://www.redhat.com/en/topics/virtualization/what-is-KVM>.
- [11] MELL, Peter a GRANCE, Timothy. The NIST Definition of Cloud Computing [online]. Gaithersburg: National Institute of Standards and Technology, 2011. NIST Special Publication 800-145. Dostupné z: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf> [cit. 2025-03-11].
- [12] MICROSOFT. What is cloud computing? – Cloud Computing Dictionary [online]. © 2024. Dostupné z: <https://azure.microsoft.com/cs-cz/resources/cloud-computing-dictionary/what-is-cloud-computing> [cit. 2025-05-26].

- [13] AMAZON WEB SERVICES. Overview of Amazon Web Services [online]. © 2024. Dostupné z: <https://docs.aws.amazon.com/whitepapers/latest/aws-overview/introduction.html> [cit. 2025-03-15].
- [14] GOOGLE CLOUD. Google Cloud overview [online]. © 2024. Dostupné z: <https://cloud.google.com/docs/overview> [cit. 2025-03-15].
- [15] MICROSOFT. What is Azure? [online]. © 2024. Dostupné z: <https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-azure/> [cit. 2025-05-26].
- [16] CRN. *AWS Vs. Microsoft Vs. Google Cloud Earnings Q4 2024 Face-Off* [online]. © 2025. Dostupné z: <https://www.crn.com/news/cloud/2025/aws-vs-microsoft-vs-google-cloud-earnings-q4-2024-face-off> [cit. 2025-05-26].
- [17] MICROSOFT. Azure Virtual Desktop [online]. © 2024. Dostupné z: <https://learn.microsoft.com/cs-cz/azure/virtual-desktop/overview> [cit. 2024-10-21].
- [18] MANGAN, Ryan. *Mastering Azure Virtual Desktop: A Practical Guide to Designing, Implementing, and Managing Azure Virtual Desktop Environments*. 2nd ed. Packt Publishing, 2024. ISBN 978-1835884140.
- [19] BRINKHOFF, Christiaan a Per LARSEN. *Mastering Microsoft Intune*. 2. vydání. Birmingham: Packt Publishing, 2024. ISBN 978-1-83546-851-7.
- [20] STEFANOVIC, Vladimir a Milos KATINSKI. *Pro Azure Administration and Automation*. Amsterdam: APress, 2021. ISBN 978-1-4842-7324-1.
- [21] SABALE, Arun a Balu N. ILAG. *Microsoft Azure Virtual Desktop Guide: Configuring and Operating Microsoft Azure Virtual Desktop (Exam AZ-140)*. Springer, 2022. ISBN 978-1-4842-8063-8.
- [22] MICROSOFT. Azure Virtual Desktop service architecture and resilience [online]. © 2023. Dostupné z: <https://learn.microsoft.com/en-us/azure/virtual-desktop/service-architecture-resilience> [cit. 2025-05-29].
- [23] IBM. Role-Based Access Control (RBAC) [online]. © 2024. Dostupné z: <https://www.ibm.com/think/topics/rbac> [cit. 2024-10-21].
- [24] MICROSOFT. Přidání virtuálních počítačů (session hosts) do existujícího host poolu v Azure Virtual Desktop [online]. © 2024 [cit. 20. 4. 2025]. Dostupné z: <https://learn.microsoft.com/cs-cz/azure/virtual-desktop/add-session-hosts-host-pool?tabs=portal%2Cgui&pivots=host-pool-session-host-configuration>.
- [25] MICROSOFT. Plan your virtual desktop migration - Cloud Adoption Framework [online]. © 2024. Dostupné z: <https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/scenarios/azure-virtual-desktop/plan> [cit. 2025-05-29].
- [26] MICROSOFT. How to configure FSLogix Profile Container with Microsoft Entra ID (hybrid identity) [online]. © 2024. Dostupné z: <https://learn.microsoft.com/en-us/fslogix/how-to-configure-profile-container-entra-id-hybrid> [cit. 2025-05-06].

- [27] MICROSOFT. Azure Pricing Calculator – Virtual Desktop [online]. © 2024. Dostupné z: <https://azure.microsoft.com/en-us/pricing/calculator/?service=virtual-desktop> [cit. 2025-05-13]
- [28] MICROSOFT. Azure Virtual Desktop terminology [online]. © 2024. Dostupné z: <https://learn.microsoft.com/en-us/azure/virtual-desktop/terminology> [cit. 2024-10-21]
- [29] MICROSOFT. Azure Virtual Desktop licensing [online]. © 2024. Dostupné z: <https://learn.microsoft.com/en-us/azure/virtual-desktop/licensing> [cit. 2025-05-29].
- [30] MICROSOFT. Licence a požadavky pro používání služby Azure Virtual Desktop [online]. © 2024 Dostupné z: <https://learn.microsoft.com/en-us/azure/virtual-desktop/licensing> [cit. 2025-05-15].
- [31] CITRIX. Calculate your savings with Citrix and Windows Virtual Desktop [online]. 17. 3. 2021. Dostupné z: <https://www.citrix.com/blogs/2021/03/17/calculate-your-savings-with-citrix-and-windows-virtual-desktop/> [cit. 2025-05-15].
- [32] V2CLOUD. The True Cost of Citrix [online]. Dostupné z: <https://v2cloud.com/blog/true-cost-of-citrix> [cit. 2025-05-15].
- [33] MICROSOFT. Virtual machine recommendations for Windows Virtual Desktop [online]. © 2024. Dostupné z: <https://learn.microsoft.com/en-us/windows-server/remote/remote-desktop-services/virtual-machine-recs> [cit. 2024-04-02].
- [34] MICROSOFT. Resize a Windows VM in the Azure portal [online]. © 2024. Dostupné z: <https://learn.microsoft.com/en-us/azure/virtual-machines/sizes/resize-vm?tabs=portal> [cit. 2025-05-20].
- [35] MICROSOFT. *Create and assign an autoscale scaling plan for Azure Virtual Desktop* [online]. © 2024. Dostupné z: <https://learn.microsoft.com/en-us/azure/virtual-desktop/autoscale-create-assign-scaling-plan?tabs=portal%2Cintune&pivots=power-management> [cit. 2024-10-21].
- [36] MICROSOFT. *Enable GPU acceleration for Azure Virtual Desktop* [online]. © 2024. Dostupné z: <https://learn.microsoft.com/en-us/azure/virtual-desktop/graphics-enable-gpu-acceleration> [cit. 2024-10-21].

SEZNAM OBRÁZKŮ

Obrázek 1 Architektura služby AVD a logika připojení uživatele (Depth-first).....	34
Obrázek 2 Výčet komponent pro správu AVD.....	35
Obrázek 3: Rozhraní Marketplace.	38
Obrázek 4: Rozhraní vytvoření Host pool.	39
Obrázek 5: Rozhraní přímého uživatelského licencování.....	43
Obrázek 6: Rozhraní automation account.....	46

SEZNAM TABULEK

Tabulka 1: Porovnání výkonu dle použití typu disků.....	50
Tabulka 2: Základní náklady na provoz AVD.....	56
Tabulka 3: Roční odhad nákladů.....	56
Tabulka 4: Kombinované náklady na provoz AVM a Citrix.....	59
Tabulka 5: Roční odhad nákladů (OPEX + CAPEX).....	59

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AWS	Amazon Web Services
GCP	Google Cloud Platform
AVD	Azure virtual desktop
VM	Virtual machine
SA	Storage account
IDE	Integrated development environment
MDM	Správa mobilních aplikací
MAM	Správu mobilních aplikací
SAAS	Software as a Service
PAAS	Platform as a Service
IAAS	Infrastructure as a Service
RBAC	Role based access control
NIST	Národní institut pro standardy a technologie
DSC	Desired State Configuration
OPEX	Operating Expenses
CAPEX	Capital Expenditures
TCO	Total Cost of Ownership

SEZNAM PŘÍLOH

Příloha P I: POWERSHELL SCRIPTY PRO IMPLEMENTACI A SPRÁVU AVD,
KOMPLETNÍ SCRIPTY ZAZIPOVÁNY V PŘÍLOZE

PŘÍLOHA P I: POWERSHELL SCRIPTY PRO IMPLEMENTACI A SPRÁVU AVD

Součástí bakalářské práce je návrh a realizace nástroje pro nasazení a správu prostředí Azure Virtual Desktop (AVD) pomocí PowerShell skriptů. Veškeré skripty a podpůrné soubory jsou uspořádány do přehledné adresářové struktury v hlavní složce s názvem AVD_UTB_Project, která je dostupná v příloze elektronicky.

Projekt je rozdělen do několika podsložek podle logických celků, které reflektují jednotlivé fáze životního cyklu nasazení a správy AVD prostředí. Každý skript je navržen jako samostatná PowerShell funkce, která očekává přímé parametry a obsahuje integrovanou nápovědu pro snadné použití.

Složka General/

Tato složka obsahuje skripty pro obecné úkony správy AVD, které jsou využitelné napříč celým životním cyklem. Zahrnují funkce pro:

`Assign-AVDUserAppGroup.ps1`: Přiřazování uživatelů nebo Azure AD skupin k aplikačním skupinám AVD.

`Connect-Tenant.ps1`: Připojení k Azure účtu a výběr relevantní subscription.

`Disable-ScalingPlan.ps1` a `Enable-ScalingPlan.ps1`: Ovládání stavu plánů automatického škálování pro host pooly.

`Get-AVDUserSessionInfo.ps1`: Získání informací o aktivních uživatelských relacích na session hostech.

`Set-VMSizeBySelection.ps1`: Změnu podkladního stroje (např. Intel nebo AMD) vybraného virtuálního stroje.

Složka Deployment/

V této složce se nachází jádro celé automatizace pro nasazení AVD infrastruktury. Jednotlivé skripty pokrývají kompletní proces vytvoření AVD prostředí. Každý skript reprezentuje samostatný krok, který je možné spustit nezávisle nebo v posloupnosti dle potřeby. Mezi tyto skripty patří:

Create-Subscription.ps1: Ilustruje proces vytvoření nové Azure subscription, jelikož programová tvorba vyžaduje specifická fakturační oprávnění.

Create-ResourceGroup.ps1: Založení potřebných skupin prostředků.

Create-HostPool.ps1: Vytvoření a základní konfigurace tzv. host poolu, tedy skupiny virtuálních strojů sloužících jako vzdálené plochy pro koncové uživatele.

Create-ApplicationGroup.ps1: Vytvoření nové aplikační skupiny

Create-Workspace.ps1: Vytvoření pracovního prostoru AVD, který sdružuje aplikační skupiny.

Create-SessionHost.ps1: Nasazení samotných session hostů (virtuálních strojů).

Join-SessionHostToHostPool.ps1: Instalace AVD agenta a připojení existujícího virtuálního stroje do host poolu.

Configure-FSLogixProfileContainers.ps1: Konfigurace nastavení pro uživatelské profily pomocí nástroje FSLogix na session hostech, což zajišťuje jednotné prostředí napříč relacemi.

Složka Decommission/

Skripty v této složce se využívají pro bezpečné a řízené odstranění prostředků, které byly během nasazení vytvořeny. Tato fáze je důležitá zejména pro testování a opakované nasazování bez zanechání zbytkových zdrojů v Azure, a také pro úklid nepotřebných komponent. Zahrnuje:

Remove-AVDHostPool.ps1: Odstranění vybraného host poolu.

Remove-AVDResourceGroup.ps1: Zrušení celé skupiny prostředků a veškerého jejího obsahu.

Remove-AVDSessionHosts.ps1: Odstranění jednotlivých session hostů a jejich podkladových virtuálních strojů.

Remove-AVDUserAppGroup.ps1: Odebrání přiřazení uživatelů nebo skupin z aplikačních skupin.

Soubor README.md

V kořenové složce projektu se nachází soubor README.md, který slouží jako dokumentace celého řešení. Obsahuje podrobný přehled struktury projektu, podrobný návod k použití jednotlivých skriptů, seznam předpokladů pro spuštění (např. verze PowerShellu, potřebné Azure moduly), informace o autorovi a licenci, a také upozornění na povahu projektu (akademická práce, bez aktivní údržby).