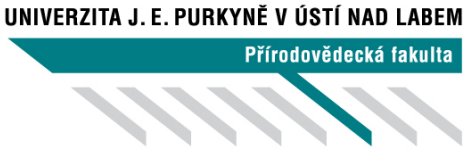
Univerzita Jana Evangelisty Purkyně
v Ústí nad Labem
Přírodovědecká fakulta



Analýza využití tenkých klientů a jejich nasazení v PC učebnách

BAKALÁŘSKÁ PRÁCE

Vypracoval: Jan Drozd

Vedoucí práce: RNDr. Jan Krejčí, Ph.D.

Studijní program: Aplikovaná informatika

Studijní obor: Informační systémy

Ústí nad Labem 2024

UNIVERZITA JANA EVANGELISTY PURKYNĚ V ÚSTÍ NAD LABEM

Přírodovědecká fakulta

Akademický rok: 2022/2023

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jméno a příjmení:	**Jan DROZD**
Osobní číslo:	**F20161**
Studijní program:	**B1802 Aplikovaná informatika**
Studijní obor:	**Informační systémy**
Téma práce:	**Analýza využití tenkých klientů a jejich nasazení v PC učebnách**
Zadávající katedra:	**Katedra informatiky**

Zásady pro vypracování

Cílem bakalářské práce je analyzovat aktuální stav PC učeben a na základě současných i možných budoucích potřeb navrhnout revitalizaci počítačové infrastruktury a PC učeben školy za použití tenkých klientů. Následně je cílem navržené technologie nasadit a začlenit do stávající infrastruktury využívané pro didaktický proces i administrativní potřeby školy. Součástí práce bude také rešerše v oblasti kybernetické bezpečnosti školských organizací a praktická instalace a konfigurace serverů.

Osnova:

Teoretická část

1. Popis aktuálního stavu počítačové infrastruktury a PC učeben školy
2. Aktuálně používané technologie pro vzdálený přístup k serveru
   2.1. popis jednotlivých možností pro vzdálený přístup
   2.2. rešerše dostupných řešení tenkých klientů
3. Virtualizace
4. Windows Server 2022
   4.1. AD
   4.2. DNS
   4.3. DHCP
   4.4. RDS
5. Kybernetická bezpečnost školských organizací
   5.1. zajištění perimetru
   5.2. MAC filtrace
   5.3. žákovské Wi-Fi

Praktická část

1. Analýza potřeb školy
2. Testování dostupných technologií tenkých klientů
3. Návrh řešení
4. Rekonfigurace počítačové sítě
5. Příprava serverové infrastruktury
6. Instalace a konfigurace virtualizace
7. Instalace a konfigurace MS Windows Server
8. Nasazení tenkých klientů
9. Ověření funkčnosti nasazených technologií

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

Seznam doporučené literatury:

1. HORÁK, Jaroslav a Milan KERŠLÁGER. *Počítačové sítě pro začínající správce*. 5., aktualiz. vyd. Brno: Computer Press, 2011. ISBN 978-80-251-3176-3.
2. RUEST, Danielle a Nelson RUEST. *Virtualizace: podrobný průvodce*. Brno: Computer Press, 2010. ISBN 978-80-251-2676-9.
3. VELTE, Anthony T., Toby J. VELTE a Robert C. ELSENPETER. *Cloud Computing: praktický průvodce*. Brno: Computer Press, 2011. ISBN 978-80-251-3333-0.

Vedoucí bakalářské práce: **RNDr. Jan Krejčí, Ph.D.**
Katedra informatiky

Datum zadání bakalářské práce: **27. října 2022**
Termín odevzdání bakalářské práce: **14. května 2024**

L.S. RNDr. Jiří Škvor, Ph.D. Digitálně podepsal RNDr. Jiří Škvor, Ph.D. Datum: 2024.05.10 12:37:42 +02'00'

doc. RNDr. Michal Varady, Ph.D.
děkan

RNDr. Jiří Škvor, Ph.D.
vedoucí katedry

V Ústí nad Labem dne 10. května 2024

Prohlášení

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně a použil jen pramenů, které cituji a uvádím v přiloženém seznamu literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona c. 121/2000 Sb., ve znění zákona c. 81/2005 Sb., autorský zákon, zejména se skutečností, že Univerzita Jana Evangelisty Purkyně v Ústí nad Labem má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Jana Evangelisty Purkyně v Ústí nad Labem oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladu, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

V Ústí nad Labem dne 13. května 2024 Podpis: Jan Drozd

Děkuji vedoucímu práce RNDr. Janu Krejčímu, Ph.D.
za neocenitelné rady a pomoc při tvorbě bakalářské práce.

Analýza využití tenkých klientů a jejich nasazení v PC učebnách

Abstrakt:

Tato bakalářská práce se zaměřuje na analýzu a revitalizaci počítačové infrastruktury v PC učebnách Základní školy Františkovy Lázně. Hlavním cílem je navrhnout a implementovat řešení založené na technologii tenkých klientů, které vyhovuje současným i budoucím potřebám školy, a to jak v didaktickém procesu, tak v administrativních činnostech. Práce dále obsahuje teoretickou rešerši technologií spojených s tenkými klienty, včetně virtualizace, protokolů pro vzdálené připojení a vhodných serverových operačních systémů. Zvláštní pozornost je věnována také kybernetické bezpečnosti školských zařízení.

V praktické části práce je provedena podrobná analýza současného stavu technologického vybavení počítačových učeben školy společně s analýzou potřeb školy a na jejím základě je navržena nová konfigurace učeben a infrastruktury. Součástí praktické části je příprava a rekonfigurace počítačové sítě, nastavení serverové infrastruktury a implementace virtualizačních řešení s potřebnými virtuálními stroji. Finální fází je instalace a konfigurace tenkých klientů a jejich nasazení do PC učeben s následným testováním funkčnosti. Na závěr jsou vyčísleny náklady na celé řešení a provedeno jejich porovnání s alternativními řešeními, společně s analýzou úspory elektrické energie.

Klíčová slova: virtualizace, tencí klienti, infrastruktura PC učeben

Analysis of the use of thin clients and their deployment in PC classrooms

Abstract:

This bachelor thesis focuses on the analysis and revitalization of the computer infrastructure in the PC classrooms of the Františkovy Lázně Primary School. The main objective is to design and implement a solution based on thin client technology that meets the current and future needs of the school, both in the didactic process and in administrative activities. The thesis also includes a theoretical investigation of the technologies associated with thin clients, including virtualization, remote connection protocols and suitable server operating systems. Special attention is also paid to the cybersecurity of school facilities.

In the practical part of the thesis, a detailed analysis of the current state of the technological equipment of the school's computer labs is performed, together with an analysis of the school's needs, and based on this analysis, a new configuration of classrooms and infrastructure is proposed. The practical part includes the preparation and reconfiguration of the computer network, the setup of the server infrastructure and the implementation of virtualization solutions with the necessary virtual machines. The final phase is the installation and configuration of thin clients and their deployment in the PC classrooms with subsequent functionality testing. Finally, the cost of the entire solution is quantified and compared with alternative solutions along with an analysis of the power savings.

Keywords: virtualization, thin clients, PC classroom infrastructure

Obsah

Úvod

V současné době jsou informační technologie neodmyslitelnou součástí vzdělávacích institucí, které jsou na jejich bezchybném fungování do značné míry závislé. Cílem bakalářské práce je analyzovat aktuální stav PC učeben Základní školy Františkovy Lázně a na základě současných i možných budoucích potřeb navrhnout revitalizaci počítačové infrastruktury a PC učeben školy za použití tenkých klientů. Následným cílem je takto získané poznatky využít a navržené technologie nasadit a začlenit do stávající infrastruktury využívané pro didaktický proces i administrativní potřeby.

Teoretickou součástí práce je rešerše a popis technologií souvisejících s tenkými klienty a identifikace způsobů, jak jsou tyto technologie využívány v praxi. Zvláštní pozornost je věnována virtualizaci, protokolům pro vzdálené připojení ke grafickému uživatelskému rozhraní a vhodným serverovým operačním systémům. Dále je část věnována kybernetické bezpečnosti školských organizací s ohledem na fyzickou bezpečnost a ochranu sítě.

Praktická část této práce se soustředí na testování hardwaru a operačních systémů tenkých klientů a následné nasazení do počítačových učeben školy. Základem pro návrh efektivního řešení je podrobná analýza současného stavu, která poskytuje přehled o existující infrastruktuře počítačových učeben. Na ni navazuje analýza potřeb školy, v níž jsou popsány požadavky ze strany vedení, správce sítě a učitelů. Na základě těchto poznatků je navrženo nové řešení počítačových učeben, včetně související síťové a serverové infrastruktury školy. Následující část zahrnuje přípravu a rekonfiguraci počítačové sítě, přípravu serverové infrastruktury, instalaci a konfiguraci virtualizačního řešení, instalaci virtuálních strojů společně s jejich následnou konfigurací. Finální etapou praktické části je instalace a konfigurace tenkých klientů, jejich nasazení do počítačových učeben a zapojení do již připravené infrastruktury. Následně je popsáno ověření funkčnosti nasazených technologií. Speciální pozornost je věnována také nákladům na realizaci a jejich porovnání s alternativními řešeními, aby bylo možné vyhodnotit ekonomickou efektivitu projektu po stránce pořizovacích nákladů a spotřeby elektrické energie.

Práce si klade za cíl poskytnout komplexního průvodce pro nasazení virtualizace a tenkých klientů nejen ve vzdělávacích organizacích, ale i mimo ně, a ukázat jaké benefity jejich nasazení nabízí.

1 Virtualizace

Virtualizace je jedním z nejdůležitějších pojmů moderních informačních technologií a jsou s ní spojeny značné výhody, jako flexibilita, škálovatelnost, jednodušší obnova v případě havárie, efektivní využití zdrojů a úspora nákladů na provoz IT infrastruktury. Je základem moderního cloud computingu.

Mezi základní prvky virtualizace patří možnost rozdělení a sdílení hardwarových prostředků daného hardwaru mezi více virtuálních strojů (virtual machine, VM). Rozdělení hardwarových prostředků má na starosti hypervizor, který slouží jako rozhraní mezi fyzickým hardwarem (nejčastěji server) a VM. Virtuální stroj má pomocí abstraktní vrstvy přidělený počet jader procesoru, operační paměť, síťové karty a úložiště, které mu jsou k dispozici. Každý VM se tak chová jako samostatný počítač, který provozuje svůj vlastní OS pro potřeby dané aplikace nebo nasazení. Virtualizovány nemusí být jenom samotné VM, ale i CPU, GPU, úložiště, sítě a aplikace. [1]

Důležitými prvky v oblasti virtualizace jsou také pojmy jako hostitel (host) a host (guest). Hostitel interaguje přímo se základním hardwarem, zatímco host je název pro VM, na kterém běží samostatný OS [2]. Spojení více hostitelů do jednoho výpočetního celku se nazývá cluster.

Bez využití virtualizace by pro spuštění každého OS musel běžet nezávislý server, což by s sebou neslo vysoké pořizovací náklady nejen na samotný hardware, ale i potřebné licence. Rovněž by to vedlo k nízké efektivitě a značně složitější správě.

Dále je potřeba zmínit, že ne vždy je virtualizace žádoucí, a to z důvodu potřeb provozované aplikace, ať už kvůli nutnosti přímého přístupu k fyzickému hardwaru, tak z důvodu snížení výkonu při využití virtualizace, jelikož nemusí být dostupné potřebné instrukce procesoru či grafická akcelerace [3]. Další překážkou mohou být i licenční podmínky provozovaného softwaru.

1.1 Hypervizor

Hypervizor je software umožňující správu a běh virtuálních strojů, který jednotlivým hostům přiděluje hardwarové prostředky hostitele dle jejich potřeb. Může se jednat o konkrétní, k tomu určený OS (Typ 1) nebo aplikaci (Typ 2). Největší výhodou je jednoduchá přenositelnost VM mezi různými stroji se stejným hypervizorem a hardwarovou architekturou. [4]

Jednotlivé VM nejsou mezi různými typy hypervizorů vzájemně kompatibilní kvůli rozdílným ovladačům hostovaných VM, formátům virtuálních disků a konfiguračním souborům. Pokud je potřeba změnit provozovaný hypervizor za jiný se zachováním aktuálních VM, je potřeba virtuální

disk převést do potřebného formátu, vytvořit nový VM s potřebnou konfigurací a nainstalovat příslušné kompatibilní ovladače.

Typ 1 (nativní)

Typ 1 hypervizor je odlehčený operační systém primárně určený k provozu VM, který se instaluje přímo na daný hardware (server). Jeho hlavní výhodou je vyšší bezpečnost a lepší efektivita než u hostovaných hypervizorů. [4]

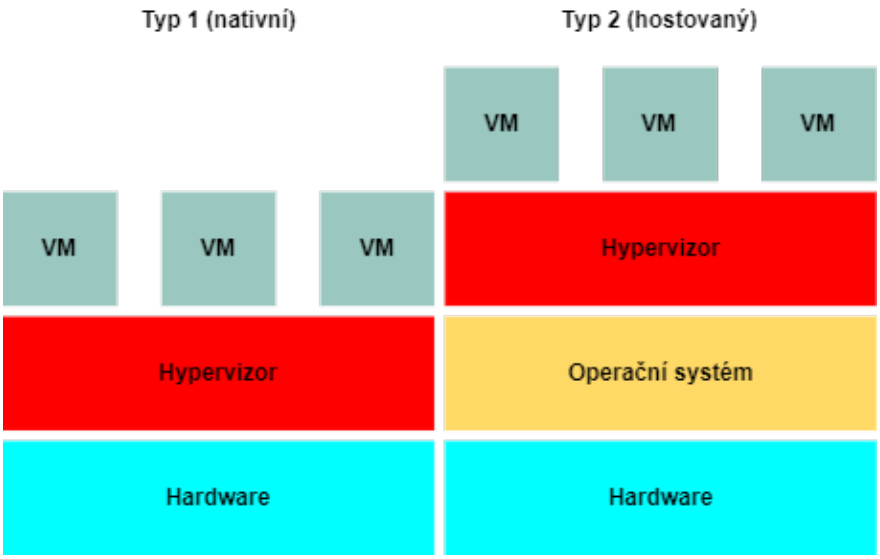
Tento typ hypervizoru nachází využití všude tam, kde je vyžadována vysoká dostupnost a jednoduchá škálovatelnost do budoucna, ať už se jedná o malé organizace nebo datová centra.

Mezi typické zástupce patří VMware ESXi, Hyper-V, XenServer, KVM [5].

Typ 2 (hostovaný)

Typ 2 hypervizor je aplikací instalovanou na OS. Obecně lze říci, že nabízí stejné funkce jako hypervizor typu 1, avšak má vyšší latenci a o něco nižší výkon, a to kvůli mezivrstvě, kterou tvoří OS.[4] Tento typ je vhodný spíše k testovacím účelům nebo domácímu použití.

Mezi typické zástupce patří VMware Workstation, VirtualBox, QEMU, Parallels [6].



Obrázek 1.1: Vizualizace základního dělení hypervizorů, inspirováno [7]

1.2 Základní dělení virtualizace

Virtualizace se dle funkčnosti a nasazení dělí na několik základních kategorií. Níže jsou uvedena některá nejčastější využití.

Hardwarová virtualizace

Jedná se o typ virtualizace, při které jsou vytvářeny jednotlivé VM nad hardwarovými prostředky hostitele. Na úrovni hostitele probíhá emulace procesoru, grafické karty, paměti, disků a dalších komponent. [8]

Mezi důležité prvky hardwarové virtualizace patří virtualizace CPU a GPU, které patří mezi nejdůležitější komponenty každého PC a nejvíce se podílejí na uživatelském zážitku ze strany výkonu. Virtualizace CPU byla na počátcích řešena pouze softwarově, ale moderní procesory pracují s instrukční sadou, která již virtualizaci podporuje, což se projevuje lepším výkonem VM. U GPU virtualizace je situace obdobná. GPU může být buďto rozdělena na několik vGPU a přiřazena více VM, nebo může pracovat v průchozím režimu, ve kterém je celá tato GPU dostupná pouze jednomu konkrétnímu VM. Takové řešení je vhodné třeba pro práci s náročnými grafickými aplikacemi (CAD). [1]

Plná virtualizace

Při plné virtualizaci dochází ke kompletní simulaci fyzického hardwaru pro VM. Každý takový stroj je nezávislý a pro instalovaný OS se jeví jako samostatný počítač. Díky tomu je možné na hypervizoru provozovat VM s různými OS nezávisle na sobě. Na takovýto provoz není potřeba žádná modifikace OS ani aplikací. Mezi další výhody patří nezávislost na hardwaru hostitele a s tím související jednoduchá přenositelnost. Nevýhodou tohoto řešení je pokles výkonu VM. [8]

Paravirtualizace

Při použití paravirtualizace nejsou všechny hardwarové prostředky emulovány, ale využívá se část hardwarových prostředků hostitele, dochází tedy jenom k částečné abstrakci. Například hostitel může sdílet svůj procesor s VM, i když s neúplnou instrukční sadou. Takové řešení přináší benefity v podobě zvýšení výkonu a efektivity. Mezi nevýhody patří nutné úpravy OS pro takové použití. [8]

Aplikační virtualizace

Jedná se o typ virtualizace, u které není aplikace instalována přímo do OS, ale do izolovaného prostředí, které ji odděluje od OS a ostatních aplikací. Pro samotnou aplikaci se vše jeví, jako by běžela přímo na OS, přičemž má virtualizované některé jeho komponenty potřebné pro správný

chod. Typicky se jedná o potřebné knihovny a runtime komponenty. Virtualizace aplikací typicky nachází využití v situacích, kdy je potřeba spouštět například starší aplikace, které už nejsou kompatibilní s aktuálním klientským OS. Dále také nacházejí využití tam, kde je například potřebné používat aplikaci napsanou pro Windows na jiném OS (macOS, Linux, Chrome OS, Android atd.). Nejčastěji probíhá virtualizace aplikací na vzdáleném serveru a obraz aplikace je pomocí sítě přenášen k připojenému klientovi, tudíž není nutná přímá instalace aplikace na klientském zařízení. [9]

Kontejnerová virtualizace

Kontejnerová virtualizace je moderní a efektivní způsob využívaný k vývoji, nasazování a správě aplikací. K její popularizaci došlo hlavně v posledních letech, ale její základy jsou datovány již od roku 1979, kdy se tento koncept zrodil. Při nasazení kontejnerové virtualizace jsou aplikace umisťovány do kontejnerů, které izolují jak samotnou aplikaci, tak její závislosti od hostitelského systému, se kterým sdílí jádro OS. Největší předností při využívání kontejnerové virtualizace je rychlost nasazení, zachování identického prostředí napříč různými systémy (konzistentnost a přenositelnost) a vysoká míra bezpečnosti. Jednotlivé kontejnery se navzájem neovlivňují a z důvodu vyšší bezpečnosti mohou například používat vlastní virtualizovanou síť. [10]

K izolaci jednotlivých kontejnerů se využívají jmenné prostory jádra (namespaces), které se starají o oddělení jednotlivých procesů (kontejnerů) a cgroups, které zajišťují rozdělení systémových prostředků mezi jednotlivé procesy. [11]

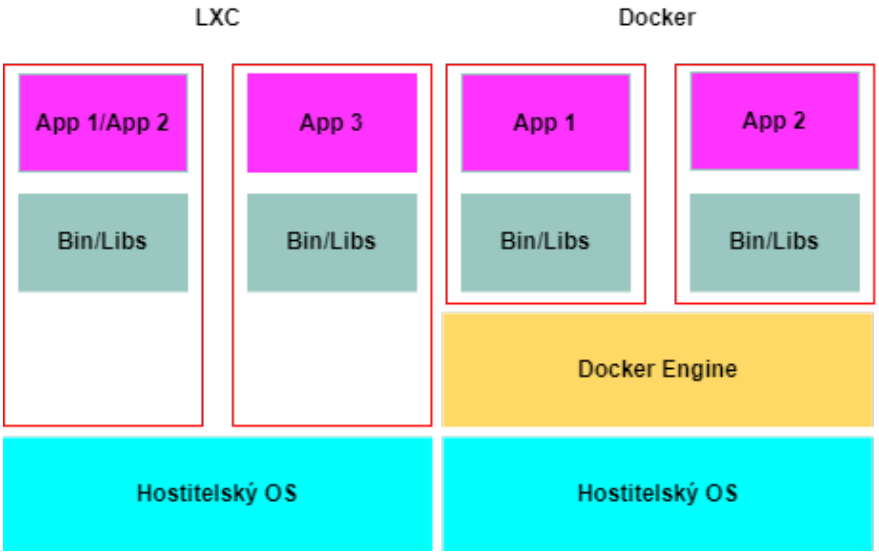
Dvěma nejpoužívanějšími způsoby, které jsou využívány pro kontejnerovou virtualizaci, jsou LXC (Linux Containers) a Docker, který je často používán společně s Kubernetes k jejich hromadné správě, při nasazení většího počtu kontejnerů. [10]

LXC (Linux Containers)

LXC umožňuje současně provozovat a spravovat virtualizované linuxové stroje na jednom hostiteli se systémem Linux. Každý takový systém je umístěn ve vlastním izolovaném kontejneru a s hostitelským systémem sdílí jádro OS. LXC kontejner se pro hostující OS jeví jako běžící proces s vlastním uživatelským prostorem, který vytváří nové procesy aplikací uvnitř kontejneru. Výhodou LXC je možnost instalovat aplikace stejně jako při práci s hostitelským OS nebo běh více procesů najednou v rámci jednoho kontejneru, což ho přibližuje více tradiční virtualizaci, a je tak možné jednotlivé kontejnery použít jako samostatná desktopová prostředí. Mezi další přednosti patří menší hardwarové nároky oproti tradiční virtualizaci, lepší škálovatelnost a vysoká úroveň zabezpečení. [12]

Docker

Docker je na rozdíl od LXC navržen tak, aby na jeden kontejner spouštěl pouze jednu aplikaci se všemi jejími závislostmi, nezávisle na hostitelském OS. Každá aplikace tudíž využívá svůj samostatný kontejner se všemi potřebnými závislostmi a je izolována od ostatních kontejnerů. Dále zavádí abstrakci sítě a úložiště, k čemuž využívá knihovnu libcontainer (součást Docker Engine), díky které jsou kontejnery méně závislé na hostitelském OS, z čehož vyplývá jejich jednoduchá přenositelnost napříč různými systémy. Správa jednotlivých kontejnerů probíhá pomocí příkazového řádku Dockeru. Při vysokém počtu kontejnerů se používá centralizovaná správa pomocí Kubernetes. Aktuálně je Docker jedním z nejpopulárnějších řešení pro nasazování aplikací s podporou široké škály OS. Mezi jeho nevýhody patří nutnost běhu jednotlivých kontejnerů pod uživatelem root, což může představovat potencionální bezpečnostní riziko. [12]



Obrázek 1.2: Porovnání LXC a Dockeru, inspirováno [12]

Desktopová virtualizace

Desktopová virtualizace (VDI) umožňuje na jednom či více fyzických serverech provozovat více desktopových OS, jelikož každý běží jako samostatná instance VM pod hypervizorem. Uživatelé se nejčastěji k těmto stanicím připojují vzdáleně a pracují s daty a aplikacemi přímo na tomto stroji. Díky možnosti personalizace se dané řešení jeví uživateli jako jeho vlastní pracovní stanice. Výhodou je možnost vzdáleným klientům poskytnou různé OS bez potřeby jejich přímé instalace na klienta. VDI je často nasazováno společně s tenkými klienty. [1]

Další možností je nasazení tohoto řešení na hypervizor typu 2, který je nainstalován na uživatelském OS. [1]. Toto řešení se uplatňuje v situacích, kdy uživatel potřebuje pracovat s různými OS, nebo pro testovací účely.

Jako další možné řešení se nabízí využití LXC kontejnerů se samostatným uživatelským prostředím

a jejich následné zpřístupnění uživatelům. Nevýhodou je omezení pouze na rodinu OS Linux, protože takové řešení nemusí být pro dané uživatele ideální, což je potřeba zvážit.

Virtualizace sítě

Vytváří abstrakci nad hardwarovými prvky, jako jsou síťové karty, přepínače a směrovače a implementuje tyto funkce do softwaru běžícího na hypervizoru. Jediným požadavkem je, aby této softwarové vrstvě byly předány pakety z fyzického síťového rozhraní a naopak, což umožňuje komunikaci, jako by VM byl samostatný fyzický stroj. Výhodou je, že do těchto virtuálních přepínačů mohou být přidělovány běžící VM, aniž by muselo docházet k fyzickým zásahům přímo do hardwaru, což s sebou přináší zjednodušenou správu. [1]

Mezi další přednosti patří možnost vytvářet izolované podsítě pouze v rámci skupiny VM, přičemž tato skupina nemusí mít vůbec přístup k fyzickému síťovému adaptéru. Z toho vyplývá nezávislost na fyzické topologii. Do této skupiny se můžou řadit i samotné sítě VLAN, které zajišťují oddělení a izolaci částí sítě. [13]

Virtualizace úložiště

Umožňuje spojit různá síťová úložiště do jednoho celku nazvaného fond úložišť a sjednotit tak jejich následnou správu. Z tohoto fondu je možné potřebnou část přiřadit VM v síti. Výhodou je maximální možné využití dostupné kapacity úložiště, což přispívá ke snížení celkových nákladů, a také jednoduchá škálovatelnost dle potřeby, jelikož fond může být dále rozšiřován. [1]

1.3 Vybraná aktuálně využívaná řešení

Následující část představí aktuálně nejčastěji využívaná virtualizační řešení. Všechna vybraná řešení jsou typu 1, tedy nativní hypervizory, z důvodu potřeby provozu na serverových technologiích. Jsou nasazovány v produkčním prostředí za účelem co nejvyššího výkonu. Vhodný výběr virtualizační platformy závisí na potřebách dané organizace, která se chystá virtualizační platformu nasadit, přičemž jednotlivé platformy mohou být vhodnější na specifické využití než jiné. Dalším faktorem jsou také finanční možnosti organizace, které nemusí být dostatečné na pokrytí nákladů v případě pořízení komerčního řešení. V takové situaci se nabízí jako řešení použití open-source virtualizačních platforem.

Microsoft Hyper-V

Microsoft Hyper-V je jeden z nejvíce využívaných hypervizorů, a to z důvodu jeho provázanosti na OS Windows. Nabízí kompletní řešení pro podnikovou virtualizaci, ať už se jedná o jednoduchý

provoz jednotlivých VM, širokou podporu virtualizovaných OS či vytváření a provoz virtuálních přepínačů. Byl představen v roce 2008 jako součást produktu Windows Server 2008[14].

Mezi základní prvky patří podpora snapshotů (zachycení aktuálního stavu počítače), živá migrace VM mezi hostiteli nebo podpora dynamických virtuálních disků ve formátu vhdx. Samozřejmostí je podpora vytvoření clusteru z několika serverů. Jednotlivé VM, virtuální přepínače nebo disky lze spravovat skrze PowerShell, Hyper-V Manager, Windows Admin Center za použití webového prohlížeče, nebo nástroje SCVMM (System Center Virtual Machine Manager), který je určen pro správu velkého počtu serverů s mnoha virtuálními stroji. Je nabízen v několika možných řešeních. [15, 16]

Hyper-V jako role Windows serveru

V případě tohoto nasazení je potřeba roli Hyper-V doinstalovat pomocí Správce Serveru a následně provést jeho restartování. Po restartování serveru se zpřístupní služba Hyper-V, kterou lze spravovat pomocí Správce technologie Hyper-V nebo dalšími již zmíněnými nástroji. [17]

Role Hyper-V je dostupná v edicích Standard i Datacenter a liší se podmínkami použití, přičemž na jednom fyzickém serveru pod stejnou licencí lze provozovat více instancí Windows Serveru. Aktuálně nejnovější nabízená verze je Windows Server 2022. [17]

- **Standard** — 1 hostitel Windows Server + 2x Windows Server VM.
- **Datacenter** — 1 hostitel Windows Server + neomezeně Windows Server VM. [17]

Hyper-V jako samostatný server

Je založen na minimalistickém Windows Server Core, který obsahuje pouze základní jádro a funkce systému Windows Server, společně s Hyper-V. Správa je primárně prováděna pomocí PowerShellu, přičemž již představené nástroje je možné využít po dodatečné konfiguraci. [18]

Tento systém byl distribuován zdarma, bez omezení, jako konkurence k ostatním virtualizačním produktům, ale s nástupem Hyper-V Server 2019 byla tato strategie ukončena.

Podpora serverových verzí Hyper-V závisí na verzi Windows Serveru, na které jsou provozovány. U hlavních vydání je poskytována plná podpora po dobu 5 let, poté následuje období poskytování bezpečnostních záplat, které trvá dalších 5 let. [19]

Hyper-V jako součást desktopových Windows

Jedná se v podstatě o stejný produkt jako u verze Windows Server. Nepodporuje některé funkce, jako vytváření clusteru, živou migraci, sdílení vhdx disku mezi více stroji nebo replikaci jednotlivých VM. Mezi přidané funkce oproti serverové edici patří předdefinovaná virtuální síť s funkcí NAT a možnost rychlého vytváření VM z několika předpřipravených distribucí OS. Hyper-V lze doinstalovat do všech systémů s licencí Pro a vyšší. [15]

VMware ESXi/vSphere

VMware ESXi/vSphere se řadí mezi standardy virtualizace napříč podnikovým prostředím, kde poskytuje jak značnou stabilitu, tak širokou podporu hardwaru, OS a široké škály softwaru. Jedná se o jedno z nejstarších řešení na poli virtualizace. [20]

Jeho předností je jednoduchá architektura, jelikož samotný hypervizor vyžaduje jen minimální místo na disku, což značně zvyšuje jeho bezpečnost a stabilitu. Správa hypervizoru je prováděna skrze webový prohlížeč po připojení na jeho management IP, případně pomocí příkazového řádku. Pro správu většího množství serverů je nabízeno řešení vCenter, které poskytuje jejich hromadnou správu, kontrolu nad přiřazenými zdroji a komplexní správu VM. [21]

Samozřejmostí je podpora klíčových funkcí, mezi které patří virtuální přepínače, podpora dynamických virtuálních disků, vytváření snapshotů, živá migrace, replikace apod. [20]

Podpora k jednotlivým verzím je standardně poskytována po dobu 5 let od jejich uvedení [22].

Licencování vSphere a vCenter

Licencování probíhá na základě počtu fyzických procesorů a jejich jader, přičemž dostupnost určitých funkcionalit závisí na konečném výběru licence. Řešení vCenter je součástí všech prodávaných licencí a jeho instalace probíhá na samostatný VM. [23] Dlouhou dobu byla také nabízena bezplatná licence vSphere Hypervisor s omezenou sadou funkcí. Nabídka této verze produktu byla ukončena v únoru 2024 po akvizici firmou Broadcom a náhrada nebyla oznámena. Společně s touto změnou nastala také změna u licencování ostatních produktů, kdy licence nejsou již trvalé, ale jsou nabízené pouze formou předplatného. Pro jejich správnou funkčnost je tedy nutné mít předplatné zaplacené. [24]

- **vSphere Hypervisor** – ESXi ve verzi zdarma, v této verzi nepodporuje centralizovanou správu skrze vCenter, vysokou dostupnost nebo živou migraci. Navíc obsahuje limit na maximálně 8 vCPU pro každý VM a 480 logických CPU na hostitele. [25]
- **vSphere Essentials Plus Kit** – nejnižší z nabízených licencí s omezenou sadou funkcí, obsahuje produkty vSphere Essentials Plus a vCenter Server Essentials s omezením na maximálně 3 hostitele, dohromady s 96 fyzickými jádry. [26]
- **vSphere Standard** – standardní edice, která oproti základní edici nabízí možnosti, jako jsou replikace VM nebo jejich živá migrace. Licencování probíhá na základě počtu jader jednotlivých serverů. Součástí této licence jsou produkty vSphere Standard a vCenter Server Standard. [26]
- **vSphere Foundation** – nejvyšší nabízená licence, která nabízí plnou sadu funkcí společně s produkty vSphere Enterprise Plus, vCenter Server Standard, Tanzu Kubernetes Grid a Aria Suite Standard. Tato licence je vhodná pro velká datová centra využívající ve svém provozu kontejnerizaci. [26]

Citrix Hypervisor

Vznikl jako open-source hypervizor na univerzitě v Cambridge pod názvem Xen v roce 2003. V roce 2007 byl odkoupen firmou Citrix od firmy XenSource, Inc., která zachovala verzi zdarma, ale přidala k ní placené varianty. XenServer byl následně roku 2009 uvolněn jako open-source. V průběhu roku 2017 došlo k rozhodnutí o odstranění některých funkcí z produktu XenServer free, které vedlo ke vzniknu XCP-ng, jakožto open-source forku hypervizoru XenServer. O dva roky později došlo k přejmenování XenServeru na Citrix Hypervisor. [27]

Samozřejmostí je podpora všech funkcionalit jako u již dříve představených řešení, s důrazem na optimalizaci pro produkty jako Citrix Virtual Apps and Desktops, které patří mezi klíčové produkty společnosti Citrix v oblasti virtualizace. Správa jednotlivých hostitelů probíhá skrze XenCenter, přičemž maximální počet hostitelů v clusteru je omezen na 64. [28]

Pro instalaci lze zvolit dvě dostupné verze, které se liší délkou jejich podpory. Aktualizace pro verzi s dlouhodobou podporou (LTS, Long Term Support) jsou dostupné po dobu 5 let od vydání, přičemž existuje možnost prodloužení poskytování bezpečnostních záplat až na 10 let. U standardní verze není interval podpory pevně stanoven. [28]

Licencování

Citrix Hypervisor je nabízen ve dvou edicích rozdělených podle dostupných funkcí. Licencování probíhá na základě počtu obsazených CPU socketů.

- **Standard Edition** – základní edice pro zákazníky, kteří nepožadují pokročilé funkce.
- **Premium Edition** – edice vhodná pro náročné zákazníky, kteří vyžadují například virtualizaci desktopů z důvodu podpory virtualizace GPU. Dále nabízí funkce jako automatickou aktualizaci ovladačů Windows VM, automatické aktualizace management agenta nebo podporu dynamického vyrovnání pracovní zátěže. [28]

XCP-ng

Open-source alternativa k Citrix Hypervisoru, která je dostupná ke stažení zdarma. Je distribuován pod licencí GNU a klade si za cíl být funkčně srovnatelný. Obsahuje stejné omezení na maximální počet hostitelů v clusteru jako Citrix Hypervisor. Jeho správa je prováděna pomocí Xen Orchestra, který je také potřeba provozovat jako samostatný VM. [29]

Podpora XCP-ng se odvíjí od zvolené verze. Standardní vydání je podporováno do okamžiku vydání následující verze a ještě několik měsíců poté, což poskytuje uživatelům dostatečný čas na aktualizaci. Verze s dlouhodobou podporou nabízí podporu po dobu 5 let od vydání. [29]

Licencování

XCP-ng nemá žádné licenční omezení, které by se vztahovalo na počet procesorů, počet jader nebo velikost obsazené paměti RAM, ale funguje na principu předplatného, přičemž se u každého hostitele platí za podporu ze strany vývojářů. Tím dávají vývojáři prostor jednotlivým zákazníkům rozhodnout se, zda si podporu od vývojářů zaplatí, nebo si v případě potřeby postačí s podporou komunity, která nemusí být vždy schopna daný problém vyřešit. [29]

- **Standard** – omezeno na maximálně 6 ticketů ročně, reakční doba 1 den.
- **Enterprise** – neomezený počet ticketů, reakční doba 1 hodina, asistence při instalaci a následujících aktualizacích. [29]

Licencování Xen Orchestra je řešeno podobně jako u samotného XCP-ng, ovšem s tím rozdílem, že se neplatí jenom za podporu ze strany vývojářů, ale i za některé pokročilé funkce. Další možností, jak získat plnou funkcionalitu bez podpory a záruky od vývojářů, je kompilace Xen Orchestra přímo ze zdrojového kódu. [30]

- **Free** – základní edice dostupná zdarma, obsahuje omezenou sadu funkcí.
- **Starter** – přidává k základní edici podporu ze strany vývojářů a možnost provádět plné zálohy VM.
- **Enterprise** – podpora plné replikace VM nebo inkrementálních záloh.
- **Premium** – podpora inkrementální replikace, plánovače úloh a dalších pokročilých funkcí. [30]

KVM

Open-source hypervizor, sloužící pro virtualizaci na úrovni hardwaru je součástí Linuxu od roku 2006. KVM (Kernel based Virtual Machine) je přímo součástí linuxového jádra, což s sebou nese značné výhody v oblasti bezpečnosti, aktualizací a implementování nových funkcí. Je distribuován pod licencí GNU. [31]

Jedná se o typ 1 hypervizor a obsahuje všechny potřebné komponenty ke spouštění virtuální počítačů. Každý VM je v KVM provozován jako samostatný proces s předem daným vyhrazeným hardwarem, který je spravován pomocí linuxového plánovače. Mezi značné výhody KVM patří podpora jakéhokoliv úložiště podporovaného linuxem, široká podpora zařízení napříč výrobci a jednoduchá škálovatelnost. Mezi nejznámější zástupce využívající KVM patří Red Hat Virtualization, Proxmox VE a oVirt. [31]

Licencování

K využívání KVM není potřeba zakoupit žádnou licenci, jelikož je plně zdarma k využití jako součást linuxového jádra. Komerčně nabízené produkty pracující s virtualizací KVM mohou

nabízet některé pokročilé funkcionality, které nejsou dostupné zdarma. Součástí předplatného bývá i podpora přímo od vývojářů daného řešení. [31]

Proxmox VE

Jedná se o open-source platformu s podporou virtualizace a kontejnerů LXC založenou na KVM. Byl představen roku 2008 ve verzi 0.9, jako první dostupné řešení kombinující kontejnerovou virtualizaci s hypervizorem KVM, společně s integrovanou správou pomocí webového rozhraní. Již od počátku byl jeho součástí nástroj pro zálohování VM a kontejnerů. Roku 2020 byl představen Proxmox Backup Server, jakožto podnikové řešení pro zálohování virtuální infrastruktury. [32]

Mezi jeho přednosti patří snadná instalace, dobrá dokumentace, silná komunita a integrované webové rozhraní pro správu. Dále je dostupná aplikace pro mobilní telefony, ze které je možné spravovat celé virtualizační řešení. Spravován může být i skrze linuxový terminál, což u některých pokročilých konfigurací je i nutností z důvodu chybějící funkcionality ve webovém rozhraní. Je distribuován pod licencí GNU. [32]

Je založen na Debianu, což zaručuje vysoký výkon, stabilitu a spolehlivost při daném nasazení. Díky využití Debianu a KVM je zaručena široká kompatibilita napříč hardwarem a kompatibilita s OS běžícím na VM. Nevýhodou použitého Debianu je kratší doba podpory ze strany vývojářů oproti ostatním virtualizačním řešením, jelikož je poskytována pouze po dobu 3 let od vydání dané verze. Součástí webového rozhraní je i jednoduchá správa clusteru, sítí, úložišť či monitoring clusteru, hypervizorů a jednotlivých VM. Samozřejmostí je také podpora ostatních již představených pokročilých funkcí. [32]

Licencování

Proxmox VE je v komunitní edici dostupný zcela zdarma včetně všech funkcí a zálohovacího serveru. Nevýhodou je přístup pouze do komunitního repositáře, který slouží spíše k testování nových funkcí a nemusí být vždy zcela stabilní. Z tohoto důvodu vývojáři nedoporučují používání komunitní edice v produkčním prostředí, jelikož může obsahovat chyby a zranitelnosti. Ke komunitní edici nabízejí několik plánů předplatného, které umožňuje přístup do enterprise repositáře. Liší se hlavně typem podpory a předplaceným časem technické podpory. Jednotlivé licence se kupují na základě počtu soketů v jednotlivých serverech. [32]

- **Community** – základní edice, umožňuje přístup k enterprise repositáři, bez podpory vývojářů.
- **Basic** – přidává podporu skrze zákaznický portál, maximálně 3 tickety za rok, reakční doba 1 den.
- **Standard** – 10 ticketů za rok, reakční doba 4 hodiny v pracovní dny, vzdálená podpora skrze ssh, možnost offline aktivace.
- **Premium** – neomezené množství ticketů, reakční doba 2 hodiny v pracovní dny. [32]

oVirt

Virtualizační platforma oVirt je komunitní projekt založený společností Red Hat. Jeho vývoj začal v roce 2011 a první oficiální vydání ve verzi 3.0 bylo uvolněno v roce 2012. Společnost Red Hat používá oVirt jako základ virtualizační platformy Red Hat Virtualization. [33]

Stejně jako Proxmox využívá pro provoz VM hypervizor KVM, ale na rozdíl od něj nepodporuje provoz kontejnerů LXC a nenabízí vlastní zálohovací řešení. Instalaci je možné provést na linuxové distribuce vycházející z Red Hat Enterprise Linux (RHEL), nebo použít oficiální upravenou distribuci oVirt Node založenou na distribuci CentOS Stream. Pokud je použita odvozená distribuce z RHEL, například Rocky Linux, je potřeba postupovat dle pokynů dokumentace a provést potřebné úpravy. Po instalaci oVirt Node je možné pomocí webového prohlížeče přistoupit na jeho webové rozhraní. [34]

Pro správu jednotlivých VM, úložišť, sítí a celého clusteru se používá oVirt Engine, který může být nainstalován na samostatný fyzický stroj. Pro zajištění vysoké dostupnosti se doporučuje instalace do samostatného VM, která je automaticky nabídnuta po instalaci a prvním spuštění oVirt Node. Sada dostupných funkcí je podobná jako u ostatních platforem a lze je také libovolně spravovat z linuxového terminálu. [34]

Podpora pro jednotlivé verze je poskytována podobně jako u standardní verze XPC-ng, a to pouze do vydání další verze, kdy je poté ponecháno časové okno pro potřebnou aktualizaci. [34]

V porovnání s již představenými virtualizačními platformami nabízí nejmenší uživatelskou základnu, což se značně odráží na uživatelské zkušenosti s tímto řešením. Jelikož není dostupná podpora ze strany vývojářů, na rozdíl od Proxmoxu, je uživatel odkázán pouze na komunitní fóra či komerční firmy. Další podstatnou skutečností je odklon společnosti Red Hat od platformy Red Hat Virtualization, která je nyní nahrazována produktem OpenShift Virtualization, což má za následek odklon od přispívání do vývoje platformy oVirt. [34, 35]

Licencování

K provozování platformy oVirt není potřeba zakoupit žádnou licenci, a tudíž je možné ji provozovat zcela zdarma. [34]

2 Aktuálně používané technologie pro vzdálený přístup k serveru

Na tuto problematiku lze nahlížet ze dvou různých pohledů, a to ze strany použitých protokolů pro vzdálený přístup ke grafickému uživatelskému rozhraní serveru, kde se nabízejí možnosti využití protokolů RDP, VNC, Citrix ICA, VMware Blast Extreme a dalších, nebo z pohledu použitého hardwaru a OS, který musí dané protokoly podporovat a být na dané použití optimalizován pro co nejlepší možný uživatelský zážitek [36]. Volba vhodné kombinace protokolu, hardwaru a OS se v konečném důsledku odvíjí od specifických potřeb a požadavků organizace.

2.1 Základní dělení operačních systému dle počtu souběžně pracujících uživatelů

Dalším důležitým faktorem, který má vliv na finální architekturu, je volba typu OS, jelikož se dělí na dvě základní kategorie (single-session/multi-session) podle možnosti souběžného připojení více uživatelů najednou. Od použitého typu OS se dále odvíjí potřebný serverový hardware, přičemž lze obecně říci, že multi-session řešení má menší nároky na použitý hardware díky tomu, že není potřeba spouštět více instancí daného OS. [37]

Session (relace)

Relace je důležitým pojmem v kontextu OS. Vytváří se při přihlášení uživatele a představuje časové období, během kterého může uživatel interagovat s OS, soubory a programy nezávisle na ostatních uživatelích. Po jeho odhlášení je relace ukončena. Každý proces v rámci uživatelské relace má svůj vlastní kontext, který zahrnuje informace o stavu procesu, paměťové alokaci a otevřených souborech. Relace jsou mezi sebou procesově odděleny, aby se uživatelé při práci vzájemně neovlivňovali. Rozdělení systémových prostředků mezi uživatele může být řešeno zavedením kvót na zdroje OS, mezi které patří zavedení diskových kvót, maximální využití paměti nebo počtu spuštěných procesů. Kvůli rozdílným návrhům přistupuje k této problematice každá rodina OS specificky. [38]

Single-session

Do této kategorie spadají OS, které podporují pouze jednu relaci. Jedná se o tradiční přístup a využívá se především na osobních počítačích. Neklade žádné zvláštní nároky na software, který by musel podporovat souběžnou práci několika uživatelů najednou, a všechny jeho dostupné zdroje může využívat aktuálně přihlášený uživatel. Typickými zástupci jsou Windows (v základních edicích) a MacOS. [37]

Multi-session

Jedná se o kategorii OS podporující několik souběžně přihlášených uživatelů, kteří sdílejí stejné hardwarové a softwarové prostředky bez vzájemného ovlivňování. Typické je nasazení těchto OS na serverech, kde je potřeba souběžná práce více uživatelů, která se využívá především u vzdáleného připojení. Dalším důležitým faktorem je použitý software, který musí být na takové nasazení připraven a podporovat souběžnou práci více uživatelů. Základními zástupci této kategorie jsou Linux a Windows Server. [37]

2.2 VDI vs Session Based Desktops

Důležitým rozhodnutím je volba mezi VDI (Virtual Desktop Infrastructure, virtuální desktopová infrastruktura) nebo Session Based Desktops (desktopy založené na relacích). Od tohoto rozhodnutí se dále odvíjí nejen potřebný software, ale i hardware. Dále je důležité si ujasnit, jaké funkcionality jsou od řešení očekávány, zda je to práce s jednoduchými programy, nebo práce s CAD. Další překážkou může být použitý software, který nemusí podporovat multi-session OS. Proto je nezbytné vybrat vhodný protokol pro vzdálené připojení, který odpovídá specifickým požadavkům. [39]

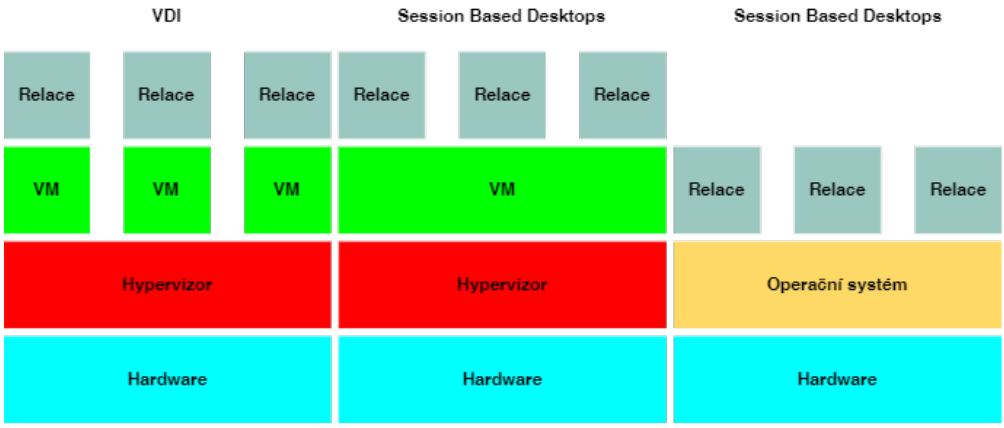
VDI

U VDI má každý připojený uživatel k dispozici svůj vlastní virtuální stroj, na kterém pracuje. Takovéto řešení s sebou přináší jak zvýšené náklady na pořizování licencí, tak i daleko větší nároky na údržbu a hardwarové prostředky. Mezi výhody naopak patří možnost personalizace VM a z pohledu bezpečnosti izolace takového prostředí od ostatních. Obecně se dá říci, že nasazení VDI je finančně náročnější. [39]

Session Based Desktops

Výhodou nasazení desktopů založených na relacích je značná jednoduchost na instalaci a správu. Klienti se připojují ke stejnému serveru, ale každý pracuje ve vlastní relaci. Takový server lze provozovat na VM (za cenu snížení výkonu), nebo přímo na HW. Nevýhodou může být menší

personalizace nebo sdílení výpočetních zdrojů s více uživateli, jelikož nelze každému uživateli přesně přiřadit hardwarové prostředky, které může využít. Využití desktopů založených na relacích s sebou také přináší finanční úsporu jak na hardwaru, tak softwaru. Nejznámějším zástupcem z této kategorie je role RDS (Remote Desktop Services), která je součástí Windows Serveru. [39]



Obrázek 2.1: Porovnání VDI a Session Based Desktops provozovaných na VM, nebo přímo na HW, inspirováno [40]

2.3 Protokoly pro vzdálený přístup k serveru

K porovnání byly vybrány následující protokoly na základě jejich rozsáhlého využití, podpoře široké škály OS a různému typu použití dle potřeb organizace, jelikož každý z protokolů přistupuje k dané problematice jinak. Základem každého z protokolů je zprostředkování přístupu ke grafickému uživatelskému rozhraní vzdálené stanice nebo serveru a k jejich prostředkům. Jejich úkolem je také zpřístupnit další funkcionality, které mohou zahrnovat přesměrování USB portů na vzdálenou stanici, přenos zvuku či podporu vzdáleného tisku.

RDP

Remote Desktop Protocol (RDP) je jeden z nejvíce využívaných protokolů ke vzdálenému přístupu na pracovní stanici nebo terminálový server vyvinutý společností Microsoft. Je součástí Windows od roku 1998, kdy byl představen společně s Windows NT 4.0 Terminal Server Edition. Byl vyvinut za účelem poskytnout možnost práce na novějších verzích systému Windows i pro uživatele, u kterých takový upgrade nebyl možný, a mezi jeho přednosti patřila možnost hostovat více uživatelských relací najednou. [41]

Role hostitele vzdálené plochy umožňuje připojení k danému PC a je podporována v desktopových verzích Windows od edice Pro a vyšších. U serverových produktů je součástí všech aktuálních verzí Windows Serveru. Roli klienta může zastupovat jakákoliv verze OS Windows díky přítomnosti programu Připojení ke vzdálené ploše (mstsc.exe). [42]

V současnosti se RDP protokol neomezuje pouze na produkty Windows, ale našel uplatnění i v jeho open-source verzi xrdp, která umožňuje připojení pomocí RDP k linuxovým strojům a podporuje většinu jeho klíčových funkcí. [43].

Nejčastěji je RDP využíváno pro přístup a práci na vzdáleném serveru, kde umožňuje souběžnou práci několika klientů, dále pro vzdálenou technickou podporu nebo vzdálenou správu jednotlivých pracovních stanic či serverů. Mezi další funkce podporované RDP patří vystavení pouze vybraných aplikací pomocí Remote Desktop app a umožnění práce s nimi. Není vhodný pro použití v prostředí, kde je potřeba přehrávání videa nebo využívání graficky náročných aplikací.

Protokol RDP podporuje několik možností přihlášení. Základní a nejstarší metodou je připojení přímo na vzdálenou přihlašovací obrazovku PC a přímé zadání přihlašovacích údajů, stejně jako na fyzickém PC, což se časem projevilo jako nedostatečné, jelikož to značně zvětšovalo vektor útoku. Dalším rozšířením bylo přidání NLA (Network Level Authentication), které vyžaduje zadání přihlašovacích údajů ještě před vytvořením RDP spojení. Tyto přihlašovací údaje jsou šifrovány pomocí protokolu CredSSP. Mezi další podporované autentizační metody patří čipové karty, certifikáty nebo Azure AD. Při použití Remote Desktop Gateway je možné využít také dvoufaktorové ověření pomocí SMS nebo mobilní aplikace, a tím zvýšit zabezpečení. Nasazení služby Remote Desktop Gateway s sebou nese další benefity, například v podobě nasazení vyrovnávání zátěže mezi několika RDP servery. [44]

Špatné nastavení protokolu RDP má za následek značné bezpečnostní riziko nejen pro samotný server, ale i pro počítačovou síť, přičemž se na hledání otevřeného portu útočníci často zaměřují různými skenovacími nástroji. Nejčastějším prohřeškem v této oblasti je otevření RDP skrze veřejnou IP do internetu, jelikož je poté velmi jednoduché podniknout na takovýto server kybernetický útok. Nejčastějším typem takového útoku je brute-force, v rámci kterého se útočník snaží uhádnout přihlašovací údaje hrubou silou, nebo také zneužití známých zranitelností. [45]

Funkce

RDP při připojení vytváří vyhrazené šifrované TLS/SSL spojení mezi klientem a vzdáleným počítačem pomocí protokolu TCP (alternativně lze použít protokol UDP). Takto vytvořeným spojením je ze vzdáleného počítače posílán směrem k připojenému klientovi obrazový výstup a směrem na vzdálený server vstupy z klávesnice, myši a dalších podporovaných zařízení. Mezi další podporované funkce patří přenos zvuku, souborů, schránky, přesměrování disků, USB připojených zařízení a lokálně připojených tiskáren do vzdáleného počítače nebo podpora více připojených monitorů. [44]

Specifikace a parametry protokolu

RDP protokol používá připojení pomocí protokolu TCP/UDP na portu 3389. Pro provoz je možné využít oba dva zmíněné transportní protokoly. V novějších verzích Windows je primárně

využíváno spojení pomocí protokolu UDP. Použití protokolu UDP nemusí být v některých nasazeních stabilní a může se projevovat artefakty v obrazu nebo zpožděním videa či zvuku, jelikož se RDP pokouší o rekonstrukci obrazu. Dále se mohou vyskytovat problémy se zaseknutím RDP na černé obrazovce či vzdálené ploše, nebo s neschopností vytvořit samotné spojení. Takovéto problémy se nejčastěji objevují v prostředí, ve kterém dochází ke ztrátě paketů, například při použití mobilního datového připojení. Řešením jmenovaných problémů s připojením je vynucení použití protokolu TCP. Nastavení parametrů spojení je závislé na dostupné šířce pásma, jelikož se v průběhu připojení tyto parametry mohou dynamicky měnit dle aktuální situace. [44, 46]

Dále podporuje široké množství parametrů, pomocí kterých je možné si ho přizpůsobit potřebám daného nasazení, ať už se jedná o výběr barevné hloubky, video kodeku, nastavení chování při přesouvání oken, zobrazení tapety plochy či jemného písma. Samozřejmostí je možnost vynutit vypnutí, nebo zapnutí již výše zmíněných funkcí. Aktuálně nejnovější dostupnou verzí je RDP 10 s podporou kodeku H.264/AVC. [44]

VNC

Virtual Network Computing (VNC) je systém sloužící k ovládání vzdáleného počítače a zobrazení jeho pracovního prostředí pomocí protokolu RFB (Remote Frame Buffer), který byl vytvořen na konci 90. let. Mezi jeho přednosti patří jeho jednoduchost a široká podpora operačních systémů. [47]

Základními prvky VNC jsou VNC server, který musí být nainstalován na hostiteli, a VNC klient, pomocí kterého se připojuje vzdálený uživatel. Na rozdíl od RDP je vhodný na vzdálenou technickou pomoc, neboť lokálně přihlášený uživatel vidí, co dělá vzdáleně připojený technik a může do této relace aktivně zasahovat. Protokol není vhodný na rychle měnící se obraz, kvůli strmému nárůstu náročnosti na přenášená data. [48]

VNC pro svou komunikaci využívá protokol TCP a port 5900, přičemž může být používán i skrze webový prohlížeč pomocí portu 5800. [47] Na Linuxových serverech je možné provozovat VNC s možností souběžného připojení více uživatelů, což umožňuje jejich práci v odděleném prostředí. V takovém případě se připojují na port 5900 + N dle jim přiřazeného čísla. Na systému Windows takové nasazení není podporováno. [49]

Značnou nevýhodou VNC je slabé šifrování přihlašovacího hesla, zbytek komunikace není šifrován vůbec, což s sebou nese značné bezpečnostní riziko. [48] Z tohoto důvodu je při použití VNC dobré uvažovat o nasazení VPN. Funkcí VPN (Virtual Private Network) je vytvoření privátního šifrovaného tunelu mezi klientem a serverem, který slouží pro bezpečný přenos dat.

Citrix ICA

Independent Computing Architecture (ICA) je protokol vyvinutý společností Citrix jako alternativa k protokolu RDP. Jeho úkolem je stejně jako u ostatních protokolů umožnění ovládání vzdáleného

počítače, přístup k předem vybraným aplikacím a přesměrování vybraných periférií na vzdálený počítač. Podporuje i nasazení společně s multi-session OS. [50]

Protokol ICA je vhodný pro graficky náročné aplikace, streamování videa nebo práci s 3D obsahem. Jako u jiných protokolů jsou i zde integrovány pokročilé bezpečnostní funkce, dvoufaktorové ověřování, vyrovnávání zátěže nebo šifrování přenášených dat. [50]

K připojení využívá protokol TCP a port 1494, na který se připojuje vzdálený klient, který je součástí sady Citrix HDX. Ke komunikaci může být také využit protokol UDP. Je navržen tak, aby využíval co nejmenší šířku pásma, jelikož využívá adaptivní kompresi. Díky tomu je schopen zvolit optimální kodek s ohledem na zatížení CPU a GPU. Dále také podporuje síťovou deduplikaci dat, což znamená, že jsou přenášeny pouze změny v obrazu či jiných datech.[50]

VMware Blast Extreme

VMware Blast Extreme je moderní protokol vyvinutý společností VMware pro přístup ke vzdálené ploše, virtuálním strojům nebo aplikacím, který je součástí VMware Horizon. Je možné ho využívat pro připojení k samostatným desktopům nebo Windows Serveru, kde podporuje připojení více uživatelů najednou za předpokladu kombinace se službou RDS. Zahrnuje také širokou paletu podporovaných zařízení a operačních systémů. [51]

Na rozdíl od protokolů RDP a VNC je dobrou volbou pro graficky náročné aplikace z důvodu podpory hardwarové akcelerace přímo na hostiteli. Tato schopnost ho činí vhodným na streamování videa nebo náročné 3D modelování. Mezi další podporované vlastnosti patří přesměrování připojených periferií na vzdálený server, stejně jako u protokolu RDP. Samozřejmostí je podpora dvoufaktorového ověřování nebo vyrovnávání zátěže mezi více servery. [51]

Ke komunikaci může využívat protokol TCP nebo UDP, přičemž je každý přenos šifrován pomocí protokolu TLS. Pro přenos obrazu je možné zvolit jeden z následujících kodeků: JPG/PNG, H.264, H.265 nebo Blast Codec. Připojení probíhá pomocí Horizon Clienta, který se připojuje na TCP port 443 ke Connection Serveru, dále se komunikace řídí podle daného nasazení, kde záleží, jestli se klient připojuje pouze v rámci vnitřní sítě, nebo ze sítí WAN. V případě sítí WAN se nejdříve klient připojuje na Unified Access Gateway, která požadavek přeposílá na Connection Server. Další podrobnosti lze nalézt v dokumentaci VMware. [51]

SPICE

Simple Protocol for Independent Computing Environments (SPICE) je open-source protokol určený pro vzdálený přístup k virtuálním strojům, vyvinutý společností Red Hat. Protokol je primárně navržen pro použití ve VDI, přičemž nepodporuje více relací, jelikož na jeden virtuální stroj může být současně připojen pouze jeden uživatel. Je implementován v open-source virtualizačních platformách, mezi které patří například KVM a Proxmox VE. [52]

Základními vlastnostmi protokolu jsou podpora více monitorů, obousměrný přenos zvuku, sdílení schránky či přesměrování USB portů. Mezi pokročilé funkce protokolu lze zařadit podporu přesměrování složek nebo podporu živé migrace VM. Dále podporuje bezeztrátovou adaptivní kompresi na základě dostupné šířky pásma pomocí speciálně navržených algoritmů přímo pro tento protokol, mezi které patří QUIC, LZ a GLZ. Díky podpoře těchto funkcí poskytuje vynikající výkon a kvalitu zobrazení grafického výstupu, což ho činí optimálním pro práci v náročných grafických programech či pro střih videa. Připojení je možné z desktopového klienta nebo webového prohlížeče. [52]

Pro svoji funkci využívá šifrované spojení pomocí protokolu TLS společně s transportním protokolem TCP a portem 3128. Šifrované spojení je použité jak pro přenos přihlašovacích údajů, tak pro přenos grafických a zvukových dat. K autentizaci připojovaných uživatelů může být využita čipová karta či kombinace jména a hesla. V pokročilých nasazeních pak lze použít i jednotné přihlášení (single sign-on) v kombinaci s LDAP, nebo MS AD. [52]

3 Tenký klient

Tenký klient je zařízení, které má za úkol zprostředkovat připojení ke vzdálenému serveru a práci v jeho pracovním prostředí s využitím jeho hardwarových prostředků [53].

Pracuje dle modelu klient-server, což s sebou přináší značné výhody. Směrem k tenkému klientovi je přenášen ze strany serveru obraz, který je poté zobrazován na připojeném monitoru. Směrem od tenkého klienta jsou na server přenášeny vstupy z klávesnice, myši a dalších k němu připojených periférií. Jeho předností jsou nízké pořizovací náklady, snadná škálovatelnost, nízká spotřeba energie nebo delší životní cyklus zařízení oproti klasickým PC, jelikož stačí upgradovat pouze serverovou část. [53]

Tencí klienti jsou nejčastěji nasazováni tam, kde je zapotřebí co nejjednodušší správa zařízení. Často nacházejí využití v PC učebnách škol nebo ve veřejných knihovnách. Dále také ve firmách, kde se například v nepřetržitém provozu střídají zaměstnanci u jednoho tenkého klienta, čímž dochází k úspoře provozních nákladů. Z pohledu bezpečnosti nabízejí větší zabezpečení dat než běžné klientské stanice, jelikož jsou všechna data uchovávána na serveru. Výhodou může také být jednoduchá nahraditelnost v případě havárie, protože stačí vyměnit pouze „kus za kus“ a uživatel může pokračovat ve svém pracovním prostředí bez nutnosti dlouhé prodlevy. [53]

Jsou plně závislí na připojení ke vzdálenému serveru a v případě jeho výpadku ztrácí daný uživatel schopnost pracovat. Předpokladem je tedy stabilní připojení k počítačové síti. Jejich použití může být také limitováno v případech, kdy je potřeba využívat specializovaných programů, pro které není tenký klient příliš vhodný, jako střih videa, hraní PC her či náročné CAD programy. Tento problém lze částečně řešit použitím správného protokolu pro vzdálené připojení. [53]

3.1 Hardware

Hardware tenkého klienta by měl být navržen co nejefektivněji tak, aby plnil svoji úlohu dle očekávání. Měl by obsahovat dostatečně výkonný procesor pro zpracování vstupních a výstupních dat. Důležitým faktorem je také jeho energetická efektivita, která by měla být co nejvyšší. Dalšími nezbytnými předpoklady jsou dostatečná kapacita paměti RAM a úložného prostoru, aby hardware splňoval nároky na instalaci a provoz OS a potřebných aplikací pro vzdálený přístup na server. [53]

Důležitý je také dostatečný počet vstupních a výstupních konektorů, tenký klient by měl podporovat různé druhy grafických výstupů pro co možná nejširší podporu různých monitorů. Dále je

potřeba vhodný počet USB portů, aby klient obsloužil nejen klávesnici a myš, ale také například externí disky, webkamery a jiná zařízení. Vhodné je při návrhu uvažovat také o připojení k počítačové síti s využitím alespoň gigabitového Ethernetu nebo rychlého Wi-Fi připojení. V neposlední řadě by klient měl také obsahovat zvukový vstup a výstup. Ideálně by měl dané parametry splňovat v co možná nejmenším formátu, aby zabíral co nejmenší prostor na pracovní ploše uživatele. Jako vhodné řešení se nabízí uchycení k monitoru pomocí VESA držáku.

Na trhu se objevuje široká nabídka vhodného HW, který se dá použít pro provoz tenkého klienta. Nejčastěji se jedná o mini PC založené na architektuře x86 s úspornými variantami procesorů. Dále jsou nabízeny různé mikropočítače založené na architektuře ARM, kde mezi nejznámější zástupce patří Raspberry Pi.

3.2 Operační systém

Operační systém tenkého klienta by měl být navržen co možná nejvíce odlehčeně a obsahovat pouze nezbytné komponenty pro jeho správné fungování. Ideálně by měl podporovat možnost vzdálené správy za účelem co nejjednoduššího nasazení a následné údržby. Rovněž by měly být dostupné pravidelné aktualizace OS, které zajistí jeho dlouhodobou podporu a udržitelnost. Při jeho návrhu lze také uvažovat o využití PXE bootu, tedy zavedení celého OS do RAM paměti tenkého klienta po jeho spuštění ze vzdáleného serveru. Důležitá je také podpora široké škály protokolů pro vzdálené připojení k serveru a jejich optimalizace pro co nejplynulejší připojení k VDI nebo RDS infrastruktuře. Nespornou výhodou může být také grafické uživatelské rozhraní, které by mělo být co nejvíce jednoduché a uživatelsky přívětivé. Operační systém by měl dále také podporovat širokou škálu architektur jako x86 a ARM pro použití na různém typu hardwaru. [54]

Dalším důležitým faktorem může být bezpečnost, přičemž by měl být systém navržen tak, aby poskytoval co největší bezpečnost pro připojování ke vzdálenému serveru a ochranu před různými typy útoků.

Na trhu je nabízená široká škála OS určená pro tenké klienty postavené na různých hardwarových architekturách, nejčastěji pro x86 a ARM, které dnes patří mezi nejpopulárnější. Níže jsou vyjmenovány některé z dostupných neproprietárních OS na základě podporované architektury, které jsou volně dostupné k zakoupení/stažení bez nutnosti nákupu konkrétního HW. Většina vybraných OS podporuje jak architekturu x86, tak ARM.

- **x86** - TLXOS, WTware, NoTouch OS, Porteus Kiosk, Openthinclient, W10 IoT, IGEL OS
- **ARM** - TLXOS, WTware, NoTouch OS, xtc, W10 IoT

3.3 Hotová HW řešení

Na trhu v oblasti tenkých klientů nabízí řada známých i menších výrobců již hotová řešení v různých cenových relacích. Některé nabízené produkty začínají v řádu tisíců Kč, zatímco ty od

značkových výrobců jako Dell, HP apod. se blíží hranici 20 000 Kč a více.

Jsou nabízena různá hotová řešení od malých jednoduchý PC typu Raspberry Pi 3/4/5 až po přenosné tenké klienty ve stylu notebooku, kdy správný výběr závisí na požadavcích na podporované protokoly pro vzdálené připojení, portovou výbavu, přenositelnost či spotřebu.

Níže jsou vybrána některá řešení, která jsou na trhu nabízena ve značném množství, a tudíž tato práce nemůže pokrýt celou aktuální nabídku tenkých klientů.

Dell

Společnost Dell nabízí širokou řadu produktů z oblasti tenkých klientů ve třech různých provedeních. Základní řadou jsou tencí klienti ve formátu mini PC řady OptiPlex 3000 a Micro, dále jsou nabízeny All-in-One tencí klienti řady OptiPlex a přenosná řešení na bázi notebooků řady Latitude 3000 a 5000. Všechny zmíněné řady využívají procesory rodiny Intel. [55]

Tencí klienti jsou dodáváni se dvěma možnými OS, a to s proprietárním Dell ThinOS nebo Windows 10 IoT. Dell ThinOS je založen na bázi OS Ubuntu s důrazem na co největší efektivitu a míru zabezpečení. Windows 10 IoT je vhodný pro zákazníky využívající v široké míře cloudové produkty společnosti Microsoft. V základním systému jsou například nabízeny aplikace jako webový prohlížeč Edge nebo MS Teams. Mezi další přednosti může také patřit široká podpora periferií. Oba zmíněné OS podporují připojení ke vzdáleným serverům pomocí VPN a širokou řadu protokolů pro vzdálený přístup, mezi které patří Citrix ICA, VMware Blast Extreme a RDP. [56, 57]

Ke všem typům tenkých klientů je nabízen software pro vzdálenou centrální správu Wyse Management Suite, který umožňuje vzdálenou změnu parametrů připojení, monitoring nebo centrální řízení aktualizací. Je nabízen ve dvou verzích, a to ve verzi Standard a Pro. Verze Standard je dostupná zdarma a je vhodná pro malé nasazení s omezenou možností správy. Verze Pro nabízí plnou sadu možností a může být hostována on-premise nebo v cloudu. [58]

Obrázek 3.1: Tenký klient Dell OptiPlex 3000, převzato z [59]

HP

Společnost HP, stejně jako společnost Dell, staví svoji nabídku na mini PC řadách t540, Elite a mobilních klientech řady Elite. Tencí klienti jsou nabízeni jak ve variantách s procesory Intel, tak AMD. Dále nabízejí speciální řadu nulových klientů Zero Client, určených pro použití s protokolem VMware Blast Extreme, kteří pro načtení OS využívají PXE boot. [60]

HP tencí klienti jsou dodáváni se širokou řadou OS zahrnující proprietární ThinPro OS, Windows 10 IoT nebo IGEL OS. ThinPro OS je založen na rodině OS Linux. Jeho výhodou je značná jednoduchost používání, vysoká úroveň zabezpečení a nízké hardwarové nároky. Každý z výše jmenovaných OS podporuje základní sadu protokolů pro vzdálený přístup, mezi které patří Citrix ICA, VMware Blast Extreme a RDP. Výběr vhodné kombinace tenkého klienta a OS je vždy potřeba určit na základě požadavků koncového uživatele. [61]

Pro vzdálenou správu tenkých klientů využívající ThinPro OS a Windows 10 IoT je nabízen software HP Device Manager, který umožňuje vzdálenou konfiguraci tenkých klientů, jejich monitoring nebo aktualizaci. Pro klienty používající IGEL OS je dostupný separátní software na webových stránkách společnosti IGEL. [62]

Fujitsu

Fujitsu nabízí v oblasti tenkých klientů mini PC řady FUTRO a mobilní tenké klienty LIFEBOOK. Hardware je založen na variantách s procesory Intel a AMD. Chlubí se vysokou odolností v náročných provozních podmínkách. [63]

Fujitsu na rozdíl od výše zmíněných výrobců nenabízí OS Windows 10 IoT, ale využívá OS eLux od společnosti Unicon. Jedná se o ultralehký OS založený na rodině OS Linux, který je navržen pro architekturu x86. Využívá ochranu proti škodlivému kódu použitím souborového systému chráněného proti zápisu. Mezi podporované protokoly pro vzdálené připojení patří Citrix ICA, VMware Blast Extreme a RDP. [64]

Vzdálená správa tenkých klientů je prováděna pomocí Scout Enterprise Management od společnosti Unicon. Umožňuje základní nastavení tenkých klientů, řízení jejich zabezpečení, správu aktualizací nebo jejich monitoring a následný reporting. [64]

Dále je důležité zmínit, že společnost Fujitsu ukončila prodej osobních počítačů v celé Evropě k dubnu 2024. Servery a disková pole budou v Evropě prodávány dále. [65].

Ncomputing

Firma Ncomputing nabízí širokou škálu tenkých klientů založených na hardwaru Raspberry Pi 3/4 a x86, společně s podporou protokolů RDP, Citrix ICA a VMware Blast Extreme. Za tímto účelem vyvíjí vlastní OS LeafOS, který je založen na Linuxu a podporuje architektury x86 a ARM. LeafOS

podporuje jak lokální instalaci, tak spuštění z připojeného externího zařízení. Mezi další nabízené benefity patří centrální správa tenkých klientů. [66]

Dalším nabízeným produktem je VERDE VDI, určený pro virtualizaci desktopů pro firemní zákazníky a školské organizace, který poskytuje centralizovanou správu pomocí webového prohlížeče. [66]

Obrázek 3.2: Tenký klient Ncomputing RX420 na bázi RPi 4, převzato z [66]

ClearCube

ClearCube má ve své nabídce tenké klienty založené na architekturách x86 a ARM, kde v kategorii x86 nabízí varianty procesorů Intel a AMD. V kategorii ARM využívá Raspberry Pi 3/4/5. Mezi přednosti uvádí vysokou energetickou účinnost jejich tenkých klientů a snadnou centrální správu. V produktové nabídce lze nalézt i speciální tenké klienty s pasivním chlazením určené do průmyslového prostředí. [67]

Tencí klienti RPi jsou dodáváni s OS StratoDesk NoTouch OS. Klienti založení na architektuře X86 jsou dodáváni s OS Win 10 IoT, NoTouch OS nebo IGEL OS. Operační systém si volí zákazník sám dle potřeby. Podporovanými protokoly pro vzdálené připojení jsou Citrix ICA, VMware Blast Extreme a RDP. [67]

Vzdálená správa tenkých klientů je realizována skrze webový prohlížeč. Nabízí jejich základní konfiguraci, monitoring či aktualizaci, jako u ostatních konkurenčních řešení. [67]

4 Vhodný serverový OS

Při výběru vhodného serverového OS pro instalaci a správnou funkčnost s tenkými klienty hraje klíčovou roli široká škála faktorů. Vše se odvíjí od daného nasazení a potřeb organizace. Při výběru je potřeba znát odpověď na následující body, které pomohou s následným výběrem OS pro danou implementaci:

1. předpokládaná cena,
2. podpora produktů společnosti Microsoft,
3. běh programů, které požadují specifický OS,
4. využití graficky náročných programů,
5. plánovaný počet současně připojených klientů,
6. požadavek na podporu určitého protokolu pro vzdálené připojení,
7. stav stávající infrastruktury.

Na základě těchto proměnných lze přistoupit k doporučení vhodného OS.

4.1 Open-source řešení

Na trhu se vyskytuje široká nabídka linuxových distribucí, které lze použít jak pro nasazení na relaci založených desktopech, tak pro VDI. Jako vhodné se jeví linuxové distribuce založené na Ubuntu, Debianu nebo RHEL, které nabízejí širokou podporu komunity a HW. Výhodou jejich použití může být také vyšší míra zabezpečení než u jiných OS. Dále by mělo být přítomné přívětivé uživatelské rozhraní, kdy může při konečném výběru záležet na předchozích zkušenostech s použitím těchto distribucí nebo na požadavku na dlouhou podporu či stabilitu systému. Pro VDI je vhodná jakákoliv distribuce s podporou vzdáleného připojení a její výběr je závislý na preferencích koncového uživatele. [68]

Open-source řešení nabízí nulové náklady jak na licence pro samotný OS v případě použití nekomerčních distribucí, tak na počet připojených klientů, který je limitován pouze dostupnými HW zdroji. Pro vzdálené připojení k linuxovým OS jsou dostupné protokoly RDP, VNC a SPICE. Využití ostatních protokolů se váže na nasazenou virtualizační platformu. Výhodou řešení na bázi Linuxu jsou nižší hardwarové nároky oproti konkurenčním OS. Níže je uveden výčet několika vhodných distribucí:

- **Ubuntu Server,**
- **Debian,**
- **Rocky Linux,**
- **Red Hat Enterprise Linux,**
- **SUSE.** [68]

Linux Terminal Server Project

Linux Terminal Server Project je open-source projekt, který je vyvíjen za účelem zjednodušení nasazování tenkých klientů do firemního a školního prostředí. Podporuje linuxové distribuce založené na Ubuntu a Debianu. Řešení v sobě integruje linuxové nástroje potřebné pro provozování tenkých klientů a jejich připojení k terminálovému serveru. Mezi podporovanými službami lze nalézt DHCP server (isc-dhcp-server), DNS server (dnsmasq) nebo PXE server (iPXE). [69]

Pro jednotlivé tenké klienty jsou připraveny obrazy OS, které jsou po jejich startu zavedeny přes síť skrze PXE, což značně usnadňuje jejich údržbu a případné aktualizace. Tenký klient se nepřipojuje přímo na server za využití již představených protokolů, ale místo toho dochází k zobrazení aplikací běžících na terminálovém serveru skrze protokol X11. Protokol X11 zajišťuje přenos grafických a dalších informací mezi serverem a tenkým klientem oběma směry. Za tímto účelem je využíván X server běžící na terminálovém serveru, který se stará o vykreslování GUI a přímou interakci s HW serveru. [69]

Pro uživatele pracujícího na tenkém klientovi se tak systém jeví, jako by pracoval přímo s lokálním PC. Přestože je možné po instalaci potřebných balíčků využívat standardní protokoly pro vzdálený přístup, vývojáři takové nasazení nepodporují ani nedoporučují. [69]

4.2 MS Windows Server

Windows Server je řada OS od společnosti Microsoft určená pro nasazení v serverových řešeních. Používá se v širokém spektru prostředí, od malých podniků až po rozsáhlá datová centra. Jeho historie sahá již do 90. let 20. století, kdy byla vydána první verze pod názvem Windows NT 3.1 Advanced Server. K přejmenování na Windows Server došlo v roce 2003 s vydáním Windows Serveru 2003. Jedná se o jeden z nejvíce využívaných serverových OS napříč firemním i školním prostředím v návaznosti na ostatní produkty společnosti Microsoft a řadu dalších programů využívajících jeho funkcí. [19]

Nabízí podporu širokého spektra funkcí společně s přehledným grafickým uživatelským rozhraním Windows. Mezi nejzásadnější podporované funkce patří adresářové služby Active Directory, DNS, DHCP, RDS (terminálový server), IIS (webový server), Microsoft SQL či síťové sdílení složek. Dostupné funkce také zahrnují roli Hyper-V, která server povýší na hypervizor a poté ho lze provozovat jako hostitele VM, jak bylo probráno v kapitole 1.3 na straně 20. [19]

Správa serveru je prováděna pomocí aplikace Správce Serveru (Server Manager), který nabízí přehled nad nakonfigurovanými rolemi a stavem serveru na jednoduchém ovládacím panelu. Další jeho funkcí je zjednodušení přístupu k položkám, jako je konfigurace síťových rozhraní, povolení vzdáleného připojení, změna názvu serveru či možnosti instalace jednotlivých rolí a jejich následné konfigurace. Za tímto účelem jsou otevírána jednotlivá konfigurační rozhraní ve vlastních oknech. Z rozhraní Správce Serveru lze spravovat i jiné servery dostupné v počítačové síti, popřípadě lze jednotlivé funkce serveru spravovat pomocí konzole PowerShell. [19]

Verze

Aktuálně dostupnou verzí je Windows Server 2022 postavený na OS Windows 10 21H2. Jeho předchůdci jsou Windows Server 2019, 2016 nebo 2012. Mezi jednotlivými verzemi lze nalézt rozdíly, a to již v základním systému, nebo v podpoře nových funkcí. Jednou z nejzásadnějších změn mezi verzemi 2019 a 2022 je přechod od webového prohlížeče Internet Explorer k prohlížeči Edge. Dále byla vylepšena podpora napojení serveru ke cloudovým službám Azure, zabezpečení samotného systému, podpora protokolu QUIC pro přenos SMB protokolu. Také došlo k přidání nových funkcí Hyper-V. [19]

Pro zákazníky jsou dostupné verze Standard a Datacenter, jak již bylo nastíněno v kapitole 1.3 na straně 20. Mezi licencemi je značný cenový rozdíl a nejzásadnějším rozdílem je podpora maximálního počtu VM. Verze Datacenter je vhodná pro provoz v režimu hypervizoru nebo v případě, že je vyžadován větší počet samostatných instalací Windows Serveru jako VM. Při instalaci je nutno zvolit, zda bude nainstalována pouze verze Core se správou pomocí příkazového řádku a PowerShellu, nebo verze s desktopovým prostředím a grafickými nástroji. [19]

Licencování

Licencování Windows Serveru lze rozdělit na dvě samostatné větve. Výběr správného licenčního modelu závisí na použití samotného serveru, instalovaných rolích a plánech na budoucí rozšíření jeho použití. První větví jsou samotné licence OS a druhou větví přístupové licence, které opravňují uživatele/zařízení přistupovat k serverovým prostředkům. Správný výběr je důležitý také z důvodu, že se může značně promítnou do nákladů celého nasazení, případně způsobit problémy s budoucím rozšířením. [19]

Licence Windows Serveru

Licencování Windows Serveru probíhá na základě počtu fyzických jader všech procesorů serveru, zakoupené licence vždy tento počet musí pokrýt. Jednotlivé licence jsou prodávány po dvou jádrech, počet vláken procesorů nehraje roli. Minimálně lze zakoupit 8 licencí, což pokrývá 16 fyzických jader serveru. Další licence lze dokupovat po jedné a pokrýt jimi zbylá jádra. V případě nasazení Windows Serveru jako VM na konkurenčním virtualizačním řešení je také potřeba pokrýt

všechna fyzická jádra hostitele, nehledě na počet přiřazených jader VM. Níže jsou uvedeny příklady možného licencování. Verze Standard i Datacenter mají stejné podmínky pro licencování a liší se pouze v počtu maximálních instancí Windows Serveru při jeho virtualizaci. Správné licencování lze ukázat na následujících příkladech, kde je v závorce udáván celkový počet jader/vláken serveru a jedna licence se rovná dvěma fyzickým jádrům.

1. **příklad** - server (1 CPU (celkem 16 jader/32 vláken)) = 8 licencí (1 licence = 2 fyzická jádra).
2. **příklad** - server (2 CPU (celkem 16 jader/32 vláken)) = 8 licencí.
3. **příklad** - server (1 CPU (celkem 24 jader/48 vláken)) = 12 licencí.
4. **příklad** - Windows Server VM (8 vCPU), server (16 jader/32 vláken) = 8 licencí.
5. **příklad** - Windows Server VM (8 vCPU), server (32 jader/64 vláken) = 16 licencí. [19]

Přístupové licence

K pořízené licenci Windows Serveru je potřeba zakoupit přístupové licence CAL (Client Access License) opravňující klienty přistupovat k prostředkům, které poskytuje Windows Server (vztahuje se na osoby či na zařízení v síti). Mezi tyto prostředky patří například adresářové služby AD, použití DHCP serveru, přístup ke sdíleným síťovým složkám, RDS, využití DNS serveru nebo použití databáze Microsoft SQL společně s webovým serverem. Licence CAL se vždy kupují ve stejné verzi, jako je instalovaná verze Windows Serveru. Lze je použít i k provozování starších verzí Windows Serveru, ale naopak nelze používat starší licence CAL s vyšší verzí Windows Serveru, než pro kterou byly určeny. [19]

Přístupové licence se dělí na licence pro jednotlivé uživatele serveru (Client CAL), na zařízení přistupující k serveru (Device CAL) a na licence pro externí uživatele mimo organizaci (External Connector). Licence lze jednotlivým uživatelům/zařízením dokupovat dle potřeby. Pro každou organizaci je důležité zvolit správný licenční model, jelikož jeho výběr výrazně ovlivňuje celkové náklady na pořízení celého řešení. Jednotlivé přístupové licence lze kombinovat, ale není to doporučováno kvůli zhoršení přehlednosti. Každá licence by měla podléhat evidenci, jakému uživateli nebo zařízení byla přiřazena. Jednotlivé licence jsou přenositelné po ochranné lhůtě 90 dnů. [19]

User CAL

Licencování na základě počtu uživatelů přistupujících k prostředkům serveru se odvíjí od počtu osob využívajících služby serveru. Předností této licence je, že každý uživatel může přistupovat k serveru a jeho službám z neomezeného počtu zařízení. Toto je výhodné zejména v prostředích, kde není pevně stanoven počet zařízení, ale počet uživatelů je předem znám. [19]

Device CAL

Licencování na základě počtu zařízení je vhodné do prostředí, kde je předem znám počet zařízení, ale není dostupný přehled o počtu uživatelů. Vhodným příkladem může být počítačová učebna, u které je znám přesný počet PC, ale počet uživatelských účtů může tento počet značně přesáhnout. [19]

External Connector Licenses

External Connector Licenses jsou ideální pro situace, kdy server a jeho služby využívají osoby mimo provozující organizaci, jelikož není možné přesně určit počet uživatelů nebo zařízení. Nejčastěji se jedná o použití webového serveru společně s MS SQL, například pro provoz komplexního školního systému, ke kterému přistupují i rodiče žáků. [19]

Active Directory (AD)

Adresářové služby Active Directory jsou jednou z nejzásadnějších funkcí, kterou Windows Server nabízí. Jedná se o komplexní správu uživatelů, síťových politik, přístupových práv, politik hesel, bezpečnostních skupin a zařízení. Všechny tyto záznamy jsou uloženy v hiearchické struktuře. Nachází uplatnění v široké škále organizací a je základem mnoha systémů, které využívají její přednosti a jednoduchou obsluhu. Server, na kterém je spuštěna služba AD, se nazývá řadič domény. Pokud je služba spuštěna na více serverech, je jeden server určen jako primární řadič domény a další servery jako sekundární, pro případ selhání primárního řadiče. Instalace této role je doporučována na samostatný server nebo do samostatného VM, bez instalace dalších rolí kromě role DNS. [19]

Nasazení řadiče AD je spojeno s instalací role DNS serveru, na kterém je založena nová kořenová doména, kterou bude organizace využívat. Při zakládání nové domény se doporučuje použít subdoménu již existující domény organizace. Pokud se jedná o testovací prostředí, je doporučeno použití testovací TLD .lan. Po nakonfigurování domény je nutné jako primární DNS pro PC nastavit IP adresu doménového serveru a jednotlivá PC do domény připojit. Pro připojení PC do domény je nutné, aby na něm byl nainstalován OS Windows minimálně ve verzi Pro. [19]

Jednotliví uživatelé a počítače jsou v doménové struktuře zařazováni do organizačních jednotek (OU) na základě jejich příslušnosti, například do vedení a zaměstnanců firmy. Na jednotlivé OU lze aplikovat skupinové politiky (GPO) a řídit jimi chování uživatelů nebo počítačů připojených do domény. [19]

DNS

Role DNS je klíčová při nasazení společně s AD, jelikož slouží k vyhledávání všech členů připojených do domény, ať už jde o řadiče domény nebo jednotlivá PC. Veškeré DNS záznamy

jsou sdíleny mezi jednotlivými řadiči domény, aby byla zaručena funkčnost v případě výpadku primárního řadiče domény. Veškerá komunikace mezi členy domény je realizována skrze jejich doménová jména, přičemž jako primární DNS musí být nastaven doménový řadič. Další funkcí, kterou plní v doménové struktuře, je role rekurzivního DNS serveru, který předává dotazy mimo spravovanou zónu nadřazeným DNS serverům. Tato role může být nasazena i bez AD. [19]

Podporovaná je široká škála DNS záznamů, které lze jednoduše spravovat přes ovládací panel DNS serveru. Mezi pokročilé funkce lze zařadit podporu load balancingu (vyrovnávání zátěže, např. mezi webovými servery) nebo DNSSEC, který chrání před zfalšováním odpovědí DNS serveru (DNS spoofingem). [19]

DHCP

Po instalaci role DHCP serveru může Windows Server fungovat také jako DHCP server, což zjednodušuje správu sítě, jelikož tento krok umožňuje centralizaci všech síťových služeb do jednotného prostředí, což je výhodné při využití zmíněných rolí Windows Serveru. Správa probíhá skrze ovládací panel DHCP serveru, který nabízí přehled nad zapůjčenými adresami či statickými rezervacemi pro jednotlivá zařízení. Podporuje přidělování všech potřebných parametrů protokolu DHCP pro připojená zařízení v síti. [19]

Remote Desktop Services (RDS)

Remote Desktop Services, dříve známé pod názvem Terminal Services, jsou klíčovým prvkem, který nabízí Windows Server v oblasti vzdáleného připojení a souběžné práce více uživatelů na jednom serveru. Server, který takovou roli v síti zastává, je často nazýván terminálovým serverem, a pro připojení k němu je využíván protokol RDP popsaný v kapitole 2.3 na straně 29. [19]

Role RDS může být nasazena ve dvou rolích v závislosti na potřebách organizace. Mezi klíčové faktory pro volbu patří přizpůsobitelnost prostředí pro jednotlivé uživatele, omezení softwaru pro souběžnou práci více uživatelů nebo finanční prostředky. [19]

- **Hostitel relací vzdálené plochy** – umožňuje souběžné připojení více uživatelů k terminálovému serveru. Každému uživateli je vytvořena samostatná relace vzdálené plochy, ve které následně pracuje. Jedná se o jedno z nejčastěji používaných řešení pro vzdálené připojení, hlavně díky jeho jednoduchosti. Výhodou je správa pouze terminálového serveru, což přináší značné časové a finanční úspory. Mezi nevýhody takového řešení patří nemožnost správy HW prostředků přidělených jednotlivým uživatelům. [19]
- **Hostitel virtualizace vzdálené plochy** – jednotlivým uživatelům jsou přiřazeny VM v rámci VDI infrastruktury, což zaručuje práci v odděleném prostředí. Výhodou je vyšší bezpečnost než u připojení založených na relacích, lepší personalizace a podrobná správa přidělených HW prostředků. Podporované OS zahrnují Windows 10 a 11 ve verzi Enterprise, Windows Server, případně může být použita jakákoliv Linuxová distribuce.[19]

Další klíčovou rolí podporovanou RDS je Remote Desktop Connection Broker, který nachází využití v nasazeních s více terminálovými servery. Stará se o distribuci jednotlivých vzdálených připojení mezi terminálové servery a zajištění vysoké dostupnosti. [19]

Pro připojení mimo perimetr sítě je dostupná role Remote Desktop Gateway, která se stará o zabezpečené připojení vzdálených klientů k terminálovým serverům. Komunikace mezi klientem a serverem probíhá pomocí šifrovaného spojení za použití protokolu HTTPS, což umožňuje obejít omezení některých firewallů. Pro zvýšení zabezpečení může být po uživateli vyžadováno přihlášení pomocí dvoufaktorového ověřování. [19]

Dalším způsobem vzdáleného připojení je použití webového prohlížeče skrze roli Remote Desktop Web Access. Tato role poskytuje přístup ke vzdáleným plochám uživatelů nebo jednotlivým aplikacím vystavených správcem systému. [19]

Licencování

Pro provoz RDS je potřeba zakoupit licence RDS CAL, jelikož bez těchto licencí není možné terminálové služby provozovat. K jejich použití nestačí samotné licence CAL, které opravňují uživatele nebo zařízení přistupovat k prostředkům serveru. Na rozdíl od licencí CAL je nutné licence RDS CAL aktivovat po instalaci role licenčního serveru, který se stará o jejich správu a přiřazování licencí jednotlivým uživatelům a zařízením v síti, které se připojují k terminálovým serverům. Licencování je prováděno na základě počtu uživatelů (RDS User CAL) nebo zařízení (RDS Device CAL), která se k serverům připojují. Kombinace obou typů těchto licencí není možná, a proto je při realizaci důležité zvážit a vybrat nejvýhodnější řešení, přičemž je vhodné myslet i na budoucí potřeby. Níže jsou uvedeny jednotlivé typy licencí s jednoduchými příklady. [19]

- **RDS User CAL** - umožňuje jednomu uživateli přistupovat k terminálovým službám z libovolného počtu zařízení. Používá se v případech, kdy u jednotlivých uživatelů dochází k častému střídání zařízení, ze kterých se připojují. [19]
- **RDS Device CAL** - umožňuje libovolnému počtu uživatelů přistupovat k terminálovým službám z jednoho zařízení. Používá se v případech, kdy dochází na jednom zařízení k častému střídání uživatelů, tudíž by bylo nevýhodné pro každého uživatele kupovat licenci zvlášť. Často se využívá například v počítačových učebnách, kde dochází k častému střídání uživatelů, ale počet PC zůstává neměnný. [19]

Pro oba typy licencí RDS CAL platí stejná omezení ohledně verzí, ve kterých byly zakoupeny, jako je tomu u standardních CAL. Lze je libovolně kombinovat jak s licencemi User CAL, tak Device CAL, ale ve většině nasazení dochází ke kombinaci stejných typů licencí. [19]

5 Kybernetická bezpečnost školských organizací

Kybernetická bezpečnost hraje v dnešním světě důležitou roli, přičemž v této oblasti je nezbytné předcházet rizikům spojeným s provozem škol. Školy v dnešní době ve velké míře spoléhají na digitální infrastrukturu a jsou na jejím fungování závislé. To zahrnuje nejen informační systém školy a cloudové služby, ale také další infrastrukturu školy, jako jsou kamerové systémy, serverové adresářové služby, Wi-Fi síť školy a „vratné“ čipové otevírání dveří.

Mezi hrozby, kterým čelí školské organizace, patří například riziko úniku citlivých údajů o zaměstnancích, žácích či jejich zákonných zástupcích, případně rozšíření ramsomware mezi zařízeními v síti či různé phishingové a malwarové útoky. Častým typem útoků, se kterým se lze setkat, je také sociální inženýrství, jehož cílem je z dané oběti vylákat důvěryhodné informace. Důležitou roli v této oblasti hraje pravidelné vzdělávání zaměstnanců a žáků, které zahrnuje představení možných rizik při používání digitálních technologií. Kybernetická bezpečnost celé organizace stojí na každém jednom uživateli v příslušné síti. [70]

Zranitelností ve školských organizacích může být celá řada, ať už se jedná o nedostatečně udržovaný informační systém, zastaralost a špatný návrh celé infrastruktury, nevyhovující ochranu perimetru, nedbalý monitoring sítě nebo nedostatečné bezpečnostní povědomí uživatelů a administrátorů. [70]

Každá školská organizace by měla provádět analýzu rizik a následné vyhodnocení, jak je daným rizikům předcházeno. Po provedené analýze rizik by měla být zajištěna realizace opatření tak, aby byla rizika odstraněna, nebo zmírněna. Všechna zjištěná rizika a nápravná opatření by měla být pravidelně monitorována a kontrolována, přičemž by celý proces měl být po určité době opakován z důvodu možného výskytu nových rizik. [70]

5.1 Fyzická bezpečnost

Jedná se o důležitou součást kybernetické bezpečnosti, která je velice často podceňována, což může vést ke značným škodám na samotných zařízeních či k úniku dat. Jejím úkolem je tato rizika minimalizovat. Fyzická bezpečnost se věnuje správnému zabezpečení perimetru, kontrole přístupu a ochraně počítačových systému před jejich neoprávněnými úpravami. [70]

Úkolem zabezpečení perimetru je vymezit prostor, kde se nacházejí chráněná aktiva (prvky sítě, PC systémy, servery). Pro správné vymezení perimetru je potřeba provést analýzu rizik jednotlivých

prostor, v nichž se prvky nachází a na základě provedené analýzy určit, jaká opatření v rámci těchto prostor je potřeba aplikovat. Prostory je možné zajistit například kamerovým systémem, systémem detekce pohybu či identifikací osob a jejich následným monitoringem při pohybu v rámci chráněných prostor. [70]

Další součástí fyzické bezpečnosti je kontrola přístupu, která má na starosti určení oprávněných osob pro vstup do chráněných prostor tak, aby nedošlo k neoprávněným zásahům do chráněných aktiv. Nejčastěji používaným způsobem zabezpečení jsou klasické zámky nebo čtečky karet. Pokud by bylo potřeba zajistit ještě větší kontrolu přístupu, může být využito ostrahy nebo různých biometrických zabezpečovacích systémů. [70]

Chránění počítačových systémů a klíčových systémů sítě by mělo být realizováno v oddělených prostorách, které by mělo být možno uzamknout. Pokud plné uzamčení prostor není možné, měla by ochrana být realizována alespoň formou zamykatelné rackové skříně. Pro případ překonání těchto opatření by měla být realizována ochrana i na samotných zařízeních, a to formou detekce manipulace se zařízením, šifrováním dat či omezením přístupu k nastavení pomocí hesla. [70]

Ve školských organizacích by taková opatření měla být realizovaná minimálně na úrovni uzamykatelných rackových skříních, oddělené serverové místnosti s kritickými systémy a servery, případně umístěním prvků na těžko dosažitelná místa. U počítačových systémů, jako jsou počítače v učebnách či zařízení učitelů, by měla být ochrana realizována alespoň zabezpečením přístupu do UEFI, šifrováním dat na disku, popřípadě uzamykatelnými PC skříněmi. [70]

5.2 Ochrana sítě

Správně nastavená a chráněná počítačová síť je jedním za základních pilířů kybernetické bezpečnosti. Pokud síť není dostatečně chráněná, pak není možné zaručit ochranu počítačových systému a dalších zařízení nacházejících se v ní. Při implementaci bezpečnostních mechanizmů by neměl být brán zřetel pouze na samotné prvky sítě a počítačové systémy, ale i na ochranu jiných osob využívající síť, případně celého internetu, před útoky ze spravované sítě. [70]

Důležitým prvkem při ochraně sítě je účinná ochrana na 1. vrstvě TCP/IP. Mezi nejvíce používané metody se řadí logické rozdělení sítě pomocí VLAN na různé segmenty a jejich následné přiřazení na porty přepínače. Rozdělení sítí do VLAN by mělo být realizováno tak, aby kritické systémy a jejich management byly v sítích oddělených od ostatních zařízení. Stejným způsobem by mělo být řešeno oddělení ostatních systémů, které spolu nemusí přímo komunikovat, nebo to dokonce není žádoucí. Při implementaci VLAN nesmí být zanedbáno jejich následné oddělení na 2. vrstvě TCP/IP pomocí firewallových pravidel, a to omezením komunikace mezi nimi, případně nastavením kompletní blokace. [70]

Dalšími prvky, které pro zvýšení zabezpečení lze implementovat, jsou MAC filtrace nebo ověřování připojených uživatelů a zařízení pomocí protokolu 802.1X. MAC filtrace je způsob ochrany sítě, přičemž jsou na jednotlivých portech přepínačů, případně přístupových bodech, specifikovány

povolené MAC adresy zařízení, které se k těmto prvkům mohou připojit. Jedná se o relativně funkční opatření, které vyžaduje značné časové nároky na udržování nastavení jednotlivých prvků a přiřazení správných MAC adres. Takovéto opatření lze obejít pomocí MAC spoofingu, při kterém útočník zfalšuje MAC adresu povoleného zařízení. V případě nasazení 802.1X je pro připojení do drátové, případně bezdrátové sítě, vyžadováno ověření pomocí uživatelského jména a hesla nebo pomocí certifikátu. Rozhodnutí o přidělení do příslušné VLAN je realizováno na základě členství uživatele v určité skupině. Pro přenos informací mezi klientem a RADIUS serverem je používán EAP protokol, který se stará o autentizaci připojovaných klientů. [70]

Nedílnou součástí ochrany sítě je také dostatečné zabezpečení Wi-Fi sítí, které k útokům vybízí útočníky nejvíce, a to díky jednoduché dosažitelnosti. Nejpoužívanější metodou je oddělení zaměstnaneckých Wi-Fi sítí od sítí pro hosty či soukromá zařízení. Zabezpečení těchto sítí by mělo být realizováno alespoň pomocí protokolu WPA2, ideálně protokolem WPA3, případně v kombinaci s MAC filtrací nebo protokolem 802.1X. [70]

V neposlední řadě by mělo být nasazeno dostatečné zabezpečení na perimetrových prvcích sítě, jako jsou routery či modernější firewallová řešení. V případě těchto prvků by měla být nasazena pravidla, která řídí přicházející a odcházející provoz ze sítě, ať už na základě cílových/zdrojových IP adres nebo zdrojových/cílových portů. Případně lze zabezpečení rozšířit o kontrolu šifrovaného provozu nebo IDS (Intrusion Detection System)/IPS (Intrusion Prevention System) řešení. Systém IDS se používá k detekci podezřelého provozu v síti v reálném čase. Za tímto účelem monitoruje síťový provoz a hledá v něm útoky na základě předem určených pravidel a vzorců chování. Dokáže detekovat širokou škálu útoků, od jednoduchého skenování sítě až po pokusy o zneužití zranitelností různých systémů. Na základě detekce takovýchto útoků může upozornit správce systému. Pokud je IDS kombinován s IPS, může systém při detekci útoku reagovat a podniknout patřičná opatření k jeho zastavení, například blokováním škodlivého provozu. [70, 71]

5.3 Standard konektivity

Pro usnadnění naplnění základních bezpečnostních pravidel ve školských organizacích vznikl v roce 2022 dokument „Standard konektivity škol“. Tento standard se týká základních škol, středních škol, vyšších odborných škol a konzervatoří. Specifikuje cílový stav školní síťové infrastruktury. Jeho cílem je podpora digitální gramotnosti a informatického myšlení žáků, zároveň se zvýšením kybernetické bezpečnosti ve jmenovaných institucích. S představením tohoto standardu zároveň vznikla dotační výzva, která je součástí Integrovaného regionálního operačního programu (IROP) 2021-2027. Na základě této výzvy mohou školy žádat finanční prostředky na obnovu síťové infrastruktury. [72]

Standard konektivity určuje povinné a doporučené parametry vnitřní infrastruktury, ke kterým by zapojené vzdělávací instituce měly směřovat. Zároveň je jeho splnění nutné k čerpání dalších prostředků z IROP. Je rozdělen do několika částí, které se týkají konektivity školy k veřejnému internetu (WAN), vnitřní konektivity školy (LAN a WLAN) a dalších bezpečnostních prvků, které lze

pro zvýšení kybernetické bezpečnosti nasadit. Zapojené instituce se zároveň zavazují k připojení k federované autentizační a autorizační službě eduroam sdružující vzdělávací instituce, kterou spravuje sdružení CESNET. [72]

U připojení k veřejnému internetu jsou stanoveny minimální rychlosti, které se odvíjí od počtu žáků nebo koncových uživatelských zařízení. Zároveň má být přidělena veřejná IPv4 adresa společně se zajištěním monitoringu a logování síťového provozu v minimální délce 3 měsíců. Logování by mělo být realizováno s cílem umožnit sledování veřejného provozu směřujícího k vnitřnímu koncovému zařízení a naopak. Doporučeno je také nasazení protokolu IPv6. Dále jsou specifikována doporučení na síťové prvky, mezi které patří například firewall, který by měl podporovat již představené funkce IDS/IPS a kontrolu šifrovaného provozu. V neposlední řadě jsou také specifikovány požadavky na web školy, poskytovatele síťového připojení či na zajištění bezpečnosti DNS serverů. [72]

Vnitřní konektivita školy specifikuje rychlost sítě LAN, která by měla být minimálně 1 Gbit/s. Dále se věnuje správě uživatelských účtů, jelikož zakazuje používání anonymních účtů. Instituce by měla využívat centrální řešení pomocí LDAP nebo MS AD, aby bylo umožněno auditovat přístup k síti s dohledáním na jednotlivé uživatele. Také specifikuje požadavky na zálohování serverové infrastruktury, antivirovou ochranu počítačových systémů a páteřní rozvody mezi budovami. U síťových prvků specifikuje minimální parametry, které musí splňovat. Mezi ně patří například podpora VLAN nebo protokolu 802.1X. Kromě toho se také věnuje bezdrátovým sítím (WLAN), u kterých je vyžadována podpora izolace klientů, standardu IEEE 802.11ac (Wi-Fi 5) nebo vyššího, společně se zajištěním oddělených sítí pro zaměstnance, žáky/studenty a hosty. Pro zabezpečení by měl být nasazen standard WPA2-Enterprise nebo WPA3-Enterprise. [72]

Nakonec se věnuje doporučeným bezpečnostním prvkům, mezi které lze zařadit systémy pro monitorování síťové a serverové infrastruktury. Dalšími zmiňovanými prvky jsou nástroje pro detekci nelegitimního provozu, podpora VPN, nástroje pro centrální správu a audit ICT prostředků, systém uživatelské podpory nebo zavedení dvoufaktorové autentizace. [72]

Ve školských organizacích by představená opatření měla být minimálním standardem pro budování bezpečných sítí a zajištění jejich dlouhodobého správného fungování ve vzdělávacím procesu.

6 Stav před realizací

Analýza současného stavu je důležitou součástí práce, jelikož bude implementována do praktické části, která se od ní bude odvíjet. Praktická část tak bude navazovat na některá již použitá řešení - ta buď zůstanou v původní podobě, nebo bude nepatrně změněna jejich konfigurace či použití.

Před zahájením analýzy stavu před revitalizací PC učeben byla sjednána schůzka s IT správcem školy, v rámci které byla domluvena možnost nahlédnout jak do původního řešení obou učeben, tak do zbytku celé infrastruktury, a zmapovat tak jednotlivá řešení. Takto získané poznatky byly využity při následujících konzultacích, návrhu řešení a konečné implementaci.

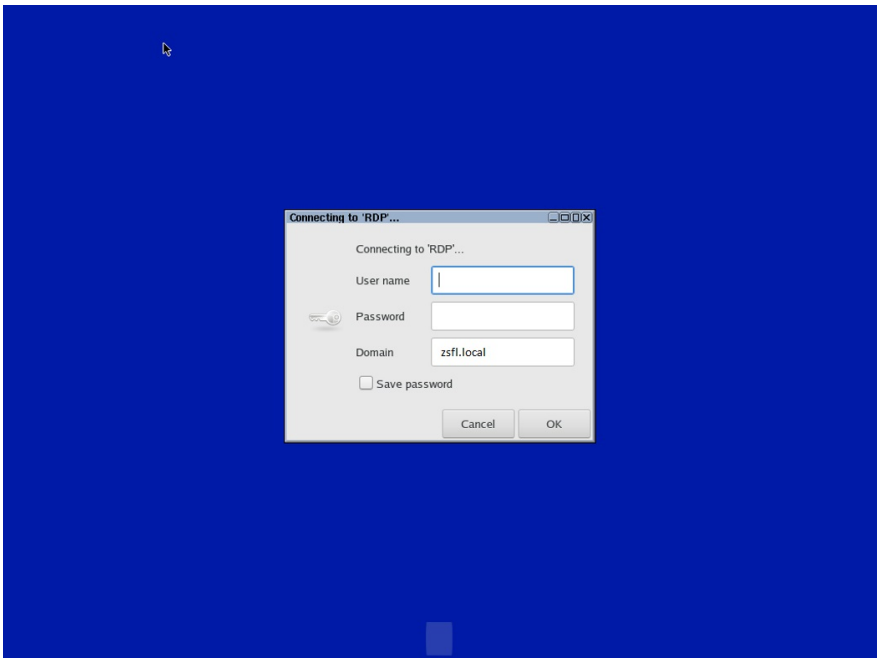
6.1 PC učebny

Škola používá pro výuku informačních a komunikačních technologií dvě PC učebny se 30 pracovními místy a jedním učitelským PC. Jedná se o 60 žákovských stanic a 2 učitelská PC, celkem tedy 62 pracovních míst. Při prohlídce žákovských stanic bylo zjištěno řešení dnes již velice zastaralými tenkými klienty HP Compaq t5720, ke kterým již není poskytována hardwarová ani softwarová podpora ze strany výrobce. Společně s nimi byly používány zastaralé monitory Samsung s poměrem stran 4:3 a rozlišením 1280x1024. Pro každou učebnu bylo zjištěno použití vlastního terminálového serveru společně se samostatnou podsítí. Vzdálené připojení k těmto serverům bylo realizováno pomocí protokolu RDP.

Vzhledem k požadavkům nových verzí RDP protokolu na ověřování NLA bylo nutné při přechodu na novější verze serverových OS nahradit OS tenkých klientů kompatibilním řešením, které dokáže jeho hardware provozovat. Při řešení tohoto problému došlo k rozhodnutí nasadit TinyCore Linux, který má velmi nízké hardwarové nároky, a softwaru Remmina, který umožňuje vzdálené připojení k serveru pomocí mnoha různých protokolů. Za účelem podpory připojení pomocí protokolu RDP byla na každém tenkém klientovi provedena instalace balíčku freerdp. Automatické spouštění Remminy s příslušnou konfigurací pro konkrétní učebnu bylo realizováno startup skriptem.

V danou chvíli bylo řešení vyhodnoceno jako nevyhovující, a to z důvodu neexistující optimalizace OS a softwaru na hardware tenkého klienta. Při vzdáleném připojení k serveru nestíhali správně zpracovávat obraz, docházelo k jeho dlouhému vykreslování a několika sekundovým zásekům. Mezi další zásadní problémy lze zařadit samotné rozhraní programu Remmina, které není uzpůsobeno na provoz v bezobslužném režimu. Často docházelo k tomu, že žáci mazali předpřipravené

připojení, upravovali ho nebo měnili nastavení samotného programu. V neposlední řadě byla zjištěna absence jakékoliv centrální správy. Její nepřítomnost měla za následek, že v případě aktualizace tenkých klientů nebo úprav jejich konfigurace bylo nutné obcházet všechny pracovní stanice, což není časově efektivní a sráží to výhody použití tenkých klientů.



Obrázek 6.1: Přihlašovací obrazovka tenkého klienta původního řešení [autor]

6.2 Serverový software

Dále bylo přistoupeno k analýze instalovaných OS na serverech, kde byla zjištěna instalace OS Windows Server ve verzích 2016 (DELL) a 2019 (skládaný). Pro tyto OS má škola zakoupené licence, včetně přístupových licencí CAL a RDS CAL na přesný počet zařízení v obou učebnách. Pro instalaci OS na serverech byly použity samostatné disky, z důvodu oddělení uživatelských dat od systémových pro případ poškození systémového disku. Takové řešení není vyhovující.

Na obou serverech byla zjištěna instalace následujících rolí: Active Directory Domain Services, DNS, Hostitel relací vzdálené plochy a licencování vzdálené plochy. Na každém ze serverů běžel samostatný řadič domény s vlastní doménou, která byla využita pouze v rámci učebny. Toto řešení není ideální a není v souladu ani s pravidly pro nasazení role Active Directory, která by měla být nainstalována na samostatném serveru/VM. Použité domény byly zsfl.local a zsfl-new.local, což neplní aktuálně doporučované standardy pro lokální doménová jména. Hlavním problémem tohoto řešení byla neprovázaná správa uživatelů skrze jednu databázi Active Directory a skupinových politik. Vše bylo nutné vytvářet a nastavovat dvakrát. Při prohlídce AD byla odhalena skutečnost, že se pro připojení z jednotlivých tenkých klientů využívají sdílené uživatelské účty ve formátu klient01 až klient30. Tudíž mohlo docházet k různým zásahům do systému bez možnosti dohledání, který žák tuto změnu způsobil, což není v souladu s frameworkem AAA.

6.3 Serverový hardware

Při prohlídce serverového řešení byla odhalena přítomnost dvou fyzických serverů bez virtualizace a pravidelného zálohování. U prvního ze serverů bylo zjištěno, že se jedná o velmi zastaralý server DELL, který je z dnešního pohledu nevyhovující jak po stránce výkonu, tak po stránce efektivity. U druhého serveru byla zjištěna skutečnost, že je sestavený z běžně dostupných komponent s dostačujícím výkonem a relativně efektivním provozem. Oběma serverům scházela podpora jakékoliv vzdálené správy typu Out-of-band management, která by administrátorovi usnadnila jejich správu, běžnou údržbu a dohled nad nimi. Dalším zjištěným neduhem byla absence technologie typu RAID, přičemž v případě selhání disku mohlo dojít k okamžitému zastavení systému a nemožnosti poskytovat danou serverovou službu.

Parametry serveru DELL PowerEdge 2950:

- **Procesor:** 2x Intel Xeon E5410 4 jádra 2,33 GHz
- **Operační paměť:** 32 GB DDR2 667 MHz
- **Úložiště:** 2x DELL SAS 300 GB

Parametry skládaného serveru:

- **Procesor:** AMD Ryzen 9 3900X 12/24 jader 3,8 GHz
- **Operační paměť:** 32 GB DDR4 3200 MHz
- **Úložiště:** 2x Samsung 970 PRO 512 GB

6.4 Síť a síťové prvky

V poslední řadě došlo ke zmapování konektivity jednotlivých učeben, která dle prokázaných skutečností byla již nevyhovující, jelikož učebny byly připojeny pouze starými nespravovatelnými přepínači s přenosovou rychlostí 100 Mbit/s. U připojení tenkých klientů bylo zjištěno, že část je připojena do přepínače v učebně a druhá polovina do zásuvek, které jsou přivedeny do centrálního racku. U propojení jednotlivých učeben s centrálním rackem bylo zjištěno použití strukturované kabeláže CAT 5e, která vyhovuje i moderním standardům ethernetu. Pro obě učebny byly použity dvě oddělené podsítě s IP adresami 10.84.45.0/24 a 10.84.47.0/24, které má na starosti firewall FortiGate 80F zajišťují přístup školy k internetu.

Jelikož strukturovaná kabeláž a firewall splňují předpoklady k dalšímu rozvoji, nebude nutné u těchto prvků přistoupit k výměně. Co se týká IP adresace, tak může být pro lepší přehlednost zachována i v rámci nového řešení.

7 Analýza potřeb školy

Před započetím samotné realizace revitalizace počítačových učeben bylo zapotřebí provést analýzu očekávaných výstupu výsledného řešení na základě požadavků vedení školy, správce IT a učitelů, kteří dané učebny používají nebo plánují používat.

Při jednání s vedením školy bylo zjištěno, že je pro ně prioritou co nejnižší konečná cena za obě počítačové učebny. Dále kladlo důraz na dlouhodobou udržitelnost řešení, nízké provozní náklady a minimální budoucí výdaje na nákup licencí, ať už za účelem aktualizací, nebo pro případ rozšíření počítačových učeben při větším počtu žáků. Mimoto bylo sděleno, že škola dostala nabídku od komerčního subjektu na realizaci jedné počítačové učebny, a to v hodnotě 504 344 Kč (práce, server, tencí klienti včetně výměny učitelského PC, monitory, bez periferií a dalších potřebných prvků). Za obě učebny se tedy jedná o částku 1 008 688 Kč. Od vedení byla dále získána informace ohledně počtu pedagogických zaměstnanců, který se pohybuje okolo 50, a počtu žáků školy, který se blíží 700. Tudíž budou učebny využívány ve výuce skoro nepřetržitě a musí být zajištěn jejich bezproblémový provoz.

Dále byla provedena konzultace se správcem IT, se kterým byla probrána aktuální situace v počítačových učebnách, zkušenosti s jejich správou, případně nejčastější problémy. Bylo sděleno několik problémů, mezi které patří slabý výkon stávajících tenkých klientů, jejich zastaralost, a to po hardwarové, softwarové a morální stránce, či jejich nedostatečné zabezpečení. Navíc byly probrány požadované výstupy v oblasti infrastruktury a jejích budoucích potřeb, na které by mělo být nové řešení připraveno. Níže jsou vypsány body, ohledně kterých proběhla shoda, a které by mělo nové řešení splňovat.

- Návrh a realizace nových PC učeben a jejich připojení do stávající síťové infrastruktury.
- Co nejjednodušší správa a údržba tenkých klientů (ideálně centrální správa ze serveru).
- Výběr vhodného protokolu pro vzdálené připojení tak, aby splňoval požadavky na použití v počítačových učebnách na základě využívaného softwaru učiteli školy.
- Zavedení virtualizovaného prostředí.
- Využití serverového OS Windows Server, se kterým má správce mnoholeté zkušenost.
- Vytvoření nové domény AD s minimálně dvěma doménovými řadiči.
- Příprava na budoucí rozšíření tak, aby byla zajištěna škálovatelnost a nedocházelo k omezení ze strany virtualizačního řešení.

Posledním a zároveň důležitým krokem bylo zjištění plánovaného použití nových učeben samotnými učiteli. Nejdříve byla sjednána schůzka s učiteli ICT, se kterými byl probrán stav obou učeben. Nejčastější připomínkou byla jejich zastaralost, dále nedostatečný výkon na základní práci s webovým prohlížečem nebo balíkem MS Office, který je ve výuce hojně využíván. Mezi další zmiňované neduhy ze stran učitelů patřila nemožnost monitorovat jednotlivé žáky při výuce, kvůli absenci softwaru zajišťujícího class management, který by usnadnil hladký průběh výuky. Díky těmto skutečnostem nebylo možné vést výuku efektivně a tyto učebny byly shledány jako nevyhovující.

Následně byla vedena diskuse na téma nových učeben, především v oblasti softwarového vybavení tak, aby byl zajištěný dostatečný výkon pro provoz požadovaného softwaru a splněny všechny jeho požadavky. Do výuky by nově měly být zavedeny základy z oblasti programování, případně práce s multimediálním obsahem. Menší důraz má být nově kladen na kancelářské balíky, které by měly najít využití především v ostatních předmětech. Na základě této diskuse byl vytvořen následující výčet požadavků na podporovaný software.

- **Výuka základů programování**: Python + PyCharm, Visual Studio, Scratch, LEGO Mindstorms
- **Výuka práce s multimédii**: Inkscape, GIMP
- **Práce s webovým prohlížečem**: Tinkercad, code.org

Nakonec byla provedena analýza požadavků na nové učebny ze stran ostatních učitelů. Nejčastěji bylo zmiňováno použití počítačových učeben ve výuce předmětů jako český jazyk, matematika, přírodopis nebo zeměpis. Mezi požadovaným softwarem byl zmiňován kancelářský balík MS Office, který by měl sloužit společně s webovým prohlížečem k podpoře výuky v těchto předmětech, například pro psaní referátů. U předmětu matematika byl dále zmíněn požadavek na podporu programu GeoGebra.

Všechny takto nasbírané požadavky a poznatky byly následně použity během testování dostupných technologií a při následném návrhu celé infrastruktury učeben tak, aby byly splněny očekávané výstupy.

8 Testování dostupných technologií tenkých klientů

Testování dostupných technologií na základě provedené rešerše v oblasti tenkých klientů hrálo zásadní roli pro budoucí návrh počítačových učeben. Na základě vyslovených požadavků byly z testování vyjmuty některé výše zmíněné technologie z oblasti virtualizace a protokolů pro vzdálené připojení, jelikož by licenční náklady nebyly pro školu únosné a s ohledem na jednotlivé požadavky by byly i zbytečné. Pokud by v požadavcích nebylo striktně vymezeno použití produktu Windows Server a softwaru, který podporuje pouze rodinu OS Windows, bylo by vhodné otestovat i open-source řešení. Nejvíce by se v takovém případě nabízelo řešení pomocí virtualizace Proxmox v kombinaci s protokolem SPICE v případě VDI, nebo VNC/RDP v případě desktopů založených na relacích.

Pro efektivní testování vybraných řešení byla důležitá volba vhodného serverového hardwaru, který se bude co nejvíce blížit reálnému nasazení v praxi tak, aby zvládal roli hostitele a provoz několika VM. Za tímto účelem byl zapůjčen server Dell PowerEdge R730 s následující konfigurací.

- **Procesor:** Intel Xeon E5- 2697A v4 16 jader 32 vláken 2,6 GHz
- **Operační paměť:** 1024 GB DDR4 2400MHz
- **Úložiště:** RAID 1 2x 200 GB SAS SSD, RAID 5 4x 600 GB SAS HDD

Jako OS pro testování byl na server nainstalován Windows Server 2022 ve verzi Datacenter ve 180 denní zkušební licenci, a to z důvodu jeho jednoduché obsluhy a podpory všech klíčových funkcí potřebných k testování. Na tento server byla poté nainstalována role Hyper-V, která sloužila pro provoz všech VM potřebných pro další testování.

Dalším krokem bylo sestavení testovacího prostředí tak, aby mezi serverem a testovanými klienty nevznikalo úzké hrdlo. Za tímto účelem bylo realizováno spojení mezi klienty a serverem pomocí gigabitového přepínače. Konektivitu směrem do internetu obstarával MikroTik hAP ac2 s IP rozsahem LAN 192.168.20.0/24. Jednotlivé IP VM byly přidělovány statickým záznamem v DHCP s vazbou na jejich MAC adresu pro lepší přehlednost.

Dále bylo přistoupeno k instalaci tří VM s OS Windows Server 2022 Datacenter. Dva z takto vytvořených strojů byly pojmenovány AD-1 a AD-2, poté jim byla zafixována IP adresa a následně na ně byly nainstalovány role Active Directory Domain Services a DNS. Za účelem testování byla vytvořena testovací doména zsfl.lan, do které byl následně přidán i virtualizační hostitel.

V doméně byly vytvořeny dva uživatelské účty, a to test1 a test2, které sloužily pro následné testování připojení z tenkých klientů.

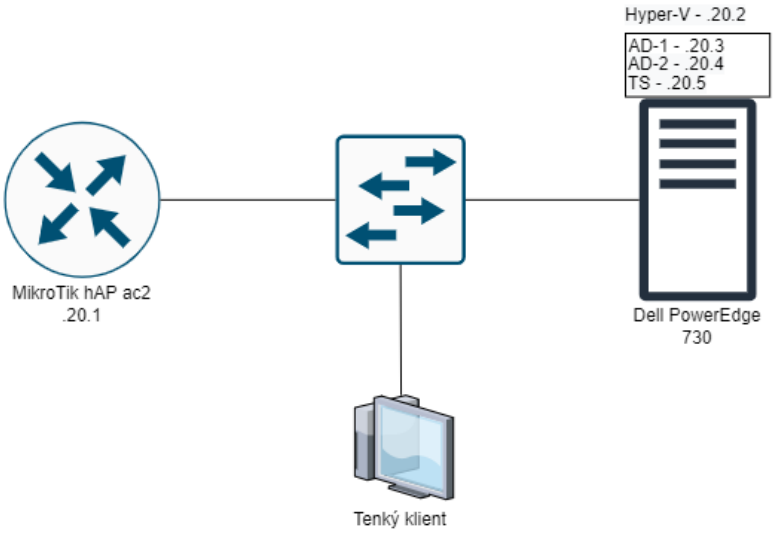
Parametry VM:

- **Procesor:** 8 virtuálních jader (vCPU)
- **Operační paměť:** 8 GB
- **Úložiště:** 256 GB

Třetí VM byl přejmenován na TS (Terminal server); bylo provedeno jeho přidání do domény a instalace rolí licencování vzdálené plochy a hostitel relací vzdálené plochy tak, aby tento virtuální stroj mohl sloužit pro testování jednotlivých tenkých klientů a připojení pomocí protokolu RDP. Na tomto stroji byly dále nainstalovány základní aplikace dle požadavků, aby mohly být otestovány.

Parametry VM:

- **Procesor:** 16 virtuálních jader (vCPU)
- **Operační paměť:** 32 GB
- **Úložiště:** 120 GB – na systémovém oddílu hostitele



Obrázek 8.1: Schéma testovacího prostředí, IP adresy jsou znázorněny posledními dvěma oktety [autor]

V neposlední řadě bylo důležité určit testovací metodiku pro řešení tenkých klientů tak, aby bylo možné vybrat na základě provedených testů ideální řešení z pohledu hardwaru a softwaru. Jelikož není možné pomocí žádných nástrojů efektivně sledovat výkon a uživatelský zážitek protokolu RDP, byl tento parametr sledován na základě uživatelské zkušenosti s používáním systému v rámci připojení. Do testování bylo zahrnuto procházení webu, základní práce s MS Office, test přehrávání videa a test požadovaných programů. U všech připojení, pokud to systém umožňoval, byly zvoleny stejné parametry protokolu RDP.

Dalším sledovaným parametrem byl vliv zátěže na spotřebu elektrické energie tenkého klienta, která byla měřena wattmetrem při probíhajících testech, s přesností měření na jedno desetinné místo. Na konci testu byly minimální, průměrné a maximální hodnoty spotřeby uloženy do tabulky, která sloužila k finálnímu zhodnocení spotřeby vybraného hardwaru. Před každým testem došlo k resetování naměřených hodnot uložených ve wattmeteru. Takové testování není úplně přesné, ale dokáže poskytnout základní přehled o spotřebě testovaného hardwaru napříč architekturami. Test spotřeby se skládal z několika kroků:

- vyčkání půl minuty na přihlašovací obrazovce tenkého klienta a následné přihlášení,
- otevření prohlížeče s několika kartami (Seznam, Wikipedia, Office365, YouTube) s vyčkáním na jejich načtení,
- dvě minuty přehrávání videa na YouTube v kvalitě 720p,
- otevření připraveného Word dokumentu,
- odhlášení a vyčkání na otevření přihlašovacího okna.

Posledním sledovaným parametrem byla zátěž na hardware serveru v průběhu testování při připojení jednoho klienta a s tím také spojené využití sítě. Pro sledování dat byl využit program HWiNFO, který zaznamenával průměrné vytížení CPU, RAM a sítě. Tento test byl proveden u vybrané kombinace hardwaru a OS tak, aby byla získána představa nad potřebnou finální konfigurací nových terminálových serverů.

8.1 Hardware

Pro testování bylo potřeba vybrat hardware, který pokryje architektury x86 a ARM tak, aby mohla být otestována široká škála OS, které lze pro provoz tenkých klientů použít. Důraz byl dále kladen na pořizovací cenu hardwaru – musel splňovat podmínku co nejlevnějšího řešení. Kvůli tlaku na finální cenu byla z testování vyřazena již hotová řešení kombinující HW a OS tenkého klienta, neboť jejich pořizovací cena by nebyla oproti řešení učebny pomocí klasických PC z pohledu školy výhodná. Dále bylo potřeba posoudit podporu ze strany výrobce pro takový hardware, aby mohla být zaručena dlouhodobá spolehlivost a udržitelnost počítačových učeben.

Jako vhodné řešení se jeví počítače typu mini PC, které nabízejí jak dostatečný výkon, tak adekvátní portovou výbavu k uspokojení všech požadavků na provoz v režimu tenkého klienta.

Pro testování OS architektury ARM bylo zvoleno Raspberry Pi 4, které patří mezi oblíbené víceúčelové minipočítače díky své nízké ceně, velikosti, flexibilitě použití, široké dostupnosti a podpoře široké škály OS. Své využití tyto počítače nalezly také v průmyslu, a to díky své jednoduchosti, nízké spotřebě a odolnosti.

U architektury x86 se nabízela široká škála možností, jelikož bylo možné otestovat OS tenkých klientů na jakémkoliv PC splňujícím minimální požadavky pro jeho běh. Nakonec byla domluvena zápůjčka repasovaných minipočítačů, aby bylo možné otestovat rozdíl ve výkonu a spotřebě mezi

těmito dvěma architekturami. Důvodem volby repasovaných počítačů byla také jejich nízká cena, která se pohybuje okolo pořizovací ceny Raspberry Pi 4 a může být tak zajímavou alternativou v konečném návrhu.

Seznam testovaného hardwaru:

- **Raspberry Pi 4** (CPU Broadcom BCM2711, RAM 4 GB, 32 GB SD karta),
- **Dell OptiPlex 3050** (CPU Intel Core i3 7100T, RAM 4 GB, 128 GB SSD),
- **Minix Neo Z83** (CPU Intel Atom x5-8300, RAM 4 GB, 64 GB eMMC).

8.2 Operační systém

Na základě provedené rešerše v oblasti tenkých klientů a možnostech jejich nasazení byla vybrána sada dostupných OS pro testování na zvoleném hardwaru. Vybraný hardware pokrývá obě zvolené architektury, aby mohlo být vybráno co nejefektivnější řešení dle požadavků školy, které byly popsány v kapitole 7 na straně 57.

U vybraných systémů byly pozorovány parametry jako jednoduchost instalace, nastavení, jejich správa, zabezpečení před neoprávněným zásahem uživatelů či samotná uživatelská přívětivost a snadné použití.

Pokud OS podporoval obě architektury, byla provedena instalace na všech testovaných zařízeních a následně porovnán uživatelský zážitek. Některé OS nebyly otestovány z důvodu nevhodnosti nebo chybějící demo licence pro testování. Raspberry Pi OS a Windows 10/11 byly z testování vynechány, jelikož se nejedná o OS určené pro provoz tenkých klientů, i když by je bylo možné nasadit. Pro testování byly zvoleny tyto operační systémy:

- **TLXOS**,
- **WTware**,
- **Openthinclient**,
- **Porteus Kiosk**,
- **xtc**.

TLXOS

Prvním zvoleným OS pro testování byl TLXOS, který lze nainstalovat na širokou škálu hardwaru, díky podpoře architektur ARM a x86, což z něj dělalo vhodného kandidáta i na porovnání výkonu mezi těmito architekturami. V rámci testování byla provedena instalace na testovací hardware a následně vyzkoušena funkčnost jak samotného OS a jeho funkcí, tak vzdálené správy tenkých klientů, kterou nabízí pomocí programu ThinLinX Management Software (TMS), který se instaluje na server.

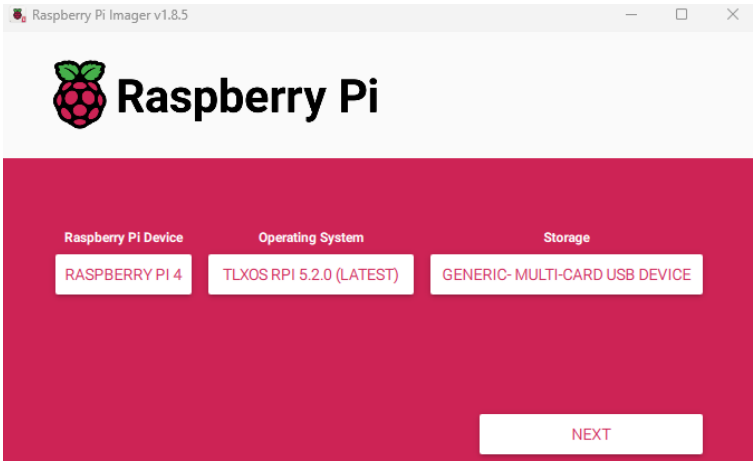
Licencování se provádí na základě počtu nakoupených licencí vázaných na registrovaný účet na stránkách tohoto projektu. Zakoupené licence jsou doživotní, včetně nároku na budoucí aktualizace. Registrace zařízení se provádí v nastavení, kde se uživatel přihlásí na příslušný účet a klikne na tlačítko „install“. Následně je navázáno spojení s licenčním serverem a zařízení je přiřazena příslušná licence. Každá takto vydaná licence je vázána na MAC adresu zařízení a je nepřenositelná. Výjimkou je havárie, kdy může být licence uvolněna pro jiné zařízení kontaktováním podpory. Pro testování je nabízena 30denní zkušební licence, která po vypršení omezí funkčnost tenkého klienta na 1 minutu. Po uplynutí 1 minuty dojde k restartu všech služeb, což znemožňuje jeho používání, jelikož se tento cyklus neustále opakuje. [73]

TLXOS podporuje širokou škálu protokolů pro vzdálené připojení, což ho činní velice univerzálním. Podporovanými protokoly jsou:

- RDP,
- Citrix ICA,
- VMWare Blast Extreme,
- VNC,
- SPICE,
- NX (NoMachine),
- RAS/2X (Parallels).

Instalace Raspberry Pi

Instalace na Raspberry Pi 4 se provádí skrze Raspberry Pi Imager, kde lze nalézt TLXOS při výběru OS v záložce Freemium and paid-for OS. Následně je zvolena příslušná SD karta a po kliknutí na tlačítko „next“ je provedena automatická instalace. Dále je možné použít průvodce SD Card Installer, který lze stáhnout ze stránek projektu. Po rozbalení archivu příslušné verze OS nabídne instalaci na SD kartu skrze program Win32 Disk Imager.



Obrázek 8.2: Instalace TLXOS pomocí Raspberry Pi Imager [autor]

Instalace x86

Instalace na libovolné PC se provádí pomocí staženého ISO souboru, který je potřeba rozbalit na instalační médium (například pomocí programu Rufus), ze kterého je následně zavedena instalace. Pokud instalační program nenajde více než jeden disk, provede jeho naformátování dle potřeby a následně nainstaluje OS. Pokud by bylo nalezeno disků více, je potřeba ručně vybrat cílový disk pro instalaci OS.

Nastavení

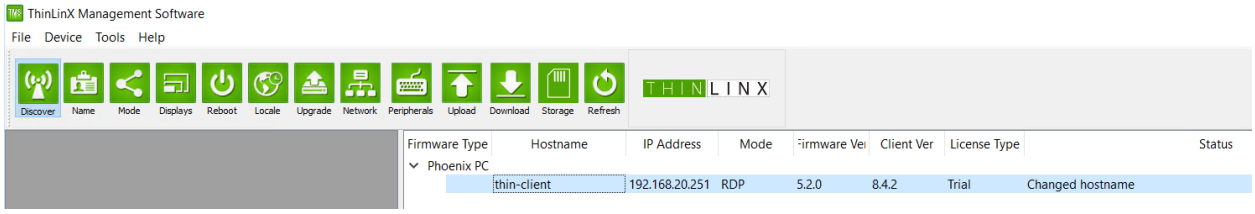
Při prvním spuštění OS se otevře nastavení, které je rozděleno do několika níže popsaných karet.

- **Device** obsahuje základní přehled o zařízení, možnost nastavení jeho názvu a licencování.
- **Displays** slouží ke konfiguraci připojených monitorů.
- **Servers** slouží ke specifikování IP adresy serveru, na kterém běží TMS pro centrální správu tenkých klientů.
- **Network** slouží ke konfiguraci sítě tenkého klienta.
- **Application** nabízí konfiguraci režimu, ve kterém bude tenký klient fungovat. Na výběr je široká škála protokolů a jejich parametrů pro vzdálené připojení k serveru, případně povolení režimu kiosk s minimálním uživatelským rozhraním, nebo možnost provozovat ho jako lokální desktop.
- **Peripherals** slouží k nastavení připojených periferií.
- **Misc** obsahuje funkce jako povolení lokálního VNC serveru či omezení přístupu do konfigurace tenkého klienta pomocí hesla.

V případě potřeby je možné nastavení vyvolat pomocí klávesové zkratky Ctrl + Alt + C.

Dále byla vyzkoušena možnost centrální správy pomocí TMS, který byl nainstalován na testovací terminálový server. Pro jeho správné fungování bylo potřeba povolit TCP port 8085 ve firewallu Windows Serveru. TMS vyhledává nainstalované tenké klienty každých 5 sekund pomocí zaslaného broadcastu na připojených sítích serveru, z čehož vyplývá, že na straně klienta nemusí být provedena žádná změna konfigurace, aby se objevil mezi spravovanými. Bezpečnějším způsobem je přidání IP adresy serveru přímo na straně klienta.

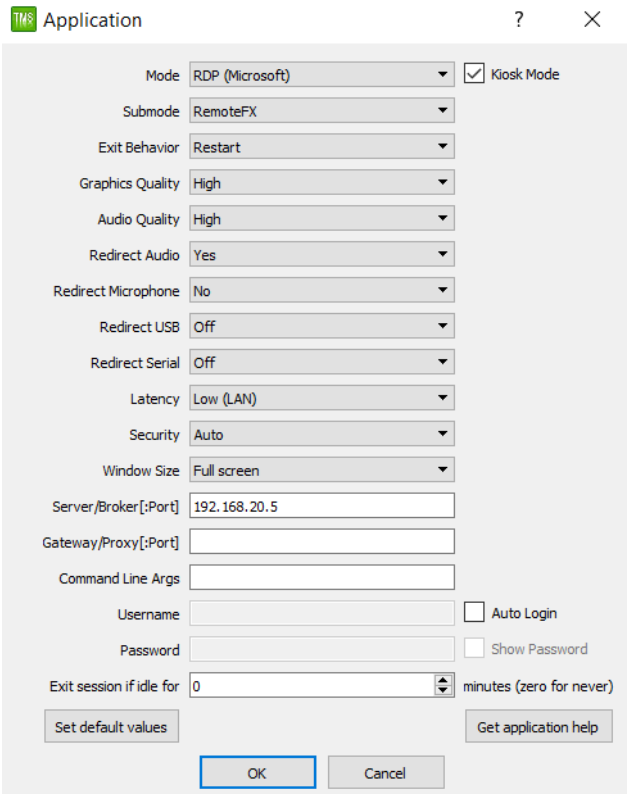
TMS umožňuje změnu všech parametrů, které lze nalézt v lokálním nastavení klienta. Dále je z něj možné provádět instalaci aktualizací jednotlivých komponent TLXOS či provést hromadný update všech připojených tenkých klientů na nejnovější verzi.



Obrázek 8.3: Centrální správa tenkých klientů TMS [autor]

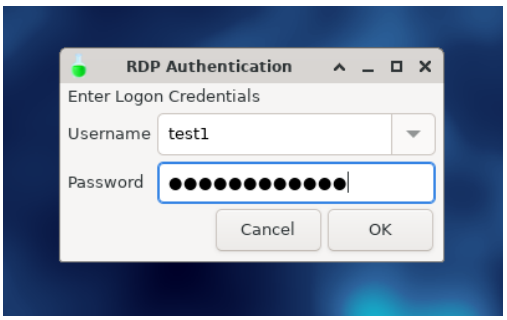
Testování

Po základním nastavení bylo přistoupeno k testování OS na základě již představených testů v kapitole 8 na straně 61. Před zahájením testování bylo nutné nastavit parametry protokolu RDP a režim kiosk, aby se testovací prostředí blížilo co nejvíce reálnému nasazení v počítačových učebnách. Po každém odpojení z relace bude zahájeno nové připojení s výzvou pro uživatelské jméno a heslo.



Obrázek 8.4: Použité nastavení pro testování RDP [autor]

Po provedeném nastavení protokolu RDP byla ověřena funkčnost všech požadovaných parametrů připojením k terminálovému serveru. Z provedeného testování vyplynulo, že TLXOS nabízí díky optimalizaci na hardware Raspberry Pi 4 vysoký uživatelský zážitek, a to jak na základě plynulosti připojení, tak jednoduchosti použití. V porovnání mezi testovaným HW byl zaznamenán nejplynulejší zážitek na počítači Dell OptiPlex 3050, následovalo Raspberry Pi 4 a na posledním místě skončil Minix Neo Z83.



Obrázek 8.5: Přihlašovací obrazovka připojení v režimu kiosk [autor]

WTware

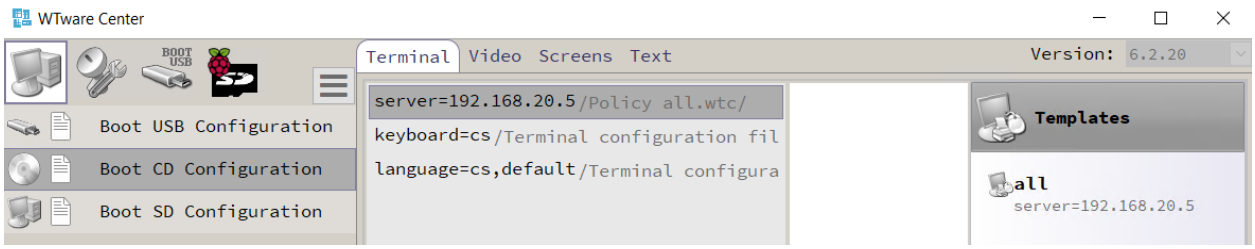
Druhým OS zvoleným pro testování byl WTware. Stejně jako TLXOS i WTware podporuje obě testované architektury. Testování tedy proběhlo v obou případech velmi podobně. V rámci testování byla zkoumána jednotlivá nastavení a centrální správa tenkých klientů.

Licencování WTware je řešeno nákupem trvalých licencí, přičemž jsou aktualizace garantovány v rámci zakoupené licence minimálně po dobu jednoho roku od zakoupení. Licence je vázána na MAC adresu zařízení a v případě jeho poruchy je každý případ řešen individuálně po kontaktování podpory. Pro testovací účely neexistují žádná omezení, kromě banneru na pravé straně obrazovky, který upozorňuje, že je instalace určena pouze k testovacím účelům. [74]

Instalace a vzdálená správa klientů je prováděna pomocí programu WTware Center, který nainstaluje následující služby: DHCP, TFTP, HTTP, HTTPS. Při instalaci je zvoleno administrátorské heslo pro správu. V případě použití zabudovaného DHCP serveru je možné určit rozsah vydávaných IP adres a definovat IP adresu terminálového serveru.

Po úspěšné instalaci je potřeba spustit WTware Center a nastavit případné bootování skrze PXE, vytvořit ISO soubor nebo image pro Raspberry Pi. Dále je nutné specifikovat požadované parametry připojení. Pro vzdálené připojení k serveru jsou podporovány tyto protokoly:

- RDP,
- VNC.



Obrázek 8.6: Rozhraní WTware Center [autor]

Instalace Raspberry Pi a x86

Při vytváření instalačních souborů je nutné určit několik klíčových parametrů: zaprvé rozhodnout, jakým způsobem bude klient získávat IP adresu, zadruhé zvolit, kde bude ukládán konfigurační soubor klienta (zda na serveru, nebo lokálně). Dále je třeba nastavit administrátorské heslo pro vzdálenou správu klienta skrze HTTPS a určit, zda bude umožněn přístup k této správě i lokálně při startu tenkého klienta.

Po dokončení tohoto průvodce je instalační soubor vytvořen a může být následně nainstalován na příslušné PC. V případě Raspberry Pi je obraz při instalaci rovnou rozbalen na SD kartu. Instalace je dále bezobslužná a jsou použity již předem připravené parametry.

Testování

Po vyzkoušení všech možností instalace se ukázalo, že optimálnější je bootování ze sítě pomocí PXE. V takovém případě stačí nastavit příslušnou konfiguraci ve WTware Center a na tenkém klientovi povolit bootování ze sítě. Následně je zaveden OS se všemi specifikovanými parametry. Nevýhodou mohou být vyšší nároky na propustnost sítě při zavádění tenkého klienta.

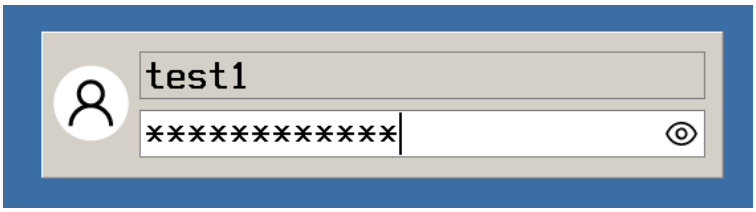
Klasická instalace nabízí menší flexibilitu. V případě aktualizací je nutné se připojit pomocí webového prohlížeče na IP adresu každého klienta zvlášť, nahrát mu novou verzi OS v podobě binárního souboru a následně ho restartovat.

Obrázek 8.7: Webové rozhraní pro správu tenkého klienta [autor]

Vzhledem k tomu, že WTware primárně nabízí pro vzdálený přístup protokol RDP, spočívala konfigurace klienta pouze v úpravě parametrů RDP tak, aby odpovídaly dříve testované konfiguraci. Po úspěšném spuštění OS je uživateli nabídnuta jednoduchá tabulka se zadáním uživatelského jména a hesla a následně je připojen na příslušný server. Z uživatelského hlediska se výkonově i použitím jeví stejně jako již testovaný TLXOS. Z hlediska správy je instalace a konfigurace

WTware podstatně složitější než u TLXOS. Při použití WTware je nezbytné nainstalovat WTware Center ještě před instalací tenkých klientů. Naopak u TLXOS je možné nasazení provést souběžně a následně upravit parametry klientů vzdáleně.

Při testování vybraného hardwaru byly zaznamenány rozdíly v rychlosti. Nejnižší rychlost byla pozorována u zařízení Minix Neo Z83, zatímco u zbývajících dvou zařízení byly rychlosti podobné.



Obrázek 8.8: Přihlašovací obrazovka připojení [autor]

Openthinclient

Třetím vybraným OS byl Openthinclient, který podporuje pouze architekturu x86. Již v základní verzi do maxima 24 klientů nabízí možnost centrální správy klientů bez jakýchkoliv omezení.

Openthinclient, na rozdíl od ostatních řešení, využívá PXE bootování ze sítě jako jedinou možnost zavedení OS tenkého klienta. Funkce je tím pádem plně závislá na centrálním serveru. Výhodou tohoto řešení je, že v případě pádu OS, chyby nebo změny nastavení je nutný pouze restart tenkého klienta. Nevýhodou tohoto řešení je, že v případě nedostupnosti serveru dojde k nefunkčnosti všech tenkých klientů.

Licencování je řešeno verzí zdarma do maximálního počtu 24 tenkých klientů, pro stažení OS je potřeba provést registraci na webových stránkách projektu. V případě většího počtu tenkých klientů je potřeba zakoupit příslušné předplatné [75]. Dostupnými protokoly pro vzdálené připojení jsou:

- RDP,
- VMware Blast Extreme,
- Citrix ICA.

Instalace

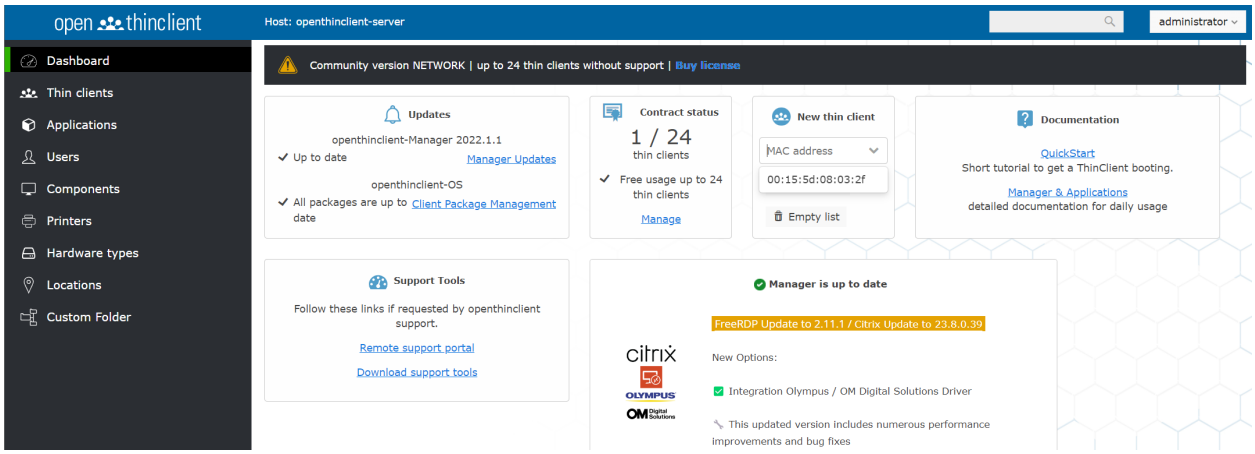
Před nasazením je potřeba provést instalaci Openthinclient manageru. K dispozici jsou instalační soubory pro platformy Windows a Linux. Rychlé nasazení lze provést pomocí již připravených virtuální strojů pro VirtualBox, VMware a Hyper-V. K testování byl stažen připravený virtuální stroj pro Hyper-V, kterému dle přiloženého manuálu byly přiděleny 2 CPU jádra a 4 GB RAM. Síť je potřeba nastavit tak, aby byl server na stejném L2 segmentu společně s tenkými klienty.

Po spuštění VM je potřeba přihlásit se zadáním hesla „0pen%TC“. Poté je nabídnuta změna hesla, které musí mít minimálně 8 znaků. Dále byla nastavena statická IP adresa na 192.168.20.6, aby

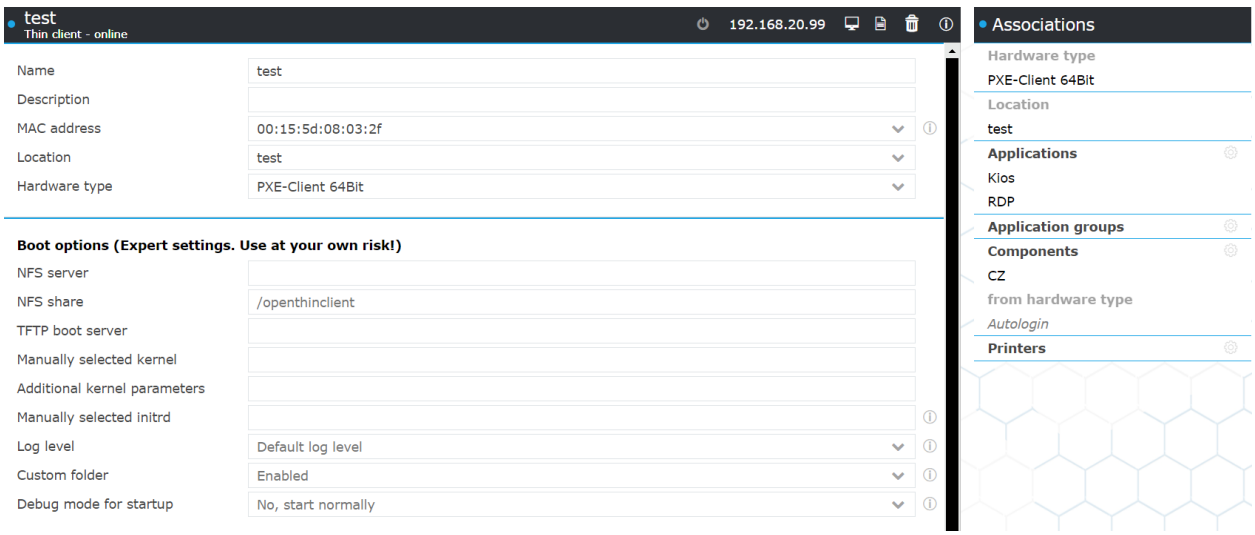
mohlo být přistupováno ke správě tenkých klientů, která je řešena skrze webový prohlížeč. Připojení k serveru probíhá skrze protokol HTTP zadáním jeho IP adresy společně s portem 8080. Po připojení je potřeba se přihlásit zadáním uživatelského jména „administrator“ a heslem „0pen%TC“.

Po přihlášení do správy serveru byla provedena aktualizace na nejnovější dostupnou verzi a následně bylo přistoupeno k samotné konfiguraci tenkých klientů. Pro požadované fungování je nutné v záložce Applications upravit požadovaný protokol pro připojení a nastavit kiosk mód v nastavení chování desktopového prostředí. Dále je potřeba nastavit jazyk tenkého klienta v záložce Components.

Poté je možné přistoupit k připojení tenkého klienta, na kterém je nutné nastavit bootování ze sítě. Po provedení testovacího spuštění se zobrazí MAC adresa tenkého klienta v rozhraní serveru, kterou je potřeba autorizovat a přiřadit jí již připravené konfigurační parametry. Po dalším restartu tenkého klienta je zaveden OS skrze síť a je možné ho začít plně používat.



Obrázek 8.9: Webové rozhraní Openthinclient [autor]



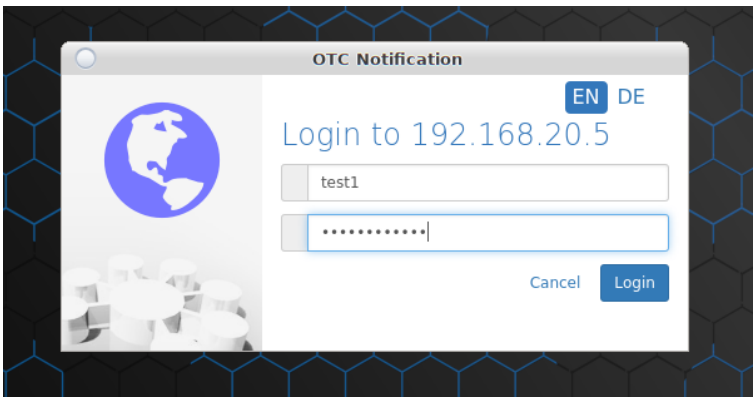
Obrázek 8.10: Konfigurace tenkého klienta [autor]

Testování

Po úspěšném náběhu OS byla provedena standardní sada testů, aby byla ověřena funkčnost systému a jeho vhodnost pro případné budoucí použití. Při prováděných testech nebyl rozdíl ve výkonu OS na testovaném HW zaznamenán.

Z pohledu administrátora se jedná o jedno z nejjednodušších řešení, díky již připraveným virtuálním strojům a potřebě pouze minimální konfigurace jak na straně serveru, tak na straně tenkých klientů. Další výhodou jsou licenční podmínky do maximálního počtu 24 tenkých klientů, což z něj dělá vhodného kandidáta pro menší PC učebny či podniky.

Z pohledu uživatele nabízí Openthinclient snadné používání a přívětivé uživatelské rozhraní. Příkladem je obrázek 8.11, který ukazuje jednoduché přihlašovací okno pro přihlášení do systému.



Obrázek 8.11: Přihlašovací obrazovka tenkého klienta [autor]

Porteus Kiosk

Čtvrtým zvoleným OS byl Porteus Kiosk. Ten podporuje pouze architekturu x86 a je nabízen společně s Porteus Kiosk Server, který poskytuje centrální správu tenkých klientů. Testovány byly pouze dostupné funkce zdarma.

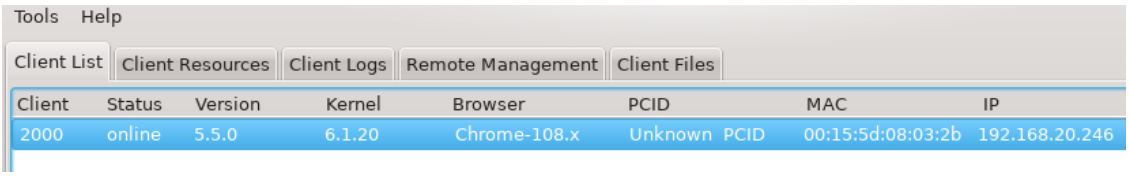
Licencování je řešeno ročním předplatným. Základní verze, která je dostupná zdarma, obsahuje pouze omezenou sadu funkcí [76]. Přitom neobsahuje automatické aktualizace, pro jejich instalaci je třeba provést kompletní novou instalaci OS. Porteus Kiosk Server je licencován zvlášť a je také nabízen s ročním předplatným. Dostupnými protokoly pro vzdálené připojení jsou:

- RDP,
- Citrix ICA,
- VNC.

Instalace

Instalace probíhá pomocí stažených ISO souborů z webových stránek projektu. Před instalací tenkého klienta byl nejprve nainstalován Porteus Kios Server v základní verzi. Během této instalace

bylo nutné zadat statickou IP adresu, aby byla zajištěna správná funkčnost systému. Poté došlo k ověření nabízených možností, kde bylo zjištěno, že se v základní verzi nachází pouze monitoring připojených klientů.



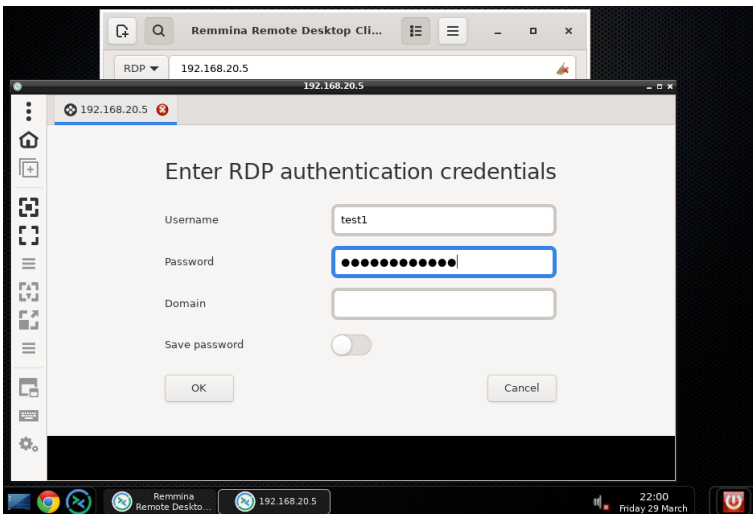
Obrázek 8.12: Rozhraní Porteus Kiosk Serveru [autor]

Po spuštění instalace Porteus Kiosk Thin Client je nabídnut jednoduchý průvodce konfigurací tenkého klienta. V prvním kroku je potřeba zvolit typ síťového připojení, ve druhém kroku umístění, z něhož se mají načítat konfigurační soubory. Mezi nabízenými možnostmi jsou: lokální úložiště, přenosné médium a stažení konfiguračních souborů ze síťového úložiště. Pro zkušební instalaci bylo zvoleno lokální úložiště s připojením k Porteus Kiosk Serveru. Dále je nabídnuta konfigurace prostředí tenkého klienta, kde mezi nabízené možnosti patří: network settings, browser settings, system settings, power saving options, additional components, experimental features a debugging options. Všechna nastavení je nutné důkladně zvážit již při instalaci, protože je následně nelze změnit.

Testování

Z testovaných řešení nabízí Porteus Kiosk nejhorší způsob instalace a z pohledu administrátora je takové řešení příliš zdlouhavé. Nemožnost měnit konfigurační soubor po instalaci klienta, a tím pádem nutnost následné reinstalace, se nejeví také jako nejvhodnější řešení pro dlouhodobý provoz. Po prvním spuštění bylo zjištěno, že je použito klasické desktopové prostředí společně s programem Remmina, který zajišťuje vzdálené připojení k serveru a automaticky se nespouští po startu tenkého klienta. Po instalaci je třeba konfiguraci připojení RDP zadat ručně, přičemž tato konfigurace může být následně kýmkoliv upravena. Takové prostředí není příliš vhodné pro použití v PC učebnách.

Uživatelský zážitek je kvůli výše zmíněným bodům u tohoto řešení nejhorší ze všech testovaných OS, jelikož je nutné nejdříve zapnout program Remmina, následně vybrat správné připojení, zadat přihlašovací údaje a až poté dojde k připojení k serveru. Po provedeném testování lze říci, že z pohledu rychlosti není také úplně ideálním řešením ve srovnání s ostatními OS, přičemž nejlépe běžel na Dell OptiPlex 3050.



Obrázek 8.13: Přihlašovací obrazovka RDP [autor]

xtc

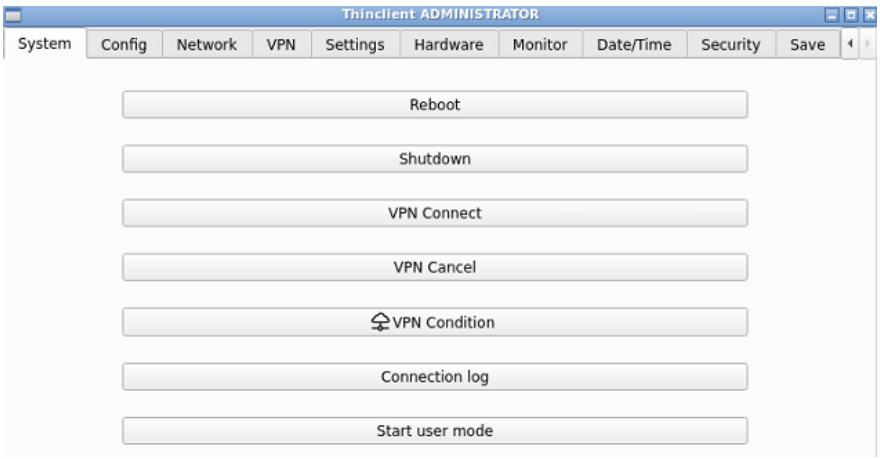
Posledním testovaným systémem pro tenké klienty byl OS xtc, který je dostupný zdarma bez jakýchkoliv omezení funkčnosti či počtu použitých zařízení. Centrální správa tenkých klientů není u tohoto řešení dostupná. Mezi podporovaný hardware v aktuální verzi patří pouze Raspberry Pi 3 a 4 [77]. Podporovanými protokoly pro vzdálené připojení jsou:

- RDP,
- VNC.

Instalace

Instalace xtc je velice jednoduchá, jelikož stačí pouze stáhnout image aktuální verze systému z webových stránek projektu a následně ho například pomocí programu Rufus rozbalit na SD kartu.

Po prvním zapnutí tenkého klienta je spuštěna jeho konfigurace, přičemž je možné nastavit širokou nabídku možností. Pro testovací účely bylo provedeno nastavení protokolu RDP do režimu kiosk, při kterém se spustí nastavené připojení s výzvou pro zadání přihlašovacích údajů po startu tenkého klienta. Dále bylo nastaveno časové pásmo, jazyk klávesnice a zákaz přístupu do této konfigurace bez zadání administrátorského hesla, aby nemohla být měněna bez oprávnění. Po dokončení nastavení byla konfigurace uložena a byl spuštěn user mode.



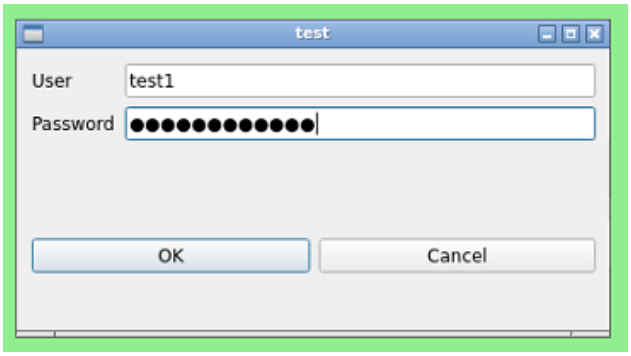
Obrázek 8.14: Konfigurace xtc [autor]

Testování

Testování xtc proběhlo dle již zavedeného postupu a bylo zjištěno, že se jeví jako velice schopný konkurent již otestovaných OS.

Z administrátorského pohledu nabízí velice výhodnou nabídku díky dostupnosti zdarma, jednoduchému nasazení a konfiguraci. Při nasazení většího počtu klientů je nevýhodou chybějící centrální správa, která by jejich provoz značně ulehčila.

Uživateli je po spuštění nabídnuta jednoduchá tabulka pro přihlášení k uloženému terminálovému serveru. V případě odhlášení ze serveru je otevřeno rozhraní thinclient, kde jsou dostupná připravená připojení, možnost tenkého klienta restartovat nebo vypnout, případně otevřít jeho konfiguraci. Z uživatelského pohledu nebyly zaznamenány žádné problémy, funkčně i rychlostí byl uživatelský zážitek srovnatelný s TLXOS, WTware i Openthinclient.



Obrázek 8.15: Přihlašovací obrazovka [autor]

8.3 Porovnání vybraných řešení

Po provedeném testování bylo přistoupeno k porovnání jednotlivých řešení vytvořením jednoduché tabulky 8.1, která ukazuje pro každý testovaný OS tenkého klienta podporovaný hardware, protokoly pro vzdálené připojení k serveru a přítomnost centrální správy.

OS	Hardware	Protokoly	Centrální správa
TLXOS	x86, všechny varianty Raspberry Pi	RDP, VMware Blast Extreme, Citrix ICA, VNC, SPICE, NX (NoMachine), RAS/2X (Parallels)	Ano
WTware	x86, Raspberry Pi 2 – 4	RDP, VNC	Ano
Openthinclient	x86	RDP, VMware Blast Extreme, Citrix ICA	Ano
Porteus Kiosk	x86	RDP, Citrix ICA, VNC	Ano
xtc	Raspberry Pi 3 a 4	RDP, VNC	Ne

Tabulka 8.1: Porovnání jednotlivých OS tenkých klientů [73, 74, 75, 76, 77]

Na základě tabulky 8.1 je vidět, že všechny OS podporují protokol RDP, který je při nasazování tenkých klientů nejvíce používán. Pokud by bylo potřeba použít jiný protokol, výběr by se již značně zmenšil. Dále lze vidět, že z rodiny procesorů ARM, je u všech OS podporováno pouze Raspberry Pi, tudíž nelze použít žádné jeho klony. Nejvíce univerzálním OS je TLXOS, který nabízí nejširší podporu hardwaru, jelikož jako jediný podporuje Raspberry Pi 5. Nabízí také nejširší sadu protokolů pro připojení k serveru, což ho činí nejvíce univerzálním. Tato skutečnost se projevila i při testování jeho jednoduchou obsluhou a správou.

Dále byla vytvořena tabulka 8.2 pro možnost cenového srovnání jednotlivých licencí OS. Na základě tabulky lze vybrat nejvýhodnější řešení. Pro konverzi amerického dolaru (USD) na českou korunu (CZK) byl stanoven směnný kurz 23,4 CZK/USD. Ceny jsou zaokrouhleny na celé koruny a v případě množstevní slevy byl brán v potaz celkový počet potřebných licencí dle počtu žákovských zařízení, kterých je 60.

OS	Cena
TLXOS	117 - 351 Kč/zařízení dle architektury
WTware	468 Kč/zařízení
Openthinclient	983 Kč/zařízení/rok
Porteus Kiosk	875 Kč/zařízení/rok
xtc	Zdarma

Tabulka 8.2: Porovnání cen licencí jednotlivých OS tenkých klientů [73, 74, 75, 76, 77]

Posledním srovnávaným parametrem byla spotřeba elektrické energie testovaného hardwaru. Cílem bylo vybrat nejefektivnější řešení z hlediska spotřeby energie, přičemž jako OS byl použit TLXOS. Za tímto účelem byla vytvořena přehledná tabulka 8.3 ukazující minimální spotřebu v nečinnosti, průměrnou spotřebu v rámci testování a maximální odběr celého zařízení v průběhu testování. Spotřeba v nečinnosti (idle) je důležitým parametrem, pokud tencí klienti budou zapnutí v rámci PC učebny pořád. Na základě měření se jako nejefektivnější zařízení ukázalo Raspberry Pi 4 s průměrnou spotřebou 4,3 W. Tato hodnota je o dost nižší než typická spotřeba desktopů, mezi které lze zařadit testovaný Dell OptiPlex 3050, u kterého se při měření pohybovala okolo 16,2 W.

Zařízení	Idle (minimální) spotřeba	Průměrná spotřeba	Maximální spotřeba
Raspberry Pi 4	3,6 W	4,3 W	5,4 W
Dell OptiPlex 3050	9,4 W	16,2 W	23,2 W
Minix Neo Z83	3,7 W	4,8 W	5,5 W

Tabulka 8.3: Porovnání spotřeby testovaných zařízení [autor]

Co se týká hardwarových nároků na straně serveru, ty jsou velice nízké. Průměrné zatížení CPU testovacího virtuálního stroje se pohybovalo okolo 3,6 %. RAM využívaná jedním připojeným klientem byla mezi 300 MB až 1 GB a využití sítě dosahovalo rychlosti okolo 10 Mbit/s. Na základě těchto výsledků lze říci, že pro provoz 30 klientů by měl mít terminálový server minimálně CPU o konfiguraci 16 jader a 32 vláken, RAM alespoň 64 GB, aby byla zaručena rezerva, a 1 Gbit síťovou kartu společně s dostatečným úložištěm.

9 Návrh řešení

Po provedeném testování bylo přistoupeno k vytvoření návrhu řešení počítačových učeben, pro které bylo nutné navrhnout potřebná zařízení a jejich zapojení. Všechny ceny v této kapitole budou uvedeny s DPH. Před začátkem realizace obdržela škola darem čtyři starší servery Dell PowerEdge R730, z nichž dva disponují 32 jádry a zbylé dva 16 jádry. Na základě jejich konfigurace bylo domluveno, že na dvou 16jádrových serverech poběží služby nezbytné pro chod školy a kromě toho budou přikoupeny dva výkonnější terminálové servery pro provoz PC učeben.

Komponenta	**Počet**	**Specifikace**
CPU	2	Intel Xeon E5-2667 v4 3,2 GHz, 8 jader/16 vláken, TDP 135 W
RAM	24	64 DDR 4 2133 MHz ECC
Síť. karta	1	Intel 10G 2P X540-t Adapter
SSD	2	200 GB SSD SAS
HDD	6	600 GB HDD SAS
Zdroj	2	Hot-plug 750W
OOB	1	iDRAC 8

Tabulka 9.1: Parametry 16jádrového serveru Dell PowerEdge R730 [autor]

9.1 Specifikace terminálových serverů

Pro provoz terminálových učeben bylo rozhodnuto o specifikování serverů Dell tak, aby zapadaly svou správou k darovaným serverům. Všechny parametry byly specifikovány na základě proběhlého testování, přičemž byly brány v potaz požadavky na výkon CPU, kapacitu RAM a velikost úložiště. Hardwarová specifikace terminálových serverů byla zvolena na základě následujících parametrů:

- CPU 16 jader a 32 vláken, kvůli licencování Windows Serveru,
- 128 GB RAM,
- dvakrát 1 TB SSD, třikrát 2 TB HDD,
- RJ-45 10 Gbit síťová karta,
- iDRAC (Out-of-band management).

Na základě tohoto požadavku byla vytvořena konfigurace, která je pro oba terminálové servery identická. Jako vhodný model byl pro terminálové servery doporučen Dell PowerEdge R550 s cenou 141 000 Kč. Vzhledem k dodaným parametrům byla vytvořena tabulka tak, aby terminálový server mohl být porovnán s infrastrukturním serverem Dell PowerEdge R730.

Komponenta	**Počet**	**Specifikace**
CPU	1	Intel Xeon Silver 4314 2.4 GHz, 16 jader/32 vláken, TDP 135 W
RAM	4	32 GB DDR 4 3200 MHz ECC
Síť. karta	1	Broadcom 57416 Dual Port 10GbE BASE-T
SSD	2	960 GB SSD SATA
HDD	3	2 TB HDD SATA
Zdroj	2	Hot-plug 800W
OOB	1	iDRAC 9

Tabulka 9.2: Parametry serveru Dell PowerEdge R550 [autor]

9.2 Specifikace serverového softwaru

Pro darované a nově navrhované servery bylo potřeba vybrat vhodné virtualizační řešení. Jako logická volba se jevilo použití Hyper-V, jelikož je součástí licence Windows Serveru, který škola požaduje a s jehož použitím má správce sítě zkušenosti. Vzhledem k tomu, že mělo být celé řešení postavené tak, aby nabízelo dostatečnou rezervu pro další růst, byla za tímto účelem zvolena licence Windows Server 2022 Datacenter EDU, aby pokryla všechny fyzická jádra použitých serverů. Do budoucna se plánuje značné navýšení virtuálních instancí Windows Serveru, což zvyšuje výslednou cenu navrhovaného řešení. Původní nabídka představená v kapitole 7 na straně 57, kterou škola dostala, tuto variantu vůbec nezahrnovala, jelikož se zaměřovala čistě na terminálové servery. Proto by bylo potřeba tyto dodatečné náklady připočítat k nabízeným cenám.

Dále bylo nutné vybrat správné licencování CAL, aby bylo co nejvýhodnější pro řešení obou učeben. Toto rozhodnutí bylo zásadní, protože se zatím nepočítalo s využitím celé infrastruktury v rámci školy, ale pouze v PC učebnách. Díky předem známému počtu zařízení v PC učebnách bylo zvoleno licencování Device CAL, do budoucna se počítá se zakoupením User CAL pro celou školu.

Nakonec bylo nutné vybrat správné licencování pro terminálové servery. Finální volbou byl nákup licencí RDS Device CAL, a to na základě počtu zařízení, jelikož se na tenkých klientech budou střídat jednotliví žáci s vlastními doménovými účty.

Název	Počet	Cena za ks	Cena celkem
Windows Server 2022 Datacenter 2 core EDU	32	5 421 Kč	173 472 Kč
Windows server 2022 CAL Device licence EDU	62	236 Kč	14 632 Kč
Windows server 2022 RDS CAL Device licence EDU	62	698 Kč	43 276 Kč
			231 380 Kč

Tabulka 9.3: Počty serverových licencí a jejich předpokládaná cena [autor]

9.3 Specifikace tenkých klientů

Na základě požadavků školy se jeví jako nejlepší varianta kombinace Raspberry Pi 4 a TLXOS, a to jak podporou požadovaného protokolu, tak centrální správou a nízkou cenou za doživotní licenci. Pokud by nemusel být naplněn požadavek na centrální správu, pak by byla vhodná kombinace Raspberry Pi 4 a xtc. Ke zvolené kombinaci HW a OS bylo nutné vybrat ostatní potřebný hardware, který je pro jejich provoz potřebný, a také náležité periferie.

U Raspberry Pi 4 byla zvolena varianta s 2 GB RAM společně s 16GB micro SD kartou, což by mělo zaručovat dostatek prostoru i pro budoucí aktualizace OS. Následně byla vybrána vhodná krabička, malý hliníkový chladič CPU a zdroj se specifikací 5,25 V a 4 A, který by měl nabízet více než dostatečnou rezervu i po připojení periferií. Vzhledem k faktu, že Raspberry Pi 4 neobsahuje žádné zapínací tlačítko, byl ke zdroji vybrán vypínač na kabelu s konektory USB-C, aby bylo možné klienty libovolně zapínat a vypínat bez nutnosti odpojovat z nich napájecí kabel. Celková cena Raspberry Pi 4 s licencemi a potřebným příslušenstvím se rovná 2 386 Kč, což je výrazně nižší cena než u již nabízených hotových řešení představených v kapitole 3.3 na straně 36.

Název	Počet	Cena za ks	Cena celkem
Raspberry Pi 4 2 GB	60	1 195 Kč	71 700 Kč
Hliníkový chladič 27.8 x 27.8 x 11.2mm	60	117 Kč	7 020 Kč
Kingston Micro SDHC Canvas Select Plus 16GB UHS-I	60	173 Kč	10 380 Kč
Zonepi krabička pro Raspberry Pi 4B, galaxy	60	179 Kč	10 740 Kč
Zdroj Zonepi USB-C 5,25 V 4 A	60	299 Kč	17 940 Kč
USB-C|USB-C kabel s vypínačem	60	189 Kč	11 340 Kč
Licence TLXOS RPi	60	234 Kč	14 040Kč
		2 386 Kč	**143 160 Kč**

Tabulka 9.4: Specifikace tenkých klientů a jejich předpokládaná cena [autor]

Pro monitor byla zvolena úhlopříčka 23,8 ″ s rozlišením Full HD, aby byl zaručen dostatečný prostor pro práci v požadovaných programech. Vzhledem ke konektorové výbavě Raspberry Pi 4 bylo zvoleno připojení pomocí kabelu HDMI micro > HDMI o délce 1 m. Klávesnice a myš byly vybrány ve formě levného setu, jelikož dochází ze strany žáků k jejich častému poškozování, a jsou tedy často měněny.

Název	Počet	Cena za ks	Cena celkem
23.8” Philips 243V7QDSB	60	2 390 Kč	143 400 Kč
micro HDMI kabel 1 m	60	129 Kč	7 740 Kč
CONNECT IT CKM-4000-CS	60	299 Kč	17 940 Kč
		2 818 Kč	**169 080 Kč**

Tabulka 9.5: Periferie a jejich předpokládaná cena [autor]

9.4 Návrh síťové infrastruktury

Vzhledem k zastaralosti síťové infrastruktury došlo k návrhu nových síťových prvků pro propojení učeben tak, aby každý z klientů měl dostupnou rychlost alespoň 1 Gbit/s a mezi servery a síťovými prvky byla dostupná rychlost 10 Gbit/s, aby byla síť připravená na budoucí rozvoj. Pro propojení síťových prvků se jevilo jako vhodné použit multimode optická vlákna, a to díky jejich nízké ceně a podpoře požadované rychlosti. Instalace optických vláken byla navržena do již stávajících lišt, aby nemusely být instalovány nové. Za tímto účelem bylo potřeba vybrat dva 24portové přepínače, které budou umístěné v učebnách, jeden 48portový do centrálního racku a poslední 24portový, který bude umístěn do racku k serverům. Vzhledem k plánům na budoucí výměnu školní Wi-Fi sítě za prvky značky Ubiquiti Unifi byl do návrhu zařazen i Unifi Controller (centrální ovladač sítě) s napájením pomocí PoE adaptéru.

Název	Počet	Cena za ks	Cena celkem
Ubiquiti USW-Pro-24	2	10 412 Kč	20 824 Kč
Ubiquiti USW-EnterpriseXG-24	1	32 464 Kč	32 464 Kč
Ubiquiti USW-Pro-48	1	15 633 Kč	15 633 Kč
Ubiquiti UCK-G2-PLUS	1	5 227 Kč	5 227 Kč
Ubiquiti CKG2-RM	1	2 788 Kč	2 788 Kč
Ubiquiti U-POE-af	1	213 Kč	213 Kč
Optický patch kabel duplex LC-LC 50/125 MM 30m	3	1 161 Kč	3 483 Kč
Ubiquiti UACC-OM-MM-10G-D-2 - MM Module, 10G	3	1 047 Kč	3 141 Kč
			83 773 Kč

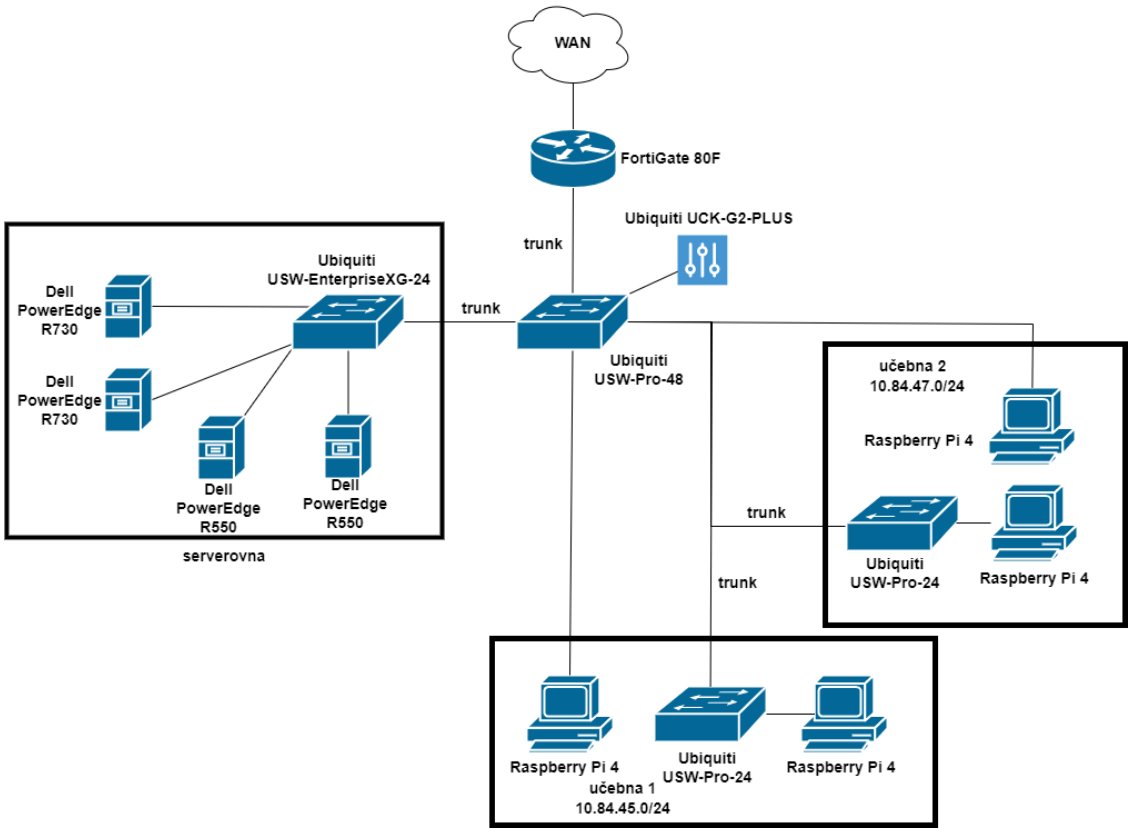
Tabulka 9.6: Síťové prvky a jejich předpokládaná cena [autor]

Na základě vybraných prvků bylo přistoupeno k návrhu fyzické topologie počítačové sítě PC učeben, přičemž bylo rozhodnuto ponechat stávající adresaci podsítí PC učeben. Pro zlepšení zabezpečení sítě byly k existujícím podsítím přidány další podsítě určené pro management, virtualizaci a virtuální stroje (VM). Takto oddělená komunikace mezi jednotlivými vrstvami pomocí firewallu umožňuje, aby byla komunikace v případě potřeby kontrolována. Pro jednotlivé spoje mezi přepínači a firewallem bylo navrženo použití trunk portů. U serverů se jevilo jako vhodné řešení jejich připojení pomocí hybridních portů. Ke všem podsítím bylo zároveň navrženo adekvátní

VLAN ID. Na základě těchto rozhodnutí byla vytvořena tabulka podsítí, ve které jsou zanedbány ostatní podsítě mimo rozsah této práce.

Název	VLAN ID	Adresa sítě
učebna 1	45	10.84.45.0/24
učebna 2	47	10.84.47.0/24
management	1777	10.84.17.0/24
virtualizace	1555	10.84.15.0/24
VM	1444	10.84.14.0/24

Tabulka 9.7: Adresace jednotlivých podsítí [autor]



Obrázek 9.1: Navržené topologie PC učeben [autor]

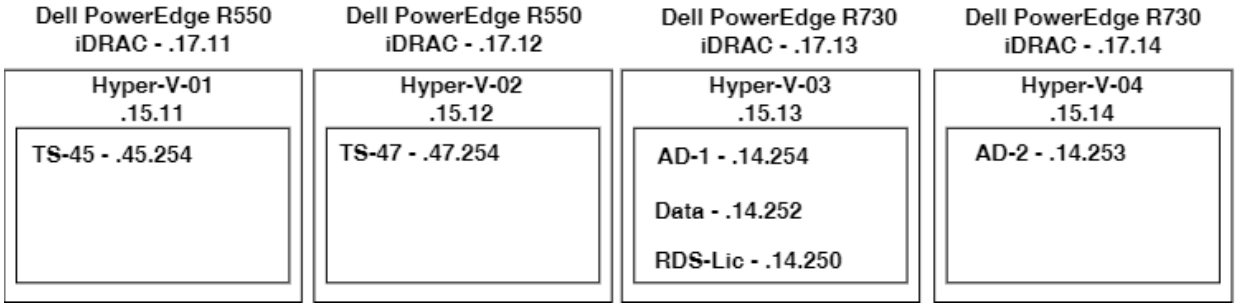
9.5 Návrh konfigurace virtualizačních serverů

Dalším krokem bylo navržení adresace a zapojení virtualizačních serverů takovým způsobem, aby byla zaručena jejich správná funkčnost a bezpečnost. K přiřazení IP adres rozhraním iDRAC byla použita navržená dedikovaná síť pro management serverů a síťových prvků. Dále bylo navrženo přiřazení IP adres z rozsahu virtualizace jednotlivým hypervizorům Hyper-V a jejich pojmenování.

Vzhledem k požadavku správce IT bylo potřeba pro nasazení Active Directory uvažovat alespoň nad dvěma doménovými řadiči (AD-1, AD-2) s nově založenou doménou ad.zsfrlazne.cz pro

případ závady na jednom z hypervizorů. Dále dva terminálové servery (TS-45, TS-47), licencování vzdálené plochy (RDS-Lic) a server, na kterém budou uložena data uživatelů (Data). Takové řešení poskytuje celkem velkou odolnost proti chybám, protože jsou jednotlivé služby oddělené do vlastních VM s instalovaným Windows Serverem 2022. Všem těmto VM byly vybrány adresy z navrženého rozsahu. Pro zvýšení odolnosti je počítáno s replikací datového i licenčního serveru každých 15 minut na druhý infrastrukturní hypervizor.

Na základě této úvahy vzniklo jednoduché schéma, které obsahuje tři vrstvy, kde první vrstvou jsou fyzické servery s rozhraním iDRAC, druhou vrstvu představují Windows Server 2022 Datacenter s nainstalovanou rolí Hyper-V a třetí vrstva se skládá z jednotlivých VM. Takto navržená serverová infrastruktura je připravená na budoucí škálování dle potřeb školy.



Obrázek 9.2: Návrh serverové infrastruktury, k zápisu IP adres jsou použity poslední dva oktety [autor]

Nakonec byla vytvořena zjednodušená přehledná tabulka 9.8 s předpokládanými náklady na realizaci počítačových učeben, včetně serverové infrastruktury a síťových prvků.

Název	**Cena celkem**
Terminálové servery	282 000 Kč
Serverové licence	231 380 Kč
Tencí klienti	143 160 Kč
Příslušenství k tenkým klientům	169 080 Kč
Síťové prvky	83 773 Kč
	909 353 Kč

Tabulka 9.8: Předpokládaná cena navrhovaného řešení [autor]

Předpokládaná cena byla spočítána zhruba o 10 % nižší (99 335 Kč) než celková nabízená cena za obě PC učebny (1 008 688 Kč) popsaná v kapitole 7 na straně 57 s tím, že obsahuje všechny potřebné licence a prvky pro budoucí rozvoj infrastruktury školy. Proto by bylo nutné tento materiál a licence zahrnout do nabízené ceny komerčního řešení, která by se vyšplhala na částku 1 166 275 Kč. Tím pádem by byl rozdíl mnohem výraznější a pohyboval by se něco přes 22 % (256 922 Kč). V navrhované ceně není započítána práce autora, jelikož realizace je součástí této bakalářské práce. Po konzultaci navrhovaného řešení se správcem sítě byl tento návrh předložen vedení školy a následně schválen, což umožnilo zakoupení potřebných prvků a licencí.

10 Realizace

Po obdržení požadovaného materiálu byla zahájena revitalizace obou učeben podle navrhovaného řešení a zároveň bylo rozhodnuto ji rozdělit do několika fází takovým způsobem, aby na sebe jednotlivé kroky navazovaly a vše proběhlo co nejvíce hladce. Jednotlivé části realizace byly stanoveny v následujícím pořadí.

1. Rekonfigurace počítačové sítě.
2. Příprava serverové infrastruktury.
3. Instalace a konfigurace virtualizace.
4. Instalace a konfigurace tenkých klientů.
5. Kompletace učeben.

10.1 Rekonfigurace počítačové sítě

Prvním krokem bylo odstranění původních prvků počítačové sítě, které byly určeny k výměně, aby na jejich místo mohlo dojít k instalaci nově zakoupených prvků. Poté došlo na firewallu FortiGate k vytvoření tří nových VLAN (management, virtualizace, VM) dle návrhu, aby do nově vytvořené management sítě mohl být zařazen management nově zakoupených přepínačů a jejich řídící jednotka. Jelikož Unifi zařízení primárně očekávají pro svou konfiguraci neoznačenou síť, byla management síť prozatím ponechána v režimu access port. Při použití portu v režimu untagged/access port je příchozí nativní komunikaci přiřazen příslušný tag dle nastaveného VLAN ID. Nově vytvořeným podsítím byly nakonfigurovány servery DHCP, u kterých bylo přidělování nastaveno v rozsahu adres 20 až 254 z toho důvodu, aby zůstal prostor pro statické adresy. Dalším nutným krokem bylo nastavit těmto nových sítím NAT, aby z jejich prostředí byl zaručen přístup do internetu. Za účelem zvýšení bezpečnosti těchto sítí bylo zapnuto logování nově vytvořených spojení, funkce IPS a antivirová kontrola.

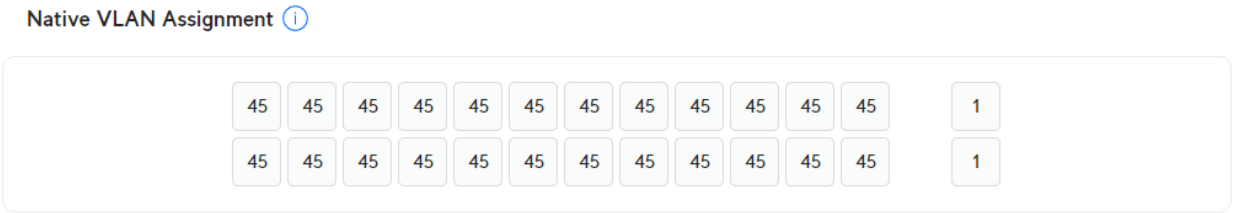
Name	From	To	Source	De...	Schedule	Servi...	Action	NAT	Security Profiles
VLAN-1444 - WAN	VM (VLAN-1444)	wan1	VLAN-1444 address	all	always	ALL	ACCEPT	Enabled	AV default IPS default SSL certificate-inspection

Obrázek 10.1: Pravidlo NAT pro síť VM [autor]

Navazujícím krokem byla výměna zastaralých síťových prvků v počítačových učebnách za nově pořízené, na které dále navazovalo natažení optických kabelů a instalace nově zakoupených prvků

do serverového a centrálního racku. Po instalaci následovalo zprovoznění Unifi Controlleru, který byl zaregistrován pod účtem školy a byla mu přiřazena statická IP adresa 10.84.17.2. Následovalo adoptování nových Unifi přepínačů a jejich aktualizace na nejnovější dostupnou verzi firmwaru. Přepínačům bylo ponecháno přiřazování IP adres pomocí DHCP a došlo k jejich zafixování pomocí statických DHCP záznamů vázaných na jejich MAC adresy. Dále byly přepínače přejmenovány dle svého umístění.

Následovalo vytvoření jednotlivých VLAN na controlleru a jejich přiřazení na porty přepínačů. V počítačových učebnách byla konfigurace jednoduchá. Spočívala v nastavení příslušné VLAN na všechny porty přepínače, kromě portů 25 a 26. U učebny 1 byly tedy porty přiřazeny do VLAN 45 a učebny 2 do VLAN 47.



Obrázek 10.2: Konfigurace přepínače pro učebnu 1 [autor]

V centrálním racku proběhla konfigurace přepínače takovým způsobem, že byla polovina portů přiřazena do VLAN 45 a druhá polovina do VLAN 47, kvůli pokrytí zbytku Ethernetových zásuvek v učebnách.

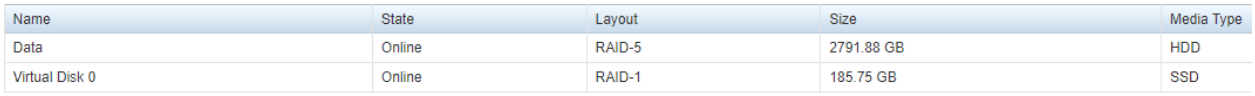
Nakonec byla provedena konfigurace přepínače v serverovém racku, kde byla 4 portům (1 až 4) přiřazena VLAN-1555 (virtualizace) a dále jim bylo nastaveno propouštění zbytku VLAN. Další 4 porty byly přidány do VLAN-1444 (management) pro budoucí připojení správy serverů skrze iDRAC.

10.2 Příprava serverové infrastruktury

Po přípravě síťové infrastruktury bylo přistoupeno k instalaci serverů do racku a jejich připojení k serverovému přepínači. U všech serverů bylo nakonfigurováno rozhraní iDRAC podle navrženého IP plánu, aby k nim mohlo být přistupováno po síti. Po přistoupení na webové rozhraní iDRAC pomocí jeho IP adresy bylo provedeno přihlášení pomocí defaultních přihlašovacích údajů „root“ a „calvin“. Následně byla zobrazena výzva ke změně hesla, jelikož výchozí heslo nelze považovat za bezpečné. Poté byla provedena konfigurace názvů jednotlivých serverů pro snadnou rozpoznatelnost s použitím formátu „model-název hypervizoru“. Nakonec byly jednotlivé servery aktualizovány na nejnovější dostupné verze firmwaru.

Dále bylo nutné provést konfiguraci raidových polí na všech serverech, kvůli zabezpečení před ztrátou dat v případě poruchy některého z přítomných disků. K jejich konfiguraci byly použity hodnoty doporučené výrobcem hardwaru.

U modelů Dell PowerEdge R730 byly pomocí rozhraní iDRAC vytvořeny dva virtuální disky, kdy jeden z nich byl nakonfigurován jako RAID-1 na přítomných SSD discích s kapacitou 200 GB pro instalaci OS. Druhý virtuální disk pro data a VM byl nakonfigurován jako RAID-5 s finální kapacitou 3 TB.



Name	State	Layout	Size	Media Type
Data	Online	RAID-5	2791.88 GB	HDD
Virtual Disk 0	Online	RAID-1	185.75 GB	SSD

Obrázek 10.3: Konfigurace disků serveru Dell PowerEdge R730 [autor]

Obdobná konfigurace proběhla i na nově zakoupených serverech Dell PowerEdge R550, kde byly SSD disky konfigurovány také v režimu RAID-1 s kapacitou 960 GB pro instalaci OS a VM, aby byla zaručena jejich vysoká rychlost. Ze tří zbylých HDD byl vytvořen RAID-5 s finální kapacitou 4 TB, který bude sloužit pro ukládání virtuálních pevných disků s daty uživatelů nebo VM.

Po úspěšném vytvoření raidových polí bylo potřeba počkat na jejich inicializaci, která při použití plné inicializace trvala u každého z použitých serverů několik hodin.

Zařízení	Typ disku	Typ pole	Stripe Size	Počet disků	Kapacita
Dell PowerEdge R730	SAS SSD	RAID-1	64 KB	2	200 GB
Dell PowerEdge R730	SAS HDD	RAID-5	64 KB	6	3 TB
Dell PowerEdge R550	SATA SSD	RAID-1	64 KB	2	960 GB
Dell PowerEdge R550	SATA HDD	RAID-5	64 KB	3	4 TB

Tabulka 10.1: Kapacity a konfigurace úložišť použitých serverů [autor]

10.3 Instalace a konfigurace virtualizace

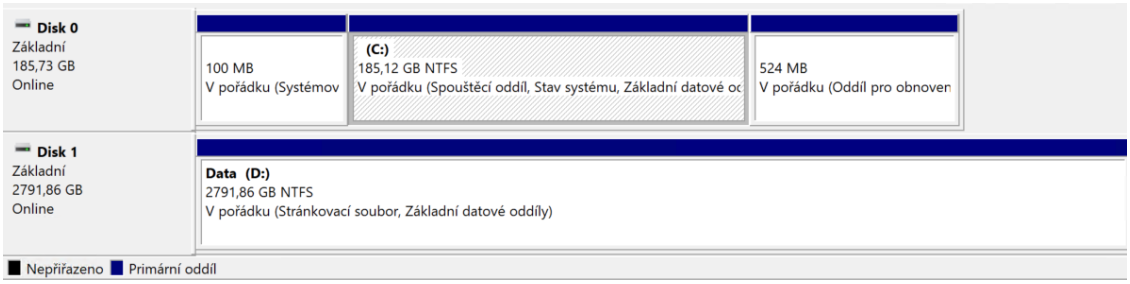
Před započetím instalace Windows Serveru 2022 Datacenter na jednotlivé servery bylo nejdříve potřeba zajistit stažení jeho instalačního ISO souboru a zaslání klíče pro jejich aktivaci od správce IT. U všech serverů byla provedena obdobná instalace a konfigurace, tudíž bude popsána instalace pouze na jednom z vybraných serverů a u zbylých bude specifikováno, jak se instalace lišila.

Prvním z instalovaných serverů byl Dell PowerEdge R730, který bude sloužit společně s druhým stejným serverem pro provoz virtuální infrastruktury školy. Následovala instalace pomocí konfiguračního rozhraní iDRAC skrze virtuální konzoli, ve které byl namapován stažený ISO soubor OS do virtuální CD/DVD mechaniky. Dále bylo určeno, že po příštím restartu má být OS zaveden z této virtuální mechaniky.

Instalace OS Windows Server je velice jednoduchá. V připraveném průvodci instalací stačí zvolit požadovanou verzi serveru, v tomto případě byla zvolena verze Windows Server 2022 Datacenter s desktopovým uživatelským rozhraním. Po zvolení požadované verze následoval výběr disku pro

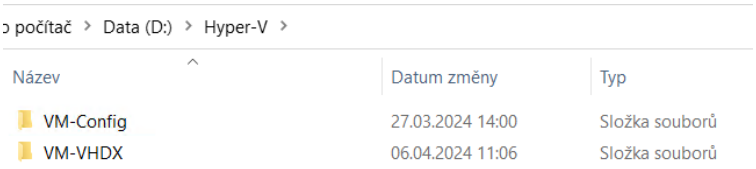
instalaci OS, kde byl vybrán vytvořený virtuální disk RAID-1. Následovalo potvrzení zápisu změn na disk a samotná instalace OS.

Po úspěšné instalaci byl proveden restart serveru, nastavení hesla pro účet administrator a přihlášení se do desktopového prostředí serveru. Důležitým krokem bylo přejmenování serveru na „Hyper-V-03“, povolení vzdálené plochy a nastavení statické IP adresy 10.84.15.13 s ostatními navazujícími parametry sítě dle návrhu. Před zahájením instalace role Hyper-V byla nejdříve pomocí správy disků provedena inicializace datového disku, přičemž jednotce bylo přiděleno písmeno D a název „Data“.



Obrázek 10.4: Konfigurace disků serveru Hyper-V-03 [autor]

Na disku D byl dále vytvořen adresář pro ukládání virtuálních strojů Hyper-V s názvem „Hyper-V“, ve kterém byly vytvořeny dva podadresáře „VM-Config“ pro ukládání konfigurací VM a „VM-VHDX“ pro ukládání virtuálních disků.



Obrázek 10.5: Vytvořené adresáře pro ukládání konfigurace a disků VM Hyper-V [autor]

Po dokončení základní konfigurace mohlo být přistoupeno k samotné instalaci role Hyper-V pomocí Správce serveru, která probíhá podle kroků v následujícím pořadí:

1. Správa serveru,
2. Přidat role a funkce,
3. výběr Instalace na základě rolí nebo na základě funkcí,
4. výběr serveru, na který je role instalována (Hyper-V-03),
5. zvolení role Hyper-V,
6. výběr rozhraní pro virtuální přepínač,
7. povolení živých migrací a výběr protokolu pro ověřování (povolit, CredSSP),
8. volba úložiště pro konfiguraci a virtuální disky Hyper-V (VM-Config a VM-VHDX),
9. potvrzení a následná instalace role Hyper-V.

Navazujícím krokem bylo restartování serveru, kdy po jeho úspěšném náběhu byla ověřena přítomnost nově nainstalovaného rozhraní Správce technologie Hyper-V jeho spuštěním a následnou změnou názvu externího virtuálního přepínače na „Virtual Switch“ pro lepší přehlednost. Takto nakonfigurovaný server byl připraven na následující instalaci jednotlivých virtuálních strojů.

U druhého serveru Dell PowerEdge R730 byla konfigurace obdobná a lišila se pouze ve změně názvu na „Hyper-V-04“ a nastavením IP adresy 10.84.15.14. Zbylým dvěma serverům Dell PowerEdge R550 byly nastaveny názvy „Hyper-V-01“ a „Hyper-V-02“, společně s IP adresami 10.84.15.11 a 10.84.15.12. Dále byla provedena změna umístění adresářů Hyper-V, které byly vytvořeny na disku C, z důvodu vyšší kapacity tohoto disku, aby byl zajištěn vyšší výkon a rychlost terminálových serverů, na kterých je závislý uživatelský zážitek celého řešení.

Zařízení	Název OS	IP	Úložiště VM	Typ úložiště
Dell PowerEdge R550	Hyper-V-01	10.84.15.11	C	SSD
Dell PowerEdge R550	Hyper-V-02	10.84.15.12	C	SSD
Dell PowerEdge R730	Hyper-V-03	10.84.15.13	D	HDD
Dell PowerEdge R730	Hyper-V-04	10.84.15.14	D	HDD

Tabulka 10.2: Přehled konfigurace jednotlivých serverů [autor]

10.4 Instalace a konfigurace VM

Úspěšná konfigurace všech virtualizačních serverů byla důležitým krokem, jelikož mohlo být následně přistoupeno k vytvoření virtualizované infrastruktury počítačových učeben tvorbou jednotlivých virtuálních strojů. Na jednotlivé hypervizory bylo přistupováno prostřednictvím vzdálené plochy, přičemž jednotlivé VM byly vytvářeny a spravovány pomocí Správce technologie Hyper-V. Dle předem připraveného návrhu došlo k započetí instalací základních VM: AD-1, AD-2, RDS-Lic a Data. U vytváření VM je vždy postup identický, tudíž bude v rámci práce popsána konfigurace jedné VM a u zbylých budou specifikovány jejich přidělené hardwarové prostředky a změny v konfiguraci samotných instalovaných OS. Pro lepší odlišitelnost bylo zvoleno pojmenování VM ve tvaru „zkratka OS-název hosta“.

AD-1

Prvním potřebným krokem před instalací ostatních VM bylo zprovoznění Active Directory a DNS serveru s nově vytvořenou doménou ad.zsfrlazne.cz, aby do ní mohly být přidány jak hypervizory, tak ostatní virtuální servery. Instalace probíhala na serveru Hyper-V-03.

Vytváření VM pomocí Správce technologie Hyper-V je velice jednoduché, přičemž je za tímto účelem přítomen jednoduchý průvodce. Příprava nové VM probíhá následujícím způsobem:

1. Správce technologie Hyper-V,
2. sekce akce,
3. nová,
4. výběr názvu VM (W22-AD-1),
5. výběr generace VM dle potřeby (Generace 2),
6. přiřazení paměti RAM (16 384 MB),
7. konfigurace sítě (Virtual Switch),
8. vytvoření virtuálního pevného disku (256 GB),
9. výběr ISO souboru pro instalaci OS (Windows Server 2022),
10. kontrola parametrů VM,
11. vytvoření VM.

Po dokončení průvodce bylo potřeba v nastavení VM dále upravit parametry počtu vCPU na 8 virtuálních jader a v nastavení síťového adaptéru povolit identifikaci virtuální sítě LAN zadáním VLAN ID pro síť VM, tedy 1444. Následně bylo přistoupeno k zapnutí VM a instalaci OS Windows Server 2022 Datacenter.

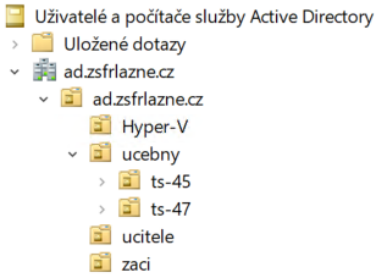
Dále pokračovala základní konfigurace, která zahrnovala změnu jména na „AD-1“, povolení vzdálené plochy, změnu IP adresy na 10.84.14.254 a aktivaci serveru. Jelikož byla dostupná licence Windows Server 2022 Datacenter, tak se aktivace jednotlivých VM prováděla pomocí rozhraní PowerShell zadáním příkazu „slmgr /ipk W3GNR-8DDXR-2TFRP-H8P33-DV9BG“, při kterém je použit generický klíč určený pro danou verzi, jak je popsáno v dokumentaci k aktivaci VM [78]. Poté byl server restartován.

Po úspěšném spuštění byla zahájena instalace role Active Directory Domain Services a DNS stejným způsobem, jako při instalaci role Hyper-V. Následuje spuštění průvodce konfigurací služby AD DS z rozhraní Správce serveru, kde byla konfigurace provedena v tomto pořadí:

1. přidat novou doménovou strukturu (ad.zsfrlazne.cz),
2. úroveň funkčnosti domény a doménové struktury (Windows Server 2016),
3. nastavení hesla pro obnovení,
4. kontrola všech ostatních kroků,
5. provedení instalace a restartování serveru.

Následujícím krokem bylo vytvoření základní doménové struktury pomocí nástroje Uživatelé a počítače služby Active Directory, a to vytvořením organizačních jednotek (OU) pro učitele, žáky, terminálové servery a Hyper-V. Do organizačních jednotek byly následně přidány jednotlivé uživatelské účty správcem IT, které byly přiřazeny do příslušné uživatelské skupiny, aby s nimi mohlo být dále pracováno při konfiguraci sdílených disků a složek. Organizační jednotka učebny byla dále rozdělena na dvě, a to ts-45 a ts-47.

Dále byly pomocí nástroje Správce DNS ve vlastnostech DNS serveru změněny DNS servery pro předávání na DNS servery poskytovatele internetu.



Obrázek 10.6: Vytvořené organizační jednotky v doméně ad.zsfrlazne.cz [autor]

Nezbytným krokem bylo upravení pravidel pro doménová hesla pomocí nástroje Správa zásad skupiny ve vlastnostech objektu Default Domain Policy, které byly nastaveny dle požadavků správce IT. Následovalo přidání objektů zásad skupiny (GPO) pro učitele a žáky, ve kterých byly omezeny některé funkce systému Windows. U žákovských zásad byly nastaveny možnosti jako: zákaz používat CMD, PowerShell, nastavení systému, upraveno chování hlavního panelu, start menu a mnoho dalších. Pro zvýšení bezpečnosti došlo také ke specifikaci povolených aplikací, které mohou být těmito skupinami spuštěny.

Dále bylo přistoupeno k přidání všech hypervizorů do nově vytvořené domény. Za tímto účelem bylo nutné vytvořit firewallové pravidlo, které povoluje pouze nezbytné porty pro komunikaci s AD servery a komunikaci mezi sítěmi, z nichž budou jednotlivé PC a servery připojovány. Pro zvýšení zabezpečení byly v konfiguraci firewallu vytvořeny virtuální IP adresy na základě použitých IP adres AD serverů, které byly následně použity v novém pravidle jako cílové IP adresy.

Před přidáním jakéhokoliv PC do domény je potřeba změnit DNS servery na IP adresy AD serverů, v tomto případě na 10.84.14.254 a 10.84.14.253. Následujícím krokem je nastavení domény ad.zsfrlazne.cz ve vlastnostech systému na kartě název PC po kliknutí na tlačítko změnit, kdy je poté vyzváno k zadání administrátorského účtu domény a příslušného hesla.

Tímto postupem byly hypervizory přidány do domény, což umožňuje přístup k nim pomocí doménových účtů. Tento přístup zjednodušuje obsluhu a umožňuje využití dalších funkcí, které to vyžadují.

AD-2

Pro zajištění redundance v případě selhání hlavního doménového řadiče byla instalace druhého doménového řadiče provedena na serveru Hyper-V-04. Konfigurace řadiče spočívala ve vytvoření VM s názvem W22-AD-2 a se stejnými parametry jako v případě W22-AD-1. Instalace byla provedena též identicky s tím, že bylo změněno jméno OS na AD-2, IP adresa na 10.84.14.253 a IP adresa DNS serveru na 10.84.14.254.

Následovalo přidáni role Active Directory Domain Services identicky jako v prvním případě s tím, že namísto výběru přidat novou doménovou strukturu, bylo zvoleno přidat řadič do již existující

domény, kde byla zadána doména ad.zsfrlazne.cz. Po úspěšné instalaci a restartování byl připraven záložní řadič domény k použití.

Data

Před započetím instalace serverů určených pro provoz tenkých klientů byl nejdříve nainstalován server pro sdílení složek a disků doménových uživatelů, aby byla data oddělena mimo doménové servery. Instalace byla provedena na serveru Hyper-V-03. Jelikož bylo počítáno s možným větším zatížením při větším počtu přístupu k datům, byly hardwarové parametry nastaveny stejně jako v případě doménových serverů, tedy název W22-Data a kapacita systémového disku na 128 GB.

Za účelem oddělení dat od OS byl tomuto VM vytvořen další virtuální disk následujícím způsobem:

1. Správce technologie Hyper-V,
2. sekce akce,
3. nová,
4. pevný disk,
5. výběr formátu disku (VHDX),
6. zvolit typ disku (Dynamicky se zvětšující),
7. volba názvu disku (data),
8. výběr velikosti virtuálního disku (1 024 GB),
9. dokončení průvodce.

Takto vytvořený virtuální disk byl následně přidán v nastavení VM pro další použití v rámci instalovaného OS.

Poté byl nainstalován OS již popsaným způsobem s tím rozdílem, že došlo ke změně jména OS na Data, povolení vzdálené plochy, nastavení IP adresy na 10.84.14.252 společně s DNS servery 10.84.14.254 a 10.84.14.253 a přidání do domény ad.zsfrlazne.cz. Po restartování serveru byl inicializován datový disk, kterému bylo přiděleno písmeno jednotky D a název data. Takto nakonfigurovaný server byl připraven k poskytování sdílených složek a disků pro uživatele domény, kde mohou být řízeny přístupy k jednotlivým sdíleným složkám na základě příslušnosti k dané skupině.

Nutným krokem k zpřístupnění diskové kapacity bylo vytvoření firewallového pravidla povolujícího přístup na IP adresu serveru pomocí protokolu SMB.

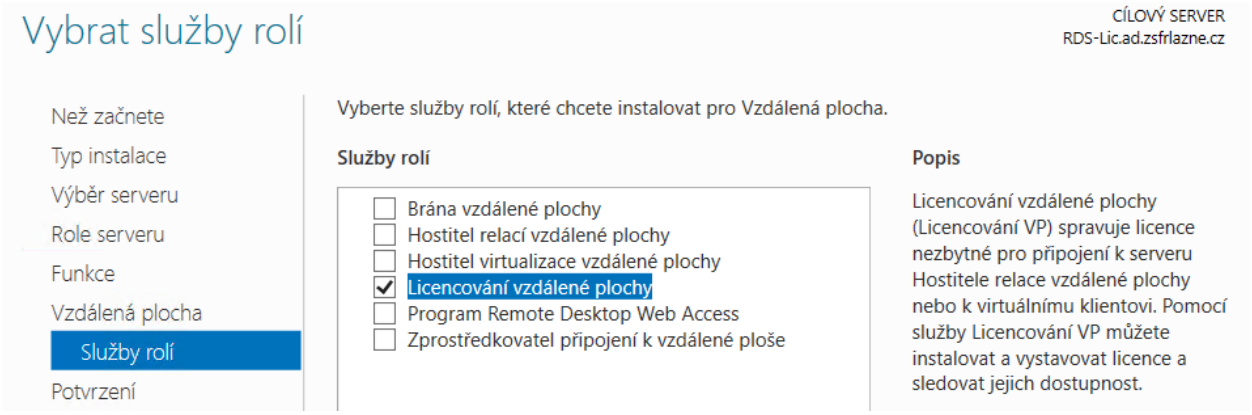
RDS-Lic

Následným krokem byla instalace serveru sloužícího pro licencování vzdálené plochy, který může v případě potřeby sloužit jako brána vzdálené plochy pro vyvažování zátěže. Jelikož se jedná

o server, který se stará pouze o licencování vzdálené plochy, jsou jeho nároky velmi nízké, a proto byly VM přiděleny 4 vCPU a 8 GB RAM, které by měly být více než dostatečné pro jeho provoz. Ostatní parametry byly zvoleny identicky jako u dříve vytvořených VM. Pro systémový disk byla zvolena kapacita 128 GB, jako hypervizor Hyper-V-03 a název W22-RDS-Lic.

Dále byl nainstalován OS, kde došlo k identické konfiguraci jako v případě datového serveru, s rozdílem změny názvu na RDS-Lic a nastavení IP adresy 10.84.14.250. Následovalo přidání serveru do domény.

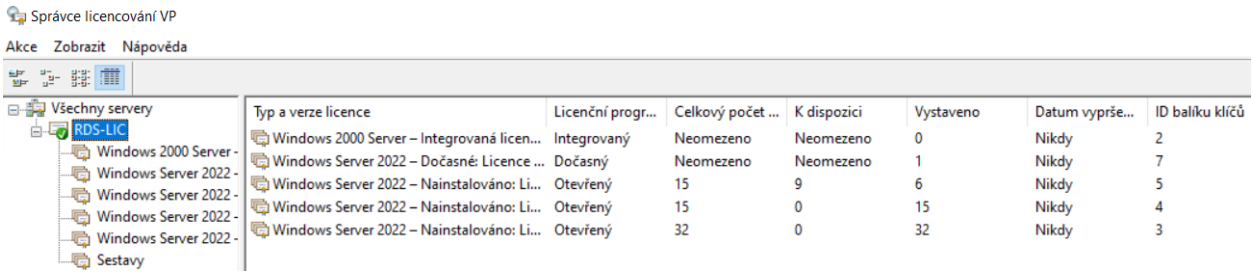
Poté byla nainstalována role serveru vzdálená plocha společně s vybranou službou role licencování vzdálené plochy, aby mohly být na server nainstalovány zakoupené licence pro vzdálenou plochu.



Obrázek 10.7: Instalace licencování vzdálené plochy [autor]

Po dokončení instalace byl vyvolán průvodce konfigurací licenčního serveru, kde bylo nutné tento server přidat do skupiny licenčních serverů terminálových serverů v AD.

Dalším krokem bylo spuštění nástroje Správce licencování VP, kde bylo potřeba nový licenční server aktivovat a vyplnit požadované údaje o organizaci, aby mohly být nainstalovány licence pro vzdálenou plochu. Aktivací se licenční server objeví mezi dostupnými servery. Licence na něj lze nainstalovat pravým kliknutím na jeho jméno a výběrem možnosti „nainstalovat licence“. Následuje otevření průvodce, kde je zvolen příslušný licenční program podle zakoupených licencí, v tomto případě Open License. Poté dojde k výzvě pro zadání autorizačního a licenčního čísla. Dokončením aktivace příslušných licencí byl server připraven pro použití společně s terminálovými servery.



Obrázek 10.8: Nainstalované licence vzdálené plochy [autor]

Posledním krokem bylo vytvoření firewallového pravidla z VLAN terminálových učeben tak, aby pro ně byl licenční server viditelný. Jelikož nemá licencování vzdálené plochy pevně dané

porty, bylo povoleno vše, kromě protokolu RDP. Pro zvýšení zabezpečení byly povoleny pouze IP terminálových serverů a jako cíl specifikován licenční server.

TS-45

Připravením všech potřebných serverů mohlo být přistoupeno na instalaci terminálových serverů počítačových učeben.

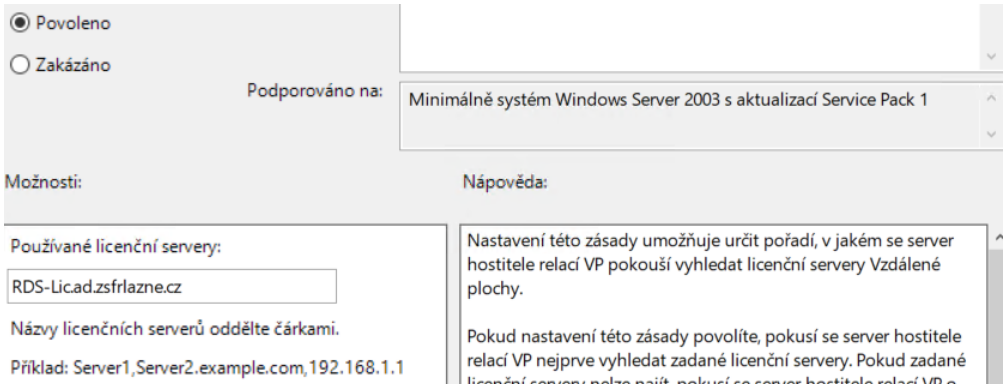
Instalace terminálového serveru pro učebnu 1 byla provedena na hypervizoru Hyper-V-01, kde byl VM pojmenován W22- TS-45. Virtuálnímu stroji byly přiděleny následující hardwarové prostředky: 32 vCPU, 64 GB RAM a systémový disk o kapacitě 256 GB. Síťový adaptér byl nastaven do VLAN 45.

Následovala instalace OS podle již zavedeného postupu se změnou jména na TS-45, IP adresy na 10.84.45.254, povolením vzdálené plochy a přidáním serveru do domény.

Před samotnou instalací a konfigurací role Hostitele vzdálené plochy bylo nutné přistoupit ke změnám nastavení licenčního režimu služby Vzdálená plocha a určení licenčního serveru. Tyto změny je potřeba provést v místních zásadách skupiny serveru. Licencování bylo zvoleno na základě zařízení, jelikož byly tyto licence zakoupeny podle připraveného návrhu, a jako licenční server byl zvolen RDS-Lic.

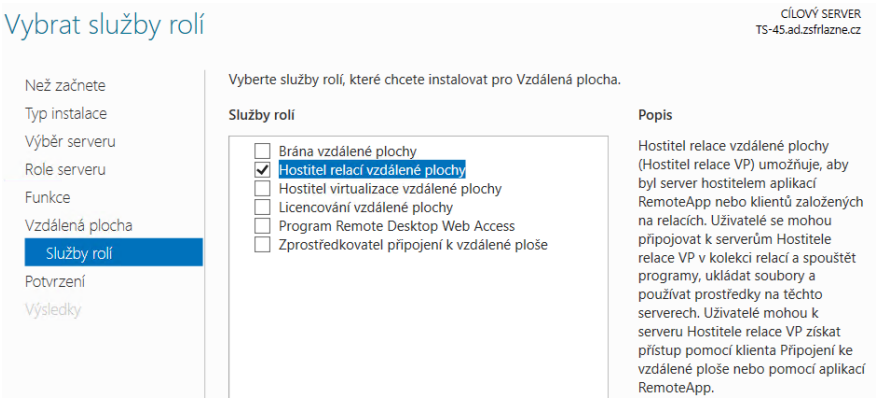
Nastavení režimu licencování a licenčního serveru bylo provedeno následujícím způsobem:

1. win + R,
2. spuštění gpedit.msc,
3. konfigurace počítače,
4. šablony pro správu,
5. součásti systému Windows,
6. služba Vzdálená plocha,
7. hostitel relací vzdálené plochy,
8. správa licencí,
9. použít určené licenční servery služby Vzdálená plocha (povoleno, RDS-Lic.ad.zsfrlazne.cz),
10. nastavit licenční režim služby Vzdálená plocha (povoleno, podle zařízení).



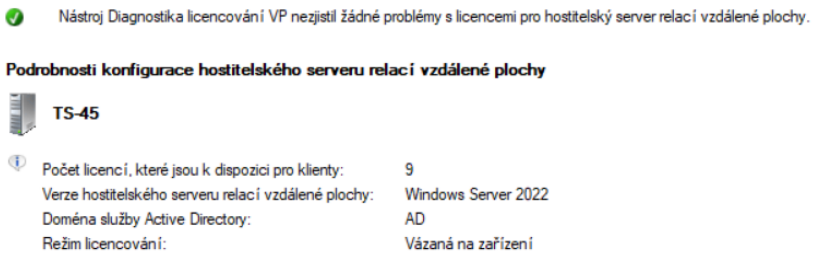
Obrázek 10.9: Konfigurace licenčního serveru vzdálené plochy [autor]

Instalace role vzdálené plochy s funkcí hostitele relací vzdálené plochy probíhá stejně jako u jiných již instalovaných rolí, a to přidáním role pomocí Správce serveru.



Obrázek 10.10: Instalace role Hostitel relací vzdálené plochy [autor]

Po úspěšné instalaci této role byla zkontrolována její funkčnost pomocí nástroje diagnostika licencování Vzdálené plochy.



Obrázek 10.11: Diagnostika licencování vzdálené plochy [autor]

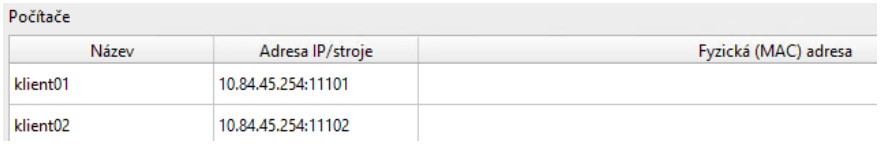
Následným krokem bylo povolení připojení pomocí vzdálené plochy skupinám pro učitele a žáky, které byly vytvořeny v AD a byly přiděleny příslušným uživatelským účtům. Tato konfigurace byla provedena v rámci nastavení vzdálené plochy, kde je po kliknutí na tlačítko vybrat uživatele možné specifikovat jednotlivé uživatelské účty či skupiny.

Po ověření funkčnosti byly nainstalovány požadované programy zjištěné v rámci analýzy potřeb školy. Jednalo se o následující programy: Mozilla Firefox, Google Chrome, Python + PyCharm,

Visual Studio, LEGO Mindstorms, Inkscape, GIMP, MS Office a GeoGebra. Tato nainstalovaná množina programů byla přidána do povolených programů ke spuštění ze strany žáků. Zároveň byl pro budoucí instalaci tenkých klientů nainstalován ThinLinX Management Software (TMS) společně s potřebným firewallovým pravidlem.

Za účelem dohledu nad žáky v hodině byl na terminálový server nainstalován program Veyon. Pro jeho konfiguraci slouží aplikace Veyon Configurator, ve které byl dále nakonfigurován na záložce služba pro multi-session mode, v jehož rámci je možné provádět dohled nad relacemi jednotlivých uživatelů. Dalším krokem ke zpřístupnění těchto relací pro dohled bylo v záložce umístění a počítače vytvoření umístění s názvem učebna a přidání jednotlivých relací, kdy bylo pro formát názvu zvoleno „klient01-30“ na základě počtu tenkých klientů. U první relace došlo k zadání IP adresy ve formátu 10.84.45.254 společně s portem 11101. Pro každou další relaci zůstává IP adresa stejná a zvedá se pouze číslo portu o jedna.

Pro dohled nad jednotlivými relacemi následně slouží aplikace Veyon Master, kde je možné nad těmito relacemi převzít i úplnou kontrolu, případně je uzamknout či odhlásit.


Počítače

Název	Adresa IP/stroje	Fyzická (MAC) adresa
klient01	10.84.45.254:11101	
klient02	10.84.45.254:11102	

Obrázek 10.12: Konfigurace relací v dohledovém programu Veyon. [autor]

Takto nakonfigurovaný terminálový server byl připraven k nasazení v počítačových učebnách společně s tenkými klienty.

TS-47

Konfigurace terminálového serveru pro druhou učebnu byla stejná a lišila se pouze ve vytvoření VM na hypervizoru Hyper-V-02 s názvem W22- TS-47. Hardwarová konfigurace tohoto VM byla zachována identicky jako u prvního serveru, pouze s rozdílným VLAN ID v případě síťového adaptéru, které bylo nastaveno na 47.

Po instalaci OS byl změněn název na TS-47, povolena vzdálená plocha, IP nastavena na 10.84.47.254 s následným přidáním do domény.

Následovala konfigurace a instalace potřebné role společně s předcházejícími a navazujícími kroky, které již byly zmíněny v rámci instalace serveru TS-45.

Po dokončení této konfigurace byla nainstalována stejná sada programů se stejným nastavením a omezeními tak, aby byla konfigurace mezi učebnami zachována identicky. Ke změně došlo pouze u programu Veyon, kde bylo použito pojmenování klientů ve formátu „klient31-60“.

Provedením všech těchto kroků byla dokončena instalace druhého terminálového serveru, který byl připraven na nasazení. Poté mohlo dojít k přípravě tenkých klientů a jejich instalaci do PC učeben.

Hypervizor	VM	vCPU	RAM	VLAN ID	IP
Hyper-V-03	W22-AD-1	8	16 384 MB	1444	10.84.14.254
Hyper-V-04	W22-AD-2	8	16 384 MB	1444	10.84.14.253
Hyper-V-03	W22-Data	8	16 384 MB	1444	10.84.14.252
Hyper-V-03	W22-RDS-Lic	4	8 192 MB	1444	10.84.14.250
Hyper-V-01	W22-TS-45	32	65 536 MB	45	10.84.45.254
Hyper-V-02	W22-TS-47	32	65 536 MB	47	10.84.47.254

Tabulka 10.3: Přehled konfigurace jednotlivých virtuálních serverů [autor]

10.5 Nasazení tenkých klientů

Navazujícím krokem na již připravené technologie byla instalace a konfigurace tenkých klientů pro nasazení v učebnách společně s nakoupeným příslušenstvím, která nebyla nikterak složitá, ale časově náročná. Instalace a konfigurace se skládala z několika kroků:

1. složení tenkých klientů,
2. instalace TLXOS,
3. montáž tenkých klientů do učeben,
4. konfigurace potřebných nastavení.

Příprava HW a počítačových učeben

Prvním krokem byla montáž chladičů na Raspberry Pi 4, aby byl zaručen odvod tepla z procesoru do okolního vzduchu. Následně byla všechna takto osazená Raspberry Pi 4 namontována do zakoupených krabiček, za účelem jejich snadné montáže a ochrany před poškozením.

Druhým krokem byla instalace OS tenkých klientů TLXOS na zakoupené SD karty, která byla provedena pomocí Raspberry Pi Imageru stejným způsobem, jako v případě testování. Takto připravené SD karty byly vloženy do příslušného slotu a tencí klienti byli připraveni pro montáž do PC učeben.

Následovala příprava pracovních míst v učebnách, přičemž nejdříve došlo k demontáži starých tenkých klientů společně s jejich periferiemi. Poté byla zkontrolována kabeláž mezi switchem/zásuvkami a tenkými klienty, aby bylo zaručeno připojení rychlostí 1 Gbit/s.

Dalším krokem byla montáž monitorů, které byly následně rozestaveny po stolech společně s připojenými HDMI kabely, aby mohlo dojít k nasazení tenkých klientů. Před instalací tenkých klientů byly ještě připraveny napájecí adaptéry společně s vypínači. Na takto připravená pracovní místa byli poté jednotliví tencí klienti připojeni společně se zakoupenými periferiemi a mohlo dojít k jejich finální konfiguraci.

Obrázek 10.13: Tenký klient Raspberry Pi 4 [autor]

Konfigurace tenkých klientů

Konfigurace v rámci učeben byla provedena identicky a liší se pouze v použitých názvech klientů a IP adrese terminálového serveru. Jelikož byl na obou terminálových serverech při jejich přípravě nainstalován program TMS, který se používá pro centrální správu tenkých klientů, mohl být zbytek nastavení proveden již vzdáleně. Tencí klienti se v programu TMS zobrazili automaticky, protože jsou na stejném segmentu sítě společně s terminálovým serverem, a tudíž funguje jejich automatické vyhledávání a připojení.

Před nastavením parametrů pro připojení k serveru bylo potřeba jednotlivým klientům nainstalovat zakoupenou licenci. Instalace licence se provádí pomocí rozbalovacího menu device v sekci update kliknutím na install license, kde je poté vyzváno k zadání přihlašovacích údajů účtu, na který byly licence zakoupeny.

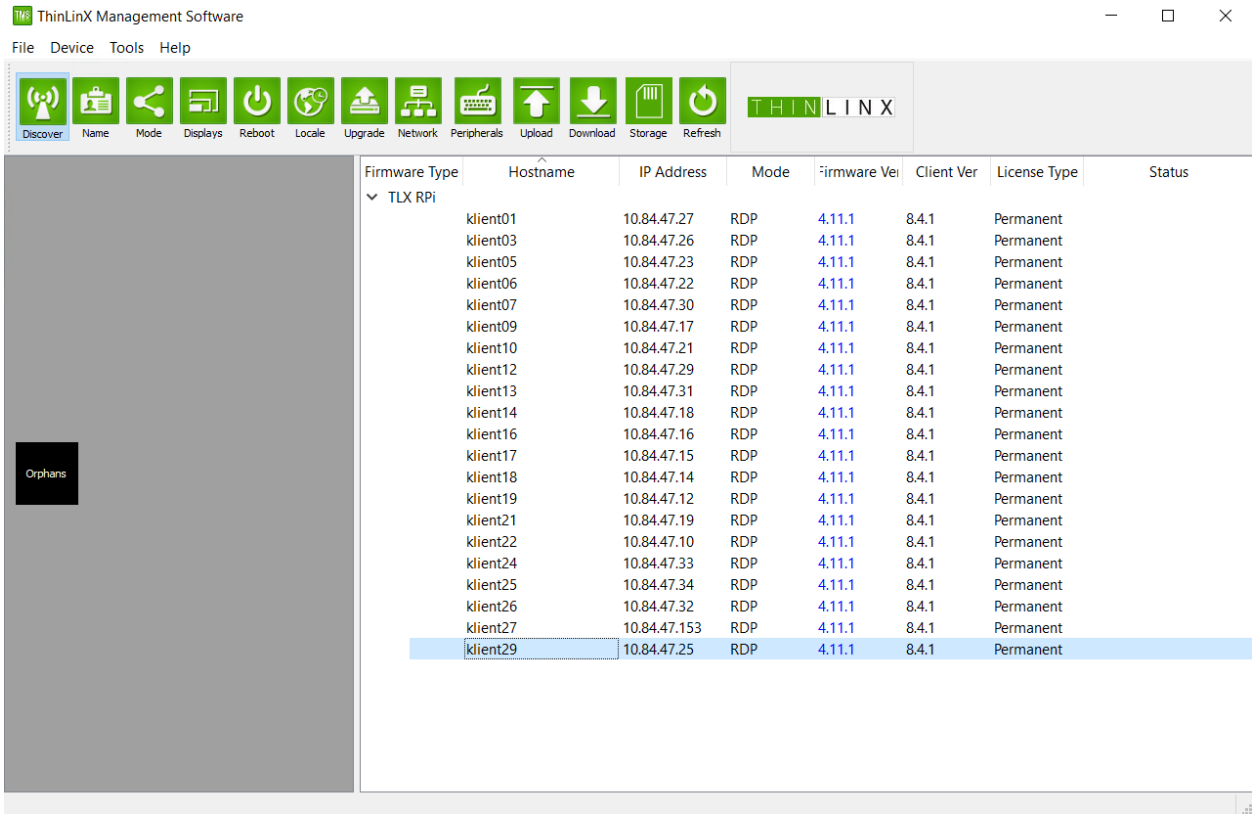
Poté byla provedena změna názvu všech tenkých klientů ve formátu „klient01-60“, přičemž rozsah 1—30 byl použit pro učebnu 1 a rozsah 31—60 pro učebnu 2. Změna jména se provádí po kliknutí na tlačítko name.

Navazujícím krokem byla změněna nastavení klávesnice na české rozložení a zapnutí num locku, přičemž ovládání těchto funkcí se nachází pod ikonou peripherals. Dále bylo po kliknutí na locale nastaveno časové pásmo Europe/Prague a jazyk na cs_CZ.

Jelikož se počítá s nepřetržitým provozem tenkých klientů bez jejich vypínání, bylo potřeba v rozbalovacím menu device v sekci local configuration zapnout možnost set power saving. V této sekci bylo dále nastaveno administrátorské heslo, což umožňuje změny nastavení na jednotlivých klientech pouze po jeho zadání. Tímto způsobem byla zaručena bezproblémová funkčnost a bezpečnost učeben. Heslo se nastavuje v možnosti set restricted feature password po jejím povolení.

Konfigurace připojení k terminálovým serverům byla provedena stejně jako v případě testovací konfigurace 8.4 na straně 65. Rozdíl spočívá v tom, že pro učebnu 1 byl specifikován server 10.84.45.254 a pro učebnu 2 10.84.47.254.

Takto nakonfigurovaní tencí klienti byli připraveni k použití v rámci počítačových učeben, tím pádem mohlo dojít k ověření jejich funkčnosti.



Obrázek 10.14: Pohled na připojené klienty v programu TMS [autor]

10.6 Ověření funkčnosti nasazených technologií

Za účelem ověření funkčnosti nasazených technologií byla pozvána třída, která provedla přihlášení na všech klientech v rámci obou počítačových učeben.

Na přihlášených klientech byla dále prověřena funkčnost všech požadovaných programů a případná lehká práce s nimi. Při testování bylo dohlíženo na jednotlivé žáky pomocí instalovaného programu Veyon.

Co se týká zátěže terminálových serverů, maximální zatížení CPU bylo naměřeno 83 %, u RAM bylo naměřeno maximální vytížení 27 % a využití sítě se pohybovalo při připojení všech klientů do 100 Mbit/s.

Po dokončeném testování bylo provedeno odhlášení na jednotlivých klientech a vyčkáno, zda se projeví nastavení úspory tenkých klientů v případě nečinnosti, kdy po 15 minutách došlo k vypnutí všech obrazovek. Takto otestované učebny byly připraveny k předání.

Na straně serverových technologií byl ještě proveden test migrace VM mezi dvěma hypervizory, aby bylo ověřeno, že je vše plně funkční. Za tímto účelem byla přesunuta VM W22-RDS-Lic na server Hyper-V-04 a zpět. K přesunu VM je potřeba použít správce technologie Hyper-V, vybrat VM, zvolit možnost přesunout a poté specifikovat cílový server a úložiště VM.

Posledním krokem bylo předání nakonfigurovaných technologií správci sítě a jeho zaškolení v jejich provozu.

Obrázek 10.15: Hotová a otestovaná PC učebna [autor]

10.7 Náklady na realizaci a porovnání možných řešení

Po úspěšném dokončení celého projektu obnovy počítačových učeben mohlo dojít k vyčíslení celkových nákladů na realizaci, které se od navrhované částky 909 353 Kč lišily jen minimálně, a to v řádu tisíců korun, jelikož bylo potřeba připočítat práci při instalaci optických kabelů a spotřební materiál.

V případě nasazení v jiné organizaci by bylo nutné započítat náklady na instalaci a konfiguraci jednotlivých technologií. Pro představu nad předpokládanými náklady v případě realizovaného řešení v rámci této práce byl proveden odhad časové náročnosti a s tím spojených nákladů na základě zkušeností z realizace.

Za tímto účelem bylo nutné určit hodinové sazby za práci na serverových technologiích a za ostatní práce (konfigurace síť. prvků, kabeláž, instalace a konfigurace tenkých klientů apod.). U serverové práce byla určena sazba 2 000 Kč/hod. a u ostatní práce 750 Kč/hod.

Za účelem lepšího přehledu byla vytvořena následující tabulka, která ukazuje odhadované hodiny.

Typ práce	Počet hodin	Kč/hod.	Cena celkem
Serverová	16	2 000 Kč	32 000 Kč
Ostatní	40	750 Kč	30 000 Kč
	56		**62 000 Kč**

Tabulka 10.4: Odhadovaný čas a náklady na realizaci obou učeben [autor]

Při sečtení navržené ceny použitého řešení a odhadnuté ceny za práci by se finální náklady na realizaci daly vyčíslit na 971 353 Kč. Pokud tyto odhadované náklady srovnáme s částkou 1 166 275 Kč za komerční řešení, které bylo popsáno v kapitole 9.5 na straně 82 a zahrnovalo by stejnou funkčnost, získáme jasnější porovnání obou variant. Cenová úspora by v takovém případě dosáhla 194 922 Kč, což představuje přibližně 17 %.

Porovnání možných řešení

Pro srovnání rozdílných řešení PC učeben bylo vytvořeno následující porovnání, které ukazuje, v jakých částkách se pohybuje řešení v případě použití klasických počítačů oproti tenkým klientům použitých v rámci této práce. Pro porovnání byl vybrán Dell Optiplex 7010 Micro MFF (i3 13100T, 8 GB, 256 GB) s cenou 11 690 Kč (aktuální cena k 11. 4. 2024), o kterém by bylo vhodné uvažovat do klasické počítačové učebny [79]. Pro terminálové učebny byla spočítána cena s použitými servery v rámci této práce jak s použitím licence Standard, tak Datacenter, pro lepší představu o rozdílu v ceně. Pro tuto kalkulaci byly použity částky uvedené v kapitole 9 na straně 77. Za tímto účelem vznikly tři varianty možného řešení.

1. varianta: 60x Dell Optiplex 7010 Micro MFF.
2. varianta: 60x Raspberry Pi 4 + TLXOS, 2x terminálový server + 16x Windows Server 2022 Standard (2 Core) + 60x device CAL a RDS licence.
3. varianta: 60x Raspberry Pi 4 + TLXOS, 2x terminálový server + 16x Windows Server 2022 Datacenter (2 Core) + 60x device CAL a RDS licence.

Pro porovnání finanční úspory byla vytvořena následující tabulka.

Varianta	Cena	Úspora
1.	701 400 Kč	–
2.	499 200 Kč	202 200 Kč (29 %)
3.	567 936 Kč	133 464 Kč (19 %)

Tabulka 10.5: Finanční porovnání jednotlivých variant [autor]

Nákup tenkých klientů společně s licencemi Windows Serveru představuje také nespornou výhodu v tom, že může být nasazeno řešení Active Directory dále v rámci celé organizace.

Představa nad spotřebou elektrické energie při rozdílných řešení počítačových učeben může být provedena na základě následující tabulky. Tabulka porovnává spotřebu mezi řešením s počítači Dell Optiplex 7010 Micro MFF a tenkými klienty Raspberry Pi 4, kteří jsou použiti společně se serverem Dell PowerEdge R550. Spotřeba počítače Dell Optiplex 7010 Micro MFF byla odhadnuta na základě nalezené recenze, jelikož nebyl dostupný k přímému testování [80]. Pro spotřebu Raspberry Pi 4 byly použity výsledky z kapitoly 8.3 na straně 75. Spotřeba serveru Dell PowerEdge R550 byla zjištěna na základě údajů z rozhraní iDRAC, které k nim umožňuje přístup. Průměrná spotřeba jednoho zařízení je uvedena ve druhém sloupci a celková spotřeba je uvedena ve třetím sloupci.

Zařízení	Průměrná spotřeba	Celková průměrná spotřeba
Dell Optiplex 7010 Micro MFF	13 W	780 W
Raspberry Pi 4	4,3 W	258 W
Dell PowerEdge R550	236 W	236 W

Tabulka 10.6: Přehled průměrné spotřeby zařízení v porovnávaných řešeních [autor]

Z tabulky vyplývá, že řešení učebny pomocí terminálového serveru a tenkých klientů má celkovou spotřebu 494 W, což při porovnání s klasickými PC se spotřebou 780 W představuje úsporu 286 W (36 %). Taková úspora se může promítnout do provozních nákladů. Pokud by terminálové servery byly použity zároveň jako infrastrukturní, bude úspora na provozních nákladech vyšší.

Pokud by se jednalo o organizaci mimo školství, bylo by dále potřeba počítat s velkým navýšením cen licencí za serverový software v řádu vyšších desítek procent. V takovémto případě se řešení pomocí tenkých klientů nemusí jevit jako výhodné ve srovnání s klasickými PC, a je tedy potřeba ho důkladně zvážit v kontextu použití.

11 Závěr

Bakalářská práce se věnovala tématu analýzy využití tenkých klientů a jejich nasazení v PC učebnách s důrazem na co nejvíce efektivní a levné řešení. Praktická část byla autorem práce realizována v počítačových učebnách a souvisejících prostorách Základní školy Františkovy Lázně, na základě jejího zadání.

V teoretickém úvodu práce byla popsána virtualizace, její různé aspekty, dělení a typy, kde byl kladen důraz na použití v kontextu počítačových učeben. V rámci této kapitoly byly diskutovány také její výhody a nevýhody. Následně byla popsána aktuálně dostupná řešení z oblasti virtualizace, u kterých byly uvedeny základní funkcionality, dostupné možnosti správy, společně s jejich licenčními podmínkami. Zkoumány byly jak komerční produkty typu Microsoft Hyper-V a VMware ESXi, tak open-source alternativy jako KVM nebo XCP-ng.

Dále byla pozornost věnována aktuálně používaným technologiím pro vzdálený přístup k serveru, kde byly popsány jednotlivé rozdíly při použití single-session a multi-session OS a s tím související možnosti nasazení, mezi které se řadí VDI a desktopy založené na uživatelských relacích. Poté byla nastíněna funkčnost a možnosti jednotlivých protokolů pro vzdálený přístup k serveru, mezi které se řadí RDP, VNC, Citrix ICA, VMware Blast Extreme a SPICE.

Následně byla věnována kapitola tenkým klientům a jejich hardwarovým a softwarovým řešením. Došlo ke specifikování základních parametrů, které by měl ideální tenký klient splňovat jak po softwarové, tak hardwarové stránce. Poté byly popsány dostupné OS pro nasazení společně s hardwarem tenkých klientů a již hotová HW řešení.

Navazujícím krokem byla analýza vhodných serverových operačních systémů, včetně open-source řešení a MS Windows Serveru. U open-source řešení byly zkoumány vhodné distribuce pro nasazení v počítačových učebnách společně s tenkými klienty a Linux Terminal Server Project, který je za tímto účelem vyvíjen. U Windows Serveru dále došlo k popsání jeho licenční politiky, přístupových licencí a rolí AD, DNS, DHCP a RDS.

V poslední řadě byla popsána kybernetická bezpečnost školských organizací z pohledu fyzické bezpečnosti a ochrany sítě, s ohledem na standard konektivity, který by měl být těmito organizacemi splňován.

Praktická část práce zahrnovala podrobnou analýzu stávající situace v základní škole, včetně infrastruktury PC učeben, serverového hardwaru a softwaru a síťových prvků.

Dále byla provedena analýza potřeb školy, kde byly sepsány požadavky ze stran vedení školy, správce sítě a jednotlivých učitelů. Takto zjištěné požadavky byly dále použity při testování tenkých klientů, návrhu finálního řešení a konfiguraci terminálových serverů.

Pro testování tenkých klientů bylo vytvořeno laboratorní prostředí tak, aby mohl být otestován vhodný hardware společně s OS. Za účelem efektivního testování byly stanoveny stejné podmínky, podle kterých se testování dále řídilo. U každého testovaného OS byla provedena instalace a její proces byl popsán. Po ukončeném testování byly jednotlivé OS porovnány podle podporovaných protokolů, vzdálené správy a ceny za licenci. Dále došlo k porovnání spotřeby použitého hardware. Z výsledků testování vyplynulo, že nejvhodnějším řešením je Raspberry Pi 4, které se vyznačovalo vynikající efektivitou provozu s průměrnou spotřebou pouze 4,3 W. Tato volba byla atraktivní i z hlediska cenové dostupnosti. Jako OS byl zvolen TLXOS, jelikož splňoval všechny požadavky z hlediska výkonu v rámci protokolu RDP, ale také podmínky pro centrální správu a nízké pořizovací náklady na jednu licenci.

Na základě provedené analýzy potřeb školy a testování tenkých klientů bylo navrženo konkrétní řešení, které zahrnovalo specifikace terminálových serverů, tenkých klientů, návrh síťové infrastruktury a konfigurace virtualizovaných serverů. Pro celé řešení byl zvolen OS Windows Server 2022 a virtualizace pomocí Hyper-V.

Poté bylo přistoupeno k samotné realizaci, kde bylo popsáno řešení zahrnující rekonfiguraci počítačové sítě, přípravu serverové infrastruktury, instalaci a konfiguraci virtualizace a VM, nasazení tenkých klientů a ověření funkčnosti nasazených technologií. Následovalo otestování a předání celého řešení společně s proškolením správce sítě.

Posledním krokem bylo sečtení celkových nákladů na realizaci, které lehce přesahovaly odhadované náklady. Poté bylo nastíněno, jaké jsou odhadované náklady za práci. Dále bylo provedeno porovnání s náklady na řešení učeben pomocí klasických počítačů.

Nakonec byla rozebrána otázka, jak by se navrhované řešení odlišovalo v případě jeho implementace mimo prostředí školských organizací.

Takto připravená infrastruktura školy a počítačových učeben je připravena pro další rozvoj. Dalším navazujícím krokem by mohlo být rozšíření použití Active Directory na všechny zařízení školy a v případě nasazení nové Wi-Fi sítě i na autentizaci jednotlivých uživatelů, kteří se do ní budou připojovat pomocí radius serveru. Co se týká virtualizace, bylo by dobré dále uvažovat o zakoupení zálohovacího zařízení NAS pro zálohování jednotlivých VM. Díky použitým licencím není řešení nijak limitováno a může být rozšiřováno libovolně dále.

Seznam použitých zdrojů

1. *What is virtualization?* [online]. [cit. 2023-07-28]. Dostupné z: https://www.ibm.com/topics/virtualization.
2. *About Virtualization* [online]. [cit. 2023-07-28]. Dostupné z: https://docs.oracle.com/cd/E89529_01/doc.124/wireless/concepts/c_cmp_configuring_pm_topology_virtualization.html.
3. SHIRINBAB, Sogand. *Performance Implications of Virtualization* [online]. Sweden, 2019 [cit. 2023-07-28]. ISBN ISBN: 978-91-7295-361-1. Dostupné z: https://www.diva-portal.org/smash/get/diva2:1260339/FULLTEXT02.pdf.
4. *What is a hypervisor?* [online]. [cit. 2023-07-28]. Dostupné z: https://www.vmware.com/topics/glossary/content/hypervisor.html.
5. WARD, Keith. *The Top 5 Enterprise Type 1 Hypervisors You Must Know* [online]. 2021. [cit. 2023-07-28]. Dostupné z: https://www.actualtechmedia.com/io/top-5-enterprise-type-1-hypervisors/.
6. *What is a Hypervisor? Types of Hypervisors 1 & 2* [online]. 2022. [cit. 2023-07-28]. Dostupné z: https://phoenixnap.com/kb/what-is-hypervisor-type-1-2.
7. MŮČKA, JAN. *Typy virtualizace serverů – je lepší KVM nebo LXC?* [online]. 2020. [cit. 2023-07-28]. Dostupné z: https://www.master.cz/blog/typy-virtualizace-serveru-kvm-nebo-lxc/.
8. MATYSKA, Luděk. *Techniky virtualizace počítačů (2)* [online]. 2011. [cit. 2023-07-28]. Dostupné z: http://webserver.ics.muni.cz/bulletin/articles/545.html.
9. *What is Application Virtualization?* [online]. [cit. 2023-07-29]. Dostupné z: https://www.hpe.com/emea_europe/en/what-is/application-virtualization.html.
10. DILLENBURG, Stefan. *A brief history of container virtualization* [online]. 2020. [cit. 2023-11-26]. Dostupné z: https://medium.com/an-idea/a-brief-history-of-container-virtualization-57fc96c02924.
11. KALKEN, Scott. *What Are Namespaces and cgroups, and How Do They Work?* [online]. 2021. [cit. 2023-11-28]. Dostupné z: https://www.nginx.com/blog/what-are-namespaces-cgroups-how-do-they-work/.
12. KAHUHA, Eric. *LXC vs Docker: Which Container Platform Is Right for You?* [online]. 2023. [cit. 2023-11-19]. Dostupné z: https://earthly.dev/blog/lxc-vs-docker/.

13. *What is network virtualization?* [online]. [cit. 2023-07-29]. Dostupné z: https://www.vmware.com/topics/glossary/content/network-virtualization.html.

14. *Microsoft's history of virtualization* [online]. [cit. 2023-08-02]. Dostupné z: https://subscription.packtpub.com/book/cloud-and-networking/9781785887932/1/ch01lvl1sec7/microsofts-history-of-virtualization.

15. *Introduction to Hyper-V on Windows 10* [online]. 2022. [cit. 2023-08-02]. Dostupné z: https://learn.microsoft.com/en-us/virtualization/hyper-v-on-windows/about/.

16. *What's new in System Center Virtual Machine Manager* [online]. 2023. [cit. 2023-11-18]. Dostupné z: https://learn.microsoft.com/en-us/system-center/vmm/whats-new-in-vmm?view=sc-vmm-2022.

17. LEE, Brandon. *Windows Server Hyper-V Licensing Considerations* [online]. 2023. [cit. 2023-08-02]. Dostupné z: https://www.bdrsuite.com/blog/windows-server-hyper-v-licensing-considerations/.

18. *Hyper-V Server 2019* [online]. [cit. 2023-08-03]. Dostupné z: https://www.microsoft.com/en-us/evalcenter/evaluate-hyper-v-server-2019.

19. *Windows Server documentation* [online]. 2024. [cit. 2024-02-29]. Dostupné z: https://learn.microsoft.com/en-us/windows-server/.

20. HUNTER, Alex. *What Is the VMware ESXi Server and Its Role in the VMware Suite?* [online]. 2021. [cit. 2023-08-19]. Dostupné z: https://www.parallels.com/blogs/ras/vmware-esxi/.

21. GILLIS, Alexander S. *What is VMware ESXi?* [online]. [cit. 2023-08-19]. Dostupné z: https://www.techtarget.com/searchvmware/definition/VMware-ESXi.

22. *VMware* [online]. 2024. [cit. 2024-04-29]. Dostupné z: https://www.vmware.com/.

23. *Licensing for ESXi Hosts* [online]. 2023. [cit. 2023-08-27]. Dostupné z: https://docs.vmware.com/en/VMware-vSphere/8.0/vsphere-esxi-host-client/GUID-7AFCC64B-7D94-48A0-86CF-8E7EF55DF68F.html.

24. WALSWORTH, Rick. *VMware End Of Availability of Perpetual Licensing and SaaS Services* [online]. [cit. 2024-02-21]. Dostupné z: https://blogs.vmware.com/cloud-foundation/2024/01/22/vmware-end-of-availability-of-perpetual-licensing-and-saas-services/.

25. *What is a vSphere Hypervisor?* [online]. [cit. 2023-08-27]. Dostupné z: https://www.vmware.com/content/vmware/vmware-published-sites/us/products/vsphere-hypervisor.html.html.

26. *VMware vSphere® Product Line Comparison* [online]. 2024. [cit. 2024-03-13]. Dostupné z: https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-datasheet-vsphere-product-line-comparison.pdf.

27. *Xen* [online]. [cit. 2023-08-27]. Dostupné z: https://en.wikipedia.org/wiki/Xen.

28. *Citrix Hypervisor* [online]. 2023. [cit. 2023-08-27]. Dostupné z: https://docs.xenserver.com/en-us/citrix-hypervisor/technical-overview.

29. *Xcp-ng* [online]. [cit. 2023-08-27]. Dostupné z: https://xcp-ng.org/.

30. *Xo-pricing* [online]. [cit. 2023-08-27]. Dostupné z: https://xen-orchestra.com/%5C#!/xo-pricing.

31. *What is KVM?* [online]. 2022. [cit. 2023-09-01]. Dostupné z: https://www.redhat.com/en/topics/virtualization/what-is-KVM.

32. *Proxmox Virtual Environment* [online]. [cit. 2023-08-27]. Dostupné z: https://www.proxmox.com/en/proxmox-virtual-environment/overview.

33. *OVirt Project Announces First Official Release and Upcoming Community Workshop* [online]. 2012. [cit. 2024-04-29]. Dostupné z: https://www.redhat.com/en/blog/oVirt-Project-Announces-First-Official-Release-and-Upcoming-Community-Workshop.

34. *OVirt* [online]. 2024. [cit. 2024-04-27]. Dostupné z: https://www.ovirt.org/.

35. *Red Hat* [online]. 2024. [cit. 2024-04-29]. Dostupné z: https://www.redhat.com/en.

36. *Remote protocols benchmarking, Citrix, VMware and RDP–Part One PCoIP vs Blast Extreme* [online]. 2016. [cit. 2023-07-14]. Dostupné z: https://msandbu.org/remote-protocols-benchmarking-citrix-vmware-and-rdppart-one-pcoip-vs-blast-extreme/.

37. *Which is Right For You – Single-Session or Multi-Session?* [online]. 2020. [cit. 2023-07-16]. Dostupné z: https://cameyo.com/which-is-right-for-you-single-session-or-multi-session/.

38. SILBERSCHATZ, ABRAHAM; GALVIN, PETER B.; GAGNE, GREG. *Operating System Concepts, Enhanced eText (10th Edition)*. WIley, 2018. ISBN ISBN 978-1-119-32091-3.

39. *VDI vs Session Based Desktops: What are they and how do they compare?* [online]. 2021. [cit. 2023-07-20]. Dostupné z: https://www.appsanywhere.com/resource-centre/vdi/vdi-vs-session-based-desktops-what-are-they-and-how-do-they-compare.

40. *Know the differences between RDS and VDI* [online]. 2019. [cit. 2023-09-15]. Dostupné z: https://www.vcloudpoint.com/rds-vs-vdi/.

41. *Microsoft Releases Windows NT Server 4.0 Terminal Server Edition* [online]. 1998. [cit. 2023-09-02]. Dostupné z: https://news.microsoft.com/1998/06/16/microsoft-releases-windows-nt-server-4-0-terminal-server-edition/.

42. *Remote Desktop client - supported configuration* [online]. 2023. [cit. 2023-07-26]. Dostupné z: https://learn.microsoft.com/en-us/windows-server/remote/remote-desktop-services/clients/remote-desktop-supported-config.

43. *Xrdp* [online]. [cit. 2023-07-27]. Dostupné z: https://www.xrdp.org/.

44. *Welcome to Remote Desktop Services* [online]. 2021. [cit. 2023-09-05]. Dostupné z: https://learn.microsoft.com/en-us/windows-server/remote/remote-desktop-services/welcome-to-rds.

45. *What is RDP? Remote Desktop Protocol Explained* [online]. 2021. [cit. 2023-07-14]. Dostupné z: https://www.twingate.com/blog/what-is-rdp.

46. *Why you need to disable UDP for RDP connections to Windows Server* [online]. 2023. [cit. 2024-04-30]. Dostupné z: https://zomro.com/blog/faq/427-otklyuchenie-udp-dlya-rdp-podklyuchenij-k-windows-server.

47. *All you need to know about VNC remote access technology* [online]. [cit. 2023-09-14]. Dostupné z: https://discover.realvnc.com/what-is-vnc-remote-access-technology.

48. SUTHERLAND, Richard. *What is VNC?* [online]. 2022. [cit. 2023-09-14]. Dostupné z: https://www.itpro.com/mobile/remote-access/368108/what-is-vnc.

49. *Chapter 11. Remotely accessing the desktop as multiple users* [online]. [cit. 2023-09-14]. Dostupné z: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html/getting_started_with_the_gnome_desktop_environment/remotely-accessing-the-desktop-as-multiple-users_getting-started-with-the-gnome-desktop-environment.

50. *Technical overview* [online]. 2023. [cit. 2023-09-15]. Dostupné z: https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/technical-overview.

51. ARAKELIAN, Caroline. *VMware Blast Extreme Display Protocol in VMware Horizon* [online]. 2020. [cit. 2023-09-14]. Dostupné z: https://techzone.vmware.com/resource/blast-extreme-display-protocol-vmware-horizon-7%5C#blast-extreme-benefits.

52. *SPICE* [online]. [cit. 2024-02-27]. Dostupné z: https://spice-space.org/.

53. GILLIS, Alexander S. *Thin client (lean client)* [online]. 2021. [cit. 2023-09-15]. Dostupné z: https://www.techtarget.com/searchnetworking/definition/thin-client.

54. *What is a Thin Client?* [online]. [cit. 2023-09-15]. Dostupné z: https://www.stratodesk.com/what-is-a-thin-client/.

55. *Thin Clients* [online]. [cit. 2024-02-22]. Dostupné z: https://www.dell.com/en-us/shop/wyse-endpoints-and-software/sc/cloud-client.

56. *Dell ThinOS* [online]. 2023. [cit. 2024-02-24]. Dostupné z: https://www.delltechnologies.com/asset/en-us/products/thin-clients/technical-support/dell-thinos-spec-sheet.pdf.external?ref=cpcl_thinos-item-050_cta_secondaryv2_learnmore.

57. *Dell thin clients with Windows 10 IoT Enterprise* [online]. 2023. [cit. 2024-02-24]. Dostupné z: https://www.delltechnologies.com/asset/en-us/products/thin-clients/technical-support/dell-windows-10iote-spec-sheet.pdf.external.

58. *Wyse Management Suite* [online]. [cit. 2024-02-24]. Dostupné z: https://www.dell.com/en-us/lp/wyse-management-suite.

59. *OptiPlex 3000 Thin Client* [online]. 2024. [cit. 2024-02-24]. Dostupné z: https://www.dell.com/en-us/shop/wyse-endpoints-and-software/optiplex-3000-thin-client/spd/optiplex-3000-thin-client/s005o3000tcus?redirectTo=SOC.

60. *HP Thin Clients* [online]. 2024. [cit. 2024-02-24]. Dostupné z: https://www.hp.com/us-en/thin-clients.html.

61. *HP Thin Clients Operating Systems* [online]. [cit. 2024-02-24]. Dostupné z: https://www.hp.com/us-en/solutions/cloud-computing/thin-client-operating-systems.html.

62. *HP Thin Client Software* [online]. [cit. 2024-02-24]. Dostupné z: https://www.hp.com/us-en/solutions/cloud-computing/thin-client-software.html.

63. *Fujitsu FUTRO Thin Clients* [online]. 2024. [cit. 2024-02-24]. Dostupné z: https://www.fujitsu.com/global/products/computing/pc/thin-clients/.

64. *Unicon* [online]. 2024. [cit. 2024-02-24]. Dostupné z: https://www.unicon.com/.

65. *Fujitsu confirms end to European client PC sales* [online]. 2023. [cit. 2024-04-30]. Dostupné z: https://www.techradar.com/pro/fujitsu-confirms-end-to-european-client-pc-sales.

66. *Ncomputing* [online]. [cit. 2023-10-18]. Dostupné z: https://www.ncomputing.com/.

67. *Thin Client Computers* [online]. 2024. [cit. 2024-02-24]. Dostupné z: https://clearcube.com/products/thin-clients/.

68. *Linux VDI* [online]. 2024. [cit. 2024-02-28]. Dostupné z: https://www.eginnovations.com/glossary/linux-vdi.

69. *Linux Terminal Server Project* [online]. 2023. [cit. 2024-02-29]. Dostupné z: https://ltsp.org/.

70. KOLOUCH, Jan; BAŠTA, Pavel. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o., 2019. ISBN 978-80--88168-34-8.

71. *IDS/IPS: Ochrana sítě před hrozbami a útoky* [online]. 2021. [cit. 2024-04-30]. Dostupné z: https://www.mydreams.cz/cz/wiki/290-ids-ips-ochrana-site-pred-hrozbami-a-utoky.html.

72. *Standard konektivity a bezpečnosti škol* [online]. 2022. [cit. 2024-04-30]. Dostupné z: https://www.edu.cz/digitalizujeme/standard-konektivity-skol/.

73. *ThinLinX Pty Ltd* [online]. 2024. [cit. 2024-04-01]. Dostupné z: https://thinlinx.com/.

74. *Wtware* [online]. 2024. [cit. 2024-04-01]. Dostupné z: https://wtware.com/.

75. *Openthinclient* [online]. 2022. [cit. 2024-04-01]. Dostupné z: https://openthinclient.com/en/.

76. *Porteus Kios* [online]. 2024. [cit. 2024-04-01]. Dostupné z: https://porteus-kiosk.org/index.html.

77. *Xtc Linux Thin Client Project* [online]. 2024. [cit. 2024-04-01]. Dostupné z: https://vmfree.org/xtc/xtcen.html.

78. *Automatic Virtual Machine Activation in Windows Server* [online]. 2024. [cit. 2024-05-01]. Dostupné z: https://learn.microsoft.com/en-us/windows-server/get-started/automatic-vm-activation?tabs=server2025.

79. *Dell Optiplex 7010 Micro MFF* [online]. 2024. [cit. 2024-04-11]. Dostupné z: https://www.alza.cz/dell-optiplex-7010-micro-mff-d7977756.htm?o=2%5C#description.

80. *Dell OptiPlex Micro Plus 7010 review: Desktop Core i7-13700 in a mini PC package* [online]. 2023. [cit. 2024-04-12]. Dostupné z: https://www.notebookcheck.net/Dell-OptiPlex-Micro-Plus-7010-review-Desktop-Core-i7-13700-in-a-mini-PC-package.760579.0.html.