Univerzita Pardubice
Fakulta elektrotechniky a informatiky

Využití distribuce RHEL9 pro výuku počítačových sítí

Petr Jiruše

Bakalářská práce

2023

Univerzita Pardubice
Fakulta elektrotechniky a informatiky
Akademický rok: 2022/2023

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Petr Jiruše**
Osobní číslo:	**I19100**
Studijní program:	**B2646 Informační technologie**
Studijní obor:	**Informační technologie**
Téma práce:	**Využití distribuce RHEL9 pro výuku počítačových sítí**
Zadávající katedra:	**Katedra informačních technologií**

Zásady pro vypracování

Cílem bakalářské práce je vytvoření manuálu pro využití distribuce RHEL9 pro výuku počítačových sítí. V teoretické části práce budou popsána distribuce, jednotlivé síťové služby a protokoly. V praktické části práce bude vytvořena s použitím virtualizovaného prostředí síťová laboratoř včetně ukázkových úloh.

Rozsah pracovní zprávy: **min. 30stran**
Rozsah grafických prací:
Forma zpracování bakalářské práce: **tištěná**

Seznam doporučené literatury:

MCCARTY, Bill. *Učíme se RedHat Linux: průvodce začátečníka operačním systémem Red Hat Linux.* Praha: Computer Press, 2000. ISBN 80-7226-277-7.

JANG, Michael a Alessandro ORSARIA. *RHCSA/RHCE Red Hat Linux Certification Study Guide: Seventh Edition (Exams EX200 & EX300) (RHCSA/RHCE Red Hat Enterprise Linux Certification Study Guide).* 7th. April 7, 2016. ISBN 978-0071841962.

PETERSEN, Richard. *Red Hat Enterprise Linux 8.* surfing turtle press, 2019. ISBN 1949857077.

Vedoucí bakalářské práce: **Ing. Miroslav Dvořák, Dipl.tech.**
Katedra informačních technologií

Datum zadání bakalářské práce: **16. prosince 2022**
Termín odevzdání bakalářské práce: **12. května 2023**

L.S.

Ing. Zdeněk Němec, Ph.D. v.r.
děkan

Ing. Jan Panuš, Ph.D. v.r.
vedoucí katedry

V Pardubicích dne 28. února 2023

Prohlašuji:

Tuto práci jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice 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 Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 9/2012, bude práce zveřejněna v Univerzitní knihovně a prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 15. 4. 2023

Petr Jiruše

PODĚKOVÁNÍ

Rád bych poděkoval vedoucímu práce, Ing. Miroslavu Dvořákovi, Dipl.tech., za cenné rady a připomínky v průběhu zpracování této práce, dále za jeho velmi ochotný přístup a zodpovězení všech mých dotazů k práci.

ANOTACE

Tato práce se zabývá tématem využití distribuce Red Hat Enterprise Linux a dalších od ní odvozených pro výuku počítačových sítí. Znázorňuje a popisuje technologie používané v počítačových sítích aplikované v prostředí distribucí založených na Red Hat Enterprise Linux. Jejím cílem je prezentovat nastavení a provoz služeb přes lokální síť a poskytnout tak návod pro konfiguraci těchto služeb. Práce porovnává jednotlivé distribuce vycházející z Red Hat Enterprise Linux a snaží se čtenářovi přiblížit jejich silné a slabé stránky. Následná implementace a testování služeb probíhá ve virtualizovaném prostředí na počítačích, které používají ke své funkci operační systém Rocky Linux.

KLÍČOVÁ SLOVA

Linux, Red Hat Enterprise Linux, Rocky Linux, virtualizované prostředí, firewall, DHCP, DNS, FTP, Apache, konfigurace služeb, server

TITLE

Using the RHEL9 distribution for teaching computer networks

ANNOTATION

This thesis deals with the topic of using the Red Hat Enterprise Linux distribution and others derived from it for teaching computer networks. Illustrates and describes the technologies used in computer networks applied in the environment of distributions based on Red Hat Enterprise Linux. Its goal is to present the setting and operation of services over the local network and thus provide instructions for the configuration of these services. The work compares individual distributions based on Red Hat Enterprise Linux and tries to bring the reader closer to their strengths and weaknesses. Subsequent implementation and testing of services takes place in a virtualized environment on computers, which uses for its function operating system Rocky Linux.

KEYWORDS

Linux, Red Hat Enterprise Linux, Rocky Linux, virtualized environment, firewall, DHCP, DNS, FTP, Apache, configuration of services, server

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM ZKRATEK

BOOTP	Bootstrap Protocol
CPU	Central Processing Unit
CRB	Code Ready Builder
CSR	Certificate Signing Request
DAC	Discretionary Access Control
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DVD	Digital Versatile Disc
FTP	File Transfer Protocol
GID	Group Identifier
GPG	GNU Privacy Guard
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IDE	Integrated Development Environment
IP	Internet Protocol
MAC	Mandatory Access Control
NAT	Network Address Translation
NFS	Network File System
NSA	National Security Agency
OCI	Oracle Cloud Infrastructure
PAM	Pluggable Authentication Modules
PID	Process Identification
PTR	Pointer Record
RHEL	Red Hat Enterprise Linux
SCSI	Small Computer System Interface
SDK	Software Development Kit
SELinux	Security-Enhanced Linux
SEV	Secure Encrypted Virtualization
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

UID	User Identifier
URL	Uniform Resource Locator
USB	Universal Serial Bus
VDI	VirtualBox Disc
VHD	Virtual Hard Disc
VMDK	Virtual Machine Disc File
VMPlayer	VMware Workstation Player
vsftpd	Very Secure FTP Daemon

ÚVOD

Při dnešním tempu vývoje počítačových sítí a operačních systémů se může klást otázka, jaké operační systémy či jejich distribuce se nejvíce hodí pro výuku technologií používaných v počítačových sítích. Výběr operačního systému pro výuku je důležitý, protože spravuje aplikace, funkce, hardware a poskytuje rozhraní pro interakci s těmito komponenty. Proto je výběr vhodného operačního systému zásadní pro zajištění vhodného prostředí, kde se studenti mohou efektivně učit a porozumět síťovým konceptům. Různé systémy se mezi sebou odlišují svými specifikacemi, funkcemi nebo uživatelskou náročností. Právě uživatelská náročnost a efektivní práce se síťovými službami jsou jedny z hlavních faktorů při výběru vhodného operačního systému pro výuku témat počítačových sítí.

Operační systém Red Hat Enterprise Linux (RHEL) je díky své robustnosti a bezpečnostním funkcím využíván velkými firmami jako základní systém pro jejich servery a další kritickou infrastrukturu. RHEL je především zaměřen na nasazení ve firmách, ale díky své vyspělosti na poli správy serverů a široké nabídce nástrojů umožňující efektivní práci se síťovými službami, je tato distribuce vhodným kandidátem pro výuku síťových technologií ve školách. Přestože RHEL je velmi inovovaná distribuce, stále poskytuje přehledné grafické rozhraní, které se výrazně neliší od jiných linuxových distribucí. Hlavním cílem této práce je demonstrovat konfiguraci a práci s jednotlivými síťovými službami na operačním systému provozující distribuci, která vychází z RHEL v prostředí lokální síťové laboratoře. Konfigurace jednotlivých služeb probíhá formou návodu, a ten by měl nastínit efektivitu a obtížnost práce při používání distribuce RHEL jako nástroje pro výuku.

Jelikož se práce se zaměřuje na distribuci RHEL a její deriváty, je hned v první kapitole zmíněno, jak se daná distribuce instaluje, a kde stáhnout potřebné ISO soubory. Společně s instalací kapitola vysvětluje také licenční politiku a koncept předplatného na RHEL pro získání podpory. Dále v druhé kapitole probíhá seznámení s virtualizačním nástrojem, který se používá v praktické části pro demonstraci nastavování síťových služeb. Třetí kapitola popisuje fungování virtuální sítě a v jakých režimech může virtuální síť pracovat. Ve čtvrté kapitole jsou zmíněny distribuce vycházející z distribuce RHEL, včetně samotné distribuce RHEL. Kromě toho jsou popsány hlavní rysy jednotlivých distribucí, zmíněné jsou také výhody a nevýhody těchto distribucí. Pátá kapitola se zabývá vysvětlením základní konfigurace systému. Jedná se hlavně o věci při prvotním spuštění, správě uživatelů na systému, řízení služeb pomocí dostupných nástrojů a je zde také popsán bezpečnostní systém Security Enhanced Linux neboli SELinux. Kapitola číslo šest popisuje teoreticky služby používané v počítačových sítích

a poskytuje informační základ pro kapitolu zabývající se implementací daných služeb. Sedmá kapitola vysvětluje vytvoření virtuální síťové laboratoře, ve které se budou implementovat síťové služby. Popisuje zapojení virtuálních počítačů, společně s dalšími síťovými prostředky a řeší, jak jsou jednotlivá síťová rozhraní nastavena. V poslední kapitole je řešena samotná implementace služeb nad distribucí Rocky Linux. Každá služba je zde ještě více vysvětlena: jak komunikuje, jaký používá protokol, návod na její konfiguraci, až po testování dané služby. Zmíněna je zde také služba Cockpit, která slouží pro správu serveru z webového rozhraní, a softwarový nástroj Wireshark, který je použit pro další testování služeb pomocí zachytávání jejich paketů.

1 DISTRIBUCE RED HAT ENTERPRISE LINUX

Red Hat Enterprise Linux, zkráceně RHEL je linuxová distribuce, vyvíjená společností Red Hat, určená pro firemní nasazení. Distribuce je založena na bezplatném modelu s otevřeným zdrojovým kódem jako všechny distribuce Linuxu. RHEL poskytuje uživatelům konzistentní a spolehlivý základ napříč prostředími. Obsahuje funkce pro rychlé poskytování aplikačních služeb a vysoké zabezpečení, které zahrnuje vestavěné bezpečnostní funkce, jako jsou oprava jádra za běhu, bezpečnostní profily, certifikace bezpečnostních standardů a důvěryhodný dodavatelský řetězec softwaru. Nabízí rozsáhlý ekosystém, který uživatelům pomáhá vytvářet a nasazovat aplikace v cloudu. Vytváření aplikací na RHEL umožňuje spravovat tyto aplikace napříč infrastrukturou pomocí stejných nástrojů na různých místech. RHEL lze optimalizovat pro nasazení na serverech a vysoce výkonných pracovních stanicích. Podporuje řadu hardwarových architektur jako jsou x86, x86-64, ARM, IBM Power, IBM Z, IBM Linuxone. [1], [2]

Jednotlivé verze RHEL poskytují deset let plné podpory, po které následuje prodloužená životní fáze obsažená v doplňkovém předplatném. Nové verze RHEL jsou vydávány v průměru každé dva až tři roky. RHEL poskytuje nástroje pro migraci dat z jiných verzí nebo jiných distribucí. Verze jsou detailně popsány v dokumentacích na oficiálních stránkách společnosti Red Hat. Popisují věci od běžného ovládání systémů až po speciální administrátorské postupy. [3]

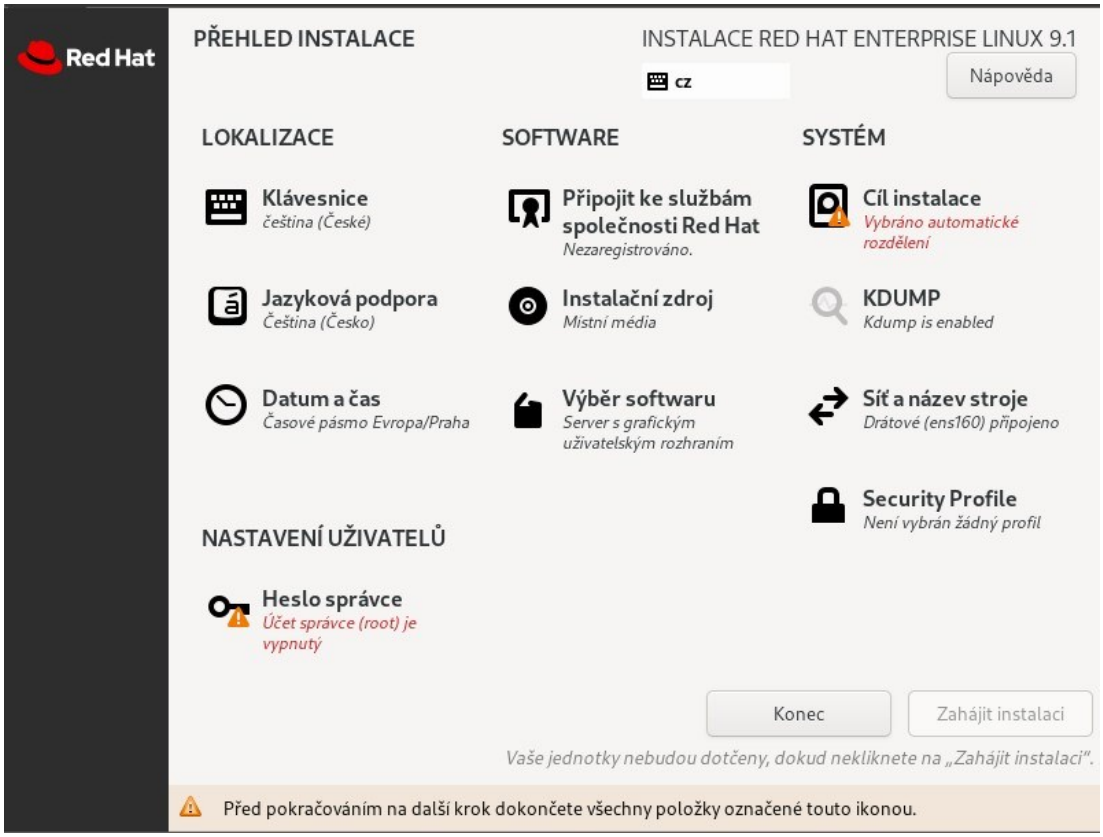
1.1 Instalace

Distribuci RHEL9 lze nainstalovat několika způsoby. Instalace pomocí uživatelského rozhraní, které se následně dělí do dalších podskupin, systémové nebo cloudové instalace a pokročilé instalace, do kterých patří například instalace s využitím automatizovaného procesu Kickstart. V této práci bude vysvětlen postup instalace za použití uživatelského rozhraní společně s ISO souborem, obsahující obraz RHEL9.

Potřebné ISO soubory lze stáhnout z následujícího odkazu: https://developers.redhat.com/products/rhel/download. Na výběr je Boot ISO (minimální instalace) a DVD ISO (standardní instalace). V případě instalace na reálný systém, nikoliv virtuální je nutné vytvořit instalační médium. Při prvotním spuštění instalační program nabízí několik možností. Pokud do 60 sekund není zvolena žádná z položek, instalační program automaticky vybere výchozí možnost. První a nejčastější možnost spustí grafické rozhraní,

pomocí kterého se v krocích provede instalace operačního systému. Zbylé dvě možnosti slouží pro kontrolu integrity instalačního média nebo řešení problémů spojených s instalací.

Po spuštění grafického rozhraní je uživatel vyzván vybrat jazyk, ve kterém bude instalace i samotný operační systém probíhat. Následně se uživatel dostane do souhrnu instalace, kde najde konfiguraci základních nastavení.



Obrázek č. 1 - Instalační souhrn RHEL9 (zdroj vlastní)

Některé položky konfigurace jsou povinné a bez nich nelze instalaci dokončit. Povinné položky jsou označeny oranžovým varovným symbolem. Mezi požadované položky konfigurace patří nastavení diskového média, na které bude daný operační systém nainstalován. Dále je nutné nastavit heslo pro správce (roota). Vhodné je i vybrat síť, ke které se má počítač připojit. V záložce „Síť název stroje“ ze seznamu uživatel vybere požadovanou síť, pokud jsou dostupné. Volitelně lze vytvořit nové uživatele a jejich hesla, případně jim přidělit práva správce. Dále uživatel může zvolit jakou podobu bude mít cílová instalace. Ve výchozím stavu je vybrána možnost instalace serveru s grafickým uživatelským rozhraním. Po nastavení všeho potřebného je možné spustit instalaci, která v průměru zabere několik minut. [4]

1.2 Registrace

Důležitým krokem po instalaci systému je jeho registrace k předplatnému. Předplatné slouží k získání určitému stupni podpory a hlavně uživatel získá přístup k důležitým aktualizacím systému. Pro registraci v příkazovém řádku uživatel zadá příkaz:

```
# subscription-manager register --username [username] --password [password]
```

Předpoklady pro úspěšné provedení předchozího příkazu, a tudíž úspěšné registrace systému, závisí na několika věcech. Uživatel má aktivní Red Hat Enterprise Linux předplatné. Status uživatelova předplatného je ověřený. Účet uživatele spadá pod nějakou organizaci. Na provedení příkazu k registraci jsou potřeba práva správce. Pokud jsou splněny všechny podmínky, proběhne úspěšná registrace a do příkazového řádku je vypsán identifikátor systému, společně s názvem domény. V dalším kroku uživatel nastaví roli pro systém. Dostupné role závisí na stupni předplatného a architektuře nainstalovaného systému. Dále uživatel zadá úroveň údržby systému. Možné stupně údržby jsou: vlastní, standardní a prémiový. Jako poslední uživatel zvolí účel daného systému. Možnosti využití také závisí na úrovni předplatného. Po nastavení všech nezbytností uživatel připojí systém k oprávněním, která odpovídají architektuře daného systému. Po úspěšné připojení předplatného se zobrazí status produktu. Alternativní způsob registrace předplatného je přihlášení se do systému jako správce a v nastavení pod záložkou „O systému“ nastavit registraci pomocí grafického rozhraní. [4], [5]

1.3 Licenční politika

Uživatel má možnost zakoupit produkty Red Hat přímo od samotné společnosti, pomocí vyplnění objednávkového formuláře na oficiálních internetových stránkách společnosti nebo jiných obchodních partnerů. Potvrzením objednávkového formuláře uživatel souhlasí se všeobecnými podmínkami a dalšími možnými podrobnostmi týkající se transakce. [6]

Dohoda mezi uživatelem a poskytovatelem produktu má tři části:

1. Všeobecné podmínky
2. Dodatky k produktu (může zahrnovat koncového uživatele)
3. Objednávkové formuláře

Produkty, jakožto předplatné, musí být zakoupené pro každý systém v organizaci, včetně virtuálních strojů, kde je nainstalován systém Red Hat Enterprise Linux. Předplatné lze migrovat z jednoho systému na druhý za předpokladu, že druhý systém má podobné vlastnosti a celkový počet předplatných stále odpovídá množství nainstalovaných systémů. Uživatel může migrovat Red Hat Enterprise Linux Server a související doplňková předplatná mezi fyzickými, virtuálními i cloudovými nasazeními, aniž by musel měnit podmínky, kupovat další předplatné nebo informovat společnost Red Hat. Předplatné Red Hat Enterprise Linux Serveru nesmí být migrováno mimo pracoviště, aniž by k tomu uživatel získal písemné povolení od společnosti Red Hat. Produkty a služby musí být používány v souladu se zákaznickou smlouvou a obsah společnosti Red Hat nesmí být měněn. Rovněž nesmí být kopírován. Obsah Red Hat podléhá všem platným zákonům a předpisům a uživatel používáním tohoto obsahu souhlasí s tím, že tyto nařízení nebude porušovat. Jakýkoliv pokus o poškození portálu Red Hat nebo obsahu Red Hat znamená porušení trestního a občanského práva. Společnost Red Hat si vyhrazuje právo požadovat od takové osoby náhradu škody v maximálním rozsahu povoleném zákonem. [6], [7]

Samotné předplatné poskytuje podporu s instalací, diagnostikou problémů a opravami chyb. Zahrnuje také poradenství v oblasti architektury, designu, vývoje a prototypování aplikací. Produkční podpora zahrnuje pomoc s testováním aplikací, jejich používání, diagnostikou problémů a opravou chyb softwaru určenému pro produkční účely. Tato podpora nezahrnuje pomoc s vývojem kódu, návrhem systému, návrhem sítě nebo implementací bezpečnostních pravidel. [7]

Předplatné může být zakoupeno s různými úrovněmi podpory. Například pro stroje vykonávající kritické úlohy je určeno předplatné se službami podpory Premium, zatímco pro ostatní stroje vykonávající běžné úlohy stačí úroveň podpory Standard. Organizace však nemůže na stroji s přiřazeným Standard předplatným využívat vyšší úroveň podpory, i když na jiném stroji má vyšší úroveň předplatného zaplaceno. Tudíž každý stroj může využívat pouze danou úroveň podpory, jaká mu byla přiřazena úrovní předplatného. Předplatné lze používat i ve zkušební verzi. Tato verze smí být používána pouze v omezeném režimu tak, jak je výslovně definováno v podmínkách použití. Předplatné softwaru slouží pouze pro interní použití, včetně přidružených organizací. Nelze převést na osoby nebo organizace třetích stran a nesmí se používat pro účely, pro které nebylo určeno. Například nelze použít předplatné Red Hat Enterprise Linux Workstation jako produkční server nebo nelze vyhledat produkční podporu pomocí vývojářského předplatného. [7]

Výjimka je předplatné pro developerské účely. To je zdarma pro jednotlivé vývojáře a je dostupné prostřednictvím programu Red Hat Developer. Bezplatné předplatné zahrnuje Red Hat Enterprise Linux spolu s dalšími technologiemi od společnosti Red Hat, jako je například Red Hat Enterprise Linux Server, nástroje a kompilátory Red Hat Developer nebo četné doplňky infrastruktury pro Red Hat Enterprise Linux. [8]

Společnost Red Hat umožňuje uživatelům spravovat jejich předplatná pomocí zákaznického portálu Red Hat. Zde lze spravovat fyzické nebo virtuální systémy, procházet jejich dokumentaci nebo získat nejnovější verzi softwaru. Další možností správy předplatných je služba Red Hat Satelite, která je součástí samostatného předplatného Red Hat Smart Management. Red Hat Smart Management poskytuje správu oprav, správu konfigurace a zajišťuje bezpečné fungování systémů Red Hat Enterprise Linux. Pomáhá také spravovat seznam předplatných poskytováním podrobných zpráv o dostupných předplatných a jejich termínech expirace. [7]

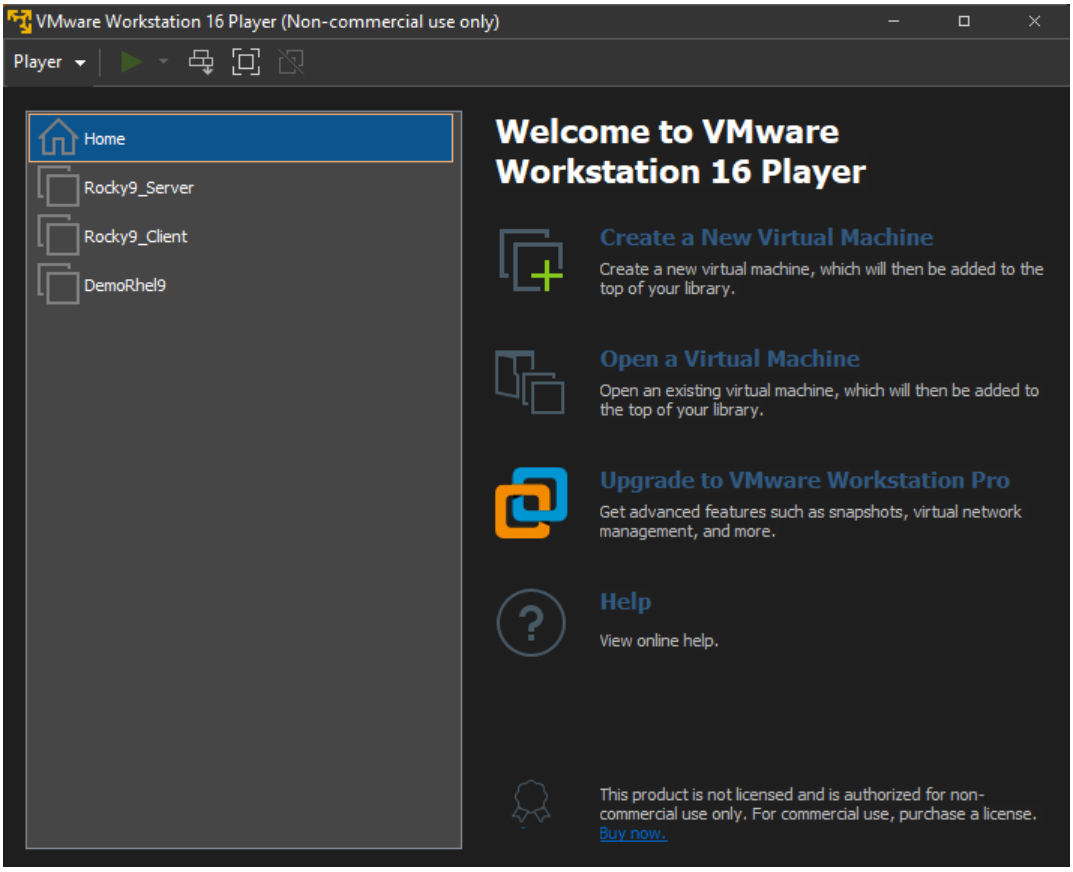
Předplatná jsou platná na omezenou dobu podle smlouvy, kterou organizace uzavřela se společností Red Hat. Předplatné jsou ve většině případu na rok a musí se vždy obnovit, aby organizace mohla čerpat výhody, které dané předplatné přináší. Organizace obdrží email 90, 60 a 30 dní před vypršením předplatného s upozorněním na obnovení předplatného. Upozornění obsahuje datum vypršení smlouvy a potřebné kroky k jejímu obnovení. Způsob obnovení závisí na typu zakoupeného předplatného. [7]

2 POPIS POUŽITÉHO VIRTUALIZAČNÍHO PROSTŘEDÍ

Za virtualizační prostředí pro vytvoření virtuálních počítačů bylo zvoleno prostředí VMPlayer. V této kapitole jsou popsány jeho rysy a funkce, které nabízí. Dále je zde popsána jeho alternativa VirtualBox a srovnání obou nástrojů. Ke konci kapitoly jsou popsána síťová rozhraní virtualizačního prostředí VMPlayer.

2.1 VMPlayer

VMPlayer je bezplatná desktopová aplikace, která umožňuje spouštět virtuální stroje na počítačích se systémem Windows nebo Linux. VMware Player poskytuje intuitivní uživatelské rozhraní pro spouštění předem konfigurovaných systémů, vytvořených s pomocí VMware Workstation, ESX Server, VMware Server nebo GSX Server. Na hostitelských systémech s operačním systémem Windows, VMware spouští služby Microsoft Virtual PC, Virtual Server a obrazy systému Symantec Backup Exec System Recorvery. VMware Player umožňuje přístup ostatních uživatelů k virtuálním strojům bez ohledu na to, zda mají zakoupené produkty VMware nebo ne. [9]



Obrázek č. 2 - Ukázka rozhraní VMPlayer (zdroj vlastní)

VMware Player nabízí spouštění předem sestavených aplikací bezpečně v prostředí virtuálních strojů. Na internetových stránkách Virtual Appliance Marketplace jsou k dispozici virtuální stroje od předních dodavatelů softwaru, jako jsou Oracle, Red Hat, IBM, MySQL a Novell, které lze využívat pro spouštění předem sestavených aplikací. Touto cestou lze zjednodušit distribuci softwaru ke koncovým zákazníkům pomocí předem nakonfigurovaného softwaru bez nutnosti nic nastavovat. [9]

Ve virtuálních strojích lze připojovat a odpojovat hostitelská zařízení, včetně USB zařízení. Samozřejmostí je přidělování operační a diskové paměti virtuálním strojům. Soubory z hostitelského zařízení jdou přesunovat do virtuálního stroje a naopak. Tato funkce je dostupná, pokud uživatel, který vytvořil daný virtuální stroj do něj nainstaloval VMware Tools. Další funkce obsažená ve VMware Tools je kopírování textu mezi hostem a hostitelským strojem. VMware Player může spustit více než jeden virtuální stroj v jeden čas. Počet běžících virtuálních strojů v jeden čas je omezen hardwarovými prostředky hostitelského systému, především pamětí. [9]

2.2 Alternativa – VirtualBox

VirtualBox je multiplatformní virtualizační software. Umožňuje rozšiřovat stávající provoz počítače o provoz vícero operačních systémů včetně Microsoft Windows, Mac OS X, Linux a Oracle Solaris. VirtualBox vyžaduje instalaci existujícího operačního sytému a funguje tak vedle aplikací nacházejících na tomto hostiteli. VirtualBox je navržený pro testování, vývoj, předvádění a řešení problémů na více platformách z jediného stroje. VirtualBox může na jednom počítači provozovat několik virtuálních strojů najednou, každý s vlastním operačním systémem a zároveň sdílet fyzické prostředky poskytované hostujícím hardwarem. Dokáže spustit jakékoliv typy aplikací na existujícím systému. Jsou dostupné doplňky pro hosta ve formě sdílených složek s virtuálním strojem nebo 3D virtualizace. Doplňky pro hosta jsou softwarové balíčky, které lze nainstalovat pro lepší integraci a komunikaci s hostitelským systémem. [10], [11]

Mezi hlavní funkce VirtualBoxu patří hostující multiprocesing. Tato funkce umožňuje provozovat až 32 virtuálních CPU bez ohledu na to, kolik jader CPU je fyzicky přítomno na hostiteli. VirtualBox implementuje virtuální USB řadič, který umožní připojení libovolného USB zařízení k virtuálním strojům, aniž by bylo potřeba instalovat ovladače pro konkrétní zařízení. VirtualBox poskytuje hardwarovou kompatibilitu, která zahrnuje řadiče pevných

disků IDE, SCSI a SATA, dále několik virtuálních a zvukových karet, virtuální sériové a paralelní porty nacházející se v mnoha počítačových systémech. Nachází se zde také podpora dovolující mnohokrát vyšší rozlišení obrazovky, než je fyzická obrazovka, což umožňuje rozdělení na velký počet individuálních obrazovek připojených k hostitelskému systému. Díky své modulární architektuře může VirtualBox odhalit svou plnou funkčnost a konfigurovatelnost pomocí sady pro vývoj softwaru (SDK), která umožňuje integraci s dalšími softwarovými systémy. [11]

2.3 VMPlayer versus VirtualBox

Oba virtualizační nástroje spadají do kategorie hostovaných hypervizorů, které jsou nainstalovány nad hostitelským systémem. Oba podporují hardwarovou virtualizaci, která emuluje hardware hostitelského stroje a pomáhá zlepšit výkon virtuálního stroje pomocí spouštění kódů napřímo. Hlavním rozdílem je podpora softwarové virtualizace ze strany VirtualBoxu, zatímco VMPlayer tuto funkci nepodporuje. Softwarová virtualizace emuluje kompletní hostitelský operační systém a vytváří hosta na něm, to umožňuje spouštět systémy s jinou platformou, než jakou má host. Oba nástroje fungují na platformách Linux a Microsoft Windows. VirtualBox pak dodatečně podporuje Solaris, macOS a FreeSBD. Pro virtualizaci oba nástroje podporují všechny zmíněné systémy s výjimkou macOS u VMPlayer, kde je potřeba použít VMware Fusion namísto VMPlayer. Snímkování virtuálního počítače je funkce, která ukládá momentální stav stroje pro potřeby znovu načíst daný stav později. VirtualBox tuto funkci obsahuje již v základu, zatímco VMPlayer ne a je obsažena až v placených verzích VMware jako je VMware Workstation Pro. VirtualBox nabízí formáty virtuálních disků jako jsou VDI, VMDK a VHD. VMPlayer používá pouze formát VMDK, který byl přímo vyvinut společností VMware. V oblasti připojení zařízení USB je výhodnější VMPlayer, který v základu podporuje použití jednoho nebo dvou zařízení USB a má povolený port USB ve výchozím nastavením. Podpora verzí USB je 2.0 a 3.0 s částečnou závislostí na hostitelském systému. VirtualBox v základu podporuje pouze USB 1.0 a je potřeba nainstalovat rozšiřující balíček pro podporu USB 2.0 a 3.0. V oblasti 3D grafiky VMPlayer umožňuje využít až 2 GB video paměti a podporuje novější verze knihoven pro ovládání hardwaru, konkrétně DirectX 10 a OpenGL 3.3 pro všechny produkty VMware. VirtualBox si vystačí s video pamětí omezenou na 128 MB a podporou 3D grafiky do Direct3D 9 a OpenGL 3.0. [12]

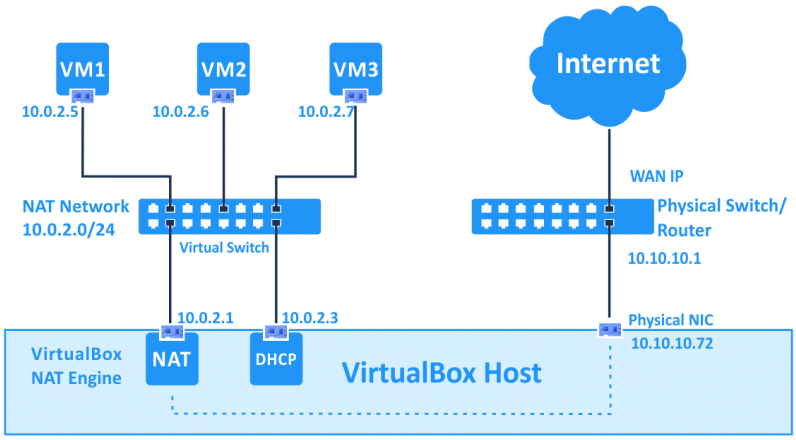
3 SÍŤOVÉ ROZHRANÍ VIRTUÁLNÍHO POČÍTAČE

Virtualizační nástroje jako jsou VMPlayer a VirtualBox umožňují vytvářet virtuální síť pro komunikaci mezi počítači, virtuálními počítači, virtuálními servery a dalšími zařízeními nacházející se v rámci sítě. Používají se virtualizované verze tradičních síťových nástrojů, jako jsou přepínače a síťové adaptéry, které umožňují jednodušší správu sítě. Díky tomu lze ve virtuálním prostředí vytvořit síť se stejnými schopnostmi jako fyzická síť. Tato kapitola se věnuje popisu tří síťových režimů. Prvním je NAT, v tomto režimu hostitelé překládají adresu IP virtuálního počítače směrovači, aby se virtuální počítač mohl připojit k Internetu. Druhým je bridge, který umožňuje sdílet síť s virtuálními počítači a všemi fyzickými počítači ve fyzické síti. Posledním režimem je síť pouze pro hostitele, ta umožňuje vzájemné spojení mezi hostitelským počítačem a virtuálními počítači, zatímco jsou odříznuti od fyzické sítě. [13]

3.1 NAT (Network Address Translation)

Nastavením síťového adaptéru na NAT virtuální stroj nemá přidělenou vlastní adresu IP na externí síti. Na místo toho je vytvořena oddělená privátní síť na hostitelském stroji. Ve výchozím nastavením dostane virtuální stroj adresu od serveru DHCP, směřující do této privátní sítě. Virtuální stroj a hostující systém sdílí jednu síťovou identitu, která není viditelná na externí síti. Při instalaci VMware Player na hostitelský systém, je síť NAT (VMnet8) již předem nakonfigurována. Když se vytváří nový virtuální stroj pomocí průvodce vytvoření virtuálního stroje a je vybrána standardní konfigurace, průvodce nastaví virtuálnímu stroji používání výchozí sítě NAT. Síť NAT může být pouze jedna. [14]

NAT překládá adresy IP virtuálních strojů v privátní síti na adresy IP hostitelského systému. V případě vyslání požadavku od virtuálního stroje na přístup k síťovému prvku, zobrazí se požadovanému síťové prvku, jako kdyby přicházel od hostitelského systému. Hostitelský systém má v síti NAT virtuální síťový adaptér. Tento adaptér umožňuje komunikaci mezi virtuálním strojem a hostitelským systémem. Zařízení NAT přepošle síťová data jednomu nebo více virtuálním strojům a externí síti, dále identifikuje příchozí pakety určené pro jednotlivé virtuální stroje a pošle je na místo určení. [14]

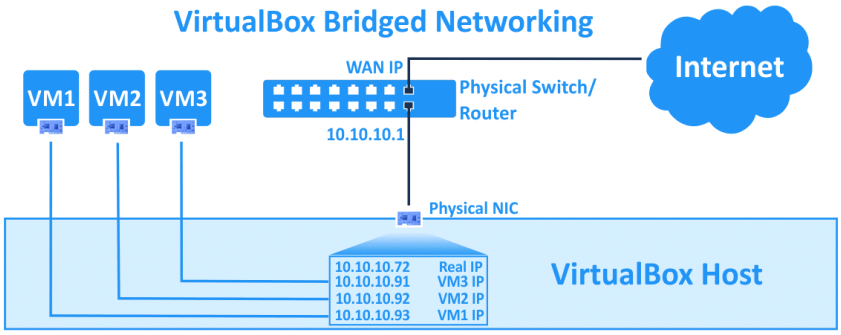


Obrázek č. 3 - Ukázka zapojení sítě s NAT (zdroj [15])

3.2 Bridge

Připojení k síti pomocí mostu probíhá připojením virtuálního počítače k síti pomocí síťového adaptéru na hostitelském systému. Pokud je hostitelský systém v síti, most je v mnoha případech nejrychlejší cesta, jak poskytnout virtuálnímu stroji přístup k této síti. Po instalaci VMware Player je most již připraven k použití pod sítí VMnet0. Při používání přemostěné sítě se virtuální adaptér ve virtuálním stroji připojí k adaptéru fyzické sítě v hostitelském systému. Síť s mostem nastavuje každému virtuálnímu stroji jedinečnou síťovou identitu a odděluje je od síťových prvků hostitelského systému. Virtuální stroj se tak stává plnohodnotným členem dané sítě. Může komunikovat s dalšími virtuálními stroji v síti a ostatní počítače s ním můžou komunikovat, jako kdyby to byl fyzický počítač. V nastavení pro přemostěná spojení lze určit jaké síťové adaptéry budou použity pro použity pro přemostění a zároveň je možné konkrétní síťové adaptéry hostitelského systému mapovat konkrétním virtuálním strojům. [14]

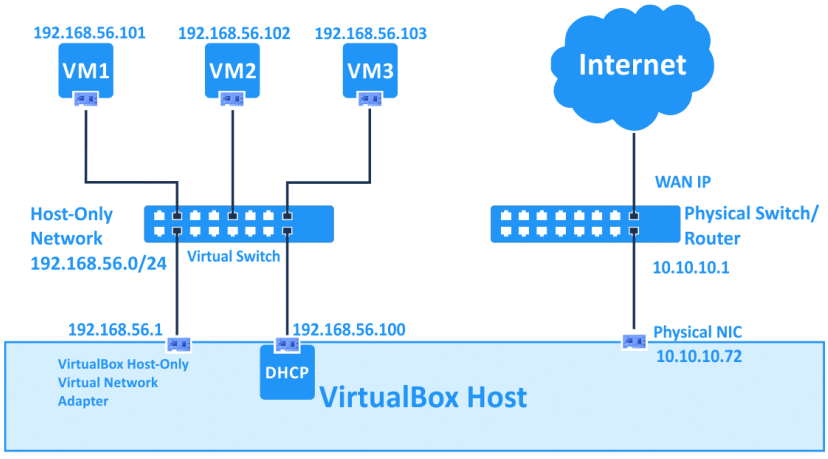
Virtuální stroj musí mít v přemostěné síti svoji vlastní identitu. V sítích TCP/IP je proto zapotřebí, aby každý virtuální stroj měl přiřazenou svoji adresu IP. Správce sítě může určit jaké adresy jsou dostupné pro virtuální stroje a jaká síťová nastavení použít v hostujícím systému. Hostující systém obvykle získává adresy IP a další podrobnosti o síti od serveru DHCP. V ostatních případech musí uživatel hostitelského systému nastavit adresu IP a podrobnosti ručně. Uživatele zavádějící více operačních ve většině případů nastavují všem stejnou adresu IP, jelikož se předpokládá, že bude běžet pouze jeden operační systém v jednu chvíli. Pokud je hostitelský systém nastaven na spouštění více operačních systémů najednou, musí mít každý systém nastavenou unikátní adresu. [14]



Obrázek č. 4 - Ukázka zapojení sítě s mostem (zdroj [15])

3.3 Host-Only Networking

Hostitelská síť vytváří spojení, které je celé obsažené pouze v hostitelském počítači. Tato síť poskytuje síťové propojení mezi virtuálním strojem a hostitelským systémem za použití virtuálního síťového adaptéru, který je viditelný v tomto systému. Ve VMware Player je hostitelská síť nastavena pod sítí VMnet1. Využití hostitelské sítě je vhodné v případě potřeby vytvoření izolované virtuální sítě. V této síti je virtuální stroj a hostitelský síťový adaptér připojen do privátní sítě Ethernet. Celá síť je tak obsažená v rámci hostitelského systému. Připojení mezi virtuálním strojem a hostitelským systémem je zprostředkováno pomocí virtuálního síťového adaptéru, který je viditelný na tomto systému. Na hostitelské síti adresy IP poskytuje virtuální server DHCP. Ve výchozím nastavení nemá virtuální stroj v hostitelské síti přístup k Internetu. Adaptéry virtuálních strojů nemají žádnou konfiguraci brány, tím pádem nemohou přistupovat k žádným jiným zařízením, než je hostitel. [14]



Obrázek č. 5 - Ukázka zapojení sítě pouze s hostem (zdroj [15])

4 SROVNÁNÍ DISTRIBUCÍ

V této části práce jsou porovnány distribuce Linuxu, které jsou založeny na RHEL. Distribuce se liší v některých vlastnostech jako je délka podpory, přístupnost, rozsah funkcí nebo cílový segment uživatelů. I přes odlišnosti všechny distribuce vycházející z RHEL sdílí stejný kód, který je open source. Čísla verzí u odvozených distribucí jsou obvykle totožné s RHEL. Zároveň jsou distribuce binárně kompatibilní s RHEL, což znamená, že obsah určený pro RHEL funguje i na ostatních distribucích. Konkrétní distribuce popsané v této kapitole: RHEL, CentOS, Oracle Linux, Rocky Linux a Alma Linux.

4.1 Red Hat Enterprise Linux 9

Komerční open-source distribuce vyvíjená společností Red Hat. RHEL využívá mnoho velkých společností v USA a má na starosti řešení kritických úkolů ve většině těchto společností. RHEL se dělí na edice Server a Workstation. Server edice dostává každé 3 až 4 roky důležité aktualizace, zvyšující hlavně bezpečnost systému. RHEL přináší vestavěné prvky zabezpečení a škálovatelnou správu systému prostřednictvím rozhraní známé uživatelům Linux i Windows. Zvyšuje zabezpečení pomocí integrovaných ovládacích funkcí, jako je centralizovaná identita řízení a Security-Enhanced Linux (SELinux) s povinným řízením přístupu (MAC). Dostává neustálé aktualizace na bezpečnost systému od týmu Red Hat Product Security, který řeší všechny kritické problémy během krátké doby. Tyto problémy jsou většinou vyřešeny ještě předtím, než se stanou veřejnými. Všechny systémy RHEL v rámci jedné společnosti lze spravovat přes webové rozhraní. Výhodou RHEL je přecházení ze starších verzí softwaru na nové, kde lze migrovat celé stroje a aplikace bez potřeby přestavovat. RHEL nabízí vysokou spolehlivost pro běh kriticky důležitých operací, jeho komponenty jsou neustále testovány a podrobovány testům. Tímto způsobem lze zaručit vysokou spolehlivost při nasazení ve firmách. [16], [17]

RHEL je navržen pro nejnáročnější úlohy v těch největších světových firmách operující v různých oblastech. Pomocí pokročilé komprese dat může systém RHEL snížit náklady na úložiště a zlepšit přístup k datům. S každou další verzí softwaru RHEL získává neustálé zlepšení výkonu, inkrementální aktualizace pro rychlejší spouštění a optimalizaci vysoce výkonné výpočetní techniky. RHEL dává svobodu při navrhování a budování infrastruktury na základě interních potřeb dané společnosti, nezávisle na systémovém hardwaru nebo cloudové

architektuře. Společnost může tak vyvíjet, nasazovat a udržovat své aplikace pomocí svých vlastních nástrojů na infrastruktuře dle jejich výběru. [17]

Nevýhodou RHEL je potřeba předplatného pro stahování a instalaci aktualizací z repositářů na webu společnosti Red Hat. Bez předplatného také nelze využít zákaznické podpory Red Hat, i přes to lze systém RHEL provozovat bezplatně. Uživatel má zdarma přístup ke zdrojovému kódu RHEL, ve kterém není obsaženo logo společnosti Red Hat. Alternativou k bezplatnému provozu jsou další distribuce, které přebírají zdrojový kód RHEL. Jednou z nich je distribuce CentOS, která je softwarově velice podobná distribuci RHEL. [18]

4.2 CentOS

Volně dostupná Linuxová distribuce s otevřeným zdrojovým kódem, která byla odvozena ze zdrojového kódu distribuce Red Hat Enterprise Linux. Tato distribuce přestala být podporována koncem roku 2021 a jeho nástupce měl být CentOS Stream, který však oproti CentOS dostává průběžné aktualizace dříve, než je tomu na distribuci RHEL, a slouží tak jako testovací prostředí, což může způsobit nestabilitu systému. Tudíž CentOS Stream není pro řadu uživatelů plnohodnotnou náhradou za CentOS. Distribuce byla vytvářena komunitou CentOS Project. Poslední verze této distribuce byla CentOS Linux 8 a jejím následníkem byla verze CentOS Stream 8. V dnešní době již verze CentOS Stream 9. [19], [20], [21]

Hlavní výhoda této distribuce spočívala v bezplatném provozu na rozdíl od Red Hat Enterprise Linux a to i přes to, že CentOS Project spolupracoval se společností Red Hat. Přebíral její zdrojový kód, odstraňoval předplatné Red Hat a poskytoval distribuci volně ke stažení. Ačkoliv vycházela z Red Hat Enterprise Linux, nezahrnovala přístup k technické podpoře společnosti Red Hat a její zdrojový kód neobsahoval integraci zákaznické podpory společnosti Red Hat. Zároveň distribuce poskytovala pevný a stabilní kód se zaručenou kvalitou. Poskytovala veškerý zdrojový kód, binární soubory, aktualizace, záplaty, které jsou komunitě volně dostupné. Měla prokazatelnou historii, záznamy stability, podporu komunity a finanční stabilitu. Obsahovala bohatý aplikační ekosystém v kombinaci s okamžitými záplatami v případě objevení zranitelných míst. [18], [22]

Mezi nedostatky distribuce CentOS patřila absence placené podpory, která by řešila rychleji problémy uživatelů. V určitých situacích síť CentOS trpěla na občasné náhodné výpadky této sítě. Oproti RHEL měla distribuce CentOS slabší zabezpečení a pomalejší načítání hotfixů,

aktualizací a záplat. Také mnoho uživatelů požadovalo možnost realtime oprav bez zpomalení serveru či nutnosti restartu celého systému jako volitelnou službu. [22]

4.3 Oracle Linux

Komerční distribuce založená na RHEL. Je určená hlavně pro použití s databázovými produkty společnosti Oracle a obsahuje vysokou úroveň integrace s těmito produkty. Společnost Oracle tuto distribuci využívá k provozu Oracle Cloud a tisíce serverů Oracle. Distribuce Oracle nabízí placenou podporu přímo od společnosti Oracle. Distribuce nabízí vysokou úroveň zabezpečení a přináší sebou alternativu k jádru RHEL známé jako Unbreakable Enterprise Kernel, které obsahuje vylepšení od společnosti Oracle. Uživatelé však mají možnost si ponechat stejné jádro dodávané jako součást RHEL. Jádro lze v Oracle Linux aktualizovat bez nutnosti restartu systému za pomoci funkce pro záplatování za běhu. [23], [24]

Oracle Linux poskytuje širokou škálu funkcí pro snadnou a efektivní manipulaci se systémem. Kompatibilní jádro Oracle Linux umožňuje uživatelům spustit jejich software kompatibilní s RHEL na Oracle Linux bez nutnosti modifikace a využít výhod optimalizace ze strany Oracle Linux. Součástí Oracle Linux je Oracle Ksplice, který detekuje známé formy zneužití systému a umožňuje provádění auditů společně s upozorněním na zranitelnosti. Nabízí také službu Oracle Cloud Native Environment ke konfiguraci, nasazení a aktualizaci infrastruktury pro provoz cloudově nativních aplikací. Oracle Linux také obsahuje virtualizaci pomocí KVM hypervizoru, který podporuje hardwarová rozšíření Intel VT-x a VT-d, dále také šifrovanou virtualizaci (SEV) pro procesory s podporou AMD-V. Oracle Linux podporuje architekturu x86 a servery ARM. Také poskytuje podporu i pro starší verze RHEL a CentOS. Má dvě úrovně placené podpory Basic a Premier. Podpora Oracle Linux Premier je dostupná zdarma pro předplatitele OCI a systémy Oracle Engineered. [22], [25]

Mezi nevýhody se dá zařadit neprůhledná historie podpory Oracle mimo Linux. Oracle Linux v současnosti není podporován hostingovou platformou cPanel. Pokud firma nepoužívá produkty Oracle, tak je pro ni nevýhodné nasazovat distribuci Oracle Linux na firemní počítače. Z důvodu, že Oracle nemůže poskytnout dostatečnou podporu pro zákazníky, kteří používají jinou databázi než od společnosti Oracle. Oracle Linux nebude moct využít svůj plný potenciál, pokud není kombinován s dalšími produkty od společnosti Oracle. [22], [26]

4.4 Rocky Linux

Open-source operační systém pro komerční využití. Založen na Red Hat Enterprise Linux, se kterým je plně kompatibilní. Rocky Linux má nahrazovat distribuci CentOS. Jedná se o nejnovějšího klona distribuce RHEL, který vytvořil Gregory Kurtzer, podílející se mimo jiné i na vytvoření nahrazované distribuce CentOS. U Rocky Linux je soustředěno úsilí, tak aby se jednalo čistě o komunitou řízený projekt. Snažící se dělat to co dělala distribuce CentOS před ním a je postaven na stejné filozofii, tudíž usiluje o to, být nekomerční distribuce bez korporátního vlivu a placené podpory. Výhodou Rocky Linux je plná kompatibilita aplikací s Red Hat Enterprise Linux a CentOS. Do Rocky Linux je možné migrovat data z předchozích systémů pomocí nástroje „migrate2rocky“. Tento skript umožňuje po spuštění změnit všechny uživatelovy repositáře na úložiště Rocky Linux. Balíčky budou podle potřeby instalovány a aktualizovány. Změní se také označení uživatelského systému. Nutno dodat, že je možné migrovat data ze systémů CentOS Stream, CentOS, Alma Linux, RHEL nebo Oracle Linux. U každého z nich jsou momentálně podporované verze 8.7 nebo 9.1. [22], [27]

Nevýhodou Rocky Linux je hlavně absence nových funkcionalit oproti svému předchůdci CentOS. Rocky Linux nemá žádnou přímou podporu. Rocky Linux je stále nová distribuce Linuxu a proto bude trvat dlouho než získá certifikaci vylepšeného zabezpečení. Distribuce Rocky Linux bude vhodná pro ty, kteří hledají bezplatného nástupce distribuce CentOS bez přímé podpory nebo se chtějí podílet na vylepšování této distribuce. Pro firemní využití chybí Rocky Linux historie verzí, výkon, rozšířené funkcionality, vylepšené zabezpečení, intuitivní správa, certifikované aplikace a přenositelnost v cloudu. [22]

4.5 AlmaLinux

Komunitou vlastněná a řízená distribuce Linuxu, která má sloužit jako náhrada za distribuci CentOS. Vyvíjená je společností Alma s podporou investora CloudLinux, který projekt AlmaLinux odstartoval. CloudLinux využívá AlmaLinux jako vlastní verzi distribuce CentOS. Tato distribuce je plně kompatibilní s Red Hat Enterprise Linux. Výhodou AlmaLinux je její absolutní přístupnost, co se týče veškerého zdrojového kódu, binárních souborů, aktualizací a systémových záplat, to vše je zdarma pro uživatele této distribuce. Uživatelé obecně vnímají kód AlmaLinux jako záruku kvality pro jejich potřeby. Migrace z distribuce CentOS je pro uživatele relativně snadná, díky poskytnutému skriptu od společnosti Alma. Distribuce obsahuje vlastní placenou podporu poskytovanou pomocí mateřské služby CloudLinux

TuxCare. Proces vydání záplaty je u AlmaLinux rychlejší než u CentOS, kde proces schvalování trvá dva dny, oproti jednomu dnu v případě AlmaLinux. Uživatelům je nabízeno i placené živé záplatování tak jak jsou vydávány prostřednictvím služby CloudLinux KernelCare. [22]

Nevýhodou této distribuce je chybějící podpora předchozích verzí vydaných před RHEL 8.3. V této distribuci také chybí dodatečné nástroje pro správu, jak v místním prostředí, tak i v cloudu, kde podpora cloudu je v AlmaLinux teprve nově přidána. V prostředí distribuce AlmaLinux může běžet jakákoliv aplikace, která funguje na RHEL, toto však neznamená, že aplikace je certifikována pro běh na AlmaLinux. Nutno zmínit, že finanční podpora ze strany CloudLinux je omezená. [22]

V porovnání s RHEL má AlmaLinux nedostatky v oblasti zabezpečení, které při nasazení ve firemním prostředí mohou způsobovat zranitelnosti a být velkým problémem pro společnosti snažící se zvýšit odolnost proti útokům ransomwarem. V tomto ohledu pomáhá služba KernelCare, která dokáže implementovat opravy zranitelností do jednoho dne. Avšak nedělá nic navíc pro řešení hlavních bezpečnostních nedostatků. Kromě nedostatečného zabezpečení se AlmaLinux potýká také s problémy jako je špatný aplikační ekosystém, chybějící podpora pro běh některých aplikací, omezená stabilita, omezené finanční prostředky pro rozvoj distribuce a nedostatky v oblasti správy systému. [22]

5 ZÁKLADNÍ KONFIGURACE RHEL

Následující kapitola se věnuje základnímu nastavení a správě systému běžící na distribuci RHEL nebo z ní vycházející. Do základního nastavení je v této kapitole zahrnuto především správa uživatelů, jakým způsobem lze přidávat nové uživatele do systému, přidělovat je do skupin, nastavování práv nebo jakým způsobem se ukládají jejich informace, a kde je lze najít. Na začátku jsou okrajově popsány balíčkovací systémy používané na distribucích RHEL. Kapitola se také věnuje popisu Security-Enhanced Linuxu zkráceně SELinux, který umožňuje administrátorovi systému mít větší kontrolu nad tím, kdo přistupuje ke spravovanému systému a zvýšit tak tím jeho bezpečnost. SELinux modifikuje jádro systému a implementuje Mandatory Access Control (MAC) sloužící pro řízení přístupu k souborům, portům nebo paměťovým segmentům. Poslední položkou základního nastavení je správa služeb. Správa služeb se vykonává pomocí správce Systemd. Systemd je démon, který obsahuje sadu stavebních bloků systému. Poskytuje správce systémových služeb a běží jako PID 1.

5.1 Správce balíčků DNF

DNF je software pro správu balíčků, který je nastaven jako výchozí správce balíčků na většině distribucí založených na balíčkovacím formátu RPM. Pomocí DNF lze balíčky instalovat, aktualizovat nebo měnit a jedná se o nástupce balíčkovacího systému YUM. Oproti YUM má lepší využití paměti, vylepšenou správu závislostí a schopnost spouštět Python 2 i Python 3. DNF provádí automatickou kontrolu závislostí, usnadňuje tím tak instalaci a údržbu balíčků. V případě závislosti nainstaluje další potřebné balíčky, a také nabízí porovnání nainstalovaných balíčků s těmi dostupnými na Internetu. Na distribuci Fedora je DNF výchozí správce balíčků od Fedory 22. Na RHEL od verze 8 je to nyní také výchozí správce. DNF poskytuje bezpečnou správu balíčků díky ověřování podpisu GPG na balíčcích podepsaných GPG. Nejsou tedy nainstalovány žádné balíčky, které nejsou podepsány správným klíčem tohoto úložiště. [28], [29]

5.2 Správce balíčků RPM

RPM je systém pro správu balíčků běžící na distribucích RHEL, CentOS a Fedora. Usnadňuje distribuci, správu a aktualizaci softwaru určeného pro RHEL, CentOS nebo Fedora. RPM poskytuje operace s balíčky jako je instalace, přeinstalace, aktualizace, odstranění a ověřování balíčků. Pro práci s balíčky RPM můžou uživatelé využít i další nástroje pro správu balíčků

jako je YUM nebo PackageKit. RPM si udržuje databázi nainstalovaných balíčků a jejich souborů, tudíž na systému lze jednoduše vyhledávat a ověřovat nainstalované balíčky. Každý balíček RPM obsahuje metadata, které v sobě nesou informace o verzi, vydání, velikosti, adrese URL projektu, pokyny k instalaci a další věci. RPM umožňuje zabalit původní zdroje softwaru společně se všemi záplatami, které byly použity do zdrojových binárních balíčků. Balíček také obsahuje kompletní instrukce pro sestavení. Tento design usnadňuje údržbu balíčků při vydání nových verzí softwaru. Podobně jako DNF, RPM podporuje digitální podpisy za pomoci GPG pro ověřování pravosti balíčku. [30]

5.3 Základní konfigurace

Po zapnutí nainstalovaného operačního systému RHEL lze na terminálu nainstalovat balíček neofetch pro kontrolu nainstalování požadovaných verzí softwaru. Neofetch se naistaluje zadáním příkazů:

```
# sudo dnf install epel-release -y
# sudo dnf install neofetch -y
```

Po zadání příkazu neofetch je vypsán souhrn informací, který obsahuje verze nainstalovaného softwaru a další systémové údaje. Do tohoto souhrnu patří typ a verze operačního systému, verze kernelu, typ a verze shellu. Nacházejí se zde také informace o hardwaru, na kterém systém běží nebo rozlišení daného systému. [31]

Jedna z prvních věcí, která je vhodná na systému provést, je zkontrolovat všechny aktualizace, zda nechybí nějaké důležité změny systému. Pro instalaci nejnovějších aktualizací lze použít příkaz:

```
# sudo dnf -y update
```

V případě, že uživatel chce změnit jméno hostitele systému. Může použít následující příkaz:

```
# sudo hostnamectl  --static hostname "rhel-workstation"
```

Doporučeným, avšak ne povinným konfiguračním krokem je povolení repozitáře CRB neboli Code Ready Builder. Tento repositář není ve výchozím nastavení povolen a obsahuje dodatečné knihovny a nástroje pro vývojáře. CRB byl přenesen z CentOS a má svůj ekvivalent v RHEL. Povolení repositáře CRB proběhne zadáním příkazu: [32]

```
# sudo dnf config-manager --set-enabled crb
```

Pokud je vytvořen RHEL Server, existuje několik kroků, jak tento server zabezpečit a zlepšit jeho použitelnost. Pro přihlášení k serveru správce potřebuje znát veřejnou adresu IP. Dále je zapotřebí znát heslo v případě instalace klíče SSH pro ověřování a soukromý klíč pro účet uživatele root. Uživatel s přístupovými právy roota se přihlásí k serveru pomocí:

```
# ssh root@adresa_IP_serveru
```

Po zadaní příkazu je vyžadováno zadání hesla. Pokud se používá klíč SSH, který je chráněn heslem, při zahájení nové relace může být uživatel vyzván k zadaní tohoto hesla, jestliže se jedná o prvotní použití klíče v dané relaci. Může se také stát, že při první přihlášení k serveru bude uživatel vyzván ke změně hesla pro účet uživatele root. Kvůli zvýšeným oprávněním účtu root, při kterých lze provádět také destruktivní činnosti, je doporučeno vytvořit alternativní účet pro každodenní práci. Tento alternativní účet v případě potřeby může získat zvýšená oprávnění také. [33]

Jakmile je uživatel přihlášen jako root, má možnost vytvořit nového uživatele. Nový uživatel může nabýt zvýšených práv pomocí příkazu sudo. To umožní i novému uživateli provádět příkazy jako root. Jestliže chce uživatel provádět administrativní operace bez toho, aniž by se musel odhlašovat z běžného uživatele a znovu se přihlašovat jako root, je zde možnost nastavit běžnému uživateli takzvaného „superuživatele“ nebo oprávnění root. To umožní běžnému uživateli provádět administrátorské příkazy zadáním klíčového slova sudo před každý příkaz. Daný uživatel musí být přidán do speciální skupiny „wheel“, která se používá na řízení přístupu k příkazům su nebo sudo. Jakmile je uživatel členem této skupiny může využívat příkazy su a sudo. Uživatel s právy roota spustí následující příkaz a přidá tak uživatele do skupiny „wheel“.

```
# usermod -aG wheel jmeno_uzivatele
```

Odteď i běžný uživatelský účet může používat práva superuživatele pomocí příkazu sudo. [33]

Po vytvoření běžného uživatele bez práv roota je vhodné nakonfigurovat přístup na server pomocí SSH. Nejdříve je však na místě ověřit dostupnost přístupu jako root. Tímto způsobem lze řešit problémy jako root a provádět potřebné změny, které vyžadují práva roota. Proces konfigurace přístupu SSH závisí na tom, zda účet uživatele root používá heslo nebo klíče SSH pro přihlášení k serveru. V případě použití hesla, je ověřování heslem povoleno pro SSH. Uživatel se pomocí svého běžného účtu může přihlásit přes SSH spuštěním terminálu a použití SSH společně se svým uživatelským jménem.

```
# ssh user@ adresa_IP_serveru
```

Poté uživatel zadá svoje heslo a bude přihlášen k serveru. Uživatel bude vyzván k zadání jeho hesla, když jde o jeho první přihlášení v dané relaci pomocí příkazu sudo a takto opakovaně při každé další nové relaci. Obecně však platí, že pro lepší zabezpečení serveru se používají klíče SSH radši než hesla. Pokud se uživatel pod účtem roota přihlašuje pomocí klíčů SSH, je přihlašování pomocí hesla na server zakázáno. Pro úspěšné přihlášení pomocí SSH musí uživatel přidat kopii svého veřejného klíče přidat do souboru „~/.ssh/authorized_keys“. Jelikož veřejný klíč uživatele je již obsažen v souboru „~/.ssh/authorized_keys“ uloženého na serveru v účtu roota, může tento soubor a struktura adresářů být zkopírována do nového uživatelského účtu. Nejjednodušší cesta, jak zkopírovat soubory a zároveň zachovat správně vlastníky a oprávnění souborů je pomocí příkazu rsync. Tento příkaz zkopíruje složku .ssh uživatele root, zachová oprávnění souborů a změní jejich vlastníky, vše v jednom příkazu. Příkaz rsync zachází jinak se zdroji a cíli, které končí s koncovým lomítkem než s těmi, co nekončí koncovým lomítkem. Pokud se stane, že uživatel přidá koncové lomítko při kopírování složky ~/.ssh do uživatelského adresáře, rsync zkopíruje obsah složky ~/.ssh do domovské složky uživatele sudo místo kopírování celé struktury složky ~/.ssh. Tyto soubory skončí ve špatné cílové složce a SSH je nebude moct poté najít a použít. [33]

5.4 Správa uživatelů

Na linuxových distribucích je každý uživatel přiřazen do skupiny, takzvané uživatelovi primární skupiny. Skupina se může skládat z jednoho nebo více uživatelů. Jeden uživatel je členem minimálně jedné skupiny a zároveň může být členem jedné nebo více skupin, které nejsou jeho primární. Tyto skupiny jiné, než primární se nazývají doplňkové. Uživatelské skupiny a samotní uživatelé jsou spravováni pomocí unikátních číselných identifikátorů GID a UID. Pro uživatele se používá identifikátor UID a pro skupiny slouží GID. Oba identifikátory jsou rozpoznány jádrem operačního systému, což indikuje, že Super Admin nemusí být uživatel root. Super Admin však musí mít hodnotu UID nula. [34]

Nová skupina se dá vytvořit pomocí příkazu:

```
# groupadd [-f] [-g GID] nazev
```

Kde příznak „-f“ slouží pro automatické generování GID, v případě že GID vybrané uživatelem je již zabráno jinou skupinou. Hned po příznaku „-g“ se píše vybrané GID pro skupinu. Pokud

chce uživatel nastavit hodnotu GID od SYS_GID_MIN do SYS_GID_MAX použije pro to příznak „-r“. Hodnoty těchto proměnných jsou uvedeny v souboru „/etc/login.defs“. Název skupiny by neměl obsahovat žádné speciální znaky a měl by být odlišný od názvu existujících uživatelů v systému nebo systémových souborů. Pro modifikaci existujících skupin slouží příkaz groupmod. Jeho formát je následující:

```
# groupmod [-g GID] [-n nom] skupina
```

Příznak „-g“ nastavuje nové GID pro skupinu, u které probíhá modifikace. Při změně jména skupiny se používá příznak „-n“ a ihned za ním nový název pro skupinu. Změny lze provádět i najednou, tudíž měnit GID a jméno skupiny v rámci jednoho příkazu. Důležité je přiřadit nové GID souborům jež patřily do původní skupiny, u které proběhly změny. Odstranění skupiny probíhá jednoduše pomocí příkazu groupdel a názvu odebírané skupiny. Při mazaní skupiny může nastat situace, kdy odebíraná skupina je zároveň unikátní primární skupina určitého uživatele. V tomto případě systém ohlásí, že nemůže smazat skupinu, dokud bude tento uživatel její součástí. Pokud jde o mazání doplňkové skupiny, systém tuto skupinu smaže bez dalších varování a všichni uživatelé již nebudou součástí této skupiny. Při operaci mazání uživatele je automaticky odstraněna i jeho primární skupina, které většinou nese stejné jméno jako uživatel. Jelikož uživatel je vždy nutně součástí nějaké skupiny, doporučuje se vytvářet skupiny jako první. Skupina nutně nemusí mít žádné členy. Soubor, ve které se nacházejí informace o skupině se nazývá „/etc/group“. Jednotlivé informace jsou odděleny pomocí oddělovače „:“. Uchovávají se tu informace o názvu skupiny, heslo reprezentované pomocí „x“, GID a seznam uživatelů, pro které je tato skupina doplňková. Každý řádek v tomto souboru symbolizuje jednu skupinu. V tomto souboru nejsou uvedeni uživatelé, kteří mají danou skupinu jako primární. Informace o primárních uživatelích jsou uvedené v souboru „/etc/passwd“. Bezpečnostní informace o skupinách obsahuje soubor „/etc/gshadow“. Obsahuje jméno skupiny, šifrované heslo, jméno administrátora skupiny a doplňkové uživatele skupiny. Každý záznam v „/etc/group“ musí mít korespondující záznam v „/etc/gshadow“ a jméno skupiny musí být v obou souborech stejné. [34]

Jednotlivý uživatelé jsou uchováváni v souboru „/etc/passwd“. Tento soubor ukládá informace, jako je uživatelské jméno, heslo jako „x“, které indikuje, že uživatel používá heslo, jeho zašifrovaná forma lze najít v souboru „/etc/shadow“. Dále „/etc/passwd“ obsahuje UID uživatele, GID jeho primární skupiny, komentáře a domovský adresář. Na základě UID se dají uživatelé rozdělit na tři skupiny. [34]

1. UID 0 – systémový správce (root)
2. UID 201 až 999 – systémový uživatelé, využíváno systémem pro správu přístupových práv aplikací
3. UID vetší než 1000 – běžní uživatelé, kteří se mohou přihlásit do systému

Pro přidávání uživatelů lze využít příkaz useradd jeho syntaxe je následující:

```
# useradd [-u UID] [-g GID] [-d directory] [-s shell] jmeno_uzivatele
```

První dva příznaky nastavují identifikátor uživatele a skupiny, kde identifikátor skupiny může být i jméno skupiny. Příznak „-d“ nastavuje danému uživateli jeho domovský adresář. V opačném případě, pokud by uživatel neměl mít domovský adresář lze k tomu využít příznak „-M“. Při vytvoření nové uživatelského účtu nemá tento účet nastaveno heslo a je zamčený. Pro odemknutí musí být účtu nastaveno heslo. Pokud není nastaveno jinak, příkaz useradd vytvoří domovský adresář končící jménem uživatele. Primární skupina ponese jméno uživatele, výchozí shell je bash a UID i GID je automaticky nastaveno na hodnotě od 1000, ve většině případů je UID a GID stejné. Název účtu nesmí obsahovat velká písmena a speciální znaky. Nesmí se také shodovat s názvem již existující skupiny nebo systémového souboru. Musí být vytvořen strom domovského adresáře s výjimkou posledního adresáře. Při vytváření uživatele musí být uvedena alespoň jedna skupina, ale lze rovnou nastavit uživateli i skupiny doplňkové pomocí příznaku „-G“. Příznakem „-D“ lze při vytváření uživatele nastavit jeho hodnoty na výchozí podle systému a příznakem „-b“ nastavit výchozí adresář. Příkladem výchozího nastavení může být:

```
# sudo useradd -D -g 1000 -b /home -s /bin/bash
```

Upravování uživatele probíhá přes příkaz usermod. Příkaz vypadá následovně:

```
# usermod [-u UID] [-g GID] [-d directory] [-m] jmeno_uzivatele
```

Jako u vytváření lze měnit UID, GID a domovský adresář. Na příznak „-d“ se váže příznak „-m“, který přesune obsah starého domovského adresáře do nového. Pokud starý adresář neexistuje nebude vytvářen nový adresář. Dalšími volitelnými příznaky jsou „-e“ pro nastavení vypršení platnosti účtu, „-L“ permanentní zamčení účtu, „-U“ odemknutí účtu, „-a“ pro přidání nových doplňkových skupin, tento příznak musí být použit společně s příznakem „-G“, který upravuje uživatelovi doplňkové skupiny a přepisuje původní doplňkové skupiny. Uživatel může být modifikován v případě, že je odpojen a nemá žádné běžící procesy. Při změněně UID

uživatele musí být všem jeho souborům nastaveno nové UID. Kupříkladu staré UID je hodnota 1000 a nové UID je 1044, změna UID souborů proběhne následovně:

```
# sudo find / -uid 1000 -exec chown 1044: {} \;
```

Mazání uživatele se provádí příkazem userdel. Tento příkaz má pouze jeden příznak „-r“, který maže uživatelův domovský adresář a poštovní soubory nacházející se v adresáři „/var/spool/mail/“. Pro smazání uživatele platí stejná pravidla jako při modifikaci, tudíž musí být odpojen od všech služeb a nesmí mít žádné probíhající procesy. Zároveň příkaz userdel smaže příslušné záznamy o uživateli v souborech /etc/passwd, /etc/shadow, /etc/group, a /etc/gshadow. Soubor /etc/shadow obsahuje bezpečnostní informace o uživatelích. V tomto soubor lze najít uživatelské jméno, zašifrované heslo, které používá kódování SHA512 definované metodou „ENCRYPT_METHOD“ ze souboru „/etc/login.defs“. Dalším záznamem je, kdy bylo naposledy měněno heslo, tento záznam je ve formátu časové známky. K tomu se váže následující záznam o minimální trvanlivosti hesla, jedná se o dobu mezi změnami hesla ve dnech. Kupříkladu pokud je hodnota nastavena na 5, heslo může být změněno až po 5 dnech. Opakem je maximální trvanlivost hesla, kde se určuje po kolika dnech musí být heslo změněno. V následujícím poli je uvedeno počet dní, kdy bude uživatelovi zobrazeno varování před vypršením hesla. Předposledním záznamem je datum expirace účtu, po expiraci účtu se uživatel nemůže přihlásit do systému. Poslední záznam je rezervován pro budoucí použití. [34]

5.5 SELinux

Systém SELinux celým názvem Security Enhanced Linux je bezpečnostní systém obsahující mechanismy pro podporu bezpečnostních politik řízení přístupu. SELinux byl vytvořen společností NSA (National Security Agency) a implementuje architekturu Mandatory Access Control zkráceně MAC v subsystémech jádra Linuxu. Cílem systému SELinuxu je omezovat oprávnění nebo odstraňovat rizika spojená s kompromitováním programu nebo démona. SELinux je hlavně určen pro systémy vycházející z distribuce RHEL, přesto se dá implementovat i do jiných distribucí Linuxu, ale u těch může být implementace složitější. Předtím než se objevily systémy MAC bylo standardní zabezpečení správy přístupu založeno na systémech DAC (Discretionary Access Control). Tyto systémy dostatečně neomezovaly práva programů, u kterých bylo diagnostikováno poškození a to mohlo potencionálně vést k přístupu do podsystémů operačního systému. Na všech servisních jednotkách je definován

časový limit 5 minut, tak aby se předešlo zamrznutí systému z důvodu spuštění chybné služby. [35]

Systémy MAC posiluje oddělení důvěryhodnosti a integrity informací v systému, tak aby bylo dosaženo zádržného systému. V tomto systému neexistuje žádný superuživatel a je nezávislý na tradičním systému práv. Jádro se při každém systémovém volání dotazuje SELinuxu, zda je provedení takové operace možné. Provoz SELinuxu je odlišný od tradičních unixových práv. Bezpečnostní kontext se skládá z identity, role a domény. Identita přímo závisí s uživatelovým linuxovým účtem. Identitě je přiřazena jedna nebo více rolí, ale každá role má pouze jednu doménu. Práva uživateli ke zdroji se vyhodnocují podle domény kontextu zabezpečení. Kontext zabezpečení je uživateli přiřazen v okamžiku jeho připojení, vzhledem k jeho roli. Bezpečnostní kontext souboru je definován příkazem chcon. Práva procesu záleží na kontextu jeho zabezpečení. Ve výchozím nastavení je kontext zabezpečení definován trojící věcí (identita, doména, role) uživatele, který daný proces spouští. V kontextu SELinuxu je doména specifický typ, který je spojený s procesem a zděděný uživatelem jež jej spouští. Většina důležitých procesů má přiřazenou svojí vlastní doménu. Pro správu pravidel SELinuxu se využívá příkaz semanage. [35]

SELinuxu má tři módy, ve kterých operuje. Prvním je enforcing, v tomto módu se vynucují nakonfigurovaná pravidla SELinux a jedná se o výchozí nastavení v distribuci RHEL. Druhým je permissive v tomto módu se protokolují všechny zprávy a chyby přístupu, ale jakékoliv operace jsou povoleny. Posledním módem je disabled, kdy SELinux je vypnut, nic není zakázáno a neprotokolují se žádné zprávy. Nové objekty jsou vytvářeny bez bezpečnostního kontextu. Politiky SELinuxu definují dvě základní sady pravidel. Targeted politika zabezpečující pouze služby, které jsou připojeny k síti. Strict tato politika chrání všechny démony a uzamyká celý systém. Omezení jsou kladena na celý systémový i uživatelský prostor. [35]

5.6 Správa služeb

V linuxových distribucích se používá správce Systemd pro řízení služeb. Jeho vývoj byl zaměřen, tak aby byl kompatibilní se staršími inicializačními SysV skripty. Systemd umožňuje například paralelní start služeb při zapnutí systému, spouštění démonů v případě potřeby, podporu pro snímky systému nebo správu závislostí mezi jednotlivými službami. Pomocí Systemd lze za využití snímků systému obnovovat předchozí stavy systému. Při startu systému

Systemd vytvoří na všech systémových službách naslouchací sokety a pošle je těmto službám, jakmile jsou spuštěny. Toto umožňuje restartovat službu a zároveň přijmout všechny zprávy, které službě v době její nepřítomnosti poslala síť. Příslušné sokety každé služby řadí zprávy do front a jsou přístupné i v případě, že daná služba zrovna neběží. Služby se dají restartovat nebo zastavit pouze za běhu pomocí nástroje Systemd. V dřívějších verzích, než je RHEL 7 se pokoušely zastavit služby přímo bez kontroly jejich aktuálního stavu. Systémové služby nedědí žádný kontext a každá služba pracuje ve svém vlastním kontextu provádění. [36]

Pro správu služeb z příkazové řádky se používá příkaz systemctl. Pomocí tohoto příkazu se dají služby spouštět, restartovat, vypínat nebo zobrazovat jejich stav. Příklad použití:

```
# systemctl stop nfs-server
```

Tímto příkazem se zastaví služba serveru NFS. Příkazem systemctl se daná služba může úplně zakázat nebo naopak povolit. Tato operace se provádí pomocí klíčových slov „enable“ a „disable“ následující názvem služby. Seznam povolených a zakázaných služeb lze zjistit příkazem:

```
# systemctl list-unit-files --type service
```

Od RHEL 8 jsou úrovně běhu nahrazeny pomocí cílů Systemd. Tyto cíle jsou reprezentovány cílovými jednotkami a jejich jediným účelem je seskupit další jednotky Systemd do řetězce závislostí. Seznam dostupných cílů na systému se zobrazí následovně pomocí příkazu systemctl.

```
# systemctl list-units --type target
```

Tento příkaz vypíše, zda je cílová služba načtená, aktivní a její bližší popis. Pro výpis, který cíl je nastaven jako výchozí lze zjistit zadáním klíčového slova „get-default“. Výsledkem je vypsání symbolický odkaz cíle, který je umístěn v souboru „/etc/systemd/system/default.target“. Pro změnu výchozího cíle lze použít příkaz:

```
# systemctl set-default name.target
```

Systemd umožňuje využít záchranný režim, který poskytuje prostředí pro opravu systému v případech, kdy není možné spustit systém normálním způsobem. Systém běžící v záchranném režimu se pokusí připojit všechny místní systémy souborů a spustit několik důležitých systémových služeb, avšak neumožní v danou dobou připojení ostatních uživatelů k systému. V distribuci RHEL je záchranný režim ekvivalentem k jednouživatelskému režimu vyžadující heslo účtu root. Do záchranného režimu se lze dostat pomocí systemctl a použití klíčového

slova rescue. Další režim umožňující opravu systému je nouzový režim. Tento režim poskytuje maximálně minimalistické prostředí a umožňuje opravu systému i v situacích, kdy nemůže být použit záchranný režim. Kořenový souborový systém se v tomto módu připojuje pouze pro čtení. Není spuštěn žádný jiný souborový systém, většina služeb je zakázána až na pár základních a neaktivuje se žádné síťové rozhraní. Nouzový režim se spouští za použití klíčového slova emergency. Příkaz systemctl nahrazuje řadu příkazů pro správu napájení používaných v předchozích verzích. Pomocí systemctl tudíž lze provést operace jako měkké vypnutí, tvrdé vypnutí, restart, pozastavení, uvedení do spánku nebo uvedení do spánku a pozastavení systému. [36]

6 KONFIGURACE SLUŽEB RHEL

Tato kapitola se věnuje popisu hlavních služeb používaných v počítačových sítích. Popisuje, jaké nástroje se ke konfiguraci těchto služeb používají a co dané služby vykonávají za funkce. Popisovány jsou služby: firewall sloužící pro ochranu systému před vnějšími hrozbami přicházející z Internetu za účelem poškození nebo zmanipulování systému. DHCP, která se stará o konfiguraci nově připojených zařízení do sítě a umožňuje jim v síti komunikovat, aniž by se muselo něco nastavovat ručně. Lokální DNS zajišťující překlad doménových jmen na adresy IP a naopak. FTP dovolující přenášet po síti soubory. Apache, který spravuje webové servery a posílá je na vyžádání klientů s pomocí protokolu HTTP.

6.1 Firewall

Firewall je zařízení zkoumající příchozí komunikaci přes porty počítače z Internetu. Konfigurace firewallu v distribuci RHEL se provádí pomocí nástroje firewalld. Tento softwarový nástroj pro správu firewallu je dostupný pro mnoho distribucí Linuxu. Funguje jako frontend pro systém filtrování paketů iptables nebo nftables v jádře Linuxu. Démon firewalld spravuje skupiny pravidel pomocí entit nazývaných zóny. Zóny jsou sady pravidel, které v závislosti na důvěryhodnosti sítě určují, jaký provoz by měl být povolen. Jednotlivá síťová rozhraní jsou přiřazená k zónám, které dále určují chování brány firewall. U počítačů, které se často přesouvají mezi sítěmi, poskytuje tento druh flexibility dobrou metodu změny pravidel v závislosti na daném prostředí. Takto lze mít přísná pravidla na veřejné síti zakazující většinu provozu a zároveň mít volnější omezení při připojení do domácí privátní sítě. Pro servery tyto zóny nejsou nikterak důležité, jelikož servery mění svoje prostředí pouze zřídka nebo vůbec. [37]

Předdefinované zóny v rámci firewalld mají několik úrovní důvěryhodnosti v pořadí od nejméně důvěryhodné až po nejvíce důvěryhodné. Prvním a nejnižším stupněm důvěry je drop. V tomto stupni jsou všechna příchozí spojení zahozena a je možné pouze odchozí spojení. Podobně funguje stupeň block, který namísto aby příchozí spojení zahazoval tak zareaguje zamítavou zprávou „icmp-host-prohibited“ nebo „icmp6-adm-prohibited“. Stupeň public představuje veřejné nedůvěryhodné sítě. Každý počítač v síti se bere jako nedůvěryhodný, ale v některých případech lze povolit příchozí spojení. Dále stupeň external se používá pro externí sítě v případech, kdy je používán firewall jako brána. Maskuje NAT a chrání interní síť, takže síť zůstane soukromá, ale zároveň stále dosažitelná. Ve stupni internal jsou počítače v síti již

relativně důvěryhodné a jsou k dispozici i některé doplňkové služby. Tento stupeň představuje druhou stranu vnější zóny, která se používá pro vnitřní část brány. Stupeň dmz je určen pro počítače, které jsou izolované od zbytku sítě, tudíž nemůžou komunikovat s ostatními počítači ve vnější síti. Těmto izolovaným počítačům jsou povolena pouze určitá příchozí spojení. Další v pořadí je stupeň work určený pro pracovní stroje. Většina počítačů v těchto sítích mají důvěru a může být povoleno i několik dalších služeb. Důvěryhodnost stupně home je určeno pro domácí prostředí, to obecně znamená důvěru většině počítačů v síti a je povoleno i několik dalších služeb. Posledním a nejvyšším stupněm důvěryhodnosti je trust. Tento stupeň důvěřuje naprosto všem počítačům v síti. Jedná se o nejotevřenější ze všech možností a měla by se používat s rozvahou. [37], [38]

Ve firewalld můžou být pravidla aplikována na aktuálně běžící sadu pravidel nebo mohou být nastavená jako trvalá. Při přidání nebo změně pravidla se ve výchozím nastavením změny provedou pouze v právě běžícím firewallu. Po restartu a opětovném načtením firewallu, zůstávají pouze trvalá pravidla. Většina příkazů pro firewall přes příkazový řádek může mít příznak „--permanent“, který označuje, že provedená změna se má provést natrvalo. Kromě toho lze aktuálně běžící bránu uložit do trvalé konfigurace pomocí příkazu „firewall-cmd --runtime-to-permanent“. Toto oddělení běžících a trvalých pravidel přináší výhodu v testování různých pravidel za běhu právě aktivní brány firewall a v případě potíží znovu načíst původní pravidla. [37], [38]

6.2 DHCP

Protokol DHCP umožňuje po připojení do dané sítě automaticky získat kompletní konfiguraci pro komunikaci v této síti. Servery DHCP ukládají informace o konfiguracích a poskytují je klientům na vyžádání. DHCP se vyvinul z dříve používaného protokolu BOOTP a používá stejný formát zpráv mezi klientem a serverem. Inovací DHCP zpráv oproti BOOTP je možnost obsahovat data konfigurace pro klienta. Konfigurace adres IP jsou přidělovány klientům prostřednictvím zapůjčení, v případě že už daný klient adresu IP nepoužívá je vrácena zpět na server DHCP k dalšímu zapůjčení. V opačném případě, pokud klient stále adresu používá může zažádat o její prodloužení. Adresy jsou vždy propůjčovány na určitý časový úsek, který může mít každý server DHCP jinak nastaven. Díky půjčování adres stačí sítím provozujícím servery DHCP menší počet dostupných adres IP, než by bylo potřeba v případě nastavení trvalých adres všem klientům v síti. DHCP spravuje adresy IP bez zásahu správce a není nutno přiřazovat adresy ručně individuálním klientům. Klienti se mohou přesouvat do jiných podsítí bez nutnosti

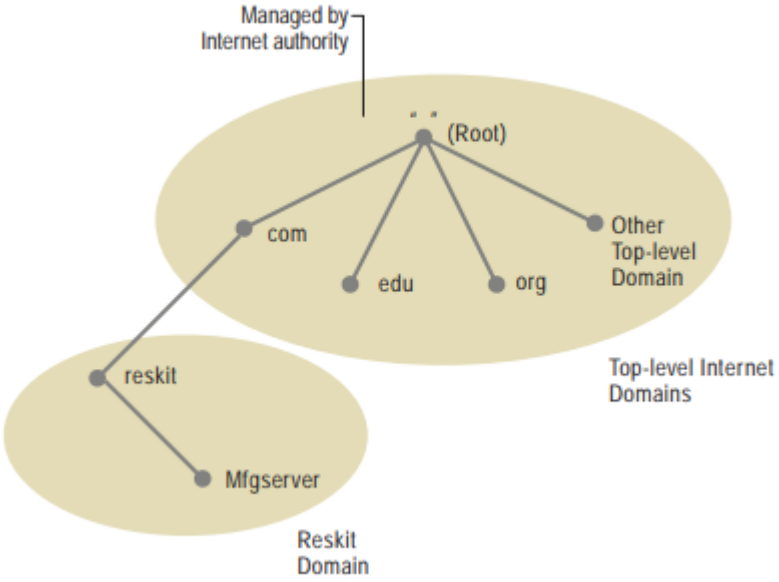
rekonfigurace, protože ze serveru DHCP získávají informace o nové síti. Server DHCP poskytuje centralizovanou správu síťových klientů a konfigurační informace jsou uloženy na jednom místě, v datovém úložišti DHCP. Server DHCP využívá multithreading ke zpracování velkého množství požadavků od klientů najednou. Datová úložiště jsou optimalizována pro velké množství provozu přicházející na server DHCP. Přístup k datovému úložišti je zpracováván pomocí samostatných modulů. Tento přístup umožňuje přidat podporu pro jakoukoliv databázi, kterou se správce rozhodne použít. [39], [40]

V RHEL je protokol DHCP výchozím konfiguračním módem síťového rozhraní, proto může nově zapojené zařízení do sítě fungovat bez dalšího nastavení. Konfigurace síťového rozhraní lze najít v RHEL ve složce „/etc/sysconfig/network-scripts/“. Pro každé rozhraní Ethernet umožňuje soubor ifcfg-ethX konfiguraci příslušných rozhraní. Konfigurace obsahuje věci jako je název rozhraní, povolení automatického spouštění rozhraní, nastavení, zda rozhraní po zapnutí vyšle požadavek na server DHCP nebo specifikace adresy MAC. Pro fungování serveru DHCP po startu systému je nutné upravit hodnoty právě v souboru „/etc/sysconfig/network-scripts/ifcfg-<interface_nazev>“. Ve výchozím nastavení je parametr BOOTPROTO nastaven na none. To ukazuje, že systém používá statickou adresu IP. Pokud chce uživatel navázat síťové připojení přes DHCP je nutno změnit tento parametr na dhcp. Další krokem je smazání parametrů IPADDR, PREFIX a GATEWAY nacházející se také v tomto souboru. Parametr ONBOOT má hodnotu yes, což říká, že připojení bude aktivováno během startu systému. Jakmile je tento soubor správně nastaven, připojení k síti probíhá přes DHCP. [41]

6.3 Lokální DNS

Ve veřejném prostoru se servery DNS používají k mapování názvů na adresy IP hostitelů a v případě PTR (reverzních) záznamů probíhá překlad z adresy IP na název domény hostitele. V privátní síti, která se používá pro vývoj více systémů lze využít soubor „/etc/hosts“ pracovní stanice RHEL uživatele k mapování názvů na adresy IP. Toto však bude fungovat pouze pro jednu stanici, aby se věci používaly univerzálně je nutno vytvořit soukromý lokální server DNS. [42]

Systém pojmenování, které DNS používá je ve formě hierarchické stromové struktury, nazývaný jmenný prostor domény. Následující obrázek ilustruje část jmenného prostoru Internetu od kořenové domény a nejvyšší úrovně internetového DNS až po doménu „reskit.com“ hostitele. [43]



Obrázek č. 6 - Jmenný prostor Internetu (zdroj [43])

Celý doménový název je tedy tvořen cestou od kořene až k hostiteli. Kořen je speciální doména symbolizovaná tečkou. Výsledné jméno domény se píše opačným směrem a kořen je zcela vpravo. Kupříkladu doména „reskit“ je subdoménou domény „.com“, proto celý název pro „reskit“ je „reskit.com“. Kořen jmenného prostoru Internetu je spravován autoritou pro registraci Internetových jmen, která pověřuje administrativní zodpovědností za část jmenného prostoru organizace, které se připojují k Internetu. Pod kořenovou doménou se nachází doména nejvyššího řádu. Domény nejvyššího řádu lze rozdělit na tři typy:

1. Organizační domény – pojmenovány pomocí tříznakového kódu, která označuje primární funkci domény.
2. Geografické domény – označeny pomocí dvou znaků symbolizující kód země nebo oblasti.
3. Reverzní doména – speciální doména s názvem „in-addr.arpa“, která se používá pro mapování adresy IP na jméno.

DNS využívá ke své funkci takzvané zóny. Každá zóna je vázána k určitému doménovému uzlu. Avšak zóna není doména, ale jedná se o část jmenného prostoru DNS uloženého v souboru a může obsahovat vícero domén. Pomocí zóny server DNS odpovídá na požadavky o hostitelích nacházejících se v rámce dané zóny a je pro zónu autoritativní server. Zóny se dělí na primární a sekundární. Primární zóna je kopie zóny, do které se provádí aktualizace, zatímco sekundární zóna se replikuje z hlavního serveru. Server DNS při přijetí požadavku se pokusí načíst potřebné informace z místních zón. Pokud se to nepodaří, jelikož server není autoritativní

a nemá tedy data o požadované doméně je nutné klienta přesměrovat na jiný server, který by mohl informace obsahovat. [43]

6.4 FTP

Protokol aplikační vrstvy, který se používá pro výměnu dat a informací mezi počítači v privátní síti nebo internetu pomocí aplikace FTP. Pro konfiguraci zabezpečeného protokolu FTP se používá například démon vsftpd (Very Secure FTP Daemon). Jedná se o výchozího démona FTP v RHEL podobně jako v mnoha dalších distribucích Linuxu. Démon vsftpd umožňuje použití virtuálních uživatelů se zásuvnými moduly PAM. Virtuální uživatelé mají pouze oprávnění používat FTP. V případě, že dojde ke kompromitaci přihlašovacích údajů virtuálního uživatele, osoba s těmito přihlašovacími údaji nebude mít po získání přístupu žádná další oprávnění. Z tohoto důvodu je nastavení démona vsftpd velmi bezpečné. K démonu vsftpd existuje také varianta sftpd, která zašifruje celý tok připojení a je v tomto ohledu bezpečnější. [44]

Démon vsftpd je provozován v takzvaném režimu chroot, který zajišťuje přiřazení nového kořenového adresáře běžícímu programu, v tomto případě vsftpd. Program nemůže přistupovat k souborům mimo kořenový adresář, který mu byl přiřazen. V případě útoku je tak zbytek systému bezpečně izolován od napadené části. Z pohledu bezpečnosti se řadí vsftpd nad ostatní servery FTP, jelikož nabízí širokou škálu bezpečnostních funkcí. [45]

Jedna z funkcí vsftpd je vytváření virtuálních uživatelů. Služba vsftpd podporuje tři druhy uživatelů:

1. Anonymní uživatel – Za pomocí tohoto uživatele se lze přihlásit k serveru FTP zadáním loginu anonymous, bez zadání hesla. Využívání anonymních přihlášení však není bezpečné a ve většině případů by mělo být zakázáno.
2. Lokální uživatel – Pro připojování na server FTP lze použít lokální uživatele definované na systému. Účtu, které mají povolení se připojovat pod svým loginem na server FTP musí být specifikovány v souboru „vsftpd.userlist“.
3. Virtuální uživatel – Tito uživatelé nemají na systému vlastní domovský adresář a jejich pohyb v rámci systému je velice omezen. Mají přístup pouze ke službám serveru FTP a přístup k dalším službám nebo adresářům systému jsou jim zapovězeny. Každému virtuálnímu uživateli lze nastavit jinou sadu oprávnění, čímž se zvedne zabezpečení

a použití virtuálních uživatelů pro přístup na server FTP se považuje za nejbezpečnější variantu. [46]

Jak již bylo řečeno použití virtuálních uživatelů je mnohem bezpečnější než klasické uživatelské účty. Pro účely používání virtuálních uživatelů je potřeba vytvořit uživatelský účet, který budou virtuální uživatelé používat a s tím také vytvořit skupinu, do které bude uživatelský účet zařazen. Nejprve je tedy nutno vytvořit novou skupinu a následně do ní přidat nového uživatele. Vytvářený uživatel musí odpovídat záznamu „guest_username=“ uvedeném v souboru „vsftpd.conf“. Dalším požadavkem je vytvořit databázi hesel na rozdíl od systémových uživatelů, kteří databázi hesel nepotřebují. Databáze hesel se využívá k ověřování virtuálních uživatelů. Databáze je vytvořena za pomocí souboru obsahující virtuální uživatele a jejich hesla. Záznamy v souboru jsou odděleny řádky, nejprve je uveden název uživatele a na nový řádek jeho heslo. Po přidání všech uživatelů do textového souboru se vygeneruje databáze hesel, kterou bude vsftpd používat pro virtuální uživatele. Generování se provádí pomocí db_load poskytující libdb-utils. Každý virtuální uživatel má svůj vlastní konfigurační soubor, který určuje jeho adresář „local_root“. Tento adresář musí být vlastněn uživatelem vsftpd a skupinou v níž se uživatel vsftpd nachází. [44]

Testování serveru FTP a připojení klientů lze provést pomocí příkazového řádku na počítači klienta a otestovat přístup k počítači provozující FTP. Alternativní cesta je testování pomocí klienta FTP, jako je například FileZilla. V případě, že při testování virtuálního uživatele na serveru se spuštěným vsftpd, dostane uživatel oznámení o tom, že server používá certifikát je nutné ho schválit pro pokračování. Poté by měl mít virtuální uživatel přístup do složky „local_root“. Odkud může stahovat a nahrávat soubory. [44]

6.5 Apache

Služba Apache provozuje webové servery a doručuje webové stránky přes internet. Jedná se o jednoho z nejrozšířenějších klientů pro obsluhu HTTP požadavků. Apache spadá do sady komponent potřebných k poskytování webového obsahu. Běžně používanou sadou komponent pro práci s webovými aplikacemi, jako je například LAMP neboli Linux, Apache, MySQL a PHP. Apache je rozšířený především díky svému otevřenému kódu a schopností zvládnout velké množství požadavků s minimální konfigurací. Lze také odstranit nepotřebné moduly a zrychlit tak činnost webového serveru Apache. Moduly jde, jak odebírat, tak i přidávat, mezi nejvíce používané doplňkové moduly patří zabezpečení komunikace SSL nebo Load Balancing

pro zpracování velkého množství požadavků. Apache funguje na platformách Linux, macOS a Windows. Apache funguje na všech platformách stejně. Liší se pouze v instalačním procesu a cestách k souborům. [47]

Komunikace Apache funguje přes síť od klienta na server a zpátky pomocí protokolu TCP/IP. Pro Apache se dá použít široká škála protokolů, v praxi se používají hlavně HTTP a HTTPS. HTTPS je zabezpečená verze HTTP a používá zašifrovanou komunikaci. Šifrovaná komunikace probíhá portem 443, zatímco nezabezpečená portem 80. Apache se nastavuje pomocí konfiguračních souborů a moduly ovlivňují jakým způsobem se bude chovat. Ve výchozím nastavením naslouchá na portu 80, Apache však může být vázán k různým portům pro různé domény. Tudíž jedna doména může běžet na portu 80, jiná zase na portu 8080 a další na portu 443. To dovoluje hostování více webových stránek a domén na jednom serveru. [47]

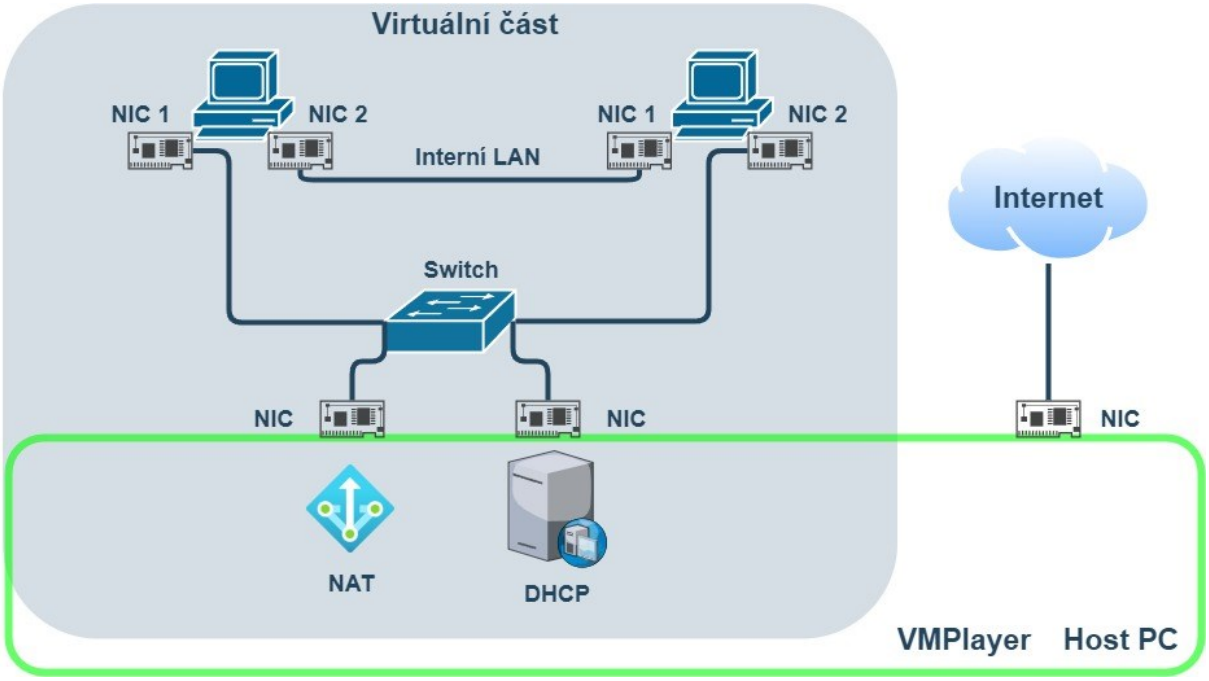
Apache může hostovat statické i dynamické webové stránky, které používají skriptovací jazyky na straně serveru, jako je PHP, Python nebo PERL. Podpora jednotlivých jazyků je implementována pomocí instalačních balíčků, přidaných ke standardní instalaci Apache. Apache také obsahuje modul pro přepisování adres URL zvaný „mod_rewrite“, ten umožňuje webmasterům vytváření vlastních adres URL. [48]

7 VYTVOŘENÍ VIRTUÁLNÍ LABORATOŘE

Kapitola demonstruje zapojení jednotlivých síťových rozhraní virtuálních počítačů. Popisuje konfiguraci jednotlivých síťových rozhraní. Udává, jaké počítače jsou potřeba pro následnou implementaci a testování jednotlivých služeb.

7.1 Schéma virtuální laboratoře – zapojení A

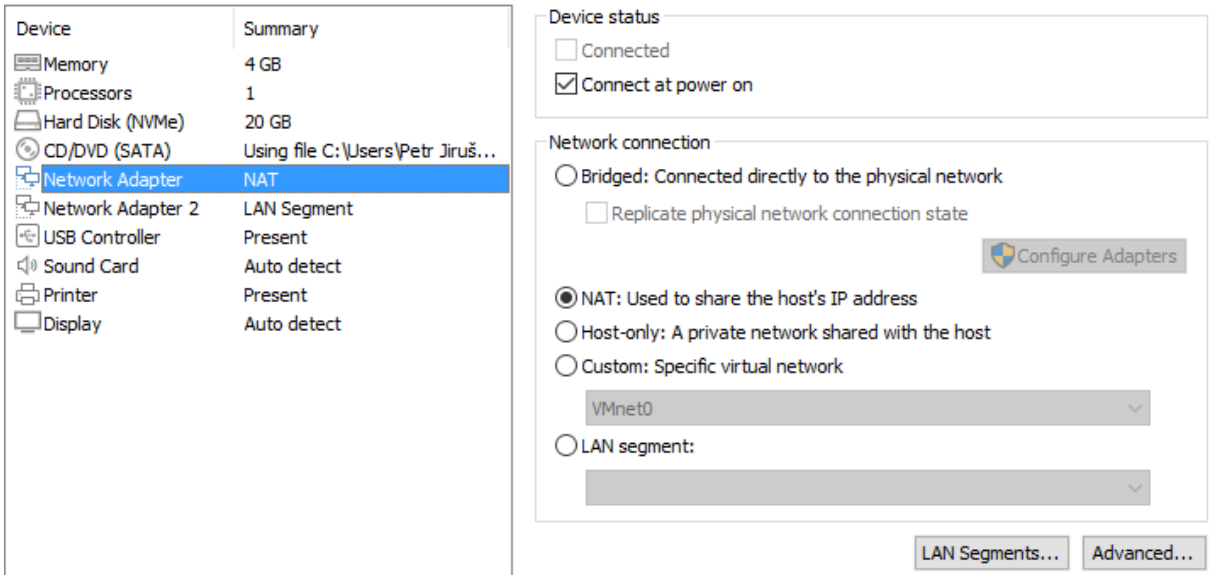
Zapojení síťové laboratoře A je realizováno pomocí lokální sítě využívající NAT k připojení internetu. Jeden virtuální počítače vystupuje v roli serveru a druhý má roli klienta. Oba virtuální počítače mají dva řadiče síťového rozhraní (NIC), kde jeden připojuje virtuální stroje k Internetu pomocí NATu a druhý spojuje virtuální počítače mezi sebou. Z čehož vzniká mezi těmito počítači privátní síť LAN pro komunikaci pouze těchto dvou strojů.



Obrázek č. 7 - Zapojení virtuální laboratoře A (zdroj vlastní)

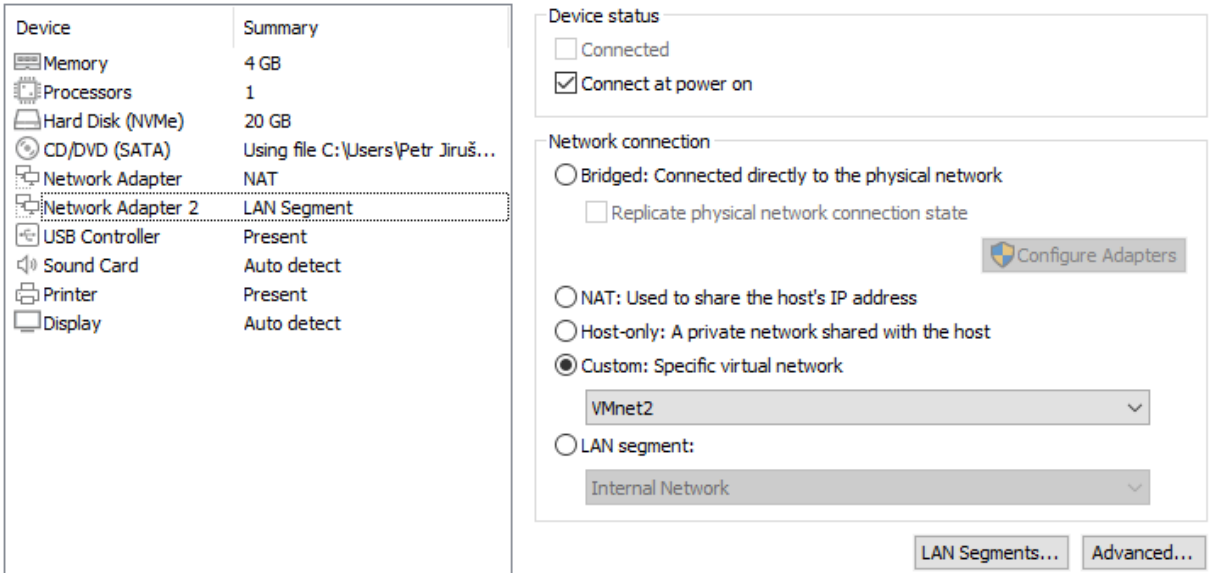
Pomocí NAT může virtuální počítač přistupovat k fyzickému hostitelskému sytému, který je napojen na Internet a případně další externí sítě. Adresy IP získají virtuální počítače automaticky od serveru DHCP, který je zabudovaný do virtualizačního nástroje. Počítače z fyzické a případně externích sítí nemají přístup k virtuálním počítačům.

Nastavení jednotlivých řadičů je rozděleno, tak že jeden nastaven řadič je nastaven pro NAT. Jeho konfigurace je zobrazena na následujícím obrázku:



Obrázek č. 8 - Konfigurace řadiče pro komunikaci pomocí NAT (zdroj vlastní)

Druhý řadič je nastaven jako segment LAN pro vytvoření interní sítě. Počítače připojené do interní sítě jsou kompletně izolovány od ostatního provozu. V tomto případě tedy mezi sebou mohou komunikovat pouze dva počítače, ani hostitelský počítač nemůže do této sítě zasáhnout. V rozhraní virtualizačního nástroje VMPlayer vypadá konfigurace interní sítě následovně:

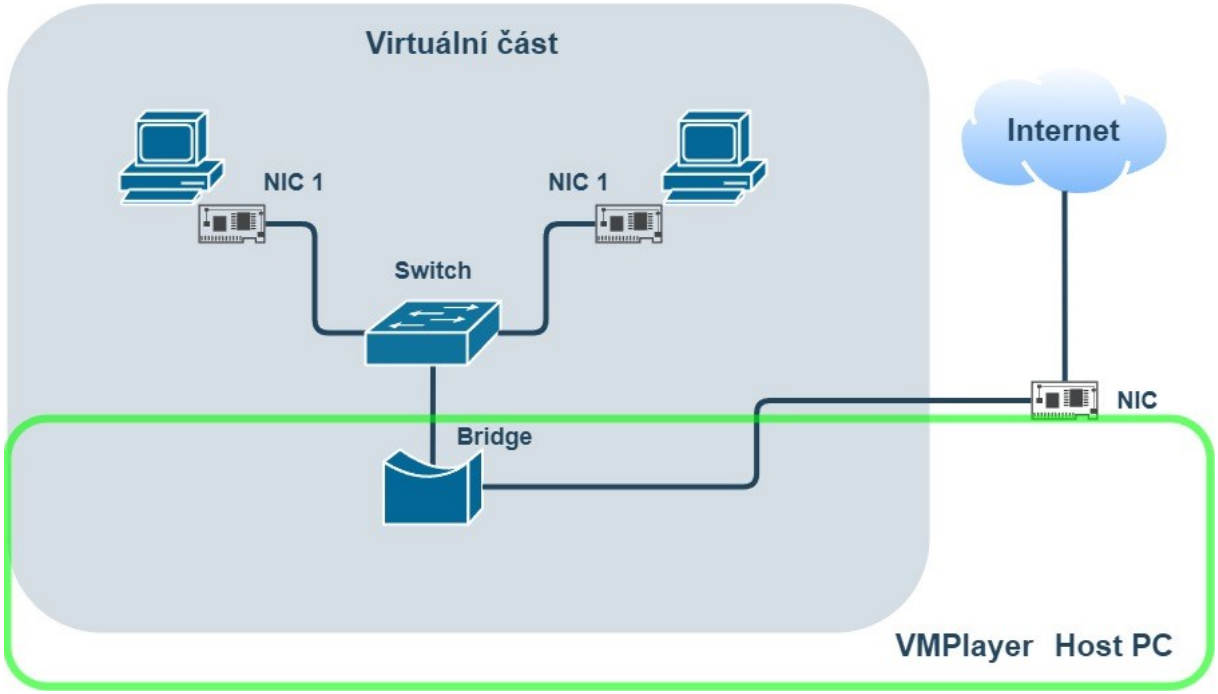


Obrázek č. 9 - Konfigurace řadiče pro realizaci interní sítě (zdroj vlastní)

Interní sítě lze dosáhnout přidáním řadiče do jedné z virtuálních sítí vmnet2 až 7 nebo vmnet 9 až vmnet 19.

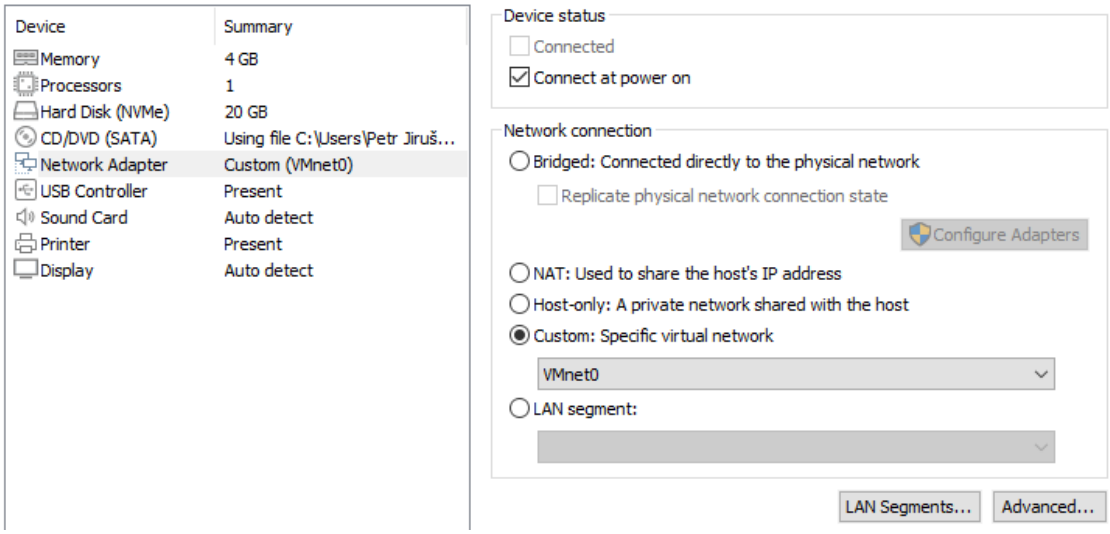
7.2 Schéma virtuální laboratoře – zapojení B

Virtuální laboratoř B je zapojena přímo do dané lokální sítě společně s dalšími fyzickými stroji. V této realizaci je na každém virtuálním stroji potřeba pouze jeden řadič síťového rozhraní, který je nastaven na vmnet0, tedy síť obsahující most.



Obrázek č. 10 - Zapojení virtuální laboratoře B (zdroj vlastní)

Virtuální řadič je v tomto módu připojen k fyzické síti a může tak virtuální počítač komunikovat s počítači nacházející se na fyzické síti a naopak. Síťové pakety jsou odesílány a přijímány napřímo bez dalšího směrování, jelikož virtuální počítače je v tomto režimu plnohodnotnou stanicí jako všechny ostatní připojené fyzicky. V nastavení VMPlayer se pro použití sítě s mostem nastaví následující možnost:



Obrázek č. 11 - Konfigurace přemostěné sítě (zdroj vlastní)

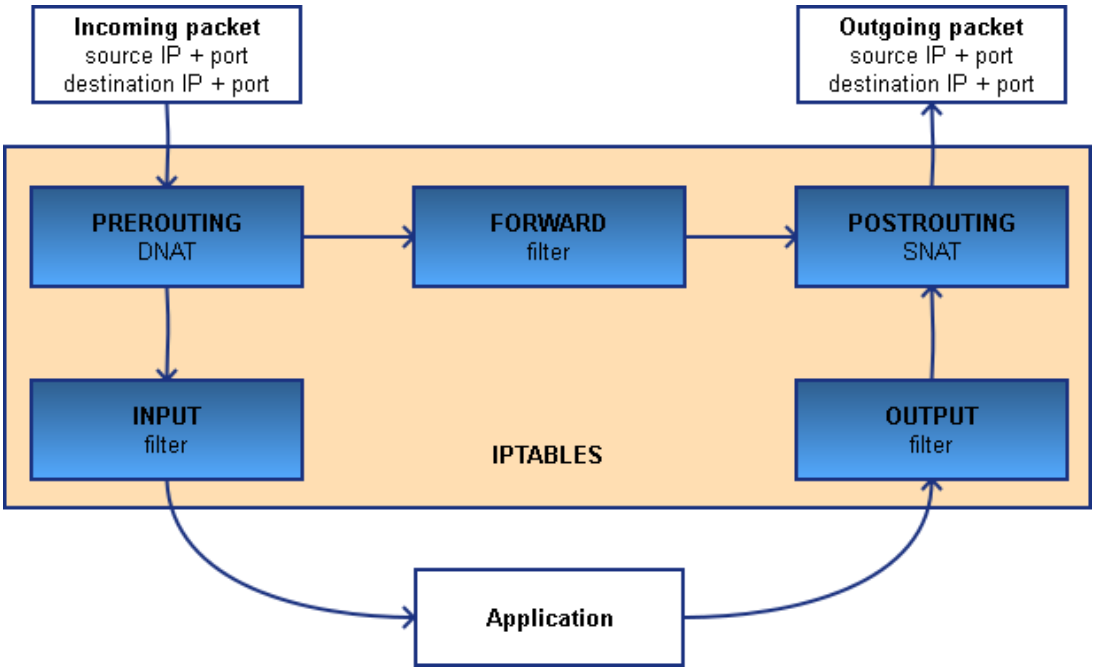
Všechny virtuální počítače přidány do sítě s mostem, v rozhraní VMPlayer pod možností sítě vmnet0 a jsou přístupné dalším fyzickým počítačům působícím v této síti. Virtuální počítače jsou součástí dané lokální sítě, ale stále jsou tyto počítače umístěné ve svém segmentu LAN a pomocí mostu se do fyzické sítě připojují. V této práci je použito právě toto zapojení, z důvodu rychlého a efektivního nasazení pro potřeby implementace síťových služeb.

8 IMPLEMENTACE SLUŽEB

V této kapitole začíná praktická část práce a je zde pospán postup implementace výše popsaných služeb. Implementace probíhá na virtuálních počítačích s operačním systémem Linux a distribucí Rocky Linux 9. Distribuce Rocky Linux byla zvolena autorem hlavně z důvodu své stability a jednoduchého zprovoznění bez nutnosti registrovat systém ani řešit jakoukoliv formu licence pro provoz. Jeden virtuální počítač vždy vystupuje v roli serveru, který implementuje zmíněné služby v rámci této kapitoly. Druhý virtuální počítač se na tento server připojuje, testuje na něm dostupnost a správné fungování služeb. Kapitola popisuje nastavení síťových služeb, jakým způsobem tyto služby komunikují, jaké používají protokoly a následně jak je lze nastavit za pomocí příkazového řádku. Jedná o základní služby běžně používané v domácích i podnikových sítích sloužící pro zvýšení zabezpečení, zcentralizování správy nebo zefektivnění práce.

8.1 Nastavení firewallu

Firewall v linuxových distribucích kontroluje příchozí a odchozí komunikaci a rozhoduje o tom jaký síťový provoz bude vpuštěn a naopak jaký bude odfiltrován. Jádro Linuxu obsahuje subsystém zvaný Netfilter, který rozhoduje o manipulaci síťového provozu na serveru. Při přijetí paketu na server je paket předán k odmítnutí, přijetí nebo manipulaci do subsystému Netfilter na základě různých pravidel obdržených od iptables.



Obrázek č. 12 - Průchod paketu přes iptables (zdroj [49])

Iptables je nástroj pro správu pravidel firewallu na linuxových distribucích. Při průchodu paketu firewallem je kontrolován jeho obsah, ten obsahuje informace o jeho cíli, původu, protokolu, který se chystá použít. V následujícím návodu je pro nastavení firewallu použit nástroj firewalld, který podobně jako iptables slouží pro správu pravidel brány firewall. Jeho konfigurace je jednodušší oproti iptables a je výchozím nástrojem firewallu pro RHEL a od něj odvozené distribuce. Dokáže nastavit složitá pravidla, která by za normálních okolností bylo obtížné nastavit do iptables. [50]

Firewalld pracuje na počítači jako služba. Spouští se ve stejnou chvíli jako počítač. V případě, zda by na konkrétním počítači nebyl ještě firewalld povolen. Lze ho spustit následujícím příkazem:

```
# systemctl enable --now firewalld
```

Příznak „--now“ spustí službu firewalld jakmile bude připravena k použití a přeskočí se tím jeden příkaz, kde by se služba musela spustit pomocí klíčového slova start. Ověřit, zda služba funguje tak jak má lze pomocí příkazu:

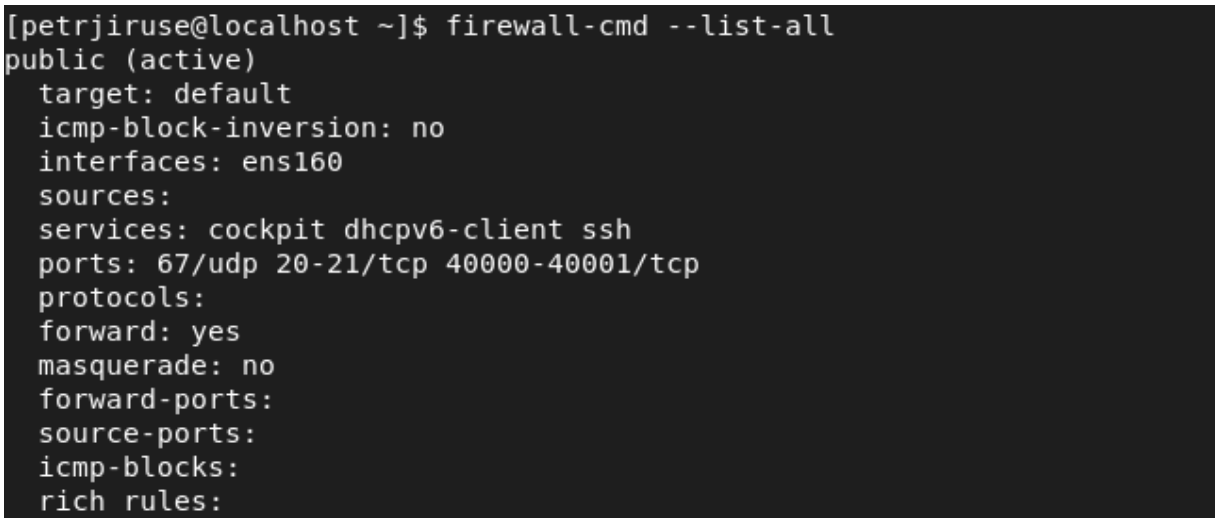
```
# systemctl status firewalld
```

Obdobně lze předchozí příkaz použít s klíčovým slovem stop pro zastavení služby. Pro tvrdý restart služby slouží příkaz s klíčovým slovem restart. Služba firewalld se konfiguruje příkazem „firewall-cmd“. Například stav brány se zkontroluje pomocí příkazu:

```
# firewall-cmd --state
```

Při provedení trvalých změn na firewallu je potřeba firewall znovu načíst, aby se změny projevily. V tomto případě stačí měkký restart pomocí příznaku „--reload“. Zároveň všechny změny na firewallu, které nebyly označeny jako trvalé zmizí. Ve výchozím nastavení jsou všechny změny provedené na firewallu dočasné. Nejlepší je otestovat změny, které chce uživatel provést jednu po druhé za běhu a v případě, že by se uživatel zablokoval nebo jiným způsobem službě znemožnil její chod, tak může systém restartovat a vrátit se k původní funkční konfiguraci. Teprve pokud jsou změny otestované a funkční je vhodné je nastavit jako permanentní. Pokud si je uživatel tedy naprosto jistý, co dělá nastaví pravidlo jako trvalé příznakem „--permanent“. Všechny změny a nastavení lze najednou zobrazit příkazem:

```
# firewall-cmd --list-all
```



Obrázek č. 13 - Ukázka výpisu konfigurace firewallu (zdroj vlastní)

Pokud chce uživatel zobrazit v jaké výchozí zóně se jeho systém nachází, může zadat příkaz:

```
# firewall-cmd --get-default-zone
```

Pro zobrazení všech zón, které jsou aktivní na daném systému se používá příznak „--get-active-zones“. Zóna může být aktivní pouze v případě, že je přiřazena k síťovému rozhraní a jsou jí přiřazené zdrojové IP adresy nebo rozsahy sítí. Výchozí zónu lze změnit použitím příkazu:

```
# firewall-cmd --set-default-zone [zvolená zóna]
```

Zónu lze přidat danému rozhraní pomocí příkazu:

```
# firewall-cmd --zone=[zvolená zóna] --add-interface=[síťové zařízení]
```

Podobnými příkazy lze měnit rozhraní pro dané zóny příznakem „--change-interface“ nebo odebírat rozhraní za použití příznaku „--remove-interface“. [38]

Při práci s firewallem je důležité rozumět konceptu portů. Port je v podstatě virtuální koncový bod, který spojuje dva počítače, tak aby si mohli mezi sebou posílat informace. Každý port má přiřazené svoje číslo a některé porty jsou rezervovány pro konkrétní služby. Například port 80 umožňuje posílat data přes protokol HTTP a port 443 je rezervován pro protokol HTTPS, což je v podstatě HTTP, ale používá šifrování. Pro zobrazení všech portů, které jsou na systému otevřené lze zjistit za použití příkazu:

```
# firewall-cmd --list-ports
```

Přidání nového portu do zóny firewallu se provede pomocí následujícího příkazu:

```
# firewall-cmd --zone=public --add-port=9001/tcp
```

V tomto případě se přidá port 9001 do zóny se stupněm public. Pro úspěšnost operace musí být port 9001 otevřený. Koncovka „/tcp“ v příkazu říká firewallu, že připojení budou probíhat přes protokol TCP, který se používá většinou pro věci týkající se serverů a domácností. Odebrání portu probíhá takřka stejně jako přidání, stačí zaměnit příznak „--add-port“ příznakem „--remove-port“. [38]

Démon firewalld je nastaven, tak aby většinu standardizovaných služeb byl schopen otevřít kdykoliv je potřeba. Tento způsob je preferovaný pro otevírání nejběžnějších portů pro služby, jako jsou HTTPS, FTP, SSH či Samba. Získání seznamu všech dostupných služeb, které mohou být potencionálně přidány do firewallu lze za pomocí příkazu:

```
# firewall-cmd --get-services
```

Naopak pro získání seznamu služeb již běžících na firewallu se použije příznak „--list-services“. Přidání služby do firewallu probíhá pomocí:

```
# firewall-cmd --zone=public --add-service=[název služby]
```

Odebírání probíhá stejný způsobem za použití „--remove-service“. [38]

V některých případech je zapotřebí zprivatizovat server a definovat kdo k němu může přistupovat přes SSH nebo si prohlížet soukromé webové stránky. Pomocí firewallu lze toho stavu dosáhnout zvolením jedné z více restriktivních zón, přidat k ní své síťové zařízení, přidat službu SSH a poté přidat vlastní veřejnou adresu IP na seznam povolených adres příkazem:

```
# firewall-cmd --permanent --zone=trusted --add-source=192.168.0.118
```

Obdobně lze adresu IP odebrat ze seznamu povolených adres za použití příznaku „--remove-source“. V případě, že se jedná o vzdálený webový server s webovou stránkou, která je veřejná, a přesto chce správce otevřít SSH spojení pouze pro jednu adresu IP nebo rozsah adres lze toho dosáhnout pomocí využití takzvaného „rich rule“. V praxi vypadá příkaz takto:

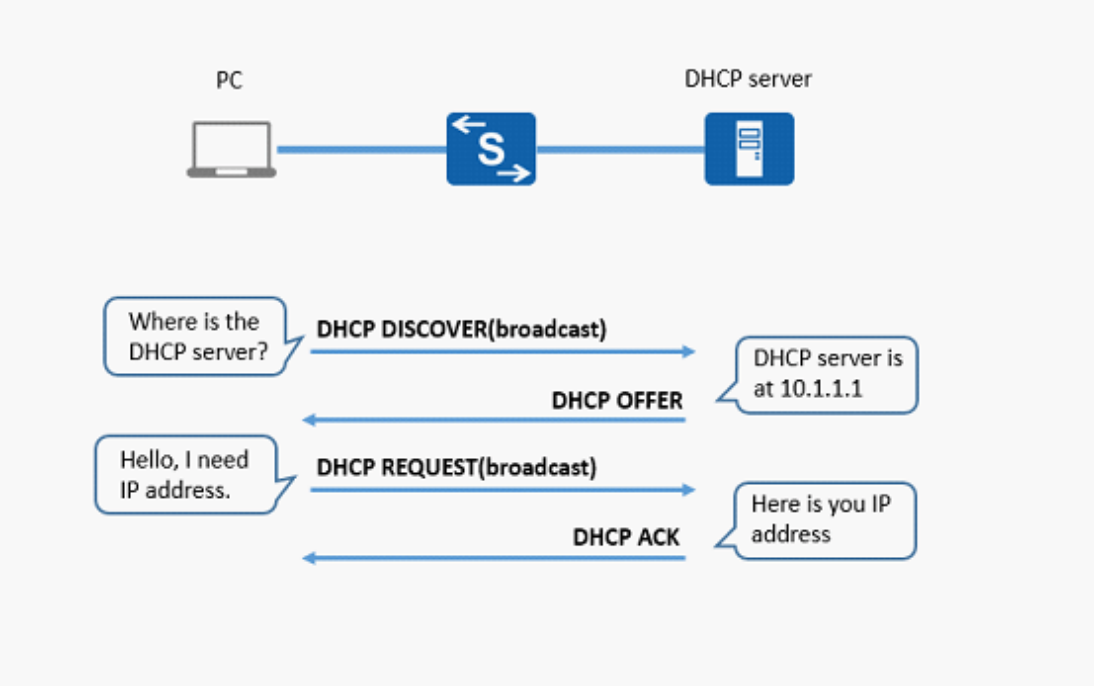
```
# firewall-cmd --permanent --zone=public --add-rich-rule='rule family="ipv4" source address="192.168.0.118/24" service name="ssh" accept'
```

Při aplikaci „rich rule“ není doporučeno dělat trvalé změny na firewallu. Nejdříve je doporučeno odstranit službu SSH z konfigurace veřejné zóny a otestovat připojení, zda se lze stále připojit na server pomocí SSH. Další řešení této problematiky, kdy je potřeba otevřít spojení pouze pro omezený kruh adres, je používání dvou různých zón najednou. Za předpokladu, že je rozhraní navázáno na veřejnou zónu, může správce přidat další zónu přidáním zdrojové adresy IP nebo rozsahu adres, jak je uvedeno výše. Poté odstraní službu SSH

z veřejné zóny a přesune jí do nové, kterou vytvořil. Nutno zdůraznit, že předchozí techniky fungují pouze za předpokladu používání statické adresy. Pokud se adresa mění při každém restartu modemu dojde k uzamčení serveru a správce ztratí přístup. V místní síti, kde správce ovládá všechny počítače a může jim nastavit ručně adresy IP lze tyto pravidla používat bez omezení. [38]

8.2 Nastavení serveru DHCP

Zprovozněním serveru DHCP v síti dojde k zcentralizování správy. Jednotlivé počítače při připojení do sítě získají potřebnou konfiguraci pro komunikaci v síti, konfigurace obsahuje informace o adrese IP, masce podsítě, adresu výchozí brány, serveru DNS a dalších věcech potřebných pro komunikaci. Stručně řečeno klient vyšle do sítě zprávu pomocí broadcastu a dostupné servery DHCP mu odpoví. Princip fungování procesu, kdy se klient připojuje do sítě a získá potřebné informace pro komunikaci se skládá ze čtyřech základních kroků. [51], [52]



Obrázek č. 14 - Komunikace serveru DHCP a klienta (zdroj [53])

1. Klient vyšle do sítě zprávu DHCPDISCOVER. Klient odesílá požadavek z portu 68 pomocí protokolu UDP. Zdrojová adresa zprávy je 0.0.0.0, jelikož klient zatím postrádá jakoukoliv síťovou konfiguraci. Cílová adresa zprávy je 255.255.255.255 (broadcast), na tuto zprávu odpoví všechny právě dostupné servery DHCP v síti.

2. Všechny dostupné servery odpoví zprávou DHCPOFFER. Zprávu server odesílá z portu 67 (protokol UDP), který je pro servery DHCP rezervovaný. Server DHCP touto zprávu nabízí klientovi konfiguraci. Zpráva je doručena všem počítačům v síti, jelikož server zatím neví adresu klienta.
3. Klient si vybere jednu konfiguraci z dostupných nabídek a odpoví zprávou DHCPREQUEST zpátky serveru DHCP.
4. Server DHCP přiřadí klientovi danou konfiguraci a pošle mu zprávu DHCPACK. Zpráva obsahuje informace o adrese IP, času zapůjčení konfigurace a dalších detailech.

Pokud klient chce nadále využívat zapůjčenou adresu, včas před skončením doby zapůjčení si může zažádat o prodloužení pomocí zprávy DHCPREQUEST. Pokud server DHCP povolí nadále využívat danou konfiguraci, odpoví zprávou DHCPACK. V případě, že klient už nepotřebuje zapůjčenou konfiguraci odešle serveru zprávu DHCPRELEASE. Server zařadí tuto konfiguraci mezi volné k dalšímu zapůjčení. [52]

Před instalací samotného serveru DHCP je vhodné zkontrolovat verzi správce balíčků, případně provést aktualizaci. Pro stažení a instalaci serveru DHCP se použije příkaz:

```
# sudo dnf install dhcp-server
```

Po instalaci je nutné nakonfigurovat soubor s informacemi pro server DHCP. Tento soubor se nachází v adresáři „/etc/dhcp/dhcpd.conf“. V tomto souboru se nastaví základní údaje o rozsahu adres, které bude server propůjčovat, adresa výchozí brány a adresa serveru DNS. Po nastavení a uložení všech potřebných informací je možné server DHCP povolit a spustit pomocí příkazů:

```
# sudo systemctl start dhcpd

# sudo systemctl enable dhcpd
```

Pokud po provedení předchozích příkazů není vypsána v terminálů žádná zpráva, server DHCP se úspěšně spustil. Dalším krokem je nakonfigurovat firewall pro otevření portu 67 a umožnění klientům komunikovat se serverem. Následně je firewall potřeba znovu spustit pro aplikaci změn. [54]

```
# sudo firewall-cmd --add-port=67/udp --permanent
```

Pokud je potřeba klientovi přiřadit specifickou statickou adresu, lze toho docílit přidáním jeho fyzické MAC adresy a požadované adresy IP do konfiguračního souboru serveru DHCP.

```
host klient1 {
```

```
 hardware ethernet 00:0C:29:8C:64:99;
 fixed-address 192.168.0.150;
}
```

Funkčnost přiřazování adres počítačům se v tomto případě ověří pomocí spuštění druhého virtuálního počítače sloužící jako klient. Na klientovi se spustí příkaz ifconfig a ověří se, zda dostal přiřazenou adresu. Pro názornost je klientovi přiřazena konkrétní adresa podle adresy MAC z konfiguračního souboru, která je zmíněná výše. [54]

```
[petrjiruse@localhost ~]$ ifconfig
ens160: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.150  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::20c:29ff:fe8c:6499  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:8c:64:99  txqueuelen 1000  (Ethernet)
        RX packets 51  bytes 6536 (6.3 KiB)
        RX errors 0  dropped 10  overruns 0  frame 0
        TX packets 70  bytes 7822 (7.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Obrázek č. 15 - Výpis síťové konfigurace klienta (zdroj vlastní)

8.3 Nastavení serveru FTP

Protokol FTP je nejčastější způsob pro přenos souborů. FTP pracuje podle standardu klient/server, tudíž je zapotřebí mít server s nakonfigurovaným protokolem FTP a klienta s nástroji umožňující se mu připojit na server FTP. Server FTP uchovává data a klient během přenosu nahrává svá data nebo stahuje ty, které server uchovává. Klient se nejčastěji připojuje na server FTP pomocí portu 21 a datový přenos probíhá přes port 20. Pro samotný přenos dat se využívá protokol TCP. Komunikace začíná synchronizovaným příkazem klienta na server. Pokud server odpoví a klient úspěšně projde autorizací, je mu umožněn přístup k souborům na serveru. Typicky existují souběžně dvě spojení mezi klientem a serverem. Připojení pro přenos dat a řídící připojení. Pokud klient spustí příkaz pro spuštění datového přenosu, je zkoumáno, zda soubor existuje a zda klient má dostatečné oprávnění pro tento soubor. V případě, že všechno proběhne v pořádku server odpoví kladně a přenos souboru začne. [55]

První krokem v nastavení serveru na systému je instalace démona vsftpd. To se provede pomocí příkazu:

```
# sudo dnf install vsftpd
```

Následně je potřeba démona vsftpd povolit, avšak nezapínat ho ještě. Povolení démona se provede příkazem:

```
# sudo systemctl enable vsftpd
```

Obecně platí, že po instalaci vsftpd jsou již nastaveny nejrozumnější možnosti, ale je dobré se ujistit, které nastavení jsou povolena nebo zakázána. Potřebný konfigurační soubor se nachází v souboru „/etc/vsftpd/vsftpd.conf“. Důležité je zkontrolovat, zda řádek „anonymous_enable=“ je nastaven na hodnotu NO a není okomentovaný. Pokud by byl označen komentářem znamenalo by to povolení anonymních přihlášeních. [44], [56]

Pokud tato informace souhlasí zapnutí démona proběhne příkazem:

```
# sudo systemctl start vsftpd
```

Funkčnost démona se dá ověřit příkazem:

```
# sudo systemctl status vsftpd
```

Před tím, než se začnou provádět změny v konfiguračním souboru démona vsftpd, je vhodné vytvořit si jeho kopii, aby v případě nefungující konfigurace se daly změny jednoduše navrátit do původní podoby. Kopírování konfiguračního souboru se provede příkazem „cp“:

```
# sudo cp /etc/vsftpd/vsftpd.conf /etc/vsftpd/vsftpd.conf.bak
```

Další krokem po vytvoření kopie, je konfigurovat server FTP pro lokální uživatele a nastavit potřebná práva na základě loginů. Nejprve je potřeba vstoupit do originálního konfiguračního souboru a změnit následující řádek na:

```
allow_writeable_chroot=YES
```

Tento řádek umožní lokálním uživatelům přistupovat do složky chroot. Pokud není okomentovaný řádek:

```
chroot_local_user=YES
```

Způsobí tento řádek, že domovské adresáře uživatelů budou uzamčeny ve složce chroot, což znamená, že démon vsftpd nepovolí zápis do domovských adresářů uživatelů z bezpečnostních důvodů. Nastavení řádku „allow_writeable_chroot“ na „YES“ vypne uzamykání domovských adresářů pro zápis. Záleží na prioritách a v jakém prostředí se server FTP bude využívat, jelikož povolení tohoto zápisu může vést k bezpečnostním zranitelnostem. Vhodné je také nastavit číselný rozsah pasivních portů pro otevírání připojení od klienta k serveru a využívání dalších příkazů, jako například příkazu „ls“ sloužící pro zobrazení obsahu aktuálního adresáře. Pro aktivaci pasivního režimu je nutné přidat do konfiguračního souboru následující řádky. [56]

```
pasv_min_port=40000
pasv_max_port=40001
```

Kompletní podoba konfiguračního souboru démona vsftpd je k nalezení v přílohách tohoto souboru.

Nyní je načase vytvořit profily uživatelů, pod kterými se budou lokální uživatelé přihlašovat na server FTP. Nový uživatel je vytvořen za pomoci:

```
# sudo useradd ftpuser
```

Následně mu změnit heslo příkazem:

```
# sudo passwd ftpuser
```

Heslo musí mít alespoň 8 znaků, musí obsahovat alespoň 3 ze 4 typů znaků (malá písmena, velká písmena, číslice, speciální znaky) a nesmí se shodovat se jménem uživatele. Nově vytvořený uživatel musí být zahrnut v souboru „/etc/vsftpd.user“, aby měl přístup k serveru FTP. To lze docílit pomocí příkazu echo společně s přepínačem „-a“ pro připojení údaje na konec souboru. [56]

```
# echo "ftpuser" | sudo tee -a /etc/vsftpd.userlist
```

Následujícím krokem je vytvořit dva adresáře a nastavit jim oprávnění. Jeden z adresářů bude vytvořen pod rodičovským adresářem a bude sloužit pro nahrávání nebo stahování souborů. [56]

```
# sudo mkdir -p /home/ftpuser/ftp/files
```

Příznak „-p“ způsobí vytvoření podadresáře v rodičovském adresáři, pokud rodičovský adresář ještě neexistuje, je vytvořen. Z důvodu bezpečnosti je vhodné odebrat práva pro zápis do adresáře „ftp“ a změnit jeho vlastníka na uživatele „nobody“. [56]

```
# sudo chown nobody: /home/ftpuser/ftp
# sudo chmod a-w /home/ftpuser/ftp
```

Obdobně se nastaví práva na druhý adresář.

```
# sudo chown -R ftpuser: /home/ftpuser/ftp/files
# sudo chmod -R 750 /home/ftpuser/ftp/files
```

Nově nastavená oprávnění lze ověřit zadáním příkazu:

```
# sudo ls -la /home/ftpuser/ftp
```

Pro účely testování je vhodné vytvořit textový soubor v adresáři „files“.

```
# echo "ftp_test_File" | sudo tee -a /home/ftpuser/ftp/files/ftptest.txt
```

Poslední krokem v zprovoznění serveru FTP je nastavení pravidel firewallu, tak aby povolil porty 20 a 21 pro FTP. Dále jsou také potřeba porty 40000 a 40001 pro pasivní komunikaci vsftpd. Příkazy pro nastavení firewallu jsou následující:

```
# sudo firewall-cmd --permanent --add-port=20-21/tcp
# sudo firewall-cmd --permanent --add-port=40000-40001/tcp
# sudo firewall-cmd --reload
```

Po nastavení firewallu je nutno restartovat službu vsftpd a zkontrolovat její stav za pomocí příkazu „status“ zmíněný výše. [56]

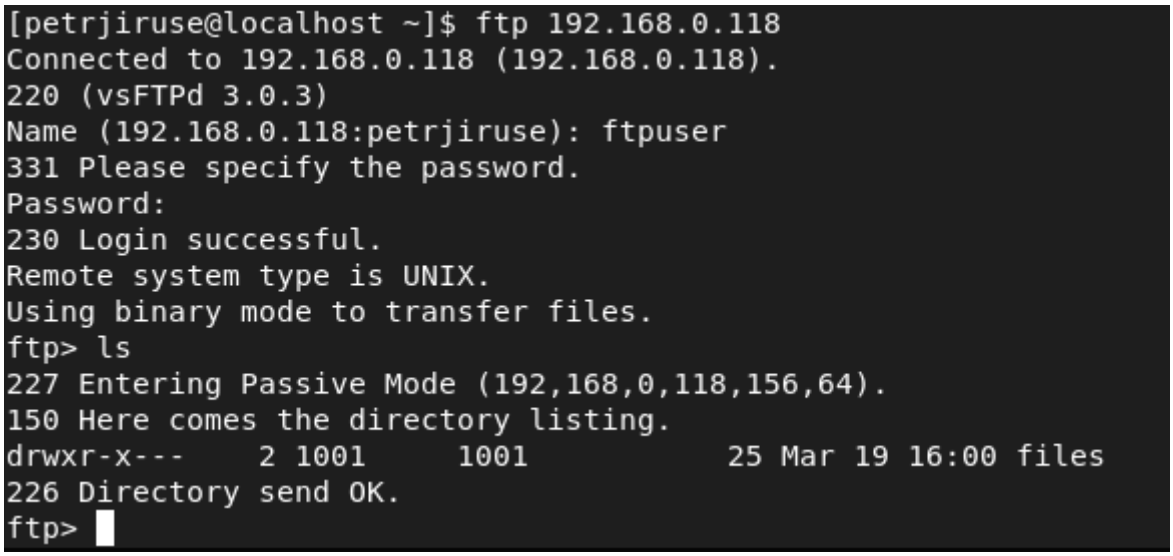
Poté co je server FTP nakonfigurován je možné se přesunout ke klientovi a otestovat jeho připojení na server. V případě, že klient ještě nemá balíček nástrojů pro klienta FTP, lze tento balíček doinstalovat příkazem:

```
# sudo dnf install ftp
```

V případě pokusu o připojení bez potřebných nástrojů k serveru FTP je uživatel vyzván k instalaci nástrojů. Po nainstalování potřebných nástrojů se lze připojit na server FTP příkazem „ftp“ a adresy serveru.

```
# ftp 192.168.0.118
```

Po zadaní příkazu uživatel musí zadat přihlašovací jméno a heslo, pokud jsou přihlašovací údaje validní je navázáno spojení se serverem FTP. Po připojení je možné zjistit obsah aktuálního adresáře s pomocí pasivního módu. [56]



Obrázek č. 16 - Připojení klienta na server FTP (zdroj vlastní)

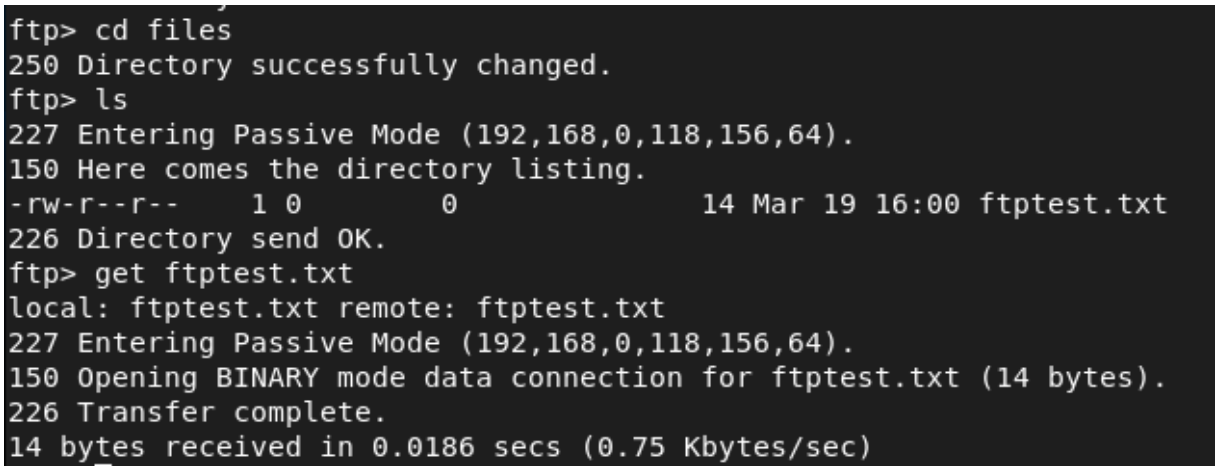
Následně se testuje, zda lze ze serveru FTP získat předtím vytvoření testovací soubor „ftptest.txt“. Soubory se dají stahovat za použití příkazu „get“. Předtím než lze stahovat je potřeba přejít do korektního adresáře uchovávající soubory ke stažení. Adresář se mění příkazem „cd“ a adresář nebo cesta k adresáři. [56]

```
ftp> cd files
```

Po přesunu do správného adresáře se soubor stáhne zadáním příkazu:

```
ftp> get ftptest.txt
```

Po zadání požadavku na stažení existujícího souboru na serveru se provede převod souboru ze serveru na klienta.



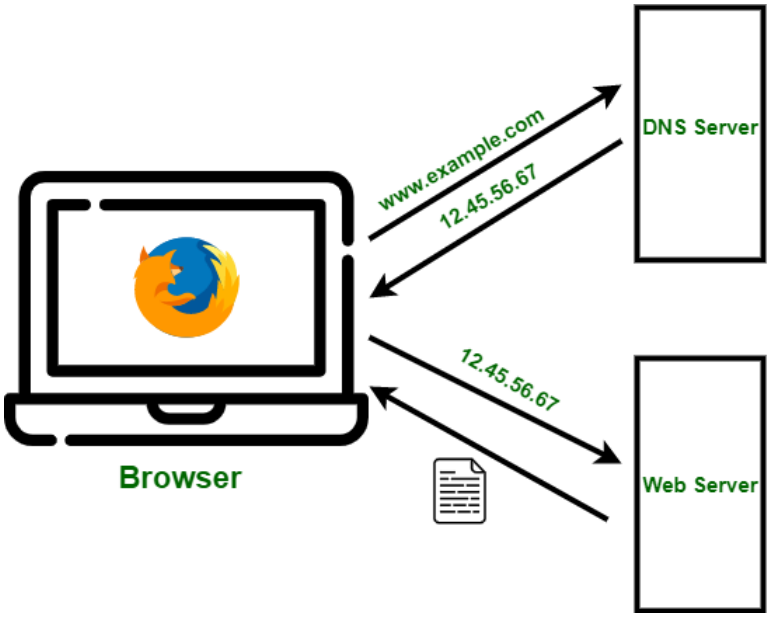
Obrázek č. 17 - Výsledek stahování souboru ze serveru FTP (zdroj vlastní)

Z výstupu terminálu lze vidět, že převod proběhl v pořádku. Obdobně jde soubory na server vkládat, akorát na místo příkazu „get“ se použije příkaz „put“ a název souboru. Po skončení interakce se serverem FTP se uživatel dá odpojit zadání příkazu „bye“. [56]

```
ftp> bye
```

8.4 Nastavení lokálního serveru DNS

Služba DNS umožňuje použití doménových jmen na místo adres IP v síti. V praxi to znamená, že služba DNS je spuštěna na počítači, který obsahuje databázi doménových jmen a informace o stromové struktuře domén DNS.



Obrázek č. 18 - Princip komunikace při překladu adres pomocí DNS (zdroj [57])

Server DNS zpracovává dotazy klientů, pokud daný server DNS nemůže poskytnout přesné informace o dané doméně, poskytne alespoň ukazatel na další server, který může vyřešit dotaz. Programy, které používají dotazy DNS k dotazování na informace od serverů se nazývají resolvery DNS. Tyto resolvery mohou komunikovat s místním serverem DNS nebo se vzdálenými servery DNS. Servery DNS používají pro svou funkci protokoly TCP a UDP. Jejich komunikace probíhá přes port 53. [43]

Pro vytvoření místního serveru DNS, který nebude vystavován vnějšímu světu bude stačit nástroj zvaný bind. Nástroj bind se instaluje pomocí balíčků následujícím příkazem:

```
# dnf install bind bind-utils
```

Démon pro nástroj bind se nazývá named a pro jeho fungování je potřeba povolit spouštění při bootování systému. [42]

```
# systemctl enable named
```

Následně je nutno daný démon zapnout pomocí obdobného příkazu a klíčového slova start.

```
# systemctl start named
```

Pro konfiguraci serveru DNS je potřeba upravit obsah souboru „/etc/named.conf“. První věc, která je potřeba nastavit v tomto souboru, je vypnout naslouchání na localhostu, což se provede označením dvou řádků v sekci options znakem „#“. Konfigurace tak vypadá následovně:

```
options {
#       listen-on port 53 {127.0.0.1;};
#       listen-on-v6 port 53 {::1; };
```

Tato konfigurace efektivně vypne jakékoliv spojení s vnějším světem. V praxi to znamená, že server DNS reaguje pouze tehdy, když je adresa IP požadující službu lokální a neodpovídá vůbec pokud daná služba je vyhledávána na internetu. V dalším kroku je potřeba nastavit sekci pro místní síť, která se nachází na konci souboru „named.conf“. Následující příklad demonstruje vytvoření záznamu pro doménu „example“. [42]

```
//dopředná zóna
zone "example.lan" IN {
    type master;
    file "example.lan.db";
    allow-update { none; };
   allow-query {any; };
};
//reverzní zóna
zone "1.168.192.in-addr.arpa" IN {
    type master;
    file "example.lan.rev";
    allow-update { none; };
   allow-query { any; };
};
```

Po provedení a uložení všech změn uživatel nyní musí vytvořit dva soubory v „/var/named“. Tyto soubory se poté upravují v případě, že do sítě se přidávají stroje, které mají využívat služeb serveru DNS. Prvním soubor je určen pro mapování uživatelské adresy IP na název hostitele.

Nově vytvořený soubor pro doménu example se nazývá „/var/named/example.lan.db“. Nastavený soubor pro překlad adresy IP na název vypadá takto:

```
$TTL 86400
@ IN SOA dns-primary.example.lan. admin.example.lan. (
   2019061800 ;Serial
   3600 ;Refresh
   1800 ;Retry
   604800 ;Expire
   86400 ;Minimum TTL
)
@ IN NS dns-primary.example.lan.
//Adresa IP jmenného serveru
dns-primary IN A 192.168.0.118
server      IN A 192.168.0.118
desktop     IN A 192.168.0.150
```

Do souboru lze přidat neomezený počet adres IP, které mají být serverem DNS přeloženy. Oba soubory používají určitou terminologii. Vysvětlení jednotlivých výrazů je následující:

1. TTL (Time To Live) – tento záznam říká serveru, jak dlouho má uchovávat obsah mezipaměti, než zažádá o novou kopii. Hodnota se určuje v sekundách a výchozí hodnota je 86400 sekund (24 hodin).
2. IN – zkratka pro Internet, jelikož v tomto návodu je popisováno nastavení lokálního serveru, význam této zkratky je spíše Intranet.
3. SOA (Start Of Authority) – udává primární server pro doménu
4. NS – zkratka pro Name Server
5. Serial – záznam, podle které server DNS pozná, zda je obsah souboru zóny aktuální.
6. Refresh – určuje, jak často má podřízený server DNS provádět přenos zóny z hlavního serveru.
7. Retry – čas v sekundách po jaké době server DNS opětovně zkusí provést přenos zóny, pokud nastalo selhání u předchozího přenosu
8. Expire – čas v sekundách specifikující, jak dlouho má podřízený server čekat, pokud je hlavní server nedostupný
9. A – adresa hostitele nebo dopředný záznam

10. PTR – ukazatel na reverzní záznam, poskytuje doménové jméno spojené s adresou IP [42]

Druhý potřebný soubor „/var/named/example.lan.rev“ je reverzní soubor ukládající informace k mapování názvu hostitele na adresu IP. V tomto případě je potřeba pouze poslední oktet adresy IP hostitele a poté PTR společně s názvem hostitele. Příklad souboru s reverzními záznamy:

```
$TTL 86400
@ IN SOA dns-primary.example.lan. admin.example.lan. (
   2019061800 ;Serial
   3600 ;Refresh
   1800 ;Retry
   604800 ;Expire
   86400 ;Minimum TTL
)
@ IN NS    dns-primary.example.lan.
@ IN PTR  example.lan.
dns-primary IN A 192.168.0.118
server          IN A 192.168.0.118
desktop        IN A 192.168.0.150
118 IN PTR dns-primary.example.lan.
150 IN PTR desktop.example.lan.
```

Po vytvoření je nutné ověřit, zda konfigurační soubory a zóny jsou ve funkčním stavu předtím, než je opětovně spuštěna služba bind. Hlavní konfigurace lze zkontrolovat příkazem:

```
# sudo named-checkconf
```

Pokud je všechno v pořádku tento příkaz vrací prázdný výsledek. Dále je doporučeno zkontrolovat dopřednou a reverzní zónu pomocí „named-checkzone“. Pro dopřednou zónu:

```
# sudo named-checkzone example.lan /var/named/example.lan.db
```

Následně příkaz pro reverzní:

```
# sudo named-checkzone 192.168.0.118 /var/named/example.lan.rev
```

Oba příkazy vrací v případě úspěchu název zóny následovanou hláškou „OK“. [42]

```
[root@server named]# named-checkzone example.lan /var/named/example.lan.db
zone example.lan/IN: loaded serial 2019061800
OK
[root@server named]# named-checkzone 192.168.0.118 /var/named/example.lan.rev
zone 192.168.0.118/IN: loaded serial 2019061800
OK
```

Obrázek č. 19 - Testování dopředné a reverzní zóny DNS (zdroj vlastní)

Dále je server DNS je dále přidán do seznamu aktivních serverů DNS na všech klientech, kteří mají mít k doméně přístup a stává se tak aktivním v síti. Tato akce je provedena příkazem:

```
# nmcli con mod ens160 ipv4.dns '192.168.0.118'
```

8.5 Nastavení webového serveru Apache

Software Apache spravující webový server má za úkol především navazovat spojení mezi serverem a prohlížeči klientů, kteří se k serveru připojují. Po navázaném spojením s klientem Apache doručuje soubory ze serveru a zpět, jako klasická struktura klient-server. Při požadavku klienta o načtení webové stránky vyšle jeho prohlížeč požadavek na server a Apache odpoví ve formě souborů, obsahující texty, obrázky, formuláře a další elementy nacházející se na webových stránkách. Server a klient komunikují mezi sebou pomocí protokolu HTTP a Apache je zodpovědný za bezproblémovou komunikaci mezi těmito dvěma stroji. Pro realizaci webových stránek je zapotřebí mít nainstalovanou verzi PHP a případně nějakou databázi. Z repositářů Rocky Linux lze získat nejnovější verzi PHP společně s httpd. V průběhu provozování webu budou možná potřeba i balíčky php-bcmath nebo php-mysqlind, které však jdou jednoduše doinstalovat. Tento návod se věnuje základnímu nastavení webového serveru Apache a jejím cílem je vytvořit funkční webovou stránku přístupnou z lokální sítě. [58], [59]

Základem je mít nainstalované httpd. Pro instalaci httpd se použije příkaz:

```
# dnf install httpd
```

Po dokončení instalace httpd je nutné zkontrolovat nastavení konfigurace. Konfigurační soubor se nachází v adresáři „/etc/httpd/conf/httpd.conf“. Řádky, které je nutno zkontrolovat jsou „DocumentRoot /var/www/html“ a „Listen 80“. První řádek udává výchozí adresář webového

serveru a druhý říká, na kterém portu služba má poslouchat. Pro spuštění webového serveru se použije příkaz:

```
# sudo systemctl start httpd
```

Jeho úspěšné spuštění lze ověřit příkazem:

```
# sudo systemctl status httpd
```

Pokud by správce chtěl spouštět službu httpd automaticky po každém startu systému použil by proto příkaz:

```
# sudo systemctl enable --now httpd
```

Dalším krokem konfigurace je otevřít firewall pro povolení provozu HTTP. Prvním příkazem se přidá služba http do firewallu. [60]

```
# sudo firewall-cmd --permanent --zone=public --add-service=http
```

Následně je potřeba firewall restartovat:

```
# sudo firewall-cmd --reload
```

Pro kontrolu se uživatel muže podívat do výpisu konfigurace firewallu v řádku „services“, že se zde nachází služba http. Konfigurace firewallu pro public zónu se zobrazí příkazem:

```
# sudo firewall-cmd --list-all --zone=public
```

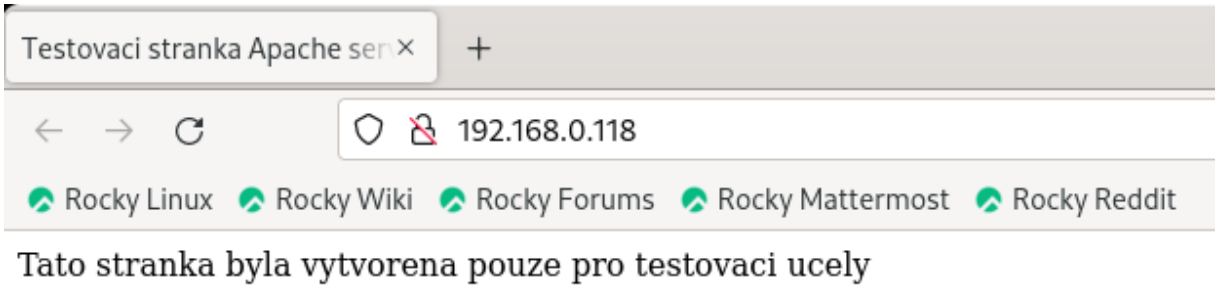
Funkčnost serveru lze dále zkontrolovat přímo v prohlížeči zadáním adresy „localhost:80“ výsledkem v aktuálním stavu by měla být výchozí stránka webového serveru Apache. Pro další účely testování lze vytvořit v adresáři „/var/www/html“ triviální soubor index.html pro simulaci webové stránky nebo případně i vložit celý stažený web do tohoto adresáře. Do tohoto adresáře lze přidávat i soubory ke stažení, pro demonstraci je vytvořen soubor „testovaci-soubor.txt“. Soubory lze následně stáhnout z webového serveru pomocí nástrojů curl a wget z příkazové řádky. [60]

V dalším kroku je otestován webový server pomocí jiného počítače nacházejícího se ve stejném segmentu sítě. Jeden ze způsobů, jak otestovat funkčnost serveru je otevřít na klientském

počítači prohlížeč a napsat do něj adresu IP počítače, který provozuje webový server Apache. Další možností je spustit na klientském počítači příkaz firefox z terminálu. [60]

```
# firefox http://192.168.0.118
```

Výsledkem obou metod má být uvítací webová stránka, která se nachází v kořenovém adresáři webového serveru.



Obrázek č. 20 - Připojení klienta na webovou stránku na serveru Apache (zdroj vlastní)

Pro stažení souborů uložených na webovém serveru se dá použít jeden z nástrojů pro přenos souborů mezi serverem a klientem. Následující ukázka stahuje textový soubor ze serveru pomocí příkazu wget doplněný o adresu serveru a cestu k souboru. [60]

```
[petrjiruse@localhost ~]$ wget http://192.168.0.118/testovaci-soubor.txt
--2023-03-30 19:22:32--  http://192.168.0.118/testovaci-soubor.txt
Connecting to 192.168.0.118:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 67 [text/plain]
Saving to: 'testovaci-soubor.txt'

testovaci-soubor.tx 100%[===================>]      67  --.-KB/s    in 0s

2023-03-30 19:22:32 (10.9 MB/s) - 'testovaci-soubor.txt' saved [67/67]
```

Obrázek č. 21 - Stahování souboru z webového serveru (zdroj vlastní)

Na počítači provozující server, lze dodatečně ověřit přenos staženého souboru za pomoci příkazu:

```
# sudo cat /var/log/httpd/access_log | grep -I download-this.txt
```

Nyní je nastaven základní webový server Apache. Takový server postačuje pro lokální sítě, ale v případě vystavení webového serveru vnějšímu světu je nutné takový server vylepšit hlavně v ohledu bezpečnosti. Vylepšení by se týkalo především změny portu pro naslouchání požadavků na port 443 pro šifrovanou komunikaci. V dnešní době je obecně doporučeno, aby každý webový server běžel společně s SSL. Proces SSL začíná generováním soukromého klíče

a CSR neboli žádostí o podpis certifikátu. Podpis je následně zaslán certifikační autoritě za účelem zakoupení certifikátu SSL. Generování klíčů je rozsáhlé, tudíž má vlastní dokument. Klíče a soubory certifikátů jsou umístěny do souborového systému na webovém serveru. Klíče a soubory certifikátů mají být umístěny s doménou, nesmí být vloženy do kořenového adresáře (složka html), což by způsobilo bezpečnostní zranitelnosti. [59]

8.6 Vzdálená správa serveru pomocí služby Cockpit

Cockpit je nástroj pro vzdálenou správu a monitoring serverů, sponzorovaný společností Red Hat. Jeho cílem je vytvořit uživatelsky přívětivé prostředí a snadnou správu serverů odkudkoliv. Distribuce RHEL 7 obsahovala Cockpit jako doplňkovou službu a od RHEL 8 je Cockpit již ve výchozím nastavení součástí operačního systému. [61]

Hlavními benefity Cockpitu je jeho snadné používání a nenutnost konfigurovat službu po instalaci. Ve výchozím nastavení Cockpit nevyžaduje žádnou konfiguraci, avšak jeho fungování se dá na míru přizpůsobit pomocí doplňkových modulů s možností vytvářet i vlastní moduly. Poskytuje webové rozhraní, ze kterého správce může obsluhovat vícero serverů najednou. Cockpit nemá zvláštní oprávnění a nespouští se jako root. Při přihlášení se Cockpit spouští s právy přihlašovaného uživatele. Tudíž pro vykonávání administrativních operací je zapotřebí mít oprávnění k použití sudo nebo PolicyKit ke zvýšení oprávnění. [61]

Cockpit je k dispozici na mnoho linuxových distribucích, včetně Rocky Linux. Nainstalovat Cockpit, pokud již není na systému přítomen, lze příkazem:

```
# sudo dnf install cockpit
```

Následně se Cockpit povolí pomocí systemd soketu a nevyužívá žádnou operační paměť, když je v provozu.

```
# sudo systemctl enable --now cockpit.socket
```

V případě, že ještě není Cockpit povolen na firewallu, jeho povolení proběhne příkazem:

```
# sudo firewall-cmd --add-service=cockpit --permanent
```

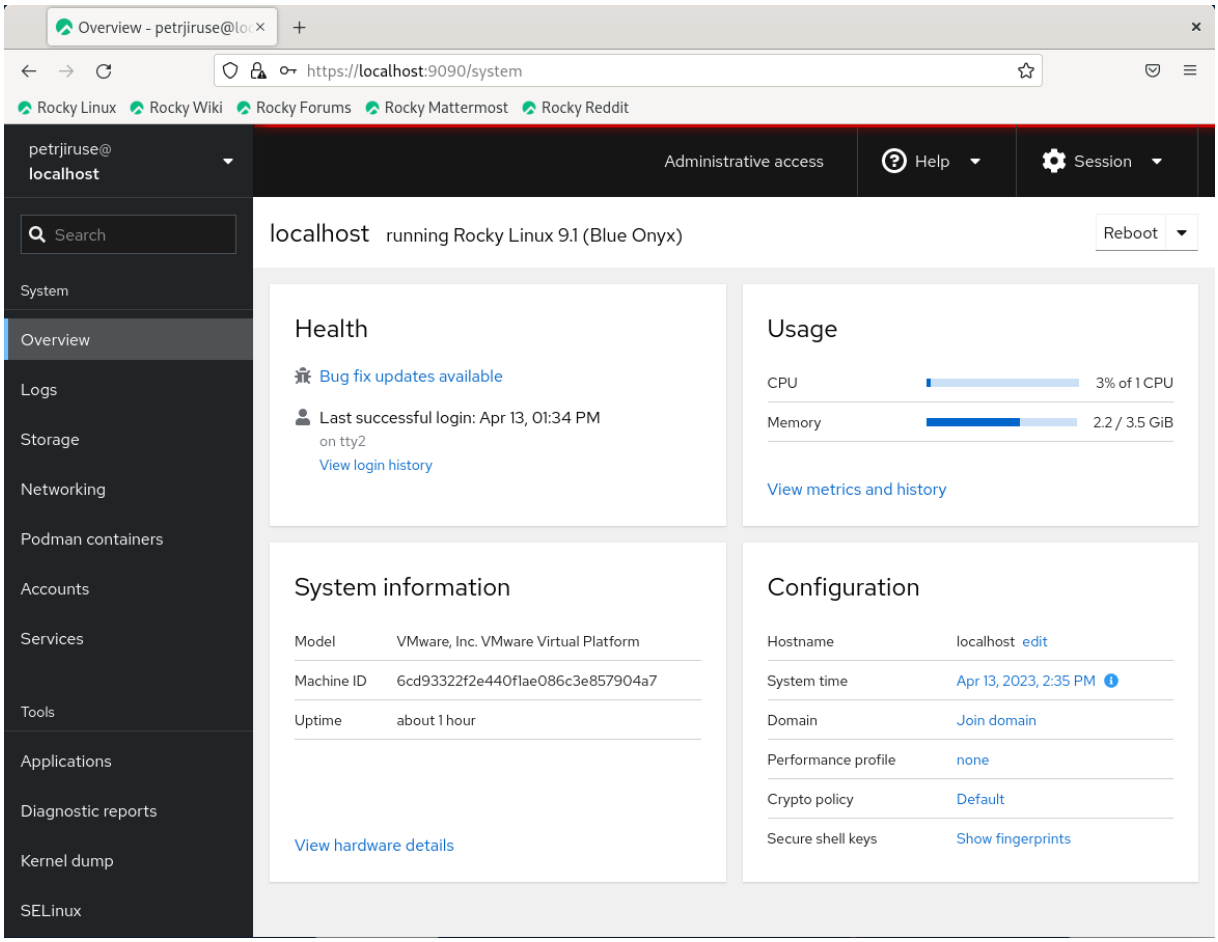
Po této změně je službu nutno restartovat.

```
# sudo firewall-cmd --reload
```

Dále není nic potřeba konfigurovat a služba Cockpit je nyní dostupná v prohlížeči na localhostu nebo na adrese IP serveru. Služba běží na portu 9090. Syntaxe požadavku v prohlížeči:

https://Adresa IP serveru:9090

Po zadaní adresy se v prohlížeči objeví přihlašovací okno, kde se uživatel přihlásí pod svým účtem a na základě toho jsou mu nastaveny oprávnění. V případě správce se může přepnout do administrativního režimu a provádět změny na serveru. [61]



Obrázek č. 22 - Ukázka rozhraní služby Cockpit (zdroj vlastní)

Rozhraní poskytuje informace o všech důležitých aspektech systému, včetně využití procesoru nebo paměti, konfiguraci systému, prohlížení logů, využití úložiště, síťovém provozu, běžících službách nebo existujících uživatelích a dalších věcech. Pomocí rozhraní lze například měnit jméno domény nebo přidávat další servery pod společnou správu zadáním adresy serveru a uživatele, pod kterým se na server má uživatel připojit. [61]

8.7 Testování služeb pomocí nástroje Wireshark

Wireshark je software používaný pro sledování síťového provozu v síti, prostřednictvím síťového rozhraní. Jedná se o nejpoužívanější nástroj pro monitorování sítě, používaný ať už síťovými experty, tak i nadšenci pro síťovou techniku. [62]

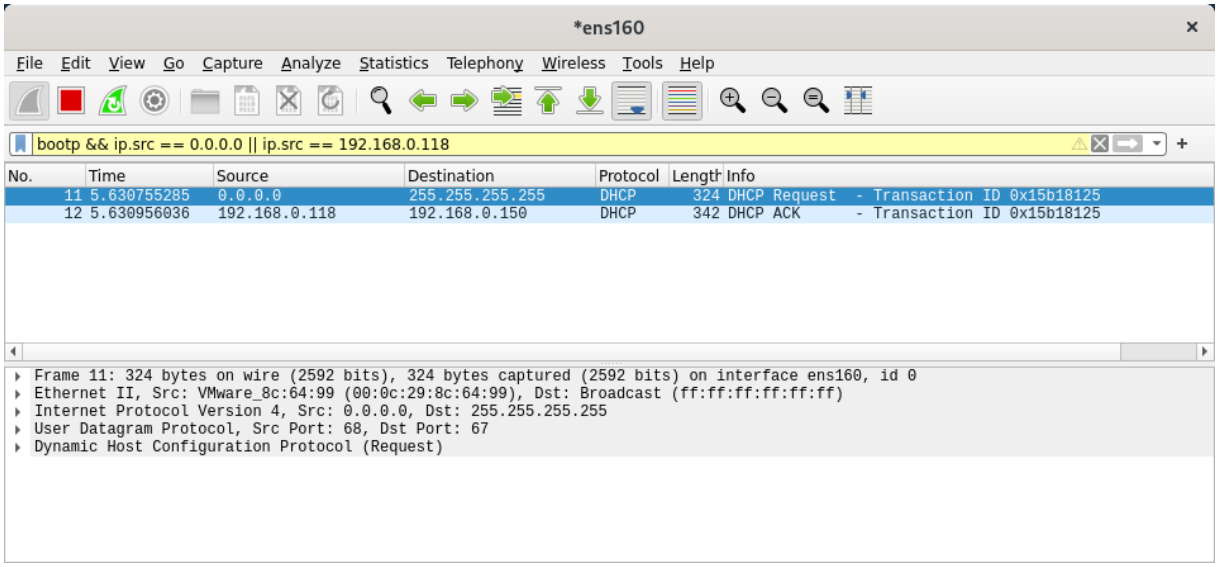
Wireshark nabízí monitorování téměř všech síťových standardů jako jsou například ethernet, wlan nebo Bluetooth. Jedná se o open-source projekt, na kterém pracuje početná komunita podporovatelů a vývojářů. Wireshark obsahuje veškeré komponenty potřebné pro analýzu a dokumentaci síťového provozu. Zachytáváním paketů Wireshark poskytuje informace o jednotlivých paketech, jako je čas přenosu, zdroj, cíl, typ protokolu nebo data hlavičky. Tyto informace mohou být užitečné při mapování zranitelnosti sítě nebo odstraňovaní problémů pro lepší zabezpečení sítě. Mimo jiné lze Wireshark použít také k odposlechu, tudíž organizace používající tento nástroj by měla mít jasně definované zásady ochrany osobních údajů. [62], [63]

Pro instalaci programu Wireshark stačí pouze příkaz:

```
# sudo dnf install wireshark
```

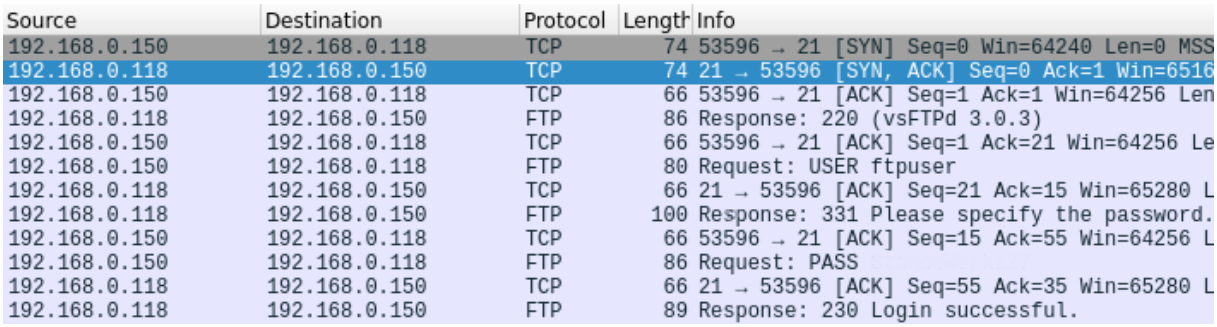
Po zapnutí Wiresharku ze záložky „Activites“ nebo pomocí příkazového řádku s názvem služby se uživateli otevře hlavní okno rozhraní. Nutné zmínit, že pro zachytávání paketů musí být uživatel přidán do skupiny „wireshark“ nebo je potřeba spustit Wireshark jako správce.

Následně je možné pakety filtrovat a zjistit tak funkčnost jednotlivých služeb běžících v síti. Pro zjištění funkčnosti serveru DHCP je třeba napsat do řádku pro filtraci slovo „bootp“, nikoliv dhcp. Na následujícím obrázku lze vidět, že nově připojený počítač do sítě žádá o přidělení konfigurace z adresy „0.0.0.0“ a posílá svůj požadavek na broadcast. Server mu pak z adresy 192.168.0.118 odpoví a přidělí mu adresu.



Obrázek č. 23 - Odchytávání DHCP paketů (zdroj vlastní)

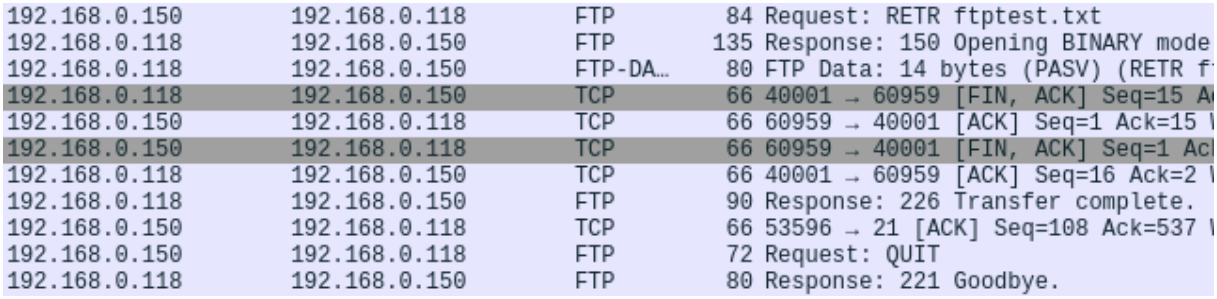
Při komunikaci klienta se serverem FTP se používá port 21 na straně serveru. Komunikace probíhá v aktivním a pasivním módu. Následující dva obrázky demonstrují komunikaci mezi klientem a serverem. Nejprve se klient přihlásí, server se zeptá na uživatelské jméno a následně heslo. V případě, že vše souhlasí server mu pošle potvrzení a přihlášení je tak úspěšné.



Source	Destination	Protocol	Length	Info
192.168.0.150	192.168.0.118	TCP	74	53596 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS
192.168.0.118	192.168.0.150	TCP	74	21 → 53596 [SYN, ACK] Seq=0 Ack=1 Win=6516
192.168.0.150	192.168.0.118	TCP	66	53596 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len
192.168.0.118	192.168.0.150	FTP	86	Response: 220 (vsFTPd 3.0.3)
192.168.0.150	192.168.0.118	TCP	66	53596 → 21 [ACK] Seq=1 Ack=21 Win=64256 Le
192.168.0.150	192.168.0.118	FTP	80	Request: USER ftpuser
192.168.0.118	192.168.0.150	TCP	66	21 → 53596 [ACK] Seq=21 Ack=15 Win=65280 L
192.168.0.118	192.168.0.150	FTP	100	Response: 331 Please specify the password.
192.168.0.150	192.168.0.118	TCP	66	53596 → 21 [ACK] Seq=15 Ack=55 Win=64256 L
192.168.0.150	192.168.0.118	FTP	86	Request: PASS
192.168.0.118	192.168.0.150	TCP	66	21 → 53596 [ACK] Seq=55 Ack=35 Win=65280 L
192.168.0.118	192.168.0.150	FTP	89	Response: 230 Login successful.

Obrázek č. 24 - Odchytávání komunikace FTP (zdroj vlastní)

Přihlášený klient může stahovat nebo nahrávat soubory do složek jemu přístupných. Klient zde posílá požadavek na stažení souboru „ftptest.txt“ a server následně vytváří datové spojení s klientem pro přenos požadovaných dat. Klient potvrdí serveru úspěšné doručení souboru a přenos je tak kompletní. Po dokončení akcí uživatel vyšle požadavek „QUIT“ pro ukončení spojení.



192.168.0.150	192.168.0.118	FTP	84	Request: RETR ftptest.txt
192.168.0.118	192.168.0.150	FTP	135	Response: 150 Opening BINARY mode
192.168.0.118	192.168.0.150	FTP-DA…	80	FTP Data: 14 bytes (PASV) (RETR f
192.168.0.118	192.168.0.150	TCP	66	40001 → 60959 [FIN, ACK] Seq=15 A
192.168.0.150	192.168.0.118	TCP	66	60959 → 40001 [ACK] Seq=1 Ack=15
192.168.0.150	192.168.0.118	TCP	66	60959 → 40001 [FIN, ACK] Seq=1 Ac
192.168.0.118	192.168.0.150	TCP	66	40001 → 60959 [ACK] Seq=16 Ack=2
192.168.0.118	192.168.0.150	FTP	90	Response: 226 Transfer complete.
192.168.0.150	192.168.0.118	TCP	66	53596 → 21 [ACK] Seq=108 Ack=537
192.168.0.150	192.168.0.118	FTP	72	Request: QUIT
192.168.0.118	192.168.0.150	FTP	80	Response: 221 Goodbye.

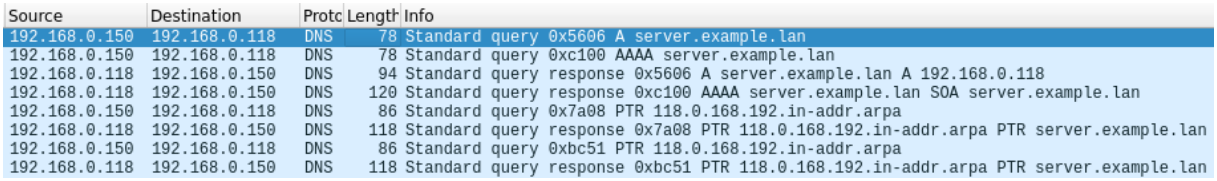
Obrázek č. 25 - Odesílání souboru ze serveru FTP na klienta (zdroj vlastní)

V případě testování serveru DNS je z klienta nacházejícího se ve stejné síti vyslán požadavek ping s názvem domény. V tomto případě se klient dotazuje na doménu „server.example.lan“.

```
[petrjiruse@desktop ~]$ ping server
PING server.example.lan (192.168.0.118) 56(84) bytes of data.
64 bytes from server.example.lan (192.168.0.118): icmp_seq=1 ttl=64 time=0.255 ms
64 bytes from server.example.lan (192.168.0.118): icmp_seq=2 ttl=64 time=0.309 ms
64 bytes from server.example.lan (192.168.0.118): icmp_seq=3 ttl=64 time=0.304 ms
64 bytes from server.example.lan (192.168.0.118): icmp_seq=4 ttl=64 time=0.302 ms
^C
--- server.example.lan ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3112ms
rtt min/avg/max/mdev = 0.255/0.292/0.309/0.021 ms
```

Obrázek č. 26 - Testování domény serveru DNS (zdroj vlastní)

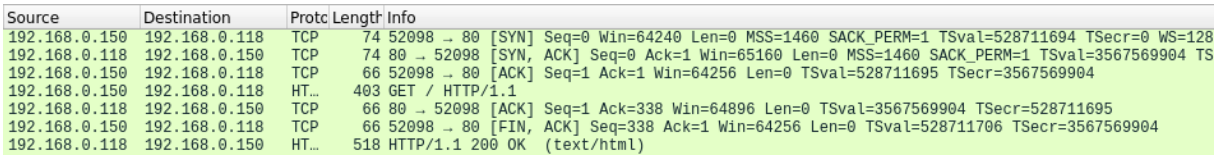
Pro podrobné zobrazení komunikace serveru DNS a klienta se v programu Wireshark použije filtr „dns“. Komunikace probíhá na portu 53 na straně serveru. Klient vyšle požadavek pro doménu „server.example.lan“. Server DNS přijme požadavek a podívá se do zóny „example.lan“ a pokusí se najít záznam „server.example.lan“, v případě shody je klientovy vrácena ze serveru adresa IP korespondující s požadovanou doménou.



Source	Destination	Protc	Length	Info
192.168.0.150	192.168.0.118	DNS	78	Standard query 0x5606 A server.example.lan
192.168.0.150	192.168.0.118	DNS	78	Standard query 0xc100 AAAA server.example.lan
192.168.0.118	192.168.0.150	DNS	94	Standard query response 0x5606 A server.example.lan A 192.168.0.118
192.168.0.118	192.168.0.150	DNS	120	Standard query response 0xc100 AAAA server.example.lan SOA server.example.lan
192.168.0.150	192.168.0.118	DNS	86	Standard query 0x7a08 PTR 118.0.168.192.in-addr.arpa
192.168.0.118	192.168.0.150	DNS	118	Standard query response 0x7a08 PTR 118.0.168.192.in-addr.arpa PTR server.example.lan
192.168.0.150	192.168.0.118	DNS	86	Standard query 0xbc51 PTR 118.0.168.192.in-addr.arpa
192.168.0.118	192.168.0.150	DNS	118	Standard query response 0xbc51 PTR 118.0.168.192.in-addr.arpa PTR server.example.lan

Obrázek č. 27 - Odchytávání komunikace mezi klientem a serverem DNS (zdroj vlastní)

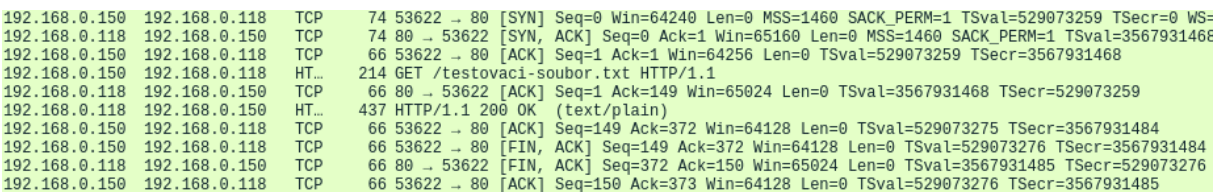
Poslední testovanou službou je webový server Apache, jeho testování proběhne z klienta zadáním adresy serveru, na kterém služba Apache běží. Při navázání komunikace proběhne mezi klientem a serverem takzvaný tří cestný handshake. Klient vyšle synchronizující paket SYN na port 80 serveru a ten mu pošle synchronizující paket SYN společně s potvrzením ACK. Klient následně pošle také potvrzení ACK. Nyní je vytvořené spojení a server může přijímat požadavky klienta. V tomto případě klient žádá webovou stránku ze serveru, server přijme požadavek a odešle mu zprávu obsahující požadovaný html soubor. Následně server indikuje ukončení přenosu a spojení pomocí paketu FIN, ACK.



Source	Destination	Protc	Length	Info
192.168.0.150	192.168.0.118	TCP	74	52098 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=528711694 TSecr=0 WS=128
192.168.0.118	192.168.0.150	TCP	74	80 → 52098 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=3567569904 TS
192.168.0.150	192.168.0.118	TCP	66	52098 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=528711695 TSecr=3567569904
192.168.0.150	192.168.0.118	HT…	403	GET / HTTP/1.1
192.168.0.118	192.168.0.150	TCP	66	80 → 52098 [ACK] Seq=1 Ack=338 Win=64896 Len=0 TSval=3567569904 TSecr=528711695
192.168.0.150	192.168.0.118	TCP	66	52098 → 80 [FIN, ACK] Seq=338 Ack=1 Win=64256 Len=0 TSval=528711706 TSecr=3567569904
192.168.0.118	192.168.0.150	HT…	518	HTTP/1.1 200 OK (text/html)

Obrázek č. 28 - Navázání připojení se serverem Apache (zdroj vlastní)

V případě požadavku klienta pro stažení souboru ze serveru je znovu navázáno spojení pomocí tří cestného handshaku. Následně pomocí GET je vybrán požadovaný soubor. Server požadavek zpracuje a odpoví klientovi zprávou obsahující daný soubor. Po přenosu je opět spojení ukončeno.



192.168.0.150	192.168.0.118	TCP	74	53622 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=529073259 TSecr=0 WS=
192.168.0.118	192.168.0.150	TCP	74	80 → 53622 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=3567931468
192.168.0.150	192.168.0.118	TCP	66	53622 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=529073259 TSecr=3567931468
192.168.0.150	192.168.0.118	HT…	214	GET /testovaci-soubor.txt HTTP/1.1
192.168.0.118	192.168.0.150	TCP	66	80 → 53622 [ACK] Seq=1 Ack=149 Win=65024 Len=0 TSval=3567931468 TSecr=529073259
192.168.0.118	192.168.0.150	HT…	437	HTTP/1.1 200 OK (text/plain)
192.168.0.150	192.168.0.118	TCP	66	53622 → 80 [ACK] Seq=149 Ack=372 Win=64128 Len=0 TSval=529073275 TSecr=3567931484
192.168.0.150	192.168.0.118	TCP	66	53622 → 80 [FIN, ACK] Seq=149 Ack=372 Win=64128 Len=0 TSval=529073276 TSecr=3567931484
192.168.0.118	192.168.0.150	TCP	66	80 → 53622 [FIN, ACK] Seq=372 Ack=150 Win=65024 Len=0 TSval=3567931485 TSecr=529073276
192.168.0.150	192.168.0.118	TCP	66	53622 → 80 [ACK] Seq=150 Ack=373 Win=64128 Len=0 TSval=529073276 TSecr=3567931485

Obrázek č. 29 - Stahování souboru z webového serveru (zdroj vlastní)

ZÁVĚR

Rozhodnutí učitele nebo školy o výběru operačního systému pro výuku počítačových sítí je bezesporu důležité. Každý operační systém přichází se svou sadou nástrojů, jiným zaměřením a hlavně s rozdílnou efektivitou, co se týče potřeby pro vyučování počítačových sítí. Počítačové technologie se stále vyvíjejí, a proto operační systémy, které bylo ideální provozovat v minulosti, nemusí být to nejvhodnější řešení i do budoucna.

Tato práce měla za cíl využít operační systém založený na distribuci RHEL k implementaci běžně používaných síťových služeb a demonstrovat jejich konfiguraci na daném operačním systému. RHEL, jakožto distribuce určená především pro firmy s placenou podporou a službami, už z principu není nejvhodnějším řešením pro školní systém. Avšak v průběhu práce bylo představeno několik operačních systémů vycházejících z distribuce RHEL, každý méně či více vhodný stát se nástrojem pro výuku. Autor práce zvolil pro praktickou část operační systém s distribucí Rocky Linux, především kvůli bezplatnému provozu, stabilitě a spolehlivosti, z důvodu přijímání pouze ověřených aktualizací z jiných distribucí. Dalším méně důležitým faktorem při rozhodování byla i dobře zpracovaná dokumentace distribuce, obsahující popis konfigurace některých služeb.

V praktické části bylo úkolem nakonfigurovat a otestovat dané služby pomocí nástrojů, které distribuce Rocky Linux poskytuje. Vytvořeny byly dva virtuální počítače, jeden v roli serveru a druhý v roli klienta, oba běžící na distribuci Rocky Linux. Na serveru byly konfigurovány služby DHCP, DNS, FTP, Apache a brána firewall. Brána firewall byla nakonfigurována pomocí nástroje firewalld a její nastavení bylo demonstrováno výpisem konfigurace. Server DHCP byl zprovozněn za použití nástroje dhcpd a jeho funkčnost byla demonstrována na klientovi, který obdržel předem určenou adresu na základě jeho adresy MAC. Pro konfiguraci serveru FTP byl použit démon vsftpd a ověření fungování služby proběhlo úspěšným přenosem souboru ze serveru FTP na klienta. Server DNS byl nakonfigurován nástrojem bind-utils za použití jeho démona named. Z klienta byla funkčnost DNS serveru ověřena dotazem na doménu definovanou v rámci zóny, nacházející se v konfiguračních souboru démona named. Webový server Apache byl nakonfigurován za pomoci nástroje httpd. Z klientského systému byla ověřena dostupnost webu poskytovaného serverem Apache a následně i stažením souboru z webového serveru. Funkčnost všech služeb byla ještě dodatečně zkontrolována programem Wireshark, který zachytával komunikaci mezi klientem a serverem při používání výše zmíněných služeb.

Distribuce Rocky Linux je uživatelsky přívětivá, i přestože se jedná o relativně novou, stále vyvíjející distribuci, je stabilní a spolehlivá. Snaží se být tím, co byl CentOS před jeho zánikem a to jí dává potenciál do budoucna. Nastavení služeb nebylo složité a zvládnout by ho měl každý se základními znalostmi sítí a fungování operačního systému Linux.

POUŽITÁ LITERATURA

[1] ZOLA, Andrew. What is Red Hat Enterprise Linux (RHEL) and how is it used?. TechTarget [online]. Newton, 2023 [cit. 2023-04-10]. Dostupné z: https://www.techtarget.com/searchdatacenter/definition/Red-Hat-Enterprise-Linux-RHEL

[2] Red Hat Enterprise Linux operating system. Red Hat [online]. Raleigh, 2023 [cit. 2023-04-10]. Dostupné z: https://www.redhat.com/en/technologies/linux-platforms/enterprise-linux

[3] Red Hat Enterprise Linux Life Cycle. Red Hat Customer Portal [online]. Raleigh, 2023 [cit. 2023-04-10]. Dostupné z: https://access.redhat.com/support/policy/updates/errata

[4] Red Hat Enterprise Linux 9: Performing a standard RHEL 9 installation. In: Red Hat [online]. Raleigh, 2023 [cit. 2023-04-10]. Dostupné z: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/pdf/performing_a_standard_rhel_9_installation/red_hat_enterprise_linux-9-performing_a_standard_rhel_9_installation-en-us.pdf

[5] Red Hat Enterprise Linux 9: Configuring basic system settings. In: Red Hat [online]. Raleigh, 2023 [cit. 2023-04-10]. Dostupné z: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/pdf/configuring_basic_system_settings/red_hat_enterprise_linux-9-configuring_basic_system_settings-en-us.pdf

[6] THE RED HAT ENTERPRISE AGREEMENT. In: Red Hat [online]. Raleigh, 2018 [cit. 2023-04-10]. Dostupné z: https://www.redhat.com/licenses/Enterprise_Agreement_WebversionGlobal_English_20180416.pdf

[7] Red Hat Enterprise Linux subscription guide. In: Red Hat [online]. Raleigh, 2019 [cit. 2023-04-10]. Dostupné z: https://www.redhat.com/cms/managed-files/li-rhel-subscription-guide-f19421wg-201911-en.pdf

[8] No-cost Red Hat Enterprise Linux Individual Developer Subscription: FAQs. Red Hat Developer [online]. Raleigh, 2021 [cit. 2023-04-10]. Dostupné z: https://developers.redhat.com/articles/faqs-no-cost-red-hat-enterprise-linux#

[9] Getting Started Guide. In: Vmware [online]. Palo Alto, c2007 [cit. 2023-04-10]. Dostupné z: https://www.vmware.com/pdf/vmware_player200.pdf

[10] Oracle VM VirtualBox Overview. In: Oracle [online]. Austin, 2021 [cit. 2023-04-10]. Dostupné z: https://www.oracle.com/assets/oracle-vm-virtualbox-overview-2981353.pdf

[11] Features Overview. VirtualBox [online]. Austin [cit. 2023-04-10]. Dostupné z: https://www.virtualbox.org/manual/ch01.html#features-overview

[12] SIMIC, Sofija. Virtualbox vs VMware: Head-to-Head Comparison. PhoenixNAP [online]. Phoenix, 2021 [cit. 2023-04-10]. Dostupné z: https://phoenixnap.com/kb/virtualbox-vs-vmware

[13] What is Virtual Networking?. Vmware [online]. Palo Alto, c2023 [cit. 2023-04-10]. Dostupné z: https://www.vmware.com/topics/glossary/content/virtual-networking.html

[14] Getting Started with VMware Player. In: Vmware [online]. Palo Alto, c2011 [cit. 2023-04-10]. Dostupné z: https://www.vmware.com/pdf/vmware_player40.pdf

[15] VirtualBox Network Settings: Complete Guide. In: Nakivo [online]. Nevada, 2019 [cit. 2023-04-19]. Dostupné z: https://www.nakivo.com/blog/virtualbox-network-setting-guide/

[16] In: VUGT, Sander. Red Hat Enterprise Linux 6 Administration : Real World Skills for Red Hat Administrators [online]. 1. Hoboken: Wiley, 2013 [cit. 2023-04-10]. ISBN 9781299189997. Dostupné z: https://books.google.cz/books?hl=cs&lr=&id=CIUhu9HKrFoC&oi=fnd&pg=PT10&dq=red+hat+enterprise+linux&ots=TvsXo-zjoK&sig=WQVHAXd3sPWakqCFaRaEoAX2t44&redir_esc=y#v=onepage&q=red%20hat%20enterprise%20linux&f=false

[17] RED HAT ENTERPRISE LINUX SERVER DATASHEET. In: Red Hat [online]. Raleigh, c2018 [cit. 2023-04-10]. Dostupné z: https://www.redhat.com/cms/managed-files/li-enterprise-linux-server-datasheet-f11191jm-201803-en_2.pdf

[18] In: SMYTH, Neil. CentOS 8 Essentials [online]. 1. Payload Media, 2019, s. 5 [cit. 2023-04-11]. ISBN 9781951442088. Dostupné z: https://www.ebookfrenzy.com/pdf_previews/CentOS8EssentialsPreview.pdf

[19] In: MEMBREY, Peter, Tim VERHOEVEN a Ralph ANGENENDT. The Definitive Guide to CentOS [online]. 1. Apress, 2009, s. 3 [cit. 2023-04-11]. ISBN 9781430219316. Dostupné z: https://link.springer.com/chapter/10.1007/978-1-4302-1931-6_1

[20] CentOS Linux EOL. CentOS [online]. c2023 [cit. 2023-04-11]. Dostupné z: https://www.centos.org/centos-linux-eol/

[21] MIKESELL, Les. Why is the CentOS stream not a good option for production?. In: Quora [online]. 2021 [cit. 2023-04-11]. Dostupné z: https://www.quora.com/Why-is-the-CentOS-stream-not-a-good-option-for-production

[22] STAIMER, Marc. The Winner for the Best CentOS Linux Replacement is…. In: Oracle [online]. Austin, 2021 [cit. 2023-04-11]. Dostupné z: https://www.oracle.com/a/ocom/docs/dsc-ol-centos-replacement.pdf

[23] The 7 Best Red Hat-Based Linux Distributions. MakeUseOf [online]. Québec, 2021 [cit. 2023-04-11]. Dostupné z: https://www.makeuseof.com/best-red-hat-based-linux-distros/

[24] What is Oracle Linux?. In: TrustRadius [online]. Austin, c2013-2023 [cit. 2023-04-11]. Dostupné z: https://www.trustradius.com/products/oracle-linux/reviews?qs=pros-and-cons#overview

[25] Oracle Linux. In: Oracle [online]. Austin, c2023 [cit. 2023-04-11]. Dostupné z: https://www.oracle.com/a/ocom/docs/linux/oracle-linux-ds.pdf

[26] COHEN, Alan. What are the pros/cons of Oracle Linux vs Red Hat Enterprise Linux?. In: Quora [online]. 2012 [cit. 2023-04-11]. Dostupné z: https://www.quora.com/What-are-the-pros-cons-of-Oracle-Linux-vs-Red-Hat-Enterprise-Linux

[27] BRUNI, Ezequiel. How to Migrate to Rocky Linux from CentOS Stream, CentOS, Alma Linux, RHEL, or Oracle Linux. Rocky Linux Documentation [online]. Los Angeles: The Rocky Enterprise Software Foundation, 2023 [cit. 2023-04-11]. Dostupné z: https://docs.rockylinux.org/guides/migrate2rocky/

[28] Using the DNF software package manager. Fedora Documentation :: Fedora Docs [online]. 2022 [cit. 2023-04-11]. Dostupné z: https://docs.fedoraproject.org/en-US/quick-docs/dnf/

[29] KHURANA, Vijay. A Quick Guide to DNF Package Manager. GEEKFLARE [online]. London, 2022 [cit. 2023-04-11]. Dostupné z: https://geekflare.com/dnf-intro/

[30] MILLER, Adam, Maxim SVISTUNOV a Marie DOLEŽALOVÁ. Why Package Software with RPM?. RPM Packaging Guide [online]. 2023 [cit. 2023-04-11]. Dostupné z: https://rpm-packaging-guide.github.io/

[31] KUMAR, Pradeep. How to Install Rocky Linux 9 Step by Step with Screenshots. LinuxTechi [online]. 2022 [cit. 2023-04-11]. Dostupné z: https://www.linuxtechi.com/how-to-install-rocky-linux-9-step-by-step/

[32] Top 10 things to do after Rocky Linux 9 install. CIQ [online]. Reno: CIQ Engineering, 2022 [cit. 2023-04-11]. Dostupné z: https://ciq.co/blog/top-10-things-to-do-after-rocky-linux-9-install/

[33] BOUCHERON, Brian a Jamon CAMISSO. Initial Server Setup with Rocky Linux 8. DigitalOcean [online]. 2021 [cit. 2023-04-11]. Dostupné z: https://www.digitalocean.com/community/tutorials/initial-server-setup-with-rocky-linux-8

[34] User Management. Rocky Linux Documentation [online]. Los Angeles: The Rocky Enterprise Software Foundation, 2022 [cit. 2023-04-11]. Dostupné z: https://docs.rockylinux.org/books/admin_guide/06-users/

[35] MORVAN, Antoine. SELinux security. Rocky Linux Documentation [online]. Los Angeles: The Rocky Enterprise Software Foundation, 2022 [cit. 2023-04-11]. Dostupné z: https://docs.rockylinux.org/guides/security/learning_selinux/

[36] Systemd. Rocky Linux Documentation [online]. Los Angeles: The Rocky Enterprise Software Foundation, 2022 [cit. 2023-04-11]. Dostupné z: https://docs.rockylinux.org/books/admin_guide/10-boot/?h=systemctl#systemd_1

[37] GARNETT, Alex. How To Set Up a Firewall Using firewalld on Rocky Linux 8. DigitalOcean [online]. 2022 [cit. 2023-04-11]. Dostupné z:

https://www.digitalocean.com/community/tutorials/how-to-set-up-a-firewall-using-firewalld-on-rocky-linux-8

[38] BRUNI, Ezequiel. Firewalld for Beginners. Rocky Linux Documentation [online]. Los Angeles: The Rocky Enterprise Software Foundation, 2022 [cit. 2023-04-11]. Dostupné z: https://docs.rockylinux.org/guides/security/firewalld-beginners/

[39] About the DHCP Protocol. Oracle [online]. Austin, c1999-2011 [cit. 2023-04-11]. Dostupné z: https://docs.oracle.com/cd/E18752_01/html/816-4554/dhcp-overview-2.html

[40] Advantages of Using DHCP. Oracle [online]. Austin, c1999-2011 [cit. 2023-04-11]. Dostupné z: https://docs.oracle.com/cd/E18752_01/html/816-4554/dhcp-overview-12a.html

[41] DHCP configuration. Rocky Linux Documentation [online]. Los Angeles: The Rocky Enterprise Software Foundation, 2022 [cit. 2023-04-11]. Dostupné z: https://docs.rockylinux.org/books/admin_guide/12-network/#dhcp-configuration

[42] SPENCER, Steven. Private DNS Server Using Bind. Rocky Linux Documentation [online]. Los Angeles: The Rocky Enterprise Software Foundation, 2022 [cit. 2023-04-11]. Dostupné z: https://docs.rockylinux.org/guides/dns/private_dns_server_using_bind/

[43] Introduction to DNS. In: Rutgers [online]. New Jersey, [cca 2000] [cit. 2023-04-11]. Dostupné z: https://people.cs.rutgers.edu/~pxk/417/notes/content/ms_dns.pdf

[44] Secure FTP Server - vsftpd. Rocky Linux Documentation [online]. Los Angeles: The Rocky Enterprise Software Foundation, 2023 [cit. 2023-04-12]. Dostupné z: https://docs.rockylinux.org/guides/file_sharing/secure_ftp_server_vsftpd/

[45] KNOPF, Mario a Jürgen POHL. Vsftpd - An Introduction to the Very Secure FTP Daemon. In: Ibiblio [online]. LinuxFocus Editor team, 2005 [cit. 2023-04-12]. Dostupné z: https://www.ibiblio.org/pub/Linux/docs/linux-doc-project/linuxfocus/English/Archives/lf-2004_07-0341.pdf

[46] How to construct VSFTP and configure virtual users. Alibaba Cloud [online]. Hangzhou, 2020 [cit. 2023-04-12]. Dostupné z: https://www.alibabacloud.com/help/en/elastic-compute-service/latest/how-to-construct-vsftp-and-configure-virtual-users

[47] HERNANDEZ, Jovan. What is Apache? In-Depth Overview of Apache Web Server. Sumo logic [online]. Redwood City, 2019 [cit. 2023-04-12]. Dostupné z: https://www.sumologic.com/blog/apache-web-server-introduction/

[48] CHRISTENSSON, Per. Apache. TechTerms.com [online]. Minnesota: Sharpened Productions, 2011 [cit. 2023-04-12]. Dostupné z: https://techterms.com/definition/apache

[49] Linux iptables. In: Massive Technical Interviews Tips: Archives [online]. 2016 [cit. 2023-04-19]. Dostupné z: https://massivetechinterview.blogspot.com/2016/09/linux-iptables.html

[50] Linux Firewall: Introduction to Linux Firewall. JavaTpoint [online]. Noida, c2011-2022 [cit. 2023-04-13]. Dostupné z: https://www.javatpoint.com/linux-firewall

[51] BOYCE, Gregory. In: Linux Networking Cookbook [online]. 1. Birmingham: Packt Publishing, 2016, s. 10 [cit. 2023-04-13]. ISBN 9781785287916. Dostupné z: https://books.google.cz/books?hl=cs&lr=&id=Jv1vDQAAQBAJ&oi=fnd&pg=PP1&dq=linux+dhcp+configuration&ots=j6KevGEKZV&sig=OUbaEVNn-O6mr5lpubbgy7nmCfU&redir_esc=y#v=onepage&q=linux%20dhcp%20configuration&f=false

[52] Dynamic Host Configuration Protocol - DHCP: Feature Overview and Configuration Guide. In: Allied Telesis [online]. c2022 [cit. 2023-04-13]. Dostupné z: https://www.alliedtelesis.com/sites/default/files/documents/configuration-guides/dhcp_feature_overview_guide.pdf

[53] Quick Understanding of DHCP in ONU and Routers. In: BT-PON [online]. Shenzhen, 2021 [cit. 2023-04-19]. Dostupné z: https://www.bt-pon.com/quick-understanding-of-dhcp-in-onu-and-routers.html

[54] How To Configure DHCP Server on Rocky Linux 9. Idroot [online]. 2023 [cit. 2023-04-13]. Dostupné z: https://idroot.us/configure-dhcp-server-on-rocky-linux-9/

[55] FTP – The File Transfer Protocol. In: SRT [online]. Annapolis: South River Technologies, 2015 [cit. 2023-04-13]. Dostupné z: https://southrivertech.com/wp-content/uploads/FTP_Explained2.pdf

[56] GOMEZ, John. How to set up FTP server in Rocky Linux 8.4. LinuxTeck [online]. 2023 [cit. 2023-04-13]. Dostupné z: https://www.linuxteck.com/how-to-set-up-ftp-server-in-rocky-linux/

[57] Working of Domain Name System (DNS) Server. In: GeeksforGeeks [online]. Noida, 2020 [cit. 2023-04-19]. Dostupné z: https://www.geeksforgeeks.org/working-of-domain-name-system-dns-server/

[58] What Is Apache? An In-Depth Overview of Apache Web Server. Hostinger [online]. Larnaca, 2023 [cit. 2023-04-13]. Dostupné z: https://www.hostinger.com/tutorials/what-is-apache

[59] SPENCER, Steven. Apache Web Server Multisite Setup. Rocky Linux Documentation [online]. Los Angeles: The Rocky Enterprise Software Foundation, 2023 [cit. 2023-04-13]. Dostupné z: https://docs.rockylinux.org/guides/web/apache-sites-enabled/

[60] GARN, Damon. How to deploy an Apache web server quickly. Red Hat [online]. Raleigh, 2022 [cit. 2023-04-13]. Dostupné z: https://www.redhat.com/sysadmin/install-apache-web-server

[61] ZAMOT, Michael. An introduction to Cockpit, a browser-based administration tool for Linux. Red Hat [online]. Raleigh, 2020 [cit. 2023-04-13]. Dostupné z: https://www.redhat.com/sysadmin/intro-cockpit

[62] Introduction to Wireshark. GeeksforGeeks [online]. Noida, 2022 [cit. 2023-04-14]. Dostupné z: https://www.geeksforgeeks.org/introduction-to-wireshark/

[63] Wireshark. TechTarget [online]. Newton, 2011 [cit. 2023-04-14]. Dostupné z: https://www.techtarget.com/whatis/definition/Wireshark

PŘÍLOHY

PŘÍLOHA A - UKÁZKA KONFIGURAČNÍHO SOUBORU DHCPD.CONF

```
subnet 192.168.0.0 netmask 255.255.255.0 {
 range 192.168.0.100 192.168.0.200;
 option routers 192.168.0.1;
 option domain-name-servers 8.8.8.8, 8.8.4.4;
}

host klient1 {
 hardware ethernet 00:0C:29:8C:64:99;
 fixed-address 192.168.0.150;
}
```

PŘÍLOHA B - UKÁZKA KONFIGURAČNÍHO SOUBORU VSFTPD.CONF

```
anonymous_enable=NO
local_enable=YES
write_enable=YES
local_umask=022
dirmessage_enable=YES
xferlog_enable=YES
connect_from_port_20=YES
xferlog_std_format=YES
chroot_local_user=YES
allow_writeable_chroot=YES

listen=NO
listen_ipv6=YES

pam_service_name=vsftpd
userlist_enable=YES

pasv_min_port=40000
pasv_max_port=40001
```

PŘÍLOHA C - UKÁZKA KONFGURAČNÍHO SOUBORU NAMED.CONF

```
options {
#       listen-on port 53 { 127.0.0.1; };
#       listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        secroots-file   "/var/named/data/named.secroots";
        recursing-file  "/var/named/data/named.recursing";
        allow-query     { localhost; };
};
zone "." IN {
        type hint;
        file "named.ca";
};
zone "example.lan" IN {
    type master;
    file "example.lan.db";
    allow-update { none; };
   allow-query {any; };
};
zone "0.168.192.in-addr.arpa" IN {
    type master;
    file "example.lan.rev";
    allow-update { none; };
   allow-query { any; };
};
include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
```

PŘÍLOHA D - UKÁZKA KONFIGURAČNÍHO SOUBORU HTTPD.CONF

```
ServerRoot "/etc/httpd"
Listen 80
Include conf.modules.d/*.conf
User apache
Group apache
ServerAdmin root@localhost

<Directory />
    AllowOverride none
    Require all denied
</Directory>

DocumentRoot "/var/www/html"
<Directory "/var/www">
    AllowOverride None
    Require all granted
</Directory>

<Directory "/var/www/html">
    Options Indexes FollowSymLinks
    AllowOverride None
    Require all granted
</Directory>

<IfModule dir_module>
    DirectoryIndex index.html
</IfModule>
```

```
<Files ".ht*">
    Require all denied
</Files>


ErrorLog "logs/error_log"
LogLevel warn


<IfModule log_config_module>
    LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined
    LogFormat "%h %l %u %t \"%r\" %>s %b" common


    <IfModule logio_module>
      LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\" %I %O" combinedio
    </IfModule>
    CustomLog "logs/access_log" combined
</IfModule>


AddDefaultCharset UTF-8
EnableSendfile on
IncludeOptional conf.d/*.conf
```