

Bakalářská práce



České  
vysoké  
učení technické  
v Praze

**F3**

Fakulta elektrotechnická  
Katedra počítačů

## Nasazení správy IP adres ve středně velké síti

**Jonáš Neuvirt**

Vedoucí: Ing. Jan Kubr, Ph.D.

Studijní program: Softwarové inženýrství a technologie

Leden 2021



## I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení: **Neuvirt** Jméno: **Jonáš** Osobní číslo: **420347**  
Fakulta/ústav: **Fakulta elektrotechnická**  
Zadávající katedra/ústav: **Katedra počítačů**  
Studijní program: **Softwarové inženýrství a technologie**

## II. ÚDAJE K BAKALÁŘSKÉ PRÁCI

Název bakalářské práce:

**Nasazení správy IP adres ve středně velké síti**

Název bakalářské práce anglicky:

**Pilot Implementation of IP Address Management**

Pokyny pro vypracování:

- 1) Analyzujte aktuální nabídku open-source software implementující funkce DHCP, DHCPv6 a DNS serveru.
- 2) Analyzujte aktuální nabídku open-source software umožňující správu a dohled využívání IP a IPv6 adres v sítích LAN.
- 3) Navrhněte a realizujte laboratoř pro otestování nasazení zvolených software.
- 4) Vytvořte doporučení a popis postupu pro implementaci těchto služeb v reálné síti. Po dohodě s vedoucím práce vytvořte pilotní implementaci na části reálné sítě.
- 5) V případě nutnosti navrhněte, implementujte a otestujte software (nebo jeho část/doplňek) usnadňující správu IP adres a DNS jmen pomocí výše zvolených nástrojů.
- 6) Navrhněte postup pro otestování správného nasazení správy IP adres.

Seznam doporučené literatury:

Pekárek, Vít. Správa IP adres ve středně velké síti. Bakalářská práce. Praha: České vysoké učení technické v Praze, Fakulta informačních technologií, 2019.  
DROMS, Ralph. Dynamic Host Configuration Protocol [online]. 1993. Dostupné z: <https://www.rfc-editor.org/rfc/rfc1541.txt>. RFC. RFC Editor.  
MOCKAPETRIS, Paul. Domain names – implementation and specification [online]. 1987. Dostupné z: <https://www.rfc-editor.org/rfc/rfc1034.txt>. RFC. RFC Editor.

Jméno a pracoviště vedoucí(ho) bakalářské práce:

**Ing. Jan Kubr, Ph.D., katedra počítačové grafiky a interakce FEL**

Jméno a pracoviště druhé(ho) vedoucí(ho) nebo konzultanta(ky) bakalářské práce:

Datum zadání bakalářské práce: **14.02.2020**

Termín odevzdání bakalářské práce: **14.08.2020**

Platnost zadání bakalářské práce: **30.09.2021**

Ing. Jan Kubr, Ph.D.  
podpis vedoucí(ho) práce

podpis vedoucí(ho) ústavu/katedry

prof. Mgr. Petr Páta, Ph.D.  
podpis děkana(ky)

### III. PŘEVZETÍ ZADÁNÍ

Student bere na vědomí, že je povinen vypracovat bakalářskou práci samostatně, bez cizí pomoci, s výjimkou poskytnutých konzultací.  
Seznam použité literatury, jiných pramenů a jmen konzultantů je třeba uvést v bakalářské práci.

\_\_\_\_\_  
Datum převzetí zadání

\_\_\_\_\_  
Podpis studenta

## Poděkování

Rád bych poděkoval panu Ing. Janu Kubrovi, Ph.D. za podporu a schovitavost, kterou projevil během vedení mé bakalářské práce. Zároveň děkuji mé rodině za jejich podporu během celého studia.

## Prohlášení

Prohlašuji, že jsem předloženou práci vypracoval samostatně, a že jsem uvedl veškeré použité informační zdroje.

V Praze 5. ledna 2021

## Abstrakt

Cílem práce je navrhnout a otestovat laboratoř pro správu IP adres ve středně velké síti použitím vybraného softwaru pro DHCP, DNS a IPAM služby. Dalším úkolem je navrhnout postup pro implementaci těchto služeb v rámci reálné sítě a nakonec navrhnout postup pro otestování správného nasazení všech vybraných aplikací.

**Klíčová slova:** PowerDNS, Kea, phpIPAM, DNS, DHCP, IPAM, správa sítě

**Vedoucí:** Ing. Jan Kubr, Ph.D.

## Abstract

The goal of this thesis is to design and test an implementation of IP address management in laboratory conditions using selected software for DHCP, DNS and IPAM services. Additional task is to design a method of deploying selected software in live environment and developing a strategy to test proper software deployment.

**Keywords:** PowerDNS, Kea, phpIPAM, DNS, DHCP, IPAM, network management

**Title translation:** Pilot Implementation of IP Adress Management

# Obsah

<b>1 Úvod</b>	<b>1</b>
<b>2 Analýza</b>	<b>3</b>
2.1 Nynější stav .....	3
2.2 Požadavky na síť .....	3
2.3 Výhody přechodu na PowerDNS .	3
2.4 Výhody přechodu na Kea .....	4
2.5 Zavedení IPAM systému .....	6
2.6 Budoucí stav .....	6
<b>3 Návrh a realizace laboratoře</b>	<b>9</b>
3.1 Použité technologie .....	9
3.1.1 Hardware .....	9
3.1.2 Software .....	9
3.2 Architektura sítě .....	10
3.3 Vytvoření a nastavení testovací sítě .....	10
3.3.1 MySQL .....	10
3.3.2 PowerDNS .....	11
3.3.3 PowerDNS Admin.....	13
3.3.4 PhpIPAM.....	15
3.3.5 Kea .....	16
3.3.6 Stork .....	17
3.4 Postup v reálné síti .....	18
3.4.1 Nasazení DNS .....	18
3.4.2 Nasazení DHCP .....	18
3.4.3 Nasazení databáze .....	18
<b>4 Postup testování</b>	<b>19</b>
4.1 Testování funkčnosti .....	19
4.2 Zátěžové testování .....	19
<b>5 Závěr</b>	<b>21</b>
<b>Bibliografie</b>	<b>23</b>
<b>A Seznam zkratk</b>	<b>27</b>

## Obrázky

## Tabulky

2.1 Dva způsoby nasazení Kea DHCP serverů v režimu High Availability s použitím jedné databáze ( <i>Zdroj: [2]</i> ). . . . .	5
3.1 Znázornění konfigurace bez rekurzoru. ( <i>Zdroj: [16]</i> ). . . . .	11
3.2 Znázornění konfigurace s rekurzorem. ( <i>Zdroj: [16]</i> ). . . . .	12
3.3 Ukázka části konfiguračního souboru master rekurzoru. . . . .	12
3.4 Ukázka části konfiguračního souboru autoritativního serveru. . . . .	12
3.5 Ukázka konfigurace api webového rozhraní. . . . .	13
3.6 Ukázka správy uživatelů v aplikaci PowerDNS Admin. . . . .	14
3.7 Ukázka přiřazení uživatelů fit-admin1 a fit-admin2 pod účet fit. . . . .	14
3.8 Ukázka vytvoření nové domény feld.cvut.cz. . . . .	15
3.9 Ukázka vytvoření nového záznamu pro doménu felk.cvut.cz. . . . .	16
3.10 Přehled všech hostovaných domén. . . . .	16
3.11 Ukázka správy doménových záznamů PowerDNS v phpIPAM. . . . .	17



# Kapitola 1

## Úvod

Správa větších počítačových sítí není jednoduchá, zvláště pokud by daná síť měla být spravována několika správci. V rámci sítě je potřeba mít služby Dynamic Host Configuration Protocol (DHCP) pro automatickou konfiguraci zařízení v síti a Domain Name System (DNS) pro převod doménových jmen na IP adresy. Zároveň je užitečné mít v rámci sítě dostupný IP monitoring system (IPAM), který poskytuje informace o dostupnosti a využití adres v síti.

Na Karlově náměstí se nachází budova Českého vysokého učení technického v Praze (ČVUT). Počítačová síť v této budově je spravována několika správci, ale pouze jeden je administrátorem, který může provádět změny v konfiguraci. Pokud by některý ze správců chtěl provést změny v konfiguraci pro část sítě, za kterou je zodpovědný, musí požádat administrátora, aby tyto změny implementoval, čímž dochází ke zbytečným prodlevám. Bylo by proto vhodné, aby měli všichni jednotliví správci možnost provádět změny v nastavení sítě. V ideálním případě by měl každý správce mít možnost přístupu pouze k těm serverům či částem sítě, za které je zodpovědný. Použitím vhodných monitorovacích nástrojů pro přehled zapůjčených ip adres v síti pak bude možné zlepšit celkové využití přidělených adresních prostorů.

Přínosem této práce bude modernizace nynější sítě na Karlově náměstí. Použitím aktuálních technologií pro DHCP a DNS servery a přidáním IPAM tak dojde ke usnadnění správy sítě pro jednotlivé správce. Zároveň se tímto urychlí a z pohodlní proces provádění změn v konfiguraci, protože nebude třeba čekat na to, až administrátor implementuje požadované změny v konfiguraci. Využití vhodných monitorovacích nástrojů pak usnadní optimalizaci adresních prostorů v rámci jednotlivých podsítí tak, aby se zvýšil celkový počet dostupných ip adres v rámci celé sítě.



# Kapitola 2

## Analýza

V této kapitole je popsán nynější a plánovaný zmodernizovaný stav sítě. Tato práce vychází (a navazuje) z analýzy vypracované v bakalářské práci předcházejícího studenta [1]. Závěry z této práce jsou zde ověřeny a doplněny o nové informace. Dále jsou zde zmíněny různé možnosti a nastavení jednotlivých vybraných nástrojů.

### 2.1 Nynější stav

Momentálně je pro DHCP server použitý nástroj ISC DHCP a pro DNS server je použitý nástroj Bind9. Oba nástroje jsou poměrně staré, je možné je spravovat pouze přes konfigurační soubory, což způsobuje mnohá omezení. Níže jsou uvedeny možné výhody a vylešení, kterých se dá docílit přechodem na novou sadu nástrojů.

### 2.2 Požadavky na síť

Na síť jsou kladeny jisté požadavky, aby mohla dobře a spolehlivě fungovat. Jedná se o eliminaci potenciálních SPOF, čehož se dá docílit implementací hlavního a záložního serveru. DHCP i DNS servery musí umět pracovat jak s IPv4 tak s IPv6 adresami.

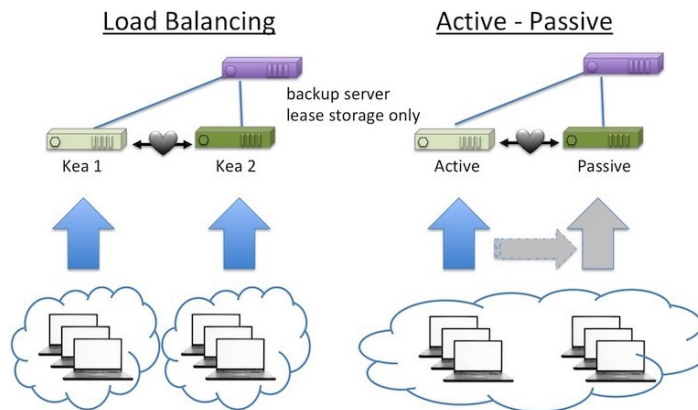
V rámci sítě je potřeba mít monitorovací nástroje, které umožní zobrazení různých statistik v rámci celé sítě. Především se jedná o přehled vypůjčených adres v rámci různých podsítí, aby se případně mohly optimalizovat konfigurace jednotlivých adresních prostorů těchto podsítí.

Pro efektivnější a bezpečnější správu sítě je požadována možnost omezit správu sítě pro jednotlivé administrátory. Každý správce by měl mít práva k provádění změn pouze v rámci jemu přidělené části sítě.

### 2.3 Výhody přechodu na PowerDNS

Pokud je nutné provést nějaké změny v DNS záznamech Bind9 serveru, existuje pouze jedna možnost, jak zajistit, aby se tyto změny projevíly – restartování serveru, jelikož konfigurace se načítá pouze při nastartování dané





**Obrázek 2.1:** Dva způsoby nasazení Kea DHCP serverů v režimu High Availability s použitím jedné databáze (Zdroj: [2]).

aktivním vývoji.

Obdobně jako v případě DNS, i zde jsou jisté požadavky na aplikaci, která usnadní správu sítě. Zde se jedná především o přehledný výpis statistik využití adres v rámci sítě či konfigurace podsítí jednotlivých serverů. Tyto možnosti nabízí aplikace Stork, která je poskytnutá stejnými vývojáři a je určena přímo pro práce s Kea. Stork momentálně nabízí možnost přehledu statistik jednotlivých podsítí (celkový počet adres, počet aktivně přidělených adres, počet volných adres), přehled rezervovaných adres (a zařízení, pro které jsou rezervované), informace o stavu jednotlivých serverů (jejich status, vytížení CPU a paměti) a informace o aktuální konfiguraci podsítí pro daný server.

Do budoucna jsou plánovány další funkcionality, aplikace Stork je v aktivním vývoji. Jedná se například o možnost nastavení alarmů a notifikací při pádu serverů či vyčerpání ip adres (přes email či v kombinaci s jinými aplikacemi, např. Grafana), podporu pro práci s logy nebo přidání testovacího prostředí (možnost simulovat uživatele v různých konfiguracích a scénářích). Dále se pak jedná o možnost přidání více uživatelských rolí a možnost správy a konfigurace serverů přímo přes aplikaci Stork, s tím že přístup k těmto konfiguracím bude možné omezit uživatelskými rolemi.

## 2.5 Zavedení IPAM systému

V síti není momentálně používán žádný IPAM software. PhpIPAM nabízí nejen možnost monitorování IP adres v síti, ale nabízí i integraci s PowerDNS. Dá se tak připojit na databázi autoritativního PowerDNS serveru a provádět změny přímo z grafického rozhraní. V předchozí bakalářské práci je zmíněna plánovaná podpora i pro Kea DHCP, dle [6] ale tato funkcionality stále není plně implementována<sup>2</sup>, momentálně umožňuje pouze čtení, ale ne zápis.

PhpIPAM je velmi robustní aplikace s velkým počtem možností. Hlavní výhodou je možnost běhu na databázi MySQL, stejně jako Kea a PowerDNS. Drobnou nevýhodou je fakt, že pro správnou funkčnost je třeba instalovat velké množství podpůrných aplikací a knihoven, které mohou u některých verzí a distribucí způsobovat problémy s kompatibilitou. Jak již bylo zmíněno výše, phpIPAM je schopen se připojit k databázím PowerDNS serverů a provádět změny v jejich konfiguracích.

Další možností je nainstalovat aplikaci Stork, která je primárně určena pro spolupráci s DHCP serverem Kea, ale v rámci zobrazení statistik ohledně využívání a zapůjčování IP adres v síti zároveň poskytuje i určité informace o připojených zařízeních (např. MAC adresy).

## 2.6 Budoucí stav

V ideálním případě by v síti byly nasazeny dva PowerDNS servery v konfiguraci master-slave. Ve skutečnosti by se však jednalo o čtyři servery, jelikož jeden server PowerDNS by využíval dva procesy, rekurzor a autoritativní server. Zároveň by bylo potřeba nainstalovat dva databázové servery, do kterých by se ukládaly jednotlivé DNS záznamy. Tyto databáze se mezi sebou budou vzájemně synchronizovat, aby byly DNS záznamy vždy aktuální.

Aby bylo možné spravovat tyto servery dle požadavků vycházejících ze zadání, bude třeba nainstalovat i aplikaci PowerDNS Admin. Ta umožní správu uživatelů a editaci jejich přístupových práv. Uživatelé tak budou schopni spravovat pouze ty domény, které jim byly přiděleny.

Dále by byly nasazeny dva Kea servery v režimu HA, aby byly pokryty případné výpadky. Zde je opět vhodné podotknout, že by se ve skutečnosti jednalo o celkem čtyři servery, jelikož Kea implementace je rozdělena na DHCPv4 a DHCPv6. K optimálnímu chodu je nutné<sup>3</sup> mít i databázi. Do této databáze se ukládají informace o aktuálně zapůjčených adresách. Toto je především nutné v případě, že Kea běží v režimu HA s možností load-balancing, kdy si servery rozdělují zátěž rovnoměrně mezi sebe. K synchronizaci vypůjčených adres se pak využívá tato společná databáze.

Pro umožnění a usnadnění správy DHCP serverů bude nainstalována

<sup>2</sup>Podpora pro Kea byla prvně zmíněna už v roce 2016, ale dodnes není plně funkční.

<sup>3</sup>Databáze není pro HA chod klíčová, jelikož Kea může běžet i v konfiguraci s tzv. memfile, kdy si každý server ukládá data k sobě na disk a zároveň informuje ostatní serveru o případných změnách.

aplikace Stork. Ta je schopna monitorovat stav jednotlivých serverů a zároveň podávat statistiky a informace o vypůjčených adresách v rámci sítě, včetně kapacit jednotlivých podsítí. Do budoucna je pak plánováno přidat podporu pro logování a konfiguraci přímo přes tuto aplikaci.

Na závěr by byl ještě nasazen phpIPAM, což znamená, že by byla třeba mít minimálně jeden webový server a jeden databázový server. Dle požadované úrovně zabezpečení a redundance se nabízí hned několik možností.

V první konfiguraci by byl použit jeden z už běžících databázových serverů, který by v ideálním případě byl umístěný na localhostu a zároveň by hostoval i databázi pro jeden z PowerDNS serverů. Nevýhodou je, že se tato konfigurace trochu blíží ke SPOF<sup>4</sup>. Druhou možností by bylo nainstalovat phpIPAM na vlastní stroj, kde by běžel pouze webový server. Pro databázi by se použil jeden z už nainstalovaných a nakonfigurovaných serverů s tím, že by se k němu muselo přistupovat vzdáleně.

Z výše zmíněného je vidět, že k implementaci všech nástrojů bude potřeba mít v síti minimálně jeden webový server, dva databázové servery, dva Kea DHCPv4 a Kea DHCPv6 servery, dva autoritativní PowerDNS servery a dva rekurzory.

---

<sup>4</sup>Na jednom stroji by běželo větší množství aplikací najednou.





## Kapitola 3

### Návrh a realizace laboratoře

Před jakýmkoliv pokusem o nasazení v reálné síti je vhodné nejdříve instalovat a konfigurovat dané technologie v rámci laboratorního prostředí. V této kapitole je popsáno, jak byla tato testovací laboratoř navržena a realizovaná. Návrh vychází z provedené analýzy, ale je limitován dostupným hardwarem.

#### 3.1 Použité technologie

Níže jsou uvedena všechna reálná i virtuální zařízení, která byla v rámci laboratoře použita. Dále jsou zde uvedeny i všechny aplikace, které byly na těchto zařízeních nainstalované.

##### 3.1.1 Hardware

Celá laboratoř je realizovaná ve virtuálním prostředí na stroji s operačním systémem Windows 10 s procesorem Intel Core i5-7200U CPU @ 2.5 GHz a 20 GB operační paměti.

Všechny virtuální stroje používají Debian ve verzi 10.4.0 se 4 GB operační paměti a pevnými disky o velikosti 32 GB. Jednalo se o čisté instalace ve VirtualBoxu pomocí příslušného iso obrazu [7].

##### 3.1.2 Software

Většina aplikací byla k instalaci dostupná z debian repozitáře, výjimkou byly aplikace phpIPAM a PowerDNS Admin, které se musely instalovat z git repozitářů. U žádné z aplikací nebyla vyžadována specifická verze, vždy byly instalovány v nejnovější stabilní verzi. Při samotné instalaci nedošlo k žádným velkým potížím, ale vzhledem k velkému množství instalovaných nástrojů není možné vyloučit, že se v budoucnu nějaké problémy vyskytnou, a to především při případném updatování již instalovaných nástrojů a knihoven.

U instalovaných balíčků se konkrétně jedná o phpIPAM v1.3, powerDNS v4.1, Kea v1.6, mariaDB v10.3, apache2 v2.4, nginx 1.14.2, node.js 10.21.0 a php v7.3. Dále pak ještě phpIPAM vyžaduje php-pear v1.10 a řadu php modulů. Některé tyto moduly se nenainstalují automaticky v rámci php instalace a musí být instalovány manuálně. V několika případech nebyly

některé požadované balíčky přímo dostupné z Debian repozitáře, místo toho se nainstalovaly v rámci instalace jiných balíčků. Celý list těchto modulů je dostupný v phpIPAM dokumentaci [8].

Pro vytvoření virtuální sítě byl použit nástroj VirtualBox ve verzi 6.1.

## 3.2 Architektura sítě

V síti se nachází celkem čtyři virtuální stroje, z nichž jeden funguje čistě jako testovací stanice pro všechny aplikace.

Dále zde operují dva stroje, kde na každém z nich je nainstalována MySQL databáze, phpIPAM a PowerDNS. Na prvním stroji běží PowerDNS server v režimu master, na druhém pak PowerDNS server v režimu slave. Na prvním stroji ještě navíc běží Kea DHCPv4 a Kea DHCPv6.

Na posledním stroji je nainstalována Kea DHCPv4 a Kea DHCPv6 společně s vlastní MySQL databází. Tato databáze je používána pouze servery Kea.

## 3.3 Vytvoření a nastavení testovací sítě

Všechny virtuální stroje měly nastavený síťový adaptér v režimu NAT Network. V nastavení VirtualBoxu v záložce files > preferences > network se musela daná síť nejprve vytvořit a nakonfigurovat. Všechny virtuální stanice běží v tomto režimu a nacházejí se tak v jedné síti.

Adresní rozsah IPv4 byl nastaven na 10.0.0.0/8 a záměrně byla v rámci této sítě vypnuta podpora DHCP. Virtuální stroje fungující jako servery měly síťové adaptéry nastaveny manuálně, první měl adresu 10.0.0.10, druhý 10.0.0.20 a obdobně pro další stanice.

Adresy pro IPv6 byly zvoleny z rozsahu 2001:DB8::1:0/64 a jednotlivé virtuální stroje měly přidělené adresy 2001:DB8::1:10, 2001:DB8::1:20 a obdobně pro další stroje.

### 3.3.1 MySQL

Jelikož je databáze potřebná pro funkci PowerDNS, Kea i phpIPAM, bylo vhodné ji nainstalovat a nakonfigurovat jako první. V rámci sítě byly nastaveny tři databázové servery. První sloužil jako hlavní databáze, ve které se nacházela data pro PowerDNS master server a phpIPAM. Druhý MySQL server sloužil jako záložní databáze pro PowerDNS slave server a zároveň na něm běžel phpIPAM. Třetí server byl nastaven tak, aby se k němu dalo přistupovat vzdáleně a byl využíván kea DHCPv4 a kea DHCPv6 servery.

Pro všechny tři aplikace byly vytvořeny potřebné databáze, jejichž schémata jsou dostupná online nebo v instalačním adresáři jednotlivých aplikací. Tato schémata se pak dají snadno nainportovat, jen je třeba mít na paměti, že se mohou měnit v rámci vydání nových verzí, např. pro PowerDNS jsou databáze pro verze 4.1 a 4.2 odlišné.

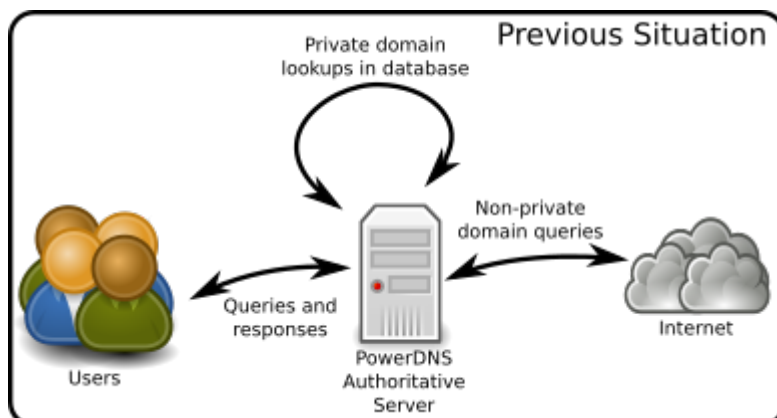
Samotná instalace pak probíhala dle pokynů v dokumentaci [9] a s pomocí online návodu [10]. Vytváření a nastavení jednotlivých databází a uživatelských účtů se pak řídilo pokyny pro instalaci jednotlivých aplikací, které tyto databáze využívaly.

V rámci instalace obou MySQL databází bylo nastaveno master-slave replikování dle dokumentace [11]. Tato varianta nastavení je doporučena především při použití PowerDNS master-slave konfigurace viz dokumentace [12]. Alternativním řešením pro synchronizaci záznamů v databázi je použití AXFR. Nevýhodou AXFR je to, že pokud dojde k smazání zóny na master serveru, slave server se tímto nikdy nedozví. Jediným řešením je pak nepoužívané zóny odebírat ručně. Tento problém v případě replikace přes databázi nehrozí.

### 3.3.2 PowerDNS

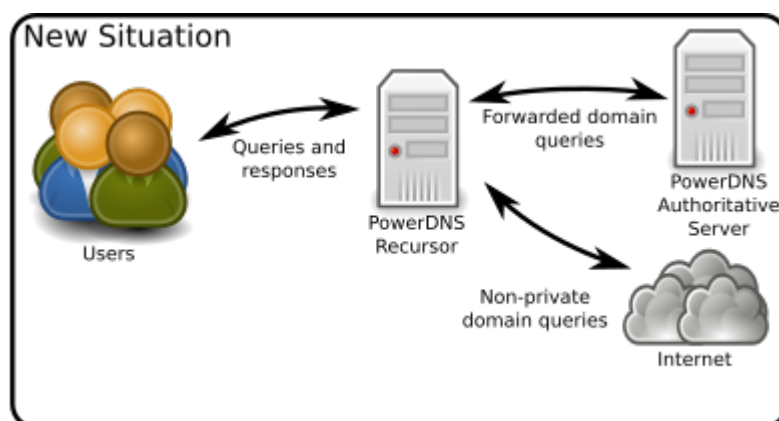
Instalace PowerDNS probíhala dle příslušných dokumentací pro autoritativní server [12] a rekurzor [13]. PowerDNS byl konfigurován v režimu master-slave. Na prvním stroji se nacházela příslušná primární MySQL databáze a master autoritativní server s rekurzorem. Na druhém stroji se pak nacházela záložní MySQL databáze a k ní patřící slave autoritativní server se sekundárním rekurzorem.

Pro nasazení byla zvolena konfigurace s rekurzorem. Rozdíl mezi konfiguracemi je znázorněn na obrázcích 3.1 a 3.2. Tato konfigurace je v praxi akceptována jako nejvhodnější a je doporučena i v rámci RFC2010 [14]. Má výhody především v oblasti bezpečnosti (např. zvýšená odolnost proti DoS útokům) a výkonnosti serverů (lepší rozložení zátěže), více informací např. zde [15].



**Obrázek 3.1:** Znázornění konfigurace bez rekurzoru. (Zdroj: [16]).

U rekurzorů je potřeba nastavit domény, u kterých dojde k přeposílání všech DNS dotazů na autoritativní server, viz obrázek 3.3. Zároveň je u rekurzoru dobré omezit adresní rozsahy, ze kterých bude přijímat dotazy. Implicitně jsou povoleny pouze privátní adresní rozsahy definované RFC 1918 a loopbacky. Pro master a slave rekurzor je konfigurační soubor stejný, výjimkou je pouze lokální adresa serveru. U autoritativních serverů je kromě



**Obrázek 3.2:** Znáznornění konfigurace s rekurzorem. (Zdroj: [16]).

lokální adresy potřeba změnit i přihlašovací údaje pro připojení do databáze, příklad takové konfigurace je zobrazen na obrázku 3.4 .

```
local-address=10.0.0.10, 2001:DB8::1:10
local-port=53
allow-from=127.0.0.0/8, 10.0.0.0/8, 001:DB8::1:0/64

forward-zones=example.com=127.0.0.1:5300
forward-zones+=pokus.example.com=127.0.0.1:5300
```

**Obrázek 3.3:** Ukázka části konfiguračního souboru master rekurzoru.

```
launch=gmysql
gmysql-host=127.0.0.1
gmysql-user=admin
gmysql-password=debian
gmysql-dbname=powerdns

local-address=127.0.0.1
local-ipv6>:::1
local-port=5300
```

**Obrázek 3.4:** Ukázka části konfiguračního souboru autoritativního serveru.

Dále je nutné nakonfigurovat webserver a api, aby bylo možné použít PowerDNS Admin aplikaci pro správu jednotlivých uživatelů, jejich práv, domén a zón. Údaje uvedené v těchto konfiguračních souborech se poté musí nakonfigurovat i v PowerDNS Admin aplikaci, jinak nebude databázové spojení správně fungovat. V úspěšné konfiguraci byla použita adresa autoritativního serveru. Aby bylo možné navázat spojení s databází přes PowerDNS Admin, musela být do konfigurace přidána adresa, ze které mohou aplikace přes api k databázi přistupovat. Jedná se o řádek `webserver-allow-from`, viz ukázka konfigurace na obrázku 3.5.

<p>Relevantní část konfigurace autoritativního serveru</p> <pre>api=yes api-key=api webserver=yes webserver-address=10.0.0.10 webserver-allow-from=0.0.0.0/0,:::/0,10.0.0.10 webserver-port=8081</pre>	<p>Relevantní část konfigurace rekurzoru</p> <pre>webserver=yes webserver-address=10.0.0.10 webserver-port=8082 webserver-allow-from=0.0.0.0/0,:::/0,10.0.0.10</pre>
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------

Obrázek 3.5: Ukázka konfigurace api webového rozhraní.

### 3.3.3 PowerDNS Admin

Hlavní informace k instalaci pocházejí z wiki stránky projektu na gitlabu [17]. Tyto informace ale neobsahují všechny potřebné kroky pro správné nastavení a nakonfigurování aplikace. Proto úplně zprovoznění tak byly použité i návody z webových stránek a blogů nacházejících se zde [18] a [19] a [20].

Mnoho komplikací se správnou funkčností spočívalo ve správném nastavení práv pro určité soubory a některé adresáře. Bylo nutné správně nastavit vlastníka pro kořenový webový adresář aplikace (v mém případě www-data:www-data). Zároveň ale bylo třeba u některých podadresářů nastavit vlastníka a skupinu tak, aby odpovídaly hodnotám setuid a setegid uvedeným v konfiguračních souborech pro aplikaci PowerDNS.

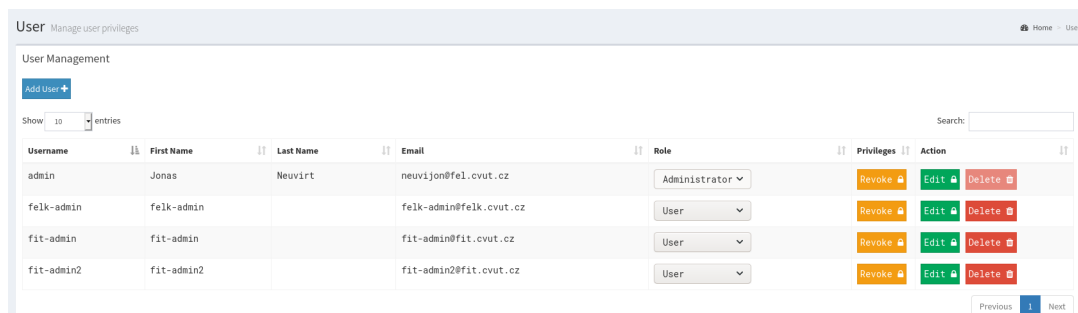
Další komplikací bylo zprovoznění socketu, na kterém PowerDNS Admin naslouchal. Při konfiguraci se samostatně nastavuje PowerDNS-Admin.service a PowerDNS-Admin.socket viz [21]. Správně by se měla zapnout PowerDNS-Admin.service, která pak spustí i příslušný socket. Pokud ale dojde k restartování této service, dojde i k restartování socketu. Z nějakého důvodu (který dodnes není znám) se tento socket po restartování nejdříve otevře, ale poté se ihned uzavře. Proces PowerDNS-Admin.service si i přesto myslí, že je vše v pořádku. Výsledkem je, že aplikace není schopná se spojit s PowerDNS databází.

Nalezené řešení je, že před každým restartováním PowerDNS-Admin.service je nejprve nutné manuálně zastavit PowerDNS-Admin.socket. Až poté je možné nastartovat proces PowerDNS-Admin.service, který si zároveň při inicializaci otevře i svůj příslušný funkční socket.

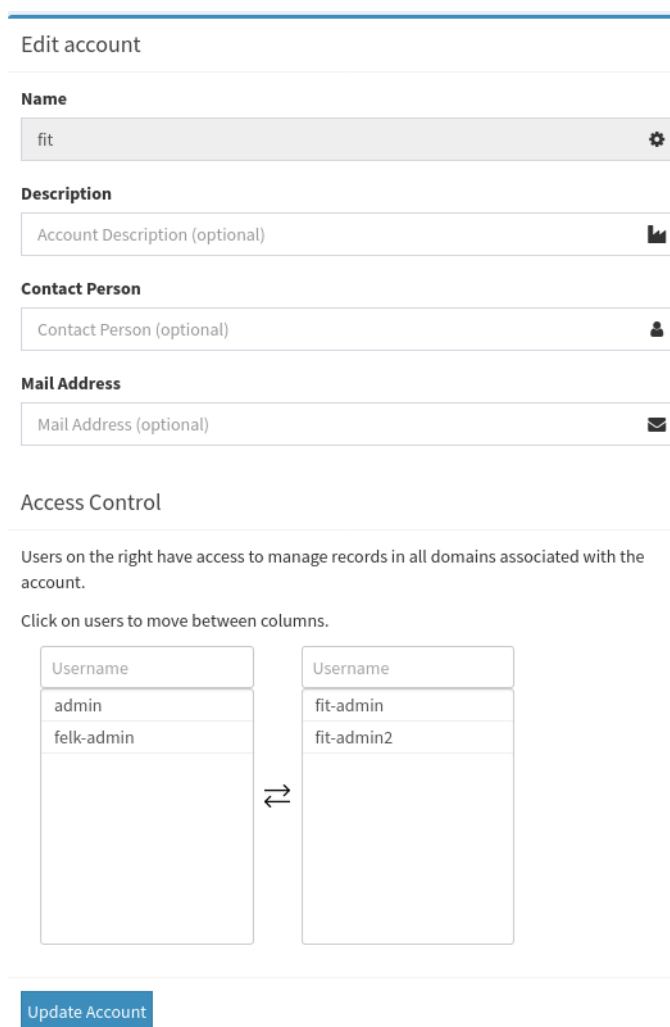
Při prvním spuštění PowerDNS-Admin je nutné se nejprve zaregistrovat. První registrovaný uživatel se pak stává administrátorem s plnými přístupovými právy, všichni následující registrovaní uživatelé začínají v roli user. Admin uživatel poté může tyto role libovolně měnit, ukázka na obrázku 3.6.

Přiřazení jednotlivých uživatelů ke správě domén pak probíhá pomocí tzv. accounts (účetů). Po registraci uživatel nemůže nic spravovat. Nejprve je nutné ho přiřadit do skupiny uživatelů, která má právo editovat všechny domény, které jsou vlastněny daným účtem. Na obrázku 3.7 je ukázána konfigurace pro účet jménem fit. Na levé straně je okno se všemi registrovanými uživateli v rámci celé aplikace. Na pravé straně jsou uživatelé fit-admin1 a fit-admin2, kteří spadají pod účet fit. Tito uživatelé pak mohou spravovat všechny domény, které rovněž spadají pod tento účet.

Na obrázku 3.8 je ukázka pro vytvoření domény feld.cvut.cz. Při jejím



Obrázek 3.6: Ukázka správy uživatelů v aplikaci PowerDNS Admin.



Obrázek 3.7: Ukázka přiřazení uživatelů fit-admin1 a fit-admin2 pod účet fit.

vytváření je nutno uvést účet, pod který tato doména spadá (zde se jedná o účet feld). Všichni uživatelé, kteří jsou přiřazení k účtu feld, pak mohou provádět změny v konfiguraci této domény. Na obrázku 3.9 je pak ukázka vytváření nového záznamu pro doménu felk.cvut.cz, kde lze rovněž vidět i všechny ostatní záznamy spadající pod tuto doménu.

The screenshot shows the PowerDNS-Admin interface. On the left is a dark sidebar with navigation options: Dashboard, New Domain, PDNS, Global Search, History, Domain Templates, Accounts, Users, API Keys, and Settings. The main content area is titled 'Domain Create new' and contains a 'Create new domain' form. The form has the following fields and options:

- Domain name: feld.cvut.cz
- Zone name: feld
- Type: Native (selected), Master, Slave
- Select a template: No template
- SOA-EDIT-API: DEFAULT (selected), INCREASE, EPOCH, OFF
- Buttons: Submit, Cancel

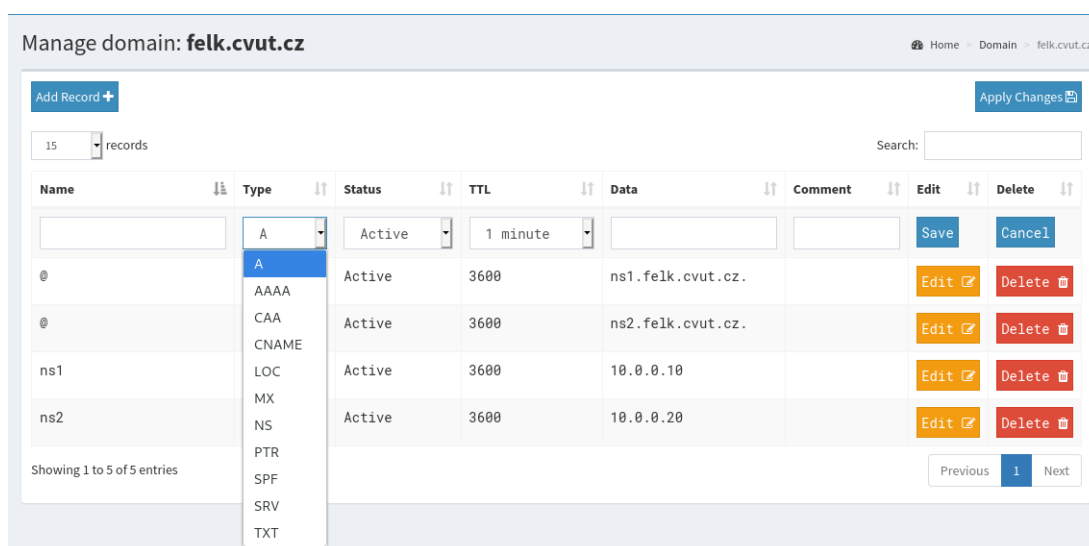
**Obrázek 3.8:** Ukázka vytvoření nové domény feld.cvut.cz.

Při přihlášení je vidět na úvodní straně přehled všech hostovaných domén. Ukázka je na obrázku 3.10, kde vybraná záložka Hosted Domains, která zobrazuje domény ipv4.

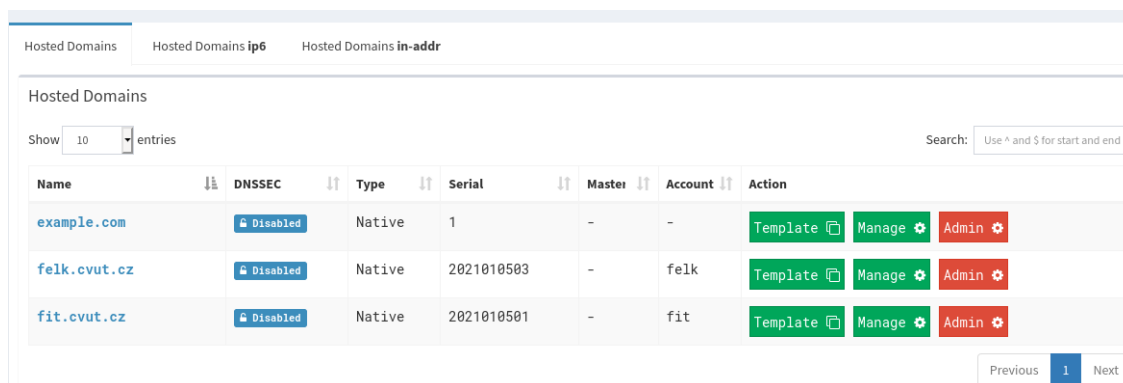
### 3.3.4 PhpIPAM

K instalaci phpIPAM byla použita dokumentace [8] a návod [22], v rámci konfigurace apache2 serveru byla ještě využita dokumentace pro VirtualHosts [23].

PhpIPAM byl instalován na stejných strojích, kde byly instalovány PowerDNS servery. Prvním důvodem je přístup k příslušné databázi pouze z localhost, a to z důvodu bezpečnosti. V případě, že by se vzdálený přístup k databázi nepovažoval za bezpečnostní riziko, postačila by pouze jedna instalace phpIPAM. Pokud by pak bylo potřeba přistupovat k databázi mimo localhost, stačilo by vytvořit uživatele s oprávněním přístupu z venčí. Lze nastavit i přístup z



Obrázek 3.9: Ukázka vytvoření nového záznamu pro doménu felk.cvut.cz.



Obrázek 3.10: Přehled všech hostovaných domén.

konkrétní ip adresy, takže limitovat přístup na konkrétní stanici v síti<sup>1</sup>

Druhým důvodem pro dvojí instalaci je eliminace single point of failure (SPOF), aby bylo možné v případě výpadku primárního serveru stále využívat phpIPAM k monitorování sítě.

Po instalaci je nutné integraci s PowerDNS zapnout v záložce nastavení. Aby bylo možné spravovat DNS záznamy, musí se nastavit přihlašovací údaje pro připojení k databázi PowerDNS serveru. K tomu je potřeba vytvořit pro phpIPAM uživatelský účet se správně nastavenými přístupovými právy.

### 3.3.5 Kea

Podle dokumentace [24] přibyla od verze 1.6 možnost instalovat Kea pomocí balíčků. Konfigurace pak vycházela z online dokumentace [25] a záznamu z webinaru [26]. Zároveň zde byla nainstalována i MySQL databáze. Kea je

<sup>1</sup>Za předpokladu, že daná ip adresa je nakonfigurována staticky.



Name	Type	Content	TTL
NS records			
test.com	SOA	ns1.bakal.cz admin.test.com 2020081405 21600 7200 86400 10800	86400
test.com	NS	ns1.bakal.cz	86400
test.com	NS	ns2.bakal.cz	86400
main records			
more.test.com	A	192.0.0.5	1800
test.com	A	192.168.0.5	86400

**Obrázek 3.11:** Ukázka správy doménových záznamů PowerDNS v phpIPAM.

implementovaná zvláště pro DHCPv4 a DHCPv6, takže nakonec v rámci sítě musí běžet celkem čtyři Kea servery a jeden MySQL server.

Tento server má povolený vzdálený přístup, který je nutný v případě, že požadujeme, aby v síti mohlo být více DHCP serverů najednou. Tyto servery jsou pak nastaveny v konfiguraci High Availability, kdy oba sdílejí danou Kea databázi.

Zároveň je dobré nastavit heartbeat interval na rozumnou hodnotu, aby při výpadku jednoho serveru netrvalo příliš dlouho, než se o tom sekundární server dozví. V dokumentaci je ještě popsána alternativní metoda nasazení, kdy každý Kea server má svou vlastní příslušnou databázi. Synchronizace pak není řešena přes Kea servery, ale je místo toho ponechána na databázových serverech.

### 3.3.6 Stork

Instalace probíhala z balíčků dostupných pro debian dle online dokumentace [27]. Stork je složený ze dvou částí - Stork Server a Stork Agent. Na celou síť stačí jeden Stork server, který pak komunikuje s jednotlivými Stork agenty. Tito agenti se nacházejí na každém stroji, kde běží nějaká instance kea-dhcp serverů. Tito agenti pak monitorují jednotlivé stroje (CPU, RAM, status) a informace posílají Stork Serveru. Momentálně je podporována pouze databáze PostgreSQL, takže musela být prozatím nainstalována v rámci laboratoře. Do budoucna je plánována i podpora dalších databázových systémů. Aby byl Stork Server schopen číst statistiky o zapůjčených ip adresách, je třeba mít nakonfigurovanou knihovnu Stat Commands. Tato knihovna je volně dostupná všem uživatelům. Pro čtení rezervovaných ip adres z databáze je

třeba mít knihovnu Host Commands, která je však placená.

Po instalaci je automaticky vytvořen uživatel admin. Ten pak může přidat další uživatele. Pro sledování statistik je nejprve nutné zaregistrovat jednotlivé stroje v rámci Stork aplikace. Přidávají se přes grafické rozhraní za použití ip adres a portů všech strojů, na kterých běží jednotlivý agenti. Po připojení agentů je pak Stork schopen zobrazovat informace i jednotlivých strojích a jejich nakonfigurovaných podsítí včetně jejich obsazení.

## ■ 3.4 Postup v reálné síti

Strategie pro nasazení všech aplikací v rámci v reálné síti by se výrazně nelišila od postupu nasazování během laborek. Ideálně by se jednotlivé servery připravily mimo aktivní síť. Konkrétně by se jednalo o nastavení konfiguračních souborů v jednotlivých virtuálech. Po otestování funkčnosti v rámci uzavřeného prostředí by se pak tyto servery zpřístupnily pro celou síť.

### ■ 3.4.1 Nasazení DNS

Pro nasazení DNS by bylo vhodné nasadit hlavní a záložní DNS server tak, že běží zároveň s aktivními DNS servery. Jelikož však nejsou nabízeny v rámci DHCP konfigurace, uživatelé v síti je nebudou využívat. Po nasazení se pak upraví adresy DNS serverů tak, aby byly nabízeny v rámci DHCP pouze nové DNS servery.

### ■ 3.4.2 Nasazení DHCP

Při nasazení DHCP služby dojde k výpadku, jelikož v opačném případě by při přechodu mezi servery došlo ke ztrátě informací o zrovna zapůjčených adresách. Nové servery totiž neví, které adresy jsou už zapůjčeny, takže by pak mohly nabízet ještě obsazené adresy. Tomuto problému se dá vyhnout tak, že se lease time nastaví na nízkou hodnotu. Zároveň poté nenecháme DHCP službu zapůjčovat nové adresy. Jakmile uplyne doba krátkého lease time, víme, že v síti už nejsou žádné obsazené adresy, můžeme tak přejít na nové DHCP servery s tím, že není šance, aby nastaly případné kolize.

### ■ 3.4.3 Nasazení databáze

MySQL databáze lze do sítě zapojit bez výraznějších problémů. Jednotlivá databázová schémata jsou dostupná u instalačních souborů či v instalačních adresářích, při samotném importování je velmi nepravděpodobné, že by došlo k chybě, která by mohla způsobit výpadek databáze. V případě, že by se v síti již nacházela běžící databáze, není problém do ní za běhu vložit nové tabulky, které by byly nutné pro instalaci nových aplikací.

## Kapitola 4

### Postup testování

V této kapitole bude rozebráno a navrženo, jak je možné síť otestovat. Testování výsledné konfigurace je možné rozdělit do dvou hlavních kategorií. Jedná se nejprve o testování funkčnosti všech instalovaných nástrojů a poté o zátěžové testování.

Druhou testovací kategorií by pak byly testy zátěžové, kde by se kladl důraz na rychlost a výkonost jednotlivých serverů. Do této části testování by bylo zahrnuto i testování sítě na výpadky různých jejích částí, a testovalo by se, jak dobře se s těmito nečekanými situacemi síť vypořádá.

#### 4.1 Testování funkčnosti

V rámci první kategorie by se jednalo o testování funkcionality všech implementovaných nástrojů. Toto testování by se soustředilo především na testování základních činností jednotlivých aplikací v kontrolovaném prostředí, kdy nehrozí, že by nastaly nějaké nenadálé situace. Pokud by se toto testování dokončilo úspěšně, bylo by možné přejít do následující fáze testování. V této fázi lze i simulovat výpadky jednotlivých serverů a testování toho, jestli správně fungují záložní servery.

Hlavními vhodnými nástroji pro toto testování jsou ping (test dostupnosti jednotlivých aplikací v rámci sítě) a nástroj dig, který je dostupný v balíčku dnstools a umožňuje vytvářet DNS dotazy. Výpadky jednotlivých serverů se dají simulovat zastavením a spouštěním příslušných procesů.

#### 4.2 Zátěžové testování

Druhou testovací kategorií by pak byly testy zátěžové, kde by se kladl důraz na rychlost odezvy a vyřízení jednotlivých požadavků. Poté by přišlo na řadu výkonnostní testování jednotlivých serverů, kde by se dalo zjistit maximální možné množství požadavků, které servery zvládnou vyřídit najednou.

Kea poskytuje vhodný nástroj pro toto zátěžové testování nazvaný perfdhcp, dokumentace a příklady použití jsou dostupné online [28] a i jako video zde [29]. Tento nástroj simuluje zařízení v síti a zároveň sbírá data a počítá

#### 4. Postup testování

---

statistiky (např. počty přijatých, odeslaných a ztracených paket či rychlost odezvy).



## Kapitola 5

### Závěr

V rámci vypracování bakalářské práce jsem potýkal se síťovými problémy, které se velice pravděpodobně v praxi běžně vyskytují. Osobně jsem vůbec nepočítal s tím, jak náročné by mohlo být navrhnout a nakonfigurovat laboratorní síť obsahující DHCP, DNS a IPAM nástroje od úplného počátku. V průběhu Jedná se například o problémy typu neviditelných chyb v konfiguračních souborech, kterých se jen velmi těžko zbavuje. Konkrétně bych zmínil třeba tečku na konci DNS záznamu, která se dostala do databáze narušila funkčnost PowerDNS serverů. Odhalena byla až po jednom dni hledání. Rovněž se mi povedlo při instalaci databáze vybrat špatnou verzi databázového schématu. Trvalo poměrně dlouho, než jsem přišel na to, proč mi nefunguje správně ukládání dat do databáze.

Celkově jsem se naučil mnoho nových věcí a především jsem získal mnoho cenných zkušeností v oblasti konfigurace počítačových sítí, tvorby a virtualizace strojů včetně práce s virtuálními sítěmi. Zároveň jsem výrazně zlepšil v rámci práce s linuxovými operačními systémy. Navíc pak ještě mnohem lépe rozumím tomu, jak přistupovat ke konfiguraci a instalaci více než jedné aplikace v rámci jedné sítě.





## Bibliografie

- [1] Vít Pekárek. *Správa IP adres ve středně velké síti*. Bakalářská práce. Praha: České vysoké učení technické v Praze, Fakulta informačních technologií, 2019. Dostupné z: <https://dspace.cvut.cz/handle/10467/83239>.
- [2] Vicky Risk. *Kea 1.4 Adds High-Availability Mode*. [online]. Naposledy navštíveno: 28.12.2020. Dostupné z: <https://www.isc.org/blogs/kea-1-4-adds-high-availability-mode/>.
- [3] Vicky Risk. *Kea 1.6 Adds Configuration Database*. [online]. Naposledy navštíveno: 14.8.2020. Dostupné z: <https://www.isc.org/blogs/kea-1-6/>.
- [4] Internet Systems Consortium. *API Reference*. [online]. Naposledy navštíveno: 28.12.2020. Dostupné z: <https://kea.readthedocs.io/en/latest/api.html>.
- [5] Internet Systems Consortium. *API Reference*. [online]. Naposledy navštíveno: 28.12.2020. Dostupné z: <https://kea.readthedocs.io/en/kea-1.6.1/api.html?highlight=config-set>.
- [6] Miha Petkovsek. *Kea DHCP management functional?* [online]. Naposledy navštíveno: 14.8.2020. Dostupné z: <https://github.com/phpipam/phpipam/issues/777>.
- [7] debian.org. *Debian CD/DVD images*. [online]. Naposledy navštíveno: 14.8.2020. Dostupné z: <https://cdimage.debian.org/debian-cd/current-live/amd64/iso-hybrid/>.
- [8] phpipam.net. *Phpipam Installation Guide*. [online]. Naposledy navštíveno: 14.8.2020. Dostupné z: <https://phpipam.net/documents/installation/>.
- [9] mariadb.com. *Where to Download MariaDB*. [online]. Naposledy navštíveno: 14.8.2020. Dostupné z: <https://mariadb.com/kb/en/getting-installing-and-upgrading-mariadb/>.
- [10] Justin Ellingwood, Brian Boucheron a Hanif Jetha. *How To Install the Latest MySQL on Debian 10*. [online]. Naposledy navštíveno: 14.8.2020. Dostupné z: <https://www.digitalocean.com/community/tutorials/how-to-install-the-latest-mysql-on-debian-10>.

- [11] MariaDB. *Setting up a Replication Slave with Mariabackup*. [online]. Naposledy navštíveno: 28.12.2020. Dostupné z: <https://mariadb.com/kb/en/setting-up-replication/>.
- [12] powerdns.com. *PowerDNS Authoritative Nameserver*. [online]. Naposledy navštíveno: 28.12.2020. Dostupné z: <https://doc.powerdns.com/authoritative/index.html>.
- [13] powerdns.com. *PowerDNS Recursor*. [online]. Naposledy navštíveno: 28.12.2020. Dostupné z: <https://docs.powerdns.com/recursor/indexTOC.html>.
- [14] P. Vixie B. Manning. *Operational Criteria for Root Name Servers*. [online]. Naposledy navštíveno: 28.12.2020. Dostupné z: <https://tools.ietf.org/html/rfc2010>.
- [15] Whalebone. *4 crucial reasons why ISPs should separate their authoritative and recursive DNS servers*. [online]. Naposledy navštíveno: 28.12.2020. Dostupné z: <https://www.whalebone.io/separate-dns-servers/>.
- [16] powerdns.com. *Migrating from using recursion on the Authoritative Server to using a Recursor*. [online]. Naposledy navštíveno: 28.12.2020. Dostupné z: <https://doc.powerdns.com/authoritative/guides/recursion.html>.
- [17] Khanh Ngo. *Home*. [online]. Naposledy navštíveno: 28.12.2020. Dostupné z: <https://github.com/ngoduykhanh/PowerDNS-Admin/wiki>.
- [18] Hitesh Jethva. *How to Install PowerDNS Server and PowerDNS Admin on Ubuntu 20.04*. [online]. Naposledy navštíveno: 28.12.2020. Dostupné z: <https://www.howtoforge.com/how-to-install-powerdns-admin-on-ubuntu-20-04/>.
- [19] Josphat Mutai. *Install PowerDNS and PowerDNS-Admin on Ubuntu 18.04 / Debian 9 with MariaDB Backend*. [online]. Naposledy navštíveno: 28.12.2020. Dostupné z: <https://computingforgeeks.com/install-powerdns-and-powerdns-admin-on-ubuntu-18-04-debian-9-mariadb-backend/>.
- [20] koromicha. *Easily Install and Setup PowerDNS Admin on Ubuntu 20.04*. [online]. Naposledy navštíveno: 28.12.2020. Dostupné z: <https://kifarunix.com/easily-install-and-setup-powerdns-admin-on-ubuntu-20-04/>.
- [21] Patrik Cevla. *Running PowerDNS Admin with Systemd, Gunicorn and Nginx*. [online]. Naposledy navštíveno: 28.12.2020. Dostupné z: <https://github.com/ngoduykhanh/PowerDNS-Admin/wiki/Running-PowerDNS-Admin-with-Systemd,-Gunicorn--and--Nginx>.
- [22] Josphat Mutai. *Install and Configure phpIPAM on Ubuntu 20.04/18.04 / Debian 10 Linux*. [online]. Naposledy navštíveno: 14.8.2020. Dostupné z: <https://computingforgeeks.com/install-and-configure-phpipam-on-ubuntu-debian-linux/>.



- [23] apache.org. *VirtualHost Examples*. [online]. Naposledy navštíveno: 28.12.2020. Dostupné z: <https://httpd.apache.org/docs/2.4/vhosts/examples.html>.
- [24] Vicky Risk, Suzanne Goldlust a Michal Nowikowski. *ISC Packages for Kea DHCP*. [online]. Naposledy navštíveno: 14.8.2020. Dostupné z: <https://kb.isc.org/docs/isc-kea-packages>.
- [25] Internet Systems Consortium. *Kea Administrator Reference Manual*. [online]. Naposledy navštíveno: 14.8.2020. Dostupné z: <https://kea.readthedocs.io/en/kea-1.6.2/index.html>.
- [26] Eddy Winstead. *Getting Started with Kea*. [online]. Naposledy navštíveno: 14.8.2020. Dostupné z: <https://www.youtube.com/watch?v=446Ew0P0kTw>.
- [27] Internet Systems Consortium. *Stork Administrator Reference Manual*. [online]. Naposledy navštíveno: 28.12.2020. Dostupné z: <https://kea.readthedocs.io/projects/Stork/en/v0.14.0/index.html>.
- [28] Marcin Siodelski Tomasz Mrugalski. *DHCP Performance Guide*. [online]. Naposledy navštíveno: 28.12.2020. Dostupné z: <https://users.isc.org/~tomasz/perfdhcp/dhcp-perf-guide.html>.
- [29] Prowse Tech. *Kea DHCP4 Basic Performance Testing*. [online]. Naposledy navštíveno: 28.12.2020. Dostupné z: <https://www.youtube.com/watch?v=IW3eXTM9skc>.





## Příloha A

### Seznam zkratk

---

AXFR	Asynchronous Zone Transfer Protocol
ČVUT	České vysoké učení technické
DHCP	Dynamic Host Configuration Protocol
DoS	Denial of Service
DNS	Domain Name System
HA	High Availability
IPAM	IP Address Management
ISC	Internet Systems Consortium
RFC	Request for Comments
SPOF	Single Point of Failure