**UNICORN VYSOKÁ ŠKOLA S.R.O.**

BAKALÁŘSKÁ PRÁCE

**2022 Vojtěch Šetina**

**UNICORN VYSOKÁ ŠKOLA S.R.O.**

**Softwarový vývoj**

****

**BAKALÁŘSKÁ PRÁCE**

**Profylaxe síťových prvků**

**Autor BP:** Vojtěch Šetina

**Vedoucí BP:** Ing. Radim Roška

*Vzor:* ***ZADÁNÍ ZÁVĚREČNÉ PRÁCE*** *– originál, kopie originálu, naskenovaná podoba – dle jednotlivých forem (originál, 2 x kopie, elektronická verze)*

*Vzor:* ***ČESTNÉ PROHLÁŠENÍ*** *– prohlášení o samostatném vypracování závěrečné práce, datum a vlastnoruční podpis (v každém výtisku práce)*

**Čestné prohlášení**

Prohlašuji, že jsem svou bakalářskou práci na téma profylaxe síťových prvků vypracoval/a samostatně pod vedením vedoucího bakalářské práce a s použitím výhradně odborné literatury a dalších informačních zdrojů, které jsou v práci všechny citovány a jsou také uvedeny v seznamu použitých zdrojů.

Jako autor/ka této bakalářské práce dále prohlašuji, že v souvislosti s jejím vytvořením jsem neporušil/a autorská práva třetích osob a jsem si plně vědom/a následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb.

Dále prohlašuji, že odevzdaná tištěná verze bakalářské práce je shodná s verzí, která byla odevzdána elektronicky.

V……Praze…. dne ……….. …….……………………………

Vojtěch Šetina

*Vzor:* ***PODĚKOVÁNÍ*** *vedoucímu BP, konzultantům, odborníků, spolupracovníkům za poskytnuté rady a podkladové materiály apod.) –* ***není povinné***

**Poděkování**

Např: Děkuji vedoucímu bakalářské práce Ing. Radimovi Roškovi za účinnou metodickou, praktickou a odbornou pomoc a další cenné rady při zpracování mé bakalářské práce.

*Vzor:* ***PRVNÍ ČÍSLOVANÁ STRANA*** *– číslice na první číslované straně se určí podle počtu předchozích stran, počínaje Titulní stranou, tzn. že pokud jsou řazené všechny dané strany – Titulní strana, Zadání (2 strany), Čestné prohlášení a Poděkování – je první číslovaná strana stranou 6.*

**

**Profylaxe síťových prvků**

**Prophylaxis of network devices**

*Vzor: ABSTRAKT A KLÍČOVÁ SLOVA*

**Abstrakt**

Cílem bakalářské práce je vytvoření programu, který výrazně usnadní a zjednoduší dokumentaci síťové infrastruktury a skrz lepší znalost prostředí pomůže zvýšit úroveň zabezpečení. Program bude řešit problém profylaxe síťových prvků a její automatizaci.

V teoretické části je hlavním cílem zmapovat trh a srovnat nabízené řešení síťové inventarizace od několika výrobců. Řešením bude rešerše a průzkum trhu.

V praktické části se práce soustředí na vytvoření a implementaci samotného scriptu. Program bude rozdělen do dvou částí. První část programu bude mít na starost dokumentaci a sběr dat ze síťových zařízení. Výsledkem budou tabulky se seznamem prvků – identifikace hardware modelu, nasazená verze operačního systému, používaných IP sítí, aktivních VLAN a IP rozhraní. Součástí bude také seznam všech portů a jejich konfigurace. V další části půjde o kontrolu nastavení zejména v kontextu doporučených bezpečnostních principů dle best-practice.

Klíčová slova: Počítačové sítě, administrace, automatizace, switch, inventarizace

**Abstract**

The aim of the bachelor thesis is to create a program that will greatly simplify and simplify the documentation of the network infrastructure and through better knowledge of the environment will help to increase the level of security. The program will address the problem of network element prophylaxis and its automation.

In the theoretical part, the main objective is to map the market and compare the network inventory solutions offered by several vendors. The solution will be a research and market survey.

In the practical part, the work will focus on the creation and implementation of the script itself. The program will be divided into two parts. The first will be in charge of the documentation and visualization of the network topology. The result will be tables with a list of elements - identification of the hardware model, deployed operating system version, IP networks used, active VLANs and IP interfaces. It will also include a list of all ports and their configurations. The next part will be a check of the settings, especially in the context of recommended security principles according to best-practice.

Keywords: Computer networks, administration, automatization, switch, inventarization

*Vzor:* ***OBSAH*** *– hierarchické uspořádání číslovaných názvů kapitol a podkapitol, včetně všech příloh, spolu s čísly jejich stran. Dále se uvádí Seznam obrázků/tabulek/grafů. Pozn.: počet a názvy kapitol samozřejmě odpovídají charakteru konkrétní práce.*

**Obsah**

[Úvod 11](#_Toc109668243)

[1 Úvod 12](#_Toc109668244)

[1.1 Motivace 12](#_Toc109668245)

[1.2 Struktura 12](#_Toc109668246)

[1.3 Cíl 12](#_Toc109668247)

[2 Rešerše a průzkum trhu 13](#_Toc109668248)

[2.1 Existující komerční řešení 13](#_Toc109668249)

[2.2 Dostupné opensource nastroje 15](#_Toc109668250)

[3 Analýza 18](#_Toc109668251)

[4 Návrh řešení 19](#_Toc109668252)

[4.1 Workflow 19](#_Toc109668253)

[Závěr 22](#_Toc109668254)

[Seznam použitých zdrojů 23](#_Toc109668255)

[Seznam obrázků (existují-li) 25](#_Toc109668256)

[Seznam grafů (existují-li) 27](#_Toc109668257)

[Seznam příloh (existují-li) 28](#_Toc109668258)

[Příloha A – Název přílohy 29](#_Toc109668259)

[Příloha B – Název přílohy 30](#_Toc109668260)

*Vzor:* ***ÚVOD*** *(cca 5-10 normostran)*

# Úvod

V mé bakalářské práci se převážně věnuji tématu profylaxe síťových prvků a její automatizaci. Ačkoli by se mohlo na první pohled zdát, že síťová dokumentace a administrace nejsou tak tíživé a náročné úlohy, ze své vlastní zkušenosti vím, že se jedná o vcelku komplexní problém. Z několika desítek projektů pro střední a velké firmy, na kterých jsem se v rámci své pracovní náplně podílel, jsem si mohl udělat obrázek, jak moc je síťová infrastruktura a její dokumentace podceňovaná. Z jednoduchého průzkumu u zákazníků a síťových specialistů jasně vyplívá, proč je administrace a dokumentace ve firmách na nízké úrovni. Jedná se totiž zpravidla o inventární a repetitivní práci. I když jde o neoblíbenou úlohu, která má na první pohled málo využití, tak hraje obrovskou roli v řešení incidentů a výrazně ovlivňuje bezpečnost celé firmy. Se stále se měnicí topologií a inventářem síťových prvků je časově velmi náročné udržovat aktuální stav celého prostředí. K mému velkému překvapení se většina firem o komplexní dokumentaci a inventarizaci vůbec nestará a pokud ano, většinu práce provádí administrátoři „ručně“ – tedy bez použití automatizovaných programů a nástrojů. To má za následek větší riziko chyb a vyšší časovou náročnost.

*Vzor:* ***VLASTNÍ TEXT*** *závěrečné práce uspořádaný hierarchicky do kapitol a podkapitol, každá kapitola (úrovně 1) musí být vždy na nové straně.*

# Úvod

Autor/autorka uvedou vlastní název kapitoly vztahující se ke konkrétnímu tématu práce

## Motivace

Hlavní motivací ke zvolení tohoto tématu byla především snaha zefektivnit a automatizovat soubor úkonů, které se používají k vytvoření takzvané profylaxe. Skládá se zejména z kontroly a získaní dat ze síťových prvků a jejich následné vyhodnocení. Vzhledem k tomu že pracuji ve firmě, která nabízí profylaxi jako jeden z mnoha produktů a dosavadní postup byl tvořen převážně kroky, u kterých byla potřeba stálá intervence technika, jako je například přihlášení se do síťových prvků a následný manuální sběr informací přímo z příkazové řádky nebo tvoření tabulek, rozhodl jsem se celý tento postup zefektivnit jak časově, tak i z hlediska využití lidských zdrojů. Téma automatizace je mi velmi blízké a v mém oboru působnosti se bez něj nelze obejít. V dnešním rychle se měnícím světě je potřeba využívat možnosti nejnovějších technologií pro automatizaci a stále tak zefektivňovat a šetřit čas na úlohy, které zatím stroje nejsou schopny vykonat za nás.

## Struktura

Struktura bakalářské práce se skládá ze dvou hlavních částí, a to z části teoretické a praktické. Teoretická část obsahuje převážně informace ohledně síťové dokumentace a inventarizace, ale také srovnání dosavadních nástrojů na trhu a jejich výhody i nevýhody. Hlavní náplní praktické části je poté vytvoření skriptu se všemi náležitostmi jako je diagram, dokumentace a popis hlavních funkcí programu.

## Cíl

Hlavním cílem této bakalářské práce je vytvoření programu, který výrazně usnadní a zjednoduší dokumentaci síťové infrastruktury a skrz lepší znalost prostředí pomůže zvýšit úroveň zabezpečení. Největší důraz bude kladen na automatizaci celého řešení profylaxe. Výstupem programu budou tabulky se seznamem prvků a jejich informacemi společně s best-practise principy pro zabezpečení a zvýšení transparentnosti síťové infrastruktury. Program bude mít konfigurační soubor a dokumentaci pomocí které bude možno script jednoduše upravit podle toho, co bude dané řešení vyžadovat. Program bude primárně podporovat prvky od výrobce Huawei a Cisco.

# Rešerše a průzkum trhu

PRIDAT ITAM – vysvetleni, odkazy, web, reference

Síťová administrace má celosvětově obrovský trh, a to hned z několika důvodů. Každá firma, ať už se jedná o malou či velkou, má několik síťových prvků, na kterých stojí celý její chod. Z pravidla se jedná o switche a routery, ale také firewally. Těchto zařízení může být ve společnosti vysoký počet a jednoduše se tak může stát, že ztratíme přehled o těchto zařízeních. Se stále narůstajícím rizikem kyberútoků je důležité mít svou infrastrukturu pod kontrolou, mít aplikované nejnovější opravy chyb (patche) a dělat pravidelné kontroly zabezpečení. S tím souvisí i délka podpory zařízení od výrobce, která garantuje vydávání patchů a nových verzí s opravami chyb ať už z hlediska funkčního nebo bezpečnostního. U různých modelů se časový úsek podpory liší a je tak velmi důležité mít přehled a dostatek informací o každém zařízení v síti.

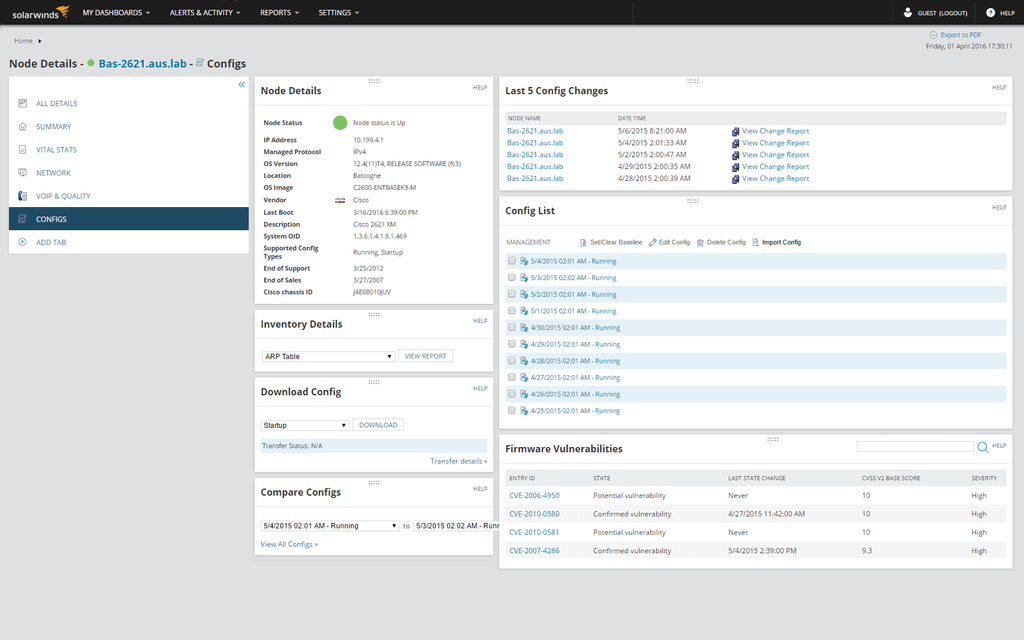
V rámci správy síťových zařízení je na začátku důležité zavést a vysvětlit zkratku ITAM. ITAM neboli “It asset management” je pojem používaný pro činnosti spojené se správou a inventatirazací veškerých firemních aktiv spjatých s informačními technologiemi. Z hardwaru může být příkladem již výše zmiňovaný switch či router, ale také server, kamerový systém a další. Ze softwaru jsou tu poté operační systémy, licence a další. Také se může jednat například i o podporu výrobce k různým zařízením či certifikáty zaměstnanců nebo firmy jako celku, které vetšinou přestavájí platit po domluveném čase. Je tedy velmi důležité mít o těchto aktivech přehled, aby se předešlo zbytečným ztrátám firemních prostředků.

## 

## Existující komerční řešení

Jeden z největších hráčů na trhu se síťovou administrací je SolarWinds. SolarWinds nabízí velké množství systému a služeb, které ulehčují práci nejen síťovým administrátorům ale také provozním inženýrům a jiným specialistům. Komerční řešení od této společnosti má mnoho skvělých funkcí, jako je například automatické nalezení nových prvků v síti nebo automatickou konfiguraci zařízení. Tento nástroj je velice robustní a vcelku spolehlivý, avšak je relativně drahý, a proto je převážně určen velkým firmám s vysokým počtem vlastních zařízení. Pro menší či střední společnosti s nižším počtem síťových zařízení se nástroj nehodí, ať už jde o pokročilé funkce, které menší podniky nevyužijí, nebo o samotnou cenu tohoto nástroje.

**Obrázek 1 SolarWinds – detail zařízení:**



Firma Armis, která byla založena v roce 2015 patří mezi špičky v odvětví zabezpečení a inventarizace počítačových sítí. Softwarová platforma je nasazována v cloudu, do kterého se skrz nainstalovaného agenta posílá telemetrie pro následné vyhodnocení. Výhodou je obrovská databáze zařízení od switchů předních výrobců po různá IOT zařízení, díky které může systém vyhodnotit o jaké zařízení se jedná a například okamžitě použít takzvaný „Virtual Patching“ pro ochranu zařízení bez nutnosti instalace softwaru přímo na daném zařízení. Firma se primárně zaměřuje na bezpečnost sítě, ale systém má i několik funkcí ke konfiguraci zařízení.

Další společností, která se specializuje na automatizaci síťové administrace je firma Auvik. Software této firmy, který je designován tak, aby běžel přímo v cloudu, nabízí propracované funkce a širokou podporu zařízení od mnoha výrobců. Auvik klade velký důraz na automatizaci a jednoduchost používaní a nabízí také mnoho integrací do nástrojů třetích stran jako je například komunikační nástroj Slack nebo ticketovací systém Freshdesk.

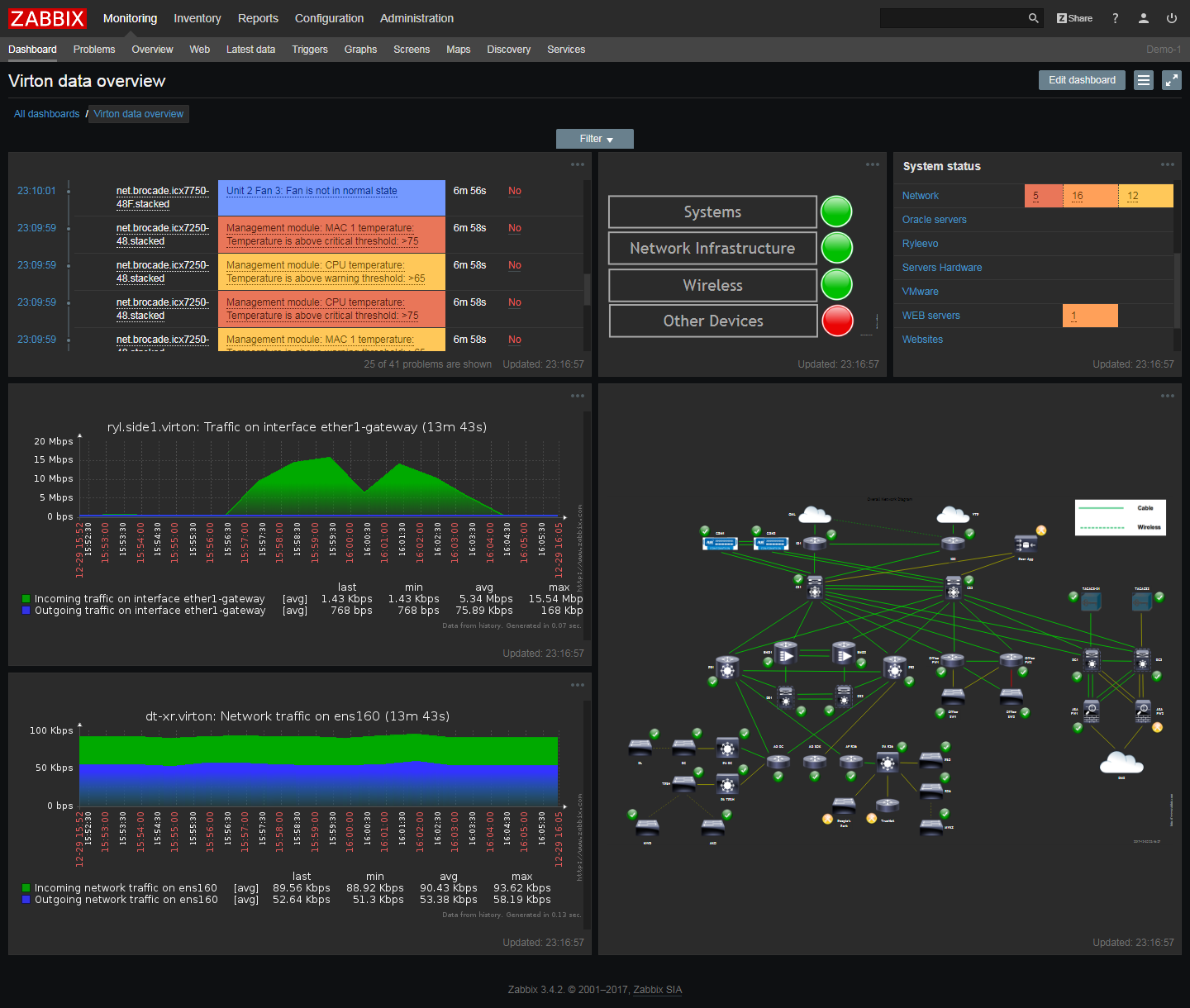
Obecně by se dalo tvrdit, že na trhu existuje již velké množství řešení, která jsou schopna spolehlivě, ale hlavně automatizovaně vyřešit problém inventarizace a následného zabezpečení zařízení na síti. Většina firem je ale primárně soustředěna na velké firmy a korporace kde z důvodu obrovského počtu zařízení není možnost udržovat přehled a transparentnost infrastruktury bez použití moderního softwaru. Z důvodu nutnosti minimalizace nákladů se u malých či středních podniků najde spoustu společností, které si jednoduše nemohou dovolit některý s výše uvedených komplexních řešení. V praxi to poté často vypadá tak, že se veškeré úkony spojené se správou zařízení nechávají na zpravidla malém týmu síťových správců, kteří bývají plně utilizovani. Absence lidských zdrojů se poté projevuje na nedostatečném či neexistujícím řešení správy prvků, čímž mohou vznikat provozní a bezpečnostní rizika.

## Dostupné opensource nastroje

Opensource nástrojů na inventarizaci a správu zařízení existuje velká řada, avšak podle mého názoru nemůžeme v tomto odvětví srovnávat z hlediska komplexnosti a funkcí, komerční a opensource řešení. V rámci průzkumu trhu jsem našel mnoho opensource programů a aplikací, které jsou zaměřeny na inventarizaci bezpečnost ale také monitoring, který je pro bezpečnost a transparentnost infrastruktury nepostradatelný. Příkladem je robustní monitorovací opensource software Zabbix nebo také konkurenční LibreNMS a další. Můžeme také nalézt velké množství programů zaměřené čistě na správu majetku firmy jako takové, kde tyto nástroje nabízí integrace s čárovými a QR kódy, nicméně chybí zde jakákoli přímá komunikace s přístroji a jejich kontrola v reálném čase či doporučení zabezpečení podle postupů best-practise nebo výše zmíněný „Virtual patching“. Nejblíže k implemtaci všech tětcho funkcí je program Nautobot který je představen níže.

Komplexní monitorovací software Zabbix je jedním z nejlepších ve svém odvětví. Má obrovskou komunitu, která základní systém stále vylepšuje. Jedná se zde převážně o takzvané šablony, které zabbix využívá pro monitorování různých zařízení. Existuje také velké množství externích skriptů pro další rozšíření funkcionalit. Podstatou většiny opensource programů je že jejich instalace a používaní není zpoplatněno, ale uživatel si sám musí systém nainstalovat a nastavit. Proto je kvalitní dokumentace nedílnou součástí většiny takových to nástrojů.

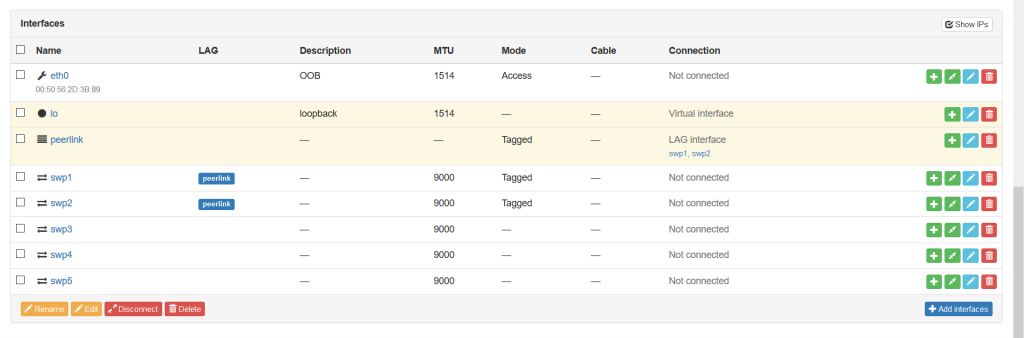
**Obrázek 2 Zabbix dashboard:**



Francouzká společnost OCS inventory a její opensource program, starající se o inventarizaci firemní infrastruktury je další z mnoha nástrojů na trhu. Díky automatickému skenování je tato aplikace schopna vytvořit kompletní seznam zařízení na síti, včetně jejich verzí softwaru a ve většině případů i její licenci. Komunikace mezi zařízeními je především řešena nainstalovanými agenty, díky kterým dokáže program zjistit i typ Hardwaru jako je například procesor, paměti ram a další. Pro zařízení, které neumožnují instalaci softwaru se používá protokol SNMP. Výrobce tvrdí možnost využití i v prostředí, kde je více než 150000 zařízení. Další funkcí je pak automatická distribuce softwarových balíčků a scriptů a jejich následné spuštění. Při získávání informací o tomto řešení se několikrát objevily nepříliš dobré recenze, ať už se jednalo o velké množství chyb nebo dokonce nefunkčnost některých modulů.

NetBox je komplexní systém pro síťovou transparentnost a SPOT (Single point of truth). Poskytuje i takzvaný „IPAM“ (IP address management) a to včetně virtuálních lokální sítí (VLAN) nebo virtuálně oddělených routovacích tabulek (VRF). Vzhledem k použití programu v datacentrech je zde i integrovaná vizualizace rackových skříní a jejich zařazení do skupin. Velkou výhodou a skvělou funkcí je databáze a její následná vizualizace fyzických ale i virtuálních propojení zařízení. NetBox zatím nepodporuje monitoring ani automatické konfigurace zařízení. Myšlenkou a podstatnou celého programu je převážně dokumentace a vizualizace, která je na vysoké úrovni vzhledem k tomu, že se jedná o menší opensource projekt. Netbox byl již v minulosti upraven a vylepšen firmou Networktocode, která přidala mnoho chybějících funkcí jako je například automatická konfigurace a dokumentace, softwarové aktualizace, validace konfigurací a mnoho dalších. Nástroj nese název „Nautobot“ a integruje spolu mnoho modulů a knihoven, příkladem může být knihovna Napalm, která bude v mém programu také použita.

**Obrázek 3 Dashboard zapojení:**



Na trhu

# Analýza

* V analyticke casti jednak analyzu jiz existujicich reseni...abys oduvodnil svuj featureset....a pak i navrhnout jak to budes psat, jaky jazyk, jake knihovny.

Z dosavadního poznání, zejména z průzkumu komerčního trhu, lze usuzovat že se v budoucnu budou nároky na bezpečnost infrastruktury jen zvyšovat. Bezpečnost nelze řešit zodpovědně, pokud nemáme stoprocentní přehled o všech zařízení v dané společnosti. V dnešní době stačí jedno malé zařízení jako je například chytrá žárovka nebo reproduktor ke kompromitaci celé firmy. O to více by se měl klást důraz na dokumentaci a inventarizaci všech zařízení na síti abychom minimalizovali rizika napadení. Svůj program budu psát převážně za účelem úspory času síťových administrátorů.

Požadované funkce můžeme shrnout rozdělením na dvě části. V První části se jedná primárně o sběr co nejvíce relevantních informací, které budou následně potřeba v druhé části programu. Ta bude mít za úkol všechna získaná data zanalyzovat a následně reprezentovat několika dokumenty včetně tabulek a výstupů z několika nástrojů jako je například aplikace „NMAP“, která se primárně využívá na prohledávání sítí a odhalovaní otevřených síťových portů zařízení. Výstupem bude také seznam prvků s doporučeními jako je například aktualizace zastaralého softwaru nebo změna výchozích přihlašovacích údajů.

Vzhledem k tomu, že pro některé funkčnosti bude nezbytně nutné přímé navázaní spojení se zařízeními, rozhodl jsem se program napsat v programovacím jazyce Python verze tři. Python, jako jeden z nejpoužívanějších jazyků na síťovou automatizaci, konfiguraci a práci s daty má s využitím několika knihoven již připravené funkce pro zabezpečené spojení s prvky využitím protokolu SSH. Příkladem a odůvodněním může být americká firma Arista, která vyvíjí špičková síťová zařízení s důrazem na automatizaci právě za pomoci programovacího jazyku python. Další výhodou je rozšiřitelnost tohoto jazyka, které se projevuje ve velké komunitě aktivních programátorů na forech zabývající se problematikou jazyka python a jeho problémů. Dalším programovacím jazykem ke zvážení je bash, který typicky najdeme na UNIX operačních systémech, které jsou velmi rozšířené u různých techniků a administrátorů.

Vzhledem k požadavkům na jednoduché použití bude mít program konfigurační soubor ve formě „INI“ což je v zásadě formát pro konfigurační soubory pocházející z Windows prostředí. V rámci pythonu je podporován a má již předpřipravené knihovny pro čtení a parsování. Program podporuje i dodatečný konfigurační soubor JSON, který obsahuje nastavení pro připojení k zařízením. Spouštění programu bude skrz příkazovou řádku, kde bude možnost pomocí argumentů pustit script s dalšími funkcemi. Dokumentace bude psána v jazyce Markdown, který umožňuje jednoduché formátovaní a psaní takzvaného „rich“ textu přehledným způsobem. U psaní dokumentace menších programů je jazyk Markdown velice rozšířený. Důvodem je také jednoduché nahrání celého scriptu do nástroje „GitHub“, kde je markdown dokument automaticky vykreslen.

Program bude využívat hned několik externích knihoven. Pro připojení a následný sběr dat bude script využívat knihovnu Napalm, která je přímo určená k použití zabezpečeného spojení se zařízením a následný sběr dat. Pro dynamické určení zařízení se bude používat knihovna Netmiko, která je již součástí již zmíněné knihovny Napalm. Dalším příkladem je knihovna openpyxl, která obsahuje metody a objekty, skrz které lze z Pythonu přímo ukládat data do tabulek z Excelu. V programu bude použita i nativní knihovna „concurrent.futures“, která nám umožnuje spouštět metody asynchronně.

# Návrh řešení

## Workflow

Program začne přečtením konfiguračního souboru po kterém nastaví proměnné pro svůj další běh. V další části script začne získávat data prostřednictvím přímého připojení

Srovnat paralelizaci s C# plus/minus

Navrh reseni – popsat diagram

+

Function diagram

Vic citaci

Popsani CLI a srovnani HUA/CISCO + zminit arista API (LEGACY vs modern)

Parsery - priklady

Popsat problem - stackoverflow

MAin funkce

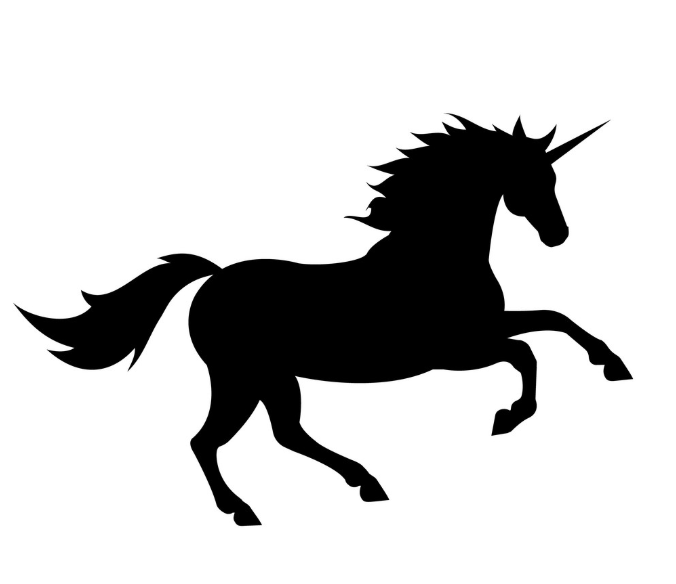
*Obrázek se v textu značí následujícím způsobem: samotný obrázek se označí: „****Obrázek 1: Název obrázku****“ (11 nebo 12 pt, černě, tučně). Obrázky se označují názvem a číslováním nad obrázkem a zdrojovým dokumentem pod obrázkem, příp. informace o vlastním zpracování (11 nebo 12 pt, černě). K popisování doporučujeme využít nástroje textového editoru, který usnadní generování seznamu obrázků na konci práce.*

**Obrázek 1: Logo**



Zdroj: č

**Obrázek 2: Obrázek jednorožce**



Zdroj: Vlastní zpracování

*Tabulky se označují názvem a číslováním nad tabulkou a zdrojovým textem pod tabulkou. Tabulky, obrázky a grafy se číslují zvlášť. Každá tabulka, obrázek nebo graf MUSÍ být v textu okomentován. Je nepřípustné, aby jednotlivé kapitoly (podkapitoly) tvořilo pouze grafické znázornění v podobě tabulek, grafů, obrázků, schémat atp. bez jejich okomentování.*

**Tabulka 1: Statistika vět zachovaných a vyřazených filtr. kritériem *FK1***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sada** | **Celkem** | **Zachováno** | **Vyřazeno** | **Zachováno** |
| **dtest** | 5228 | 2384 | 2844 | 45,6 % |
| **etest** | 5476 | 2419 | 3057 | 44,2 % |
| **train-1** | 4709 | 2204 | 2505 | 46,8 % |

Zdroj: Vlastní zpracování

**Matematické rovnice, vzorce**

*Pokud jsou v práci rovnice, nezapomeňte je správně číslovat. Pro jejich zápis používejte MS Editor rovnic, případně jinou obdobnou aplikaci. Rovnice by měla vypadat například takto (nezapomeňte proměnné popisovat):*

|  |  |
| --- | --- |
|  | (1) |

*kde S je obsah kruhu o poloměru r .*

# Závěr

Tato kapitola se nečísluje. Rozsah je zpravidla 5-10 normostran.

# Seznam použitých zdrojů

V seznamu zdrojů musí být uvedeny všechny v závěrečné práci citované zdroje. Zároveň nesmí seznam obsahovat zdroje, které nejsou v závěrečné práci použity.

Používáme citační normu ČNS ISO 690. Doporučujeme pro tvorbu citací některý z citačních nástrojů, které jsou v základní verzi zpravidla zdarma dostupné.

• HORÁK, Jaroslav a Milan KERŠLÁGER. Počítačové sítě pro začínající správce. 5., aktualiz. vyd. Brno: Computer Press, 2011. ISBN 978-80-251-3176-3.

• KUROSE, James F. a Keith W. ROSS. Počítačové sítě. Brno: Computer Press, 2014. ISBN 9788025138250.

• SUMMERFIELD, Mark. Python 3: výukový kurz. 2. vydání. Přeložil Lukáš KREJČÍ. Brno: Computer Press, 2021. ISBN 9788025150306.

• 3.10.1 Documentation. [online]. Copyright © [cit. 30.12.2021]. Dostupné z: https://docs.python.org/3/

• Welcome to NAPALM’s documentation! — NAPALM 3 documentation. [online]. Copyright © Copyright 2021, David Barroso [cit. 30.12.2021]. Dostupné z: https://napalm.readthedocs.io/en/latest/

• What is Network Penetration Testing? - Penetration Testing | aNetworks. Cyber Security, Managed IT, Cloud, & Consulting Services | aNetworks [online]. Copyright © 2021 [cit. 30.12.2021]. Dostupné z: https://www.anetworks.com/what-is-network-penetration-testing/

• Projekty ve firmě Altepro Solutions a.s.

o Rozšíření a profylaxe sítě Nemocnice Pardubického kraje

o Monitoring sítě – Česká televize

• GitHub Documentation. [online]. Copyright © [cit. 30.12.2021]. Dostupné z: https://docs.github.com/en

• Network Management Guide: How To, Best Practices, & Tools - DNSstuff. Software Reviews, Opinions, and Tips - DNSstuff [online]. Copyright © 2021 SolarWinds Worldwide, LLC. All rights reserved. [cit. 30.12.2021]. Dostupné z: <https://www.dnsstuff.com/network-management>

Obrazek ZABBIX DASHBOARD:

<https://www.zabbix.com/database_monitoring>

Obrazek C2 = <https://karneliuk.com/2019/04/documenting-your-network-infrastructure-in-netbox-integrating-with-ansible-over-rest-api-and-automating-provisioning-of-cumulus-linux-arista-eos-nokia-sr-os-and-cisco-ios-xr/>

Obrazek SOlarwinds: <https://www.solarwinds.com/network-configuration-manager/use-cases/network-inventory>

# Seznam obrázků (existují-li)

Obrázek 1: Logo 11

Obrázek 2: Obrázek jednorožce 12

**Seznam tabulek (existují-li)**

[Tabulka 1: Statistika vět zachovaných a vyřazených filtr. kritériem *FK1* 12](#_bookmark9)

# Seznam grafů (existují-li)

# Seznam příloh (existují-li)

*Každá příloha musí být alespoň jednou odkázána do vlastního textu práce. Přílohy se číslují. Každá příloha začíná na nové stránce.*

# Příloha A – Název přílohy

# Příloha B – Název přílohy