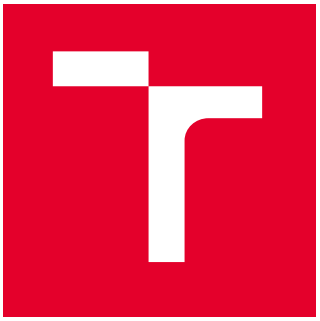


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ

DEPARTMENT OF TELECOMMUNICATIONS

OPTIMALIZACE SÍŤOVÝCH DOHLEDOVÝCH SYSTÉMŮ A JEJICH INTEGRACE S NÁSTROJI PRO PODPORU UŽIVATELŮ

OPTIMIZATION OF NETWORK MONITORING SYSTEMS AND THEIR INTEGRATION WITH USER SUPPORT TOOLS

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

AUTOR PRÁCE — **Jakub Krýcha**

AUTHOR

VEDOUCÍ PRÁCE — **Ing. Anna Kubánková, Ph.D.**

SUPERVISOR

BRNO 2023

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní program **Telekomunikační a informační systémy**

Ústav telekomunikací

Student: Jakub Krýcha ***ID:*** 221279

Ročník: 3 ***Akademický rok:*** 2022/23

NÁZEV TÉMATU:

Optimalizace síťových dohledových systémů a jejich integrace s nástroji pro podporu uživatelů

POKYNY PRO VYPRACOVÁNÍ:

Seznamte se s moderními dohledovými systémy, help desk nástroji a jejich vlastnostmi. Rozeberte důvody a možností použití těchto systémů v síti. Porovnejte vybrané dohledové a help desk nástroje jak teoreticky, tak prakticky na reálných zařízeních. Zvolte nejvhodnější řešení pro konkrétní firemní prostředí a následně toto řešení nasaďte do reálné sítě. Navrhněte scénáře integrace síťových dohledových systémů s help desk nástroji pro usnadnění řešení problémů vyskytujících se v síti. Automatizujte řešení problémů v síti pomocí realizace navržených scénářů. Analyzujte chováni nasazeného řešení, optimalizujte a navrhněte další rozvoj.

DOPORUČENÁ LITERATURA:

Podle pokynů vedoucího práce.

Termín zadání: ***Termín odevzdání:*** 17.8.2023

Vedoucí práce: Ing. Anna Kubánková, Ph.D.

prof. Ing. Jiří Mišurec, CSc.
předseda rady studijního programu

ABSTRAKT

Tato bakalářská práce je zaměřena na realizaci monitorovacích systémů, automatizované řešení a prevenci možného vzniku problémů v počítačových sítích. Cílem práce bylo implementovat monitorovací systém do sítě, zautomatizovat řešení vzniklých problémů a vytvořit skripty, jež při detekci vzniklého nebo vznikajícího problému zajistí odpovídající nápravu.

KLÍČOVÁ SLOVA

Zabbix, Nagios, SNMP, Skript, Automatizace, Implementace

ABSTRACT

This bachelor's thesis is focused on the implementation of monitoring systems, automated solutions and prevention of potential issues in computer networks. The objective was to implement a monitoring system into the network, automate the solution of encountered problems, and create scripts that would ensure appropriate remedies upon the detection of an existing or emerging problem.

KEYWORDS

Zabbix, Nagios, SNMP, Script, Automatization, Implementation

KRÝCHA, Jakub. *Optimalizace síťových dohledových systémů a jejich integrace s nástroji pro podporu uživatelů*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2023, 59 s. Bakalářská práce. Vedoucí práce: Ing. Anna Kubánková, Ph.D.

Prohlášení autora o původnosti díla

Jméno a příjmení autora:	Jakub Krýcha
VUT ID autora:	221279
Typ práce:	Bakalářská práce
Akademický rok:	2022/23
Téma závěrečné práce:	Optimalizace síťových dohledových systémů a jejich integrace s nástroji pro podporu uživatelů

Prohlašuji, že svou závěrečnou práci jsem vypracoval samostatně pod vedením vedoucí/ho závěrečné práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené závěrečné práce dále prohlašuji, že v souvislosti s vytvořením této závěrečné práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Brno ....

podpis autora*

*Autor podepisuje pouze v tištěné verzi.

PODĚKOVÁNÍ

Rád bych poděkoval vedoucí bakalářské práce Ing. Anně Kubánkové, Ph.D. za veškerou trpělivost, konzultace, odborné a podnětné návrhy k práci, také bych rád poděkoval firmě Simac Technik za možnost realizace bakalářské práce v jejich firmě.

Obsah

Seznam obrázků

Seznam výpisů

Úvod

Dohledové nástroje jsou v dnešní době velice využívaným prvkem, jelikož se internetová síť stále rozrůstá a vyvýjí. Pomáhají technikům s kontrolou dostupnosti zařízení a služeb pomocí SNMP protokolu. Některé společnosti využívají i jiné protokoly, jako CDP nebo LLDP od Cisca. Všechny tyto protokoly získávají informace od zařízení nebo služeb v síti.

Samozřejmě je v dnešní době mnoho dohledových nástrojů, které jsou opensource nebo placené. Proto je nutné si jednotlivé nástroje porovnat a rozhodnout se, který vybrat a implementovat do sítě.

V první části se pojednává o dohledových nástrojích, proč je vlastně využívat a jaké jsou základní podmínky pro realizaci. Následně jsou rozebrány monžosti kontroly síťových prvků pomocí protokolů, které jsou v této části popsány. Dále je podrobné porovnání dohledových nástrojů. V realizaci je sepsán důvod přechodu na jiný dohledový nástroj a implementace funkcí Zabbixu. V poslední části je sepsána automatizace řešení a prevence předcházení problémům.

1 Dohledové nástroje

Dohledové nástroje jsou aplikace, které kontrolují veškerou dostupnost a výkon sítě. Mají za úkol sledovat počítačovou síť v reálném čase, kde sledují dostupnost veškerých služeb a hardwarových prvků. Díky pravidelné kontrole je možné včas odhalit problém a kontaktovat technika, aby jej vyřešil. Technika je možné automaticky kontaktovat pomocí emailu, SMS (Short message service), nebo vytvořit požadavek na helpdesku. Toto jsou nejčastější možnosti, ale samozřejmě jsou zde i jiné možnosti implementace komunikace s technikem. To následně záleží na správci daného systému co chce implementovat.[1]

1.1 Proč využívat dohledové nástroje

Dohledové nástroje se nejčastěji využívají pro detekci a prevenci chyb v síti. Díky tomu lze lépe využívat hardware, jelikož lze zjistit špatnou funkčnost nebo nadměrné vytížení. Šetří se čas techniků, kteří síť spravují, protože monitorovací systém odhalí chybu mnohem dříve. Dále je možné monitorovat i vzdálenější sítě a mít tak přehled o stavu sítě například u zákazníka nebo na vzdálené pobočce.[2]

1.2 Obecná realizace

Při realizaci dohledových prvků je nutná základní analýza, jak firma funguje a jak řeší dané problémy. Následně se vymyslí návrh, jak implementovat dohledový systém, následuje realizace a testování před nasazením do provozu.[1]

Analýza

Základní analýza problémů sítě, jak technici pracují při problému a jaké jsou softwarové a hardwarové možnosti. Jelikož je snaha o co nejefektivnější zpracování požadavků v reálném čase, je nutné, aby technici byli kontaktováni, protože je neefektivní, když musí zjišťovat problémy v dohledovém nástroji. Nutné je i zkontrolovat hardware a software a zjistit, jestli je možné zde nový dohledový systém realizovat, nebo se musí provést jejich upgrade.[1]

Návrh

Návrh je vytvářen na základě zjištěných problémů v síti, které jsou samozřejmě konzultovány se správcem dané sítě. Před implementací do reálného provozu je vhodné daný návrh otestovat např. v testovacích programech, dle možností a požadavků správce sítě.[1]

Implementace a testování

Vytvořený návrh dohledového systému implementujeme do síťového prostředí a zprovozníme komunikaci mezi dohledovým nástrojem a techniky. Následně pak provedeme testy funkčnosti nasazeného systému simulací reálných výpadků dle připravených scénářů.[1]

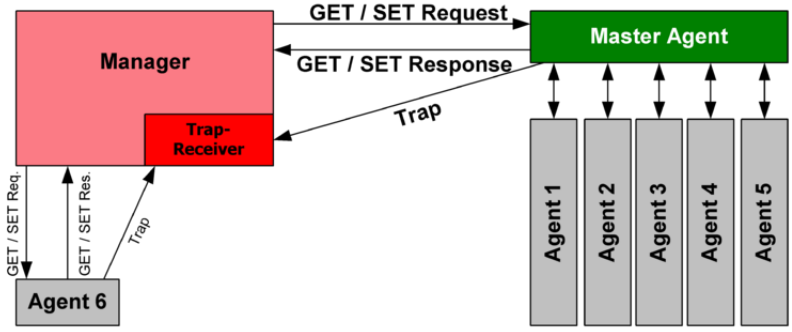
1.3 Možnosti kontroly sítě a služeb

Pro správný a efektivní chod počítačové sítě, je velice důležité sledovat stav sítě. Technik ovšem není schopen v reálném čase dozorovat celou síť, proto je užití dohledového nástroje žádoucí a efektivnější. Tyto nástroje umožňují, pomocí různých protokolů, kontrolovat počítačovou síť, služby jež poskytuje a veškerá zařízení jež tuto síť využívají, či zajišťují její funkčnost.[3]

Existuje mnoho protokolů, díky kterým lze kontrolovat počítačovou síť v závislosti na výrobci dohledových nástrojů. Nejznámější jsou protokoly ICMP (nternet Control Message Protocol), SNMP (Simple Network Management Protocol), CDP (Cisco Discovery Protokol) a LLDP (Link Layer Discovery Protocol).[3]

1.3.1 SNMP protokol

SNMP protokol funguje na principu klient-server a využívá se ke správě a monitorování sítě. Shromažďuje a organizuje data od veškerých zařízení v síti, jako jsou routery, switche, servery, počítače a dalších, které podporují SNMP. Základní fungování SNMP je zobrazeno na obrázku 1.1.[4]



Obr. 1.1: Princip fungování SNMP [4]

Manager

Manager je vždy jeden nebo více počítačů, jež má na starost veškeré monitorování sítě a správu kontrolovaných zařízení.[4]

Agent

Agent běží na všech kontrolovaných zařízeních a umožňuje komunikaci managera s datovým zařízením. Díky tomu je pak možné přijímat a spravovat data.[4]

NMS (Network management station)

NMS je součástí managera. Spouští software, který monitoruje a řídí veškerá zařízení v dané síti.[4]

MIB (Management information base)

MIB obsahuje datové prvky, které jsou hierarchicky uspořádány do stromové struktury. Tyto datové prvky jsou pak označeny jako OID (Object Identifier). Každý prvek má unikátní OID a díky tomu ho lze sledovat nebo nastavovat.[4]

Komunikace mezi Managerem a Agentem

Komunikace probíhá pomocí UDP (User Datagram Protocol) na portech 161 a 162. Pro získání informací od agenta posílá manager zprávu getRequest a agent odpovídá getReponse s aktuálními hodnotami. V případě, že manager chce na agentovi nastavit hodnotu, tak posílá setRequest a po změnění hodnoty agent posílá setReponse se změněnými hodnotami.[4]

V případě události výpadku spojení, přetížení CPU (Central processing unit) a další, odesílá agent asynchronní zprávu Trap. Tato zpráva obsahuje informace o problému a odesílá se hned, jak problém vznikne.[4]

1.3.2 ICMP protokol

ICMP protokol využívají veškerá síťová zařízení. Liší se od TCP (Transmission Control Protocol) a UDP, jelikož se nepoužívá pro přenos dat, ale pouze pro kontrolní účely v síti. Při kontrole dostupnosti se zasílají zprávy, které informují o stavu dané sítě. Díky různým ICMP příkazům lze provádět různé operace. Nejzákladnější ping testuje konetivitu v síti, dále traceroute (interpretace se může lišit v různých operačních systémech), díky kterému je možné provádět analýzu trasování v síti. ICMP funguje v IPv4 (Internet Protocol version 4) i IPv6 (Internet Protocol version 6) sítích.[5]

Nejzákladnější typy zpráv

- Echo Request a Reply: nejvíce používá ping, který slouží k ověření konektivity v síti [5]
- Time exceeded: posílá se jakmile se TTL (Time To Live) dostane na nulu, tato zpráva je většinou generována bránou[5]
- Destination Unreachable: posílá se, jakmile hostitel není dostupný [5]
- Redirect: inormuje hostitele o přesměrování na alternativní cestu a o aktualizování směrovacích informací[5]

1.3.3 CDP protokol

CDP se využívá k monitorování Cisco zařízení, které jsou navzájem propojeny v síti. Poskytuje informace o veškerých Cisco zařízeních v síti a pravidelně posílá packety s multicastovou adresou, díky které zjišťuje informace od ostatních Cisco zařízení. Veškeré informace, jež jsou zasílány, si zařízení ukládají a je možné si je zpětně zobrazit pomocí příkazu show cdp neighbors.[6]

CDP posílá každých 60 sekund zprávy. V případě, že soused neodpoví do 180 sekund, je vymazán z CDP tabulky. Časové intervaly je možné je nastavit podle potřeb. Ve výchozím nastavení je CDP povoleno na veškerých rozhaních a je možné ho globálně vypnout.[6]

1.3.4 LLDP protokol

LLDP je velice podobný protokolu CDP. LLDP byl navržen tak, aby komunikoval se všemi síťovími zařízeními. Je možné zařízení nakonfigurovat tak, aby LLDP packety byly jen přijímany, odesílány nebo přijímány a odesílány. [7]

LLDP posílá každých 30 sekund zprávy na rozhraní, kde je povoleno. V případě, že soused neodpoví do 120 sekund, je vymazán z LLDP tabulky. Tyto hodnoty jsou nastaveny jako výchozý, ale je možné je nastavit podle potřeb. Jakmile administrátor chce používat LLDP je nutné ho aktivovat pomocí lldp run, jelikož je ve výchozím nastavení deaktivováno.[7]

1.4 Nagios

Nagios je nejstarší monitorovací nástroj, který vznikl již v roce 1996. Je to open-source nástroj pro monitorování systémů a sítě, který sleduje veškeré nakonfigurované hosty a služby. Při jakémkoli problému Nagios upozorní uživatele. Je možné ho nainstalovat na jakýkoliv Unixový systém.[8]

V Nagiosu je možné realizovat mnoho funkcí. Kromě sledování hostů a služeb je možné nakonfigurovat sítovou hierarchii, kde se u hostů nakonfiguruje „rodič“ a díky tomu vznikne stromová struktura. V případě nedostupnosti se následně vytvoří pouze jedna událost. Také je možnost nakonfigurování kontaktů, kterým jsou zasílány nastavené notifikace přes SMS nebo E-mail. Webové rozhraní slouží pouze ke sledování události, stavu hostů a služeb. [8]

1.4.1 Instalace

Instalace Nagiosu je velice jednoduchá a zabere přibližně 20 minut. Instalační postup lze najít v dokumentaci, kde jsou popsány veškeré kroky k instalaci na daný systém. Může být naistalován pouze na 64-bitové Unixové systémy s minimálními specifikacemi 1 GHz frekvence procesoru, 1 GB RAM a 8 GB úložiště. Doporučené požadavky jsou však 2+ GHz frekvence procesoru, 4 GB RAM a 40 GB úložiště. [8]

1.4.2 Monitorování

Zařízení

Pomocí Nagiosu lze sledovat síťové prvky jako router nebo switch. V závislosti na zařízení lze pak nastavit, co všechno chceme sledovat. Pomocí ICMP protokolu se kontroluje dostupnost zařízení a ztráta packetů v síti, a nebo pokud dané zařízení podporuje možnost integrace SNMP, lze pak i monitorovat stav portů, šířku pásma a další.[8]

Systémy

Při monitorování systémů je možné monitorovat jednotlivé atributy počítačů - využití paměti, zatížení CPU, využití disku a další.[8]

V případě kontroly atributů u MS Windowsu je nutné naistalovat do Windowsu NCPA agenta a plugin do Nagiosu. Daný agent následně funguje jako proxy pro komunikaci mezi systémem a Nagiosem. Bez tohoto nastavení není možnost, jak by Nagios mohl kontrolovat jednotlivé atributy.[8]

U Linuxu je možností kontroly pomocí sdílení SSH klíčů nebo NRPE doplňku. Při sdílení klíče SSH je možné vzdáleně spouštět pluginy, ale bohužel to má nevýhodu

vysokého vytížení monitorovacího serveru při kontrolování mnoha atributů, jelikož je potřeba udržet dané SSH spojení. Pomocí NRPE doplňku je také možné vzdáleně spouštět pluginy, ale hodí se více pro kontrolu atributů, jelikož není tolik náročný na výkon.[8]

Služby

Je zde možnost kontroly služeb, jako je HTTP (Hypertext Transfer Protocol), IMAP (Internet Message Access Protocol), POP3 (Post Office Protocol) a samozřejmě mnoho dalších. Kontrola těchto služeb není nijak složitá a nevyžaduje žádné specifické požadavky. Ovšem při kontrolování specifikací hosta například vytížení procesoru, paměti, disku a dalších, je nutné instalovat agenta, který tyto informace bude poskytovat Nagiosu. Tento monitorovací agent pak následně musí být instalován na veškerých hostech, u kterých je potřeba tyto informace kontrolovat.[8]

1.4.3 Konfigurace

Jelikož Nagios nelze konfigurovat přes webové rozhraní, je nutné veškeré konfigurační úkony dělat přímo na monitorovacím serveru v příkazovém řádku. Konfiguraci provádí uživatel vytvářením nebo upravováním konfiguračních souborů. Dílčí konfigurační soubory jsou zahrnuty v hlavním konfiguračním souboru. Tyto soubory jsou zdrojové a objektově definované. Zdrojové soubory se využívají pro nakonfigurování maker, kde se definují uživatelská jména a hesla nebo cesty k souborům. V objektově definovaných souborech se definují veškerý hosti, skupiny hostů, kontakty a další. Veškeré tyto konfigurace mohou být v jednom konfiguračním souboru nebo ve více souborech najednou.[8]

1.4.4 Kontroly

Veškeré kontroly jsou prováděny současně a v definovaných časových intervalech. Kontroly lze rozdělit podle toho, co kontrolujeme - host nebo služba, a podle toho, jak je to kontrolováno - pasivně nebo aktivně. [8]

Kontrola hostů

U kontroly hostů se kontroluje jejich stav. V případě, že přejde ze stavu Up do stavu Down nebo Unreachable, je vytvořena událost. Samozřejmě podle stavu lze pak usoudit, o jaký problém se přibližně jedná. Stav hosta se může změnit při nastavení automatického restartu. Host pak následně může být opět dostupný a událost zmizet.[8]

Kontrola služeb

Při kontrole služeb lze problémy definovat do stavů Ok, Warning, Unknown a Critical. Kontroly, které jsou prováděny, jsou porovnávány s kontrolou, která byla provedena předtím. [8]

Aktivní kontrola

Aktivní kontroly provádí sám Nagios v pravidelných intervalech. Při kontrole spustí plugin, který zkontroluje podle nadefinovaných atributů daného hosta nebo službu. Podle informací, které zjistil pak následně provede další kroky.[8]

Pasivní kontrola

Pasivní kontrolu neprovádí Nagios, ale externí program. Není to moc využívaná kontrola, jelikož se Nagios nemůže pravidelně dotazovat na stav a spoléhá se jen na informace, které jsou mu poslány. Většinou se využívá pro zařízení za firewallem.[8]

1.4.5 Výhody a Nevýhody

Výhody

Nagios je vhodný pro menší sítě. Díky hierarchii zařízení se eliminují události, které by mohli vzniknout při výpadku nějakého ze zařízení. Jedna z předností je určitě jednoduchá instalace spolu s konfigurací, která je vysvětlena v dokumentaci.[13]

Nevýhody

Velká nevýhoda Nagiosu je, že nedokáže sám vyhledávat prvky sítě a je nutné je všechny ručně přidat. Webové rozhraní je pouze pro kontrolu stavu veškerých zařízení a služeb a není možné zde cokoliv upravovat a konfigurovat. Problémy nelze zobrazit v grafu na časové ose.[13]

1.5 Zabbix

Zabbix je open-source monitorovací nástroj, díky kterému lze monitorovat stav sítě, zařízení, virtuální stroje, servery, weby a další. Veškerá konfigurace a vizualizace problémů je ve webovém rozhraní. V případě výskytu problému je možné kontaktovat správce - SMS, E-mail, nebo Service deskový nástroj. Veškeré sledované údaje je možné zobrazit pomocí grafů anebo si celou topologii sítě poskládat pomocí map. [9]

1.5.1 Instalace

Instalace Zabbixu je jednoduchá a nezabere více než 30 minut. Instalace je možná několika způsoby, a to z distribučních balíčků, stažení archivu se Zabbixem anebo stažení virtuálního zařízení. Veškeré instalace jsou popsány v dokumentaci společně s požadavky na výkon, podle toho, kolik zařízení se bude monitorovat. Veškeré požadavky na výkon lze vidět v tabulce níže, kde metrika je jeden parametr (např. vytížení CPU, vytížení disku atd.), který je sledován. [9]

Velikost instalace	Sledované metriky	CPU jádra	Paměť (GiB)
Malý	1 000	2	8
Střední	10 000	4	16
Velký	100 000	8	64
Velmi velký	1 000 000	16	96

Tab. 1.1: Požadavky na instalaci Zabbixu [9]

Po nainstalování Zabbixu na server se konfigurace dokončí ve webovém prohlížeči, kde se nastaví veškeré zbylé informace, pro správné fungování Zabbixu.[9]

1.5.2 Monitorování

Monitorování webových stránek

Je možnost nastavení monitorování aspektů webových stránek HTTP a HTTPS (Hypertext Transfer Protocol Secure). Kontrola se skládá z nadefinovaných požadavků nebo kroků, které si administrátor nadefinuje. Při kontrole se pak monitoruje rychlost stahování, doba odezvy a kód odpovědi. Dále je možné volitelně kontrolovat poslední chybovou hlášku, nebo zobrazení kroku na které kontrola selhala.[9]

Monitorování virtuálních strojů

Zabbix má možnost monitorovat VMware a jeho aspekty. Data se shromažďují pomocí kolektorů. Sledované atributy mohou být zpožděné kvůli načítání dat z VMwaru, hlavně při sledování více virtuálních strojů zároveň.[9]

1.5.3 Konfigurace

Veškerou konfiguraci, která se v Zabbixu provádí, lze nalézt na postranní liště ve webovém rozhraní.[9]

Host

Základní konfigurace hosta zahrnuje pojmenování, zvolení typu rozhraní (Agent, SNMP, JMX, IPMI) s IP adresou a přiřazení do skupiny hostů. Hosta lze kontrolovat přes více rozhraní najednou. Může patřit do více skupin a je možné volitelně dále nastavit veškeré informace o daném zařízení jako MAC (Media Access Control) adresu, operační systém a popřípadě certifikát. [9]

Samotný host bohužel není kontrolován bez přiřazení šablony, které jsou předpřipraveny Zabbixem, nebo přidání atributů společně s časovači. Šablony je možné libovolně upravovat tak, aby se kontrolovalo, co je potřeba. Kontrolované atributy je možné nakonfigurovat ručně, společně s časovým intervalem, po jaké době se mají kontrolovat. Časovače shromažďují data od hostů a porovnávají je se svými nastavenými hodnotami. V případě, že získaná data nejsou v souladu s hodnotami, daný časovač změní svůj stav na "Problem".[9]

Grafy

Pokud administrátor chce, je možné získaná data ukázat v trendu, jak se vyvíjela za určitý časový úsek. Je tak možné přibližně odhalit, kdy problém začal, nebo lze předpokládat, kdy by se mohl problém vyskytnout. Díky možnosti zobrazení určitého časového úseku lze vidět, jak se problémy opakují. Je zde možnost i skládání vícero trendů do jednoho grafu a lze tak porovnávat hodnoty z jiných hostů.[9]

Mapy

Díky možnosti tvoření map je možné vytvořit mapu podle topologie sítě, nebo si vytvořit mapu určitého spojení. V případě problému je možné vidět kde přesně se problém nachází. [9]

Uživatelé

U veškerých uživatelů lze nastavit práva, která má daný uživatel mít a možnost kontaktování přes email, telefon, anebo propojit GitHub a mnoho dalších. Lze také nastavit, jaké upozornění se mají jednotlivým uživatelům posílat (Warning, Information, Disaster atd.). Je možné také vytvořit skupinu, ve které nastavíme určitá práva. V případě přidání uživatele do skupiny, obdrží uživatel práva nastavená v dané skupině.[9]

Automatické zjišťování

Automatické zjišťování sítě je velice efektivní a flexibilní. Díky tomu lze nastavit určitý rozsah sítě, ve kterém se mají hosti hledat, nastavení pravidla, zda se jedná například o Windows a následné přiřazení do správné skupiny, přiřazení správné šablony atd. Jakmile je zjišťování nastavené správně, je možné hosta přidat a celkově ho nastavit (přiřazení šablony, pojmenování, přidání do správné skupiny a další). Samozřejmě je možné díky kontrole aktivity i daného hosta smazat.[9]

Proxy

Zabbix umožňuje možnost kontrolovat vzdálená místa. Díky nastavení proxy serveru se data shromažďují na jednom místě. Umožnuje to jednoduše kontrolovat více topologií a všechna data zobrazovat na jednom místě. Bohužel je tato komunikace nespolehlivá. [9]

API

V případě přeposílání problémů na Service deskové nástroje jako GLPi nebo Zendesk, lze použít API kde se nastaví komunikační tokeny a nezbytné informace pro komunikaci mezi Zabbixem a se softwarem třetích stran. [9]

Šifrování

Je zde možné využít i šifrování pomocí certifikátů. Toto je možné nakonfigurovat pro Zabbix server, proxy a agenta. Komunikace je standartně nešifrovaná, proto je nutné ji dokonfigurovat. Je možné využít certifikát, nebo komunikaci šifrovat pomocí sdíleného klíče.[9]

V případě používání automatického zjišťování v síti se host přidá bez šifrování. To se následně musí ručně dokonfigurovat, aby komunikace probíhala šifrovaně.[9]

Potvrzování problému

V případě vyskytnutí problému lze přidat komentáře, jak se problém projevoval anebo jak se problém vyřešil. Problémy se zobrazují ve vyskakovacích oknech a jejich úplný seznam je možné najít v záložce Monitoring > Problems. Při přidávání komentáře je možné přiřadit vážnost dané zprávy, jestli je pouze informativní anebo vysoká.[9]

Problém je možné i potlačit a díky tomu ho dočasně skrýt ze seznamu problémů. Zobrazují se pak pouze závažné problémy, které je třeba vyřešit přednostně. Při tomto kroku je nutné nastavit dobu po kterou bude problém potlačen. Po uplynutí časového intervalu se problém opět objeví v seznamu.[9]

1.5.4 Výhody a Nevýhody

Výhody

Velká výhoda je možnost zobrazení hodnot v grafech a možnost si zde udělat mapu topologie sítě. Dále nakonfigurování pomocí API tokenů komunikaci se softwarem třetích stran. Díky výběru z mnoha přednastavených šablon není nutné zdlouhavě nastavovat základní sledované parametry. Pomocí skriptů je možné provádět na zařízeních/systémech změny anebo se na ně přes SSH, či telnet připojit a spouštět skripty přímo na zařízeních/systémech. Veliká výhoda je možnost propojit Zabbix s mnoha softwary třetích stran. [14]

Nevýhody

Prvotní nasazení a konfigurace není nejjednodušší. V případě změny parametrů v nastavení je nutné provádět mnoho ručních úprav. Při automatickém zjišťování sítě neumí sestavit topologii podle hierarchie. Grafickému rozhraní chybí přehlednost. [14]

1.6 SolarWinds

SolarWinds je jeden z nejdražších monitorovacích systémů na trhu, který se používá pro kontrolu a správu rozsáhlých sítí. Vyznačuje se dobrým grafickým rozhraním, kde se zobrazuje celková topologie sítě a její stav. Dokáže automaticky mapovat síť, automaticky zjišťovat nové zařízení v síti a udržovat si tak topologii co nejaktuálnější. Síť monitoruje pomocí SNMP, WMI (Windows Management Instrumentation), PowerShellu a dalších. Je zde mnoho předdefinovaných konfigurací a díky podpoře přes 1200 aplikací, je možné implementovat většinu aplikací. Samozřejmě je možné najít předdefinované konfigurace pro Linux a Windows servery od různých výrobců, kde následně monitoruje parametry hardwaru. Díky monitorování packetů pomocí NethPath, je jednoduší diagnostikovat problém, v případě snížení výkonu sítě. Jakmile vznikne problém, je možné technika kontaktovat přes SMS nebo Email. [10]

1.6.1 Instalace

Instalace SolarWinds je složitější než u předchozích monitorovacích nástrojů. Probíhá přes instalační program, kde se nakonfigurují všechny specifikace, které jsou potřeba. SolarWinds je možné nainstalovat na Unixové systémy, ale i na Windows server. Po nainstalování je nutné si aktivovat rozšíření zakoupená firmou. [11]

1.6.2 Monitorování

SolarWinds nabízí velkou škálu možností, jak monitorovat vaši síť. Software je určen především pro velké sítě. Díky možnosti zakoupení různých rozšíření si lze poskládat SolarWinds na míru. Rozšíření jsou rozdělena do jednotlivých kategorií, Síťový management, Systémový a aplikační management, Databázový management, IT security a IT service management. Veškeré produkty v těchto kategoriích je možné si zdarma na měsíc vyzkoušet. [12]

Síťový management

V této kategorii lze najít vše co je potřeba ke kontrole sítě. Lze si integrovat analyzování síťového provozu nebo logů, mapování sítě, monitorování vytížení sítě nebo správu IP adres. V případě kontroly uživatelů, je možnost integrovat nástroj pro sledování uživatelských zařízení. [12]

Systémový a aplikační management

Pro kontrolu systémů a aplikací je možné si vybrat z této kategorie, kde je možné najít monitorování serverů a aplikací, monitorování úložiště, virtualizační manager a další. [12]

Databázový management

Při práci s databázemi lze implementovat mapování databází, monitorování výkonu databáze, či analyzování databázového výkonu. [12]

IT security

Pro zabezpečení infrastruktury je možné využít security event manager, nebo správce přístupových práv. [12]

IT service management

Vlastní kategorie, která je zaměřena čistě na service desk. Je možné integrovat SolarWinds service desk, který si lze přikoupit a díky tomu neřešit problémy se service deskovými nástroji od jiných výrobců, v případě nekompatibility. [12]

Toto jsou ovšem jen jedny z důležitých rozšíření, ale je jich mnohem více. Díky tomu lze integrovat jen to co je opravdu potřeba a nezatěžovat systém zbytečnými doplňky. [12]

1.6.3 Výhody a Nevýhody

Výhody

Veliká výhoda je velký výběr různých doplňků. Další je automatické mapování a udržování topologie co nejaktuálnější. Možnost identifikování problému co nejpřesněji je v případě řešení jakéhokoliv problému velice vítané. [14]

Nevýhody

Jelikož je SolarWinds jeden z nejdražších softwarů na trhu, není nejvhodnější pro menší sítě. Díky možnosti přizpůsobení, jak potřebuje administrátor, je složitější konfigurace a správného fungovaní jednotlivých modulů. [14]

1.7 Další nástroje

ManageEngine je monitorovací nástroj, který dokáže monitorovat veškerá zařízení v síti, je možné ho nainstalovat na Windows i Linux. Instalace je velice jednoduchá a zabere pouze pár minut. Pomocí ManageEngine je možné v celé IT (Information technology) infrastruktuře kontrolovat virtuální zařízení, počítače, servery, ale i Wi-Fi. Dokáže automatické mapování a zjištění veškerých zařízení, která jsou do sítě připojena. V případě problémů je technik kontraktován přes SMS a E-mail. [14]

Od společnosti IBM nástroj IBM Tivoli, který se jednoduše instaluje a ovládá se přes webové rozhraní, které si lze nastavit podle svých představ. Samozřejmě je zde přístup k veškeré dokumentaci a bezplatnou podporu během pracovní doby. [14]

Je možné najít i dohledový nástroj od společnosti HP, který je sice mnohem složitější nastavit, ale vynahrazuje to velice kvalitním grafickým zpracováním, pro monitorování veškerých zařízení a služeb. V případě problému, přidává dodatečné doporučení technikům, jak problém vyřešit. [14]

Monitorovacích nástrojů je mnohem více a záleží do jakého prostředí bude nástroj aplikován a jaké má firma možnosti a požadavky. [14]

2 Realizace dohledového systému

2.1 Přechod z Nagiosu na Zabbix

Hlavní důvod přechodu z Nagiosu na Zabbix, byla nemožnost splnit předpoklady, které byly realizovány v Zabbixu. Například komunikaci s ITSM (IT service management) systémem, anebo shromažďovat efektivně data od veškerých zákazníků.

Jeden z dalších důvodů přechodu na Zabbix je kvůli zákaznickým sítím, kde je již dohled realizován pomocí tohoto dohledového nástroje. Díky tomu se tak zjednoduší kontrola více infrastruktur, které budou směřovat veškerá data na jeden dohledový server.

Další důvod byl, aby veškeré problémy, které zjistí zákazníci, zaměstnanci nebo dohledový systém, byly shromažďovány v jediném ITSM systému, kde se shromažďují tickety s jakýmikoliv problémy.

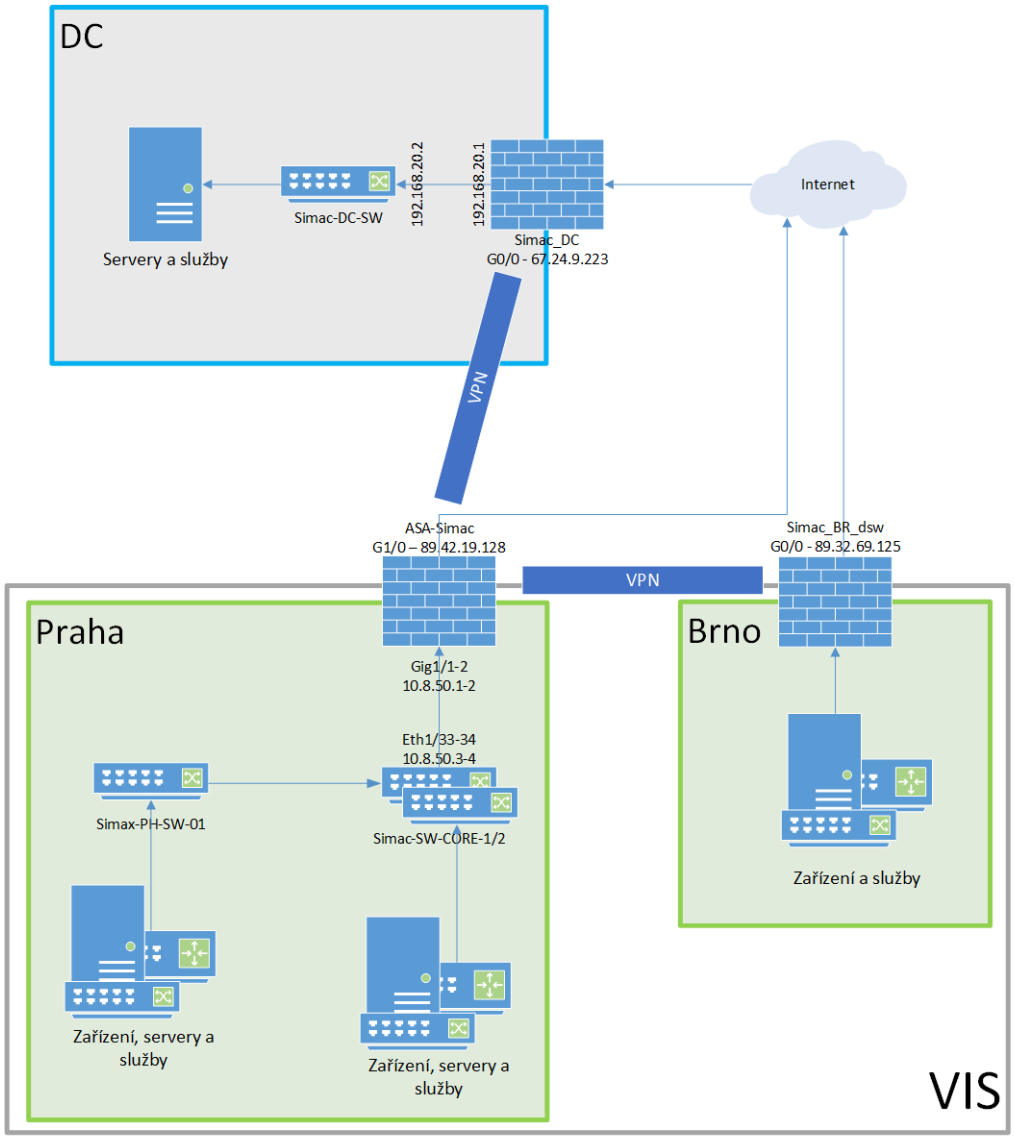
2.2 Cíle

Při implementaci Zabbixu byl kladen důraz na kontrolu sítě, tak jak byl dohled realizován v Nagiosu. Kontrolovat veškeré prvky v síti a v případě problému službu nebo zařízení restartovat. Dále využít možnosti Zabbixu, jako je automatická detekce (zařízení a služeb) v síti, tak aby se co nejvíce do budoucna eliminovaly problémy, které by mohly nastat při přidání nových hostů. Dále realizace propojení pomocí LDAP (Lightweight Directory Access Protocol) s Active Directory, aby se pro jednotlivé techniky nemuseli zakládat lokální účty, ale mohli se přihlašovat pomocí iniciálů, které jsou nastavené v AD (Active Directory).

Další cíl byl realizovat SMS bránu pro co nejrychlejší informování technika, v případě výskytu jakéhokoliv problému. Pro přehlednější seznam problémů, přeposílat požadavky na Service Deskový nástroj GLPi, kde jsou také zobrazeny problémy od zákazníků a vše tak bude na jednom místě. Dále se snažit zrealizovat automatizační skripty pro jednoduché problémy, které se díky tomu vyloučí a skripty pro nainstalování potřebných aplikaci, tak aby bylo nastavování v zabbixu, i na zařízeních co nejrychlejší.

2.3 Topologie

Níže na obrázku je topologie sítě v Simac Technik, která je rozdělena do třech segmentů Praha, Brno a Data centrum jak je vidět na obrázku 2.1. Pražská a Brněnská část slouží především jako vnitřní internetová síť (VIS), kde jsou připojeni veškeří pracovníci firmy, firemní zařízení, Wi-Fi, routery, switche a servery. Data centrum je přístupný pouze pro techniky pomocí samostatného VPN (Virtual Private Network) přístupu a využívá se pro zálohy a monitoring, který se využívá ve firmě.



Obr. 2.1: Topologie sítě Simac Technik

Na serverech umístěných ve VISu je realizováno laboratorní, testovací a produkční prostředí. V laboratorním prostředí se testují služby a programy, které by mohli být potencionálně využity ve vnitřní nebo zákaznické síti. Díky tomu se ke službám a programům, které se zde testují, nedá dostat z vnější sítě. V testovacím prostředí se služby a programy testují a ladí tak, aby se připravily na reálné podmínky. Kvůli tomu je potřeba možnost připojení z vnější sítě, aby se programy mohli otestovat, jako v reálných podmínkách. V produkčním prostředí běží veškeré nasazené služby pro firmu i zákazníky. Dále se na serverech nachází souborový systém a další funkcionality, které jsou potřeba pro správný chod firmy (Např. docházkový systém, Microsoft Active Directory, Call manager a další), ale i zařízení která jsou potřeba pro práci (Tiskárny, speciálním monitory pro schůzky v zasedacích místnostech, Wi-Fi a počítače).

Další segment sítě, který Simac využívá je datacentrum (DC), ve kterém se nachází servery se zálohami souborového systému, Veeam pro automatické zálohování na tyto servery, NTP server a nově i monitorovací Zabbix server společně se Zabbix proxy serverem. Do DC je přístup omezen pouze pomocí VPN, který mohou umožnit pouze správci sítě ve firmě.

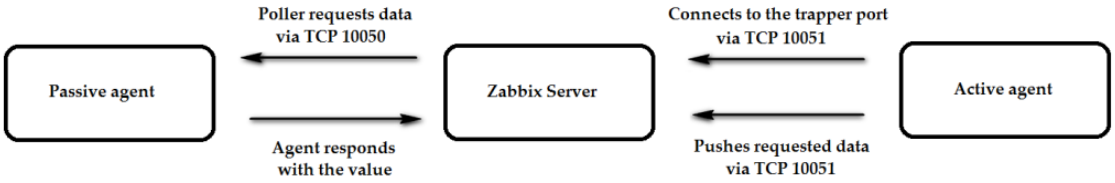
2.4 Migrace

Samotná migrace se rozdělila na několik kroků, kde se řešily jednotlivé aspekty, které bylo potřeba vyřešit, zprovoznit, nebo udělat. V prvním kroku se řešila instalace Zabbixu v data centru, Zabbix proxy v data centru a VISu, zprovoznění SMS brány a zpřístupnění přes LDAP. V druhém kroku se zprovoznilo automatické vyhledávání hostů, s přiřazováním šablon a skupin, přidání hostů, kteří nemohli být vyhledáni automaticky, utvoření map a následná kontrola všech hostů. V posledním třetím kroku se zprovoznila komunikace s GLPi, implementovaly se skripty a realizovaly se preventivní kontroly.

2.4.1 Zabbix server a proxy

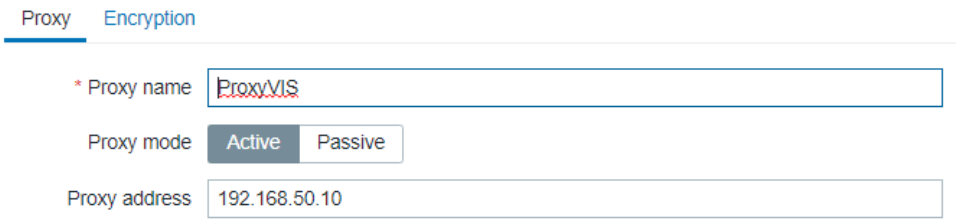
Jelikož hlavní Zabbix server je umístěn v data centru, bylo nutné nainstalovat proxy servery, které budou kontrolovat dané části sítě. Celkově se instalovali dva proxy servery, jeden v Simacu a druhý v datacentru. Proxy server v Simacu kontroluje veškeré rozsahy, které jsou umístěny v Praze a Brně. Kontrola v Brně probíhá pomocí VPN tunelu, který je realizován mezi těmito pobočkami. Další proxy server je realizován přímo v data centru, aby se nadměrně nezatěžoval hlavní server. Díky této proxy se budou následně kontrolovat i zákaznické sítě, která bude realizována skrz VPN tunely.

Oba proxy servery komunikují s hlavním serverem v aktivním režimu na portu 10051. Proxy servery posílají v pravidelných intervalech veškerá data, která zjistí od kontrolovaných hostů. Proxy server může fungovat i v pasivním režimu na portu 10050, kde se server doptává proxy serveru na informace. Komunikace je vidět na obrázku 2.2. Tyto porty se využívají ve výchozím nastavení, ale je možné využívat porty v rozsahu 1024–32767.



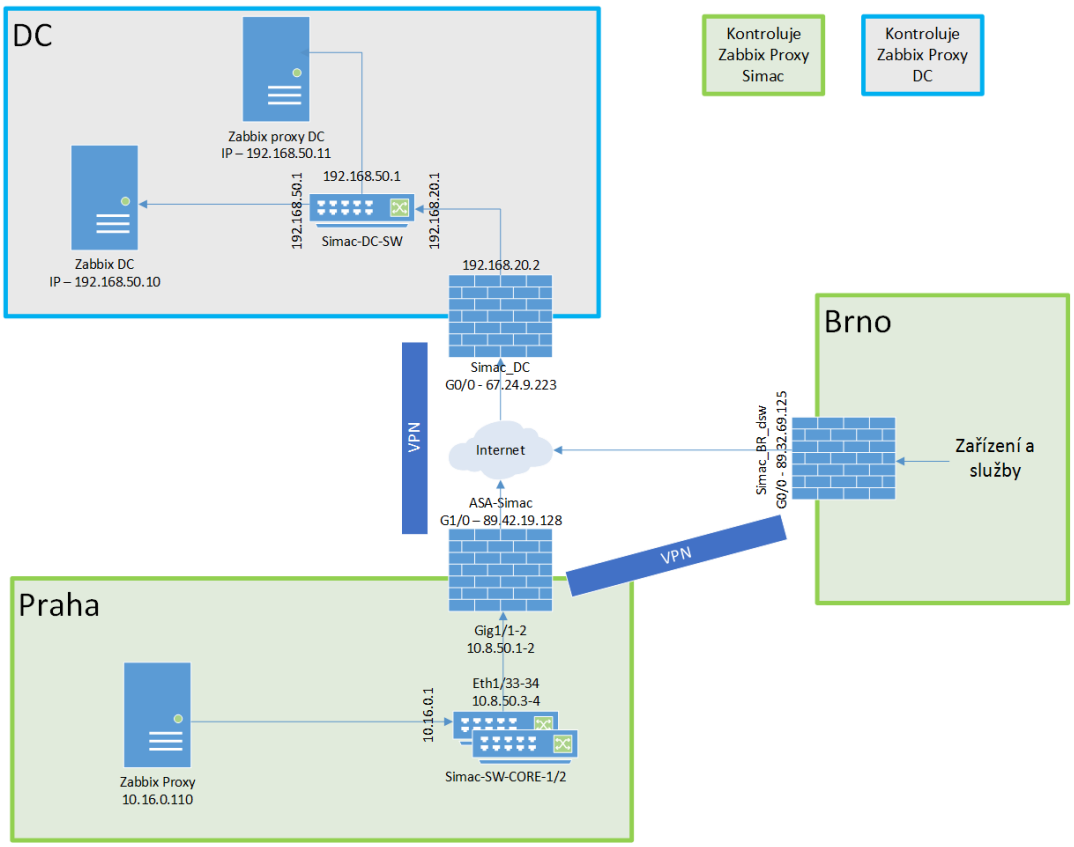
Obr. 2.2: Funkčnost agentů [21]

Zpřístupnění komunikace hlavního serveru s proxy servery, je znázorněno na obrázku 2.3. Pro správnou komunikaci bylo potřeba na firewallu vytvořit pravidla pro port 10051, aby tato komunikace byla možná.



Obr. 2.3: Nastavení komunikace server <=> proxy pro VIS

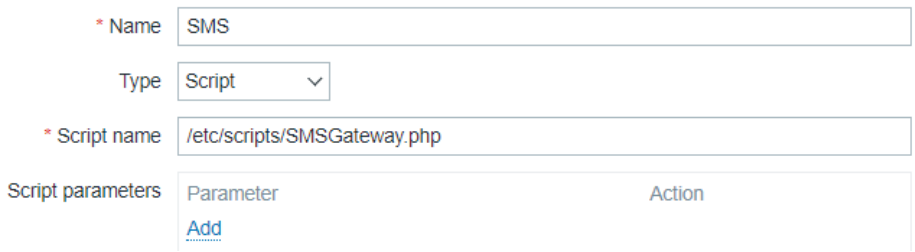
Instalace Zabbix serveru a proxy není nijak těžká a časově náročná, jak je vysvětleno v teoretické části. Na obrázku 2.4 je vidět umístění jednotlivých serverů a zároveň znázornění, jak probíhá komunikace v síti. Jednotlivé proxy servery kontrolují danou část své sítě a zjištěná data se následně posílají hlavnímu Zabbix serveru. Proxy servery kontrolují hosty pomocí Zabbix agenta, SNMP protokolu a klasického ICMP. Hlavní server pak zobrazuje data ve webovém rozhraní, které mu oba proxy servery poslaly. V případě výpadku komunikace, mezi hlavním a proxy serverem, proxy server stále sbírá data. Jakmile je spojení obnoveno, data jsou poslána na hlavní server a zobrazena.



Obr. 2.4: Umístění Zabbix serveru a proxy serverů

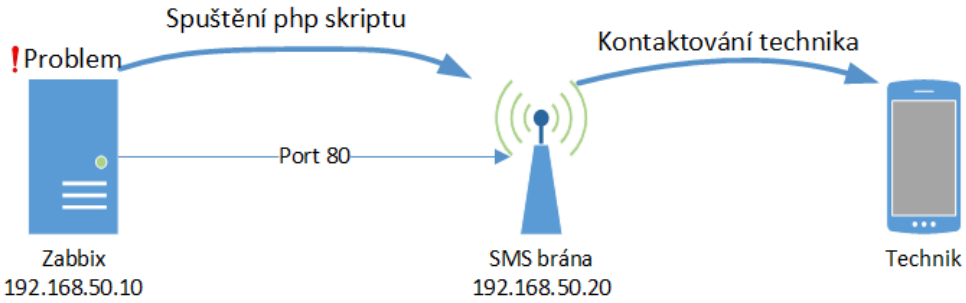
2.4.2 SMS brána

Pro posílání SMS je použita brána, od firmy HW Group - SMS-GW3 LTE. Modul je možné využít i na poplachové volání a připojit ho do LTE (Long Term Evolution) sítě. Pro komunikaci se využívá GSM (Global System for Mobile communication) anténa, která je propojena s modulem. Při implementaci je použita nová firemní SIM karta a zprovozněn skript přímo od výrobce HW group, který kontaktuje technika. Modul je připojen do sítě tak, aby s ním mohl Zabbix komunikovat pomocí skriptu od výrobce jak je vidět na obrázku 2.5.



Obr. 2.5: Nastavení SMS brány

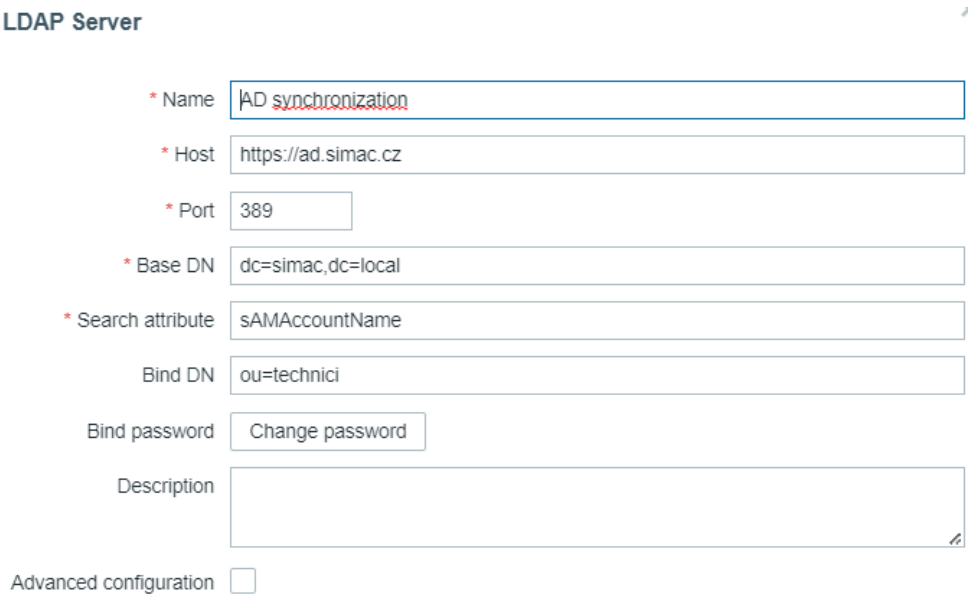
Jakmile Zabbix zjistí u jakéhokoliv hosta problém, proběhne proces, který je popsán na obrázku 2.6. Zabbix zjistí problém a využije implementovaný php skript, aby kontaktoval technika. Do SMS jsou vloženy základní informace o problému (o co jde, jaký je status a poslední hodnota). Následně jsou data odeslána technikovi.



Obr. 2.6: Schema kontaktování technika

2.4.3 LDAP (Lightweight Directory Access Protokol)

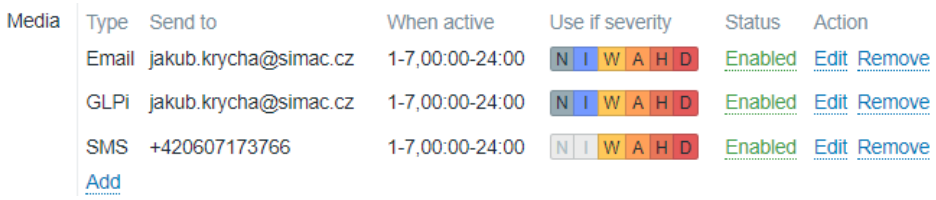
Pro techniky se vytvořila synchronizace s Active Directory pomocí LDAP. Jakmile se bude chtít technik přihlásit, Zabbix provede kontrolu v AD. Pokud technik existuje, automaticky se mu v Zabbixu vytvoří účet. V případě, že uživatel není zahrnut v AD musí účet vytvořit technik s administrátorskými právy ručně.



Obr. 2.7: Nastavení synchronizace s AD

Nastavení LDAP serveru je vidět na obrázku 2.7, kde je potřeba nastavit hosta, odkaz na LDAP server, Base DN, cesta k adresáři uživatelů, a Bind DN, vyhledávání podle skupiny uživatelů. Pro správnou synchronizaci je potřeba vytvořit uživatele v AD, přes kterého se kontrola bude provádět. Uživatel určený pro kontrolu se následně nastaví v Bind password.

Jakmile se technikovi vytvoří účet, importuje se z AD také email a telefonní číslo. Díky tomu lze technika kontaktovat přes SMS, jak je vidět na obrázku 2.8. Pro SMS se upravilo posílání notifikací s problémy pouze na varování a vyšší, zatímco u Emailu a GLPi se posílají všechna upozornění s problémy, které nastanou. Jelikož je hlavní AD umístěn ve VISu museli se na Firewallu vytvořit pravidla, aby tato synchronizace byla umožněna.



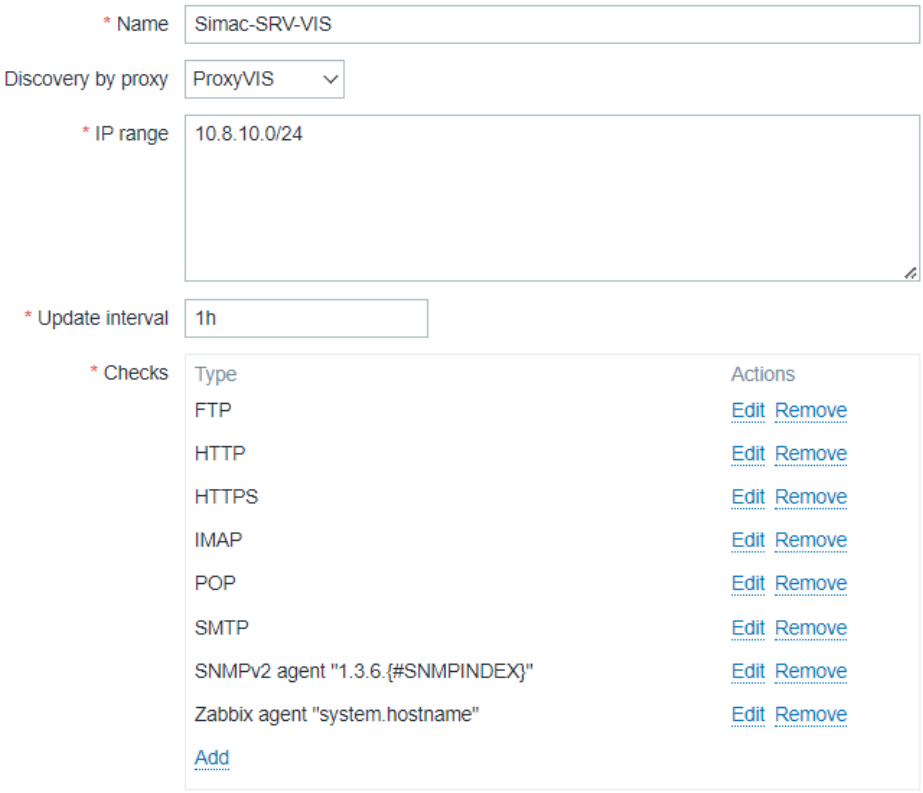
Obr. 2.8: Nastavení kontaktování uživatele

2.4.4 Přidávání hostů

Automatické vyhledávání

Při migraci z Nagiosu do Zabbixu se využívalo především funkcí implementovaného dohledového nástroje. Pro počáteční nahrání většiny hostů z vnitřní sítě se využilo automatické vyhledávání v určitých segmentech sítě. Dále se nastavilo, do kterých skupin se budou hosti přiřazovat a nastavení šablony, podle které bude kontrola hodnot probíhat. Nastavení automatického vyhledávání je vidět na obrázku 2.9.

Nastavení automatického vyhledávání obsahuje nastavení, jakým proxy serverem má být vyhledávání prováděno. Dále je nastaven IP rozsah a nastavení portů, na kterých má být vyhledávání prováděno. Je také možné nastavit předdefinované TCP nebo UDP porty, které lze nastavit jednotlivě nebo na určitý rozsah portů. V případě nastavení více IP rozsahů, není potřeba vytvářet více vyhledávacích pravidel, ale stačí rozsahy oddělit čárkou. V případě nastaveného proxy serveru u vyhledávání, se server automaticky přidělí k vyhledaným hostům v tomto rozsahu. Kontrolu pak provádí daný proxy server.

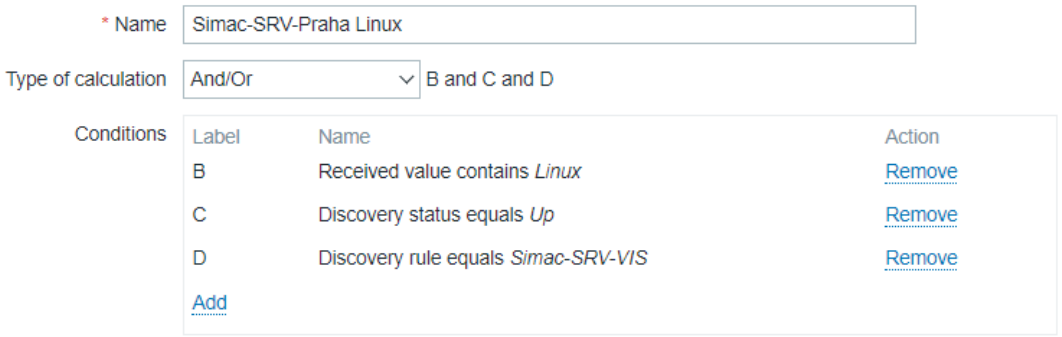


Obr. 2.9: Nastavení parametrů pro automatické vyhledávání

Počáteční vyhledávací interval byl nastaven na krátký čas, aby byly vyhledány veškeré služby a zařízení. Po vyhledání se časový úsek prodloužil, aby se zbytečně nezatěžoval proxy server.

Vyhledávání je nastaveno na obrázcích 2.10 a 2.11. Je zde ukázáno nastavení pro zjišťování Linuxových operačních systémů a veškerých operací, které se provedou při přidání hosta. Operace které se provedou při zjištění nového hosta, jsou ukázány na obrázku 2.11.

Při vyhledávání se kontroluje, zdali je daný host aktivní (Up), jestli splňuje podmínku s OS Linux a spadá do vyhledávacího pravidla Simac-SRV-VIS. Jakmile Zabbix zjistí, že host vyhovuje všem podmínkám, pokračuje vykonáním operací. Automaticky se na hosta nainstaluje SNMP protokol společně s Firewall pravidly, dále se host přidá do předdefinovaných nastavených skupin, přiřadí se šablona, podle které se bude kontrolovat a následně se kontrola povolí. Host je díky těmto operacím nastaven a může se začít kontrolovat. Následně administrátor provede kontrolu a popřípadě doplní další šablony podle služby která na daném OS běží.

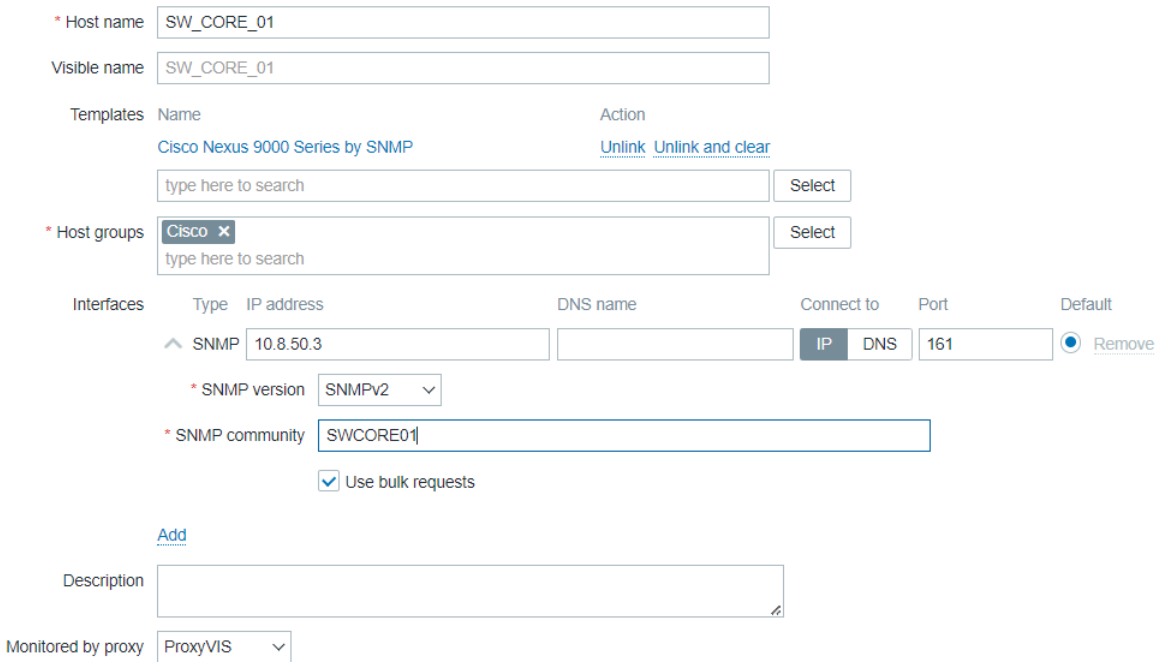


Obr. 2.10: Nastavení vyhledávání

Obr. 2.11: Nastavení operací pro vyhledávání

Ruční přidání

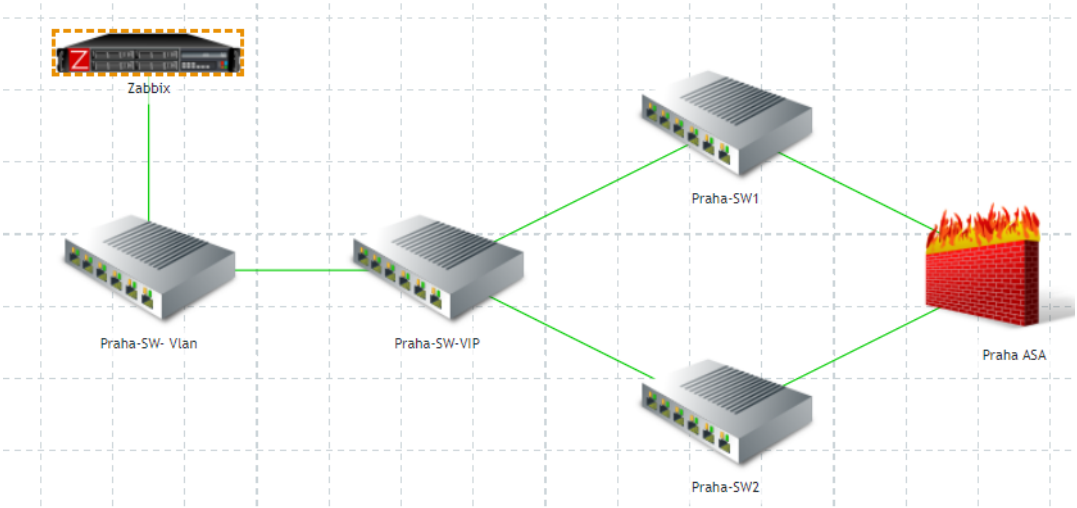
Po přidání všech hostů automaticky se zbylí hosti přidají ručně. Jde například o síťové prvky, jako jsou switche, routery anebo veřejné adresy, které je potřeba kontrolovat. Na obrázku 2.12 je vidět kompletní nastavení přidání switche, kde se nastaví jméno, šablona, do které skupiny se host přiřadí a jaký proxy server má tohoto hosta kontrolovat. Kontrola se provádí podle vyplněné IP adresy, nastavené SNMP verze a do jaké SNMP komunity prvek spadá.



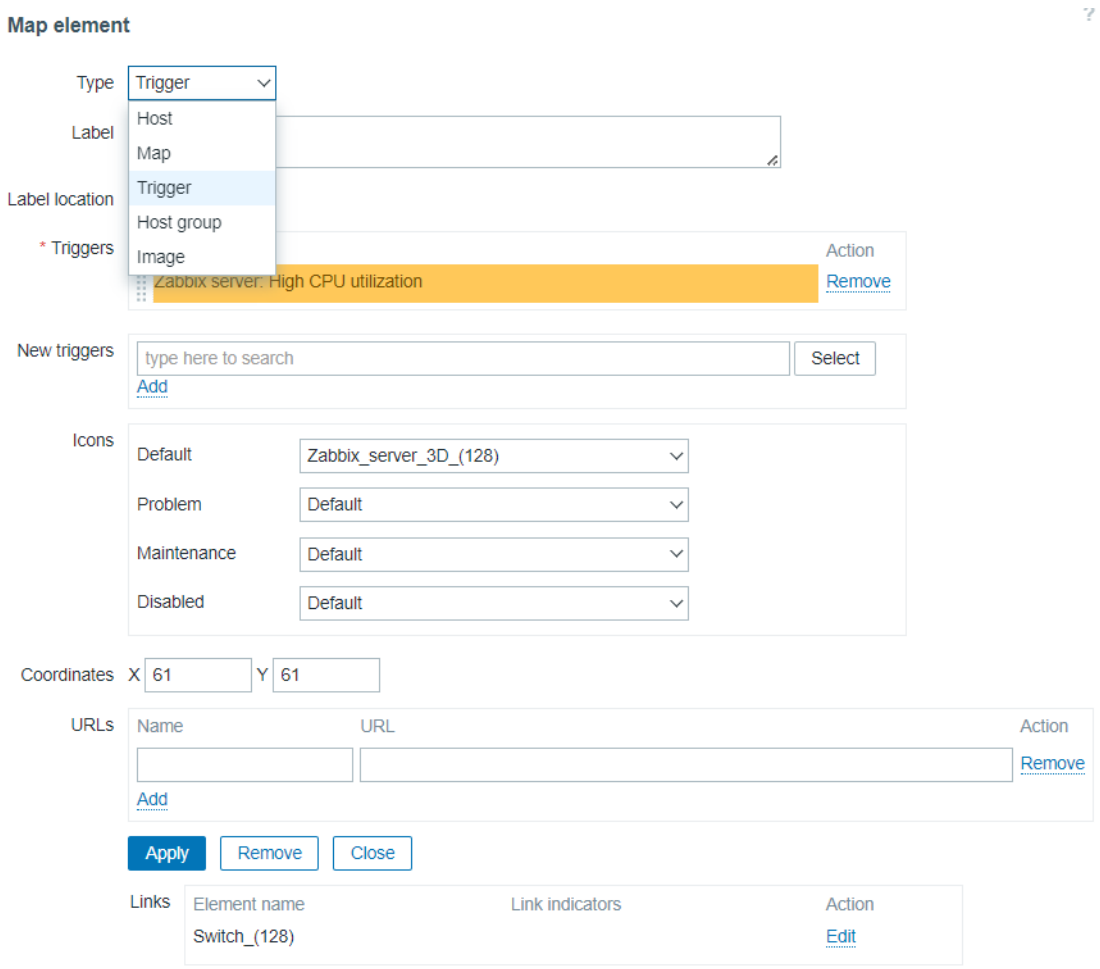
Obr. 2.12: Nastavení hosta při ručním přidání

Nastavení mapy

Po zjištění zařízení a služeb se vytvořily jednotlivé segmenty sítě pomocí map viz. obrázek 2.13. Jelikož mapy umožňují odkazovat se na další mapu a skupinu, viz obrázek 2.14 bylo toho využito pro přehlednost jednotlivých částí sítě, aby nebylo vše v jedné velké mapě. Jakmile vznikne nějaký problém v síti, je možné daný problém najít v mapě a přesně lokalizovat na jakém místě se stal.



Obr. 2.13: Nastavení mapy



Obr. 2.14: Nastavení Závislostí v mapě

2.4.5 Nastavení na zařízení

Na kontrolovaných zařízeních a službách je nutné povolit SNMP a nainstalovat Zabbix agenta, aby bylo možné kontrolovat všechny aspekty zařízení a služeb. Poté je nutné vytvořit firewall pravidla pro SNMP protokol, aby se zpřístupnila komunikace mezi zařízeními a proxy serverem.

Cisco switch/router

Cisco switche a routery tvoří celou interní síť firmy, proto se pomocí jednoduchého příkazu níže nainstaluje SNMP protokol. Díky tomu mohou být routery a switche kontrolovány. Na switche a routery nemůže být nainstalován Zabbix agent, a proto je SNMP protokol jediná možnost, jak je kontrolovat.

```
snmp-server community public RO
```

Samotný router nebo switch nemá přímo implementovaný firewall a díky tomu není potřeba nastavovat firewall pravidla. V případě, že je router používaný jako vstupní bod do internetu a je nutné jej kontrolovat, musí se implementovat firewall pravidla.

Windows a Linux

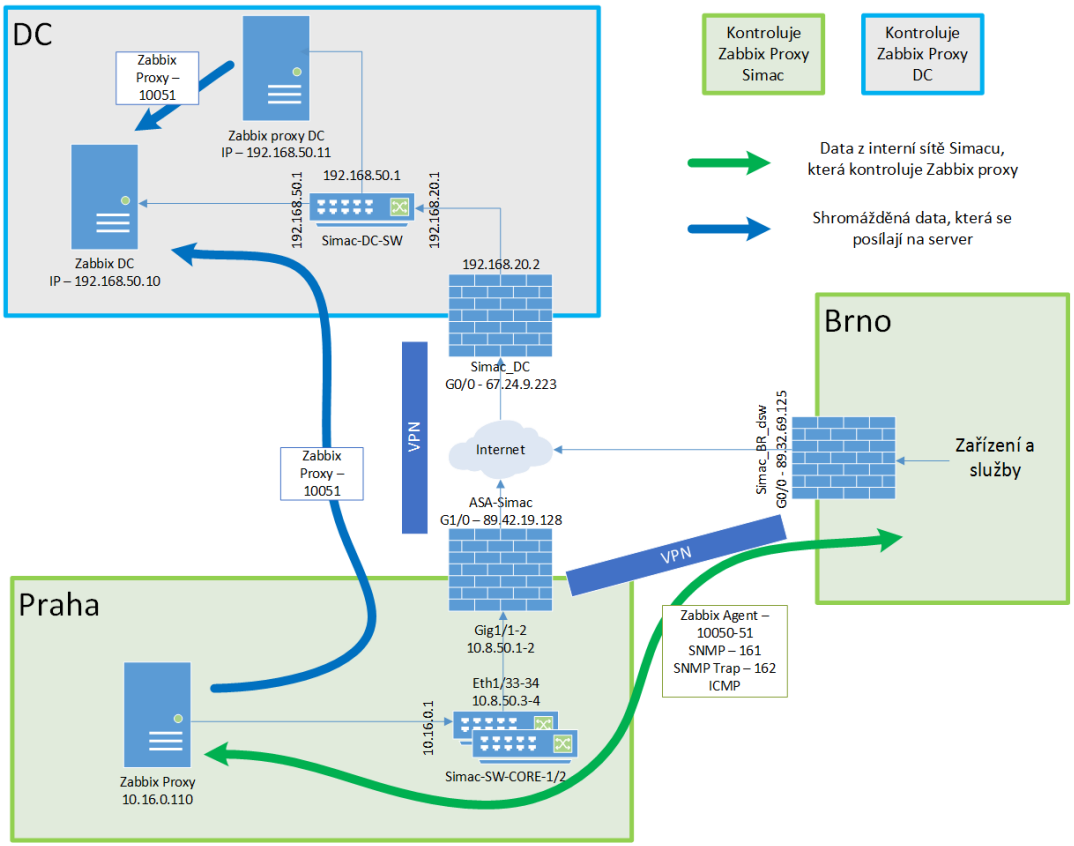
Pro Windows i Linux je nutné nainstalovat SNMP, Zabbix agenta a implementovat firewall pravidla. V případě neimplementování firewall pravidel je možné, že Zabbix nebude přijímat žádné hodnoty, jelikož neprojdou přes firewall operačního systému.

Ve Windowsu je možné SNMP nainstalovat přes Přidat volitelnou funkci, kde se následně vyhledá SNMP protokol a agen. Celkové nastavení SNMP lze najít v seznamu služeb, kde si technik nastaví vše, co potřebuje pro správnou komunikaci a funkčnost. Druhá možnost je instalace pomocí PowerShellu, který je popsán níže v automatické instalaci SNMP protokolu. Zabbix agenta lze nainstalovat pomocí návodu, který je podrobně popsán na stránkách Zabbixu.

V Linuxu se SNMP instaluje pouze v příkazovém řádku, kde se upravuje i SNMP konfigurační soubor. Technik následně upraví daný soubor dle svých požadavků. Návod na nainstalování Zabbix agenta je taktéž popsán na stránkách Zabbixu. Instalace agenta na oba operační systému není nijak těžká a ani časově náročná.

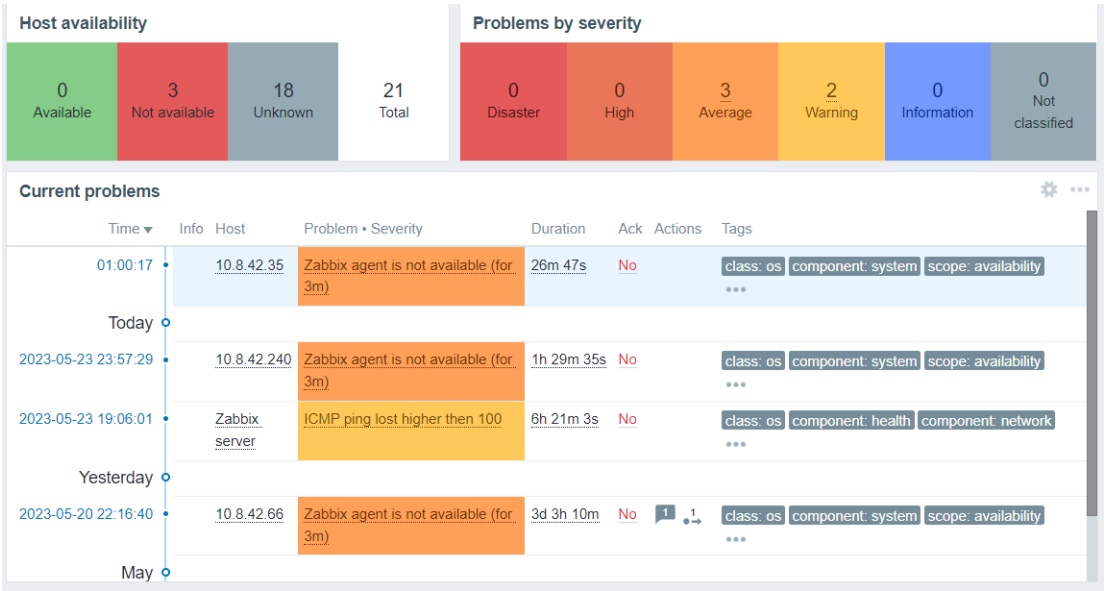
2.5 Provádění kontroly

Při provádění kontroly v Simac Technik jsou nainstalovány Zabbix proxy servery do jednotlivých segmentů sítě, jak je vidět v topologii na obrázku 2.4. Zabbixy, které kontrolují segmenty sítě pro VIS a DC jsou nainstalovány jako proxy servery a posílají data na hlavní Zabbix server, který se nachází v datacentru. Stejné řešení je implementováno i pro zákazníky, kde je také nainstalován proxy server. Jak komunikace probíhá v síti je vidět na obrázku 2.15. Pro kontrolu byly potřeba firewall pravidla pro jednotlivé porty, které se k dohledu využívají, aby Zabbix proxy ve VISu byl schopen kontrolovat všechny hosty i v Brně. Dále bylo potřeba implementovat firewall pravidlo pro port 10051, mezi VIS a DC, aby mohl proxy server posílat data na hlavní Zabbix.



Obr. 2.15: Komunikace v síti

Celkový souhrn je zobrazen na dashboardu, který se zobrazí přímo po přihlášené do Zabbixu. Nejdůležitější sekce je zobrazena na obrázku 2.16 Je zde zobrazen souhrn informací, jako dostupnost hosta, počet jednotlivých problémů a seznam problémů, které jsou zobrazeny v časové ose.



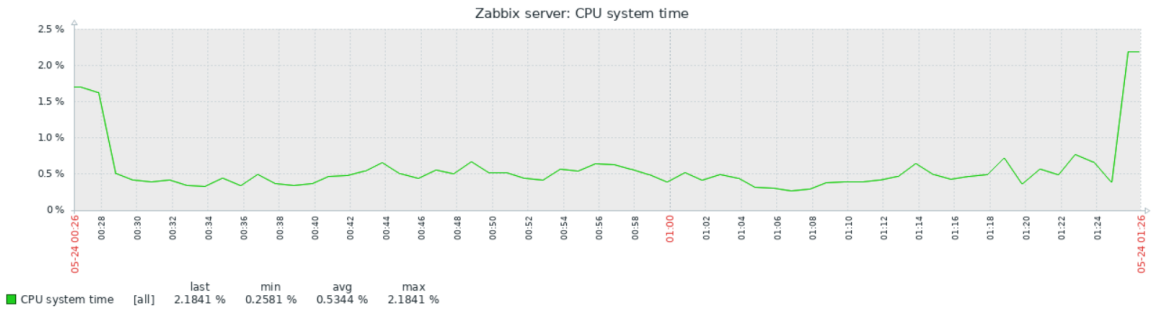
Obr. 2.16: Dashboard Zabbixu

Při řešení problému je možné si zobrazit veškeré parametry hosta, které momentálně Zabbix dostává. Některé sledované parametry je možné vidět na obrázku 2.17. Pro zobrazení určitých hodnot je možné využívat filtr, pomocí kterého je možné odfiltrovat parametry ostatních hostů anebo si zobrazit například CPU parametry.

CPU system time	9s	0.383 %	-0.2748 %	component: cpu
CPU user time	9s	1.1073 %	-0.0833 %	component: cpu
CPU utilization	9s	2.7616 %	-0.6537 %	component: cpu
Free memory	9s	5.89 GB	+3.42 MB	component: memory
Free swap space	9s	4 GB		component: memory component: storage
Free swap space in %	27s	100 %		component: memory component: storage
ICMP loss	2s	0 %		component: health component: network
ICMP ping	2s	Up (1)		component: health component: network
ICMP response time	2s	0.13ms	+0.027ms	component: health component: network
Interface ens160(): Bits received	9s	3.05 Kbps	+192 bps	component: network description interface: ens160
Interface ens160(): Bits sent	9s	30.3 Kbps	+9.41 Kbps	component: network description interface: ens160

Obr. 2.17: Zobrazení hodnot

U některých sledovaných parametrů je nakonfigurováno vykreslování hodnot do grafu, jak je vidět na obrázku 2.18. Graf tak může odhalit kdy problém přibližně začal, i přesto, že se nevytvořila varovná událost. V grafu je možné zobrazit vývoj hodnot za celý rok.



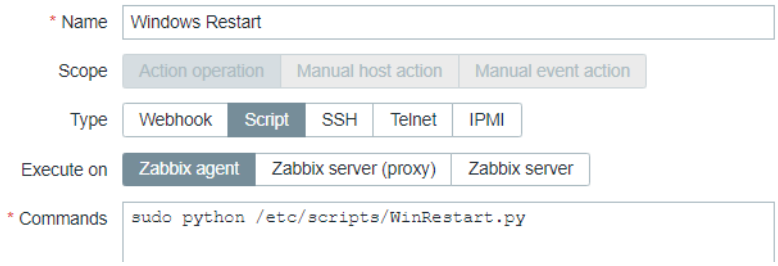
Obr. 2.18: Zobrazení grafu

2.6 Automatizace

V rámci automatizace je v Zabbixu implementováno několik automatizačních procesů. Pro upozornění technika na problém je připojena SMS brána pro zasílání upozornění na telefonní číslo, která je vysvětlena výše. Dále je Zabbix propojen s LDAP databází, aby se pro jednotlivé techniky nemusely vytvářet lokální účty, ale měli možnost se přihlašovat pomocí iniciálů z AD, popsáno také výše. Nakonec je zprovozněna komunikace mezi Zabbixem a GLPi, pro automatické vytváření ticketů s problémy, které nastanou.

Pro kontrolované hosty jsou implementovány skripty, které dokážou u hostů s operačním systémem Windows a Linux, změnu DNS, automatickou instalaci SNMP protokolu a automatický restart zařízení a služeb, které provozujeme (web server, GLPi a další). Dále je zrealizováno automatické zálohování konfigurací vybraných síťových prvků a pro snadnější řešení problémů, je v rané fázi vývoje, využívání porovnávání ticketů pomocí umělé inteligence.

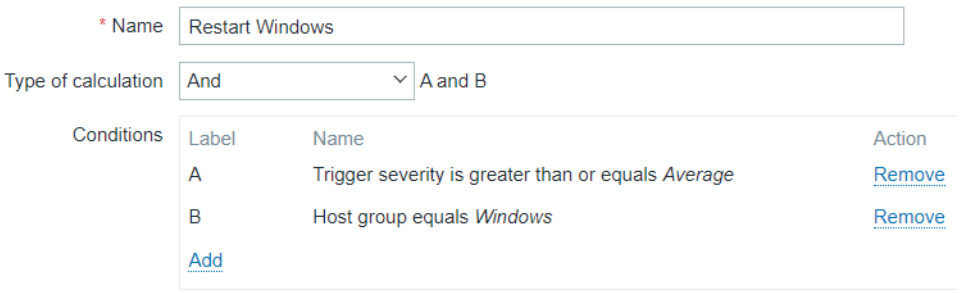
Skripty je možné implementovat přímo v Zabbixu anebo je možné vytvořit samostatný skript. Skript je uložen v souborovém systému Zabbixu a je spouštěn skrz odkaz na konkrétní skript viz. obrázek 2.19.



Obr. 2.19: Spouštění Windows skriptu

2.6.1 Automatický restart zařízení a služeb

V případě změny stavu triggeru do stavu Avarege a horší se host automaticky restartuje, viz. obrázek 2.20. Jakmile dochází k restartu, operace jsou nastaveny identicky jako na obrázku 2.22. Je možné, že bude mnohem lepší změnit restart z globálních stavů triggerů, na restartování podle určitých parametrů a hodnot, jelikož to může v budoucnu znamenat zacyklení restartu například při vysokém obsazení úložiště.



Obr. 2.20: Nastavení operací pro restartování Windowsu

Restart Linuxu

```
sudo reboot
```

```
sudo reboot
```

Restart Windowsu

```
import os

os.system("shutdown␣/r␣/t")
```

Restart služeb

Webový server

```
sudo systemctl restart httpd.service

sudo systemctl restart nginx.service
```

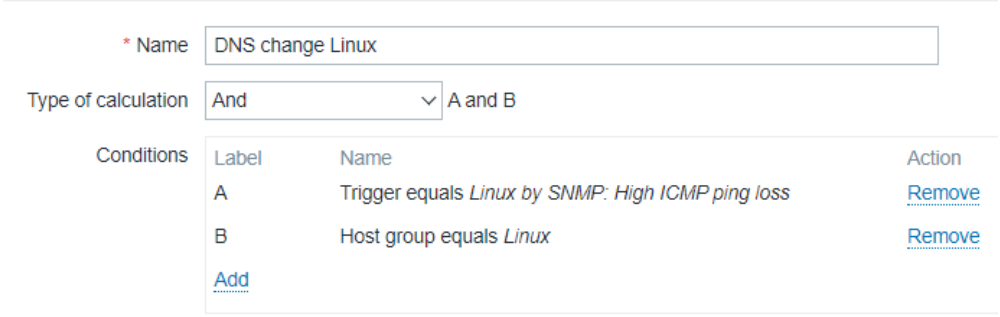
Zabbix agent a proxy

```
sudo systemctl restart zabbix-agent

sudo systemctl restart zabbix-proxy
```

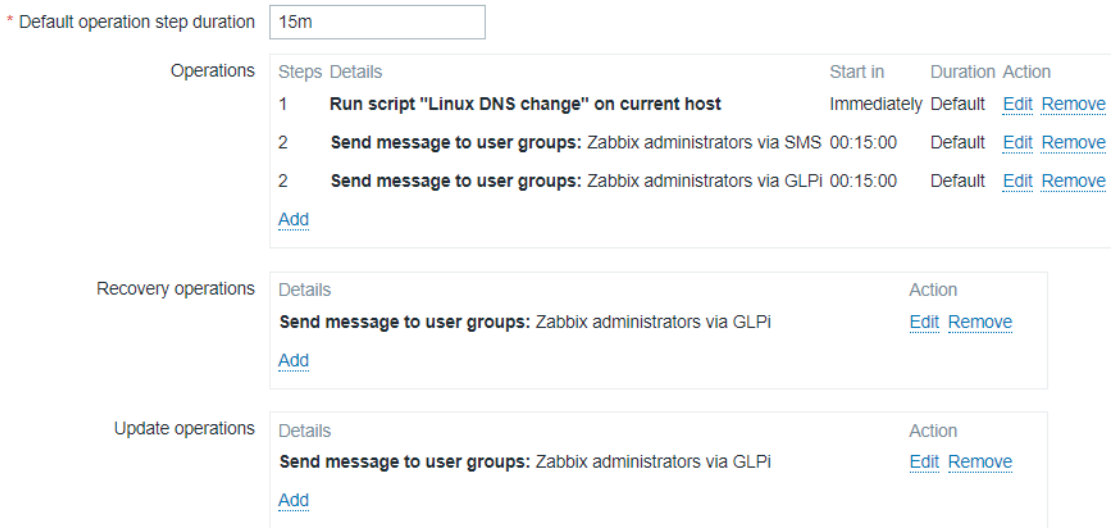
2.6.2 Změna DNS (Domain Name System)

V případě velké ztráty ICMP packetů je implementovaný skript na změnu DNS, jak je vidět na obrázku 2.21 a 2.22. Je zde nastavení podmínek, kde host, který má problém musí splňovat, že je ve skupině Linux a nastavený trigger, který je v templatu Linux by SNMP, je ve stavu Warning. Na druhém obrázku jsou nastaveny operace, které se provedou, jakmile jsou splněny podmínky z prvního obrázku. Jako první se spustí skript, který je vypsaný dále. Pokud změna DNS nepomůže, po

patnácti minutách se kontaktují Zabbix administrátoři pomocí GLPi a SMS. V případě vyřešení, nebo jakékoliv aktualizace daného problému, se posílají aktualizace na GLPi ticket.



Obr. 2.21: Nastavení podmínek



Obr. 2.22: Nastavení operací

Níže jsou vidět skripty na změnu DNS u Linuxu i Windowsu. U Linuxu se musí přistoupit do složky kde se připíše řádek s alternativními DNS, zatímco u Windowsu skript změní DNS u Ethernetového i Wi-Fi připojení.

Změna DNS na Windowsu

```
import os

os.system( netsh interface ipv4 set dns name="Ethernet"
static 4.4.4.4 )
```

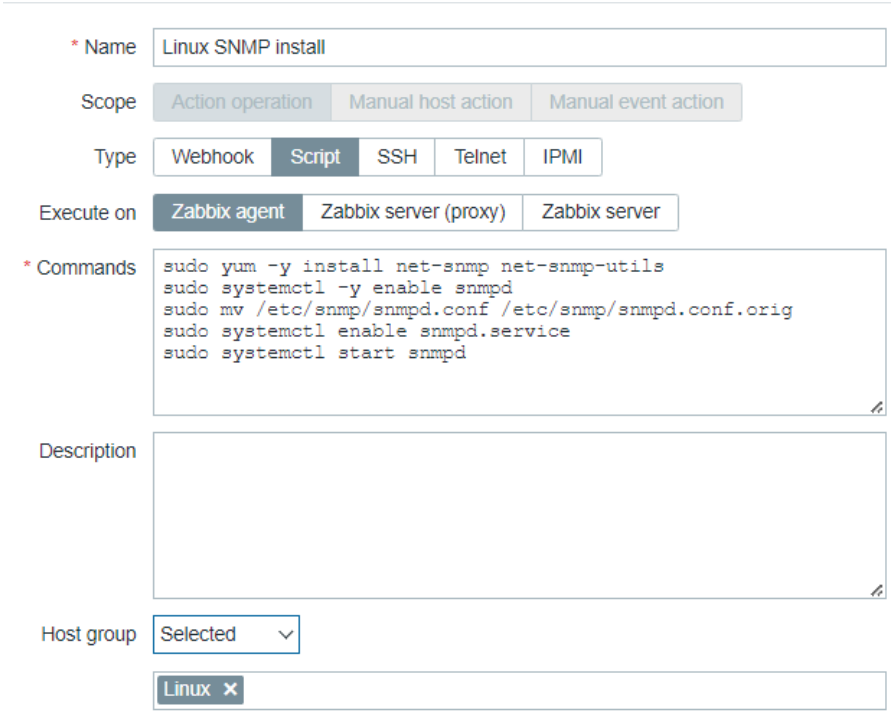
```
os.system( netsh interface ipv4 set dns name="Wi-Fi"
static 4.4.4.4 )
```

Změna DNS na Linuxu

```
from configparser import ConfigParser

  file = "/etc/resolv.conf"
  config = ConfigParser()
  config.read(file)

  config.set("nameserver␣4.4.4.4")

  with open(file, "w") as configfile:
config.write(configfile)
```

2.6.3 Automatická instalace SNMP

Při automatickém zjišťování je použita instalace SNMP a implementace firewall pravidel, pro zjednodušení prvotního nastavení a kontrolování. Na obrázku 2.23 je nastavení skriptu v Zabbixu, pro instalaci SNMP protokolu na Linux. Díky tomu se můžou vyhledané prvky začít hned kontrolovat.



Obr. 2.23: Nastavení skriptu v Zabbixu

Implementování Firewall pravidel a instalace SNMP Linux

```
sudo yum -y install net-snmp net-snmp-utils
sudo systemctl -y enable snmpd
sudo mv /etc/snmp/snmpd.conf /etc/snmp/snmpd.conf.orig
sudo systemctl enable snmpd.service
sudo systemctl start snmpd

sudo firewall-cmd --zone=public --add-port=161/udp --permanent
sudo firewall-cmd --zone=public --add-port=161/tcp    -permanent
sudo firewall-cmd --zone=public --add-port=162/udp --permanent
sudo firewall-cmd --zone=public --add-port=162/tcp --permanent
sudo firewall-cmd --reload
```

Implementování Firewall pravidel a instalace SNMP Windows

Při instalaci SNMP na Windows je implementováno zjištění operačního systému, aby se skript použil správně. Operační systémy Windows nemají mezi verzemi stejný globální příkaz pro instalaci SNMP. Proto je nutné si verzi operačního systému, tedy formát příkazu, zjistit a následně provést instalaci.

```
import os
import platform
import subprocess

def run(self, commandline):
  complete = subprocess.run(["powershell", "-Command",
  commandline],  capture_output=True)
  return complete

os.system("cd␣..")
os.system("cd␣..")

if platform.release() ==    10   :
  os.system(  Add  -WindowsCapability -Online -Name
  "SNMP.Client~~~~0.0.1.0"   )
  os.system("DISM␣/online␣/add-capability
␣␣/capabilityname:SNMP.Client~~~~0.0.1.0")
  os.system("DISM␣/online␣/add-capability
␣␣/capabilityname:WMI-SNMP-Provider.Client~~~~0.0.1.0")

elif platform.release() ==    11   :
```

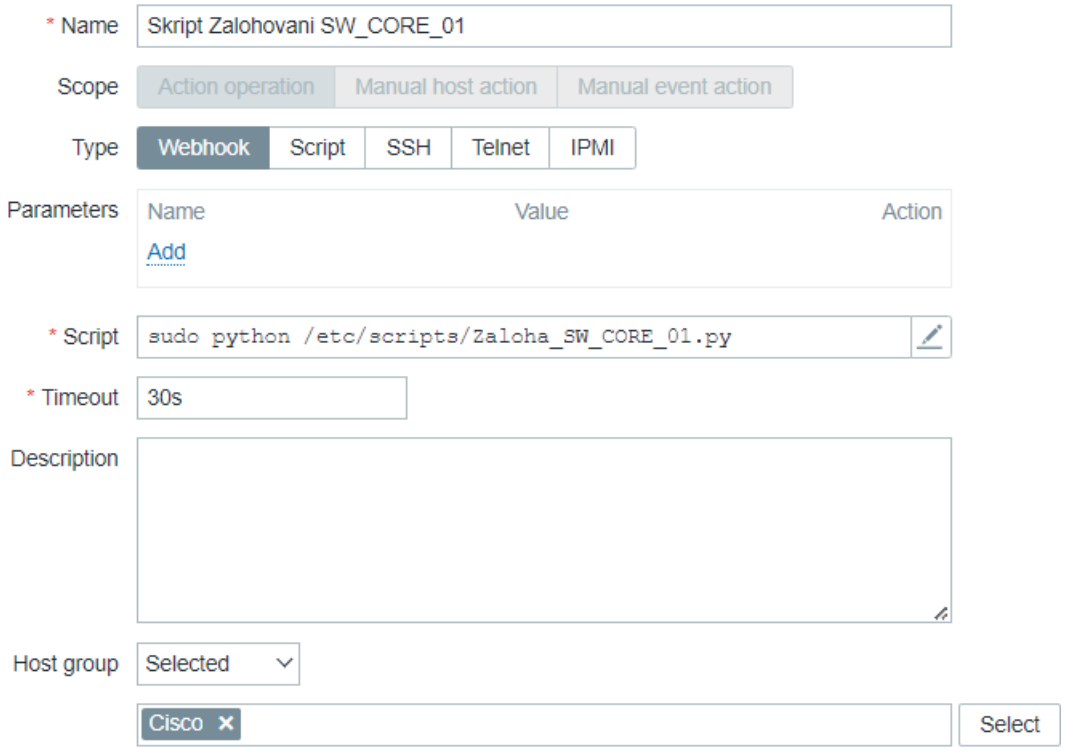
```
  os.system( Get -WindowsCapability -Online -Name
  "*SNMP*"|select name,DisplayName, State )
  os.system( Add -WindowsCapability -Online -Name
  "SNMP.Client~~~~0.0.1.0"  )
  os.system( Add -WindowsCapability -Online -Name
  "WMI-SNMP-Provider.Client~~~~0.0.1.0"  )
else:
  os.system("Get-WindowsFeature␣SNMP*")
  os.system("Install-WindowsFeature␣SNMP-Service,
␣␣SNMP-WMI-Provider-IncludeManagementTools")

import os
os.system( netsh advfirewall firewall add rule name=
  "SNMP␣UDP␣Port␣161␣In" dir=in action=allow protocol=
  UDP localport=161  )
os.system( netsh advfirewall firewall add rule name=
  "SNMPTRAP␣UDP␣Port␣162␣In" dir=in action=allow protocol=
  UDP localport=162  )
os.system( netsh advfirewall firewall add rule name=
  "SNMP␣UDP␣Port␣161␣Out" dir=out action=allow protocol=
  UDP localport=161  )
os.system( netsh advfirewall firewall add rule name=
  "SNMPTRAP␣UDP␣Port␣162␣Out" dir=out action=allow
  protocol=UDP localport=162  )
```

Automaticke zálohování konfigurací

Jelikož většina sítě se skládá z Cisco zařízení, k zálohování se použil skript, kde se využívá knihovna Netmiko. Pomocí této knihovny je možné se připojit na zařízení pomocí SSH a vykonat nakonfigurované příkazy. Skript obsahuje připojení pomocí ConnectHandleru, vypsaní konfigurace pomocí show running-config a zapsaní do textového souboru. Samotná implementace skriptu je omezena pouze na skupinu Cisco a díky tomu se nebude spouštět na jiných zařízeních. Realizace je vidět na obrázku 2.24.

```
from netmiko import ConnectHandler

ssh_SW_CORE_01 = ConnectHandler(
'device_type': 'cisco_ios',
'ip': '10.8.50.3',
```

```
'port': 22,
'username': 'admin',
'password': 'Heslo123*',
)

output = ssh_SW_CORE_01.send_command("show run")
save_run = open("SW_CORE_01_running.txt","w")
save_run.write(output)
save_run.close()
ssh_SW_CORE_01.disconnect()
```

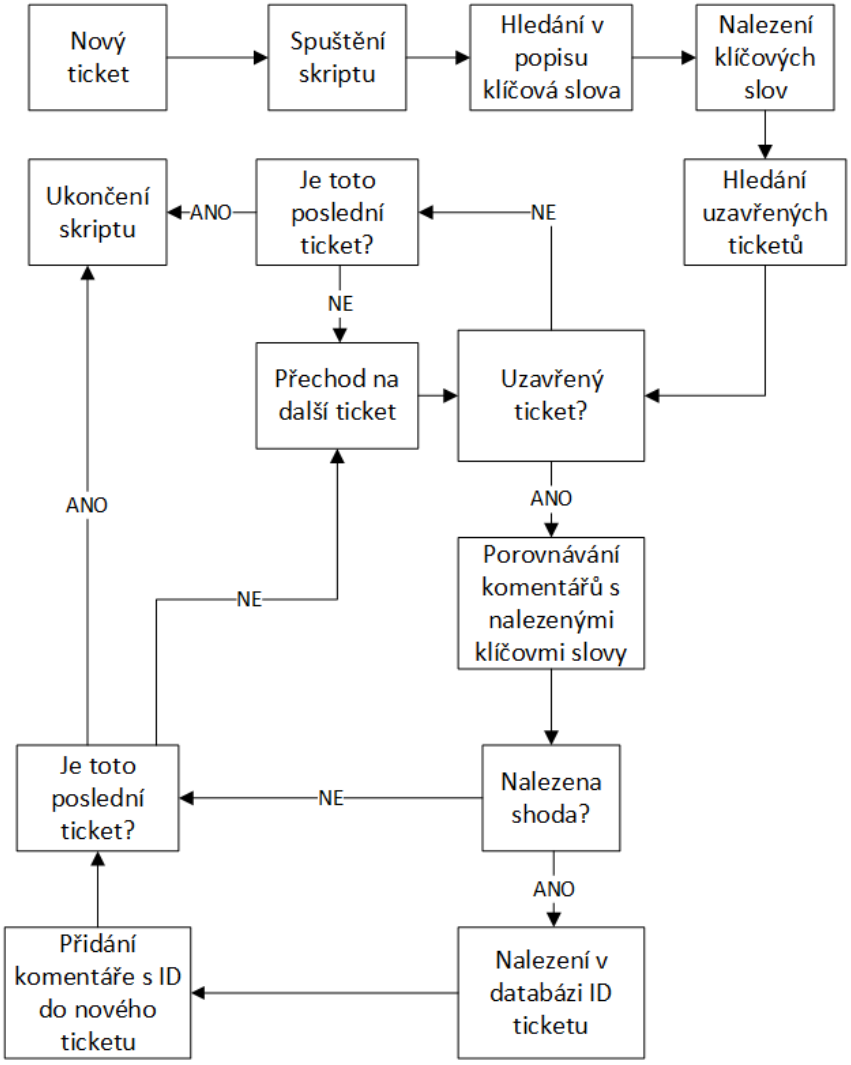


Obr. 2.24: Nastavení implementace zálohování

Porovnávání ticketů pomocí umělé inteligence

Realizace porovnávání ticketů je realizována na základě klíčových slov, které jsou obsaženy v popsání problému, když se ticket zakládá. Skript podle nakonfigurovaných slov a frází hledá podobnost v novém ticketu a porovnává nalezené podobnosti v uzavřených ticketech. V případě nalezení ticketu s podobnými frázemi, skript dohledá v databázi ID ticketu, který pak vloží do ticketu jako komentář.

Na obrázku 2.25 je vidět podrobnější funkčnost, jak by měl skript fungovat. Jakmile je vytvořený nový ticket, spustí se skript, který začne hledat v popisu problému klíčová slova (ESET, ARUBA, Firewall a další), nebo začne hledat podobná Trigger ID, která posílá v popisu Zabbix. Následně se spustí hledání uzavřených ticketů. Jakmile je ticket uzavřený hledají se podobnosti na základě vyhledaných klíčových slov nebo ID. V případě, že je nalezena podobnost vkládá se komentář s ID nalezeného ticketu do ticketu. V případě, že je ticket uzavřený, ale nenajdou se žádné podobnosti, zkontroluje se, jestli není tento ticket v seznamu poslední. Kontrola, zdali je ticket poslední je implementována, aby se skript nezacyklil a nevytěžoval tak GLPi. Jakmile se dojde na konec seznamu ticketů skript je ukončen a čeká se na další nový ticket.

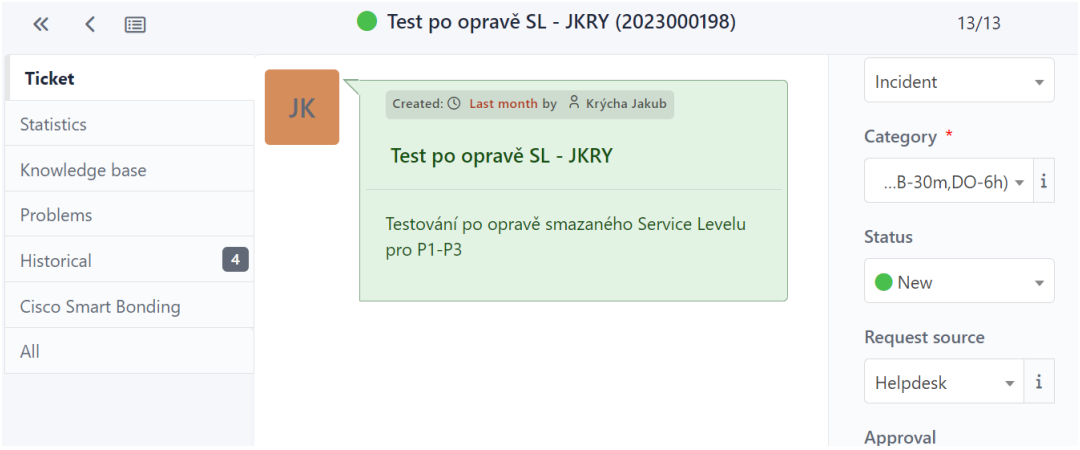


Obr. 2.25: Schema porovnávání

Skript může provádět porovnání, jelikož má přístup do databáze GLPi. Na obrázcích 2.26 a 2.27 je vidět jak vypadá vytvořený ticket v databázi a jak vypadá v GLPi. Jakmile skript začne hledat podobnosti, vyhledává v textu, který je menším písmem v zelené bublině. Text, který je zde napsaný, je obsažený v databázi pod proměnou content. Jakmile najde klíčová slova, začne procházet tickety a kontrolovat sloupec status. V případě, že má status hodnotu 6 znamená to, že daný ticket je uzavřený a skript může v daném ticketu nacházet podobnosti podle nalezených klíčových slov. Jakmile najde podobná slova, zjistí si ID ticketu ze sloupce id a vloží zjištěné ID do komentáře, který se přidá do ticketu.

id	enti	name						status			content
2,023,000,197	1	test glpi	)23-	ULL	ULL	)23-	)23-	237	2	237	2	<p>upload files >1</p>¶<p>
2,023,000,198	4	Test po opravě SL - JKRY	)23-	ULL	ULL	ULL	)23-	280	1	280	1	<p>Testování po opravě smazaného Service Levelu pr
2,023,000,199	4	Test ticket - JKrych	)23-	ULL	ULL	ULL	)23-	280	1	280	1	Testování SLA
2,023,000,200	4	Test ticket P2 - JKrych	)23-	)23-	)23-	)23-	)23-	280	6	280	1	Test
2,023,000,201	4	Test ticket P3 - JKrych	)23-	)23-	)23-	)23-	)23-	280	6	280	1	test

Obr. 2.26: Ukázka databáze GLPi



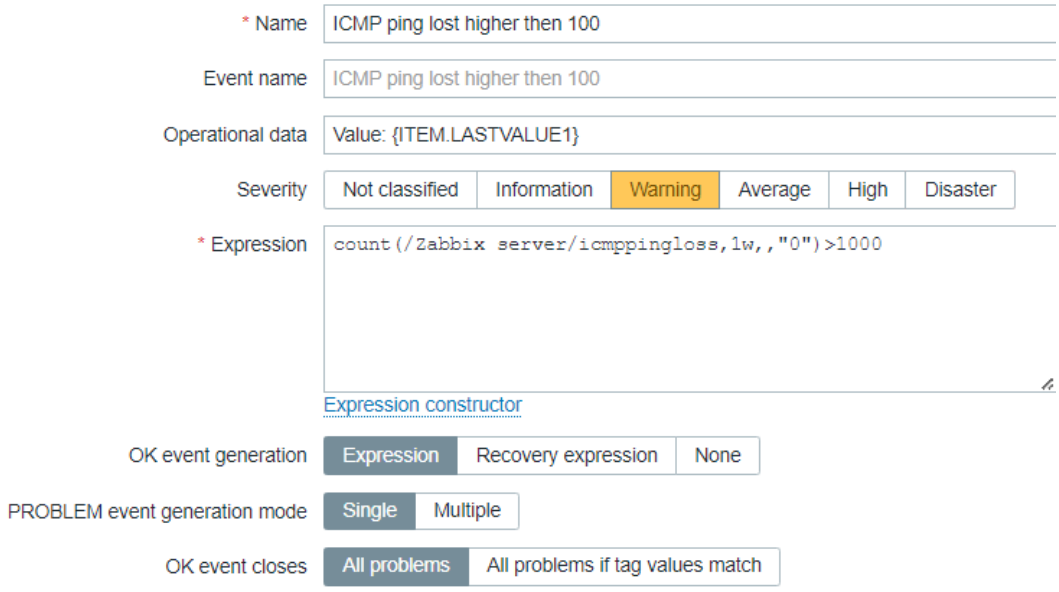
Obr. 2.27: Ukázka ticketu v GLPi

2.7 Prevence

Prevence je u Zabbix šablon udělaná dobře, jelikož je již implementováno mnoho parametrů, které se kontrolují. Některé preventivní kontroly se ovšem musely přidat anebo upravit. Doplnit se musela kontrola vytížení příchozího provozu ethernetového portu, počítadlo automatických restartů a úprava hodnot při vytížení CPU, paměti, zaplnění vnitřního úložiště a dalších.

2.7.1 Prevence při pravidelném restartování

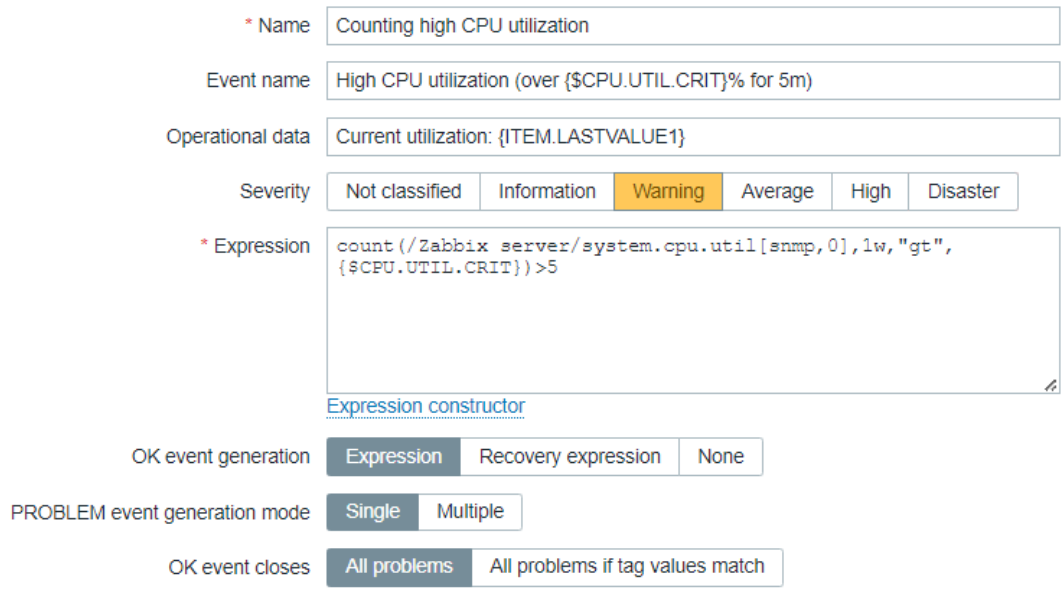
Nastavení sledování ztracených packetů, jakmile dochází k častějšímu restartování ztracené packety se započítávají. Jakmile je paketů za týden více než 1000 vytvoří se varování, které může indikovat, že je potřeba zařízení zkontrolovat.



Obr. 2.28: Nastavení podmínek

2.7.2 Prevence při pravidelném vytížení CPU

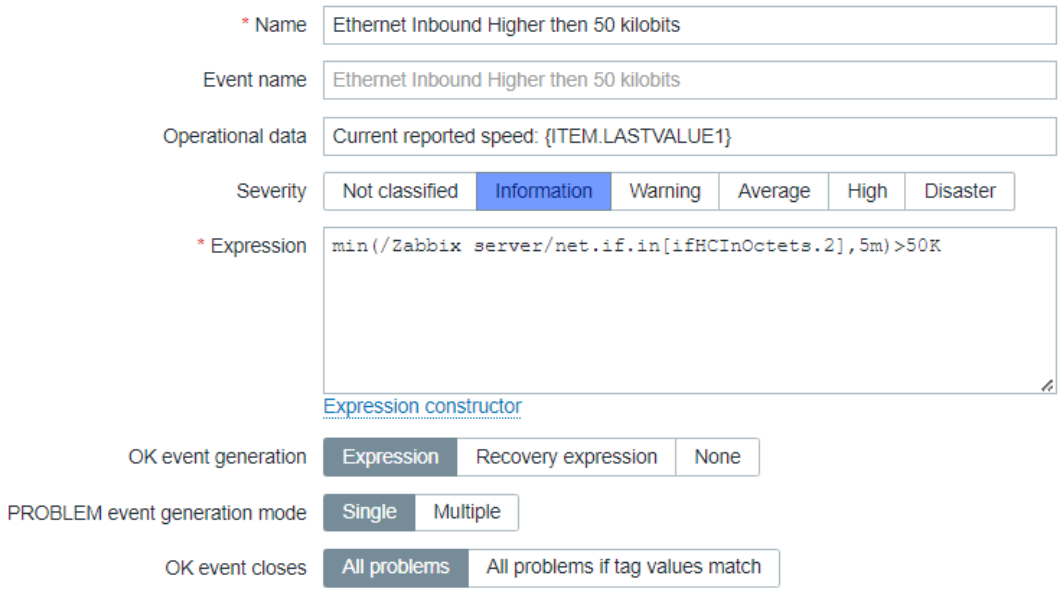
Kontrola vytížení procesoru, kde se počítá překročení kritické hodnoty procesoru za jeden týden. Jakmile procesor přesáhne pětkrát za týden kritickou hodnotu vytvoří to událost s varováním.



Obr. 2.29: Nastavení podmínek

2.7.3 Prevence při vysokém příchozím provozu

Kontrola příchozího provozu, kde se kontroluje vytížení ethernet portu. Jakmile je po dobu pěti minut vytížení větší než 50 kilobit a automaticky se vytvoří informační událost. Technici tak budou automaticky informováni o tom, že někdo nadbytečně vytěžuje síť.



Obr. 2.30: Snížení rychlosti pod 50 kilobit

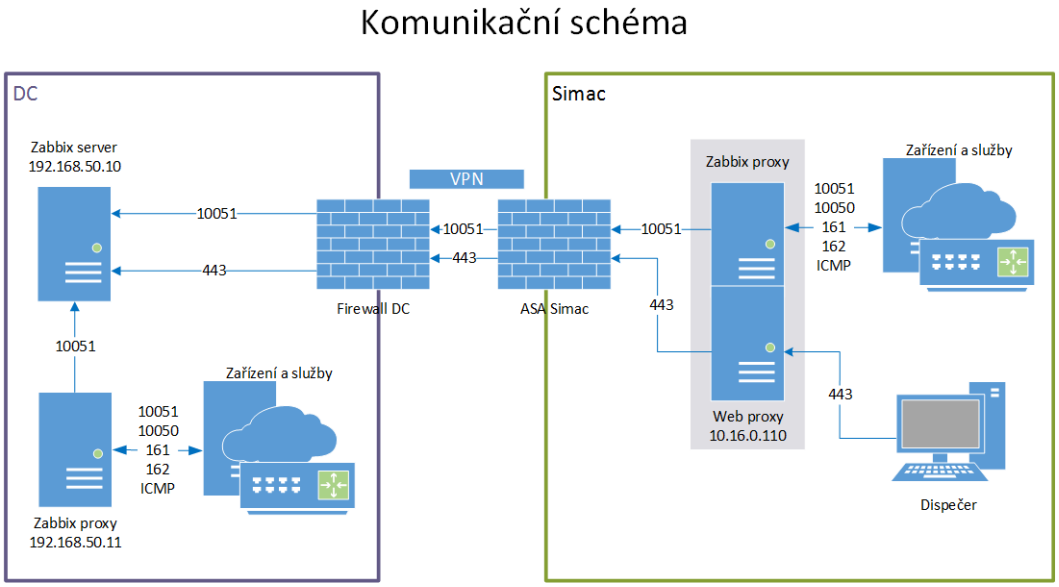
2.8 Plány do budoucna

2.8.1 LDAPS (Lightweight Directory Access Protocol Secure) a Webová proxy

V rámci zabezpečení je v plánu realizovat připojení do AD pomocí LDAPS. Zabezpečení je pomocí SSL certifikátu, který se musí vložit do složky s certifikáty v souborovém systému Zabbixu. LDAPS komunikuje na portu 636 na rozdíl klasického LDAP které komunikuje na portu 389

Dále se implenetuje webová proxy, která bude na stejném OS jako Zabbix proxy ve VISu. Díky tomu se technici a dispečeři nebudou muset, vždy připojovat na VPN do data centra. Jelikož je firewall v DC mnohem přísnější než ve VISu, tak nemohou vyřizovat emaily od zákazníků nebo firem, v případě řešení nějakého problému.

Jak je znázorněno na obrázku 2.31, dispečer bude přistupovat na webovou proxy, která je prostředníkem. Jakmile dispečer bude provádět jakékoliv změny, webová proxy bude posílat požadavky na hlavní Zabbix server skrz port 443, který je bude vykonávat.



Obr. 2.31: Komunikace mezi Zabbixem a hostem

2.8.2 Úprava zálohovacího skriptu

Momentálně se zálohují pouze důležité prvky v síti, co zajišťují komunikaci pro celou firmu. Do budoucna se vytvoří připojení do hlavní databáze, ze které si skript bude brát IP adresy prvků a zálohovat je do jednotlivých textových souborů podle nastaveného jména v konfiguraci.

Skript si z databáze zkontroluje, zdali host patří do skupiny Cisco, jakmile je host v této skupině, doplní si IP adresu a provede zálohu momentálně běžící konfigurace do textového souboru, který je uložen v souborovém systému Zabbixu. Jakmile bude vše fungovat, do skriptu se doprogramuje ukládání na FTP (File Transfer Protocol) server, aby byla konfigurace dohledatelná i na souborovém serveru.

2.8.3 Větši prevence a implementace dalších skriptů

Další monitorování odhalí více problémů a co jim předcházelo. Díky tomu se vytvoří další triggery, které budou dané parametry kontrolovat a upozorňovat na možnost vzniku problému. V případě projevení problému se nakonfiguruje skript, který bude opravovat problém, který se projevil.sa

Závěr

V rámci bakalářské práce byla nastudována literatura ohledně dohledových nástrojů, jako je důvod použití, které protokoly se dají použít pro kontrolu zařízení a služeb a sepsání informací o jednotlivých dohledových nástrojích. Proběhlo seznámení s použitým dohledovým nástrojem, tak aby se využily veškeré funkce při implementaci do sítě.

Po nastudování informací se začaly funkce implementovat do reálné sítě. Implementovalo se automatické vyhledávání s přiřazováním do jednotlivých skupin a přiřazení šablony, podle které se data budou kontrolovat. Následně se implementoval skript pro automatické nainstalování SNMP protokolu a povolily firewall pravidla pro SNMP protokol. Využily se další možnosti Zabbixu, jako propojení s AD a posílání problémů na sevice desk a SMS. Následně se vymyslely skripty pro usnadnění implementace a automatické opravy problémů. V poslední řadě je implementovaná prevence na upozornění opakujících se událostí a sepsány plány do budoucna.

Literatura

[1] MARDIYONO, Anggi, Walidatush SHOLIHAH a Faisal HAKIM. *Mobile-based Network Monitoring System Using Zabbix and Telegram. In:* 2020 3rd International Conference on Computer and Informatics Engineering (IC2IE) [online]. IEEE, 2020, 2020-9-15, s. 473-477 [cit. 2023-05-22]. ISBN 978-1-7281-8245-2. Dostupné z: doi:10.1109/IC2IE50715.2020.9274582

[2] FMS TEAM, Pandora. *Importance of having a good monitoring system.* PandoraFMS Monitoring blog [online]. Madrid: PandoraFMS, 2022, Nov 8 [cit. 2023-05-22]. Dostupné z: <https://pandorafms.com/blog/why-you-need-a-monitoring-system>

[3] *Types of Network Management Protocols* [online]. LiveAction, July 12, 2021 [cit. 2023-05-22]. Dostupné z URL: <https://www.liveaction.com/blog/types-of-network-monitoring-protocols>.

[4] Simple Network Management Protocol: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation. [cit. 2023-04-17]. Dostupné z URL: <https://en.wikipedia.org/wiki/Simple_Network_Management_Protocol>.

[5] Internet Control Message Protocol: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation. [cit. 2023-04-17]. Dostupné z URL: <https://learningnetwork.cisco.com/s/article/cisco-discovery-protocol-cdp-x>.

[6] *Cisco Discovery Protocol (CDP)* Cisco, 2020 [cit. 2023-04-17] [online] Dostupné z URL: <https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol>.

[7] *Link Layer Discovery Protocol (LLDP)* Cisco, 2020 [cit. 2023-04-17] [online] Dostupné z URL: <https://learningnetwork.cisco.com/s/article/link-layer-discovery-protocol-lldp-x>.

[8] *Nagios Core.* Nagios Docs [online]. Nagios, 2023, 25.05. [cit. 2023-05-25]. Dostupné z:<https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/4/en/toc.html>

[9] *Zabbix Manual.* Zabbix Documentation [online]. Zabbix, 2023, 25.05. [cit. 2023-05-25]. Dostupné z:<https://www.zabbix.com/documentation/6.2/en/manual>

[10] KEARY, TIM. *The Best Network Monitoring Tools & Software of 2023.* Comparitech [online]. Maidstone, 2023, May 10 [cit. 2023-05-22]. Dostupné z URL: <https://www.comparitech.com/net-admin/network-monitoring-tools>.

[11] *Documentation for SolarWinds Platform and Orion Platform: Install SolarWinds Platform products in a new environment* SolarWinds customer success [online]. California: SolarWinds, 2023, May 10 [cit. 2023-05-22]. Dostupné z: <https://documentation.solarwinds.com/en/success_center/orionplatform/content/install-new-deployment.htm>

[12] *Documentation for SolarWinds* SolarWinds customer success [online]. California: SolarWinds, 2023, May 10 [cit. 2023-05-22]. Dostupné z: <https://documentation.solarwinds.com>

[13] FMS TEAM, Pandora. *The 16 Best Network Monitoring Tools.* PandoraFMS Monitoring blog [online]. Madrid: PandoraFMS, 2022, Dec 22 [cit. 2023-05-22]. Dostupné z: <https://pandorafms.com/blog/network-monitoring-tools>

[14] QADAH, EHAB. *15 Best IT Infrastructure Monitoring Tools & Software [2023 Comparison].* Sematext [online]. 2023, January 6 [cit. 2023-05-25]. Dostupné z: <https://sematext.com/blog/infrastructure-monitoring-tools>

[15] SYSTEMS, Cisco. *Configure SNMP Community Strings.* Cisco [online]. Cisco Systems, 2022, June 7 [cit. 2023-05-22]. Dostupné z: <https://www.cisco.com/c/en/us/support/docs/ip/simple-network-management-protocol-snmp/7282-12.html>

[16] *How to Install SNMP and Configure the Community String For CentOS.* Managed [online]. 2016, Červenec 6 [cit. 2023-05-22]. Dostupné z: <https://support.managed.com/kb/a2390/how-to-install-snmp-and-configure-the-community-string-for-centos.aspx>

[17] *Install and Configure SNMP on RHEL/CentOS/Fedor.* Windows OS Hub [online]. 2021, May 14 [cit. 2023-05-22]. Dostupné z: <https://woshub.com/install-configure-snmp-linux>

[18] KARDASHEVSKY, Cyril. *HOW TO INSTALL AND CONFIGURE SNMP SERVICE ON WINDOWS 10/11?.* The IT Bros [online]. 2023, May 15 [cit. 2023-05-22]. Dostupné z: <https://theitbros.com/snmp-service-on-windows-10>

[19] RUPARELIA, ARJUN. *How to Install and Configure SNMP on Windows 10.* Make us of [online]. 2021, AUG 26 [cit. 2023-05-22]. Dostupné z: <https://www.makeuseof.com/install-and-configure-snmp-on-windows-10>

[20] PHILLIPS, Jamie. *Executing PowerShell from Python.* Philipsj [online]. 2020, 10. 25. [cit. 2023-05-22]. Dostupné z:<https://www.phillipsj.net/posts/executing-powershell-from-python>

[21] LAMBERT, Dmitry. *Zabbix Agent: Active vs. Passive.* Zabbix blog [online]. Zabbix, 2020 [cit. 2023-08-14]. Dostupné z: <https://blog.zabbix.com/zabbix-agent-active-vs-passive/9207/>

[22] *Python File Write* W3 Schools [online]. [cit. 2023-08-15]. Dostupné z: <https://www.w3schools.com/python/python_file_write.asp>

[23] *Network Automation Solution : How to save configuration file of Cisco Router/Switch devices using Python Script.* Cisco Community [online]. Cisco, 2019 [cit. 2023-08-15]. Dostupné z: <https://community.cisco.com/t5/networking-knowledge-base/network-automation-solution-how-to-save-configuration-file-of/ta-p/3952283>

Seznam symbolů a zkratek

SNMP	Simple Network Management Protocol
ICMP	Internet Control Message Protocol
CDP	Cisco Discovery Protokol
LLDP	Link Layer Discovery Protocol
OS	Operační systém
AD	Active Directory
SSH	Secure Shell
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IMAP	Internet Message Access Protocol
POP3	Post Office Protocol
CPU	Central processing unit
API	Application Programming Interface
SMS	Short message service
LDAP	Lightweight Directory Access Protocol
IT	Informační technologie
DNS	Domain Name System
OID	Object Identifier
UDP	User Datagram Protocol
TCP	Transmission Control Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
TTL	Time To Live
GHz	GigaHertz

GB	GigaByte
RAM	Random-access memory
JMX	Java Management Extensions
IPMI	Intelligent Platform Management Interface
MAC	Media Access Control
WMI	Windows Management Instrumentation
GSM	Global System for Mobile communication
VPN	Virtual Private Network
LTE	Long Term Evolution
FTP	File Transfer Protocol