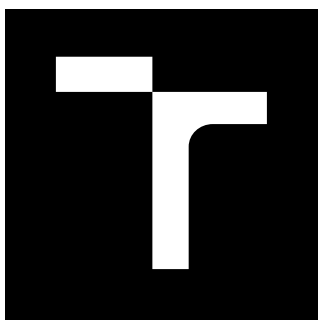


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky  
a komunikačních technologií

BAKALÁŘSKÁ PRÁCE



# 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

## DOHLED ZAŘÍZENÍ V POČÍTAČOVÝCH SÍTÍCH

DEVICES MONITORING IN COMPUTER NETWORKS

### BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

### AUTOR PRÁCE

AUTHOR

Matej Kutaj

### VEDOUCÍ PRÁCE

SUPERVISOR

doc. Ing. Vladislav Škorpil, CSc.

BRNO 2019



# Bakalářská práce

bakalářský studijní obor **Teleinformatika**  
Ústav telekomunikací

**Student:** Matej Kutaj

**ID:** 186127

**Ročník:** 3

**Akademický rok:** 2018/19

## NÁZEV TÉMATU:

### Dohled zařízení v počítačových sítích

#### POKYNY PRO VYPRACOVÁNÍ:

Analyzujte problematiku dohledu počítačových sítí a s tím spojených technologií. Seznamte se s dohledovým systémem Zabbix a krátce jej popište. Navrhněte a optimalizujte nasazení systému Zabbix prostřednictvím virtualizační technologie HyperV. Implementujte síťové prvky do dohledového systému Zabbix s využitím technologií a protokolů, které jste získal jako produkt analýzy problematiky. Zhodnoťte výsledky nasazení systému a zobecněte je.

#### DOPORUČENÁ LITERATURA:

- [1] SAVILL, J. Mastering Windows Server Hyper V. John Wiley, Indianapolis, NY 2016, ISBN 978-1-119-28618-9
- [2] RFC 1098. A Simple Network Management Protocol (SNMP). MIT Laboratory for Computer Science, Network Working Group, 1990

**Termín zadání:** 1.2.2019

**Termín odevzdání:** 27.5.2019

**Vedoucí práce:** doc. Ing. Vladislav Škorpil, CSc.

**Konzultant:** Ing. Igor Šimkovský (The Best Network Solution s.r.o.)

**prof. Ing. Jiří Mišurec, CSc.**  
*předseda oborové rady*

#### UPOZORNĚNÍ:

Autor bakalářské práce nesmí při vytváření bakalářské práce porušit autorská práva třetích osob, zejména nesmí zasahovat nedovoleným způsobem do cizích autorských práv osobnostních a musí si být plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č.40/2009 Sb.

## ABSTRAKT

Táto bakalárska práca sa venuje dohľadovaniu počítačových sietí a technológiám s nimi spojených. Bakalárska práca popisuje jednotlivé technológie, topológiu dohľadovanej siete, zoznam Vlan sietí, popis systému Zabbix, jeho implementáciu v Hyper-V a nastavenie jednotlivých sieťových adaptérov, popis vyriešenia chyby pomocou vytvorenia skriptu a následne vytváranie všetkých prvkov pomocou webového rozhrania. Vo výsledkoch sa vytvorili mapy jednotlivých sledovaných sietí a vytvorené grafy z prioritných prepínačov.

## K ÚVODNÉ SLOV

SNMP, OID, MIB, ICMP, WMI, Vlan, Monitorovací systém, Zabbix, Zabbix appliance, Hyper-V, DHCP

## ABSTRACT

This bachelor thesis deals with the supervision of computer networks and related technologies. The bachelor thesis describes individual technologies, topology of supervised network, list of Vlan networks, description of Zabbix system, its implementation in Hyper-V and setting of individual network adapters, description of error solving by creating script and then creating all elements using web interface. The results are created by maps of individual monitored networks and created graphs from priority switches.

## KEYWORDS

SNMP, OID, MIB, ICMP, WMI, Vlan, Monitoring system, Zabbix, Zabbix appliance, Hyper-V, DHCP

KUTAJ, Matej. Dohled za řízení v počítačových sítích. Brno, Rok, 70 s. Bakalárska práca. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedoucí práce: doc. Ing. Vladislav Škorpil, CSc.

## VYHL`SENIE

Vyhlasujem, že som svoju bakalársku prácu na tómu „Dohled za ízení v počítařových sítích“ vypracoval samostatne pod vedením vedeceho bakalárskej práce, využitím od nej literatúry a /alších informačných zdrojov, ktorú sú v tetky citovanú v práci a uvedené v zozname literatúry na konci práce.

Ako autor uvedenej bakalárskej práce /alej vyhlasujem, že v súvislosti s vytvorením tejto bakalárskej práce som neporušil autorskú právu tretích osôb, najmä som nezasiahol nedovoleným spôsobom do cudzích autorských práv osobnostných a /alebo majetkových a som si plne vedomý následkov porušení ustanovení nasledujúcich autorského zákona České republiky č. 121/2000 Sb., o práve autorskom, o právech súvisiacich s právom autorským a o zmene niektorých zákonov (autorský zákon), v znení neskorších predpisov, vrátane možných trestnoprávných dôsledkov vyplývajúcich z ustanovenia č. 42 druhého, hlavy VI. diel 4 Trestného zákóníka České republiky č. 40/2009 Sb.

Brno .....

.....

podpis autora

## POĀKOVANIE

RĀed by som tŷmto poĀkoval pĀEnovi Ing. Igorovi ŤmkovskØmu za odbornœe pomoc, konzultĀcie, podnetnØ nĀvrhy, cennØ rady a nakoniec za ve'a trpezlivosti pri vypracovanŷi mojej bakalĀrskej prĀce.

Brno .....

.....

podpis autora

# Obsah

1	Analýza problematiky monitorovania počítačových sietí	12
1.1	čo je to monitorovacia sieť a prečo sa používa	12
1.1.1	Monitorovanie podstaty	12
1.1.2	Interval monitorovania	12
1.1.3	Protokol a jeho typy	13
1.1.4	Proaktívne monitorovanie a prahy	13
1.1.5	Okamžité upozornenie na základe porušenia prahu	14
1.2	SNMP protokol	14
1.2.1	MIB databáza	15
1.3	ICMP protokol	16
1.4	Porovnanie SNMP protokolu a ICMP protokolu	18
1.4.1	Príklad sledovania SNMP protokolu v programe Wireshark	18
1.4.2	Príklad sledovania ICMP protokolu v programe Wireshark	18
1.5	WMI (Web-Based Enterprise Management)	19
1.5.1	Triedy WMI	19
1.5.2	Príklad s použitím WMI	20
1.6	Siete - Vlan	20
1.6.1	Izolované siete	21
1.6.2	Routované siete	21
1.7	Analýza klientov siete - kategorizácie	22
1.8	Základné požiadavky na monitorovacie systémy	22
2	Popis systému Zabbix	24
2.1	Zabbix	24
2.2	Instalácia	28
2.2.1	Instalácia Linuxu a databáze	28
2.2.2	Appliance a dostupné platformy	30
2.3	Zabbix agent	31
2.4	Pridanie agenta	33
2.5	Zabbix agent Windows	34
2.6	Prvky monitorovacieho systému Zabbix	35
3	Zabbix appliance v MS Hyper-V	37
3.1	Implementácia Zabbix v Hyper-V	37
3.2	Nastavenie jednotlivých sieťových rozhraní v MS Hyper-V	40
3.2.1	Pridanie sieťových adaptérov	40
3.2.2	Nastavenie jednotlivých sieťových adaptérov	42

3.2.3	DHCP nastavenie . . . . .	43
3.3	Výskyt chyby v Zabbix a jeho riešenie . . . . .	44
4	Implementácia sieťových prvkov do monitorovacieho systému Zabbix . . . . .	47
4.1	Vytvorenie nového sledovaného zariadenia . . . . .	47
4.2	Vytvorenie šablóny . . . . .	49
4.3	Vytvorenie aplikácie a položky . . . . .	49
4.3.1	Hodnota SNMP OID . . . . .	51
4.4	Vytvorenie grafu . . . . .	52
4.5	Vytvorenie mapy . . . . .	54
5	Získané výsledky monitorovacieho systému Zabbix . . . . .	56
5.1	Vytvorené Mapy . . . . .	56
5.1.1	Mapa HB Rebel . . . . .	56
5.1.2	Mapa prvkov vo výrobe . . . . .	57
5.1.3	Mapa kamier . . . . .	58
5.2	Graf . . . . .	59
5.2.1	Grafy z prepínača SW-STEXPEDICE . . . . .	59
6	Záver . . . . .	60
	Literatúra . . . . .	61
	Zoznam symbolov, veličín a skratiek . . . . .	63
	Zoznam príloh . . . . .	64
A	Tabuľky rezervácii na DHCP serveri . . . . .	65
A.1	Tabuľka rezervácii prepínačov . . . . .	65
A.2	Tabuľka rezervácií prvkou vo výrobe . . . . .	66
A.3	Tabuľka rezervácii kamier . . . . .	66
A.4	Tabuľka rezervácii tlačiarň . . . . .	67
A.5	Grafy . . . . .	68
A.5.1	Grafy z prepínača SW01 . . . . .	68
A.5.2	Grafy z prepínača SW02 . . . . .	69

# Zoznam obrázkov

1.1	Rozdelenie zariadení podľa priorít . . . . .	13
1.2	Príklad OID hodnoty . . . . .	15
1.3	Zapuzderenie a formát ICMP správy . . . . .	16
1.4	Správy get-request a get-response . . . . .	18
1.5	Správy echo request a echo reply . . . . .	18
1.6	Získanie a výpis informácií . . . . .	20
1.7	Rozdelenie vlan a ich priradenie na sw01 a sw02 . . . . .	21
2.1	Ukážka hlavnej stránky monitorovacieho systému Zabbix . . . . .	24
2.2	História alarmov s históriou tiketov . . . . .	25
2.3	Zoznam monitorovaných zariadení . . . . .	26
2.4	Zabbix inštalované CD / DVD zavádzacie menu . . . . .	30
2.5	Zavedenie Zabbix appliance . . . . .	31
2.6	Platformy Zabbix appliance . . . . .	31
2.7	Zavedenie Zabbix appliance . . . . .	32
2.8	Zabbix pustený v systéme Linux . . . . .	32
2.9	Zabbix pustený v systéme Windows . . . . .	33
3.1	Implementácia Zabbix appliance . . . . .	38
3.2	Hyper-V - špeciálne meno . . . . .	38
3.3	Hyper-V - generácia . . . . .	39
3.4	Hyper-V - využitie pamäte . . . . .	39
3.5	Hyper-V - pripojenie Zabbix appliance . . . . .	40
3.6	Pripojenie sieťového adaptéru . . . . .	41
3.7	Hyper-V nastavenie sieťového adaptéru . . . . .	42
3.8	Hyper-V nastavenie sieťového adaptéru . . . . .	43
3.9	Výpis z DHCP serveru . . . . .	44
3.10	Vytvorený skript na reštart sieťových kariet . . . . .	45
4.1	Vytvorenie nového monitorovacieho zariadenia . . . . .	47
4.2	Atribúty hostiteľa . . . . .	48
4.3	Nastavenie SNMP rozhrania . . . . .	49
4.4	Vytvorenie novej šablóny . . . . .	50
4.5	Vytvorenie novej položky . . . . .	51
4.6	OID hodnoty rozhraní . . . . .	52
4.7	OID hodnoty broadcastových hodnot paketov na daných rozhraniach . . . . .	52
4.8	Atribúty vytvárania grafu . . . . .	53
4.9	Náhľad vykresleného grafu . . . . .	53
4.10	Atribúty vytvorenej mapy . . . . .	54
4.11	Vytvorená mapa prvkom vo výrobe . . . . .	55

5.1	Mapa HB Rebel . . . . .	56
5.2	Mapa prvkov vo výrobe . . . . .	57
5.3	Mapa kamier . . . . .	58
5.4	Prepínač SW-STEXPEDICE - ICMP doba odozvy . . . . .	59
A.1	Prepínač SW01 - využitie pamäte . . . . .	68
A.2	Prepínač SW01 - sieťová premávka interface1 . . . . .	68
A.3	Prepínač SW01 - sieťová premávka interface5 (private) . . . . .	68
A.4	Prepínač SW01 - sieťová premávka interface12 (wi) . . . . .	69
A.5	Prepínač SW02 - využitie pamäte . . . . .	69
A.6	Prepínač SW02 - sieťová premávka Trunk1 . . . . .	69
A.7	Prepínač SW02 - sieťová premávka interface2 . . . . .	69
A.8	Prepínač SW02 - sieťová premávka interface12 (wi) . . . . .	70

# Zoznam tabuliek

1.1	Analýza klientov siete - kategorizace . . . . .	22
2.1	’peci kácie doporučeného výkonu serveru pre daný počet sledovaných staníc . . . . .	27
2.2	Výhody a nevýhody monitorovacieho systému Zabbix . . . . .	28
3.1	Virtuálne rozdelenie siete a ich parametre . . . . .	41
A.1	Tabu©ka rezervácii prepínačov . . . . .	65
A.2	Tabu©ka rezervácii prvkov vo výrobe . . . . .	66
A.3	Tabu©ka rezervácii kamier . . . . .	66
A.4	Tabu©ka rezervácii tlačiarní . . . . .	67

# Úvod

Na začiatku bakalárskej práce som sa zameril hlavne na teoretickú časť, v ktorej som analyzoval monitorovanie počítačovej siete a technológie, ktoré budem na monitorovanie siete využívať. Nasledovne som podrobne analyzoval sieť, ktorú chcem monitorovať a jednotlivé zariadenia som si kategorizoval do jednotlivých skupín, ktorým som určil metódy monitorovania.

V druhej časti som sa začal zaoberať monitorovacím systémom Zabbix, ktorý použijem na monitorovanie siete. Čez podrobné preštudovanie dokumentácie monitorovacieho systému Zabbix som sa dostal k jeho inštalácii/implementácii a následným možnostiam sledovania zariadení.

Po zoznámení sa s monitorovacím systémom Zabbix som sa dostal ku kapitole, ktorá najskôr popisuje jednotlivé kroky implementácie Zabbix appliance do virtualizačnej technológie MS Hyper-V a následne obsahuje postup nastavenia sieťových adaptérov, u ktorých som sa stretol s chybou pridelenia IP adres.

V poslednej kapitole som sa dostal k konfigurácii webového rozhrania monitorovacieho systému Zabbix, kde som vysvetlil jeho konfiguráciu a sledovanie jednotlivých sietí, ktoré chcem monitorovať. Získané výsledky zhodnotím a popíšem vo výsledku bakalárskej práce.

# 1 Analýza problematiky monitorovania počítačových sietí

## 1.1 Čo je to monitorovacia sieť a prečo sa používa

V dnešnom svete je pojem monitorovanie siete rozšírený v IT priemysle. Monitorovanie siete je kritický proces IT, kde sú všetky sieťové komponenty, ako sú smerovače, prepínače, brány, firewall, servery a virtuálne počítače, monitorované z hľadiska chýb a výkonu a priebežne hodnotené, aby sa zachovala a optimalizovala ich dostupnosť. Jedným z dôležitých aspektov monitorovania siete je, že by mal byť proaktívny. Hľadanie problémov s výkonom a úzkych miest aktívne pomáha pri identifikácii problémov v počiatočnej fáze. Efektívne, proaktívne monitorovanie môže zabrániť výpadkom siete alebo zlyhaniam.

Dôležité aspekty monitorovania siete:

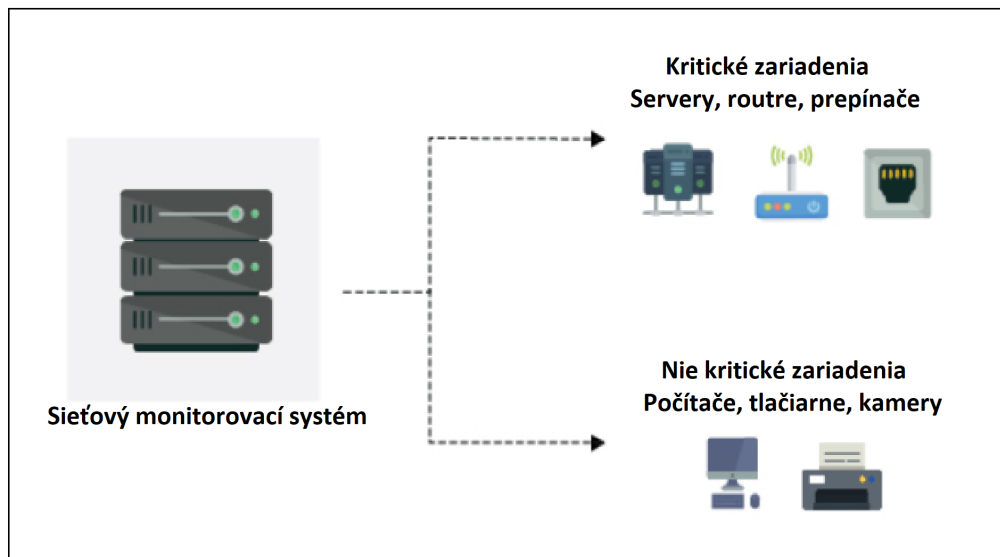
- Monitorovanie podstaty
- Optimalizácia intervalu monitorovania
- Výber správneho protokolu
- Nastavenie prahových hodnôt

### 1.1.1 Monitorovanie podstaty

Chybné sieťové zariadenia ovplyvňujú výkon siete. Toto je možné eliminovať včasnou detekciou, a preto je nevyhnutné nepretrité monitorovanie siete a súvisiacich zariadení. Pri efektívnom monitorovaní siete je prvým krokom identifikácia zariadení a súvisiacich meraní výkonu, ktoré sa majú monitorovať. Druhým krokom je určenie intervalu monitorovania. Zariadenia, ako sú stolové počítače a tlačiarne, nie sú kritické a nevyžadujú časté monitorovanie, zatiaľ čo servery, smerovače a prepínače vykonávajú obchodné kritické úlohy, ale zároveň majú kľúčové parametre, ktoré možno selektívne monitorovať.

### 1.1.2 Interval monitorovania

Interval monitorovania určuje frekvenciu, v akej sú sieťové zariadenia a súvisiace metriky vyzvané na identifikáciu stavu výkonu a dostupnosti. Nastavenie intervalov monitorovania môže pomôcť odstrániť zaťaženie zo systému monitorovania siete a následne aj vaše zdroje. Interval závisí od typu sledovaného sieťového zariadenia alebo parametra. Stav dostupnosti zariadení musí byť sledovaný najmenej v intervale času, výhodne každú minútu. Štatistiky CPU a pamäte je možné monitorovať raz za každých 5 minút. Interval monitorovania pre iné metriky, ako je napríklad Využitie



Obr. 1.1: Rozdelenie zariadení podľa priorit

disku, môže byť rozšírený a postačuje, ak je raz za 15 minút vyzvaný. Monitorovanie každého zariadenia v najmenšom intervale len pridá zbytočné zaťaženie do siete a nie je celkom potrebné.

### 1.1.3 Protokol a jeho typy

Pri monitorovaní siete a jej zariadení je bežným dobrým postupom prijatie bezpečného a neproporcionálneho protokolu sieťového riadenia, ktorý minimalizuje vplyv na výkon siete. Väčšina sieťových zariadení a serverov Linux podporuje protokol SNMP (Simple Network Management Protocol) a protokoly CLI a zariadenia so systémom Windows podporujú protokol WMI. SNMP je jedným zo široko akceptovaných protokolov na správu a monitorovanie sieťových prvkov. Väčšina sieťových prvkov je dodávaná s agentom SNMP. Musia byť povolené a nakonfigurované na komunikáciu so systémom riadenia siete. Povolenie prístupu SNMP na čítanie a zápis poskytuje úplnú kontrolu nad zariadením. Pomocou SNMP je možné nahradiť celú konfiguráciu zariadenia. Systém monitorovania siete pomáha správcovi preziať sieť prostredníctvom nastavenia privilégií čítania a zápisu SNMP a obmedzením kontroly pre ostatných používateľov.

### 1.1.4 Proaktívne monitorovanie a prahy

Sieťové prestojky môžu stať veľkou peňazí. Vo väčšine prípadov koncový užívateľ ohlásí sieťový problém tímu správy siete. Dôvodom je zlý prístup k proaktívnemu monitorovaniu siete. Kľúčovou výzvou pri monitorovaní siete v reálnom čase je proaktívne

identi ková výkonnostné prekážky. Práve tu hrajú hlavnú úlohu pri monitorovaní siete prahy. Prahové limity sa lížia od zariadenia k zariadeniu na základe prípadu použitia.

### 1.1.5 Okamžitá upozornenie na základe porušení prahu

Konfigurácia prahov pomáha proaktívne monitorovať zdroje a služby bežiacie na serveroch a sieťových zariadeniach. Každé zariadenie môže mať nastavený interval alebo prahovú hodnotu na základe preferencií a potrieb používateľa. Viacúrovňový prah môže pomôcť pri klasifikácii a rozbití akejkoľvek zistenej chyby. Využitím prahových hodnôt môžu byť upozornenia vyvolané aj pred tým, ako zariadenie klesne alebo dosiahne kritický stav.[2]

## 1.2 SNMP protokol

SNMP protokol je základný sieťový protokol určený pre správu a monitorovanie sietí. Umožňuje sledovanie siete a zber dát o jej stave. Bežne tento protokol beží na porte 161. Protokol SNMP je dostupný v troch verziách. Prvá verzia je určená k základnému zberu dát, druhá verzia je obohatená o autentizáciu a tretia verzia podporuje šifrovanie komunikácie.

Z pohľadu monitorovania, zariadenia využívajúcich protokol SNMP sa delí na dva druhy. Prvý druh poskytuje informácie a nazýva sa Agent. Druhým je server, ktorý informácie zbiera.

MIB tabuľka obsahuje data v stromovej štruktúre. Obsahuje objekty typu root, subtree a leaf. Je rozdelená do logických skupín. Prvá skupina, je určená pre autoritu ISO, druhá ccitt, spravovaná organizáciou ITU-T (bývalá CCITT) a posledná joint-iso-ccitt, ktorá je spoločne spravovaná organizáciou ISO a ITU-T[3].

Celá MIB tabuľka je logicky členená a rozdelená do sekcií. V každej sekcii sa nachádzajú položky rôznych typov. Jedná sa o nasledujúce typy:

Integer - jednoduché celé číslo, väčšinou o veľkosti 32 bit

Counter - nezáporný celočíselný typ, stále rastie, pri dosiahnutí hodnoty  $2^{32}-1$ , začína znova od nuly

Gauge - nezáporný celočíselný typ, rovnaký ako counter, ale môže z neho aj odpôliť

TimeTicks - nezáporný celočíselný typ, reprezentuje v stotínach sekundy čas od určitej chvíle (napríklad spustenie systému)

IpAddress - 32bit IP adresy

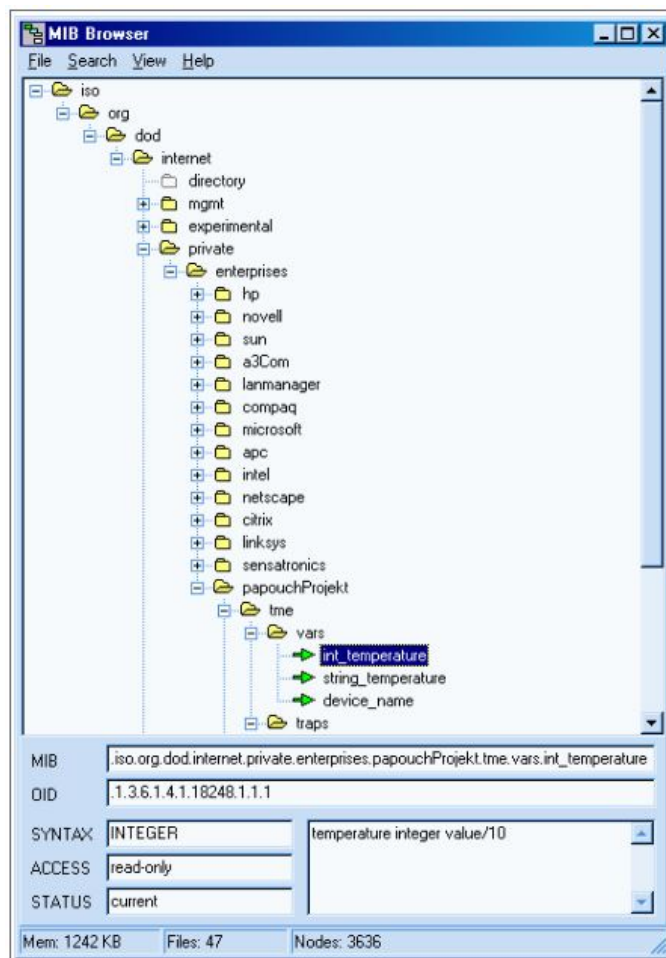
OCTET STRING - vyjadrenie ľubovlnného reťazcu znakov alebo ľubovlnných binárných dát

OBJECT IDENTIFIER - reprezentácia mena uzlu

### 1.2.1 MIB databáza

Každá hodnota v protokole SNMP je jednoznačne identifikovaná pomocou ľíselného identifikátoru OID. OID je tvorený postupnosťou ľísel oddeľovaných bodkou, táto hodnota vznikne tak, keď sa vezme OID nadradeného prvku a doplní sa bodka a aktuálne ľíslo. Celá táto stromová štruktúra je uložená v MIB databáze. Navyše MIB databáza obsahuje mená a popisy jednotlivých hodnôt (OID)[2].

Príklad OID môže byť napríklad hodnota 1.3.6.1.4.1.18248.1.1.1 alebo textová forma iso.org.dod.internet.private.enterprises.papouchProjekt.tme.vars.int . Tento príklad môžeme názorne vidieť na Obr. 1.2 - Príklad OID hodnoty.



Obr. 1.2: Príklad OID hodnoty

## 1.3 ICMP protokol

Zakladný protokol sieťovej vrstvy architektúry TCP/IP, protokol IP, poskytuje službu nespojovanú. Znamená to, že nevytvára spätnú väzbu medzi koncovými uzlami a tak nie je zajištená možnosť vyslať správu zdrojovému systému, že behom prenosu datagramu došlo k neštandardnej situácii. Túto spätnú väzbu vytvára ďalší protokol sieťovej vrstvy, protokol ICMP.

ICMP je služobný protokol, ktorý je považovaný za súčasť protokolu IP a tak povinne implementovaný na každom systéme s architektúrou TCP/IP. Entity protokolu ICMP vytvárajú správy, ktoré sú vkladané do IP datagramu. Za záhlavím IP datagramu nasleduje záhlavie ICMP správy, pričom v záhlaví IP datagramu v poli "PROTOCOL" je nastavená hodnota "1".

ICMP správy sú generované na všetkých uzloch, ktoré vytvárajú prenosovú cestu datagramu, behom tohto prenosu došlo k neštandardnej situácii. Sú to nasledujúce uzly:

- Smerovače, ktorými datagram prechádza

- Cieľový systém (počítač), ktorému je datagram určený.

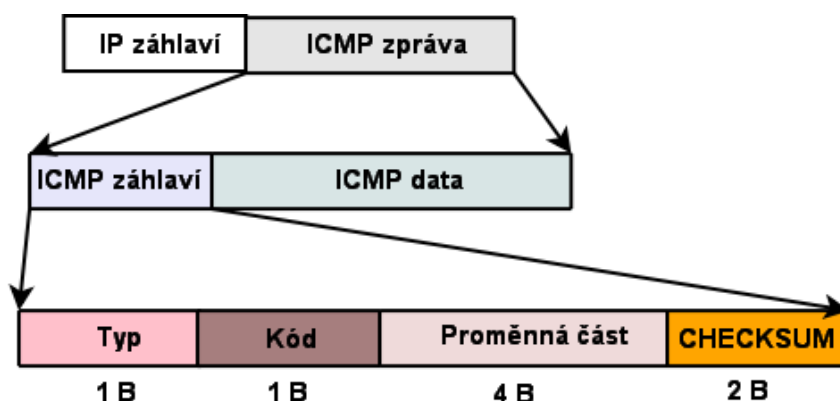
ICMP správy nie sú generované v prípade že:

- IP datagram, v ktorom došlo k neštandardnej situácii, prenáša inú ICMP správu

- Cieľová adresa inkriminovaného datagramu je typ IP broadcast alebo IP multicast

- Inkriminovaný datagram obsahuje iný fragment ako prvý

- IP adresa odosielateľa datagramu je 0.0.0.0, 127.0.0.1, IP broadcast alebo IP multicast. Tieto datagramy sú striktne diskartované.



Obr. 1.3: Zapuzderenie a formát ICMP správy

Správa ICMP obsahuje ICMP záhlavie a dátovú časť, do ktorej vloží ICMP entita dáta, ktoré je potreba predať systému, ktorý odoslal inkriminovaný datagram. Princíp zapúzdrenia ICMP správy do IP datagramu a základný formát ICMP správy je znázornený na Obr. 1.3 - Zapuzdrenie a formát ICMP správy.

ICMP správy sú správy:

Chybové.

Informatívne.

Diagnostické.

Sú označené špeciálnym kódom uloženým v poli Typ záhlaví ICMP správy. V nasledujúcom rozdelení uvedieme obvyklé typy ICMP správ a ich charakteristiku:

Typ správy 8 - Echo request : je diagnostická správa. Jedná sa o vyslanie požiadavku, aby oslovený uzol odpovedal ICMP správou Echo reply, čím sa overí dostupnosť dotazovaného uzlu v IP sieti. Do premennej časti záhlaví sa vloží identifikátor a poradové číslo požiadavku, do dátovej časti @ubovolné dáta. Obsah oboch častí bude skopírovaný do odpovede.

Typ správy 0 - Echo reply : je odpoveď na správu Echo request. Overuje dosiahnulosť uzlu na Ip sieti.

Typ správy 11 - Time Exceeded : je chybová správa o nedoručení datagramu. V záhlaví je uvedený kód 0 alebo 1. Premenná časť záhlaví nie je použitá, je naplnená nulami. Do dátovej časti je vložené záhlavie inkriminovaného IP datagramu a ďalších 8 B jeho obsahu.

Typ správy 3 - Destination Unreachable : je chybová správa o nedoručení datagramu. V záhlaví sú uvedené kódy 0 - 15. Premenná časť záhlaví nie je použitá, je naplnená nulami. Do dátovej časti je vložené záhlavie inkriminovaného IP datagramu a ďalších 8 B jeho obsahu.

Typ správy 5 - Redirect Error : je informatívna správa o chybe v smerovacej tabuľke odosielateľa inkriminovaného datagramu. Datagram je doručený, korektnú prenosovú zabezpečuje smerovač, ktorý ICMP správu vyslal. V záhlaví sú uvedené kódy 0 - 3. Do premennej časti záhlaví je vložená IP adresa smerovača, kam by inkriminovaný datagram preposlal. Do dátovej časti je vložené záhlavie inkriminovaného IP datagramu a ďalších 8 B jeho obsahu.

Typ správy 13 - Time Stamp Request : je diagnostická správa, prostredníctvom ktorej si vysielací uzol vypočíta RTT na komunikáciu s osloveným uzlom. V premennej časti záhlaví je identifikátor správy a jeho poradové číslo. V dátovej časti je vložený časový údaj o odoslaní správy.

Typ správy 14 - Time Stamp Reply : je odpoveď na ICMP Time Stamp Request. V premennej časti záhlaví je identifikátor prijatej správy a jeho poradové číslo. Do dátovej časti sa ďalej skopíruje čas odoslania požiadavky.

davku a pripojí sa čas prijatia požiadavky a čas odoslania odpovede. Po prijatí odpovedi môže uzol, ktorý poslal požiadavku, vypočítať hodnotu RTT[4].

## 1.4 Porovnanie SNMP protokolu a ICMP protokolu

### 1.4.1 Príklad sledovania SNMP protokolu v programe Wireshark

SNMP protokol pracuje na odosielaní paketu s názvom set-request. Potom čaká na odpoveď s názvom get-response. Akonáhle bude prijatý paket get-response, čas sa vypočíta medzi get-request a get-response, aby sa vygeneroval a vypočítal "Response Time" z uzla. Tieto správy môžeme vidieť na Obr. 1.4 - Správy get-request a get-response.

Time & Date	Time	Source	Destination	Protocol	Length	Info
2015-12-24 08:47:04.151516000	20.0001350	192.168.1.161	192.168.1.80	SNMP	83	get-request 1.3.6.1.2.1.1.2.0
2015-12-24 08:47:04.157132000	20.0057510	192.168.1.80	192.168.1.161	SNMP	92	get-response 1.3.6.1.2.1.1.2.0
2015-12-24 08:47:14.152540000	30.0011590	192.168.1.161	192.168.1.80	SNMP	83	get-request 1.3.6.1.2.1.1.2.0
2015-12-24 08:47:14.158196000	30.0068150	192.168.1.80	192.168.1.161	SNMP	92	get-response 1.3.6.1.2.1.1.2.0
2015-12-24 08:47:24.171199000	40.0198180	192.168.1.161	192.168.1.80	SNMP	83	get-request 1.3.6.1.2.1.1.2.0
2015-12-24 08:47:24.176855000	40.0254740	192.168.1.80	192.168.1.161	SNMP	92	get-response 1.3.6.1.2.1.1.2.0
2015-12-24 08:47:34.154729000	50.0033480	192.168.1.161	192.168.1.80	SNMP	83	get-request 1.3.6.1.2.1.1.2.0
2015-12-24 08:47:34.160580000	50.0091990	192.168.1.80	192.168.1.161	SNMP	92	get-response 1.3.6.1.2.1.1.2.0
2015-12-24 08:47:44.156084000	60.0047030	192.168.1.161	192.168.1.80	SNMP	83	get-request 1.3.6.1.2.1.1.2.0
2015-12-24 08:47:44.164050000	60.0126690	192.168.1.80	192.168.1.161	SNMP	92	get-response 1.3.6.1.2.1.1.2.0
2015-12-24 08:47:54.157057000	70.0056760	192.168.1.161	192.168.1.80	SNMP	83	get-request 1.3.6.1.2.1.1.2.0
2015-12-24 08:47:54.162688000	70.0113070	192.168.1.80	192.168.1.161	SNMP	92	get-response 1.3.6.1.2.1.1.2.0
2015-12-24 08:48:04.156459000	80.0050780	192.168.1.161	192.168.1.80	SNMP	83	get-request 1.3.6.1.2.1.1.2.0
2015-12-24 08:48:04.162091000	80.0107100	192.168.1.80	192.168.1.161	SNMP	92	get-response 1.3.6.1.2.1.1.2.0

Obr. 1.4: Správy get-request a get-response

### 1.4.2 Príklad sledovania ICMP protokolu v programe Wireshark

Príkladom je nástroj ping, ktorý používa ICMP protokol. Posiela správu Echo request a očakáva správu Echo reply aby zistil či je cieľové zariadenie dosiahnuteľné a zároveň vypočítal ako dlho trvá paketom, než sa dostanú k cieľu a späť. Správy protokolu môžeme vidieť na Obr. 1.5 : Správy echo request a echo reply[5].

Time & Date	Time	Source	Destination	Protocol	Length	Info
2015-12-24 09:06:39.831562000	229.481325000	192.168.1.161	192.168.1.80	ICMP	65	Echo (ping) request id=0x0011, seq=600/22530, ttl=128 (reply in 647)
2015-12-24 09:06:39.832759000	229.482522000	192.168.1.80	192.168.1.161	ICMP	65	Echo (ping) reply id=0x0011, seq=600/22530, ttl=255 (request in 647)

```

Frame 647: 65 bytes on wire (520 bits), 65 bytes captured (520 bits) on interface 0
Ethernet II, Src: vmware_0:40:46:fa (00:50:56:a9:46:fa), Dst: CiscoInc_12:fb:80 (00:02:b9:12:fb:80)
Internet Protocol Version 4, Src: 192.168.1.161 (192.168.1.161), Dst: 192.168.1.80 (192.168.1.80)
Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0x495a [correct]
  Identifier (BE): 17 (0x0011)
  Identifier (LE): 4352 (0x1100)
  Sequence number (BE): 600 (0x0258)
  Sequence number (LE): 22530 (0x5902)
  Response frame: 6481
Data (23 bytes)
  Data: 536f6c617257696e647320537461747573205175657279
  Length: 23
  
```

Obr. 1.5: Správy echo request a echo reply

## 1.5 WMI (Web-Based Enterprise Management)

Windows Management Instrumentation (WMI) je súbor 2peci kácií spoločnosti Microsoft na konsolidáciu správy zariadení a aplikácií v sieti z počítačových systémov Windows. Služba WMI poskytuje používateľom informácie o stave lokálnych alebo vzdialených počítačových systémov. Podporuje aj také akcie, ako je konfigurácia nastavení zabezpečenia, nastavenie a zmena vlastností systému, nastavenie a zmena oprávnení pre oprávnených používateľov a skupiny používateľov, priradenie a zmena meníčov jednotiek, procesy plánovania, ktoré sa majú spúšťať v určitých časoch, zálohovanie archívu objektov a zapnutie alebo vypnutie protokolovania chýb.

„ažšia generácia WMI sa nazýva Windows Management Infrastructure (MI). Rozhranie API pre programovanie aplikácií (MI) obsahuje rozhrania, enumerácie, štruktúry a odbory, ktoré vývojári potrebujú na vytvorenie natívnych poskytovateľov a klientov WMI. Podľa spoločnosti Microsoft je MI plne kompatibilný s predchádzajúcimi verziami WMI, čo znamená, že ak sú noví poskytovatelia napísaní pomocou rámca MI, môžu byť prístupné pomocou skriptov a aplikácií WMI.

Historicky, WMI bola implementácia Microsoft Web Based Enterprise Management (WBEM), ktorá je postavená na spoločnom informačnom modeli (CIM), štandarde počítačového priemyslu na definovanie charakteristík zariadení a aplikácií tak, aby správcovia systémov a riadiace programy mohli ovládať zariadenia a aplikácie viacerých výrobcov alebo zdrojov rovnakým spôsobom.

### 1.5.1 Triedy WMI

V nasledujúcej sekcii si rozoberieme 2peci kčné WMI triedy so stručným popisom:

- Win32 Classes : Hlavné triedy pre prácu s operačným systémom Windows.
- WMI Registry Classes : Triedy určené na manipuláciu s registrami.
- WMI System Classes : Triedy poskytujúce základnú funkčnosť WMI.
- IPMI Classes : Triedy, ktoré dodávajú dáta z IPMI (Intelligent Platform Management Interface) poskytovateľa, keď je prístupný vhodný BMC (Baseboard Management Controller) hardware.
- Monitor Display Classes : Triedy poskytujúce dáta o zobrazovacej jednotke.
- MSFT Classes : Iné triedy poskytujúce prostriedky a manipuláciu s osobitnými vlastnosťami operačného systému. Obsahujú WMI Troubleshooting Classes.
- CIM Classes : Triedy určené na vývoj vlastných WMI tried.

Standard Consumer Classes : Sada WMI udalostí určená na spúšťanie akcii s podmienkou prijatia @ubovo@nej udalosti.

MSMCA Classes : Triedy poskytujúce prostriedky na manipuláciu a zobrazenie systémových udalostí.

WMI C++ Classes : Kompletný výpis WMI C++ tried.

Po vybratí nejakej možnosti zo sekcie tried (napr. Win32 Classes) sa zobrazí uožia možnosti výberu so zameraním na určitú oblasť. Po ďalšom výbere (napr. Computer system hardware) obsahuje dokumentácia konkrétne triedy, ktoré poskytujú informácie o požadovanej veci (napr. Win32DiskDrive)[6].

## 1.5.2 Príklad s použitím WMI

V nasledujúcom Obr. 1.6: Získanie a výpis informácií bude použitá WMI trieda Win32DiskDrive na získanie a výpis informácií o názve, výrobcovi, modeli, veľkosti v bytoch, typu rozhrania a počtu partícií pevných diskov na počítači (výpis je smerovaný do tabučky)[7].

```
private ManagementClass manClass;
private ManagementObjectCollection manObjectCollection;

private void GetDiscsInfo() {
    listViewDiscs.Items.Clear();

    // nastavenie typu WMI ManagementClass
    manClass = new ManagementClass("Win32_DiskDrive");
    // vloženie instancií do kolekcie
    manObjectCollection = manClass.GetInstances();

    // výpis vybraných informácií o disku do ListView
    foreach(ManagementObject disc in manObjectCollection) {
        ListViewItem item = new ListViewItem(disc.GetPropertyValue("Name").ToString());

        item.SubItems.Add(disc.GetPropertyValue("Manufacturer").ToString());
        item.SubItems.Add(disc.GetPropertyValue("Model").ToString());
        item.SubItems.Add(String.Format("{0:n0} B", Convert.ToInt64(disc.GetPropertyValue("Size").ToString())));
        item.SubItems.Add(disc.GetPropertyValue("InterfaceType").ToString());
        item.SubItems.Add(disc.GetPropertyValue("Partitions").ToString());

        listViewDiscs.Items.AddRange(new ListViewItem[] {item});
    }
}
```

Obr. 1.6: Získanie a výpis informácií

## 1.6 Sieťe - Vlan

Virtuálne lokálne siete (VLAN) oddeľujú existujúce fyzické siete do viacerých logických sietí. Každá VLAN teda vytvára svoju vlastnú vysielačiu doménu. Komunikácia medzi dvoma sieťami VLAN sa môže uskutočniť iba prostredníctvom smerovača, ktorý je pripojený k obojím sieťam. VLAN fungujú tak, ako keby boli vytvorené pomocou nezávislých prepínačov[8].

Implementácia VLAN sietí umožňuje väčšiu flexibilitu pre podporu remných cieľov. Medzi hlavné výhody VLAN sietí patria:

- bezpečnosť skupiny, ktoré pracujú s dôvernými dátami sú oddelené od zvyšku siete
- zníženie nákladov redukovaním broadcast domén nie sú potrebné časté vypĺnenia zariadení
- vyšší výkon siete a aplikácií
- minimalizácia zahltenia siete broadcast rámcami segmentáciou LAN sa redukuje počet zariadení, ktoré sa môžu podieľať na zahltení
- zlepšenie výkonu IT personálu

V našom prípade máme sieť rozdelenú do viacerých virtuálnych sietí. Tieto siete sú vytvorené na základe rozdelenia rôznych zariadení podľa ich používania. Jednotlivé rozdelenie vlan a ich priradenie na určité porty si môžeme pozrieť na Obr. 1.7: Rozdelenie vlan a ich priradenie na sw01 a sw02.

SW01												Vlans		Rozsah IP	
1	3	5	7	9	11	13	15	17	19	21	23	Vlan1 - private	192.168.1.0/24		
2	4	6	8	10	12	14	16	18	20	22	24	Vlan100 - internet	10.0.0.0/24		
												Vlan3 - Production	192.168.3.0/24		
												Vlan4 - Wifi_private	192.168.4.0/24		
												Vlan5 - Cameras	192.168.5.0/24		
												Tagged a trunk	propoj switchú a serverú		

Obr. 1.7: Rozdelenie vlan a ich priradenie na sw01 a sw02

### 1.6.1 Izolovaná sieť

špecializovaný typ VLAN je súkromný (izolovaný) VLAN. Keď je takto nastavená množina VLAN, zariadenia z portov v sieti VLAN nemôžu navzájom komunikovať. V situáciách, ako je externá smerujúca bezpečnostná zóna, často chceme, aby servery komunikovali s používateľmi z iných sietí VLAN, ale bezpečnosť je posilnená tým, čo bráni tomu, aby servery navzájom nadväzovali reláciu[9].

### 1.6.2 Routovaná sieť

V prostredí LAN VLAN sa rozdeľujú vysielačie domény. Ak hostiteľ v jednej sieti VLAN musí komunikovať s hostiteľom v inej sieti VLAN, prevádzka musí byť smerovaná medzi nimi. Tento typ smerovania sa nazýva inter-VLAN smerovanie. Na inteligentnom prepínači môžete nastaviť smerovanie medzi VLAN vytvorením rozhrania vrstvy 3, t.j. virtuálneho rozhrania prepínača (SVI)[10].

## 1.7 Analýza klientov siete - kategorizácie

V sieti, ktorú chceme monitorovať sa nachádzajú rôzne druhy zariadení. Na tieto rôzne zariadenia neplatia vždy rovnaké princípy monitorovania. Preto si zariadenia v našej sieti rozdelíme na konkrétne kategórie, ku ktorým priradíme na ňu zvolenú metódu monitorovania:

Tab. 1.1: Analýza klientov siete - kategorizácie

Kategorie zariadení	Metóda monitorovania
Hardverové stanice - Windows 10	WMI
Windows server	RDPcheck
Prepínače	SNMP
Tlačiarne	ICMP
PLC vo výrobe	ICMP
Kamery	ICMP

## 1.8 Základné požiadavky na monitorovacie systémy

Pre výber monitorovacieho systému bolo stanovených niekoľko základných požiadavkov, ktoré budú ďalej popísané.

Úlohou monitorovacích systémov je neustále dohľad nad stavom daných prvkov, ktoré sa nám nachádzajú v sieti. Na tento stav by mal monitorovací systém primerane reagovať s výpisom chybovej hlásky na riadiacom paneli a doručením upozornenia administrátorovi cez email alebo SMS.

Hlavným požiadavkom bola podpora protokolu pre správu siete SNMP (Simple Network Management Protocol), ICMP alebo WMI. Je nevyhnutné aby bol systém schopný spracovať výstup daného protokolu a zobrazí ho v prijateľnej podobe pracovníkovi, ktorý vykonáva monitorovaciu činnosť nad sieťov.

Ako ďalší požiadavok je nárok kladený na schopnosť systému rozlíziť dôležitosť daného problému. Tieto kategórie dôležitosti by mali byť rozdelené podľa závažnosti problému a jasne poukazovať na skutočný stav systému.

Monitorovací systém musí byť dostupný pre viacerých ľudí, ktorí chcú daný systém sledovať. Tým pádom vzniká potreba existencie používateľských rolí, ktoré deňujú zobrazený obsah webového prostredia, ktorý bude používateľovi dostupný. Je teda nevyhnutné aby monitorovací systém bol schopný používateľov rozdeliť na administrátorov, bežných používateľov, dohľadových pracovníkov a iné. Ako výhodu môžeme brať možnosť vytvárania vlastných používateľských rolí. Nasledovne vzniká ale ďalšia potreba, ktorá poukazuje na podporu skupin sledovaných systémov. Je nevyhnutné, aby systém umožňoval zobrazenie prvkou, iba de novej skupine používateľov. To znamená, že používateľom nemusia byť dostupné všetky prvky systému.

Ako ďalší bol stanovený požiadavok pre možnosť pridávanie a odoberanie sledovaných prvkov za behu systému, za pomoci webového prostredia. S týmto požiadavkom sa spája aj nevyhnutná funkcia, ktorú by mal vybraný monitorovací systém mať. Jedná sa o delenie sledovaných prvkov do skupín. Tieto skupiny by mali byť schopné akceptovať rôzne zariadenia (smerovače, prepínače, serverové stanice, modemy, kamery atď.).

Posledným požiadavkom je otvorenosť kódu a voľne šíriteľná licencia celého monitorovacieho systému. Riešenie nesmie byť uzavreté a nutnosťou je upraviteľnosť systému bez porušenia licenčných podmienok poskytovateľa

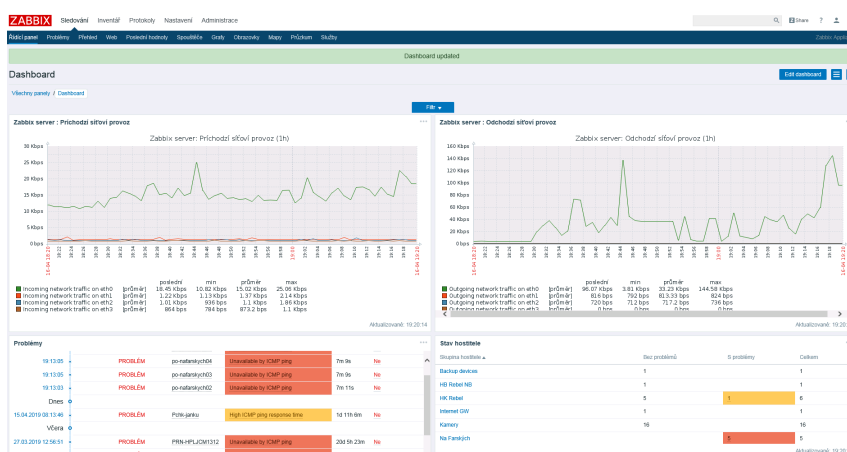
## 2 Popis systému Zabbix

### 2.1 Zabbix

Vlastnosti monitorovacieho systému a podrobný popis

Monitorovací systém Zabbix disponuje veľkou používateľskou upraviteľnosťou. Je vybavený vlastným agentom na strane monitorovaného hosta. Tento agent nie je nutnosťou, je však výhodou. Poskytuje možnosť jednoduchej vzdialenej správy sledovaného systému. Pokiaľ je zvolená verzia monitorovania nad stanicou bez Agentu je možnosť využitia protokolu SNMP a ICMP. Tieto protokoly sú implementované automaticky a nie je potreba dodatočná inštalácia.

Hlavná stránka webového rozhrania je variabilná a je možné ju meniť ťahaním kurzorov s daným prvkom. Celkovo je možné na hlavnej stránke vytvoriť tri štvorcové boxy s informáciami. V prípade Obr. 2.1: Ukážka hlavnej stránky monitorovacieho systému Zabbix sa nám na prvých miestach nachádzajú grafy s prichádzajúcou a odchádzajúcou sieťovou premávkou. V grafoch sa nachádzajú jednotlivé sieťové rozhrania, ktoré sú vyobrazené v závislosti zaťaženia v čase. Ako môžeme vidieť pod grafmi sa nachádza aj tabuľka s aktuálnymi problémami, v ktorej sú vypísané jednotlivé zariadenia s problémom. Problémy sú zobrazené v dvoch farbách. červená farba značí katastrofu a oranžová farba značí vysoký stupeň. Tieto jednotlivé zariadenia s problémom sú ešte priradené do jednotlivých skupín kvôli jednoduchosti rozoznania. Problémy tu majú v základnej konfigurácii šesť stupňov. Ide o: katastrofu, vysoký stupeň, priemerný, varovací, informovací a posledný stupeň je neklasifikovaný. Veľkou výhodou tohto monitorovacieho systému je možnosť upraviteľnosti týchto stupňov. Každý stupeň je možné premenovať a deňovať jeho úroveň vzniku.



Obr. 2.1: Ukážka hlavnej stránky monitorovacieho systému Zabbix

Tiketovací systém v monitorovacím systéme Zabbix funguje na princípe automatického vytvorenia tiketu pri vzniku problému. Pomocou tiketu je možné problémy komentovať a je možné vidieť históriu komentárov v rámci daného problému. Na spätné dohadanie rovnakého problému funguje náhľadové okno, ktoré sa vyvolá pri nabenutí kurzorovou myšou na zobrazený čas problému. Históriu alarmov môžeme vidieť na Obr. 2.2: História alarmov s históriou tiketov. V okne s históriou môžeme vidieť čas zaznamenaného problému a jeho celkovú dobu trvania. V poslednom stĺpci sa nachádza tiket, ktorý k tomuto problému vznikol.

Seznam událostí [posledních 20]						
Čas	Doba obnovy	Stav	Stáří	Trvání	Potvrzeno	Akce
10.05.2019 15:43:02		PROBLÉM	6h 45m 23s	6h 45m 23s	Ne	
13.04.2019 17:38:02	15.04.2019 10:24:02	OPRAVENO	27d 4h 54m	1d 16h 46m	Ano 1	
15.03.2019 17:44:02	15.03.2019 17:50:01	OPRAVENO	1m 26d 3h	5m 59s	Ano 1	
12.03.2019 15:15:02	12.03.2019 15:17:01	OPRAVENO	1m 29d 6h	1m 59s	Ano 1	
12.03.2019 13:35:02	12.03.2019 13:38:01	OPRAVENO	1m 29d 7h	2m 59s	Ano 1	
09.03.2019 23:50:01	09.03.2019 23:51:01	OPRAVENO	2m 1d 21h	1m	Ano 1	
24.02.2019 17:04:03	01.03.2019 11:40:02	OPRAVENO	2m 15d 4h	4d 18h 35m	Ano 1	
14.02.2019 11:22:02	14.02.2019 11:25:02	OPRAVENO	2m 25d 10h	3m	Ano 1	
13.02.2019 13:19:02	14.02.2019 09:23:01	OPRAVENO	2m 26d 8h	20h 3m 59s	Ano 1	
12.02.2019 14:01:01	12.02.2019 14:02:01	OPRAVENO	2m 27d 7h	1m	Ano 1	
30.01.2019 21:18:02	05.02.2019 14:16:01	OPRAVENO	3m 10d	5d 16h 57m	Ano 1	
11.01.2019 10:14:02	11.01.2019 10:15:02	OPRAVENO	3m 29d 11h	1m	Ano 1	
03.01.2019 12:18:01	03.01.2019 14:04:02	OPRAVENO	4m 7d 9h	1h 46m 1s	Ano 1	
14.12.2018 13:53:01	14.12.2018 13:54:01	OPRAVENO	4m 27d 7h	1m	Ano 1	
13.12.2018 02:10:02	13.12.2018 02:12:01	OPRAVENO	4m 28d 19h	1m 59s	Ano 1	

Obr. 2.2: História alarmov s históriou tiketov

Systém Zabbix má pridávanie nových zariadení pomocou administrácie webového rozhrania. Ako hlavné je opäť pomenovanie zariadenia. „alej je možné pridať meno, ktoré bude v systéme viditeľné. Pokiaľ toto meno nieje vyplnené, bude použité originálne meno. Nasleduje pridanie hosta do skupiny. Je možné priamo vytvoriť novú skupinu. Ako ďalšie sú definované IP adresy s portami daných služieb. Je možné pridať IP adresu pre Zabbix Agent, SNMP protokol, JMS rozhranie a IPMI rozhranie. U každého je možné definovať novú rozdielnu adresu a port. Posledné položky, ktoré je možné vyplniť sú: popis prvku a pokud je to nutné, tak i proxy server, ktorý je pred hostom.

„ďalší dôležitý krok pri pridávaní nového zariadenia, sú šablóny, ktoré definujú monitorované hodnoty. Môžeme napríklad monitorovať pomocou protokolu SNMP

iba sieťové rozhrania alebo napríklad zaťaženie procesorovej jednotky. „alšie nastavenie závisí na zvolenom protokole. Môžeme využiť zifrovaného spojenia medzi monitorovacím serverom a hostom.

V administrácii sa nachádza zoznam, ktorý obsahuje všetky monitorované zariadenia (viz Obr. 2.3: Zoznam monitorovaných zariadení). Z tohto zoznamu je možné vyčítať nasledujúce informácie:

Jméno	Aplikace	Polohy	Spouštěče	Graty	Průzkum	Web	Rozhraní	Šablony	Stav	Dostupnost	Agent Sítování	Info
alfa	Aplikace	Polohy	Spouštěče	Graty	Průzkum	Web	192.168.1.2:3369	RDP_Testing	Povoleno	SNMP [OK] [PM]	ZAKAZANO	
beta	Aplikace	Polohy	Spouštěče	Graty	Průzkum	Web	192.168.1.6:3369	RDP_Testing	Povoleno	SNMP [OK] [PM]	ZAKAZANO	
cam-boeni-95d	Aplikace	Polohy	Spouštěče	Graty	Průzkum	Web	192.168.5.74:10050	Template Module ICMP Ping	Povoleno	SNMP [OK] [PM]	ZAKAZANO	
cam-laborator01	Aplikace	Polohy	Spouštěče	Graty	Průzkum	Web	192.168.5.53:10050	Template Module ICMP Ping	Povoleno	SNMP [OK] [PM]	ZAKAZANO	
cam-prod-ekst4	Aplikace	Polohy	Spouštěče	Graty	Průzkum	Web	192.168.5.59:10050	Template Module ICMP Ping	Povoleno	SNMP [OK] [PM]	ZAKAZANO	
cam-prod-vchod	Aplikace	Polohy	Spouštěče	Graty	Průzkum	Web	192.168.5.67:10050	Template Module ICMP Ping	Povoleno	SNMP [OK] [PM]	ZAKAZANO	
cam-prodejna	Aplikace	Polohy	Spouštěče	Graty	Průzkum	Web	192.168.5.60:10050	Template Module ICMP Ping	Povoleno	SNMP [OK] [PM]	ZAKAZANO	
cam-serverovna01	Aplikace	Polohy	Spouštěče	Graty	Průzkum	Web	192.168.5.51:10050	Template Module ICMP Ping	Povoleno	SNMP [OK] [PM]	ZAKAZANO	
cam-sklap	Aplikace	Polohy	Spouštěče	Graty	Průzkum	Web	192.168.5.68:10050	Template Module ICMP Ping	Povoleno	SNMP [OK] [PM]	ZAKAZANO	
cam-sladorna01	Aplikace	Polohy	Spouštěče	Graty	Průzkum	Web	192.168.5.54:10050	Template Module ICMP Ping	Povoleno	SNMP [OK] [PM]	ZAKAZANO	
cam-spikla01	Aplikace	Polohy	Spouštěče	Graty	Průzkum	Web	192.168.5.58:10050	Template Module ICMP Ping	Povoleno	SNMP [OK] [PM]	ZAKAZANO	

Obr. 2.3: Zoznam monitorovaných zariadení

Názov zariadenia

Počet monitorovaných služieb (aplikácie, webové stránky, apod.)

IP adresu zariadení

Používané monitorovacie šablóny

Stav monitorovania (povolené/zakázané)

Stav monitorovaných agentov (Zabbix Agent, SNMP, JMX, IPMI), kde zelená predstavuje bežiacieho agenta a červená agenta nedostupného

Zvolené zifrovanie

Vďaka veľkým možnostiam používateľa prispôsobenia celého systému, je možné v celom systéme upraviť mnoho prvkov. Celý systém sa vyznačuje vysokou prehľadnosťou. Podporuje vytváranie používateľských rolí, ktorým je možné priradiť viditeľnosť rôznych skupín monitorovaných zariadení. Týmto používateľským rolím môžeme tiež znepřístupniť rôzne časti systému (administráciu, rôzne časti stránok, apod.).

Oproti ostatným testovaným systémom ponúka monitorovací systém Zabbix tiež veľa funkcionalít. Jedná sa napríklad o automatické skenovanie adresového rozsahu v sieti a získavanie dostupných služieb na objavenom zariadení. Užitočnou funkciou je napríklad vytváranie vlastných obrazoviek, kde je možné zobrazovať rôzne prvky z celého systému[11].

Celý systém Zabbix je licencovaný pod licenciou GPL (General Public License verzie 2).

## Architektúra

Celá výkonná časť monitorovacieho systému Zabbix je naprogramovaná v jazyku C. Webové rozhranie je vytvorené pomocou programovacieho jazyka PHP, HTML, CSS a JavaScript. Webové rozhranie monitorovacieho systému nemá priamo definovaný typ webového serveru, ktorý je nutné použiť, je teda na používateľovi, do ktorého riešenia monitorovacieho systému implementuje. Ako východzí webový server Apache. Pre ukladanie systému Zabbix môže využívať jednu z databází MySQL, PostgreSQL, SQLite, Oracle alebo IBM DB2. Samotné využitie typu databáze vychádza z predpokladaného počtu sledovaných zariadení, viz časť Hardvérové nároky.

## Hardvérové nároky

Ako jediný monitorovací systém má na svojich stránkach priamo špecifikované doporučený výkon hosťujúcej stanice. (Doporučené hardvérové nároky sú uvedené v Tab. 2.1: špecifikácie doporučeného výkonu serveru pre daný počet sledovaných staníc)[12].

Tab. 2.1: špecifikácie doporučeného výkonu serveru pre daný počet sledovaných staníc

Rozdelenie systému	Doporučená platforma	CPU/Pamäť RAM	Databáza	Počet sledovaných hostov
Malý	CentOS	Možná virtualizace	MySQL InnoDB	100
Stredný	CentOS	2 CPU jadrá / 2GB	MySQL InnoDB	500
Veľký	RedHat Enterprise Linux	4 CPU jadrá / 8 GB	RAID10 MySQL InnoDB or PostgreSQL	>1000
Extra veľký	RedHat Enterprise Linux	8 CPU jadier / 16 GB RedHat Enterprise Linux	Rýchly RAID10 MySQL InnoDB or PostgreSQL RedHat Enterprise Linux	>10000

## Výhody a nevýhody monitorovacieho systému Zabbix

Nasledujúca sekcia popisuje výhody a nevýhody testovaného riešenia Zabbix. Výhody a nevýhody sú popísané v Tab. 2.2: Výhody a nevýhody monitorovacieho systému Zabbix.

Tab. 2.2: Výhody a nevýhody monitorovacieho systému Zabbix

Výhody	Nevýhody
Veľké množstvo úprav	Je treba vyživiť výkon hosťujúcej stanice
Vzdialená správa pomocou agenta	Systém je náročný na zápisy do databázy
Moderný dizajn webového prostredia	Zložité pridávanie nových zariadení/šablón

## 2.2 Inštalácia

### 2.2.1 Inštalácia Linuxu a databázy

1. Nainštalovať Debian
2. Inštalácia Zabbix

(a) Inštalácia pomocou balíčkou:

```
# wget http://repo.zabbix.com/zabbix/3.4/debian/pool/main/z/zabbix-release/zabbix-release_3.4-1+stretch_all.deb
# dpkg -i zabbix-release_3.4-1+stretch_all.deb
# apt-get update
```

(b) Inštalácia systému Zabbix a databázy MariaDB:

```
# apt-get install zabbix-server-mysql zabbix-frontend-php
```

(c) Nastavenie databázy:

```
shell> mysql -uroot -p<password>
mysql> create database zabbix character set utf8 collate utf8_bin;
mysql> grant all privileges on zabbix.* to zabbix@localhost identified by '<password>';
mysql> quit;
```

(d) Naplnenie databáze tabuľkovou štruktúrou pro systém zabbix:

```
# zcat /usr/share/doc/zabbix-server-mysql/create.sql.gz | mysql -uzabbix -p zabbix
```

(e) Nastavenie Zabbix serveru pre lokálnu databázu:

```
# nano /etc/zabbix/zabbix_server.conf  
  
DBHost=localhost  
DBName=zabbix  
DBUser=zabbix  
DBPassword=<heslo>
```

(f) Spustenie démona Zabbix-server a jeho povolenie spustenia pri štarte:

```
# service zabbix-server start  
# update-rc.d zabbix-server enable
```

(g) Nastavenie Apache serveru:

```
# nano /etc/apache2/conf-enabled/zabbix.conf  
  
php_value max_execution_time 300  
php_value memory_limit 128M  
php_value post_max_size 16M  
php_value upload_max_filesize 2M  
php_value max_input_time 300  
php_value always_populate_raw_post_data -1  
php_value date.timezone Europe/Prague
```

(h) Ak je potrebné doinštalujú sa potrebné balíčky pre PHP:

```
# apt-get install php7.0-xml php7.0-mbstring php7.0-bcmath
```

(i) Restart serveru Apache2:

```
# service apache2 restart
```

(j) Nastavenie Zabbix-serveru v prehliadači.

Na adrese <http://<adresa Zabbix-serveru>/zabbix> sa nachádza sprievodca Zabbix-serveru

Sprievodca skontroluje nastavenie webového serveru a databáze (pokiaľ je všetko v stave OK, je možné pokračovať v inštalácii)

V ďalšom kroku je potrebné nastaviť údaje k pripojeniu databáze

Nasleduje nastavenie samotného Zabbix serveru

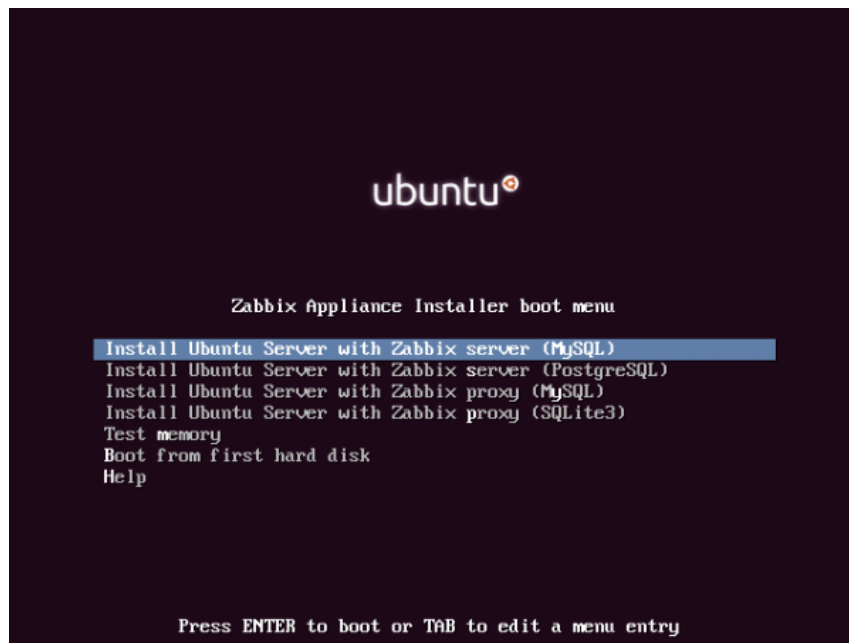
(k) Prihlásenie do Zabbix-serveru:

```
Jméno: Admin  
Heslo: zabbix
```

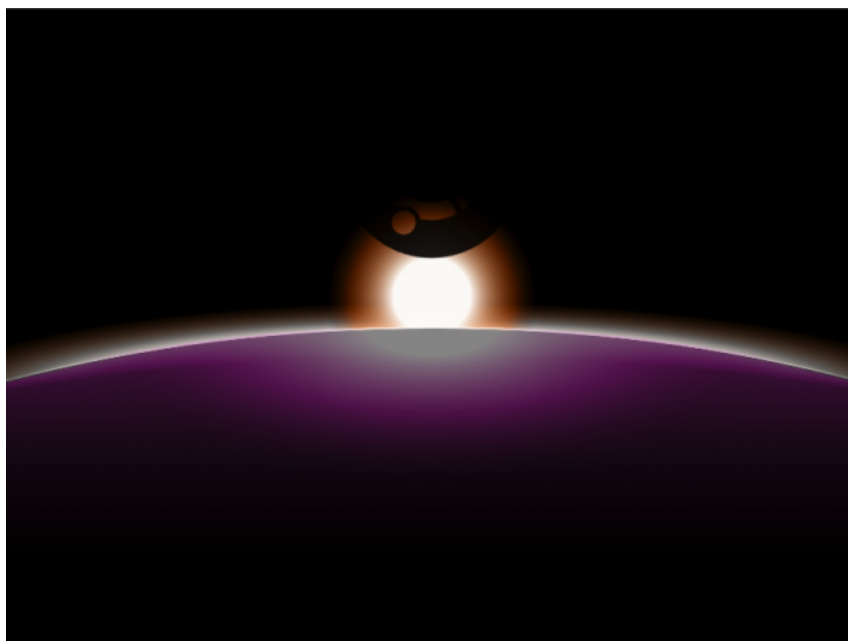
## 2.2.2 Apliance a dostupnØ platformy

Ako alternatívu k manuálnemu nastaveniu alebo opätovnému pouítiu existujúceho servera pre Zabbix môu pouívatelia prevziať zariadenie Zabbix alebo inštalačný disk CD zariadenia Zabbix. Inštalačné CD zariadenia Zabbix by mohlo byť použité na okamité nasadenie servera Zabbix (MySQL), servera Zabbix (PostgreSQL), proxy Zabbix (MySQL) a proxy Zabbix (SQLite 3)[14].

Virtuálne stroje Zabbix Appliance pripravili server Zabbix s podporou MySQL. Je vytvorený pomocou inštalačného CD zariadenia Zabbix[13].



Obr. 2.4: Zabbix inštalačné CD / DVD zavádzacie menu



Obr. 2.5: Zavedenie Zabbix appliance

Dostupné platformy Zabbix appliance:

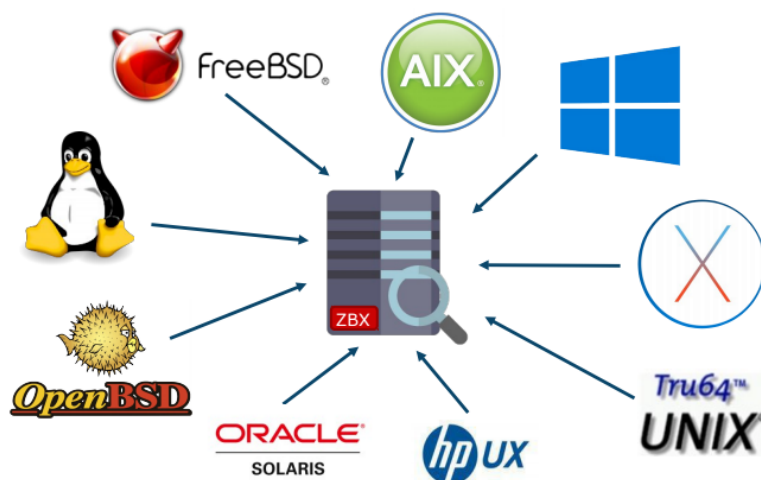
Zabbix 4.2			Zabbix 4.0 LTS	Zabbix 3.0 LTS	Zabbix 2.2 LTS	
Version	Release	Date	Platform	Release Notes	Zabbix Manual	Download
Zabbix 4.2	4.2.1	Apr 17, 2019	Installation CD/DVD (.iso)	<a href="#">Download</a>	<a href="#">Download</a>	<a href="#">Download</a>
Zabbix 4.2	4.2.1	Apr 2, 2019	VirtualBox, VMWare (.vmdk)	<a href="#">Download</a>	<a href="#">Download</a>	<a href="#">Download</a>
Zabbix 4.2	4.2.1	Apr 2, 2019	Microsoft Hyper-V 2012	<a href="#">Download</a>	<a href="#">Download</a>	<a href="#">Download</a>
Zabbix 4.2	4.2.1	Apr 2, 2019	Microsoft Hyper-V 2008	<a href="#">Download</a>	<a href="#">Download</a>	<a href="#">Download</a>
Zabbix 4.2	4.2.1	Apr 2, 2019	KVM, Parallels, QEMU, USB stick, VirtualBox, Xen (.raw)	<a href="#">Download</a>	<a href="#">Download</a>	<a href="#">Download</a>
Zabbix 4.2	4.2.1	Apr 2, 2019	KVM, QEMU (.qcow2)	<a href="#">Download</a>	<a href="#">Download</a>	<a href="#">Download</a>
Zabbix 4.2	4.2.1	Apr 2, 2019	Live CD/DVD (.iso)	<a href="#">Download</a>	<a href="#">Download</a>	<a href="#">Download</a>
Zabbix 4.2	4.2.1	Apr 2, 2019	Open virtualization format (.ovf)	<a href="#">Download</a>	<a href="#">Download</a>	<a href="#">Download</a>

Obr. 2.6: Platformy Zabbix appliance

## 2.3 Zabbix agent

Pôvodný agent Zabbix, vyvinutý v jazyku C, môže bežať na rôznych podporovaných platformách, vrátane systémov Linux, UNIX a Windows, a zhromažďovať údaje, ako napríklad použitie procesora, pamäte, disku a sieťového rozhrania zo zariadenia[15].

## AGENT AVAILABILITY



Obr. 2.7: Zavedenie Zabbix appliance

Malé rozmery a nízke zdroje

Vzhľadom na svoju malú plochu je možné agenta spúšťať na zariadeniach s obmedzenými zdrojmi.

Konfigurácie monitorovania sú centralizované v serveri Zabbix, čo uľahčuje správu agenta Zabbix, ktorý môže používať jeden konfiguračný súbor na všetkých serveroch.

Zástupca Zabbix spustený v systéme Linux:

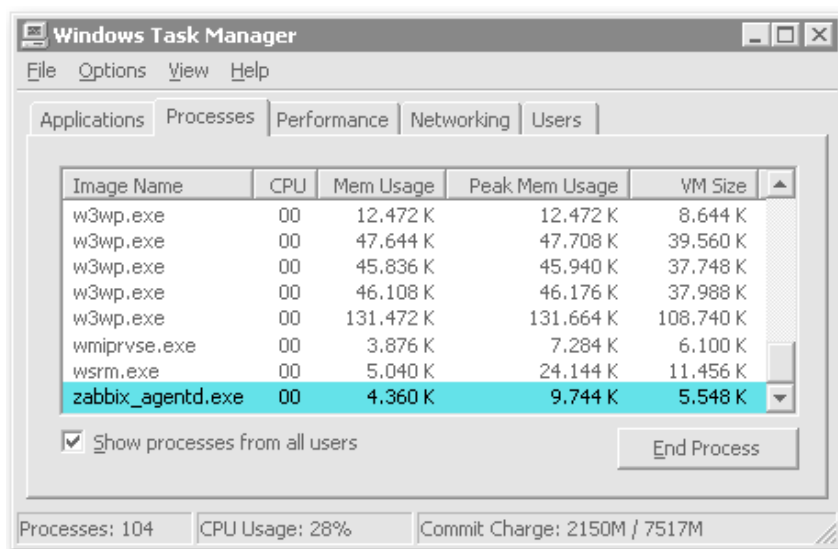
```
# ps u -C zabbix_agentd
USER      PID %CPU %MEM    VSZ   RSS  STAT  TIME  COMMAND
zabbix   15778  0.0  0.0  48212  460   SN    0:00  /usr/sbin/zabbix_agentd
zabbix   15780  0.0  0.0  48212  748   SN    9:27  /usr/sbin/zabbix_agentd
zabbix   15781  0.0  0.0  48212  424   SN    0:00  /usr/sbin/zabbix_agentd
zabbix   15782  0.0  0.0  48212  424   SN    0:00  /usr/sbin/zabbix_agentd
zabbix   15783  0.0  0.0  48212  424   SN    0:00  /usr/sbin/zabbix_agentd
zabbix   15784  0.0  0.0  48220  612   SN    0:17  /usr/sbin/zabbix_agentd
```

Obr. 2.8: Zabbix pustený v systéme Linux

Agent Zabbix spustený pod operačným systémom MS Windows:

Podpora hlasovania a odchyty

Agenti Zabbix podporujú pasívne (polling) aj aktívne kontroly (trapping). Zabbix môže vykonávať kontroly na základe intervalu, je však tiež možné naplánovať konkrétne úlohy na dotazovanie položiek.



Obr. 2.9: Zabbix pustený v systéme Windows

Pasívne kontroly (hlasovanie):

Server Zabbix (alebo proxy) po<sup>o</sup>aduje hodnotu od agenta Zabbix

Agent spracuje po<sup>o</sup>iadavku a vráti hodnotu serveru Zabbix (alebo proxy)

Aktívne kontroly (odchyt):

Agent agenta Zabbix po<sup>o</sup>aduje od servera Zabbix (alebo proxy) zoznam aktívnych kontrol

Agent posiela výsledky pravidelne

## 2.4 Pridanie agenta

1. V menu Nastavenie, v záložke Hostitelia sa po kliknutí na tlačidlo vytvorí hosta zobrazí formulár s potrebnými údajmi k vyplneniu.
2. Do príslušného po<sup>o</sup>a po<sup>o</sup>adovanej, monitorovanej slu<sup>o</sup>by sa vyplní adresa monitorovaného agenta.
3. V záložke <sup>z</sup>ablóny sa vyberie príslušná <sup>z</sup>ablóna pre monitorovanie agenta.
4. Indikácia správneho nastavenia hostite<sup>o</sup>a je zelená ikona monitorovanej slu<sup>o</sup>by v st<sup>o</sup>pci dostupnos<sup>o</sup>, ktorý sa nachádza v hlavnej tabulke monitorovaných hostite<sup>o</sup>ov.
5. Pri pridávaní monitorovaných hostov pomocou protokolu SNMP je treba vyplniť v makrách SNMP skupinu, do ktorej hostia spadajú. Prípadnú skupinu je možné nastaviť v menu Administracie - Obecné - Makrá. Tu sa upraví, prípadne vytvorí makro s názvom:

```
{SNMP_COMMUNITY}
```

## 2.5 Zabbix agent Windows

Môžete spustiť jednu inštanciu agenta Zabbix alebo viacero inštancií agenta na hostiteľovi systému Microsoft Windows. Jedna inštancia môže použiť predvolený konfiguračný súbor `C:\zabbixagentd.conf` alebo konfiguračný súbor zadáný v príkazovom riadku. V prípade viacerých inštancií musí mať každá inštancia agenta svoj vlastný konfiguračný súbor (jedna z inštancií môže použiť predvolený konfiguračný súbor).

Príklad konfiguračného súboru je dostupný v zdrojovom archíve Zabbix ako `conf/zabbixagentd.win.conf`.

Inštalácia agenta ako služby Windows  
Ak chcete nainštalovať jednu inštanciu agenta Zabbix s predvoleným konfiguračným súborom `c:\zabbix-agentd.conf`:

```
zabbix_agentd.exe --install
```

Ak chcete použiť iný konfiguračný súbor ako `c:\zabbix-agentd.conf`, mali by ste pre inštaláciu služby použiť nasledujúci príkaz:

```
zabbix_agentd.exe --config <your_configuration_file> --install
```

Mala by sa zadať úplná cesta k konfiguračnému súboru. Viaceré inštalácie agenta Zabbix možno nainštalovať ako služby ako je táto:

```
zabbix_agentd.exe --config <configuration_file_for_instance_1> --install --multiple-agents  
zabbix_agentd.exe --config <configuration_file_for_instance_2> --install --multiple-agents  
...  
zabbix_agentd.exe --config <configuration_file_for_instance_N> --install --multiple-agents
```

Inštalovaná služba by mala byť teraz viditeľná v ovládacom paneli [16]. Spustenie agenta

Ak chcete spustiť službu agenta, môžete použiť ovládací panel alebo to urobiť z príkazového riadka.

```
zabbix_agentd.exe --start
```

Ak chcete spustiť jednu inštanciu agenta Zabbix s predvoleným konfiguračným súborom:

Spustenie jednej inštancie agenta Zabbix s iným konfiguračným súborom:

```
zabbix_agentd.exe --config <your_configuration_file> --start
```

Spustenie jedného z viacerých inštancií agenta Zabbix:

```
zabbix_agentd.exe --config <configuration_file_for_this_instance> --start --multiple-agents
```

## 2.6 Prvky monitorovacieho systému Zabbix

Po úspešnom nastavení Zabbix serveru sa nám zobrazí úvodne prihlasovacie webové rozhranie, kde už je prednastavený používateľ pod prihlasovacím menom `Admin` a prihlasovacím heslom `zabbix`. Po úspešnom prihlásení sa dostaneme na úvodnú stránku, ktorú máme zobrazenú na Obr. 2.1: Ukážka hlavnej stránky monitorovacieho systému Zabbix[17].

Pre lepšie orientovanie v nasledujúcich stránkach, ktoré budú nasledovať, si rozoberieme niektoré výrazy ktoré sa budú v texte nachádzať:

**Host** (Host) - Zariadenie alebo systém, pridaný v systéme s vlastným názvom, priradenou IP adresou a začlenený do určitej skupiny zariadení. Jedná sa teda o sieťový prvok, ktorý chceme priamo monitorovať.

**Skupina hostov** (Host group) - Skupina zariadení, ktorých rozdelenie záleží na daných prvkoch, ktoré chceme ako skupine monitorovať.

**Prvok** (Item) - Určuje daný prvok, ktorý chceme monitorovať na koncovom zariadení alebo v systéme. Za Item môžeme považovať napríklad ICMP ping.

**Spúšťač** (Trigger) - V základnom menu Zabbix serveru sa pomocou triggerov zobrazujú rôzne upozornenia o nastávajúcej chybe alebo prekročení nastavených medzí.

**Šablóna** (Template) - V template sa nastavuje vzetok monitoring daného hostu. Je to daná šablóna v ktorej vieme nastaviť rôzne itemy, triggery a ich rôzne závislosti na seba. Práve v šablóna template po pridaní vzetkých parametrov dokáže vytvoriť prehľadný graf.

Severita - Práve Severita vyhodnocuje daný problém prednastaveného triggeru. Problémy lze nastaviť podľa úrovni od Not classified do Disaster.

Najnovšie údaje (Latest data) - Zobrazovať poslednej získanej hodnoty daného itemu a ich históriu.

## 3 Zabbix appliance v MS Hyper-V

Virtualizačná platforma Microsoftu pokrýva široké spektrum potrieb, od najjednoduchších scenárov konsolidácie niekoľkých servertov až po vysoko výkonné, škálovateľné a samoobslužné dátové centrá o stovkách a tisícoch servertov.

### Charakteristika Hyper-V

Základným stavebným kameňom je virtualizačná vrstva či hypervisor Hyper-V, ktorý v svojej prvej verzii uzrel svetlo sveta v roku 2008 ako súčasť niektorých edícií Windows Serveru 2008. Nasledovala druhá generácia, dostupná ako rola vo Windows Server 2008 R2, prípadne ako samostatný produkt Microsoft Hyper-V Server 2008 R2, ktorý je k dispozícii zdarma. Funkcionalitu doplnily technológie Dynamic Memory a RemoteFX, obsadené v Service Packu 1 pre Windows Server 2008 R2. Nasledovala tretia generácia Hyper-V, ktorá je integrovanou súčasťou Windows Serveru 2012 a klientskeho operačného systému Windows 8 Pro. Aktuálne je k dispozícii Hyper-V integrovaná súčasť Windows Serveru 2012 R2 a Windows 8.1 Pro a Enterprise[18].

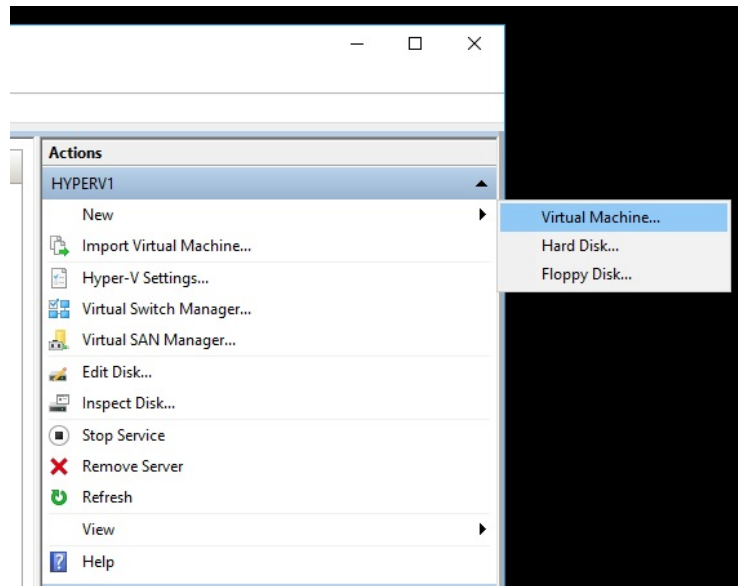
V rámci Hyper-V sú podporované nasledujúce operačné systémy:

- Windows Server od verzie 2003 vyššie
- Windows Client od verzie XP Professional SP2 vyššie
- SUSE Linux Enterprise Server verzie 10 a 11
- Oracle Linux 6.4 a vyššie
- Open SUSE 12.3
- Red Hat Enterprise Linux verzie 5.5 a vyššie
- CentOS Linux 5.5 a vyššie
- Ubuntu 12.04 a vyššie
- FreeBSD 8.2
- Debian 7.0 a vyššie

### 3.1 Implementácia Zabbix v Hyper-V

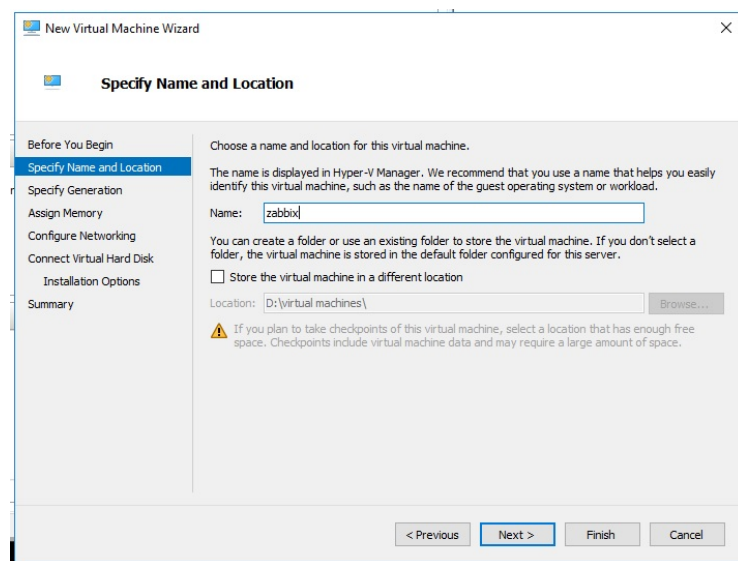
V tejto kapitole si popíšeme jednotlivé kroky implementácie Zabbix appliance vo virtualizačnom nástroji Hyper-V. V prvom kroku je podstatné si stiahnuť správnu Zabbix appliance na domovských stránkach Zabbix (Viz. Obr. 2.6: Platformy Zabbix appliance). Z ponuknutého menu si jednoduchým spôsobom stiahneme správnu Zabbix appliance pre náš Hyper-V.

Následne v menu virtualizačného nástroji Hyper-V zvolíme položku `New` a v rozboľovacom menu `Virtual Machine` .



Obr. 3.1: Implementácia Zabbix appliance

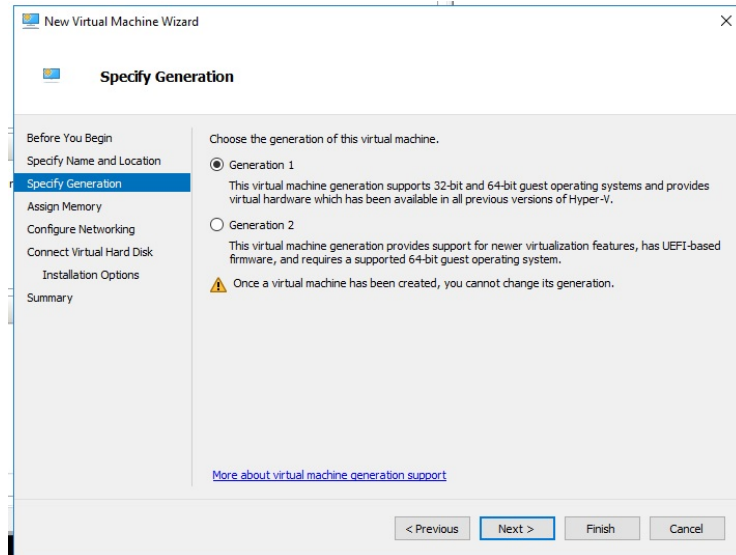
Po tomto kroku sa nám zobrazí implementačné menu, ktoré je rozložené do jednotlivých sekcií. V prvej sekcii sme vyplnili špeciálne meno novo-vytvoreného virtuálneho zariadenia.



Obr. 3.2: Hyper-V - špeciálne meno

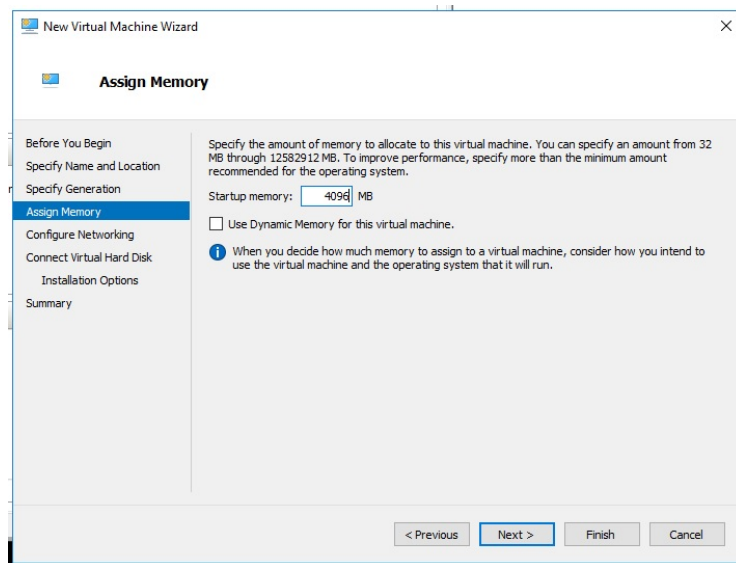
Pri voľbe generácie zaškrtneme Generation 1 . Z dôvodu že generácia 2 podporuje Win8 alebo Win2012 a vyšie.

V nasledujúcej sekcii sme pamäti pridelili 4096. Túto hodnotu sme zvolili podľa špeciálnych parametrov daným samotnými vývojármi monitorovacieho systému (viz.



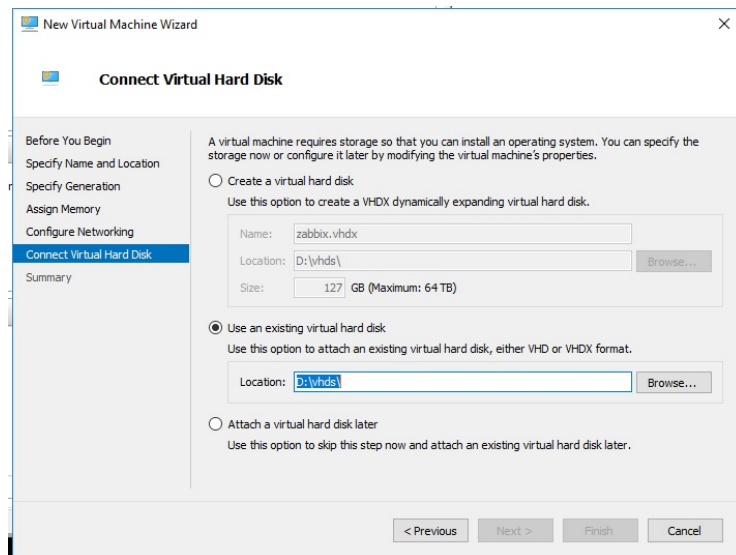
Obr. 3.3: Hyper-V - generácia

Tabl. 2.1: 'peci kácie doporučeného výkonu serveru pre daný počet sledovaných sta-  
níc).



Obr. 3.4: Hyper-V - využitie pamäte

Pripojenie virtuálneho disku, je vlastne pripojenie disku, ktorý sme si stiahli z domovskej stránky Zabbix. Jednoduchým spôsobom disk pripojíme a implementáciu dokončíme.



Obr. 3.5: Hyper-V - pripojenie Zabbix appliance

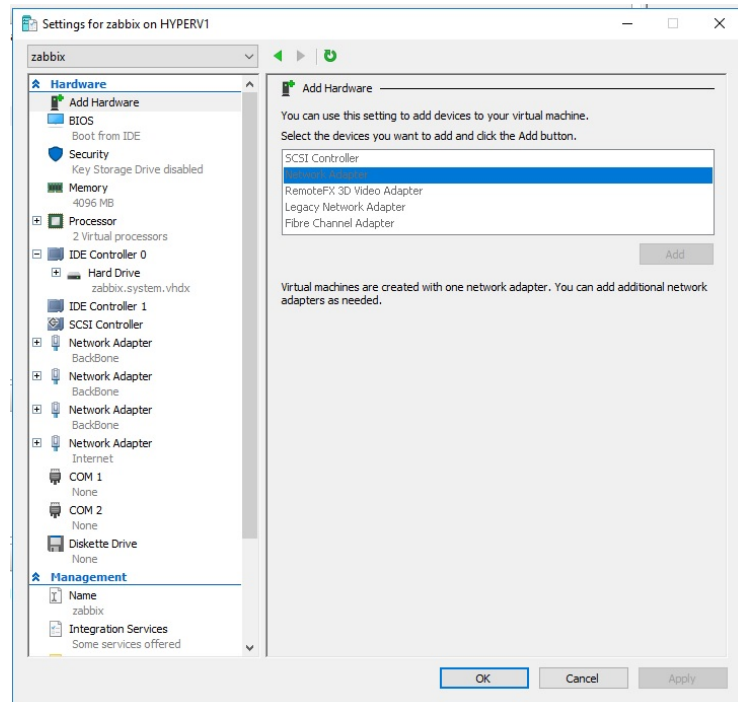
## 3.2 Nastavenie jednotlivých sieťových rozhraní v MS Hyper-V

### 3.2.1 Pridanie sieťových adaptérov

Pridajte virtuálny sieťový adaptér do bežiacieho virtuálneho počítača rovnakým spôsobom, akým ho pridáte do zastaveného virtuálneho počítača[19]:

1. V dialógovom okne Nastavenia v Hyper-V začnite na stránke Pridať hardvér. Položka sieťového adaptéra je sivá kvôli voľbe Generation1:
2. Zvýraznite Network Adapter a kliknite na Add.
3. Dostanete sa na obrazovku, kde môžete vyplniť všetky potrebné informácie pre sieťový adaptér. Nastavte všetky položky podľa potreby.
4. Keď nastavíte všetky svoje predstavy, kliknutím na tlačidlo OK pridajte adaptér a zatvorte dialógové okno alebo položku Použiť, ak chcete pridať adaptér a ponechajte dialógové okno otvorené.

Pri nastavovaní jednotlivých sieťových adaptérov vo virtualizačnom nástroji Hyper-V, sme museli dbať na virtuálne rozdelenie siete, ktorú chceme sledovať. Tá je rozdelená do jednotlivých virtuálnych sietí znázornených v Tab. 3.1: Virtuálne rozdelenie siete a ich parametre.



Obr. 3.6: Pripojenie sieťového adaptéru

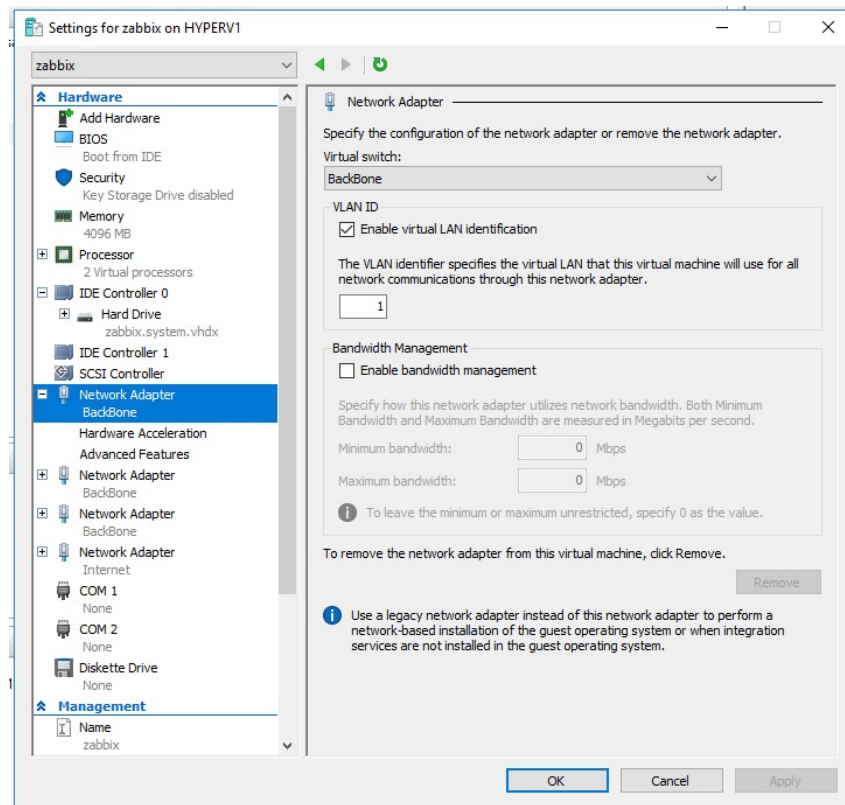
Z toho nám vyplíva že každá jedna virtuálna sieť má jeden adaptér. Nastavenie sieťového adaptéra v Hyper-V. Kde vo Vlan ID máme vyplníme dané číslo, ktoré k sieti patrí.

Tab. 3.1: Virtuálne rozdelenie siete a ich parametre

Virtual switch	Vlan ID	MAC adresa	Rozsah	Názov vlan
BackBone	1	BA-BA-DE-DA-00-01	10.0.0.0/16	Privátná LAN
BackBone	3	BA-BA-DE-DA-00-03	192.168.1.0/24	Produkcia
BackBone	5	BA-BA-DE-DA-00-05	192.168.3.0/24	Kamery
Internet	100	BA-BA-DE-DA-00-02	192.168.5.0/24	Internet

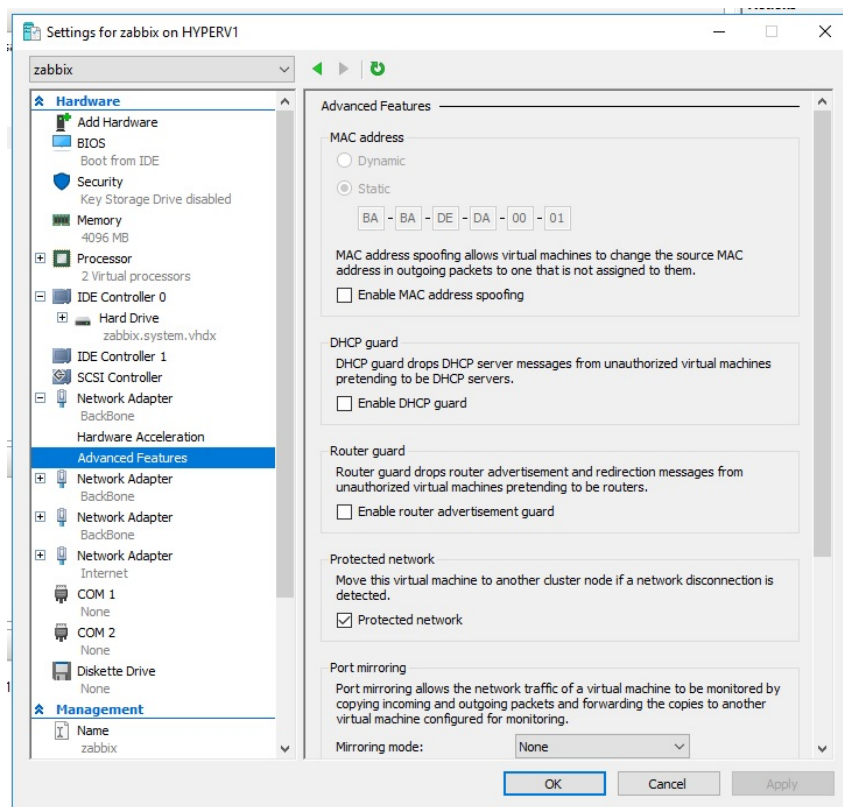
### 3.2.2 Nastavenie jednotlivých sieťových adaptérov

V nastavení virtualizačnej technológie Hyper-V sme si vytvorili štyri sieťové adaptéri. Každému adaptéru sme prideliť jedinečnú Vlan ID, ktoré môžeme vidieť v Tab. 3.1: Parametre sieťových adaptérov v Hyper-V.



Obr. 3.7: Hyper-V nastavenie sieťového adaptéru

Statické nastavenie MAC adresy sieťového adaptéru je potrebné rozkliknúť **Advanced Features** a po rozbalení menu vybrať v sekcii **MAC address** možnosť **Static**. Je nutné ešte zadať MAC adresu vybranej vlan, ktorú sme zadali u skôr.



Obr. 3.8: Hyper-V nastavenie sieťového adaptéru

### 3.2.3 DHCP nastavenie

Rezervácia DHCP je trvalé priradenie adresy IP. Je to špeciálna IP adresa v rozsahu DHCP, ktorá je natrvalo vyhradená na prenájaté používanie a konkrétneho klienta DHCP[20].

Rezervácia pozostáva z týchto informácií:

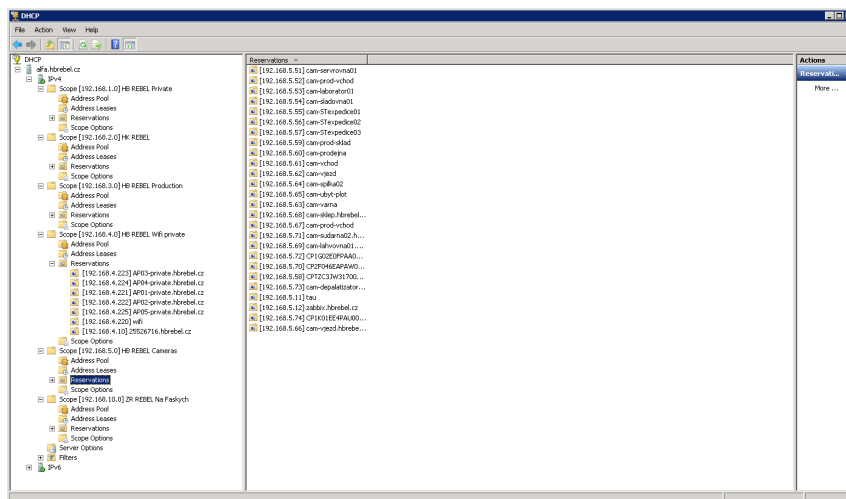
Názov rezervácie : Názov, ktorý správca priradí

IP adresa : IP adresa z rozsahu pre klienta

Adresa MAC : Adresa MAC klienta

Popis : Popis, ktorý administrátor priradí

V naďom prípade môžeme vidieť príklad na Obr. 3.9: Výpis z DHCP serveru, vytvorenú rezerváciu pre zabbix v pákovej sieti s IP adresou 192.168.5.12, ku ktorej sme pri vytváraní rezervácie pridali správnu MAC adresu daného sieťového rozhrania z MS Hyper-V.



Obr. 3.9: Výpis z DHCP serveru

### 3.3 Výskyt chyby v Zabbix a jeho riešenie

Výskyt chyby v monitorovacom systéme Zabbix spočíval o to, že sieťovými kartami neboli pridelené IP adresy z DHCP serveru. Riešenie spočívalo v reštartovaní sieťových kariet. Tohto kroku je možné dosiahnuť nasledovne:

Tento skript vypne a zapne sieťové rozhrania 0 a 3. Pri každej akcii sa vypíše príslušný konečný stav (úspech, chyba). Všetko je logované do syslogu.

Na vytvorenie skriptu je potrebné otvoriť Midnight commander. V ňom prejsť do zložky /etc/init.d/ a tu vytvoriť nový súbor, v našom prípade ifreset.sh. Do tohto súboru zapíšeme vyššie spomínaný skript. Skript sa zatiaľ chová ako obyčajný textový súbor.

```

#!/bin/bash
if ifconfig eth0 down ; then
  if ifconfig eth0 up ; then
    logger -t „ifreset“ -s „eth0 was reset correctly.“
  if ifconfig eth1 down ; then
    if ifconfig eth1 up ; then
      logger -t „ifreset“ -s „eth1 was reset correctly.“
    if ifconfig eth2 down ; then
      if ifconfig eth2 up ; then
        logger -t „ifreset“ -s „eth2 was reset correctly.“
      if ifconfig eth3 down ; then
        if ifconfig eth3 up ; then
          logger -t „ifreset“ -s „eth3 was reset correctly.“
          logger -t „ifreset“ -s „Script ifreset was executed“
        else
          logger -t „ifreset“ -s „Can't change eth3 to state up.“
        fi
      else
        logger -t „ifreset“ -s „Can't change eth3 to state down.“
      fi
    else
      logger -t „ifreset“ -s „Can't change eth2 to state up.“
    fi
  else
    logger -t „ifreset“ -s „Can't change eth2 to state down.“
  fi
else
  logger -t „ifreset“ -s „Can't change eth1 to state up.“
fi
else
  logger -t „ifreset“ -s „Can't chage eth1 to state down.“
fi
else
  logger -t „ifreset“ -s „Can't change eth0 to state up.“
fi
else
  logger -t „ifreset“ -s „Can't change eth0 to state down.“
fi

```

Obr. 3.10: Vytvorený skript na reštart sieťových kariet

Je potrebné ho teda dostať do pohybu. To môžeme spraviť príkazom:

```
chod 744 /etc/init.d/ifreset.sh
```

Teraz je skript spustiteľný. Je to možné overiť príkazom:

```
/etc/init.d/ifreset.sh
```

Teraz je potrebné nastaviť spustenie skriptu, vždy po štarte systému. Pre spustenie skriptu po štarte systému bude využitá funkcionálna služba.

Na vytvorenie service je potrebné vytvoriť súbor v nasledujúcej ceste:

/etc/systemd/system/ifreset.service

Súbor bude obsahovať nasledujúci text:

```
[Unit]
After=network.target
[Service]
ExecStart=/home/appliance/ifreset.sh
[Install]
WantedBy=default.target
```

„alej je nutné service sprevádzkovať a zaviesť do systému:

```
# chmod 664 /etc/systemd/system/disk-space-check.service
```

```
# systemctl daemon-reload
```

```
# systemctl enable disk-space-check.service
```

Ako potvrdenie by sa mala objaviť nasledujúca hláška:

Created symlink from /etc/systemd/system/default.target.wants/ifreset.service to /etc/systemd/system/ifreset.service.

Teraz je service sprevádzkovaná a po reštarte systému sa spustí. Je to možné overiť výpisom syslogu.

## 4 Implementácia sieťových prvkov do monitorovacieho systému Zabbix

### 4.1 Vytvorenie nového sledovaného zariadenia

V prvom rade je potrebné vytvoriť nastavenie nového hostiteľa, ktorá sa vykonáva v nasledujúcich krokoch, Nastavenie - Hostiteľa . Na Obr. 4.1 - Vytvorenie nového monitorovacieho zariadenia sú zobrazené postupné kroky. Pri vytváraní nového hostiteľa zaklikneme v pravom hornom rohu Vytvorenie hostiteľa . Pri vybraní tejto možnosti sa zobrazí formulár, kde zadáme parametre hostiteľa (viz Obr. 4.2 - Atribúty hostiteľa). Na vytvorenie nového hostiteľa môžeme tiež použiť tlačidlo Vytvoriť kópiu a vytvoriť úplnú kópiu vo forme existujúceho hostiteľa. Kliknutím na tlačidlo vytvoriť kópiu zostanú zachované všetky parametre hostiteľa a prepojenie šablón (ponechanie všetkých entít z týchto šablón). Na druhú stranu pri zakliknutí tlačidla vytvoriť úplnú kópiu bude navyše uchovávať priamo pripojené entity (aplikácie, položky, spúšťače, grafy, pravidlá vyhadzovania na nižšej úrovni a webové scenáre). Tieto možnosti sú zobrazené na Obr. 4.2 - Atribúty hostiteľa, zvýraznené červenou farbou.

Jméno	Aplikace	Položky	Spouštěče	Grafy	Protokoly	Web	Obnovování	Šablony	Stav	Dostupnost	Agent sledování	Info
alfa	Aplikace	Položky	Spouštěče	Grafy	Protokoly	Web	192.168.1.2: 3389	RDP_Testing	Povoleno	2023   SHARP   MAX   PING	ZALOKA	
beta	Aplikace	Položky	Spouštěče	Grafy	Protokoly	Web	192.168.1.8: 3389	RDP_Testing	Povoleno	2023   SHARP   MAX   PING	ZALOKA	
cam-bocsi-pilot	Aplikace	Položky	Spouštěče	Grafy	Protokoly	Web	192.168.5.74: 10050	Template Module ICMP Ping	Povoleno	2023   SHARP   MAX   PING	ZALOKA	
cam-laborator01	Aplikace	Položky	Spouštěče	Grafy	Protokoly	Web	192.168.5.53: 10050	Template Module ICMP Ping	Povoleno	2023   SHARP   MAX   PING	ZALOKA	
cam-prod-01st	Aplikace	Položky	Spouštěče	Grafy	Protokoly	Web	192.168.5.59: 10050	Template Module ICMP Ping	Povoleno	2023   SHARP   MAX   PING	ZALOKA	
cam-prod-vcfod	Aplikace	Položky	Spouštěče	Grafy	Protokoly	Web	192.168.5.67: 10050	Template Module ICMP Ping	Povoleno	2023   SHARP   MAX   PING	ZALOKA	
cam-prodina	Aplikace	Položky	Spouštěče	Grafy	Protokoly	Web	192.168.5.60: 10050	Template Module ICMP Ping	Povoleno	2023   SHARP   MAX   PING	ZALOKA	
cam-serverovna01	Aplikace	Položky	Spouštěče	Grafy	Protokoly	Web	192.168.5.51: 10050	Template Module ICMP Ping	Povoleno	2023   SHARP   MAX   PING	ZALOKA	
cam-01sep	Aplikace	Položky	Spouštěče	Grafy	Protokoly	Web	192.168.5.68: 10050	Template Module ICMP Ping	Povoleno	2023   SHARP   MAX   PING	ZALOKA	
cam-sladozna01	Aplikace	Položky	Spouštěče	Grafy	Protokoly	Web	192.168.5.54: 10050	Template Module ICMP Ping	Povoleno	2023   SHARP   MAX   PING	ZALOKA	
cam-sprk01	Aplikace	Položky	Spouštěče	Grafy	Protokoly	Web	192.168.5.58: 10050	Template Module ICMP Ping	Povoleno	2023   SHARP   MAX   PING	ZALOKA	
cam-sprk02	Aplikace	Položky	Spouštěče	Grafy	Protokoly	Web	192.168.5.64: 10050	Template Module ICMP Ping	Povoleno	2023   SHARP   MAX   PING	ZALOKA	
cam-STerpedico01	Aplikace	Položky	Spouštěče	Grafy	Protokoly	Web	192.168.5.55: 10050	Template Module ICMP Ping	Povoleno	2023   SHARP   MAX   PING	ZALOKA	
cam-STerpedico02	Aplikace	Položky	Spouštěče	Grafy	Protokoly	Web	192.168.5.56: 10050	Template Module ICMP Ping	Povoleno	2023   SHARP   MAX   PING	ZALOKA	
cam-STerpedico03	Aplikace	Položky	Spouštěče	Grafy	Protokoly	Web	192.168.5.57: 10050	Template Module ICMP Ping	Povoleno	2023   SHARP   MAX   PING	ZALOKA	
cam-ubyt-pilot	Aplikace	Položky	Spouštěče	Grafy	Protokoly	Web	192.168.5.65: 10050	Template Module ICMP Ping	Povoleno	2023   SHARP   MAX   PING	ZALOKA	

Obr. 4.1: Vytvorenie nového monitorovacieho zariadenia

Vytváranie hostiteľa pomocou kópie je jednoduchšie, pretože v tomto prípade stačí zmeniť len názov hostiteľa a jeho IP adresu. Preto pomocou kópie sa správna skupina hostiteľa a správne šablóny skopírujú. Pozor, tento prípad sa používa zväčša pri zhode skupiny hostiteľa.

V prípade tvorby nového hostiteľa sú všetky povinné polia označené červenou hviezdikou. Následné atribúty sú rozpísané nasledovne:

Hostitelé

Všichni hosty / cam-bocni-plot Povoleno ZBX SNMP JMX IPMI Aplikace 1 Položky 3 Spouštěče 3 Grafy 1 Objevovací pravidla Web scénáře

Hostitel Šablony IPMI Makra Host inventář Šifrování

Název hostitele

Zobrazované jméno

Skupiny

Ve skupinách

Kamery

Další skupiny

AP  
Backup devices  
Discovered hosts  
Docházka  
HB Rebel NB  
HK Rebel  
Hypervisors  
Internet GW  
Linux servers  
Na Farských

Nová skupina

Agentova rozhraní

IP adresa	Jméno DNS	Připojit k	Port	Výchozí
<input type="text" value="192.168.5.74"/>	<input type="text"/>	<input type="radio"/> IP <input type="radio"/> DNS	<input type="text" value="10050"/>	<input checked="" type="radio"/> Odstranit

[Přidat](#)

SNMP rozhraní [Přidat](#)

JMX rozhraní [Přidat](#)

IPMI rozhraní [Přidat](#)

Popis

Sledován přes proxy

Povoleno

[Aktualizovat](#) [Vytvořit kopii](#) [Vytvořit úplnou kopii](#) [Smazat](#) [Zrušit](#)

Obr. 4.2: Atribúty hostite@a

Název hostite@a : Zadáte jedinečné meno hostite@a.

Zobrazené meno : Ak toto meno nastavíte, bude to viditeľné v zoznamoch, mapách, atď ...

Skupiny : Vyberte skupiny hostite@ov, do ktorých hostite@ patrí. Hostite@ musí patriť aspoň jednej hostite@skej skupine.

Rozhranie : Pre hostite@a je podporovaný niekoľko typov hostite@skeho rozhrania: Agent, SNMP, JMX a IPMI. Ak chcete pridať nové rozhranie, kliknite na tlačidlo Pridať do bloku rozhrania a zadajte IP / DNS, Connect to a Port.

Ip adresa : Hostite@ska IP adresa.

DNS meno : Názov hostite@a DNS.

Pripojenie k : Po kliknutí na príslušné tlačidlo bude server Zabbix informovaný, čo má použiť na získavanie údajov od agentov: IP/DNS.

Port : číslo portu TCP/UDP. Predvolené hodnoty sú: 10050 pre agenta Zabbix, 161 pre agenta SNMP, 12345 pre JMX a 623 pre IPMI.

Pri tvorbe novo sledovaného zariadenia musím myslieť dopredu a ak sa jedná o zariadenie, ktoré chcem sledovať pomocou protokolu SNMP, nemôžem zabudnúť na vyplnenie kolonky SNMP rozhrania, kde IP adresa sa bude zhodovať s naším zariadením a port vyplním z pravidla na 161 (SNMP trapy sa posielajú na porte 162). Na Obr. 4.3 - Nastavenie SNMP rozhrania môžeme dané nastavenie vidieť.

The screenshot shows a configuration page for a host named 'sw-stexpedice'. It includes sections for 'Skupiny' (Groups) and 'Agentova rozhraní' (Agent interfaces). The 'Agentova rozhraní' section contains two entries. The second entry, which is highlighted with a red box, is for the IP address '192.168.1.247' and port '161'. It includes a 'Přidat' button and a checked checkbox labeled 'Použít hromadné žádosti'.

Obr. 4.3: Nastavenie SNMP rozhrania

## 4.2 Vytvorenie tablóny

Vytvorenie tablóny prebieha v nasledujúcich krokoch: Nastavenie tablóny - Vytvorenie tablóny. Na Obr. 4.4 - Vytvorenie novej tablóny, je zobrazená už predvyplnená tabuľka novej tablóny, ktorú som si niejak pomenoval, priradil k ostatným tablónam sieťových zariadení a nakoniec je umiestnený zoznam v ktorom sa nachádzajú zariadenia, ktorým bola daná tablóna pridelená.

Daná tablóna obsahuje 4 aplikácie a 4 položky. Toto ďalšie nastavenie vysvetlím v ďalšej kapitole Vytvorenie aplikácie a položky.

## 4.3 Vytvorenie aplikácie a položky

V mojom prípade zobrazenej na Obr. 4.5 - Vytvorenie novej položky, sme som hneď preskočili na sekciu Položky. Je to z toho dôvodu že samotnú aplikáciu som vytvoril

Skupina hostitelů Šablony Hostitelé Servisní okna Akce Korelace událostí Průzkum Služby

## Šablony

Všechny šablony / Interface SNMP traffic CISCO Aplikace 4 Položky 4 Spouštěče Grafy Obrazovky Objevovací pravidla Web scénáře

Šablona Připojené šablony Makra

Jméno šablony

Zobrazované jméno

Skupiny Ve skupinách  Další skupiny

- AP
- Backup devices
- Discovered hosts
- Docházka
- HB Rebel NB
- HK Rebel
- Hypervisors
- Internet GW
- Kamery
- Linux servers

Nová skupina

Hosty / šablony  Další skupina

Popis

Obr. 4.4: Vytvorenie novej šablóny

za behu vytvorenia novej položky. Táto možnosť je v kolonke s názvom Nová aplikácia. Táto aplikácia sa po vyplnení vytvorí v momente vytvorenia novej položky.

Popis samotných údajov si rozoberieme nasledovne:

Meno : Klasické pomenovanie novej položky

Typ : Vyberieme typ agenta SNMP protokolu

Kód: Každý kód musí byť jedinečný

SNMP OID : OID hodnota danej vlastnosti, ktorú chceme sledovať

SNMP komunita : Nastavená defaultne na hodnotu public, túto hodnotu nastavujeme vďaka rovnakú, kvôli jednoduchému používaniu

Typ informácie : Zadáme typ informácie, ktorú budeme sledovať

Interval aktualizácií : Interval aktualizácií sledovanej vlastnosti

Položky

Všechny šablony / Interface SNMP traffic CISCO Aplikace 4 Položky 4 Spouštěče Grafy Obrazovky Objevovací pravidla Web scénáře

Položka Preprocessing

Jméno

Typ

Klíč

SNMP OID

SNMP komunita

Port

Typ informace

Jednotky

Interval aktualizací

Vlastní intervaly

Typ	Interval	Období	Akce
<input checked="" type="checkbox"/> Flexibilní	<input type="text" value="Plánování"/>	<input type="text" value="50s"/>	<input type="text" value="1-7,00:00-24:00"/>
			<input type="button" value="Odstranit"/>
<input type="button" value="Přidat"/>			

Období uložení historie

Perioda uložení trendů

Ukázat hodnotu

Nová aplikace

Aplikace

- Žádná
- adminstatus
- broadcast**
- errors
- test

Obr. 4.5: Vytvorenie novej položky

### 4.3.1 Hodnota SNMP OID

Struktúru OID som popísali bližšie v kapitole SNMP protokol . Teraz ale popíšem bližšie ako sme sa k danej hodnote dostali. Rôzne sieťové zariadenia podporujúce SNMP protokol majú OID hodnoty rôzne. Preto podľa jednotlivých zariadení sa musia dané hodnoty dohadovať v dokumentáciách k daným zariadením. V prvom kroku som si ale dohadoval samotné OID daného rozhrania ktoré chcem sledovať, v našom prípade to bol gi1 rozhranie, ktoré malo hodnotu.1.3.6.1.2.1.31.1.1.1.3.49 . Táto hodnota je zobrazená Obr. 4.6 - OID hodnoty rozhraní.

Táto hodnota nesúhlasí s hodnotou, ktorú som zadali do kolonky SNMP OID . To preto že v tejto kolonke sa nachádza práve hodnota sledovanej vlastnosti. V mojom prípade to je hodnota.1.3.6.1.2.1.31.1.1.1.3.49 . Je to hodnota vlastnosti, ktorá nepretržite sleduje počet broadcastových paketov na rozhraní gi1, dodaných touto podvrstvou vyšie. Táto hodnota 49 sa nezmenila preto, že sa jedná o rovnaký port prepínača.

```

OID=.1.3.6.1.2.1.31.1.1.1.1.49, Type=OctetString, Value=gi1
OID=.1.3.6.1.2.1.31.1.1.1.1.50, Type=OctetString, Value=gi2
OID=.1.3.6.1.2.1.31.1.1.1.1.51, Type=OctetString, Value=gi3
OID=.1.3.6.1.2.1.31.1.1.1.1.52, Type=OctetString, Value=gi4
OID=.1.3.6.1.2.1.31.1.1.1.1.53, Type=OctetString, Value=gi5
OID=.1.3.6.1.2.1.31.1.1.1.1.54, Type=OctetString, Value=gi6
OID=.1.3.6.1.2.1.31.1.1.1.1.55, Type=OctetString, Value=gi7
OID=.1.3.6.1.2.1.31.1.1.1.1.56, Type=OctetString, Value=gi8
OID=.1.3.6.1.2.1.31.1.1.1.1.57, Type=OctetString, Value=gi9
OID=.1.3.6.1.2.1.31.1.1.1.1.58, Type=OctetString, Value=gi10
OID=.1.3.6.1.2.1.31.1.1.1.1.59, Type=OctetString, Value=gi11
OID=.1.3.6.1.2.1.31.1.1.1.1.60, Type=OctetString, Value=gi12
OID=.1.3.6.1.2.1.31.1.1.1.1.61, Type=OctetString, Value=gi13
OID=.1.3.6.1.2.1.31.1.1.1.1.62, Type=OctetString, Value=gi14
OID=.1.3.6.1.2.1.31.1.1.1.1.63, Type=OctetString, Value=gi15
OID=.1.3.6.1.2.1.31.1.1.1.1.64, Type=OctetString, Value=gi16
OID=.1.3.6.1.2.1.31.1.1.1.1.65, Type=OctetString, Value=gi17
OID=.1.3.6.1.2.1.31.1.1.1.1.66, Type=OctetString, Value=gi18
OID=.1.3.6.1.2.1.31.1.1.1.1.67, Type=OctetString, Value=gi19
OID=.1.3.6.1.2.1.31.1.1.1.1.68, Type=OctetString, Value=gi20
OID=.1.3.6.1.2.1.31.1.1.1.1.69, Type=OctetString, Value=gi21
OID=.1.3.6.1.2.1.31.1.1.1.1.70, Type=OctetString, Value=gi22
OID=.1.3.6.1.2.1.31.1.1.1.1.71, Type=OctetString, Value=gi23
OID=.1.3.6.1.2.1.31.1.1.1.1.72, Type=OctetString, Value=gi24
OID=.1.3.6.1.2.1.31.1.1.1.1.73, Type=OctetString, Value=gi25
OID=.1.3.6.1.2.1.31.1.1.1.1.74, Type=OctetString, Value=gi26
OID=.1.3.6.1.2.1.31.1.1.1.1.75, Type=OctetString, Value=gi27
OID=.1.3.6.1.2.1.31.1.1.1.1.76, Type=OctetString, Value=gi28
OID=.1.3.6.1.2.1.31.1.1.1.1000, Type=OctetString, Value=Po1
OID=.1.3.6.1.2.1.31.1.1.1.1001, Type=OctetString, Value=Po2
OID=.1.3.6.1.2.1.31.1.1.1.1002, Type=OctetString, Value=Po3
OID=.1.3.6.1.2.1.31.1.1.1.1003, Type=OctetString, Value=Po4
OID=.1.3.6.1.2.1.31.1.1.1.1004, Type=OctetString, Value=Po5
OID=.1.3.6.1.2.1.31.1.1.1.1005, Type=OctetString, Value=Po6
OID=.1.3.6.1.2.1.31.1.1.1.1006, Type=OctetString, Value=Po7
OID=.1.3.6.1.2.1.31.1.1.1.1007, Type=OctetString, Value=Po8
OID=.1.3.6.1.2.1.31.1.1.1.13000, Type=OctetString, Value=tunnell
OID=.1.3.6.1.2.1.31.1.1.1.17000, Type=OctetString, Value=loopback1
OID=.1.3.6.1.2.1.31.1.1.1.12000, Type=OctetString, Value=Logical-int 1
OID=.1.3.6.1.2.1.31.1.1.1.100000, Type=OctetString, Value=1
OID=.1.3.6.1.2.1.31.1.1.1.100002, Type=OctetString, Value=3
OID=.1.3.6.1.2.1.31.1.1.1.100003, Type=OctetString, Value=4
OID=.1.3.6.1.2.1.31.1.1.1.100004, Type=OctetString, Value=5
OID=.1.3.6.1.2.1.31.1.1.1.1300000, Type=OctetString, Value=1
Total: 44

```

Obr. 4.6: OID hodnoty rozhraní

```

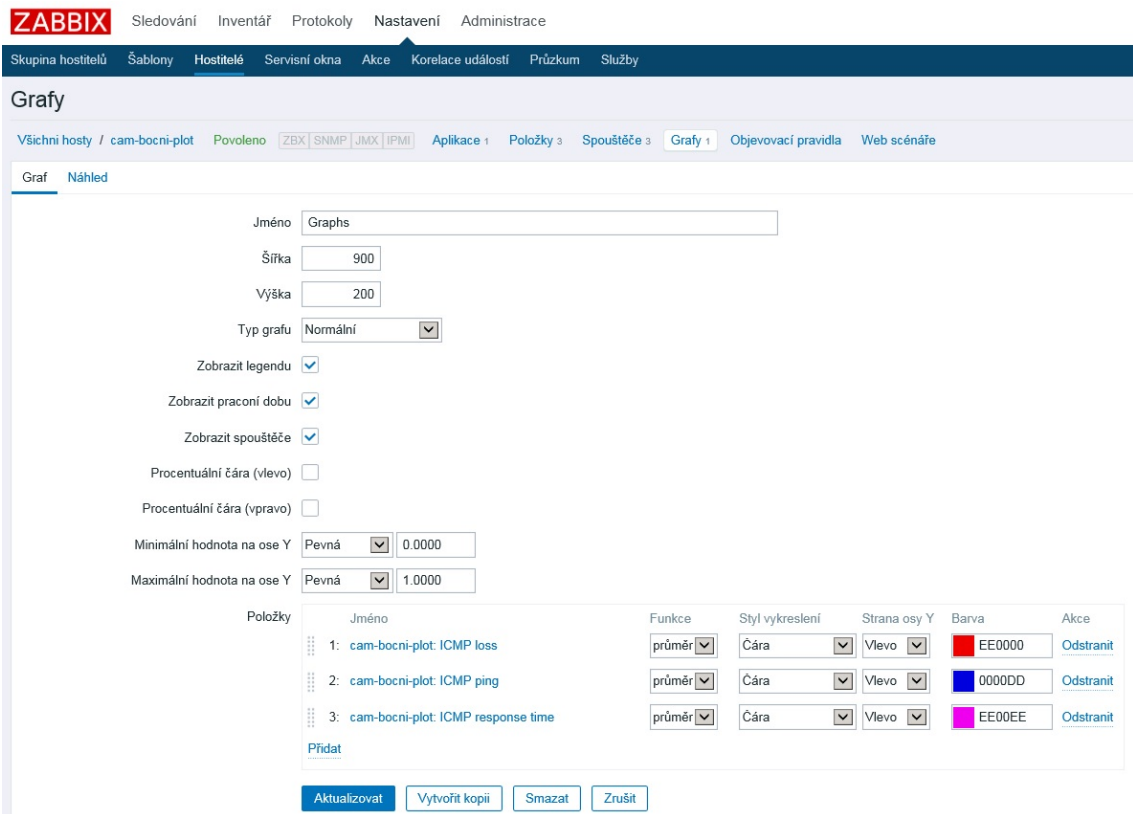
OID=.1.3.6.1.2.1.31.1.1.1.3.49, Type=Counter32, Value=9442
OID=.1.3.6.1.2.1.31.1.1.1.3.50, Type=Counter32, Value=0
OID=.1.3.6.1.2.1.31.1.1.1.3.51, Type=Counter32, Value=50776
OID=.1.3.6.1.2.1.31.1.1.1.3.52, Type=Counter32, Value=1312
OID=.1.3.6.1.2.1.31.1.1.1.3.53, Type=Counter32, Value=13
OID=.1.3.6.1.2.1.31.1.1.1.3.54, Type=Counter32, Value=199
OID=.1.3.6.1.2.1.31.1.1.1.3.55, Type=Counter32, Value=101341
OID=.1.3.6.1.2.1.31.1.1.1.3.56, Type=Counter32, Value=149638
OID=.1.3.6.1.2.1.31.1.1.1.3.57, Type=Counter32, Value=58318
OID=.1.3.6.1.2.1.31.1.1.1.3.58, Type=Counter32, Value=0
OID=.1.3.6.1.2.1.31.1.1.1.3.59, Type=Counter32, Value=309714
OID=.1.3.6.1.2.1.31.1.1.1.3.60, Type=Counter32, Value=4104105
OID=.1.3.6.1.2.1.31.1.1.1.3.61, Type=Counter32, Value=1207
OID=.1.3.6.1.2.1.31.1.1.1.3.62, Type=Counter32, Value=1059
OID=.1.3.6.1.2.1.31.1.1.1.3.63, Type=Counter32, Value=52009
OID=.1.3.6.1.2.1.31.1.1.1.3.64, Type=Counter32, Value=134859
OID=.1.3.6.1.2.1.31.1.1.1.3.65, Type=Counter32, Value=0
OID=.1.3.6.1.2.1.31.1.1.1.3.66, Type=Counter32, Value=11393
OID=.1.3.6.1.2.1.31.1.1.1.3.67, Type=Counter32, Value=1000975
OID=.1.3.6.1.2.1.31.1.1.1.3.68, Type=Counter32, Value=61127
OID=.1.3.6.1.2.1.31.1.1.1.3.69, Type=Counter32, Value=112324
OID=.1.3.6.1.2.1.31.1.1.1.3.70, Type=Counter32, Value=1428
OID=.1.3.6.1.2.1.31.1.1.1.3.71, Type=Counter32, Value=353
OID=.1.3.6.1.2.1.31.1.1.1.3.72, Type=Counter32, Value=7187
OID=.1.3.6.1.2.1.31.1.1.1.3.73, Type=Counter32, Value=0
OID=.1.3.6.1.2.1.31.1.1.1.3.74, Type=Counter32, Value=1539959
OID=.1.3.6.1.2.1.31.1.1.1.3.75, Type=Counter32, Value=0
OID=.1.3.6.1.2.1.31.1.1.1.3.76, Type=Counter32, Value=87921370
OID=.1.3.6.1.2.1.31.1.1.3.1000, Type=Counter32, Value=0
OID=.1.3.6.1.2.1.31.1.1.3.1001, Type=Counter32, Value=0
OID=.1.3.6.1.2.1.31.1.1.3.1002, Type=Counter32, Value=0
OID=.1.3.6.1.2.1.31.1.1.3.1003, Type=Counter32, Value=0
OID=.1.3.6.1.2.1.31.1.1.3.1004, Type=Counter32, Value=0
OID=.1.3.6.1.2.1.31.1.1.3.1005, Type=Counter32, Value=0
OID=.1.3.6.1.2.1.31.1.1.3.1006, Type=Counter32, Value=0
OID=.1.3.6.1.2.1.31.1.1.3.1007, Type=Counter32, Value=0
Total: 36

```

Obr. 4.7: OID hodnoty broadcastových hodnot paketov na daných rozhraniach

## 4.4 Vytvorenie grafu

Pri vytváraní grafu musím vedieť, presne ktoré položky chcem do grafu a predbežne ako graf bude vyzerať. Pri vytváraní grafu si v sekcii hostiteľ nájdem zariadenie na ktorom chcem konkrétny graf vytvoriť. Do grafu sa vynášajú informácie zo sekcii položky, tak je nevyhnutné aby táto časť bola nastavená správne. Pri vybraní konkrétneho zariadenia, rozklikneme položky graf a v pravom hornom rohu vytvorí graf. na Obr. 4.8 - Atribúty vytvárania grafu môžeme vidieť predvyplnené atribúty.



Obr. 4.8: Atribúty vytvárania grafu

Najdôležitejší čas sa nachádza v sekcii položky, kde pripájam práve predvytvorené položky. Samotný graf číta z týchto položiek jednotlivé hodnoty, ktoré potom konštantne s časom zapisuje a vytvára samotný graf, ktorý je zobrazený na Obr. 4.9 - Náhľad vykresleného grafu.



Obr. 4.9: Náhľad vykresleného grafu

## 4.5 Vytvorenie mapy

Vytvorenie mapy prebieha v nasledujúcich krokoch: Sledování - Mapy - Vytvorí mapu. Zobrazí sa nasledujúce okno, ktoré je zobrazené na Obr. 4.10 - Atribúty vytvorenej mapy.

The screenshot shows the Zabbix web interface for configuring a network map. The main navigation bar includes 'Sledování', 'Inventář', 'Protokoly', 'Nastavení', and 'Administrace'. The current page is 'Síťové mapy' with sub-tabs for 'Mapa' and 'Sdílení'. The configuration form includes the following fields and options:

- Vlastník:** Admin (Zabbix Administrator) [Vybrat]
- Jméno:** Kamery [X]
- Šířka:** 800
- Výška:** 600
- Obrázek na pozadí:** Žádný obrázek [v]
- Automatické přiřazení ikon:** <manuálně> [v] zobrazit mapování ikon
- Zvýraznění ikon:**
- Označ elementy při změně stavu spouštěče:**
- Display problems:** Rozvést jeden problém | Number of problems | Number of problems and expand most critical one
- Rozšířený popis:**
- Typ popisku ikony:** Popisek [v]
- Umístění popisku ikony:** Dole [v]
- Zobrazit problémy:** Vše [v]
- Minimální závažnost spouštěče:** Neuřešeno | Informační | Upozornění | Střední | Závažný | Kritický
- URL:** Jméno [ ] | URL [ ] | Prvek: Hostitel [v] | Akce: Odstranit [v]

Buttons at the bottom include: Aktualizovat, Vytvořit kopii, Vytvořit úplnou kopii, Smazat, Zrušit.

Obr. 4.10: Atribúty vytvorenej mapy

Po nastavení atribútou sa mi vytvorí prázdna mapa do ktorej musím jednotlivé obrázky alebo prvky vkladať ručne a jednotlivito. Vytvorená mapa je zobrazená na Obr 4.11 - Vytvorená mapa prvku vo výrobe.

Obr. 4.11: Vytvorená mapa prvku vo výrobe

Na mape je prekreslená topológia prvku vo výrobe. V prvom kroku pri aktualizácii mapy je nutné zakliknúť políčko aktualizovať mapu . Po tomto kroku je možné do mapy vkladať rôzne prvky, ktoré by mali odpovedať danému zariadení. Vo vlastnostiach konkrétneho zariadenia je možné pridávať rôzne aplikácie, ktoré sa nám potom zobrazia v mape.

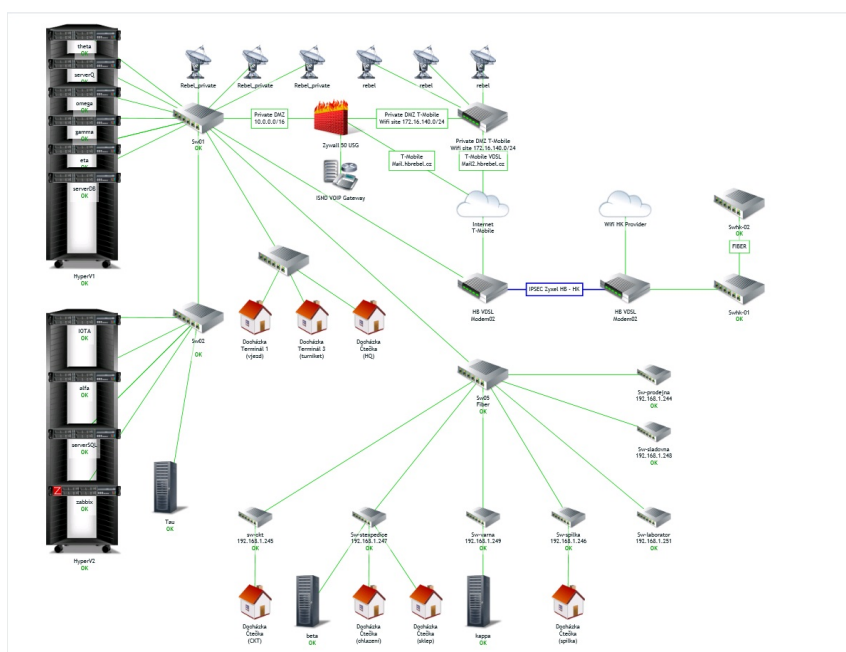
# 5 Získané výsledky monitorovacieho systému Zabbix

## 5.1 Vytvorené Mapy

### 5.1.1 Mapa HB Rebel

Kostra celej siete je znázornená na Obr. 5.1 - Mapa HB Rebel, táto topológia je prekreslená zjednodušene a ostatné zariadenia sú zobrazené na ďalších dvoch mapách. V mape som si pridali ku každému prepínaču aplikáciu status, ktorá mi zjednodušene ukazuje či je dané zariadenie zapnuté alebo vypnuté. Táto hodnota sa zobrazí pod zariadením na mape a ja mám možnosť jednoducho a rýchlo zistiť stav zariadenia.

Pri serverových zariadeniach som použil aplikáciu s názvom RDPcheck. Túto aplikáciu som si vytvoril z dôvodu nefunkčnosti ICMP protokolu na serverových zariadeniach a tak aspoň takýmto spôsobom kontrolujem chod daných serverových zariadení. Aplikácia sa dotazuje na port 3389 a kontroluje či je daný port otvorený. Ak je daný port otvorený obdrží návratovú hodnotu 0, v inom prípade to bude nenulová hodnota čo zaznamená nastavený spúšťač a vyhodí chybovú hlášku.



Obr. 5.1: Mapa HB Rebel

## 5.1.2 Mapa prvkov vo výrobe

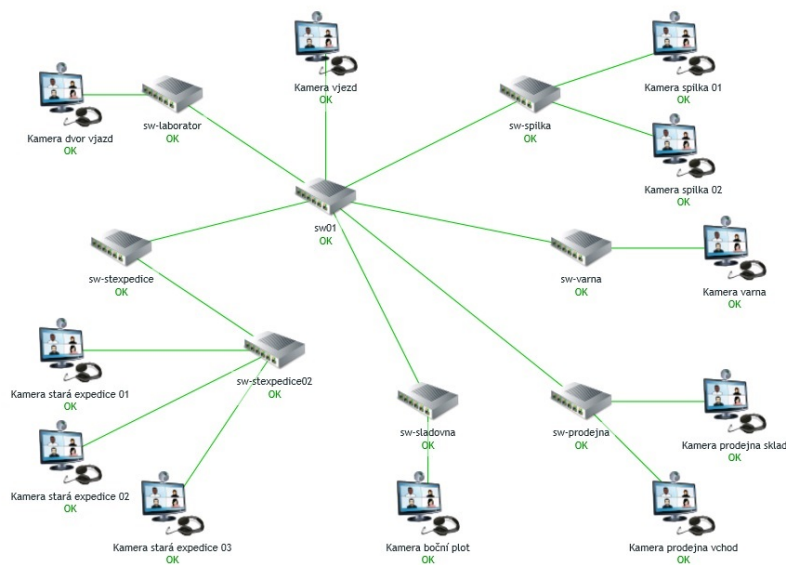
Obr.5.2 - Mapa prvkou vo výrobe mi znázorňuje produkčnú sieť, ktorá je prevádzkovaná bez prístupu na internet kvôli bezpečnosti a ochrane pred napadnutím z externej siete. Táto sieť je na samostatnej vlane s názvom `Production`. Na Obr. 8.2 - Mapa prvkou vo výrobe sú dve zariadenia nedostupné na dotaz ICMP pingu, je to z dôvodu presunu a potrebných opráv týchto zariadení.

Sledovanie funkčnosti týchto zariadení je jednou z najpodstatnejších činností nášho monitorovacieho systému. Je to z toho dôvodu že pri výpadku, ktorého koľvek zariadenia zo siete `production`, môžeme na danú situáciu zareagovať a tak predísť zbytočným problémom, ktorým sa vo výrobe chceme najväčším oblúkom vyhnúť. Jedná sa hlavne o výpadok výrobného procesu alebo v horšom prípade poškodenie niejakého zo zariadení. Obidva tieto problémy sú závažné a veľmi náročné.

Obr. 5.2: Mapa prvkov vo výrobe

### 5.1.3 Mapa kamier

Poslednou z máp je mapa kamier, ktorá je zobrazená na Obr. 5.3 - Mapa kamier. Mapa, ktorá mi zjednodužuje vypátranie problému, pri vzniknutej chybe. Všetky kamery sú kontrolované pomocou ICMP protokolu, pomocou ktorého zistím okamžite výpadok zariadenia a môžem hneď pracovať na náprave daného výpadku. Zásadne môžem vidieť štruktúru mapy je nastavená rovnako ako predchádzajúce mapy a stav dosiahnuteľnosti pomocou protokolu ICMP je umiestnený pod daným zariadením.

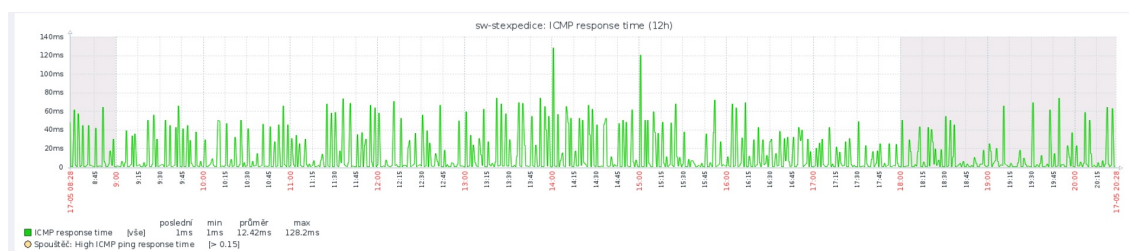


Obr. 5.3: Mapa kamier

## 5.2 Graf

### 5.2.1 Grafy z prepínača SW-STEXPEDICE

Z prepínača sw-stexpedice som vytvoril graf. Na y osy je vynesená hodnota odpovede ICMP v čase a na osy x je čas, kedy boli hodnoty získané. Táto hodnota je v mili sekundách (mS). Ak hostite© nie je dostupný (časový limit vyprší), položka sa vráti v 0.



Obr. 5.4: Prepínač SW-STEXPEDICE - ICMP doba odozvy

„ažie grafy sw01 a sw02 exportované z monitorovacieho systému Zabbix sú pridané do prílohy.

## 6 ZÁver

V úvodnej časti som sa zoznámil s teoretickou časťou monitorovania počítačových sietí a s technológiami, ktoré budem používať. Po analýze vŕetkých zariadení som ich rozdelil do jednotlivých kategórií : windows pc stanice, windows servery, prepínače, plc zariadenie vo výrobe, tlačiarne, kamery a pridelil metódy na ich sledovanie.

V druhej časti som sa zoznámil s monitorovacím nástrojom Zabbix. Naštudoval som si jeho dokumentáciu cez ktorú som sa dostal od praktickej inštalácii/implementácii a po jeho možnosti sledovania zariadení.

V praktickej časti bakalárskej práce som implementoval Zabbix appliance na virtualizačnú technológiu MS Hyper-V a následne som nastavil sieťové adaptére podľa získaných parametrov siete v každej ktorá nieje routovaná - 4 izolované siete. V tomto bode som sa stretol s chybou pridelenia IP adres sieťovým kartám Zabbixu, túto chybu som odstránil pomocou vytvorenia skripta.

Po úspešnom spustení samotného systému som vykonal konfiguráciu webového rozhrania. Nastavil som monitorovanie sietí: internet, private, produkcia a kamery, pomocou pridania jednotlivých zariadení a ich nastavením. Dôležitá úloha monitorovania siete spočíva hlavne v monitorovaní produkčnej siete v ktorej sa nachádzajú PLC zariadenia vo výrobe s vysokou prioritou funkčnosti a práve k tomu mi pomáha monitorovací systém Zabbix.

V prílohe sú pridané tabulky jednotlivých zariadení, ktoré v sieti monitorujem a pridané grafy získané z prepínačov v sieti.

# Literatúra

- [1] ManageEngine Basics of Network Monitoring [online]. ManageEngine, 2019. Dostupné z: <<https://www.manageengine.com/network-monitoring/basics-of-network-monitoring.html>>.
- [2] SNMP Simple Network Management Protocol [online]. Samuraj-cz 2005. Dostupné z: <<https://www.samuraj-cz.com/clanek/snmp-simple-network-management-protocol/>>.
- [3] RFC 1098.A Simple Network Management Protocol (SNMP) Květen 1990. MIT Laboratory for Computer Science: Network Working Group, 1990.
- [4] ICMP Úvod do ICMP [online]. Elektronická knihovna Mendlovej univerzity. Dostupné z: <[https://is.mendelu.cz/eknihovna/opory/zobraz\\_cast.pl?cast=597](https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=597)>.
- [5] SNMP. Additional Agent-based Checks [online]. Solarwinds, 2017. Dostupné z: <<https://thwack.solarwinds.com/docs/DOC-187972>>.
- [6] WMI Windows Management Instrumentation [online]. TechTarget, 2000. Dostupné z: <<https://searchwindowsserver.techtarget.com/definition/Windows-Management-Instrumentation>>.
- [7] WMI Získavanie informácií [online]. Programujte, 2003. Dostupné z: <<http://programujte.com/clanek/2006082406-ziskavanie-informacii-o-systeme-pomocou-wmi-v-net/>>.
- [8] Vlan How Do VLANs Work [online]. Intelligent Technologies, 2017. Dostupné z: <<https://www.inteltech.com/blog/how-do-vlans-work/>>.
- [9] Vlan. Isolated [online]. Infosec, 2019. Dostupné z: <<https://resources.infosecinstitute.com/vlan-network-chapter-5/#gref>>.
- [10] Vlan Routed [online]. Netgear, 2016. Dostupné z: <<https://kb.netgear.com/24754/What-is-VLAN-Routing>>.
- [11] What is Zabbix. Overview [online]. Riga: Zabbix LLC, 2019. Dostupné z: <<https://www.zabbix.com/documentation/3.4/manual/introduction/about>>.
- [12] Hardware Requirements Zabbix [online]. Riga: Zabbix LLC, 2019. Dostupné z: <<https://www.zabbix.com/documentation/3.4/manual/installation/requirements>>.

- [13] Zabbix appliance.Download [online]. Zabbix LLC, 2019. Dostupné z: [https://www.zabbix.com/download\\_appliance](https://www.zabbix.com/download_appliance) >.
- [14] Zabbix appliance.Documentation [online]. Zabbix LLC, 2019. Dostupné z: <https://www.zabbix.com/documentation/3.4/manual/appliance> >.
- [15] Zabbix agent.Description Zabbix agent [online]. Zabbix LLC, 2019. Dostupné z: [https://www.zabbix.com/zabbix\\_agent](https://www.zabbix.com/zabbix_agent) >.
- [16] Zabbix Windows agent.Install Zabbix Windows agent [online]. Zabbix LLC, 2019. Dostupné z: [https://www.zabbix.com/documentation/2.0/manual/appendix/install/windows\\_agent](https://www.zabbix.com/documentation/2.0/manual/appendix/install/windows_agent) >.
- [17] Zabbix. Element configuration [online]. Zabbix LLC, 2019. Dostupné z: <https://www.zabbix.com/documentation/3.4/manual/config> >.
- [18] MS Hyper-V. Description [online]. Microsoft, 2019. Dostupné z: <https://blogs.technet.microsoft.com/technetczsk/p/microsoft-hyper-v/> >.
- [19] MS Hyper-V. How to add network adapters [online]. Altara, 2017. Dostupné z: <https://www.altaro.com/hyper-v/hot-addremove-network-adapters-hyper-v-2016/> >.
- [20] DHCP. Reservation [online]. Tech-FAQ, 2011. Dostupné z: <http://www.tech-faq.com/dhcp-reservation.html> >.

## Zoznam symbolov, veličín a skratiek

Obr	Obrázok
Tab	Tabuľka
IT	Informačné Technologie
CPU	Central Processor Unit (centrálne procesorová jednotka)
PLC	Logický kontrolér alebo tiež samotný automat
CLI	Command Line Interface
WMI	Windows Management Instrumentation
SNMP	Simple Network Management Protocol
SMS	Short Message Service
HTML	Hyper Text Markup Language
CSS	Cascading Style Sheets
RAM	Random Access Memory
GB	Gigabyte
API	Application Programming Interface
IP	Internet protocol
MIB	Management Information Base
PHP	Hypertext Preprocessor
ICMP	Internet Control Message Protocol
IPMI	Intelligent Platform Management Interface
JMX	Java Management Extensions
GPL	General Public License
ITU-T	Telecommunication Standardization Sector of the International Telecommunications Union
ISO	International Organization for Standardization
OID	Object identifier
TCP/IP	Transmission Control Protocol/Internet Protocol

# Zoznam príloh

A	Tabučky rezervácií na DHCP serveri	65
A.1	Tabučka rezervácií prepínačov . . . . .	65
A.2	Tabučka rezervácií prvkou vo výrobe . . . . .	66
A.3	Tabučka rezervácií kamier . . . . .	66
A.4	Tabučka rezervácií tlačiarň . . . . .	67
A.5	Grafy . . . . .	68
A.5.1	Grafy z prepínača SW01 . . . . .	68
A.5.2	Grafy z prepínača SW02 . . . . .	69

## A Tabu©ky rezervácii na DHCP serveri

### A.1 Tabu©ka rezervácii prepínačov

Tab. A.1: Tabu©ka rezervácii prepínačov

Zariadenie	MAC adresa	IP adresa	Hostite©ský názov
HP ProCurve 3500yl-24G	192.168.1.254	0021f71c5240	sw01
HP ProCurve 3500yl-24G	192.168.1.253	00234758f780	sw02
Cisco SG200-50	192.168.1.252	a0554 a3606	sw03
HP 1810-24G	192.168.1.251	8851FBBB38A0	sw-laborator
Cisco WS-C3750-s12	192.168.1.250	0025839edc40	sw05
Cisco SG200-26P	192.168.1.249	bcf1f20109d7	sw-varna
Cisco SF200-18	192.168.1.248	38ed185d7a1f	sw-sladvna
Cisco SF300-28	192.168.1.247	c800849833c3	sw-stexpedice
Cisco SG300-10MPP	192.168.1.246	5006ab35a732	sw-spilka
Cisco SF200-18	192.168.1.245	38ed185d9e21	sw-ckt
Cisco SF302-08	192.168.1.244	00e16d90e50c	sw-prodejna
Cisco SF302-08	192.168.1.243	00562B1E8B2A	sw-stexpedice02
Cisco SF302-08	192.168.1.242	50f722f5ef8d	sw-sladvna02
Cisco SF300-24	192.168.2.250	0cf5a4b8f32b	swhk-01
CiscoSF302-8	192.168.2.251	6899cdd8e2c1	swhk-02

## A.2 Tabuľka rezervácií prvkou vo výrobe

Tab. A.2: Tabuľka rezervácií prvkov vo výrobe

IP adresa	Hostiteľský názov	Popis
192.168.3.50	plc-varna	PLC Varna
192.168.3.52	plc-vasnicarna	PLC Kvasnicarna
192.168.3.53	plc-ckt	PLC Ckt
192.168.3.54	plc-chlazeni01	PLC Chlazení01
192.168.3.55	plc-chlazeni02	PLC Chlazení 02
192.168.3.56	plc-chlazeni03	PLC Chlazení 03
192.168.3.57	plc-chlazeni04	PLC Chlazení 04
192.168.3.70	pc-varna01	PC Varna

## A.3 Tabuľka rezervácií kamier

Tab. A.3: Tabuľka rezervácií kamier

Zariadenie	MAC adresa	IP adresa	Hostiteľský názov
CP-UNC-TY20L2	14070802C7DF	192.168.5.58	cam-spilka01
CP-UNC-TP10L2C-V2	1407080649c1	192.168.5.59	cam-prod-sklad
CP-UNC-V4142EL3	1407080A90A8	192.168.5.63	cam-varna
CP-UNC-TP10L2C-V2	140708064874	192.168.5.64	cam-spilka02
CP-UNC-T2322L4	1407080b7d11	192.168.5.66	cam-vjezd
CP-UNC-T2322L4	1407080858d2	192.168.5.67	cam-prod-vchod
CP-UNC-DA20L3S-0280	1407081e97bc	192.168.5.69	cam-stexpedice01
CP-UNC-EE40-M	14070816a900	192.168.5.70	cam-stexpedice02
CP-UNC-DA20L3S	1407081e97a1	192.168.5.71	cam-stexpedice03
CP-UNC-TP1PFL3C-V2	1407080c938c	192.168.5.72	cam-dvur-vjezd
CP-UNC-TA13L3	1407080DF966	192.168.5.74	cam-bocni-plot

## A.4 Tabu©ka rezervácii tla©iarní

Tab. A.4: Tabu©ka rezervácii tla©iarní

Názov tla©iarne	Hostiteľský názov	IP adresa	MAC adresa
EpsonFX890	PRN-EFX890	192.168.1.50	0030C1D4F4A7
HP Color Laser-Jet CM1312	PRN-HPLJCM1312	192.168.1.51	00215ae4032f
HP Laser Jet 1100-01	PRN-HPLJ1100-01	192.168.1.53	0010835938B2
HP Laser Jet 1100-02	PRN-HPLJ1100-02	192.168.1.54	0001E6541E06
HP Laser Jet 1300	PRN-HPLJ1300	192.168.1.55	0030C1D3F74A
HP Laser Jet 1320	PRN-HPLJ1320	192.168.1.56	00143898FDC3
Samsung SL-M2825ND	prn-sam-M2825ND	192.168.1.57	8425192d7083
Konica Minolta bizhub 4422	prn-bizhub4422	192.168.1.60	AAFM021004632
HP Laser Jet 1320-07	PRN-HPLJ1320-07	192.168.1.63	00110AC14838
HP Laser Jet 1320-08	PRN-HPLJ1320-08	192.168.1.64	00170889EBD7
HP Laser Jet 1320-09	PRN-HPLJ1320-09	192.168.1.65	0030c1d4f4a8
Konica Minolta C220	PRN-C220	192.168.1.67	00206B65E67A
Samsung M267x 287x Series	prn-Sam-M2675fn	192.168.1.68	30CDA72D227E
Konica Minolta C287	prn-km-c287	192.168.1.69	00206ba32253
Godex EZPI-1200	prn-godex1200	192.168.1.73	0011E50140A8
Samsung SL-M2825ND	prn-sam-M2825-02	192.168.1.74	8425192D6f5C
Konica Minolta bizhub 4020	prn-km4020-01	192.168.1.133	0021B7F53C98

## A.5 Grafy

### A.5.1 Grafy z prepínača SW01

Obr. A.1: Prepínač SW01 - využitie pamäte

Obr. A.2: Prepínač SW01 - sieťová premávka interface1

Obr. A.3: Prepínač SW01 - sieťová premávka interface5 (private)

Obr. A.4: Prepínač SW01 - sieťová premávka interface12 (wi )

## A.5.2 Grafy z prepínača SW02

Obr. A.5: Prepínač SW02 - využitie pamäte

Obr. A.6: Prepínač SW02 - sieťová premávka Trunk1

Obr. A.7: Prepínač SW02 - sieťová premávka interface2

Obr. A.8: Prepínač SW02 - sieťová premávka interface12 (wi )