UNIVERZITA PARDUBICE
Fakulta elektrotechniky a informatiky

Analýza dohledových systémů pro datové sítě

Bc. Ondřej Mařík

Diplomová práce
2013

Univerzita Pardubice
Fakulta elektrotechniky a informatiky
Akademický rok: **2012/2013**

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Ondřej Mařík**
Osobní číslo:	**I10396**
Studijní program:	**N2646 Informační technologie**
Studijní obor:	**Informační technologie**
Název tématu:	**Analýza dohledových systémů pro datové sítě**
Zadávající katedra:	**Katedra softwarových technologií**

Zásady pro vypracování:

Cílem práce je provést analýzu dostupných dohledových systémů, vytvořit metodiku na jejich komparativní analýzu, vyhodnotit získané údaje. Cílem teoretické části je podrobně popsat principy dohledových systémů datového provozu, vyspecifikovat zásadní vlastnosti pro provedení komparativní analýzy a sestavit metodiku pro jejich analýzu. V implementační části se autor zaměří na nasazení vybraných dohledových systémů, zpracuje analýzu jejich nasazení v laboratorních podmínkách FEI UPCE a získá reálná data pro vyhodnocení metodiky z teoretické části.

Rozsah grafických prací:

Rozsah pracovní zprávy:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

MARCHETTE. Computer intrusion detection and network monitoring. 2. vyd. S.l.: Springer, 2012. ISBN 978-144-1929-372. JOHNSON, Robert Bern. Evaluating the Use of SNMP as a Wireless Network Monitoring Tool for IEEE 802.11 Wireless Networks. 1. vyd. US: Proquest, Umi Dissertation Publishing, 2011. ISBN 9781243444820. SUBRAMANIAN, Mani a With contributions from Timothy A.N WITH CONTRIBUTIONS FROM TIMOTHY A. GONSALVES. Network management principles and practice. Noida (India): Dorling Kindersley, 2010. ISBN 978-813-1727-591.

Vedoucí diplomové práce: **Mgr. Josef Horálek**
Katedra softwarových technologií

Datum zadání diplomové práce: **31. října 2012**
Termín odevzdání diplomové práce: **17. května 2013**

Univerzita Pardubice Česká republika

L.S.

prof. Ing. Simeon Karamazov, Dr.
děkan

prof. Ing. Antonín Kavička, Ph.D.
vedoucí katedry

V Pardubicích dne 15. listopadu 2012

Prohlášení autora

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

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne 23. 08. 2013 Bc. Ondřej Mařík

Poděkování

Na úvod této práce bych chtěl poděkovat za obrovskou trpělivost a pomoc vedoucímu práce, Ing. Josefu Horálkovi. Dále bych chtěl poděkovat mým rodičům za podporu, kterou mi během celého studia a psaní této práce poskytovali.

Anotace

Tato diplomová práce se zabývá výběrem vhodného dohledového systému pro datovou síť menšího rozsahu. Součástí práce je výběr vhodných kandidátů, stanovení metodik pro jejich porovnání, testování a implementace na reálné a virtuální síti a na závěr vyhodnocení testů dle stanovené metodiky. Pro účely této práce byly vybrány dohledové systémy Cacti, Nagios XI, System Center Operations Manager 2012 a Zabbix.

Klíčová slova

Dohledové systémy, Cacti, Nagios, SCOM, Zabbix, srovnání, testování

Title

The analysis of monitoring systems for data networks

Annotation

The aim of this master thesis is choosing and comparison of monitoring systems for data network. The document also includes choosing of appropriate candidate systems, creating of methodic for its comparison and evaluation. For the purpose of the master thesis were chosen Cacti, Nagios XI, System Center Operations Manager 2012 and Zabbix.

Keywords

Monitoring systems, Cacti, Nagios, SCOM, Zabbix, comparison, testing

Obsah

Seznam zkratek

ARPANET	Advanced Research Projects Agency Network
CDP	Cisco discovery protocol
EIGRP	Enhanced interior gateway routing protocol
GNS	Graphical network simulator
IaaS	Infrastructure as a service
ICMP	Internet control message protocol
IP	Internet Protocol
IPMI	Intelligent platform management interface
ITIL	Information technology infrastructure library
LAN	Local area network
MAN	Metropolitan area network
MIB	Management information base
NCP	Network control program
NIC	Network interface card
OID	Object Identifier
OS	Operační systém
QoS	Quality of services
RFC	Request For Comments
RIP	Routing information protocol
SaaS	Software as a service
Site-to-Site VPN	Trvale připojená VPN realizovaná typicky mezi dvěma směrovači
SLA	Service level agreement
SNMP	Simple Network Management Protocol
SSH	Secure shell
TCP	Transmission Control Protocol

TTL	Time to live
UDP	User datagram protocol
USA	United States of America
VPN	Virtual private network
WAN	Wide area network
WMI	Windows management instrumentation

Seznam obrázků

Seznam tabulek

1 Úvod

Od doby, kdy Graham Bell v roce 1876 (Bellis, 2013) vynalezl první použitelný telefonní přístroj, uplynulo už přes 137 let. Za tu dobu zažilo lidstvo z technologického hlediska neuvěřitelný rozvoj. Kdysi velký a těžký přístroj dnes běžně nosíme v kapse a k tomu, abychom si zavolali, nemusíme být připojeni kabelem. Spolu s tím, jak se rozvíjela telekomunikační síť, začaly nároky uživatelů stoupat a v 50. letech 20. století proběhly první experimenty s propojováním počítačů.

Nejprve se jednalo o velmi malé sítě v laboratorních podmínkách, které se později vyvinuly v projekt ARPANET. Projekt, který byl z velké části financován ministerstvem obrany USA si dal za cíl vyvinout komunikační síť, která by nebyla závislá na jednom centrálním prvku a umožňovala by tok dat směrovat dynamicky podle aktuálního stavu sítě. To se částečně podařilo pomocí protokolu NCP, který byl pro tyto účely navržen a ARPANET tak začal růst. Ze začátku ARPANET propojoval nejvýkonnější počítače na několika vybraných univerzitách a jeho vrcholem bylo připojení Norska a Spojeného království Velké Británie. V průběhu rozvoje se nicméně ukázalo, že protokol NCP už přestával potřebám této sítě stačit, a tak v roce 1983 (Leiner , a další, 2013) došlo k jednomu z největších milníku v historii datových sítí – nasazení protokolu TCP/IP, který se používá pro řízení komunikace v datových sítí dodnes. Projekt ARPANET byl ukončen v roce 1990, kdy byla tato síť odpojena a jako jeho nástupce vznikla „síť sítí“, kterou dnes nazýváme internet.

S rozvojem počítačových sítí byla zahájena digitalizace i na straně telekomunikační infrastruktury. Z hlediska datových sítí tak najednou nebyl významný rozdíl mezi hlasovými službami a ostatním datovým provozem tudíž mohlo dojít k integraci těchto sítí. Aktuálně je tak největším rozdílem mezi telekomunikačními a počítačovými sítěmi v požadavku na rychlost a spolehlivost doručení dat.

Tím, jak se technologie vyvíjely, došlo k tomu, že se na nich lidstvo stalo závislé. Asi těžko si dnes někdo dokážeme představit život bez mobilního telefonu, připojení k internetu, televize, sociálních sítí apod. Stále víc a víc společností svůj obchodní model zakládá na existenci internetu a ten se tak pro ně stává hlavním zdrojem příjmů. Problém ovšem nastává v okamžiku, když dojde k výpadku kritické části infrastruktury, která zapříčiní její nedostupnost. V případě velkých e-shopů tak může dojít k obrovským finančním ztrátám za každou hodinu či minutu výpadku. Takovéto společnosti si to samozřejmě uvědomují. Proto vznikly systémy pro sledování a monitoring infrastruktury, které mají včas odhalit přicházející problémy a upozornit na ně zodpovědné uživatele.

Porovnání těchto systémů si autor diplomové práce vybral jako její téma. Autor se v práci zaměřuje hlavně na nasazení systémů jak v reálné síti, tak i v síti virtualizované, stanovení metodiky pro objektivní srovnání těchto systémů a vyhodnocení naměřených dat. Stěžejním bodem celé práce je implementace těchto systémů v reálné síti a získávání zkušeností s jejich každodenním provozem se zaměřením na pozorování chování systémů a jejich reakcí na výpadky, nestabilitu některých bezdrátových spojů a identifikace postižených částí sítě.

Výstupem této práce je autorovo doporučení (na základě získaných data a zkušeností pro implementaci) vhodného kandidáta za účelem dohledu menší datové sítě pro poskytování ICT služeb a konektivity do internetu.

1.1 Definice datových sítí

Jak bylo zmíněno hned v úvodu, pod pojmem datové sítě si můžeme představit množinu prvků, které dohromady tvoří infrastrukturu potřebnou pro přenos dat v rámci libovolné sítě a to bez ohledu na to, jestli se jedná o síť počítačovou nebo telekomunikační.

Datové sítě je možné rozdělit do několika kategorií podle vlastnosti, která je pro nás aktuálně relevantní:

Z hlediska přepojování

- **Komutační** – sítě založené na přepojování okruhů, typicky se jedná o telefonní sítě.
- **Paketové** – sítě založené na přepínání paketů, počítačové sítě

Z hlediska typu přenášeného signálu

- **Analogová** – síť, která přenáší analogový – spojitý signál
- **Digitální** – síť, která rozlišuje signál na dvou úrovních 1 a 0. Práh, kdy se jedná o nulu a kdy o jedničku, je závislý na přenosovém médiu.

Z hlediska geografického dosahu

- **LAN** – lokální síť s dosahem v rámci budovy, podniku, domácnosti apod. Dosah řádově stovky metrů až kilometry.
- **MAN** – metropolitní síť s dosahem v rámci jednoho města. Dosah řádově kilometry.
- **WAN** – co do rozlohy největší typ sítě, spojuje sítě LAN a MAN a má rozsah na úrovni států a kontinentů

Sítě LAN, MAN a WAN se také liší v běžně dosahovaných rychlostech přenosu dat. Nejvyšších rychlostí vzhledem k počtu uživatelů a velikosti investic se běžně dosahuje na sítích LAN, které aktuálně zažívají přechod ze 100 Mb spojů na 1 Gb spoje. Naopak nejnižších rychlostí dosahují sítě WAN, kde se vysokých rychlostí dosahuje za vynaložení vysokých investic. Je to dáno především tím, že tento typ sítí pracuje se spoji na dlouhé vzdálenosti a mnohdy také se spoji bezdrátovými. Tyto spoje jsou finančně velmi nákladné.

Tato práce se dále bude zaměřovat na paketové digitální sítě, které jsou v dnešní době nejvíce využívaným typem datových sítí.

2 Dohledové systémy

Dohledový systém je možné definovat jako prvek, který je implementován do monitorované sítě., a který Periodicky zjišťuje dostupnost a stav jednotlivých uzlů a spojů. V případě problémů nebo nedostupnosti některého prvku o této události informuje administrátora sítě. V některých případech je možné pomocí dohledového systému síť také aktivně řídit, tzn. můžeme nadefinovat postupy, které se budou provádět v případě, že se pro nás kritický uzel stane nedostupný. Záleží však na typu nasazeného dohledového systému, které obecně dělíme na tři typy. Dohledové systémy mohou být nasazeny jako aplikace na serveru (případ porovnávaných systému) nebo jako samostatné jednoúčelové zařízení.

2.1 Kategorie dohledových systémů

2.1.1 Základní dohledové systémy

Základní dohledové systémy pracují typicky na protokolu ICMP. Jedná se tak o systémy, které periodicky vyhodnocují pouze stav sledovaného prvku a jsou schopny poskytovat informaci o jeho dostupnosti pouze na úrovni dostupný/nedostupný, případně přidávají informaci o době jeho odezvy. Tento typ monitorovacího systému je vhodný pouze pro menší sítě typu LAN nebo u sítí, kde nám nejsou schopna sledovaná zařízení poskytnout více informací.

2.1.2 Pokročilé dohledové systémy

Pro větší počítačové sítě je mnohem výhodnější využít pokročilé dohledové systémy. Ty typicky pracují s více protokoly jako např. SNMP, CDP, SSH apod. To těmto systémům umožňuje sledovat prakticky všechny informace o zařízeních v síti jako je stav spuštěných služeb, vytížení systémových prostředků, aktuální datový tok apod. U serverů pak typicky využívají tyto systémy lokálně spuštěné agenty, kteří pomáhají shromažďovat data nedostupná pomocí síťových protokolů.

Tím, že mají tyto dohledové systémy mnohem více informací o dění na síti, mohou o nestandardních situacích informovat administrátory mnohem dříve, ve většině případů ještě před samotným výpadkem sledovaného zařízení. Tyto systémy dále mohou vyhodnocovat a identifikovat začínající útoky na sledovanou síť. Nasazením tohoto typu dohledového systému pak administrátor získá maximum možných informací o stavu sítě.

2.1.3 Proaktivní dohledové systémy

Proaktivní systémy jsou de-facto pokročilé dohledové systémy, které ale umí síťová zařízení i ovládat. Tyto systémy jsou vhodné typicky do vysoce automatizovaného prostředí, jako jsou datacentra, rozsáhlé sítě, vysoce dostupné clustery apod. Tyto systémy zažívají s rozvojem cloudových služeb velký boom a výrobci prakticky všech dohledových systémů se tomuto trendu začínají přizpůsobovat. Je to dáno především tím, že většina systémů umí implementovat automatizované scénáře, které reagují na předem dané události. Tím dochází k významnému snížením nákladů na správu sítě a zlepšení kvality poskytovaných služeb.

2.1.4 Systémy sledující datový tok

Samostatnou kategorií jsou pak síťové monitory, které pracují na bázi odposlechu veškeré komunikace probíhající na síti. Tyto systémy jsou však extrémně náročné jak na výkon, tak zejména na zázemí, které je nutné pro jejich nasazení.

Je to dáno především tím, že „odposlech“ síťové komunikace není možné provádět na jednom centralizovaném místě. Při nasazení těchto systémů jsou využívány „inteligentní“ přepínače, které umožňují zrcadlit veškerý datový tok i na další port, do kterého je připojena jednotka pro sběr dat. Některé systémy pak také využívají speciálních průchozích jednotek, které se zapojují přímo na přenosové médium.

Tyto jednotky v dávkách odesílají data do centrálního prvku, který se stará o jejich ukládání, analýzu a vizualizaci uživateli.

2.2 Architektury

I přes fakt, že každá datová síť je v podstatě unikátní, existuje obecná představa o běžně nasazované architektuře datových sítí s ohledem na robustnost, rychlost a spolehlivost přenosu dat. Tuto architekturu, nejlépe charakterizuje a popisuje spol. Cisco pod názvem Enterprise Campus 3.0 (Cisco Systems, Inc., 2008). Architektura se primárně zaměřuje na datové sítě v rámci jedné společnosti, ale její principy jsou využívány i v ostatních typech sítí. Moje práce se zaměří pouze na základní principy této architektury vhodné k pochopení architektur a umístění dohledových systémů. Kompletní popis architektury Enterprise Campus 3.0 lze nalézt v dokumentu Enterprise Campus 3.0 Architecture: Overview and Framework, který je uveden v seznamu použité literatury.

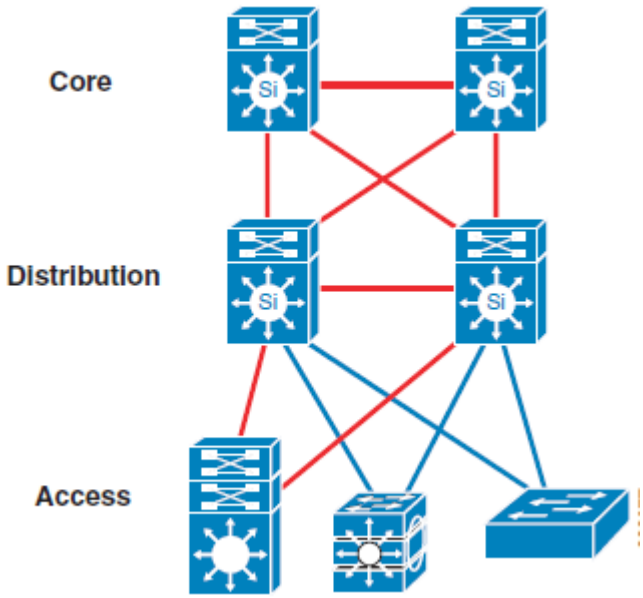
Principem této architektury je třívrstvá hierarchická síť uvedená na obrázku 1. Zavedení hierarchie a členění sítě do vrstev umožňuje a usnadňuje její budoucí růst a významně napomáhá k jednoduššímu směrování, adresaci a samostatnosti jednotlivých částí a bloků sítě.

Základní vrstvou je vrstva přístupová. Jde o místo, kde se sítí přichází do styku uživatel a je tak nutné na této vrstvě maximálně zabezpečit a omezit přístup do sítě nežádoucím uživatelům. Dochází zde k rozdělení uživatelů do příslušných VLAN, nastavení a aktivaci QoS apod. Tato vrstva je obvykle přepínaná, ale čím dál častěji také směrovaná díky L3 přepínačům.

Hlavním úkolem distribuční vrstvy je propojení jádra a přístupové vrstvy. Jejím účelem je agregace, izolace, řízení a omezení toku dat apod. Vrstva je typicky směrovaná, ale není zde kladen tak vysoký důraz na konvergenci.

Poslední vrstvou je vrstva jádra. Vrstva jádra nemá za úkol nic jiného, než co nejrychleji směrovat pakety a docílit tak maximálního možného výkonu. Zajímavostí je fakt, že na vrstvě jádra jsou zařízení konfigurována naprosto minimálně. Je to hlavně z důvodů rychlosti, kdy požadavkem na vrstvu není analýza datového toku, ale co nejrychlejší

doručení paketu. Dalším efektem vrstvy je navíc snadnější a méně nákladná rozšiřitelnost sítě, kdy odpadá nutnost spojení každý s každým v distribuční vrstvě. Výpadek na této vrstvě je kritický, proto je vyžadována vysoká konvergence.

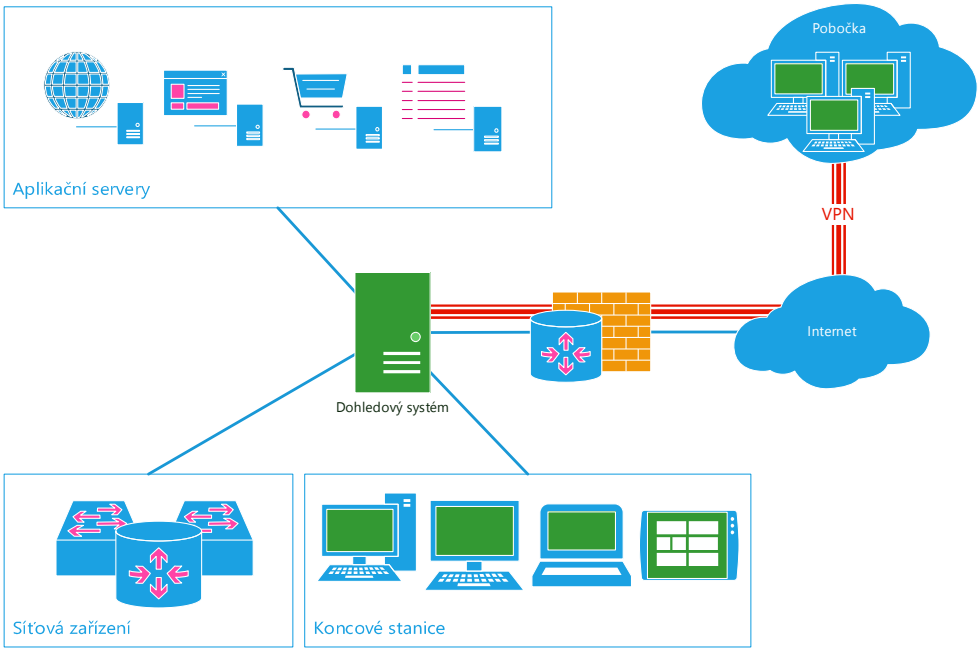


Obrázek 1 – Vrstvy architektury Enterprise Campus 3.0 (Cisco Systems, Inc., 2008)

Z pohledu dohledových systémů se jeví jako jedna z nejzásadnějších otázek jejich umístění ve sledované síti. Podle autorova názoru je logickým místem pro jeho umístění vrstva jádra, která by měla zajistit maximální dostupnost a zároveň dohledovému systému umožnit přístup ke všem prvkům v síti napříč vrstvami.

Při nasazení dohledového systému je nutné brát zřetel na velikost monitorované sítě a podle toho zvolit vhodnou architekturu. Obecně lze konstatovat, že se v dnešní době nejčastěji používají dvě architektury dohledových systémů – centralizovaná a federativní.

2.2.1 Centrální dohledový systém



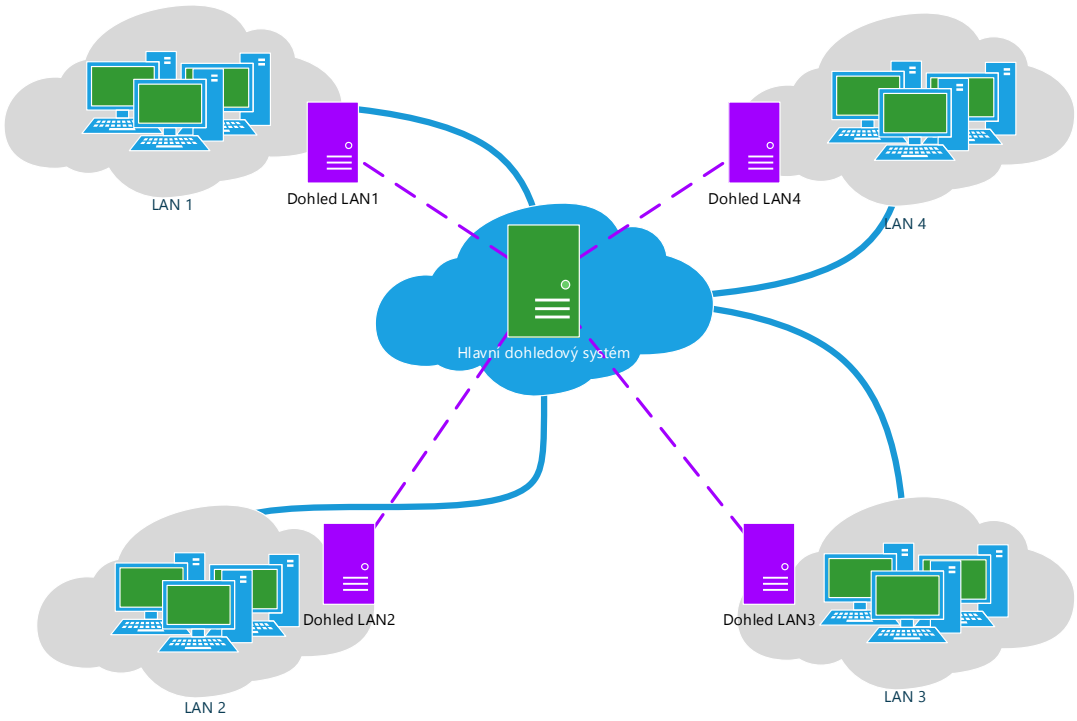
Obrázek 2 - Architektura centralizovaného dohledového systému

Základní architektura a nasazení dohledového systému je vhodné zejména pro menší sítě a sítě bez externích poboček. Dohledový systém je zde nasazen pouze na jednom serveru a sleduje prakticky celou síť. V případě, že je potřeba monitorovat i externí pobočku, využívá se ve většině případů site-to-site VPN.

Při využití této architektury je extrémně důležité zvolit vhodné umístění dohledového systému. Z logiky věci je nejvhodnější místo pro jeho připojení do sítě na jejím „středu“ (jádro sítě). Problém totiž nastává v tom, že v případě jednoho serveru není možné při výpadku segmentu sítě jeho přesná identifikace. Pokud bychom navíc dohledový systém připojili přímo do hraničního směrovače, který odděluje lokální síť od internetu, tak v případě, že by na daném zařízení došlo k výpadku, jednalo by se z hlediska dohledového systému o kompletní výpadek celé sítě, ale ve skutečnosti by v lokální síti nefungoval pouze přístup na internet.

Výhodou této architektury je snadnost a rychlost implementace. Nejrizikovějším a nejnáročnějším bodem její implementace je pak jednoznačně návrh umístění dohledového systému.

2.2.2 Federativní dohledový systém



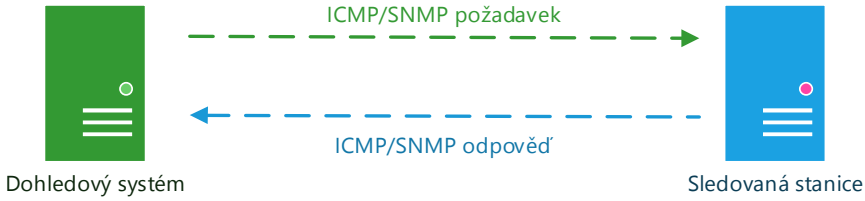
Obrázek 3 - Architektura federativního dohledového systému

Tato architektura je založena na segmentaci sledované sítě na menší části, které jsou monitorovány pomocí samostatných dohledových systémů. Tyto menší servery pak reportují veškeré informace o sítí z jejich pohledu centrálnímu dohledovému serveru. Centrální dohled pak na základě všech informací z pobočkových systémů může poměrně přesně reportovat postižený segment sítě. Při výpadku hlavního dohledového systému je i nadále možné získat data a informace z pobočkových systémů.

Tento typ architektury je vhodný zejména pro velké sítě nebo naopak pro poskytovatele služeb, kteří takto mohou sledovat sítě svých zákazníků a výstupy z hlavního dohledového systému pak prezentovat na svoje dohledové centrum. Nevýhodou této architektury je zejména fakt, že ne každý dohledový produkt umí takto pracovat. Samozřejmě také finanční a časová náročnost na implementaci je vyšší než u centralizované architektury. Mezi hlavním dohledovým systémem a pobočkami by mělo být opět zabezpečené spojení např. pomocí site-to-site VPN.

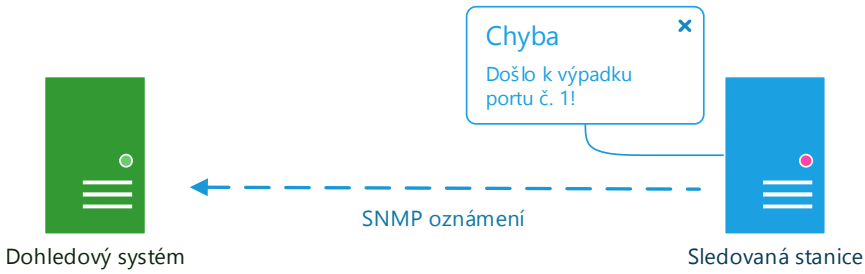
2.3 Způsoby sledování zařízení

Dohledové systémy pro získávání informací ze sledovaných zařízení využívají tři způsoby. Prvním je dotazování zařízení pomocí standardních protokolů jako je ICMP, TCP, SNMP apod. Tento způsob dotazování většinou nevyžaduje od sledovaného zařízení žádné větší zásahy do konfigurace mimo povolení výjimek ve firewallu. Zároveň se jedná o univerzální způsob získávání informací bez ohledu na výrobce a typ zařízení. Nevýhodou je pak jistá generalizace a nedostupnost některých specializovaných funkcí.



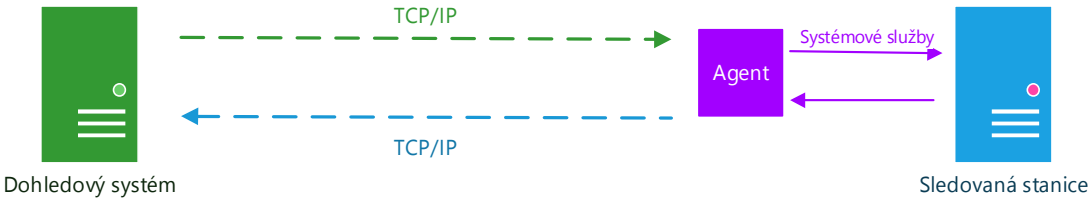
Obrázek 4 – Sledování zařízení pomocí síťových protokolů

Druhou možností je využívání SNMP oznámení tzv. SNMP trap. V tomto případě na rozdíl od první varianty nedochází k cyklickému dotazování ze strany dohledového systému, ale sledovaný prvek v případě, že nastane nějaká událost (chyba, výpadek na portu, zaplnění RAM apod.) zašle dohledovému systému zprávu, ve které dohledový systém o situaci informuje a ten pak na základě předaných informací provádí další akce. Tento způsob sledování se ve většině případů kombinuje s cyklickým dotazováním. Podrobněji se protokolem SNMP zabývá kapitola 2.4.4.



Obrázek 5 - Sledování pomocí SNMP trap

Třetí možností, jak dohledový systém získává data, je nasazení speciálního agenta na sledované zařízení. Ten pracuje na koncovém systému jako aplikace a s dohledovým systémem komunikuje na principu klient-server. Výhodou je, že nemusí být použit speciální síťový protokol, protože data se většinou přenášejí pomocí TCP/IP. Hlavním benefitem je pak možnost získávat detailní informace o sledovaném systému a v případě proaktivního dohledového systému také možnost sledovanou stanici ovládat. Tímto způsobem se typicky monitorují servery.



Obrázek 6 – Sledování zařízení pomocí instalovaného agenta

2.4 Používané protokoly

Jak bylo zmíněno v předchozí kapitole 2.3, dohledové systémy využívají pro svoji činnost řadu síťových protokolů. Ty nejdůležitější z nich jsou představeny v následující části práce.

2.4.1 IP

Protokol IP je základním protokolem pro komunikaci v počítačových sítích. Jeho specifikace je popsána v dokumentu RFC č. 791 (Information Sciences Institute University of Southern California, 1981) vydaném už v roce 1981. Jde tak o jeden z nejstarších protokolů, které se dnes běžně využívají.

Protokol IP poskytuje ostatním protokolům základní službu, která zajišťuje přenos paketů z jednoho uzlu sítě do druhého, nicméně negarantuje jejich doručení a ani nezaručuje pořadí, ve kterém do cílového uzlu dorazí. Dále tento protokol zabraňuje nestandardním situacím, jako je zacyklení apod. Pro to, aby bylo možné přenos realizovat, využívá protokol IP jednoznačné identifikátory pro každý uzel sítě, který je znám pod pojmem IP adresa. Tento identifikátor je ve veřejné síti unikátní pro celý svět a vzhledem k této skutečnosti muselo dojít k revizi tohoto protokolu. V současnosti je možné využívat dvě verze tohoto protokolu.

2.4.1.1 IPv4

Původní a současně nejrozšířenější verze protokolu. Pro adresaci je využito 32 bitových adres, což je zároveň současný největší problém tohoto protokolu. Internet totiž neustále roste a s tím, jak se připojují nová a nová zařízení, došlo k vyčerpání adresního prostoru. Z tohoto důvodů dochází k nasazení IPv6.

IPv4 datagram obsahuje dvě části: hlavičku, která má zpravidla 20 B, a datové části. Hlavička obsahuje informace o verzi IP protokolu, délku záhlaví, typu služby, informace o celkové délce datagramu, jeho identifikaci, příznaky, informaci o posunutí fragmentu od začátku datagramu, dobu životnosti TTL, protokoly vyšší vrstvy, kontrolní součet a adresu příjemce a odesílatele. Maximální velikost datagramu včetně dat je 65535 bytů.

2.4.1.2 IPv6

Relativně mladá verze protokolu IP řeší mnoho nedostatků verze předchozí. Vzhledem k tomu, že IPv4 adresy už na nejvyšší úrovni volné nejsou a metody vytváření podsítí a NAT

není možné aplikovat do nekonečna, přineslo IPv6 řešení pro zvětšení adresního prostoru a to tím, že se změnil způsob adresování na 128 bitové adresy. To přináší možnost adresovat až $3{,}4\times10^{38}$ síťových zařízení, což by v současné době umožnilo přidělit celosvětově unikátní adresu každému zařízení, které je aktuálně jakýmkoliv způsobem připojeno k internetu. Dá se tak předpokládat, že tato verze IP protokolu bude nasazena a využívána minimálně stejně tak dlouho jako IPv4.

Z hlediska hlavičky datagramů došlo k přesunu několika částí do volitelné sekce tak, aby hlavička obsahovala pouze ty nejnutnější informace. Nachází se v ní tak informace o verzi protokolu, třídě provozu, značka toku, délka dat, odkaz na následující hlavičku, informace o počtu skoků během směrování a adresy odesílatele a příjemce. Celková velikost hlavičky pak narostla na 40B přičemž celých 32B zaberou adresy příjemce a odesílatele.

S IPv6 samozřejmě přicházejí i nové servisní protokoly, a mechanismy, nicméně v současnosti ještě není IPv6 natolik rozšířené, aby bylo z hlediska této práce aktuální.

2.4.2 TCP

Dalším základním síťovým protokolem je protokol TCP, který je popsán v dokumentu RFC č. 793 (Information Sciences Institute University of Southern California, 1981). TCP je spojově orientovaný protokol pracující na transportní vrstvě ISO/OSI modelu. Jeho úkolem je zajistit potvrzené doručení paketů, které navíc budou ve správném pořadí. Tato vlastnost s sebou přináší značnou nevýhodu v nízké rychlosti procesu doručení dat. Je to dáno především tím, že pro každý přenesený paket je vyžadována značná režie na potvrzení, seřazení paketů apod., proto není použití tohoto protokolu vhodné pro všechny typy aplikací, jako je přenos videa, hlasu apod. Pro tyto potřeby se využívá jednoduššího a rychlejšího protokolu UDP, který je popsán v dokumentu RFC č. 768.

Protokol TCP je úzce spjatý s protokolem IP a dohromady tvoří základní komunikační sadu protokolů pro přenos dat v internetu.

2.4.3 ICMP

ICMP je servisní protokol jehož specifikace je popsána v dokumentu RFC č. 792 (Postel, 1981). Standardně neslouží k přenášení aplikačních dat, ale využívá se k hlášení chyb a šíření informací napříč sítí. ICMP zprávy se generují při chybových událostech jako je vypršení TTL, nedostupnost příjemce apod. Tyto informace jsou pro aktivní prvky sítě velmi důležité, protože pomocí nich mohou snadno přizpůsobovat svoje chování. ICMP zprávy ve všech případech putují po síti zabalené do jednoho IP datagramu, což značně celou komunikaci zrychluje a zjednodušuje. Mezi často používané zprávy patří např. echo request, echo reply, destination unreachable, time exceed a redirect.

Protokol ICMP také využívá mnoho utilit sloužící pro administraci a testování sítí. Typickým příkladem takovéto utility je příkaz traceroute, který periodicky posílá zprávu echo request (ping) s postupně inkrementovaným TTL. V okamžiku, kdy datagram narazí na směrovač, který TTL nastaví na 0, odešle se do stanice ICMP zpráva o nedoručitelném

paketu. Utilita pak pomocí těchto zpráv dokáže sestavit cestu ke sledovanému cíli. Dohledové systémy typicky využívají ICMP pro základní testování sledované sítě.

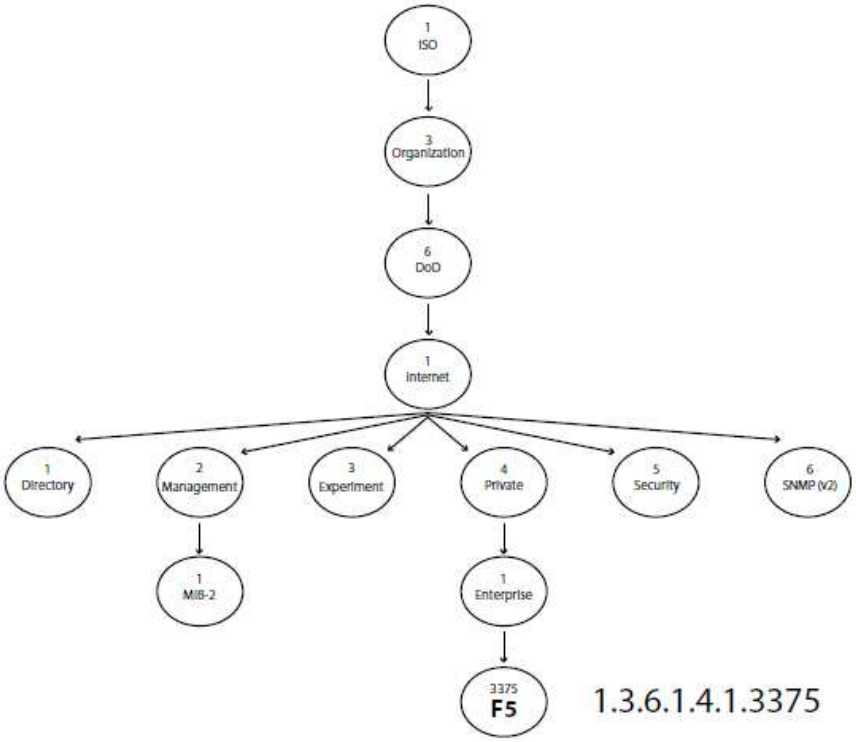
2.4.4 SNMP

SNMP je protokol navržený speciálně pro správu a dohled síťových zařízení, který je popsán v dokumentech RFC č. 3411 - 3418. Z pohledu ISO/OSI modelu se SNMP protokol pohybuje na vrstvě aplikační a princip jeho funkcionality je velmi podobný jako sledování serveru s nainstalovaným dohledovým agentem popsaným v kapitole 2.3.

Ještě než bude přikročeno k popsání mechanismu sledování, je nutné vymezit několik základních pojmů souvisejících s tímto protokolem:

OID – jednoznačný identifikátor SNMP hodnoty. Jedná se o posloupnost čísel oddělených tečkou. Příkladem OID může být řetězec 1.3.6.1.4.1.3375.

MIB databáze – databáze obsahující informace pro rozklíčování OID. Má stromovou strukturu a každé číslo OID představuje jednu úroveň databáze. Lze v ní tak snadno dohledat informace o příchozí zprávě, ale její existence není požadavkem pro využívání SNMP protokolu. Příklad rozklíčování OID je uveden na obrázku 7.



Obrázek 7 – Příklad OID hodnoty a jejího rozklíčování v MIB databázi (Murray, a další, 2008)

PDU – identifikátor typu SNMP zprávy. Zprávy se dělí do dvou hlavních kategorií *GET* a *SET*. PDU tak může nabývat následujících hodnot - GetRequest, GetNextRequest,

SetRequest, GetResponse, GetBulk, Inform a SetRequest. Dalším typem zpráv je SNMP Trap, ale tento typ zprávy využívá odlišný formát rámce a je zasílán na jiném portu.

Komunita – protokol SNMP definuje dvě úrovně přístupu k informacím. Tyto úrovně se nazývají komunita a dělí se na veřejnou a privátní. Veřejná komunita umožňuje pouze čtení informací, zatímco privátní umožňuje i jejich zápis. S pojmem komunita souvisí také komunitní heslo, které omezuje přístup k SNMP informacím pouze pro autorizované dohledové servery.

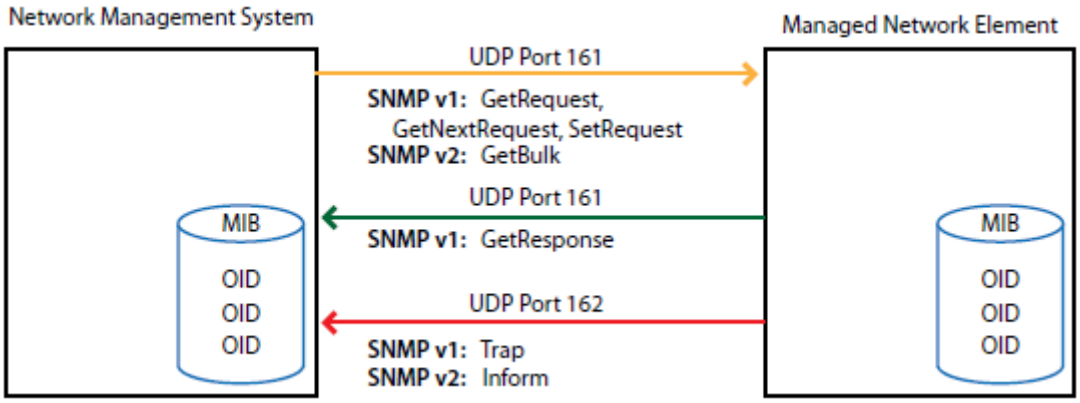
Obrázek 8 – struktura SNMP paketu typu požadavek/odpověď (Bouška, 2013)

Obrázek 9 – struktura paketu SNMP trap (Bouška, 2013)

Princip funkce protokolu SNMP je následující. Na straně sledovaného zařízení je spuštěn SNMP agent, který přijímá SNMP požadavky od SNMP serveru. Tím je v případě této práce nasazený dohledový systém. Tyto požadavky mají nastaveno odpovídající PDU a jsou zasílány protokolem UDP na portu 161. Agent ze zprávy získá OID hodnotu a podle typu požadavků jí buď nastaví, anebo do odpovědi přiloží získaná data. Pokud agent požadavek vyhodnotí jako oprávněný – je od autorizovaného zdroje a obsahuje správné komunitní informace, pošle danému serveru zpět SNMP odpověď, odpovídající požadované OID hodnotě. SNMP server přijme od sledovaného prvku SNMP odpověď a za pomoci MIB rozhodne o dalším kroku.

V případě, že je nastaveno využívání SNMP oznámení (SNMP trap), musí být v daném zařízení nakonfigurovány základní informace o tom, komu oznámení adresovat. Sledované zařízení pak zasílá na UDP portu 162 zprávy nastaveným serverům. Ty jakmile tuto zprávu obdrží, provedou definovanou akci založenou na kategorii a obsahu zprávy. Mezi SNMP oznámeními a standardními zprávami je také kromě využívaného UDP portu rozdíl ve struktuře zasílaných paketů. Ta je znázorněna na obrázcích 8 a 9. Za povšimnutí stojí počet položek, který je nutné ve zprávě typu oznámení evidovat.

Celý proces komunikace je pak přehledně znázorněn na obrázku 10, na kterém jsou vyznačeny i komunikační rozdíly mezi SNMP v1 a SNMP v2. Aktuálně je nicméně možné využívat protokol SNMP ve třech verzích.



Obrázek 10 – Komunikační mechanismus protokolu SNMP (Murray, a další, 2008)

SNMP v1

— První implementace protokolu. Pro ověřování, zda je zdroj požadavku autorizovaný využívá komunitní heslo – jednoduchý textový řetězec, který není zasílaný šifrovaný.

SNMP v2

— Významné zlepšení v oblasti výkonu protokolu a získávání velkého množství dat. Při specifikaci bohužel nebyly zohledněny požadavky na vyšší zabezpečení protokolu a tak v této oblasti nedošlo k rapidnímu zlepšení. Tato verze SNMP není s první verzí zpětně kompatibilní, protože došlo ke změně formátu zasílaných zpráv. Určité kompatibility lze dosáhnout za pomoci proxy agentů.

SNMP v3

— Opět zlepšení výkonu protokolu a hlavně významné zlepšení zabezpečení. Verze 3 přináší možnost ověřování jménem a heslem a zároveň je možné celou komunikaci šifrovat.

2.4.5 Ostatní protokoly

Výše uvedené protokoly jsou základní sadou pro každý dohledový systém. Některé technologie využívají protokoly svoje vlastní, specializované. Mohou využívat např. protokol CDP (využívá Cisco), anebo LLDP (standardizovaný protokol). Oba tyto protokoly jsou využívané síťovými zařízeními pro vyhledávání sousedních zařízení na lokální síti a dohledový systém je může využívat k zjišťování topologie sítě.

Mezi další způsoby jak monitorovat síťová zařízení patří rozhraní WMI pro stanice a servery s OS Windows, které poskytuje pomocí dotazů do WMI databáze prakticky všechny informace o dané stanici. Dále standardizované rozhraní IPMI, které vyvinula společnost Intel a je dnes běžně používané velkými výrobci hardwaru jako jsou společnosti Cisco, Dell, HP, NEC a v neposlední řadě Intel.

Způsobů jak sledovat síťová zařízení je samozřejmě mnohem více a s nadsázkou by se dalo říct, že prakticky každý výrobce hardware má svůj vlastní specializovaný způsob ať už např. přes SSH, anebo přes specializované rozhraní/protokol.

2.5 Bezpečnost dohledových systémů

Zabezpečení dohledového systému a sledované sítě by mělo být vždy naší hlavní prioritou. Je nutné si uvědomit fakt, že nasazením dohledového systému dojde k centralizaci veškerých informací o provozu a stavu sledované sítě na jedno místo a v případě, že by útočník k dohledovému systému získal přístup, mohl by nerušeně sledovanou síť ovládat a odposlouchávat.

Při nasazení by tak měl být brán zřetel zejména na nastavení zabezpečeného přihlašování, omezování přístupu k dohledovému systému pouze z vybraných pracovních stanic a IP adres, využívání šifrovaných komunikačních protokolů při sběru dat ze síťových prvků, a pokud to sledovaná zařízení umožňují, využít SNMP protokol verze 3. Samozřejmostí by pak mělo být zabránění fyzického přístupu jak ke sledovaným zařízením, tak k samotnému dohledovému systému.

3 Výběr a představení vybraných dohledových systémů

Jak už bylo zmíněno v úvodní kapitole, cílem této práce je otestovat a vybrat vhodný dohledový systém pro síť menšího rozsahu, který by nicméně dovoloval využití pokročilých funkcí jak pro správu síťových zařízení, tak i aplikačních a virtualizačních serverů. Primárně se tato práce zaměřuje na systémy vhodné pro správu a dohled sítě a nikoli pro sledování a analýzu toku dat, které sítí procházejí.

Pro dosažení stanoveného cíle bylo jako první krok zvoleno vyhledávání vhodných kandidátních systémů. Vyhledávání primárně proběhlo pomocí internetu, vyhledáváním v odborném tisku a konzultacemi s odborníky se zkušenostmi s velkými sítěmi a datovými centry. Při vyhledávání byl kladen důraz zejména na použitelnost, reference, vývojářskou základnu a samozřejmě také na to, aby byly ve výsledném výběru zastoupeny jak volně dostupné systémy, tak i ty komerční.

Výsledkem bylo vytipování těchto systémů: Nagios XI, Cacti, Zabbix, Microsoft System Center 2012 Operations Manager (dále jen SCOM 2012), IBM Tivoli, a Cisco OP Manager. Bohužel při pokusu o získání testovacích verzí muselo být zamítnuto řešení od IBM, které je implementačně příliš náročné a nebylo možné ho v testovacích podmínkách realizovat neboť samotné nasazení by vydalo na samostatnou práci. Dále musel být vyřazen komerční produkt Cisco OP Manager, protože jeho výrobce odmítnul poskytnutí testovací verze pro testovací a srovnávací účely. Rozhodnul jsem se tak v práci dále pokračovat pouze se dvěma volně dostupnými systémy – Cacti a Zabbix, a dvěma systémy komerčními – Nagios XI a SCOM 2012.

Všechny vybrané systémy splňovaly základní požadavky na hledané řešení – dostupnost, pokročilé sledování sítě, podpora různých typů zařízení.

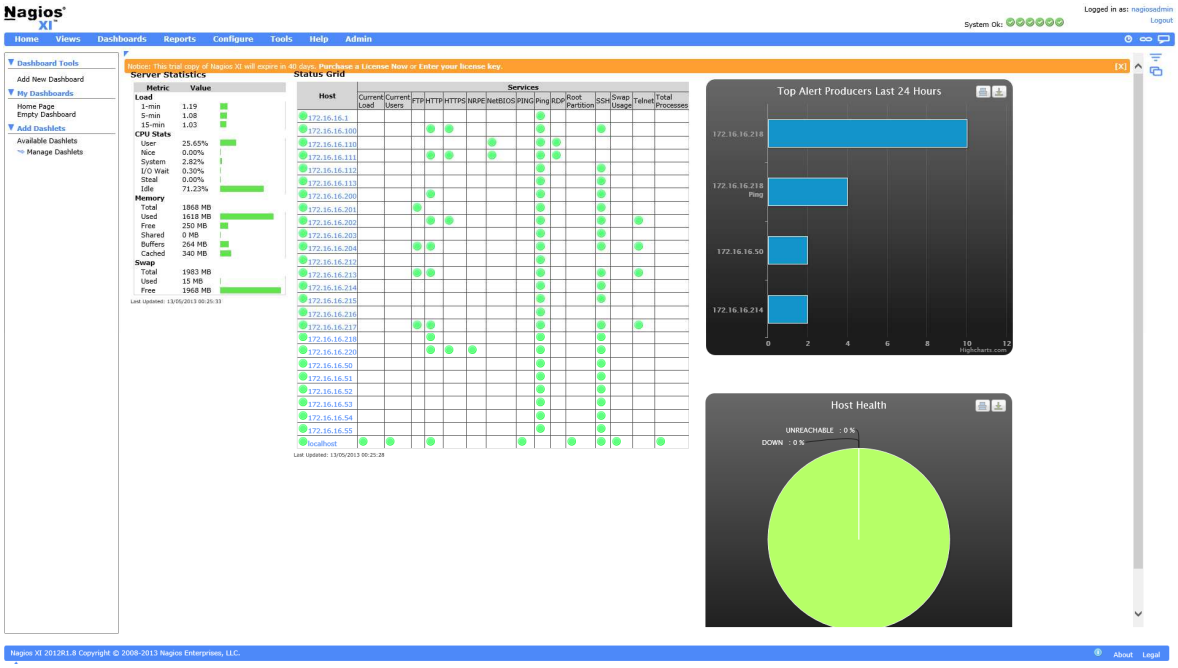
3.1 Nagios XI

Nagios, za jehož vývojem stojí společnost Nagios Enterprises, je jedním z nejpopulárnějších dohledových systémů na světě. Jeho první verze byla vydána v roce 1999 a v současnosti ho využívají tisíce uživatelů a společností po celé planetě.

Jeho obliba je dána především tím, že je založen na modulární architektuře a open source běhovém prostředí, takže je velmi snadné přizpůsobit si ho svým potřebám. Základní jádro je navíc distribuováno zcela zdarma, nicméně obsahuje pouze samotný dohledový mechanismus a jakoukoliv další funkci, kterou bychom chtěli implementovat, je nutné doinstalovat jako samostatný modul. V základní instalaci jádra navíc není obsaženo ani konfigurační rozhraní a ani pokročilejší vizualizace dat. Konfigurace tak probíhá výhradně přes příkazový řádek a to není z dlouhodobého hlediska příliš pohodlné. Z těchto důvodů může být jeho prvotní nasazení zdlouhavé a obtížné.

Naštěstí je zde i druhá cesta, jak maximálně využívat Nagios bez nutnosti instalace a vyhledávání jednotlivých modulů, zdlouhavého prohledávání a testovaní dostupných

pluginů, kterých je celá řada a liší se jak kvalitou, tak také podporou ze strany vývojářů. Tou cestou je placená verze Nagios XI, která byla zvoleny i pro testovací účely této práce. Výhodou placené verze je ucelený balík dostupných nástrojů při zachování možnosti rozšiřitelnosti a přizpůsobení pro konkrétní síťové a aplikační řešení. Společnosti, které navíc zvolí placenou verzi, dostanou možnost kontaktovat technickou podporu. Proto se výběr tohoto uceleného balíku pro produkční prostředí jeví jako nejsmysluplnější.



Obrázek 11 – Ukázka uživatelského rozhraní systému Nagios XI

Po instalaci produktu dostane uživatel k dispozici kompletní webové rozhraní s množstvím doinstalovaných nástrojů pro reportování, zobrazování map, automatické skenování sítě apod. Systém je po instalaci plně připraven na monitorování síťových zařízení, aplikačních serverů a koncových stanic. Pro sledování a vyhodnocování dat ze serverů a koncových stanic je využíváno lokálního agenta, který je součástí instalace. Samozřejmostí je sledování služeb pomocí síťových protokolů (ICMP, SSH, TELNET, TCP, …).

Z hlediska architektury je možné Nagios XI nasadit jako centrální dohledový systém, nebo jako skupinu dohledových systémů s federativní architekturou.

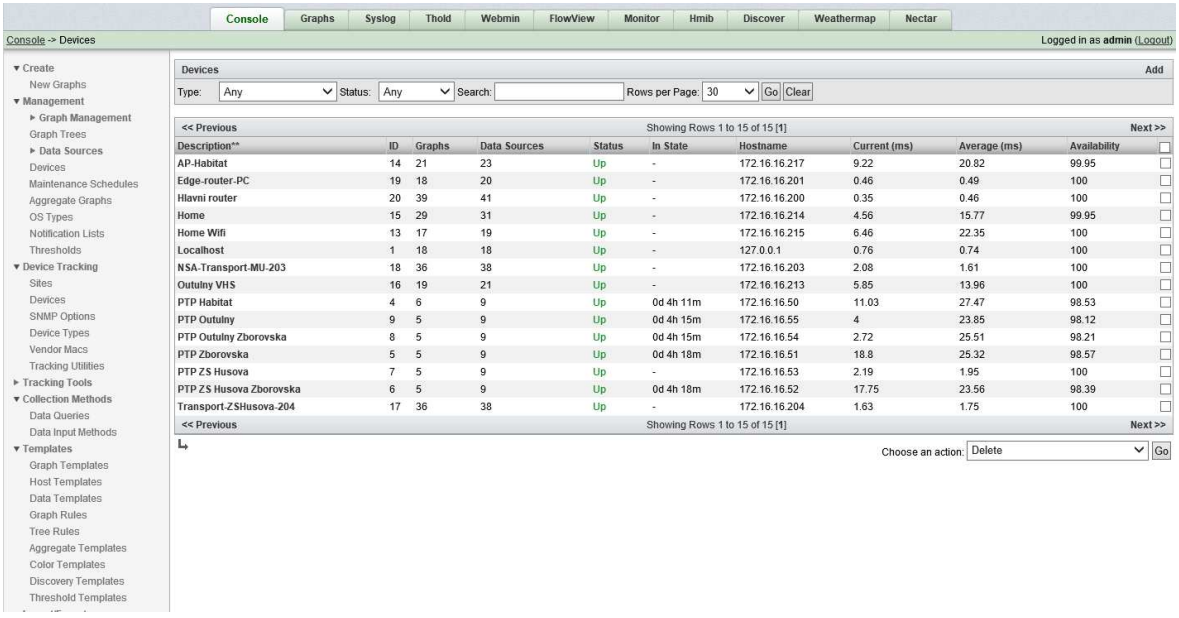
3.2 Cacti

Cacti je open source dohledový systém postavený na nástroji RRDTool. Tento nástroj byl speciálně vyvinut pro sběr a vizualizaci dat a je tak jeho využití pro dohledový systém více než vhodné. Cacti si, podobně jako Nagios, oblíbilo mnoho uživatelů po celém světě, nicméně vývojáři tohoto systému k dohledovému systému přistoupili trochu jiným

způsobem. Zatímco Nagios se snaží pracovat v reálném čase, Cacti se snaží pracovat primárně jako systém pro sběr a následnou analýzu dat. Sledování v reálném čase je zde až jako sekundární účel a upozornění na výpadky je uživateli prezentováno v řádech několika minut. Toto může být problém pro sítě, kde hodně záleží na dostupnosti. Nasazení tohoto dohledového systému na tento typ datové sítě nemusí být vhodné.

Na rozdíl od Nagiosu, nemá systém Cacti žádnou placenou variantu a jeho vývoj je závislý čistě na komunitě a koncovém uživateli. To s sebou přináší i jistá úskalí v podobě zdlouhavého nastavení pro konkrétní sledovaná zařízení, kdy je občas nutné složitě dohledávat a nastavovat parametry pro úlohy, zajišťující sběr dat. Nastavení se nicméně provádí přes webové rozhraní systému a tak je daný proces sice zdlouhavý, ale z hlediska uživatele alespoň pohodlný. Podobně jako u Nagiosu je i tento systém možné rozšířit o různé doplňky, které zajišťují nové funkce a vlastnosti systému jako je automatické rozpoznávání nových zařízení na síti apod. Za zmínku pak stojí ještě projekt jménem CactiEZ. Jde o upravenou linuxovou distribuci, po jejíž instalaci dostane uživatel k dispozici kompletní řešení včetně běžně nasazovaných doplňků a výrazně tak usnadňuje nasazení systému.

Z hlediska architektury je systém připraven spíše na centralizovaný dohled. Pro sledování aplikačních serverů je opět využito lokálních agentů, kteří slouží ke generování SNMP odpovědí na přijímané dotazy. Mezi podporované protokoly patří ICMP, TCP, UDP a SNMP.



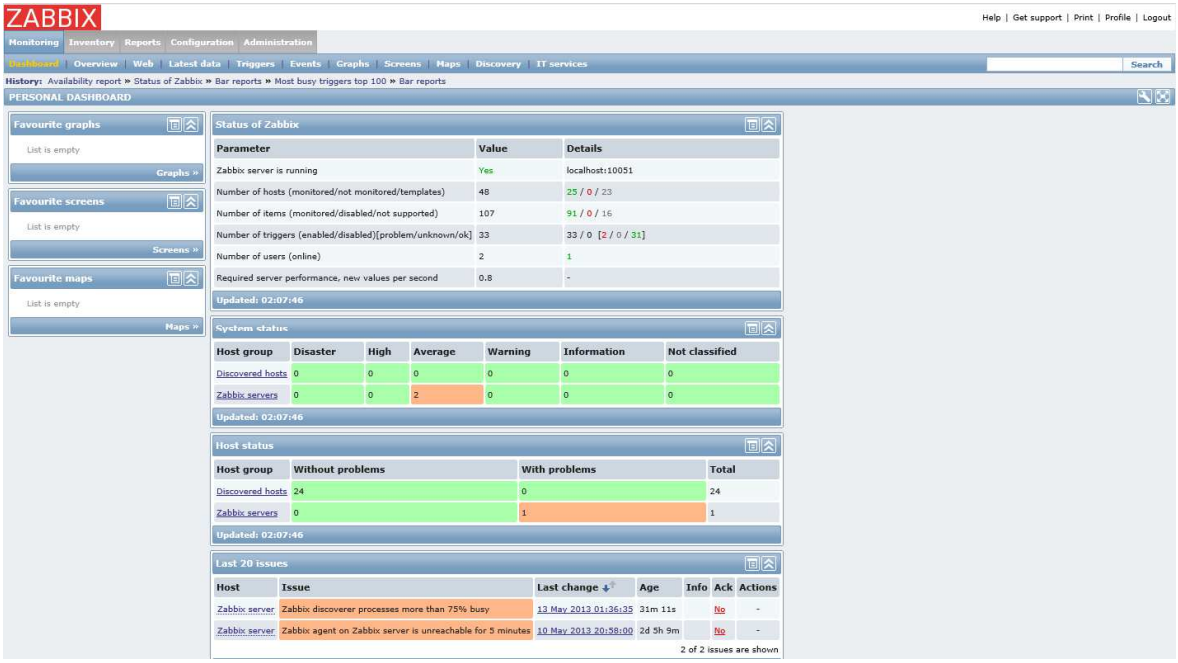
Obrázek 12 - Ukázka uživatelského rozhraní systému Cacti

3.3 Zabbix

Zabbix je dalším ze zástupců svobodného software, který je překvapivě výkonným a flexibilním řešením. Za jeho vývojem stojí tým Zabbix SIA a z hlediska možností nastavení a nasazení přináší funkce, které bychom u jiných open source produktů hledali jen těžko, anebo by byly dostupné ve formě placených doplňků.

Instalace celého systému je velmi snadná, protože vývojáři připravili instalační balíčky pro většinu používaných linuxových distribucí. Z hlediska sledování sítě je opět možné použití standardních síťových protokolů. Pro aplikační servery je pak připraveno mnoho lokálních agentů.

Pro správu systému má uživatel k dispozici webové rozhraní, které ale bohužel na první pohled nevypadá příliš přehledně a ani práce s grafy není příliš uživatelsky přívětivá. Naopak výhodou tohoto systému je možnost implementace SLA, evidence IT infrastruktury dle metodiky ITIL a mnoho dalších funkcí pro správu infrastruktury společnosti. Při nasazení Zabbixu je možné využít obou typů architektur – centralizovanou i federativní.



Obrázek 13 - Ukázka uživatelského rozhraní systému Zabbix

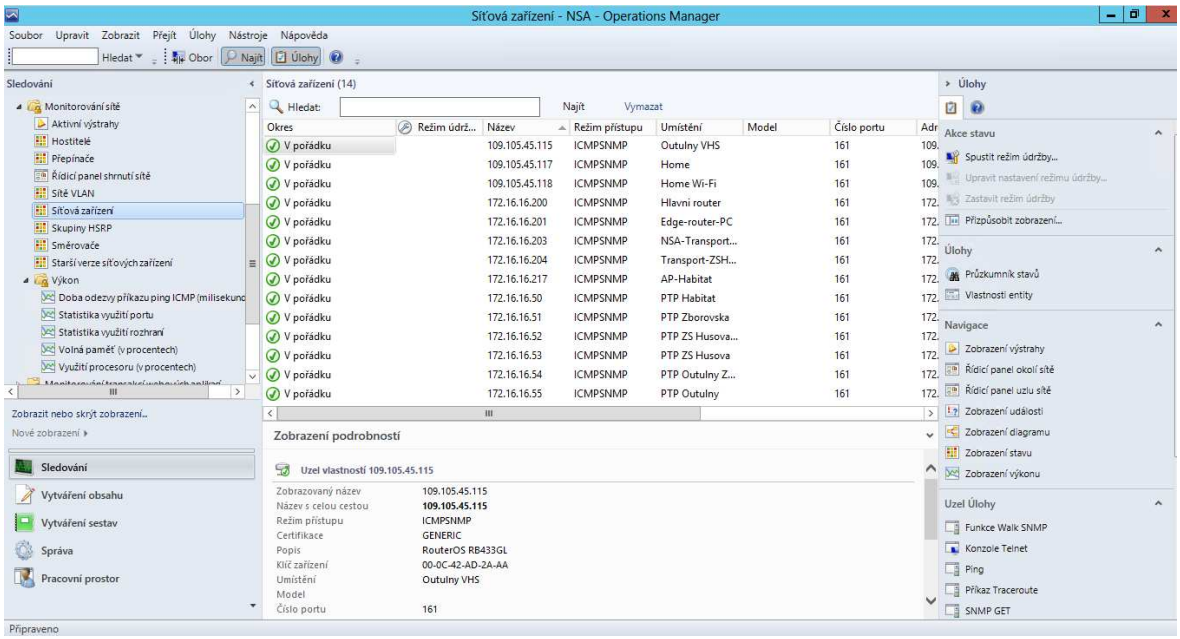
3.4 System Center Operations Manager 2012 (SCOM 2012)

SCOM 2012 je součástí nejnovějšího rodiny produktů společnosti Microsoft v oblasti správy, řízení a monitoringu IT infrastruktury, který se souhrnně nazývá System Center 2012. Dříve byl tento produkt zaměřen výhradně na velká enterprise prostředí nicméně s příchodem verze 2012 a současným rozvojem IT i v menších společnostech, dostává smysl implementovat tyto produkty i v těchto prostředích. Nasazením celé rodiny produktů pak

společnost získává kompletní kontrolu nad IT a to od řízení nakládání s daty přes správu virtualizačních a aplikačních clusterů, síťových prvků až po interní helpdesk. Nedílnou výhodou je, že jsou tyto nástroje proaktivní, a tak je možné připravovat automatizované scénáře.

Tím, že je SCOM jenom jednou součástí velkého řešení, je nutné při jeho nasazení využít poměrně výkonný hardware a to zejména kvůli databázovému serveru MS SQL, který je pro jeho běh nutný. K administraci celého systému je uživateli k dispozici speciální administrační konzole ve formě aplikace a webové rozhraní.

Pro sledování síťových zařízení systém využívá standardní síťové protokoly jako je ICMP a SNMP a pro aplikační servery je využito nativních agentů. Z hlediska architektury jsou dostupná obě řešení – centralizované i federativní.



Obrázek 14 - Ukázka uživatelského rozhraní systému SCOM 2012

4 Metodika testování dohledových systémů

Pro to, aby bylo možné objektivně otestovat a porovnat zvolené systémy, je nutné stanovit hodnotící kritéria a způsoby vyhodnocování dat. Pro účely této práce se autor rozhodnul pro každé hodnotící kritérium sestavit samostatný žebříček a v daném ohledu nejlepší systém ohodnotit 3 body. Ostatní dohledové systémy pak získali vždy o bod méně, než systém před nimi. V případě, že by v některém žebříčku zůstalo více systémů na stejné pozici, bude všem systémům přidělen nejvyšší možný bodový příděl.

Takto sestavené hodnocení by mělo být podle mého názoru dostatečně průkazné, aby bylo možné za jeho pomoci zvolit nejvhodnější software.

4.1 Hodnotící kritéria

4.1.1 Cena

V okamžiku, kdy se budeme rozhodovat o tom, který dohledový systém nasadit bude vždy jedno z našich nejzásadnějších kritérií cena. Bohužel je to právě cena, která bývá až příliš přeceňována a valná většina společností neumí tento parametr správně vyhodnotit. Cenu by totiž měla být vyhodnocována vždy poměrově k tomu, co nám daný systém přinese a kde nám ušetří náklady na práci nebo zefektivní procesy.

Pro účely této práce je však velmi obtížené tyto benefity uchopit, proto jsem se rozhodnul, že systémy srovnám pouze pomocí prostého seřazení.

4.1.2 Systémové nároky

Kritérium hodnotící minimální požadavky pro spuštění systému a to jak z hlediska výkonu, tak také z hlediska podpůrných aplikací. Parametry pro hodnocení tohoto kritéria byly převzaty z dokumentace k jednotlivým systémům.

4.1.3 Uživatelské rozhraní

Asi nejméně vypovídající kritérium. Je to dáno především tím, že vzhled a práce s uživatelským rozhraním je natolik subjektivní záležitost, že objektivní hodnocení prakticky nelze získat. Autor se přesto pokusil systém z tohoto úhlu pohledu zhodnotit a to zejména z pohledu vizualizace sítě, zobrazování výstupních grafů a celkového uživatelského komfortu.

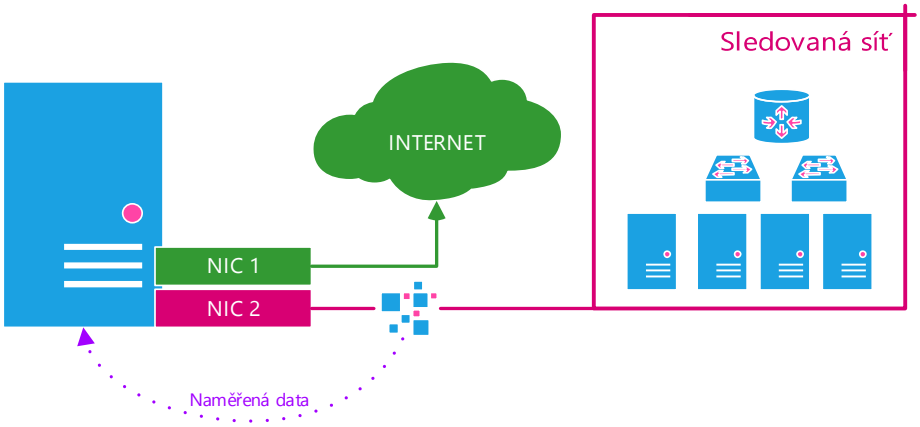
4.1.4 Náročnost implementace

Kritérium hodnotící náročnost instalace a základní konfigurace dohledového systému. Při hodnocení byla pozornost zaměřena především na dobu nutno pro nasazení systému, kvalitu dokumentace, která celý proces popisuje a časovou a odbornou náročnost při zadávání sledovaných hostů.

4.1.5 Zátěž na síťové kartě

Hodnocení síťového provozu, který dohledový systém generuje. Měření probíhalo po dobu 24 hodin, kdy došlo ke sběru dat pomocí programu Wireshark, který zachytával veškerou komunikaci na samostatné síťové kartě připojené do sledované sítě. Aby bylo zabráněno nežádoucí komunikaci byl každý dohledový systém nasazený na dedikovaný virtuální server a měl k dispozici dvě síťové karty. První s přístupem do internetu mimo sledovanou síť a s nastavenou výchozí bránou a druhou, která byla připojena do sledované sítě s nastavenou pouze pevnou IP adresou bez výchozí brány. Na této kartě pak probíhalo samotné měření. Měření probíhalo v běžný pracovní den a naměřená data tak odpovídají běžnému provozu ve sledované síti.

U všech systémů probíhalo měření současně, takže data byla získána za stejných podmínek. Tím byla zajištěna objektivita v rámci testování v tomto kritériu.



Obrázek 15 - Schéma měření zátěže na síťové kartě

4.1.6 Rychlost reakce na výpadek

Kritérium hodnotící schopnost systému reagovat na výpadek libovolného prvku v síti. Původní myšlenkou tohoto kritéria bylo zhodnocení reakčního času systému. Nicméně v průběhu testování bylo zjištěno, že tento způsob hodnocení by nebyl dostatečně objektivní, protože většina testovaných dohledových systémů umožňuje nastavit interval sledování sítě a některé systémy tuto hodnotu přímo vyžadují při přidávání sledovaného prvku do systému.

V tomto dohledu tak bylo hodnoceno, jestli je možné interval nastavit globálně, pro každý prvek zvlášť, anebo interval nastavit není možné. Při hodnocení byla brána v potaz také možnost nastavení minimální velikosti intervalu.

4.1.7 Schopnost identifikovat postižený segment

Hodnocení zejména z pohledu možnosti definice hierarchie sledované sítě a následné schopnosti identifikovat postižený segment v případě výpadku. V tomto bodě je zejména hodnocena možnost budování závislostí a vazeb mezi síťovými uzly a to jak z pohledu konfigurace a její pohodlnosti, tak z hlediska sledování výpadku.

4.1.8 Automatické vyhledávání

Funkce, která automaticky skenuje okolí dohledového systému a vyhledává uzly sítě pro sledování. Dohledové systémy pro toto sledování využívají protokoly ICMP a SNMP. Některé systémy pak využívají také utilitu traceroute pro zjišťování přenosové trasy k nalezenému uzlu. Z hlediska tohoto kritéria je hodnocena zejména kvalita skenování, rychlost a rozpoznání skutečné topologie sítě.

4.1.9 Způsoby upozorňování

Hodnocení z hlediska informací zasílaných administrátorovi o dění na síti. Při bodování je udělen systému bod za každou dostupnou technologii. Typicky systémy preferují email případně SMS. Některé ale navíc přidávají podporu různých komunikačních sítí jako Jabber apod.

4.1.10 Doplňkové funkce

Kritérium hodnotící doplňkové funkce, které nejsou standardní výbavou všech testovaných dohledových systémů. Body jsou uděleny podle počtu dostupných funkcí.

4.1.11 Spolupráce s jinými systémy

Zkoumá interoperabilitu mezi dohledovými systémy a způsob, pokud existuje, jakým je možné systémy propojit, anebo kombinovat. Bod je udělen každému dohledovému systému, který je možné propojit s jinými systémy.

4.1.12 Hloubka monitoringu

Hodnotí zkoumaný systém z pohledu dostupných informací o sledovaných zařízeních. Jako nejnižší vrstva je v tomto případě brána odpověď na ICMP požadavek echo. Za nejvyšší vrstvu je pak považováno sledování činnosti běžících aplikací.

4.1.13 Reálné nasazení

Toto kritérium hodnotí zejména osobní a praktické zkušenosti z testovacího provozu, který probíhal přes 2 měsíce. Za tuto dobu bylo možné jednotlivé dohledové systémy řádně posoudit a získat cenné zkušenosti z jejich používání. Podařilo se zachytit a otestovat i situace, kdy se vlivem rušení začal opakovaně chovat nestandardně bezdrátový spoj realizovaný v centru města (nárůst latence, výpadky spojení, ztrátovost dat apod.). Dohledové systémy tak byly prověřeny na všechny běžně vyvstalé situace na sledované síti.

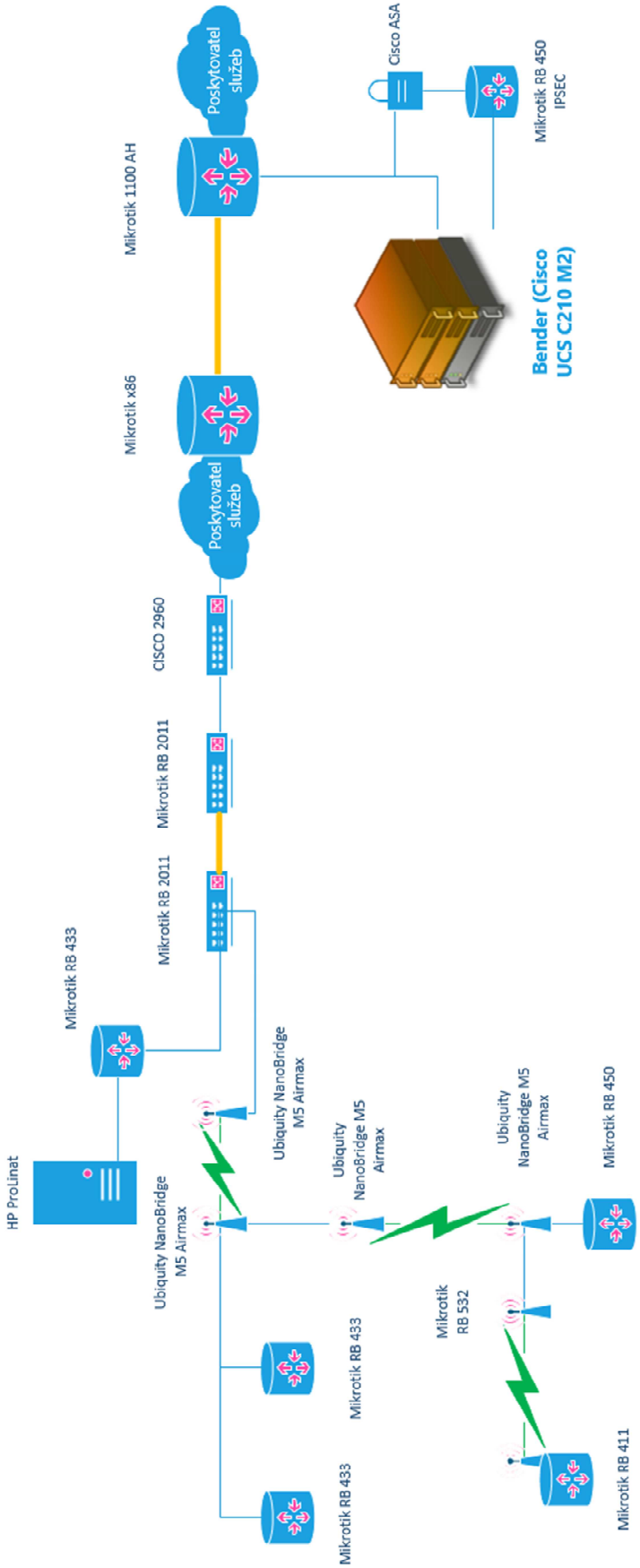
4.2 Testovací prostředí

Testování vybraných dohledových systémů probíhalo na menší reálné síti, která je geograficky rozložená mezi dvě města – Brno a Náměšť nad Oslavou. Města jsou od sebe vzdálená zhruba 46 km a propoj mezi nimi je realizován optickým kabelem přes datacentrum v Invačicích. Účelem této sítě je zprostředkování internetové konektivity pro koncové

zákazníky a poskytování datových a hostingových služeb. V současné době také dochází k implementaci technologie pro poskytování SaaS a IaaS služeb na této síti.

Z technologického hlediska jsou v síti zastoupeny jak optická a metalická přenosová média, tak i bezdrátové spoje. Jako aktivní prvky jsou nasazeny přepínače Cisco, směrovače Mikrotik a pro bezdrátové spoje je využita technologie od spol. Ubiquity. Z hlediska serverů jsou zastoupeny jak klasické „poskládané“ počítače, tak servery IBM, HP a Cisco. Z aplikačního pohledu se v síti nachází OS Windows Server 2012 a Cent OS 6.3 včetně dostupných rolí a služeb a databázové servery MS SQL 2012, Oracle 10g a MySQL.

Na obrázku 16 je zobrazeno aktuální zjednodušené schéma sítě. Schéma je zjednodušené pouze na podstatné prvky, které se nacházejí ve VLAN pro správu. Ta byla předmětem sledování a je vždy ukončena na hranici přenosové a zákaznických sítí.

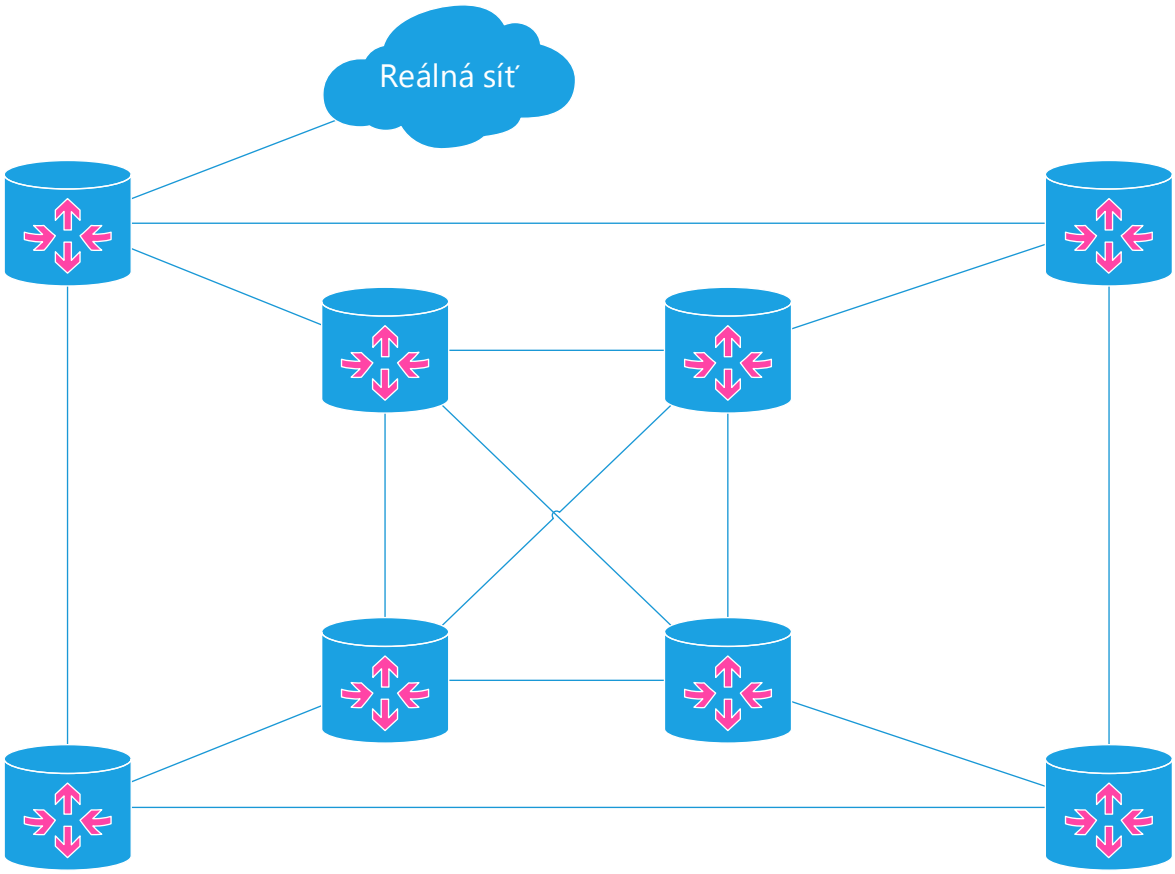


Obrázek 16 – Schéma testované sítě

Každý dohledový systém byl nasazen na dedikovaný virtuální server, který byl spuštěn na virtualizačním serveru s technologií Hyper-V (Hyper-V Server 2012). Výkon virtuálních serverů byl nastaven na doporučené požadavky a serverům bylo povolené dynamické přidělování systémových zdrojů. Virtuální servery byly spuštěny na fyzickém serveru označeném na obrázku 16 jako „Bender“.

Ve druhé fázi testování dohledových systémů došlo k jejich připojení k simulátoru počítačových sítí GNS. Zde byla připravena testovací síť v zapojení uvedeném na obrázku 17. Směrovače byly spuštěny se systémem Cisco IOS pro modely C2600. Směrování v této síti bylo zajištěno pomocí protokolu EIGRP ve vnitřní síti a protokolem RIP vůči síti reálné. Spojení s reálnou sítí zajišťoval Windows Server 2012 s rolí směrovače a povoleným směrovacím protokolem RIP.

Na této síti byla testována funkce automatického vyhledávání a identifikace postiženého segmentu. K tomuto kroku bylo přistoupeno hlavně proto, že předchozí síť byla produkční a nebylo v ní možné vyvolávat výpadky pro potřeby této práce.



Obrázek 17 – Schéma testovací sítě v simulátoru GNS

5 Zhodnocení testovaných systémů dle metodiky

Zhodnocení jednotlivých programů je založeno na autorově dlouhodobém testování vybraných systémů v reálné síti, které probíhalo přes dva měsíce. Všechny systémy byly v testované síti spuštěny společně a bylo tak možné pozorovat jejich odlišnosti a rozdíly v chování v různých situacích na sledované síti. V průběhu testování docházelo k běžným okolnostem a chybám na standardní síti. Reakce dohledových systémů na výpadek byla řádně otestována hlavně u bezdrátových spojů, které se vlivem okolního rušení staly problémovým místem sledované sítě.

5.1 Nagios XI

5.1.1 Cena

Cena produktu Nagios XI je závislá na edici a počtu sledovaných zařízení. Standardně je k dispozici edice Standard a Enterprise, kdy rozdíl je hlavně v dostupnosti pokročilých funkcí, jako je vylepšené prohledávání sítě, možnost tvorby auditů, nová konfigurační rozhraní, plánová tvorba reportů a výpadků, …

Počet hostů	Cena
Neomezeně	104 500 Kč
101-200	52 250 Kč
Do 100	45 600 Kč

Tabulka 1 - Ceník licencí Nagios XI (Nagios Enterprises, LLC, 2013)

V ceně je navíc zahrnuta technická podpora a v případě, že máme velmi malé prostředí do 7 sledovaných hostů, je možné Nagios XI využít zdarma. Pro účely srovnání byla zvolena cena pro sítě do 100 sledovaných prvků.

5.1.2 Systémové požadavky

Minimální systémové požadavky se samozřejmě liší podle velikosti sledované sítě a celkovém počtu sledovaných služeb. Tyto hodnoty jsou vyobrazeny v Tabulka 2 a pro hodnocení tohoto kritéria tak využijeme parametry odpovídající velikosti sledované sítě.

Sledovaných hostů/uzlů	Sledovaných služeb	Lokální úložiště	Počet jader CPU	RAM
50	250	40 GB	1 – 2	1 – 4 GB
100	500	80 GB	2 – 4	– 8 GB
> 500	> 2500		> 4	> 8 GB

Tabulka 2 – Systémové požadavky Nagios XI

Mezi další nutné požadavky pak patří OS na bázi Linuxu. Automatizovaný instalační balíček je připraven pro distribuce na bázi distribuce Red Hat.

5.1.3 Náročnost implementace

Samotná instalace produktu byla velmi jednoduchá záležitost. Je to dáno především tím, že je k dispozici velmi dobře připravený instalační skript, který nicméně funguje pouze v případě, že je server nainstalovaný jako „minimální server“ (Cent OS 6.3) obsahující pouze nejnutnější balíčky. Když byla instalace testována i na instalaci serveru s nainstalovanými základními balíčky pro chod serveru (Cent OS 6.3 instalace základní server), tak bohužel během instalace došlo k chybě a neproběhla korektně. Tato skutečnost je naštěstí výslovně uvedena v instalační dokumentaci, takže při dodržení pokynů by se neměl vyskytnout problém. Dalším způsobem, jak je možné systém nainstalovat, je využití předpřipraveného virtuálního stroje, který je naneštěstí dostupný pouze pro platformu VMware.

Po instalaci je pak nutné provést základní konfiguraci dohledového systému jako je nastavení administrátorských účtů, jazykové předvolby, nastavení emailového serveru, způsoby upozorňování apod. Celá instalace je zakončena konfigurací samotných hostů pro sledování.

Tento proces může být urychlen pomocí funkce automatického vyhledávání, která je podrobněji rozebrána v kapitole 5.1.8. V případě tohoto systému je funkce automatického vyhledávání založená na prostém skenování zadaného adresního rozsahu a běžně dostupných služeb (ICMP, TELNET, apod.). Jejím výstupem je seznam nalezených hostů s přednastavenými službami pro sledování. Na uživateli je už pak pouze definice hierarchie sledované sítě a nastavení detailních informací o sledování a pravidlech pro upozorňování pro konkrétní hosty. V tomto směru se nicméně projevila jedna z největších slabin tohoto systému z pohledu uživatele. Není totiž možné hromadně vybrat několik sledovaných prvků a nastavit jim stejné vlastnosti. De-facto to pak znamená, že bude muset uživatel definovat vlastní nastavení pro všechny sledované prvky a to v sítích, kde jsou stovky až tisíce sledovaných hostů, může být problém.

5.1.4 Uživatelské rozhraní

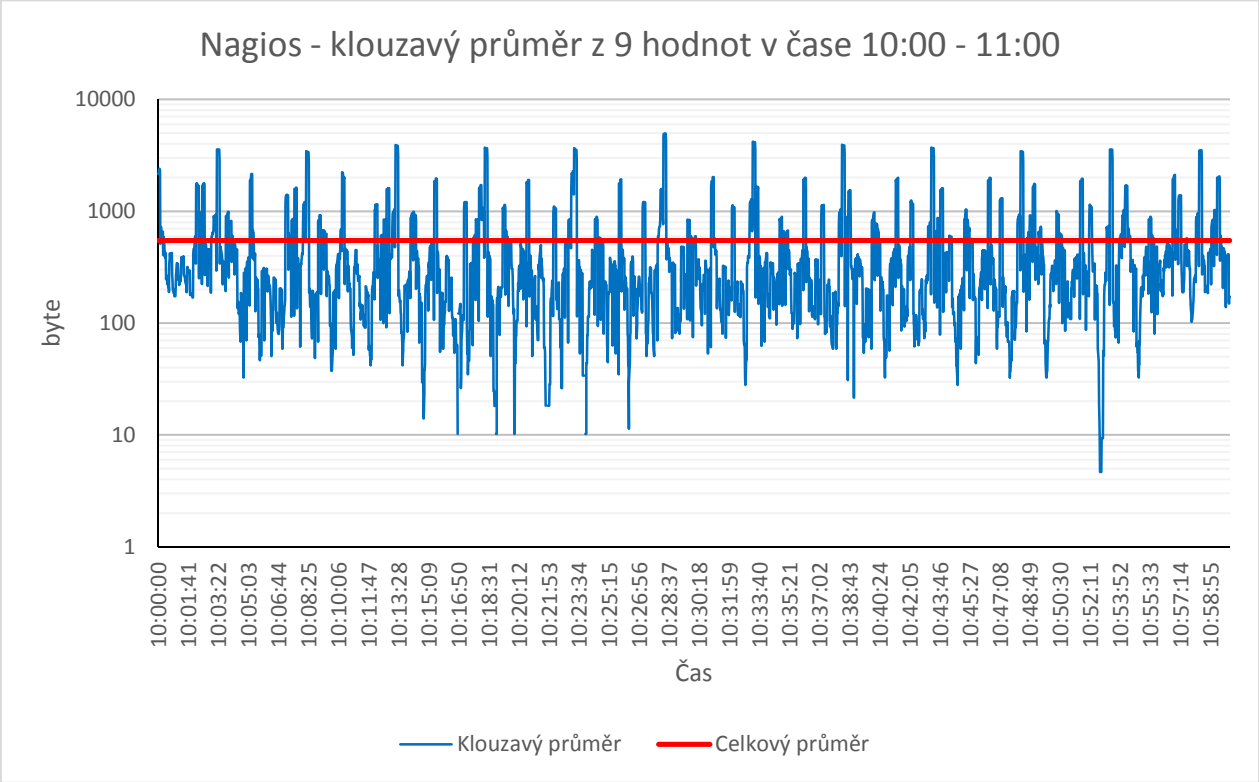
Uživatelé přistupují k administračnímu rozhraní tohoto dohledového systému pomocí internetového prohlížeče. K dispozici mají subjektivně pěkné a přehledné rozhraní, které je možné si v mnohém přizpůsobit. Jako součást rozhraní je možná definice vlastních dashboardů a vizualizace mapy dohledové sítě, která je v případě tohoto systému velmi povedená. Je tak možné využít toto rozhraní také pro vizualizace v centrálním dohledovém středisku. Malou nevýhodou je nedostupnost uživatelského rozhraní v českém jazyce což by mohlo některým uživatelům způsobovat problémy.

5.1.5 Zátěž na síťové kartě

Z pohledu generovaného datového toku na síťové kartě byly u tohoto dohledového systému naměřeny, vzhledem k ostatním testovaným systémům, poměrně vysoké hodnoty.

Celkový průměr se vyšplhal na 547,5 Bytů za vteřinu. Za zmínku také stojí pravidelné výkonové špičky resp. poklesy. Podle autorova názoru je to způsobeno tím, že všechny sledované prvky byly nastaveny na kontrolu stejným intervalem. Z hlediska běžné provozu sítě, se nicméně nejedná o žádnou kritickou zátěž, kterou by standardní datová síť nebyla schopna přenést, anebo která by ovlivnila její celkovou výkonost.

Na obrázku 18 je zobrazen vzorek dat naměřený v době od 10:00 do 11:00. Byl zvolen pouze tento segment, protože zobrazení celkových dat nebylo technicky možné z důvodů velké nepřehlednosti grafu. Pro lepší grafické znázornění bylo také přistoupeno ke zprůměrování dat klouzavým průměrem z 9 hodnot.



Obrázek 18 – Nagios – naměřená zátěž na síťové kartě

5.1.6 Reakce na výpadek

V oblasti nastavení sledovacích intervalu je systém Nagios XI z testovaných systémů hodnocen jako jeden z nejlepších. Je to především dáno tím, že umožňuje správci nastavit interval pro každý sledovaný prvek sítě zvlášť, přičemž nejkratší možný interval je jedna minuta. To umožňuje efektivně určovat prioritní části sítě a extrémně rychlou reakci na výpadek ze strany uživatele.

Z hlediska funkčnosti Nagios využívá nastaveného intervalu, ve kterém periodicky sleduje daný prvek a v případě, že je zaznamenán výpadek, dojde k intenzivnímu sledování problémového prvku a pravidelném informování uživatele do doby jeho zotavení. Jak již bylo zmíněno v předchozím odstavci, všechny parametry jsou nastavitelné a je tak možné

chování a počet nastavit podle potřeb uživatele. Samozřejmostí je sledování prvků sítě na úrovni služeb což pomáhá k rychlejšímu předvídání a upozornění na budoucí problémy a v mnoha případech to může zabránit kompletnímu výpadku prvku.

Při praktickém testování se sledovací mechanismy tohoto dohledového systému velmi dobře osvědčily a byly schopné reagovat i na kolísání bezdrátového spoje, které se objevovalo v důsledku okolního rušení, ale v běžném provozu se prakticky neprojevovalo.

5.1.7 Identifikace postiženého segmentu

Pro identifikaci postiženého segmentu Nagios primárně využívá topologii sítě zadanou uživatelem. Ta musí být bohužel definována ručně uživatelem a vždy se jedná o hvězdicovou hierarchii, kde jsou prvky ve vztahu předek – následník. Tento fakt bohužel značně omezuje, za použití jediného dohledové systému, možnost dohledat postižený spoj. Na místo toho systém vyhodnocuje za nefunkční celou „větev“ sledované části sítě začínající postiženým prvkem. V nastavení je sice možné určit každému sledovanému prvku více předchůdců, ale systém tyto vlastnosti není schopen zachytit do vizualizace celkového přehledu sítě a tak i v případě, že máme k následujícím prvkům k dispozici i jiné spoje, nadále je vyhodnocuje jako nedostupné. Tato vlastnost by se dala pravděpodobně eliminovat použitím více dohledových serverů umístěných na různých částech sítě. To by si nicméně vyžádalo vyšší investice a provozní náklady spojené s dohledovým systémem.

5.1.8 Automatické vyhledávání

Technologie automatického vyhledávání v systému Nagios je založena na prohledávání zadaného rozsahu IP adres, kdy jsou jednotlivé adresy testovány na dostupnost předem definovaných služeb (ICMP, Telnet, SSH, …). Jakmile systém narazí na adresu, která na dané službě odpovídá, dojde k jejímu zařazení do sledovaných prvků a je na něj aplikována šablona pro sledování a vizualizaci dat, která byla definována spolu s adresním rozsahem.

V praxi jsem bohužel narazil na problémy s prohledáváním větší adresních rozsahů s 16 bitovou maskou. Úloha, která je naštěstí vždy spuštěna jako samostatná a tak neomezuje činnost uživatele ani dohledové části systému, byla započata a po dobu cca 8 hodin zůstávala ve stavu „probíhající“. Po jejím ukončení systém zahlásil, že se mu nepodařilo nalézt žádná zařízení v tomto rozsahu. Po rozdělení prohledávaného rozsahu na více úloh s 24 bitovou maskou systém už hledaná zařízení bez problémů vyhledal a umožnil jejich zařazení do sledování. Tuto situaci jsem otestoval třikrát, nicméně vždy se systém choval stejně. S velkou pravděpodobností se tak jedná o chybu programu a ne sledované sítě. Mezi další nevýhody tohoto způsobu vyhledávání patří také situace, kdy potřebujeme sledovat směrovač, který má dvě rozhraní s různými IP adresami. Systém není schopen tuto skutečnost rozpoznat a zařízení vyhodnotí jako dva nezávislé prvky. Tato situace je pravděpodobně způsobena hlavně nedostupnosti podpory pro protokol SNMP, který je možné zpřístupnit až instalací speciálního pluginu. Ten však není součástí standardní instalace.

5.1.9 Způsoby upozorňování

V oblasti upozorňování je dohledový systém Nagios vybaven velmi dobře a oproti jiným systémům uživateli nabízí také něco navíc. Uživatelé tak mají k dispozici upozornění pomocí emailu, SMS a také pomocí komunikačního klienta Jabber. Z pohledu administrátora je možné specifikovat kontaktní skupiny, pracovní dobu, informace, které se mají odesílat, typ zpráv apod. Pomocí těchto možností je tak bez menších problémů možné nasadit Nagios i do běžné společnosti, kde se zaměstnanci střídají na směny a zároveň tak bude vždy někdo vědět o kritických situacích, které se ve sledované síti objeví.

5.1.10 Doplňkové funkce

Nagios XI je systém zaměřený čistě na dohled na sledovanou sítí. Z tohoto pohledu se tak vývojáři zaměřují pouze na tuto činnost a ostatních funkce nechávají na vývojářích v podobě různých doplňků.

5.1.11 Spolupráce s jinými systémy

Nagios je podobně jako většina testovaných systémů založen nad databází – v tomto případě MySQL a navíc zpřístupňuje pro vývojáře vlastní API. Podle mého názoru je tak ostatním dohledovým systémům otevřen více než dost, ale ve většině případů to bude znamenat programování vlastního spojení a to nemusí být pro mnoho uživatelů nebo společností finančně výhodné.

5.1.12 Hloubka monitoringu

Základní „vrstvou“ pro dohled sítě je v případě Nagiosu protokol ICMP. Ten se využívá pro zjištění základních informací o sledovaném prvku. Dále jsou pak vrstvy pro sledování dostupné především podle typu použité šablony a způsobu sledování.

Pokud sledujeme prvek bez pomoci lokálního agenta, jsou pro sledování k dispozici síťové protokoly ICMP, Telnet, SSH, HTTP, SMTP, LDAP, FTP, IMAP, POP, DHCP a WMI. V tomto případě má nicméně uživatel k dispozici pouze omezené informace a stav sledovaných služeb.

V případě, že je sledován server pomocí lokálně instalovaného agenta, je systém schopen získat mnohem více informací jako je např. vytížení CPU, RAM, stav a zaplnění disků apod. Lokální agent navíc dohledovému systému umožňuje proaktivně zasahovat do jeho chodu v případě potřeby např. restart služby apod.

Protokol SNMP je sice ve specifikacích a dokumentaci uváděn jako podporovaný, ale v základní instalaci nebyl obsažen a bylo nutné ho doinstalovat pomocí volně stažitelného doplňku.

5.2 Cacti

5.2.1 Cena

Dohledový systém Cacti je zástupcem volně dostupných dohledových systémů a jeho cena je tak pro porovnání počítána jako 0 Kč.

5.2.2 Systémové požadavky

Bohužel dokumentace k produktu minimální hardwarové požadavky neudává. Vývojáři produktu to zdůvodňují tím, že jsou výrazně závislé na počtu sledovaných prvků a intervalu sběru dat. V diskuzních fórech na internetu lze nalézt tak rozličné konfigurace, že ani z nich není možné určit přesné hodnoty. Rozhodnul jsem se proto požadavky odhadnout na virtuálním stroji za použití dvoujádrového procesoru a dynamicky přidělované operační paměti. Celý server pro sledování se po týdnu provozu ustálil na hodnotách:

- dvoujádrový procesor
- 846 MB RAM
- 8GB HDD

Mezi další nutné požadavky pro běh systému patří databáze MySQL, webový server s podporou PHP 5.1+ a nástroj RRDTool 1.4+. Vše může být spuštěno jak na Windows, tak i na libovolné distribuci Linuxu.

5.2.3 Náročnost implementace

Samotné spuštění dohledového systému není nikterak náročné. Prakticky jde o konfiguraci požadovaných požadavků tj. běžná konfigurace webového serveru s podporou PHP, instalace a vytvoření MySQL databáze a instalace samotné aplikace. Jediné problémy, které byly při instalaci testovacího serveru zaznamenány, byly s nasazením RRDTool. Ty se podařilo odstranit za pomoci diskuzních fór a dokumentace k produktu.

Fáze implementace samotného sledování je bohužel velmi zdlouhavá. Je to dáno především tím, že systému v základní instalaci chybí podpora funkce automatického vyhledávání a je tak nutné přidávat sledované prvky a jejich služby ručně, což u rozsáhlých sítí může být otázkou dnů. Dalším problémem, který jsem objevil je fakt, že aby bylo možné získat alespoň nějaký rozumný přehled o zařízeních v testovací síti, bylo nutné dohledat a doinstalovat šablony pro konkrétní zařízení, protože systém obecných informací neposkytuje mnoho. Po instalaci jednotlivých šablon a použití protokolu SNMP získá uživatel o jednotlivých zařízeních přehled velmi detailní.

5.2.4 Uživatelské rozhraní

Uživatelské rozhraní je dostupné pomocí internetového prohlížeče a působilo na mě subjektivně nejhůře z testovaných systémů. Několik položek nutných pro konfiguraci bylo, podle mého názoru, umístěno nelogicky a zabralo hodně času je dohledat. Problémy

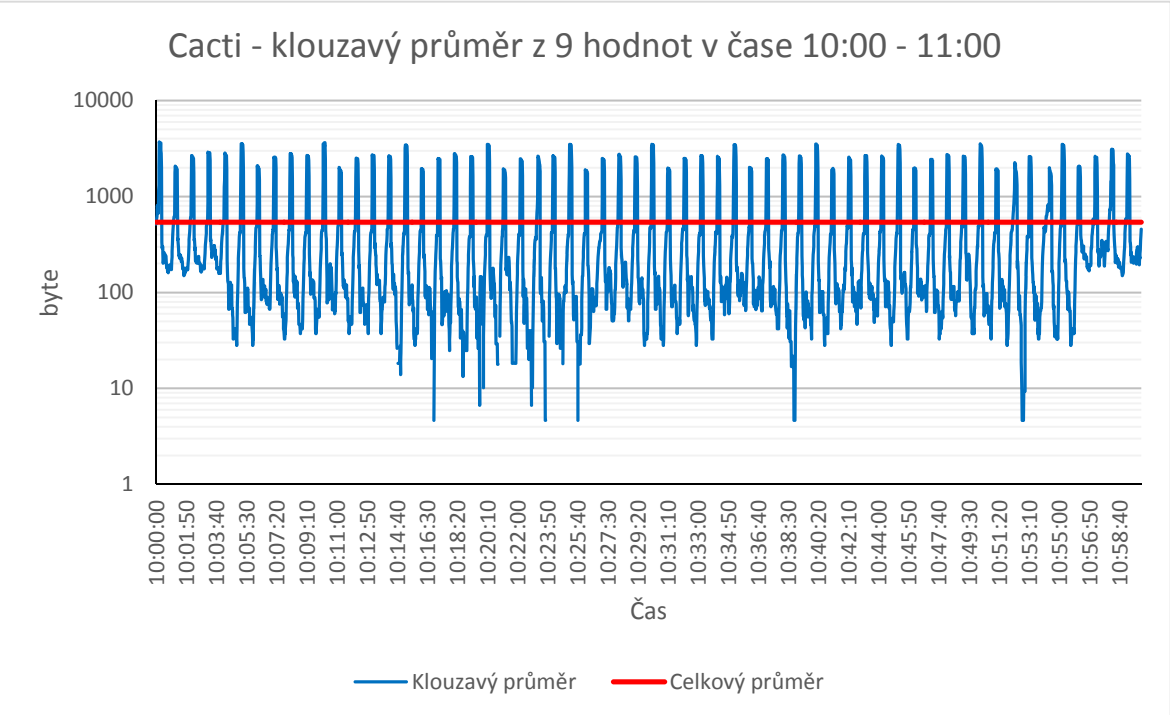
s šablonami byly zmíněny už v přechozí kapitole, nicméně i po jejich instalaci se mi na některých místech nepodařilo zobrazit potřebné přehledy.

Celkově je Cacti hodně zaměřeno na sběr dat a jejich vizualizaci v grafech a to je s velkou pravděpodobností také důsledek toho, že chybí některé podstatné funkce pro optimální přehled o dění na síti. Jedním z těchto prvků je vizualizace mapy celé sítě. Sice zde existuje náznak v podobě záložky „monitor“, nicméně ten ani zdaleka nedosahuje takových kvalit jako u konkurenčních systémů. Obecně by se dalo konstatovat, že Cacti je zaměřeno spíše na detailní přehled o konkrétních zařízeních a nikoli na celkový pohled na síť.

5.2.5 Zátěž na síťové kartě

Z hlediska naměřeného datového provozu na síťové kartě je na tom Cacti velmi podobně jako Nagios. U obou byly naměřeny poměrně vyšší hodnoty než u zbývajících dvou systémů. V průměru byla za dobu 24 hodin v Cacti naměřena hodnota 539 Bytů za vteřinu, nicméně oproti Nagiosu lze pozorovat vyrovnanější průběh, s výrazně nižšími výkonovými špičkami.

Na obrázku 19 je zobrazen vzorek dat naměřený v době od 10:00 do 11:00. Byl zvolen pouze tento segment, protože zobrazení celkových dat nebylo technicky možné z důvodů velké nepřehlednosti grafu. Pro lepší grafické znázornění bylo také přistoupeno ke zprůměrování dat klouzavým průměrem z 9 hodnot.



Obrázek 19 – Cacti - naměřená zátěž na síťové kartě

5.2.6 Reakce na výpadek

Cacti pracuje na prakticky stejném principu jako ostatní dohledové systémy. V zadaném intervalu jednotlivé prvky testuje na dostupnost a v případě chyby provede požadovanou akci. U Cacti je nicméně základním problémem délka tohoto intervalu, protože jeho nejnižší hodnota je 10 minut a to je dle mého názoru pro moderní datové sítě nedostatečné. Tato hodnota je globální pro celý systém a není možné ji přizpůsobit pro konkrétní sledované prvky. V důsledku této vlastnosti se tak Cacti příliš nehodí na sítě s potřebou sledování kritických prvků, u kterých záleží na každé minutě výpadku.

Z praktického pohledu se Cacti osvědčilo u delších výpadků, které bylo schopné zachytit. Na druhou stranu Cacti nedokázalo identifikovat problémy s rušením na bezdrátovém spoji a v tomto ohledu tak dopadlo o něco hůře než ostatní systémy.

5.2.7 Identifikace postiženého segmentu

Bohužel Cacti nemá k dispozici ucelený přehled o sledované síti, který by zároveň definoval vazby sledovaných prvků a umožňoval tak identifikovat postižený segment sítě.

V případě výpadku kořenového směrovače tak uživatel prakticky nemám k dispozici nástroj, který by mu pomohl odhalit, kde přesně se problém nachází a jeho identifikace tak zůstává na uživateli. V tomto ohledu dopadl dohledový systém Cacti nejhůře.

5.2.8 Automatické vyhledávání

Už dříve bylo zmíněno, že dohledový systém Cacti nemá v základní instalaci k dispozici funkci automatického vyhledávání. Funkci lze přidat instalací bezplatného doplňku o kterém se nyní zmíním. Doplněk však nelze v rámci objektivity hodnotit jako standardní součást dohledového systému.

Jeho princip je založen, podobně jako u ostatních dohledových systémů, na skenování zadaného rozsahu IP adres. Systém pak automaticky testuje každou zadanou adresu pomocí základních síťových protokolů a v případě odezvy je zařadí do seznamu nalezených zařízení. Uživatel z tohoto seznamu vybere nalezené prvky, které chce zařadit do sledování a přidělí jim odpovídající šablonu nastavení. Od té chvíle jsou prvky k dispozici pro vizualizaci naměřených dat.

5.2.9 Způsoby upozorňování

Cacti obsahuje ten nejzákladnější, nicméně asi nejpoužívanější, způsob upozorňování a to email. Uživatel má možnost měnit základní parametry emailu a navíc i za pomoci speciálních proměnných i jeho text. Co trochu chybí je možnost nastavení časových údajů, kdy se upozornění na výpadek mají posílat. Naopak vytváření seznamu příjemců nechybí a je možné tyto seznamy definovat na konkrétní prvky.

Další možností pro získávání informací o událostech je syslog server, který je dostupný v aplikaci, anebo může být využit jakýkoliv jiný dostupný na síti. Možnost tohoto logování

může být hlavně pro velké organizace velkým bonusem, protože většina síťových prvků tuto možnost využívá jako centrální server pro zapisování událostí.

5.2.10 Doplňkové funkce

Během testování Cacti jsem nenarazil na žádnou funkci, kterou by jiný dohledový systém neměl.

5.2.11 Spolupráce s jinými systémy

Podobně jako Nagios i Cacti běží nad klasickou databází MySQL a tak by neměl být problém, za cenu vlastního vývoje, tento systém propojit s jiným dohledovým systémem. Dále Cacti nabízí vlastní API, které umožňuje prakticky jakémukoliv systému s tímto produktem komunikovat. Z praxe je tak možné využívat Cacti jako zdroj dat a nad nasbíranými daty realizovat zákaznický portál se zobrazením vytíženosti zákazníkovy linky.

5.2.12 Hloubka monitoringu

Základním protokolem pro práci dohledového systému Cacti je ICMP a SNMP. Další protokoly nejsou pro aktivní dohled v základní instalaci podporovány. Je to dáno především tím, že samotný protokol SNMP, pokud ho sledované zařízení podporuje, je více než dostačující k získání potřebných informací o sledovaném zařízení. Cacti podporuje SNMP verze 1 – 3.

Cacti bohužel neumožňuje sledovat služby na sledovaném zařízení jinak, něž přes protokol SNMP. Tak v okamžiku, kdy budeme chtít sledovat nějaké zařízení bez podpory tohoto protokolu, bude nutné si vystačit pouze s tzv. základním monitoringem, který nicméně moderní ICT prostředí nemůže dostatečně pokrýt. Po zběžném průzkumu diskusních fór nicméně po podpoře více protokolů uživatelé volají a je tak možné že, přibydou v dalších verzích. Pro servery je k dispozici lokální agent.

5.3 Zabbix

5.3.1 Cena

Zabbix je podobně jako Cacti zástupcem volně dostupných systémů, proto je jeho cena počítána jako nulová. Jediným omezením ve využívání tohoto dohledového systému je licence GPL, pod kterou je vydáván. Licence je zároveň omezující pro případné komerční úpravy, protože veškeré úpravy musí být v jejím souladu. Nelze tedy zdrojové kódy Zabbixu využívat jako základ komerčních produktů a ty dále prodávat. Vývojáři systému však nabízejí možnost zakoupení komerční licence, která toto umožňuje.

5.3.2 Systémové požadavky

Podobně jako u Nagiosu i vývojový tým, který stojí za systémem Zabbix, uvádí doporučenou hardwarovou konfiguraci podle počtu sledovaných prvků.

Platforma	CPU/RAM	Databáze	Sledovaných hostů
Ubuntu Linux	PII 350MHz 256MB	MySQL, MyISAM	20
Ubuntu Linux 64 bit	AMD Athlon 3200+ 2GB	MySQL, InnoDB	500
Ubuntu Linux 64 bit	Intel Dual Core 6400 4GB	RAID10 MySQL InnoDB nebo PostgreSQL	>1000
RedHat Enterprise	Intel Xeon 2xCPU 8GB	Rychlý RAID10 MySQL InnoDB nebo PostgreSQL	>10000

Tabulka 3 – Hardwarové požadavky systému Zabbix (ZABBIX SIA, 2012)

Dalším hardwarovým požadavkem je připojený GSM modul pro případ, že by uživatel chtěl zasílat upozornění pomocí SMS. Ten nicméně není nutnou podmínkou pro jeho chod.

5.3.3 Náročnost implementace

Implementace systému Zabbix žádným výrazným způsobem nevybočovala z běžných standardů. Podobně jako ostatní testované systémy, Zabbix vyžaduje server s několika základními komponentami před samotou instalací. Tou první je webový server Apache 1.3.12+ s podporou PHP ve verzi 5.0 a vyšší. Dále bylo nutné nainstalovat databázový server. V této oblasti má Zabbix nezvykle široký výběr a je tak možné zvolit mezi IBM DB2, MySQL, Oracle, PostgreSQL a SQLite, což dává Zabbixu velkou šanci na začlenění do stávající infrastruktury společnosti a nainstalovat ho tak prakticky pouze na aplikační server. Pro větší sítě pak vývojáři v dokumentaci výslovně doporučují využít odděleného databázového serveru.

Pro instalaci na mnou vybranou platformu tj. Cent OS 6.3 tak stačilo zvolit instalační balíček ze standardního repozitáře. Samozřejmostí je také možnost instalace ze zdrojových kódů a jejich kompilace. Tento proces je podrobně popsán v dokumentaci produktu. Po úspěšné instalaci a základním nastavení systému jsem nicméně narazil na problém s přidáním sledovaných prvků sítě, kdy se mi nedařilo přidat prvky odpovídajícím způsobem. Nakonec jsem musel důkladně pročíst příslušné kapitoly v dokumentaci, kde jsem zjistil, že postup je prakticky stejný jako v případě ostatních systémů (najít hosta > aplikovat šablonu > získávat data), ale v uživatelském rozhraní jsem nenašel žádné průvodce, který by tento proces sjednotil podobně jako u jiných systémů. Tento fakt tak brání rychlé implementaci i pro začínající uživatele, nicméně s pomocí dokumentace lze poměrně snadno tento nedostatek překonat.

5.3.4 Uživatelské rozhraní

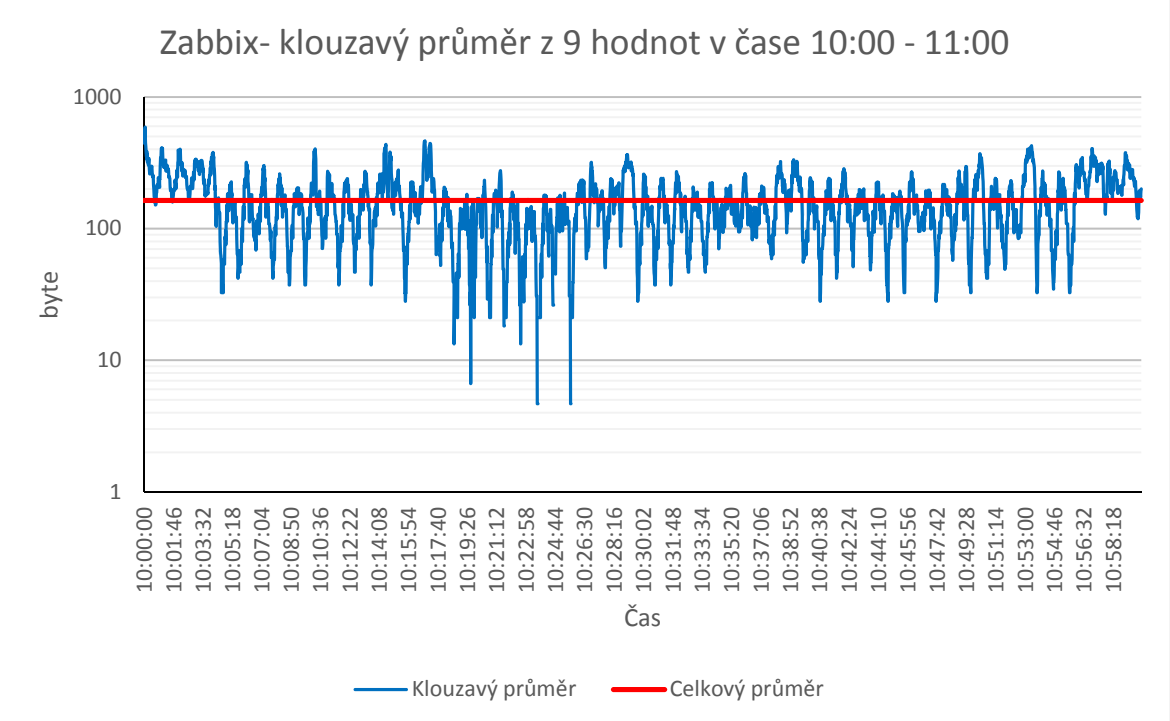
Uživatelské rozhraní Zabbixu, dostupné přes webový prohlížeč, na mě hned po instalaci nepůsobilo zrovna nejlépe. Bylo to dáno především tím, že se mi subjektivně zdálo nepřehledné. Po delší době testování se mi ho však podařilo pochopit a nepředstavovalo výraznou překážku, která by systém znehodnocovala. Z osobního pohledu se zde nachází velký prostor pro vývojáře třetích stran.

Další oblasti, kde mě rozhraní Zabbixu poměrně zklamalo, byla vizualizace dat do grafů a topologie sítě, které konkurenční systémy umí lépe. K vytvoření grafů je totiž nutné provést několik kroků a u většiny sledovaných zařízení se mi to dokonce ani nepodařilo. Systém měl totiž problém se SNMP parametry uváděných v informacích od směrovačů a v okamžiku kdy jeden nerozeznal, vyhodnotil SNMP službu jako nefunkční a data už dále nečerpal. To by pravděpodobně vyřešila instalace a konfigurace vhodné šablony, nicméně ta už není součástí systémů a jedná se o doplňky třetích stran. Topologie sítě není generována automaticky, ale je nutné si ji „nakreslit“ a jednotlivé komponenty pak provázat na datové zdroje.

5.3.5 Zátěž na síťové kartě

V této oblasti si Zabbix naopak vedl velmi dobře. V celkovém srovnání skončil na druhém s průměrnou hodnotou 163,57 Byte za vteřinu. Podle mého názoru je to dáno především tím, že primárním sledovacím protokolem byl SNMP a Zabbix nekontaktoval sledované prvky také ostatními službami jako v případě Nagiosu, který automaticky vyhledával dostupnost i těchto služeb a zároveň nebyl schopen ze sledovaných zařízení získat podobné množství dat jako Cacti.

Na obrázku 20 je zobrazen vzorek dat naměřený v době od 10:00 do 11:00. Byl zvolen pouze tento segment, protože zobrazení celkových dat nebylo technicky možné z důvodů velké nepřehlednosti grafu. Pro lepší grafické znázornění bylo také přistoupeno ke zprůměrování dat klouzavým průměrem z 9 hodnot.



Obrázek 20 – Zabbix – zátěž na síťové kartě

5.3.6 Reakce na výpadek

Také v případě Zabbixu je možné interval pro sledování jednotlivých služeb uživatelsky měnit. V předem připravených šablonách byl tento interval pro SNMP nastaven na 3600 vteřin. Bohužel není možné měnit interval sledování pro celého hosta globálně podobně jako u ostatních systémů, ale je to nutné provést v šabloně, která je na hosta aplikována a nastavit tento interval zvlášť u každé služby. V tomto případě záleží na preferencích uživatele, který přístup mu vyhovuje více.

V porovnání s ostatními systémy je naopak výhodou Zabbixu fakt, že se interval nastavuje ve vteřinách. Je tak možné na kritické služby nasadit sledování téměř v reálném čase. Otázkou na zamyšlení nicméně zůstává, jak by se systém choval u rozsáhlých sítí a jak výkonný hardware by bylo nutné použít. Mezi další metody zachycení výpadku je využití tzv. SNMP pastí, které jsou v případě problémů vygenerovány postiženým zařízením.

Zabbix je samozřejmě také proaktivní monitoring a v případě serverů lze připravit skripty, které jsou spuštěny v případě problémů s komunikací mezi lokálním agentem a dohledovým serverem. Systém tak může provést prakticky cokoli, co si uživatel přeje.

5.3.7 Identifikace postiženého segmentu

Identifikace postiženého segmentu je dána především tím, jak přesně si uživatel zakreslí topologii své sítě a prováže ji s datovými zdroji. Zabbix v sobě totiž nemá žádný mechanismus, který by byl schopen toto řešit, a proto vždy cyklicky kontroluje hosty na zadaných IP adresách resp. rozhraních. Zabbix namísto toho umožňuje využít tzv. triggerů neboli spouští. Jsou to vlastně automatické operace, které jsou navázané na konkrétní událost např. nedostupnost hosta. Tímto mechanismem je pak možné spustit operace, které chybný spoj vyhledají, resp. omezit sledování hostů, kteří jsou umístěni za kritickým prvkem.

Bohužel spouště z mého pohledu nevnímám jako pohodlnou náhradu, protože jejich nastavení je pro rozsáhlé sítě velmi komplikované a zdlouhavé. Z pohledu uživatele by bylo mnohem příjemnější mít k dispozici mechanismus rodič-potomek, který je ve většině případů jednodušší na konfiguraci a bylo by ho možné ho využít i k sestavení automatické topologie sítě.

5.3.8 Automatické vyhledávání

Automatické prohledávání je v Zabbixu řešeno dedikovanou úlohou, která periodicky prohledává zadaný adresní rozsah. Této úloze je nutné definovat spoušť, která je spuštěna vždy při nalezení nového prvku. Ve spoušti je nutné definovat akci přiřazení vhodné šablony a zařazení do množiny sledovaných zařízení. I zde je dobré v případě první konfigurace postupovat podle dokumentace, protože v nastavení úlohy je k dispozici mnoho parametrů, které nemusí mít na požadovanou činnost vůbec vliv. Výhodou tohoto přístupu je možnost kategorizace vyhledaných zařízení podle parametrů, IP adresy apod. Nevýhodou je naopak počáteční nepřehlednost, kdy fakt, že je nutné nadefinovat spoušť pro nalezené prvky, se uživatel dozví až v dokumentaci.

Jak již bylo zmíněno v předchozích kapitolách, tato funkce nedokáže sestavit topologii sítě. Zároveň se jí ani nedaří odhalit prvky s více IP adresami a prakticky monitoruje jednotlivá rozhraní namísto prvku jako celku.

5.3.9 Způsoby upozorňování

V oblasti notifikací je Zabbix vybaven standardní funkcionalitou jako ostatní testované systémy. Uživatel má k dispozici emailové upozornění, v případě připojení GSM modemu SMS zprávy a také zápis do logovacího souboru, který je později možné analyzovat. U všech možností je k dispozici opakované upozorňování s možností definice pracovní doby a specifikací důležitosti událostí, které se mají odeslat.

5.3.10 Doplňkové funkce

Jednou z velkých předností Zabbixu je možnost inventarizace všech sledovaných prvků. Tato inventarizace je navíc prováděna podle metodiky ITIL a její výsledky tak zapadají do moderně řízených ICT prostředí. Inventarizace je možná vyplněním všech požadovaných vlastností, ale její častější aplikace bude při definici šablony, kde je možné namísto hodnot nadefinovat proměnné z protokolu SNMP, získávat automaticky.

5.3.11 Spolupráce s jinými systémy

Stejně jako Nagios a Cacti je i Zabbix spuštěn nad databází, takže je v případě potřeby možné data čerpat přímo z ní. Zabbix navíc zpřístupňuje vývojářům také API pro programování vlastních funkcionalit bez nutnosti znalosti zdrojového kódu Zabbixu anebo jeho databázové struktury.

5.3.12 Hloubka monitoringu

Základními protokoly pro Zabbix jsou ICMP a SNMP. Systém navíc umožňuje sledování základních síťových služeb jako SSH, LDAP, SMTP, FTP, HTTP, POP, NNTP, IMAP a TCP. Za pomoci agenta lze podobně jako u ostatních dohledových systémů získat ze serverů mnohem více informací až po stav jednotlivých služeb a aplikací. Pro síťová zařízení tuto úlohu primárně plní protokol SNMP.

V této oblasti se tedy nikterak významně neliší od ostatních testovaných systémů.

5.4 SCOM 2012

5.4.1 Cena

Jak už bylo zmíněno v úvodu této práce SCOM 2012 je součástí velkého balíku System Center 2012, jehož úkolem je řídit, podporovat a monitorovat celou ICT infrastrukturu společnosti od síťových zařízení, přes servery až po koncové stanice. Nelze tak přesně určit cenu za tento konkrétní nástroj, proto bude v rámci této práce uvažována cena za celý balík. Microsoft produkt distribuuje v mnoha licenčních programech, nicméně v praxi se nejvíce software nakupuje v licenčním programu Open Licence Program (dále jen OLP). Cena

produktu na jeden dohledový server s maximálně dvěma procesory je 1 417 € což je v přepočtu 36 672 Kč. Navíc je nutné připočítat cenu tzv. client management pack za každý sledovaný server, anebo koncový počítač a licenci za operační systém Windows Server, který je nutnou podmínkou pro běh tohoto produktu. Rázem je tak System Center nejnákladnějším dohledovým systémem ze všech testovaných.

Tento systém je dostupný ještě v licencích datacenter a essentials. Oba se liší prostředím, na které cílí. Zatímco datacentrer je cílen na rozsáhlá a hlavně virtualizovaná prostředí (finanční výhoda pro virtualizované servery), tak essentials míří do segmentu malých společností bez IT oddělení.

5.4.2 Systémové požadavky

SCOM 2012 je na poměry dohledových systémů náročnou aplikací, a tak jsou jeho systémové požadavky v oficiální dokumentaci (Microsoft Corporation, 2013) rozděleny podle jednotlivých komponent. Pro účely srovnání by nicméně měly postačit nároky samotného management serveru.

- 1024 MB volného místa na disku
- Operační systém Windows Server 2008 R2 SP1, anebo Windows Server 2012
- 64 bitový procesor
- Windows PowerShell verze 2+
- Pro server musí být povolena vzdálená správa
- .NET Framework 4+

Ze zkušeností s testovacího provozu lze konstatovat, že nároky systému SCOM byly jednoznačně nejvyšší. Je to dáno především tím, že systém pro svůj běh vyžaduje MS SQL server a doporučení na jeho provoz je také, že na každý GB databáze by měl připadat GB operační paměti. Testovací server se čtyřjádrovým procesorem si po měsíci běžného provozu alokoval 7074GB RAM.

5.4.3 Náročnost implementace

Instalace SCOM 2012 byla velmi uživatelsky přívětivá a jednoduchá. Jak bývá na platformě Windows zvykem, byl spuštěn instalační průvodce, který si od uživatele vyžádal několik vstupních informací a zbytek instalace pak proběhnul automaticky. Předpokladem pro instalaci dohledového serveru byl aktualizovaný operační systém a instalace tzv. před instalačního balíčku. Ten zajistil instalaci všech potřebných součástí jako je .NET Framework, PowerShell, nezbytné aktualizace apod. V průběhu instalace ještě dojde k instalaci MS SQL serveru ve verzi 2012.

Fáze implementace probíhá po počátečním zorientování se velmi snadno a rychle. SCOM 2012 totiž využívá sofistikovanou metodu vyhledávání (viz. 5.4.8) sledovaných zařízení, takže je reálné nasazení otázkou několika okamžiků.

5.4.4 Uživatelské rozhraní

Uživatel má k dispozici několik možností jak systém spravovat a nastavovat. Tou první a asi nejčastěji využívanou je lokálně instalovaná konzole ve formě spustitelné aplikace. Konzole se po prvním spuštění nejeví příliš přehledně, nicméně po zběžnějším seznámení je uživatel schopen se systémem pracovat velice snadno. Tato konzole je nicméně dostupná pouze pro platformu Windows. Uživatelé jiných platforem si musí vystačit s možností druhou a tou je webová konzole. I zde je ovšem menší překážka ve formě nutnosti podpory technologie Silverlight. Webová konzole je odlehčenou formou konzole lokální, ale naštěstí pro uživatele je vzhledově prakticky totožná, tudíž je velmi snadné mezi nimi přepínat.

Poslední možností, jak systém spravovat, je příkazový řádek PowerShell, který poskytuje pro uživatele sadu funkcí umožňující pohodlnou operací s objekty obsažených ve SCOM 2012.

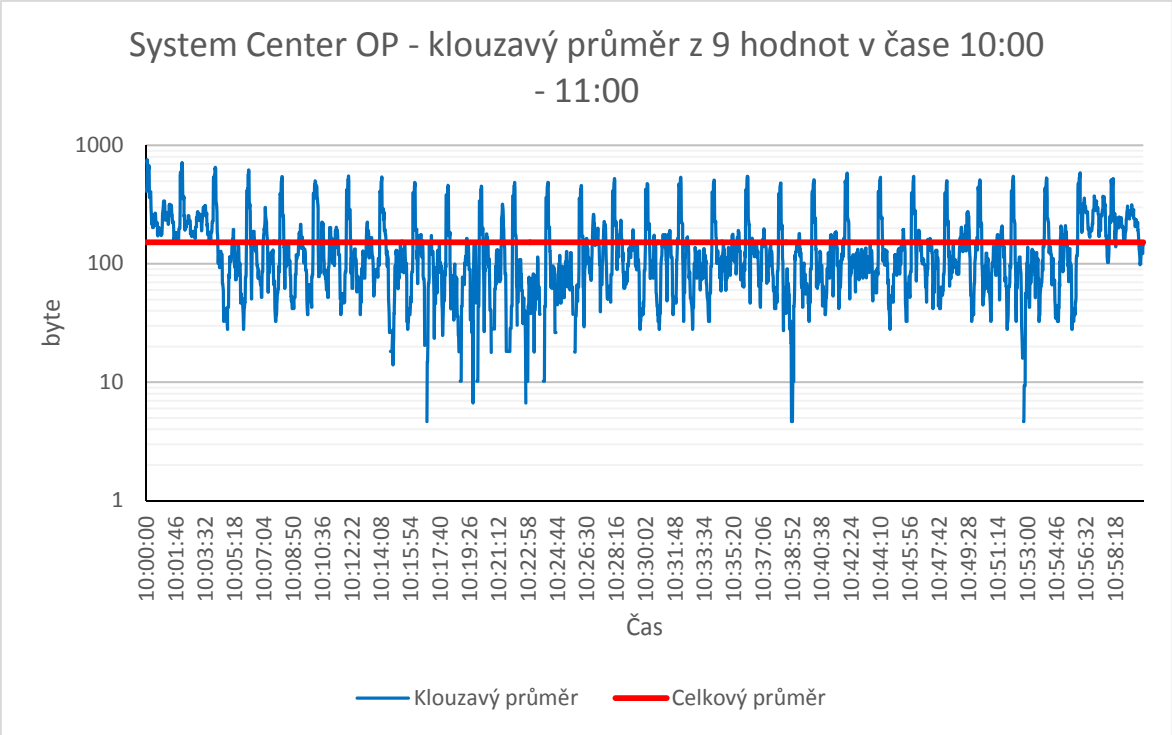
Z pohledu reportů a vykreslení topologie sledované sítě není tomuto produktu co vytknout. Jediné, co by se snad mohlo do dalších verzí zlepšit, by bylo rychlé generování přehledových grafů a matice všech sledovaných služeb a prvků. Naopak velmi hezky je ztvárněn „rozpad“ sledovaných prvků na jednotlivé běžící komponenty a aplikace.

Největší náskok ze sledovaných systémů byla existence uživatelského rozhraní v českém jazyce už v základní instalaci.

5.4.5 Zátěž na síťové kartě

V této oblasti SCOM 2012 podobně jako Zabbix zbylé systémy výrazně překonal. Během testování byla za dobu 24 hodin naměřena průměrná hodnota 150,38 Byte za vteřinu. Tato hodnota byla nejnižší z testovaných systémů. Podle mého názoru to způsobuje s vysokou pravděpodobností využívání SNMP pastí a dlouhého intervalu pro periodickou kontrolu sledovaných zařízení.

Na obrázku 21 je zobrazen vzorek dat naměřený v době od 10:00 do 11:00. Byl zvolen pouze tento segment, protože zobrazení celkových dat nebylo technicky možné z důvodů velké nepřehlednosti grafu. Pro lepší grafické znázornění bylo také přistoupeno ke zprůměrování dat klouzavým průměrem z 9 hodnot.



Obrázek 21 – SCOM 2012- zátěž na síťové kartě

5.4.6 Reakce na výpadek

Díky využívání SNMP pastí, je reakce na výpadek provedena prakticky okamžitě. Interval pro sledování je však nastaven hodnotu 300 vteřin. V praxi se mi tento údaj nepodařilo ověřit, protože reakce na výpadek byla buď výrazně rychlejší (řádově vteřiny) nebo výrazně pomalejší – naměřeno 6:28 minut. Interval není bohužel možné měnit pro individuální prvky, jde tak o jednu ze slabin tohoto dohledového systému.

Obrovskou výhodou systému SCOM 2012 je také fakt, že rozpozná jeden síťový prvek s více síťovými rozhraními. V praxi to znamená, že systém skutečně sleduje síťové prvky jako celek a nevnímá je pouze jako množinu IP adres.

5.4.7 Identifikace postiženého segmentu

Díky velmi kvalitnímu algoritmu na vybudování topologie sledované sítě, je identifikace postiženého prvku přesná a konkrétní. Při výpadku spoje pak systém za pomoci SNMP testů přesně identifikuje postižené místo a provede jeho vizualizaci na mapě.

5.4.8 Automatické vyhledávání

Funkce, která je rozhodně největší předností tohoto systému. Ke správné funkčnosti by totiž mělo stačit zadání jednoho prvku na místo celé podsítě. SCOM totiž využívá protokolů SNMP, ICMP a CDP pro rekurzivní vyhledávání nových zařízení, které jsou k tomu aktuálně zjištěnému připojené. Tím získává tento dohledový systém velmi detailní přehled o topologii sledované sítě, ze které potom těží při identifikaci postiženého systému sítě při výpadku.

Nevýhodou mechanismu je nicméně nutnost vykonávat prohledávání zadaného adresní rozsahu v jedné úloze. Programově je totiž omezena možnost spouštění více úloh na jednom serveru.

Při testování v laboratorních podmínkách bylo zjištěno, že SCOM 2012 dokáže zachytit topologii sledované sítě velice přesně a správně.

5.4.9 Způsoby upozorňování

Výbava SCOM 2012 z hlediska notifikací uživatele o problému na síti je velmi podobná tomu, co nabízejí ostatní systémy. Jsou tak k dispozici upozornění emailem, SMS a komunikačním klientem. Poslední možností je pak vykonání libovolného příkazu/skriptu. Snadno si tak můžeme připravit vlastní akce pro upozornění.

Samozřejmostí je možnost vytváření kontaktních skupin, definice pracovní doby, editace textu emailu a SMS zprávy apod.

5.4.10 Doplňkové funkce

Mezi hlavní doplňkové funkce SCOM 2012 patří jeho provázanost na ostatní nástroje z balíku System Center. Zde totiž spočívá největší síla a výhoda tohoto nástroje. V okamžiku, kdy dojde k jejich vzájemnému propojení, získává uživatel platformu, která dokáže velmi inteligentně a hlavně automatizovaně řídit celé ICT zázemí.

5.4.11 Spolupráce s jinými systémy

Podobně jako ostatní testované systémy, tak i u SCOM 2012 existuje teoretická šance propojení ostatních systémů na úrovni databáze. Bohužel se mi v dokumentaci nepodařilo dohledat žádnou oficiální cestu, jak SCOM 2012 s jiným dohledovým systémem propojit. Přesto SCOM 2012 pro vývojáře SDK by případnou cestu k propojení s jiným systémem mohlo otevřít.

Přímou integraci s ostatními systémy se dohledat v dokumentaci a ani v nastavení nepodařilo.

5.4.12 Hloubka monitoringu

Jak už bylo zmíněno v předchozích kapitolách, SCOM jako svůj hlavní protokol využívá protokol SNMP. V dokumentaci se mi nepodařilo získat explicitní výčet všech podporovaných protokolů, nicméně v praxi bylo ověřeno dostupnost SMTP, TCP, ICMP, SNMP, Telnet, SSH, POP, IMAP a mnoho dalších. Na SCOM 2012 je totiž nejvíce zajímavé, jak moc dat umí ze sledovaných prvků získat.

Po jeho nasazení na běžné Cisco přepínače, byl SCOM 2012 schopen bez lokálního agenta za pomoci SNMP získat velice detailní informace o CPU, RAM, obsazených portech a jejich IP adresách, stav jednotlivých služeb apod. S vysokou pravděpodobností toto způsobuje vysoce sofistikovaná analýza nad SNMP protokolem.

Pro sledování a koncových stanic je k dispozici podobně jako u konkurenčních systémů lokálně instalovaný agent, který je schopen proaktivně zasahovat do dění na serveru / koncové stanici.

6 Vyhodnocení testů dle metodiky

Kritérium	Cacti	Nagios XI	SCOM 2012	Zabbix
Cena	3	1	0	3
Systémové požadavky	2	1	0	3
Uživatelské rozhraní	1	2	3	0
Náročnost implementace	0	2	3	1
Zátěž na síťové kartě	1	0	3	2
Reakce na výpadek	1	2	1	3
Identifikace postiženého segmentu	1	2	3	1
Automatické vyhledávání	0	2	3	1
Způsoby upozorňování	1	2	3	2
Doplňkové funkce	0	0	0	1
Spolupráce s jinými systémy	0	0	0	0
Hloubka monitoringu	1	1	1	1
Celkem	**11**	**15**	**20**	**18**
Pořadí	**4**	**3**	**1**	**2**

Tabulka 4 - Bodové vyhodnocení testů

V Tabulka 4 je uvedeno celkové bodové vyhodnocení podle stanovených kritérií a naměřených hodnot. Z hlediska ceny se na prvním a druhém místě umístili systémy Cacti a Zabbix. Je to dáno hlavně tím, že se jedná o volně dostupné programy a jejich pořizovací cena za licence je nulová. Obě řešení tak obdržela po třech bodech. Za třetí místo byl ohodnocen jedním bodem dohledový systém Nagios XI. Jeho licenční politika je podrobně popsána v kapitole 5.1.1. Na posledním místě se z pohledu cenového kritéria umístil produkt od společnosti Microsoft System Center Operations Manager 2012, který má nejvyšší finanční nároky na implementaci viz. kapitola 5.4.1.

Z hlediska hodnotícího kritéria systémových požadavků, byly dohledové systémy seřazeny od nejnižších nároků až po ty nejvyšší. Na prvním místě se tak umístil dohledový systém Zabbix s ohodnocením tří bodů. Druhé nejnižší systémové požadavky měl systém Nagios XI, který byl ohodnocen body dvěma. Na poslední bodové pozici se ziskem jednoho bodu se umístil systém Cacti. Bez bodů v tomto ohledu opět skončil SCOM 2012.

Jak už bylo zmíněno v kapitole 4.1.3, objektivně hodnotit uživatelské rozhraní je takřka nemožné. Bodové hodnocení dohledových systémů je tak v tomto ohledu ovlivněno subjektivním pocitem a výsledky se mohou u různých osob měnit. V mém případě dopadl nejlépe SCOM 2012 a to hlavně z důvodu možnosti výběru uživatelského rozhraní mezi webovým a desktopovou konzolí. Významnou roli v tomto rozhodování sehrál také fakt, že systém je od výrobce dodáván v českém jazyce a není nutné se spoléhat na překlad třetích stran. O bod méně bylo uděleno systému Nagios a to zejména za absenci českého překladu a možnosti obsluhy pouze přes webové rozhraní. Bod za třetí místo byl udělen systému Cacti a nula bodů získal v tomto kritériu systém Zabbix. Je to dáno hlavně nepříliš logickou posloupností kroků při správě sledovaných prvků.

V oblasti implementace byl jako nejjednodušší a nejrychlejší ohodnocen SCOM 2012, který má k dispozici přehledného průvodce a jeho nasazení bylo jednoznačně nejrychlejší také z důvodů inteligentního automatického vyhledávání viz. kapitola 5.4.8. Dva body za druhé místo obdržel Nagios XI jehož instalace byla za dodržení pokynů z dokumentace bezproblémová. O něco hůře skončil systém Zabbix, který zejména při nasazení vyžadoval od uživatele o něco větší úsilí než předchozí dva systémy. S nulovým ziskem bodů skončil systém Cacti zejména kvůli nutnosti instalace speciálních šablon pro každý typ zařízení.

V oblasti zátěže na síťové kartě jsou výsledky jednoznačně měřitelné a objektivní. Celkové srovnání testovaných dohledových systémů je zachyceno v grafu v příloze A. Z něj je patrné, že nejmenší datová zátěž byla naměřena u systému SCOM 2012, následovanému systémy Zabbix a Cacti. Na posledním místě, a tedy bez bodu, se umístil systém Nagios XI. Naměřené hodnoty i s časovým průběhem zachyceném v grafu je možné najít v dříve uvedených kapitolách u jednotlivých programů.

Kritérium reakce na výpadek bylo zejména hodnoceno z pohledu možného nastavení. V kapitole 4.1.6 jsou uvedeny podrobnosti a hlavně důvody, proč nedošlo k plánovanému měření. Nejlépe si v tomto ohledu vedl Zabbix, který umožňuje nastavit interval sledování po vteřinách a za to mu byly uděleny tři body. Je však nutné konstatovat, že v případě nastavením intervalu na velmi krátký časový úsek může dojít k situaci, kdy dohledový systém nestihne větší síť zkontrolovat, resp. nebude včas ukončena komunikace se všemi síťovými prvky. Na druhém místě se v ohledu reakce na výpadek umístil Nagios s možností minimálního intervalu jedné minuty. Jeden bod byl přidělen systémům SCOM 2012 a Cacti zejména z důvodů globálního nastavení sledovacího intervalu.

V oblasti identifikace postiženého segmentu jednoznačně nejlépe skončil SCOM 2012. Je to dáno především rekurzivním prohledáváním sítě a z toho plynoucí reálné znalosti topologie sledované sítě. Jako druhý byl ohodnocen Nagios XI zejména kvůli signalizace výpadku celé sledované větve namísto jednoho prvku (viz. 5.1.7). O třetí a čtvrté místo se dělí systémy Zabbix a Cacti. Oba dva systémy sledovanou síť sledují spíše jako lineární prostor adres a zajímají je spíše jednotlivá rozhraní, než prvky a spoje jako logický celek.

Při testování automatického vyhledávání sítě byl jednoznačným vítězem systém SCOM 2012, který využívá rekurzivní analýzu sítě a má tak reálný přehled o prohledávané topologii. I přes problémy s velkými adresními rozsahy byl systém Nagios XI ohodnocen dvěma body za druhé místo a to hlavně díky uživatelské přívětivosti celého procesu. Bod za třetí místo byl přidělen systému Zabbix. Tento systém si významně uškodil zejména absencí jednoduchého průvodce, který by uživateli celý proces zpříjemnil a zrychlil. Bez bodu zůstal systém Cacti, který tuto funkci standardně k dispozici nemá.

Nejvíce možností automatického upozorňování nabízí systém SCOM 2012. Nejméně naopak Cacti, který má k dispozici pouze upozornění emailová. O něco méně možností než SCOM 2012 má systém Nagios XI. Základní, přesto dostačující možnosti v oblasti upozorňování nabízí systém Zabbix a byl proto ohodnocen jedním bodem.

Z pohledu doplňkových funkcí bylo rozhodnuto o udělení jednoho bodu systému Zabbix za možnost inventarizace sledovaných prvků podle metodiky ITIL. Ostatní systémy ve standardní výbavě žádné doplňkové funkce neobsahují.

V oblasti kooperace s jinými systémy nezískal bod ani jeden systém. Jako standardní součást systému to neumožňuje ani jeden testovaný systém i když je to realizovatelné u většiny systémů přes API nebo přímým čtením databáze. Z hlediska kritéria hloubka monitoringu bylo všem systémům přiděleno po bodu, protože všechny jsou schopné, po správném nastavení, sledovat nejen spoje, ale i servery až na úroveň aplikací a systémových služeb.

V konečném zúčtování se tak nejlépe umístil SCOM 2012. Na tomto systému je znát dlouholetá orientace na sektor velkých společností a data center a nabízí tak vše potřebné pro sledování všech typů datových sítí. Jedinou jeho nevýhodou je tak cena, která je v počáteční fázi v porovnání s ostatními testovanými systémy, velmi vysoká. S osmnácti body se na druhém místě v celkovém hodnocení umístil systém Zabbix, který vynikal zejména v možnosti nastavení intervalu sledování. Na třetím místě se v celkovém součtu umístil systém Nagios XI a na posledním systém Cacti.

7 Závěr

Cílem této práce bylo porovnat, otestovat a vybrat vhodný dohledový systém pro síť menšího rozsahu, který by zároveň splňoval všechny požadavky na dohled moderního ICT prostředí.

Po prvním průzkumu a konzultacích s odborníky bylo vybráno několik vhodných kandidátů, z nichž byly po zralé úvaze o reálnosti implementace v laboratorních podmínkách a zamítnutých žádostech o testovací verze nakonec vybrány čtyři dohledové systémy, které byly nasazeny a otestovány. Pro tyto účely byla stanovena metodika testování a kritéria pro výběr nejvhodnějšího systému. Testování všech vybraných dohledových systémů probíhalo dlouhodobě. Bylo tak možné získat skutečně relevantní data.

Nejprve je nutné konstatovat, že ani jeden z dohledových systémů vyloženě nepropadnul. Celková ztráta systému Cacti se může zdát propastná, ale to je dáno spíše jinou filozofií k přístupu sledování sítě, než u ostatních systémů. Bohužel tento systém získal v celkovém hodnocení nejméně bodů.

Na třetí pozici zůstal dohledový systém Nagios XI. Z celkového pohledu této práce je toto umístění překvapivé. Nagios XI na autora od začátku působil dojmem profesionálního dohledového systému, který je schopen uživateli nabídnout vše co potřebuje a ještě něco navíc. Tento systém má pěkné a relativně intuitivní rozhraní. Celkově byla jeho činnost i po praktických zkušenostech hodnocena velmi pozitivně.

Nagios XI na třetí pozici přeskočil volně dostupný dohledový systém Zabbix. Zabbix je funkčně i parametrově výborný dohledový systém. Za celou dobu využívání tohoto systému autorovi nicméně subjektivně nevyhovovala logika ovládání a uživatelské rozhraní. Funkčně nicméně splňuje vše, co moderní ICT prostředí žádá a tak zaslouženě skončil na druhém místě.

Jako nejlepší dohledový systém, alespoň z pohledu této práce, byl vybrán komerční produkt SCOM 2012 za jehož vývojem stojí jeden z největších dodavatelů softwaru na světě společnost Microsoft. To že SCOM 2012 zvítězil, není podle autorova názoru nic překvapivého, vždyť kdo jiný, než samotný výrobce operačního systému s pobočkami po celém světě a tisíci zaměstnanci by měl vědět, jak by měl dohledový systém pracovat. SCOM 2012 je navíc otestován přímo v produkčních podmínkách, velkých datových center kdy Microsoft tvrdí, že veškerý software, který vydává, nejprve testuje sám na svých službách alespoň šest měsíců před oficiálním uvedením na trh. Bohužel velkou nevýhodou SCOM 2012 je jeho cena a hardwarová náročnost. To může být značně limitující pro většinu menších společností, protože jeho implementace se lehce může vyšplhat na statisíce. Z hlediska funkčnosti je však SCOM 2012 naprosto fenomenální a stal se tak zaslouženým vítězem.

Na závěr je vhodné konstatovat, že cíl práce se splnit podařilo a na jejím základě byla zahájena implementace celé sady nástrojů System Center 2012 pro testovanou reálnou síť a

zázemí v datovém centru. V průběhu práce se autorovi podařilo získat cenné zkušenosti se systémy, které do té doby neznal a nepoužíval a které se mu daří zužitkovat při nasazení systému do produkčního prostředí.

Použitá literatura

Bellis, Mary. 2013. Alexander Graham Bell - Biography. *About.com Inventors.* [Online] About.com, 2013. [Citace: 19. 8 2013.] http://inventors.about.com/library/inventors/bltelephone2.htm.

Blumenthal, U., Wijnen, B. a Lucent Technologies. 2002. User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3). *www.ietf.org.* [Online] 12 2002. [Citace: 10. 5 2013.] http://www.ietf.org/rfc/rfc3414.txt.

Bouška, Petr. 2013. SNMP - Simple Network Management Protocol. *www.samuraj-cz.com.* [Online] 2013. [Citace: 12. 5 2013.] http://www.samuraj-cz.com/clanek/snmp-simple-network-management-protocol/.

Case, J., a další. 2002. Message Processing and Dispatching for the Simple Network Management Protocol (SNMP). *www.ietf.org.* [Online] 12 2002. [Citace: 10. 5 2013.] http://www.ietf.org/rfc/rfc3412.txt.

Cisco Systems, Inc. 2008. Enterprise Campus 3.0 Architecture: Overview and Framework. *Design zone for Campus.* [Online] 2008. [Citace: 2013. 8 13.] http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/campover.html.

Dobrovolný, Martin. 2009. *IPOSI - Protokol IP verze 6 (přednáška).* [PDF] Pardubice : Univerzita Pardubice, 2009.

—. 2009. *IPOSI - Síťová vrstva (přednáška).* [PDF] Pardubice : Univerzita Pardubice, 2009.

Harrington, D., a další. 2002. An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks. *www.ietf.org.* [Online] 12 2002. [Citace: 15. 8 2013.] http://www.ietf.org/rfc/rfc3411.txt.

Information Sciences Institute University of Southern California. 1981. RFC 791: Internet Protocol. *www.ietf.org.* [Online] 9 1981. [Citace: 12. 5 2013.] http://www.ietf.org/rfc/rfc791.txt.pdf.

—. 1981. RFC 793: Transmission control protocol. *www.ietf.org.* [Online] 9 1981. [Citace: 12. 5 2013.] https://tools.ietf.org/rfc/rfc793.txt.

Leiner , Barry M., a další. 2013. Brief History of the Internet. *Internet Society.* [Online] Internet Society, 2013. [Citace: 19. 8 2013.] http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet.

Levi, D., a další. 2002. Simple Network Management Protocol (SNMP) Applications. *www.ietf.org.* [Online] 12 2002. [Citace: 10. 5 2013.] http://www.ietf.org/rfc/rfc3413.txt.

Microsoft Corporation. 2013. Operations Manager. *Microsoft Technet library.* [Online] Microsoft Corporation, 15. 1 2013. [Citace: 12. 8 2013.] http://technet.microsoft.com/en-us/library/hh205987.aspx.

Murray, Peter a Stalving, Paul. 2008. *SNMP: Simplified.* [PDF] Seattle : F5 Networks, Inc, 2008.

Nagios Enterprises, LLC. 2011. Nagios – Monitoring Architecture Solutions For Managed Service Providers. *Nagios - The Industry Standard in IT infrastructure monitoring.* [Online] 9 2011. [Citace: 12. 5 2013.] http://assets.nagios.com/downloads/general/docs/Monitoring_Architecture_Solutions_For_MSPs.pdf.

—. 2013. Nagios - The Industry Standard in IT Infrastructure Monitoring. [Online] Nagios Enterprises, LLC, 2013. [Citace: 13. 5 2013.] www.nagios.com.

—. 2012. Nagios Support Wiki. *Nagios.* [Online] Nagios Enterprises, LLC, 27. 9 2012. [Citace: 2. 5 2013.] http://support.nagios.com/wiki/index.php/Main_Page.

Postel, J. 1981. Internet control message protocol. *www.ietf.org.* [Online] 9 1981. [Citace: 12. 5 2013.] http://tools.ietf.org/pdf/rfc792.pdf.

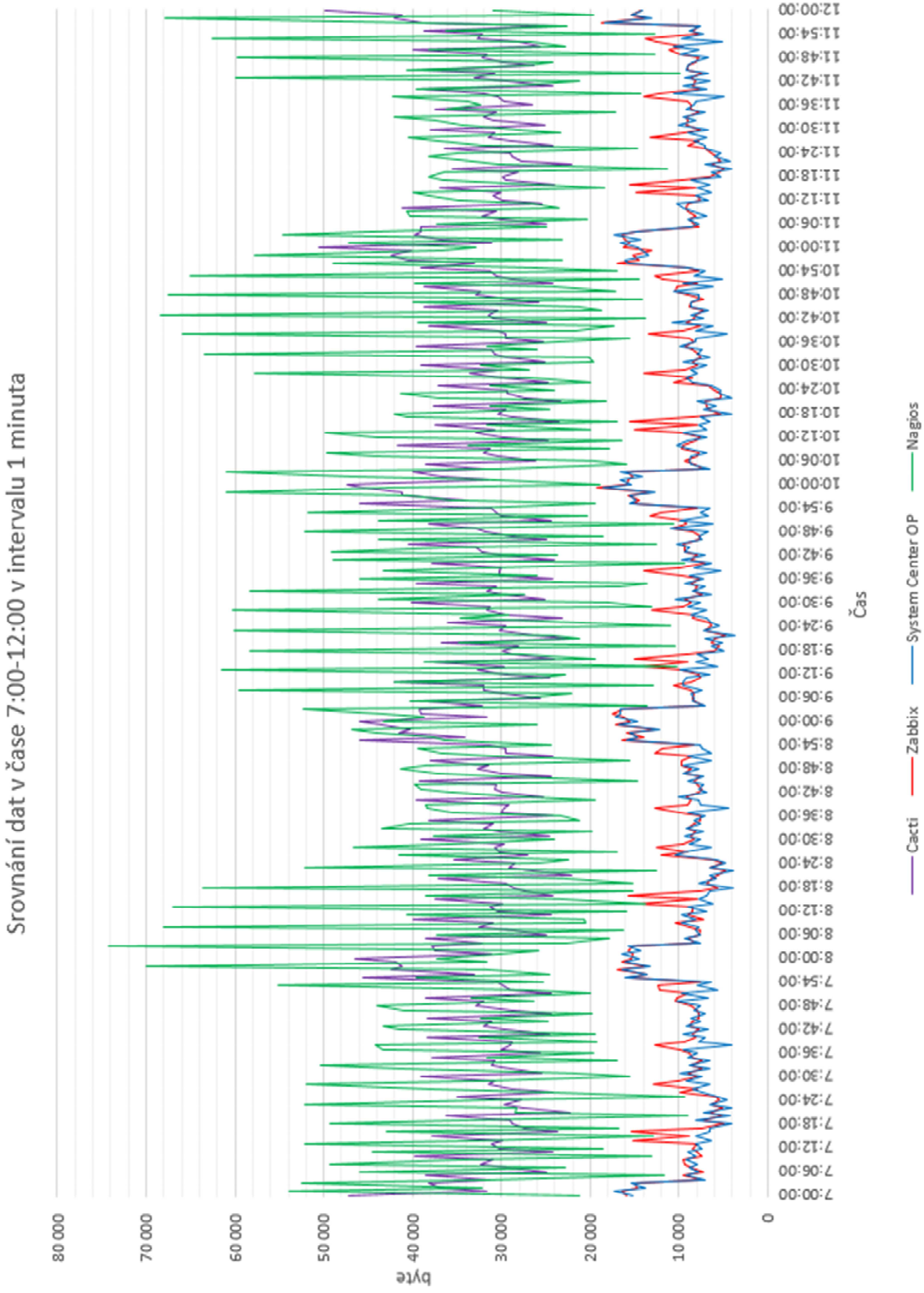
—. 1980. RFC 768: User Datagram Protocol. *www.ietf.org.* [Online] 28. 8 1980. [Citace: 12. 5 2013.] http://www.ietf.org/rfc/rfc768.txt.pdf.

The Cacti Group, Inc. 2012. Documentation. *Cacti the complete rrdtool-based graphic solution.* [Online] The Cacti Group, Inc, 2012. [Citace: 6. 5 2013.] http://www.cacti.net/documentation.php.

Wijnen, B., a další. 2002. Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP). *www.ietf.org.* [Online] 12 2002. [Citace: 10. 5 2013.] http://tools.ietf.org/rfc/rfc3416.txt.

ZABBIX SIA. 2012. Documentation. *Zabbix The Enterprise-class Monitoring Solution for Everyone.* [Online] 24. 5 2012. [Citace: 12. 8 2013.] http://www.zabbix.com/documentation.php.

Příloha A – Porovnání datového toku na síťové kartě



Příloha B – DVD s elektronickými materiály

DVD Obsahuje následující materiály:

- Text práce v PDF
- Soubor aplikace MS Excel s naměřenými daty
- Soubor aplikace MS Visio s použitými ilustracemi
- Projekt simulátoru GNS s laboratorním prostředím
- Soubory programu Wireshark s naměřenými daty