Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Monitoring počítačové sítě

Autor: Lukáš Dvořák

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Katedra informačních technologií

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Lukáš Dvořák

Informatika

Název práce

Monitoring počítačové sítě

Název anglicky

Computer network monitoring

Cíle práce

Cílem práce je detailní zhodnocení komerčních i nekomerčních řešení pro monitoring počítačové sítě.
Dílčím cílem práce je ukázat důležitost takových systémů a jejich neodmyslytelnou přítomnost u každého poskytovatele síťového připojení nebo serverových služeb.
Dalším cílem práce je nastínit práci s vybranými programy pro monitoring sítě.
Na základě všech poznatků je na závěr doporučena nejlepší kombinace dostupných řešení.

Metodika

Teoretická část představuje jednotlivé programy pro monitoring počítačové sítě. Je zde vzpomenuta důležitost těchto systémů pro co nejvíce bezproblémový chod počítačové sítě. Uvedené informace čerpá autor z dostupných zdrojů a zejména pak z řešení, která jsou provozována ve zvolené firmě. Na základě získaných informací je navrhnuto optimální řešení pro střední počítačovou síť. V poslední části jsou formulovány závěry a doporučení.

Doporučený rozsah práce

40 – 50 stran

Doporučené zdroje informací

BOUŠKA, Petr. Začínáme s monitoringem sítě. Samuraj-cz [online]. 2009 [cit. 2014-02-03]. Dostupné z: http://www.samuraj-cz.com/clanek/zaciname-s-monitoringem-site/

HORÁK, Jaroslav a Milan KERŠLÁGER. Počítačové sítě pro začínající správce. 5., aktualiz. vyd. Brno: Computer Press, 2011, 303 s. ISBN 978-80-251-3176-3

JAMRICH, Marián. Nagios: monitorovanie počítačovej siete. Nagios: monitorovanie počítačovej siete [online]. 2010, [cit. 2014-02-04]. Dostupné z: http://www.root.cz/clanky/nagios-monitorovanie-pocitacovej-siete/

JOSEPHSEN, David. Nagios: building enterprise-grade monitoring infrastructure for systems and networks. Second edition. Spojené státy: Prentice Hall, 2013, xix, 275 pages. ISBN 01-331-3573-X.

ŠTRAUCH, Adam. Icinga: monitorování sítí a serverů. Icinga: monitorování sítí a serverů [online]. 2011, [cit. 2014-02-04]. Dostupné z: http://www.root.cz/clanky/icinga-monitorovani-siti-a-serveru/

TABONA, Andrew Zammit. The Top 20 Free Network Monitoring and Analysis Tools for Sys Admins. The Top 20 Free Network Monitoring and Analysis Tools for Sys Admins [online]. 2013, [cit. 2014-02-04]. Dostupné z: http://www.gfi.com/blog/the-top-20-free-network-monitoring-and-analysis-tools-for-sys-admins/

VILEMAITIS, Marius. Hp Network Node Manager 9: Getting Started. Birmingham, U.K: Gardners Books, 2010. ISBN 18-496-8084-1

Předběžný termín obhajoby

2015/06 (červen)

Vedoucí práce

Ing. Jiří Vaněk, Ph.D.

Elektronicky schváleno dne 31. 10. 2014

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 11. 11. 2014

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 09. 03. 2015

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Monitoring počítačové sítě" jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 16. 3. 2015 _____

Poděkování

Chtěl bych touto cestou poděkovat panu Ing. Jiřímu Vaňkovi, Ph.D. za odborné vedení práce a za hodnotné připomínky. Dále chci poděkovat firmě CESNET, z. s. p. o., která mi poskytla cenné zkušenosti, které byly využity v celém rozsahu práce.

Monitoring počítačové sítě

Computer network monitoring

Souhrn

Práce se zaměřuje na zhodnocení dostupných řešení pro monitoring počítačové sítě a postupy při jejich provozu. V první části se zaměřuje na teoretické uvedení do problematiky sítí a možnosti jejich sledování. Pokračuje s uvedením příkladů nástrojů, které se k tomuto sledování používají, a jejich krátkým představením. V další části se věnuje podrobným rozpracováním možnosti práce s vybranými nástroji vhodnými pro zvolenou síť. Ukazují se zde postupy instalace i práce na konkrétních typech úloh. V závěrečné části dochází ke zhodnocení zvolených nástrojů ve scénářích, které mohou v síti nastat. Je zde uvedena reakce nástrojů na vybrané situace. Na závěr je uvedeno zhodnocení přínosu zvolených nástrojů pro síť.

Summary

The work is focused on valorization of aviable solutions for monitoring a computer network and procedures in their service. The first part is focused on theoretical introduction to problematic of networks and possibilities of their observation. It continues with introduction of examples of tools, which are used for this observation and their short introduction. The next part is focused on detailed description of possibilities of work with selected utilities suitable for selected network. There are shown procedures of instalation and work with on specific types of taks. In final part, there is appreciation of selected utilities in scenarios, which can occur in network.There are introduced examples of reactions of utilities on selected situations. In the final part, there are appreciation of benefits of selected utilities for the network.

Klíčová slova: počítačová síť, monitoring, DWDM, Nagios, Node Manager, Open View, Icinga, CTC

Keywords: computer network, monitoring, DWDM, Nagios, Node Manager, Open View, Icinga, CTC

Obsah

1 Úvod 10
2 Cíl a metodika práce 11
2.1 Cíl práce 11
2.2 Metodika práce 11
3 Teoretická východiska 12
3.1 Počítačová síť 12
3.1.1 Co je to počítačová síť 12
3.2 Monitoring počítačové sítě 12
3.3 Kategorie monitorovacích nástrojů 12
3.3.1 Upozorňování 13
3.3.2 Monitoring cloudu 13
3.3.3 Monitoring logu událostí 13
3.3.4 Monitorování provozu po síti 14
3.3.5 Nástroje pro diagnostiku sítě 14
3.3.6 Protokol SNMP 15
3.3.7 Typy nástrojů pro monitoring sítě 16
3.3.8 Co vše můžeme sledovat 17
3.3.9 Jak můžeme sledovat 18
3.4 Nástroje pro monitoring sítě 19
3.4.1 Komerční 19
3.4.2 Nekomerční 23
4 Praktická část 27
4.1 Monitorování uzlů sítě a tras mezi nimi 27
4.1.1 HP Network Node Manager 27
4.1.2 Icinga 35

4.1.3 Cisco Transport Controller 39
5 Zhodnocení výsledků 43
6 Závěr 48
7 Bibliografie 49
8 Seznam použitých obrázků a tabulek 50
9 Seznam použitých zkratek 52

1 Úvod

Pojmem počítačová síť se myslí spojení dvou a více počítačů nebo jiných koncových zařízení tak, aby mohly sdílet své hardwarové nebo softwarové prostředky. V době, kdy počítačové sítě nebyly, musel mít například každý počítač, který byl určen pro tisk, vlastní tiskárnu. Dnes jsou již věci, jako je sdílení tiskáren nebo jiných prostředků samozřejmostí. Nedílnou součástí správně fungující sítě jsou monitorovací nástroje, které sledují její chod. (1)

Monitorování sítě obecně hraje klíčovou roli ve včasném odhalení závad nebo událostí, které mohou závadu způsobit. Bez takovýchto nástrojů bychom se v každodenním životě potýkali s nepříjemnými, ale i život ohrožujícími událostmi. Mnoho lidí totiž bere přístup k síti či službám jako samozřejmost, proto musí existovat profesionální řešení, která povedou k co nejvíce bezproblémovému chodu sítě a služeb.

Monitoring sítě se objevuje v mnoha podobách a využívá mnoho nástrojů a protokolů. Pokud chceme mít nad sledovanými objekty naprostou kontrolu a do detailů znát princip upozorňování, můžeme si napsat vlastní skript či program, který bude danou akci vykonávat. Pro tento způsob ale potřebujeme detailní znalosti programování. Ve většině případů se využívají již zaběhlé, volně dostupné či placené programy. (1)

2 Cíl a metodika práce

2.1 Cíl práce

Cílem práce je detailní zhodnocení komerčních i nekomerčních řešení pro monitoring počítačové sítě. Dílčím cílem je ukázat důležitost takových systémů a jejich neodmyslitelnou přítomnost u každého poskytovatele síťového připojení nebo serverových služeb. To je provedeno výčtem možných situací, které mohou nastat, a tím, jak je nástroje zachytí.

Dalším cílem práce je nastínit práci s vybranými programy pro monitoring sítě. Ukázat jejich uživatelské prostředí a udělat doporučení pro jejich efektivní provoz.

Na základě všech poznatků je na závěr doporučena nejlepší kombinace dostupných řešení.

2.2 Metodika práce

Teoretická část představuje jednotlivé programy pro monitoring počítačové sítě. Jak komerční, tak nekomerční. Je zde vzpomenuta důležitost těchto systémů pro co nejvíce bezproblémový chod počítačové sítě.

Uvedené informace čerpá autor z dostupných zdrojů a zejména pak z řešení, která jsou provozována ve firmě CESNET, z. s. p. o., Na základě získaných informací je navrhnuto optimální řešení pro střední až velkou počítačovou síť. V poslední části jsou formulovány závěry a doporučení.

3 Teoretická východiska

3.1 Počítačová síť

První počítačové sítě se začaly objevovat v padesátých letech minulého století, přesto se začala masivněji používat až začátkem osmdesátých let. Nástup počítačové sítě dostál takového rozmachu, že dnes již jen těžko najdeme počítač nebo jiné počítačové zařízení, které není zapojeno do sítě.

3.1.1 Co je to počítačová síť

Počítačová síť je složena z aktivních a pasivních prvků. Tyto prvky jsou propojeny ethernetovými, optickými kabely anebo bezdrátovým spojením. Aktivní prvky jsou routery, switche, huby a pasivní prvky jsou ethernetové kabely, terminátory a jiné prvky, které aktivně nezasahují do chodu sítě.

(2)

3.2 Monitoring počítačové sítě

Monitoring počítačové sítě znamená využívání nástrojů, které nepřetržitě monitorují síť, aby zjistily pomalé nebo selhávající komponenty a výpadky serverových služeb, a poté notifikují administrátora prostřednictvím mailu, sms a nebo jen zobrazením varovné hlášky v prostředí nástroje.

Tato funkce je pro síťového administrátora velice důležitá, protože bez ní by stav sítě zjišťoval jen velice pomalu a složitě. Zajišťuje tedy včasné odhalení poruchy a dávají více času na nápravu problému.

Výsledkem nasazení monitorovacích nástrojů je vyšší spolehlivost sítí, serverových služeb a dalších prvků sítě, které se dají monitorovat.

3.3 Kategorie monitorovacích nástrojů

Nástroje pro monitoring se sdružují v oddělených kategoriích. Mnoho nástrojů obsahuje více kategorií, které se navzájem překrývají. Ve skutečnosti téměř všechny nástroje obsahují více než jednu kategorii. Ve výčtu níže jsou zmíněny pouze ty nejdůležitější kategorie a jejich zástupci.

3.3.1 Upozorňování

Upozorňování je v monitoringu sítě velice důležité. Díky němu se administrátor sítě nebo jiná pověřená osoba dozvídá o problémech či nastalých situacích. Probíhá různými způsoby a často dochází k jejich kombinaci. Nástroje pro upozorňování mohou být samostatnými programy nebo jsou častěji součástí monitorovacích nástrojů. Některé organizace transparentně ukazují stav svých služeb, serverů či linek na speciálně k tomu určené stránce, a tak může být upozorňován i zákazník, a nejenom administrátor.

Níže jsou uvedeny základní druhy upozornění.

- Email
- Pager
- Sms
- Systémové logy
- Webové rozhraní nástroje
- RSS
- Sociální sítě

(3)

3.3.2 Monitoring cloudu

U monitoringu cloudu je důležité kontrolovat jak hardwarovou tak softwarovou část. U hardwarové části se kontroluje vytíženost procesorů, disků nebo paměti. U softwarové části je kontrolováno vytíženost vláken a počet jednotlivých instancí a procesů. Díky těmto poznatkům můžeme předpovídat využití prostředků v čase a umožňuje se tak přizpůsobit trendům.

(4) (3)

3.3.3 Monitoring logu událostí

Tento způsob monitoringu spočívá v procházení předem vytvořených logů a hledání požadovaných událostí. Logy mohou být uloženy v různých formátech od textového

dokumentu po speciální RSS kanál. Výsledky se pak dají uložit, nebo se může provést jiná navolená akce.

Můžeme monitorovat logy například z:

- Routerů
- Switchů
- Windows platforem
- Unixových platforem
- IIS[1] web serverů
- IIS FTP serverů
- SQL[2] serverů
- Databázových serverů

(3)

3.3.4 Monitorování provozu po síti

Při provozu sítě dochází k jejímu zatížení. Pokud je šířka pásma nedostatečná, dochází ke zpomalení provozu po síti nebo jejímu úplnému zhroucení. Nástroje pro monitorování provozu po síti nám pomáhají určit slabé články, které síť brzdí a přetěžují.

(3)

3.3.5 Nástroje pro diagnostiku sítě

Při provozu sítě musíme provádět její diagnostiku a ověřovat tím, jestli je síť provozuschopná anebo jestli na ní nedochází k výpadkům. K tomu nejčastěji slouží nástroje, které provádějí test dostupnosti síťového protějšku různými způsoby.

- Ping: Nástroj pro zjištění, jestli je specifická IP adresa dostupná v síti. Můžeme nakonfigurovat počet paketů vyslaných příkazem ping, velikost a čas, který se má čekat na příchozí paket a timeout.

---

[1] IIS - Internet Information Services http://www.iis.net/

[2] SQL – Rozšířený databázový jazyk

- Ping Scan: Nástroj, který zjišťuje dostupnost velkého rozpětí IP adres. Používá základní funkci Ping
- SNMP Ping: Nástroj, který zjišťuje, zda specifická IP adresa podporuje SNMP. Pomáhá síťovým technikům ke zjištění dostupnosti zařízení a také poskytuje základní informace, jako jsou DNS názvy, systémové názvy, polohu, typ systémů a popis systému.
- SNMP Scan: Nástroj, který provádí to co SNMP Ping, ale v nějakém rozsahu IP adres.
- Proxy ping: Umožňuje provést PING test vzdáleně z jiného zařízení a zjistit tak dostupnost dálkově.
- Trace route: Umožňuje záznam cesty (cestou se myslí počet skoků, například počet routerů na trase k cíli) sítí mezi IP adresou odesílatele a specifickou adresou příjemce. Uživatel může nadefinovat věci jako počet skoků a velikost timeoutu.

(5)

Výstup může být uložen do souboru (text, XML, HMTL, nebo Excel, zatímco Ping nebo Trace route testy mohou být znázorněny graficky.

(3)

3.3.6 Protokol SNMP

Zkratka SNMP znamená Simple Network Management Protocol. Tento protokol dovoluje proaktivně sledovat, co se děje na zařízeních v síti a napravit problémy dříve, než nabudou větších rozměrů. Byl uveden v roce 1988 a nyní obsahuje tři odlišné verze SNMPv1. SNMPv2 a SNMPv3. Verze SNMPv1 a SNMPv2 má slabší zabezpečení, protože k autentizaci využívá pouze heslo v textové podobě. Verze SNMPv3 využívá k autentizaci jméno i heslo, a to celé doplňuje šifrování.

(6)

Protokol SNMP umožňuje sledovat například tiskárny, různá čidla, aktivní síťové prvky a v neposlední řadě i osobní počítače a servery po nainstalování potřebného softwaru a ovladačů. Požadované hodnoty si můžeme vyžádat anebo je sbírat v časových intervalech

a ukládat je do databáze. Z ní pak můžeme vytvořit graf a přehledně tak zobrazit stav vytížení procesoru, jeho teplotu anebo stavy portů v průběhu času.

Protokol SNMP pracuje na principu správce a agenta. Jsou zde tedy dvě strany, které mezi sebou komunikují. Komunikace probíhá dvěma různými způsoby:

- Správce posílá agentovi dotazy, na které agent odpovídá. Dotazy mohou být zasílány více správci.
- Agent zasílá oznámení v určitých situacích. V předem definovaných situacích, jako je například zvýšený CPU load na přepínači, nebo i v pravidelném časovém intervalu odesílá oznámení agent na určenou adresu správce. Využívá k tomu takzvané trapy.

(7)

Nástroje, které využívají SNMP prokolol:

- MIB Browser[3]
- Paessler SNMP Tester[4]
- Net-SNMP[5]

(7)

3.3.7 Typy nástrojů pro monitoring sítě

Pro monitoring sítě existuje řada komerčních i nekomerčních nástrojů. Liší se většinou uživatelskou podporou, možnosti konfigurace a složitostí nastavení.

Nástroje zdarma jsou často univerzální a vyžadují detailnější nastavování a znalost psaní vlastních skriptů. Výhodou je však hlubší znalost toho, co a jak monitorujeme.

Komerční nástroje mají řadu předdefinovaných šablon a nastavení je tak otázkou minut.

[3] MIB Browser - http://ireasoning.com/mibbrowser.shtml

[4] Paessler SNMP Tester - http://www.paessler.com/tools/snmptester

[5] NET-SNMP - http://www.net-snmp.org/

3.3.8 Co vše můžeme sledovat

Obecně můžeme pomocí nástrojů monitorovat:

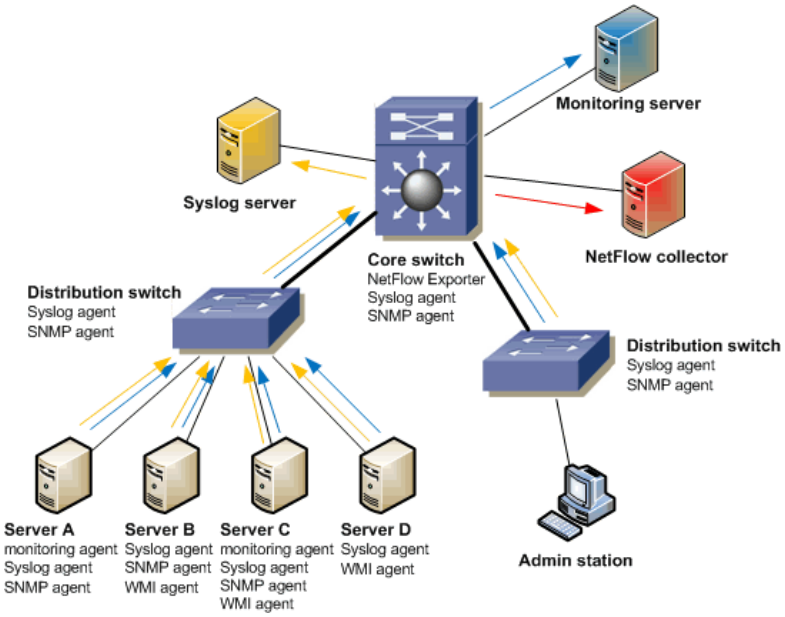
- Servery a jejich služby
- Aktivní síťové prvky
- Síťovou komunikaci
- Bezpečnost

Pak existují specifické oblasti, kde pro úplnost informací musíme použít specializované nástroje, které danou problematiku monitorují lépe. Jedná se například o IP telefonii, bezdrátové sítě a virtuální prostředí.

Podrobnější rozdělení toho, co může administrátora zajímat, je:

- Dostupnost serverů
- Dostupnost služeb / aplikací
- Události na serverech
- Vytížení zdrojů jako je procesor, paměť anebo disk
- Objem přenosu dat na linkách
- Statistiky síťového provozu
- Periferní zařízení (UPS, teplotní a vlhkostní senzory, dveřní západky a kapalinové detektory)
- Analýza nestandardního chování v síti
- Informace o portech switchů / routerů
- Monitoring Wifi nebo IP telefonie
- Bezpečnostní incidenty

(8)



Obrázek 1: Schéma monitorování sítě. Zdroj http://www.samuraj-cz.com/

3.3.9 Jak můžeme sledovat

Pro dohled nad servery se většinou používají dva způsoby:

Monitorování s agentem – to znamená instalaci speciálního softwaru na daný server a operační systém. Tento software se jmenuje agent.

Monitorování bez agenta – tímto způsobem se testují samotné služby serveru nebo se data získávají pomocí standardních protokolů, jako jsou SNMP, WMI nebo IPMI.

Níže jsou uvedeny technologie, které jsou pro daný způsob monitoringu důležité

- pomocí takzvaného ping testu se ověřuje dostupnost serveru
- dostupnost služby pomocí TCP
- zachytávání události ze serverů - Syslog
- získávání údajů pomocí klienta
- získávání údajů pomocí monitorovacích protokolů WMI, SNMP, IPMI
- sledování síťových toků - NetFlow
- analýza síťových protokolů - network protocol analyzer
- bezpečnost v síti - IDS/IPS

(1)

3.4 Nástroje pro monitoring sítě

Nástroje pro monitoring sítě můžeme rozdělit do dvou kategorií, a to komerční a nekomerční.

3.4.1 Komerční

Komerční nástroje pro monitoring počítačové sítě mají jednu velkou výhodu, a tou je podpora. Tato výhoda je ale vykoupena faktem, že tento software je většinou placený a může se používat jen s omezeními danými jeho licencí.

3.4.1.1 HP Network Node Manager

HP Network Node Manager[6] (NNM) je velmi mocným nástrojem pro monitoring počítačové sítě. Dokáže automaticky prohledávat síť a podle toho i kreslit IP mapu. Jakmile NNM rozpozná nalezená zařízení, dokáže zobrazit, jaký by byl dopad pro síť, jestliže by byla zařízení nebo rozhraní nedostupná nebo by výkonnostní parametry (jako je zpoždění) překročily nastavené limity (thresholdy). Stav sítě je NNM mapována užitím dvou typů informačních zdrojů.

- Zprávy poslané ze spravovaných zařízení (SNMP trapy)
- Standardní polly, které kontrolují stav zařízení nebo konfigurační změny

NNM dokáže monitorovat výkonnostní parametry, jako jsou využití rozhraní, chyby rozhraní, zatížení CPU nebo jakoukoliv jinou informaci o výkonu, která je poskytnuta SNMP agentem zařízení. Jestliže některý z výkonnostních parametrů překročí povolené limity (tresholdy) nebo jestliže nastane chyba ve spravovaném zařízení, NNM dokáže vygenerovat zprávu do prohlížeče incidentů. Zároveň nemůže být NNM považován za souhrnný nástroj pro management. Například NNM ve verzi 8.x nedokáže sbírat žádná data o výkonu, na delší čas je uložit anebo zobrazit pokročilou zprávu o kapacitě a výkonu. Na rozdíl od toho NNM ve verzi 9.0 už má možnosti jako jsou například výkonnostní grafy.

[6] Dříve pod názvem HP OpenView

Přesto všechno NNM jako takový nemá následující možnosti:

- Flexibilní ukládání dat
- Pokročilá analýza výkonnostních dat

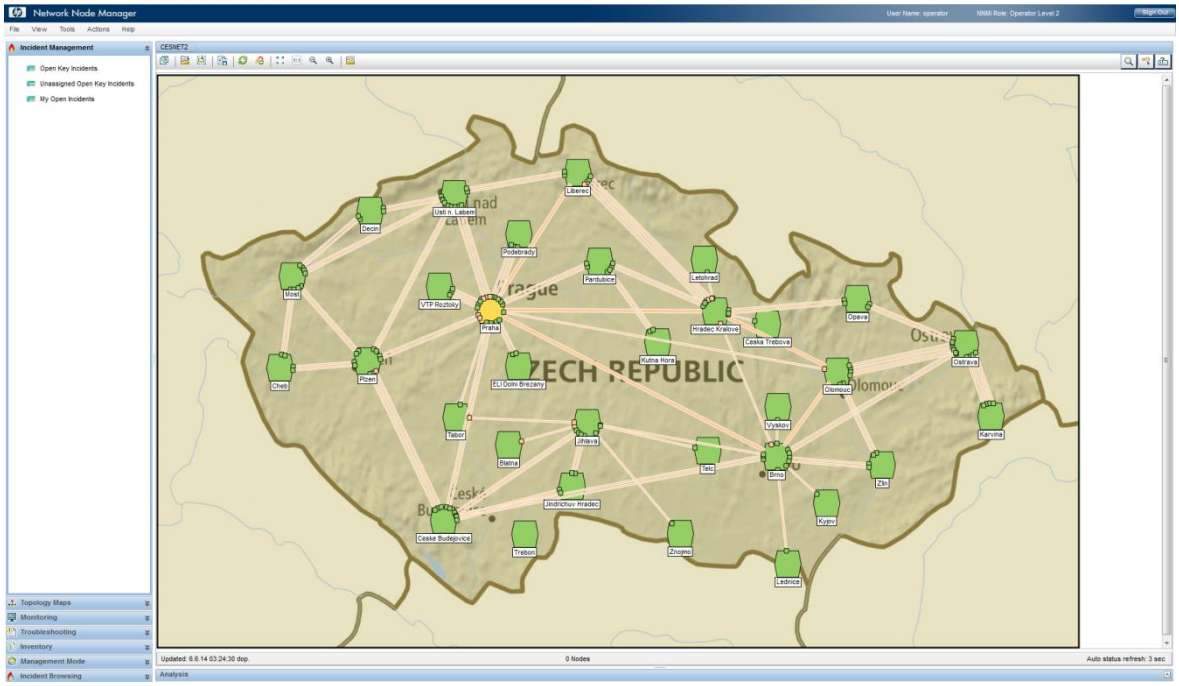
NNM poskytuje detailní informace o zařízeních, které byly buď načteny v průběhu vyhledávání, nebo vloženy manuálně NNM operátorem. Dokáže zobrazit konfigurace zařízení, jako jsou seznamy rozhraní, nakonfigurované VLANy[7], sériová čísla nebo kontaktní informace na odpovědné osoby. NNM nedokáže udělat zálohu konfigurace sítě anebo obnovit její funkci. V zásadě nedokáže jakkoliv měnit konfiguraci zařízení.

Ačkoliv je NNM navržen pro spravování zařízení určených pro chod sítě, dokáže vyhledat a monitorovat jakékoliv zařízení s IPv4 nebo IPv6 adresou. Díky tomu dokáže pracovat s pracovními stanicemi, servery nebo s jakýmikoliv zařízeními s podporou SNMP. NNM ale nemůže být považován za nástroj pro správu serverů, protože nedokáže monitorovat pro server specifické hardwarové nebo softwarové operační parametry. Dokáže vyhledat všechny IP rozhraní na serverech, ale nedokáže rozpoznat žádné jiné hardwarové informace jako je počet a kapacita disků, paměti CD/DVD mechanik atd. I když NNM nemá mnoho využití v oblasti monitoringu pracovních stanic nebo serverů, jsou případy, kdy může být monitorování serverů tímto nástrojem užitečné. Některé servery nebo pracovní stanice musejí být neustále zapnuté a zároveň nejsou monitorované nebo spravované žádným jiným nástrojem. V takovýchto případech mohou být takovéto uzly přidané do NNM pro monitorování stavu.

Zkráceně můžeme NNM považovat za nástroj, který pomůže vyřešit výpadky sítě, bude monitorovat síťové trasy, pomůže identifikovat příčinu problému a který bude monitorovat a oznamovat některé problémy v oblasti výkonu sítě.

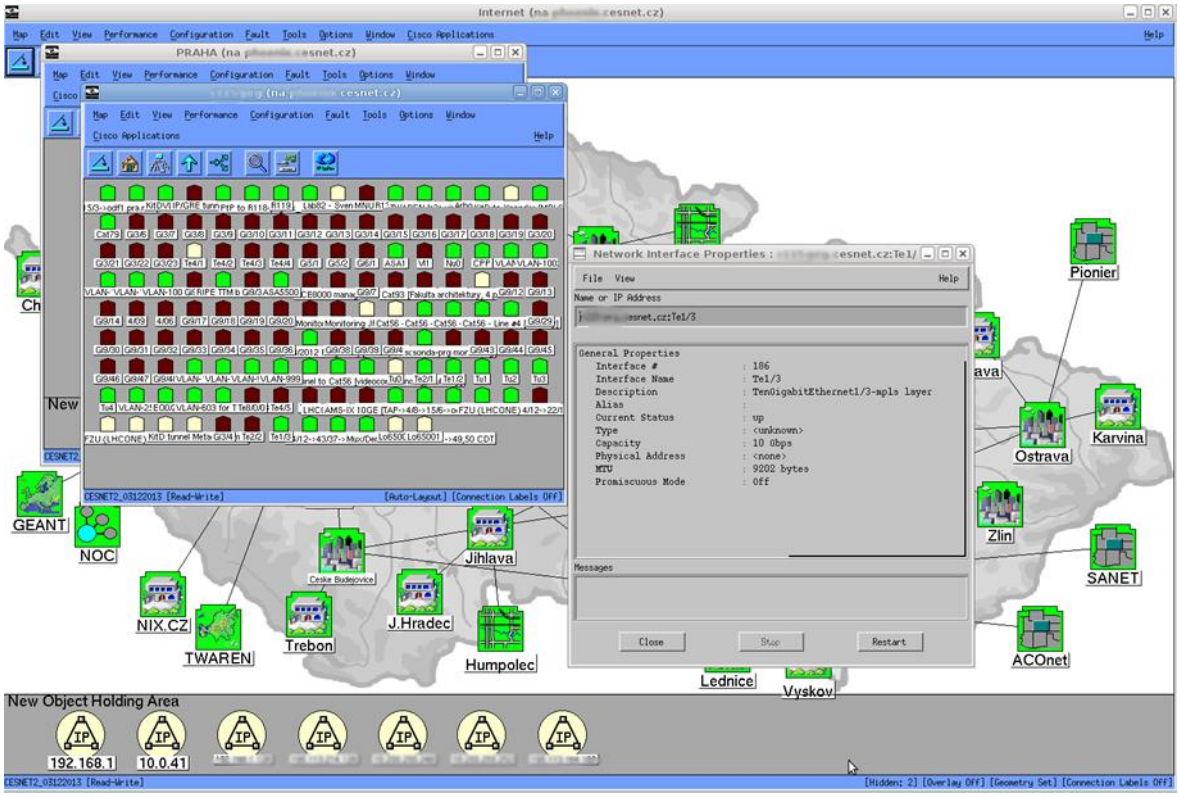
(8)

[7] VLAN – virtuální LAN. Logicky nezávislá síť nezávislá na infrastruktuře



Obrázek 2:Networkd Node Manager. Screenshot CESNET

Předchůdcem Network Node Manageru je HP OpenView, který se ještě nezobrazoval v klasickém internetovém prohlížeči a neumožňoval tolik pokročilých funkcí.



Obrázek 3: HP OpenView. Screenshot CESNET

3.4.1.2 Cisco Transport Controller

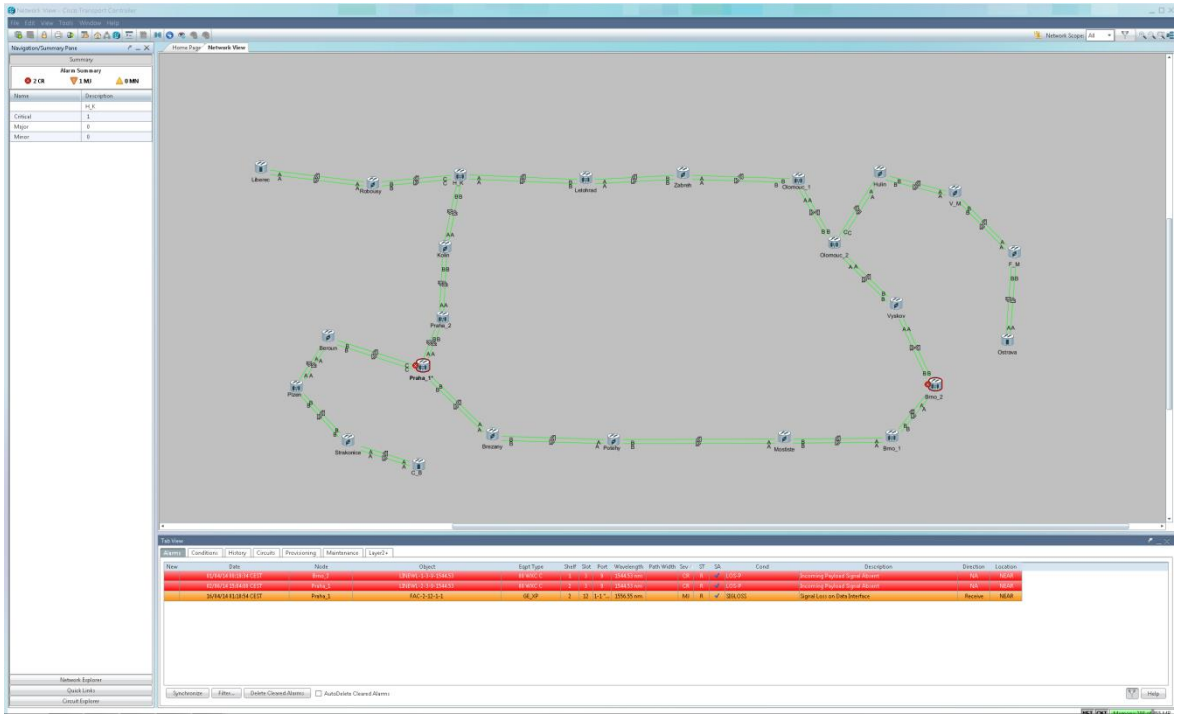
Cisco Transport Controller (CTC) je GUI[8] management nástroj, který může být použit pro operace, administraci a management různých druhů optických sítí. CTC je typicky užíván jako GUI navrhovací nástroj v průběhu vývoje a implementace optických sítí. CTC akceptuje input uživatele v grafické podobě a konvertuje příkazy do Transaction Language 1 (TL1) příkazů, které akceptují optické prvky zařízení.

CTC software je předinstalován na TCC2 kontrolních kartách ONS 15454. Jestliže je uvedena nová verze MSSP, je potřeba nainstalovat novou verzi CTC na TCC2. CTC k běhu na PC nebo jiné stanici potřebuje standardní internetový prohlížeč s povoleným Java Runtime Environment (JRE). CTC je automaticky staženo jako applet z TCC2 a nainstalováno na PC nebo jinou stanici po tom, co se uživatel zaloguje do ONS 15454.

(9)

Tento nástroj na hlavní obrazovce zobrazuje síťový přehled, který obsahuje skupiny spojených uzlů. Tato spojení jsou uskutečněna optickými vlákny. Pod touto obrazovkou jsou pak zobrazeny případné poruchy na vláknech. Pokud nastane nějaká porucha, například Incoming Payload Signal Absent nebo Signal Los on Data Interface, je zde přehledně vyobrazeno, o jaké vlákno se jedná a na jaké vlnové délce operuje.

[8] GUI – grafické rozhraní



Obrázek 4:Cisco Transport Controller. Screenshot CESNET

3.4.2 Nekomerční

3.4.2.1 Nagios

Nagios[9], neboli „Nagios Ain't Gonna Insist On Sainthood“ dokáže testovat nejrůznější síťové služby jako například ping, běžící procesy, velikost diskových kvót, zatížení systému, systém uptime, S. M. A. R. T. test HDD, vytížení procesorů atd. Je vyvíjený pod licencí GNU GPL. To znamená, že je volně k dispozici pro osobní i komerční použití a je dovoleno ho kopírovat i upravovat. Samotný Nagios, respektive jeho jádro, neumí testovat žádné služby. Tuto funkcionalitu obstarávají až zásuvné moduly (pluginy). Jsou to malé programy či skripty, které vykonávají požadované operace.

Výstup z Nagiosu je uskutečněný maximálně 80 znaky a návratový kód od 0 do 3.

[9] Nagios - http://www.nagios.org/

OK = 0	Plugin nemá problém s otestováním služby a nenarazil na žádný problém, tak je vyhodnocena jako korektně pracující.
Warning = 1	Plugin nemá problém s otestováním služby, avšak její stav je vyhodnocený jako „Warning“, protože dosáhl hodnoty nadefinované administrátorem.
Critical = 2	Plugin vyhodnocuje stav „Critical“, pokud je daná služba nedostupná, nebo její stav dosáhl kritické hodnoty.
Unknown = 3	Plugin není schopen otestovat službu, není schopen přečíst data z pasivního testu, nebo nastala neznámá chyba.

(10)

Nagios používá dvě oddělené metody, které se dělí do skupin

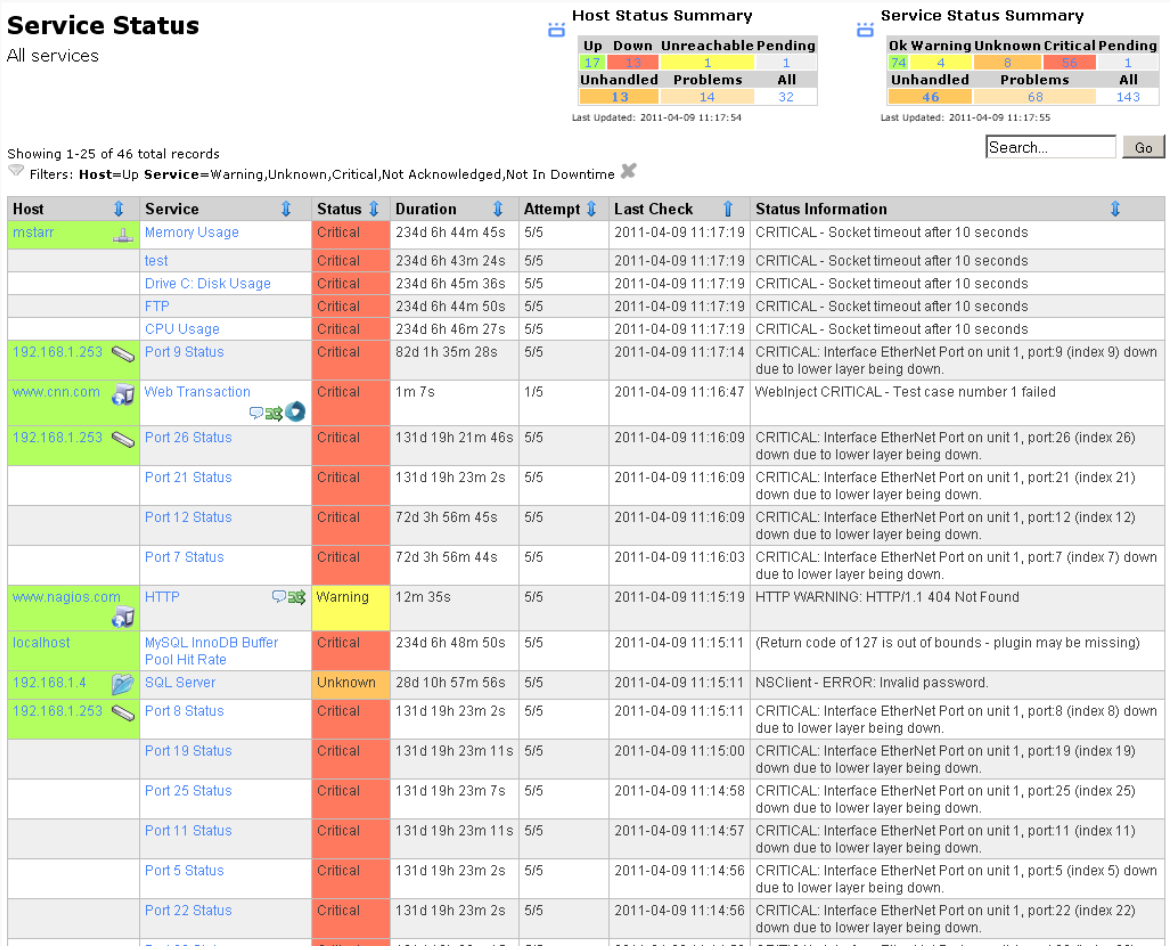
- Pasivní
- Aktivní

Pasivní monitorování spočívá v poslouchání síťového provozu, do sítě neposílá žádné testovací pakety. Nezatěžuje počítačovou síť.

Aktivní monitorování spočívá v posílání testovacích paketů do sítě a na servery, čímž aktivně kontroluje dostupnost a stav služeb. Nevýhodou je zvýšení zátěže na síť.

Nagios dovede upozorňovat nejrůznějšími způsoby. Od mailové zprávy na předdefinovaný mail až po sms zprávu.

(10)



Obrázek 5: Nagios. Screenshot http://www.nagios.com/

3.4.2.2 Icinga

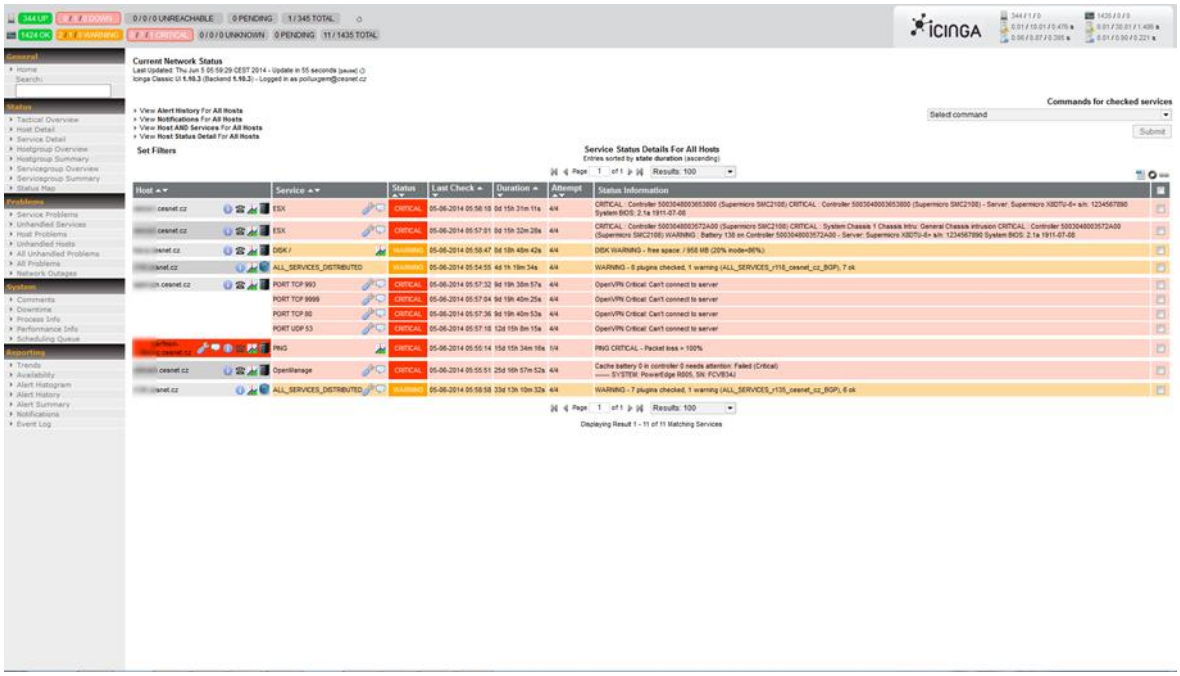
Icinga[10] vychází z Nagiosu a je s ním i s jeho pluginy zpětně kompatibilní, avšak jejich zdrojový kód se liší. Důvod, proč existují tyto dva velmi podobné nástroje, je ten, že se do Nagiosu nepodařilo prosadit některé užitečné funkce, a tak byli vývojáři nuceni udělat jeho nadstavbu.

Největšími odlišnostmi Icingy oproti Nagiosu jsou například distribuované komponenty jako je jádro, web a databáze. Tyto komponenty jsou navzájem propojeny, ale po výpadku kteréhokoli z nich nedojde k výpadku systému jako celku. Dalším rozdílem je, že Icinga disponuje v základu mobilním webovým rozhraním a je lokalizována do mnoha jazyků.

[10] Icinga - https://www.icinga.org/

Icinga obsahuje mnoho dalších více či méně zásadních rozdílů, které z tohoto nástroje dělají velikého konkurenta zaběhlému Nagiosu.

(11) (12)



Obrázek 6: Icinga. Screenshot CESNET

4 Praktická část

Praktická část této práce se podrobněji zabývá zvolenými nástroji, které jsou doporučeny pro síť s těmito parametry:

- Počet uzlů v řádu stovek
- Servery, na kterých běží služby pro zákazníky
- Velký počet aktivních síťových prvků
- Optické, rádiové i metalické vedení sítě

Pro takovouto síť je vhodné použít komerční software, jelikož se v případě problémů s daným nástrojem můžeme spolehnout na podporu. Může se doplnit i nekomerčními a volně šiřitelnými nástroji.

4.1 Monitorování uzlů sítě a tras mezi nimi

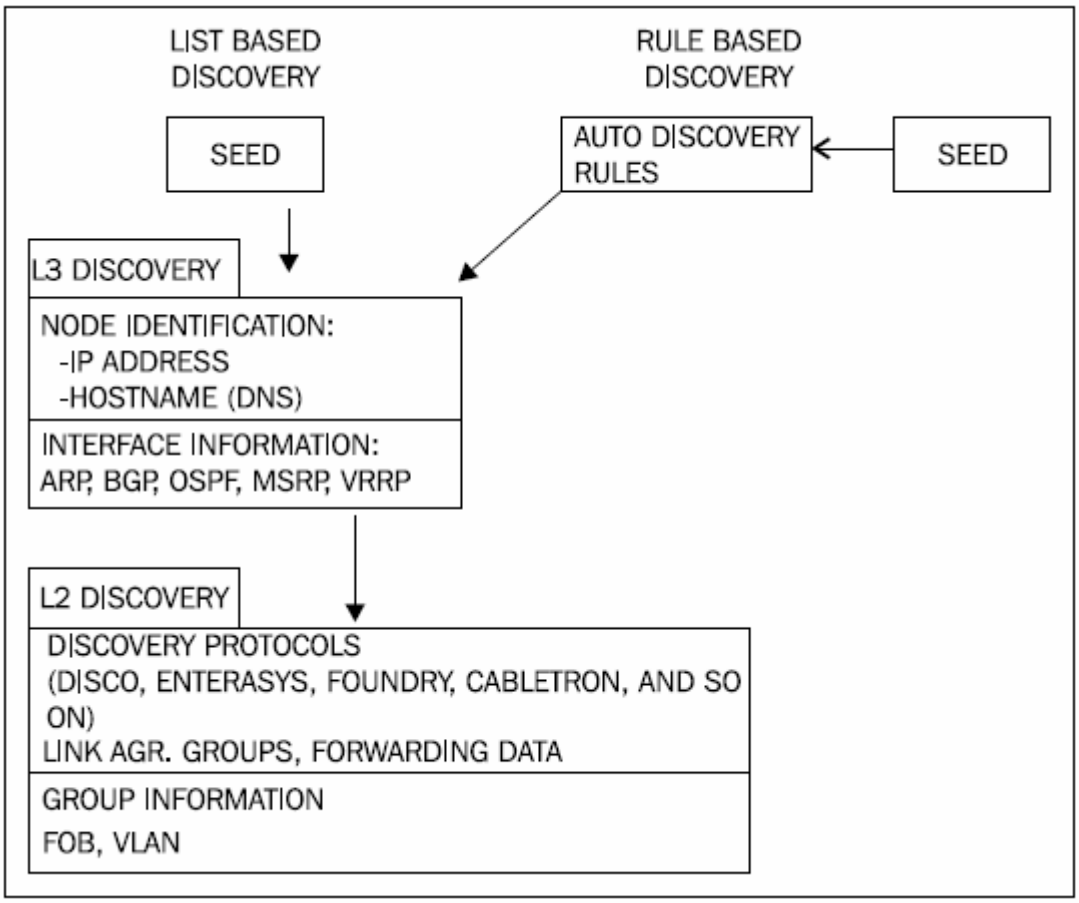
Sledováním uzlů se rozumí sledování stavu aktivních zařízení na uzlech sítě. Může se jednat o sledování stavu celého zařízení, nebo jednotlivých portů či VLAN.

4.1.1 HP Network Node Manager

Tento nástroj se vyznačuje automatickým rozpoznáváním síťových prvků a jejich nastavení. V HP Network Node Manageru jsou dva rozpoznávací módy:

- List based discovery: používá seznam prvků u kterých je zjišťován stav
- Rule based discovery: používá seznam pravidel pro hledání prvků. Například rozsah IP adres, rozsah ID, vyloučený rozsah IP adres atd.

Může být využita i kombinace módů. Nejprve se síť namapuje pomocí List based discovery, a poté se pro přesnost použije Rule based discovery.



Obrázek 7: Schéma rozpoznávacích módů. Zdroj: HP Network Node Manager 9

Když nastane jakákoliv změna v konfiguraci prvku, NNM automaticky zahájí nové rozpoznávání prvku a jeho sousedství.

Administrátor může nastavit časový interval, ve kterém se bude provádět automatické vyhledávání nových prvků. U statických sítí může být interval 48 hodin. U dynamických se doporučuje zvážit kratší interval. V síti s uzly v řádu stovek je vhodné použít hodinový interval. V praxi se tímto zajistí rychlé reakce na změny v síti, na které může operátor ihned reagovat.

Pro změnu intervalu:

- Vybrat Discovery Configuration v Configuration workspace
- Vložit novou hodnotu v políčku Rediscovery interval
- Kliknout na uložit

Výhody a nevýhody obou možností:

- List based discovery
- Striktně definovaný seznam zařízení
- Dobrý pro stabilní sítě
- NNM neobjeví nové zařízení po přidání do sítě
- Dobrá kontrola počtu uzlů vůči licenci

- Rule based discovery
- Nestriktně definovaný seznam uzlů
- Dobrý pro dynamické sítě
- Dobrá kontrola počtu uzlů vůči licenci

(8)

Obecně je vhodnější použít Rule based discovery. Je pak méně práce s udržováním aktuálnosti seznamu prvků.

4.1.1.1 Instalace Network Node Manageru

Instalace se skládá ze dvou hlavních částí:

- Kontrola požadavků
- Instalační proces

Kontrola požadavků

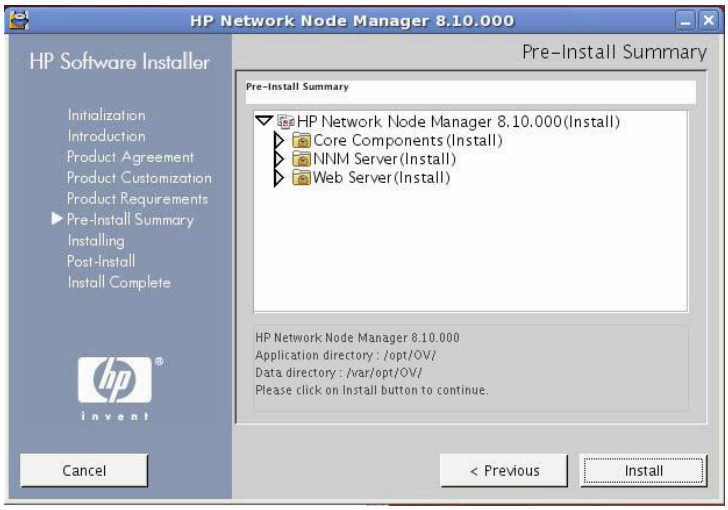
Před tím, než se správce pustí do instalace NNM, je doporučeno zkontrolovat naplnění těchto požadavků:

- Server, na kterém poběží NNM má Plně Specifikované Doménové jméno (anglická zkratka FQDN)
- Server má povoleny tyto porty: TCP: 443, 1098, 1099, 3873, 4444, 4445, 4446, 4447, 8083, 8086, a 8087 a UDP port 696

Instalační proces

Instalační proces probíhá klasicky, tedy tak, jako se instalují obvyklé programy pro operační systém Windows.

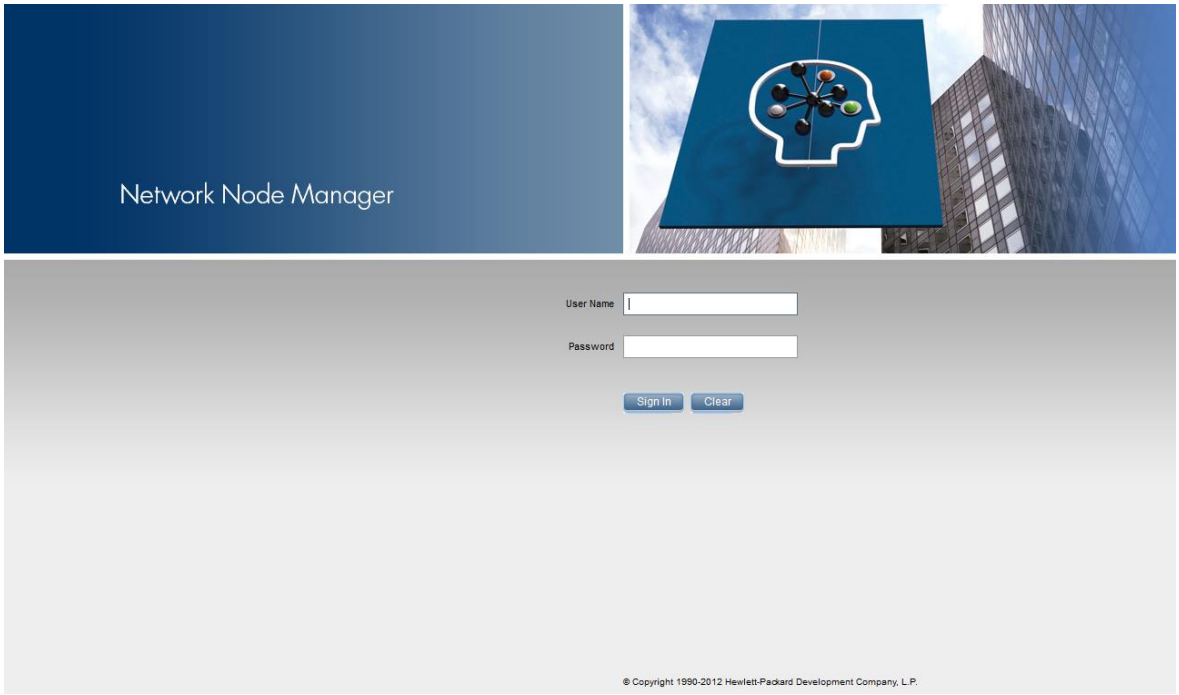
Je doprovázen grafickým prostředím a nevyžaduje téměř žádný zásah.



Obrázek 8: Instalace NNM. Zdroj: HP Network Node Manager 9

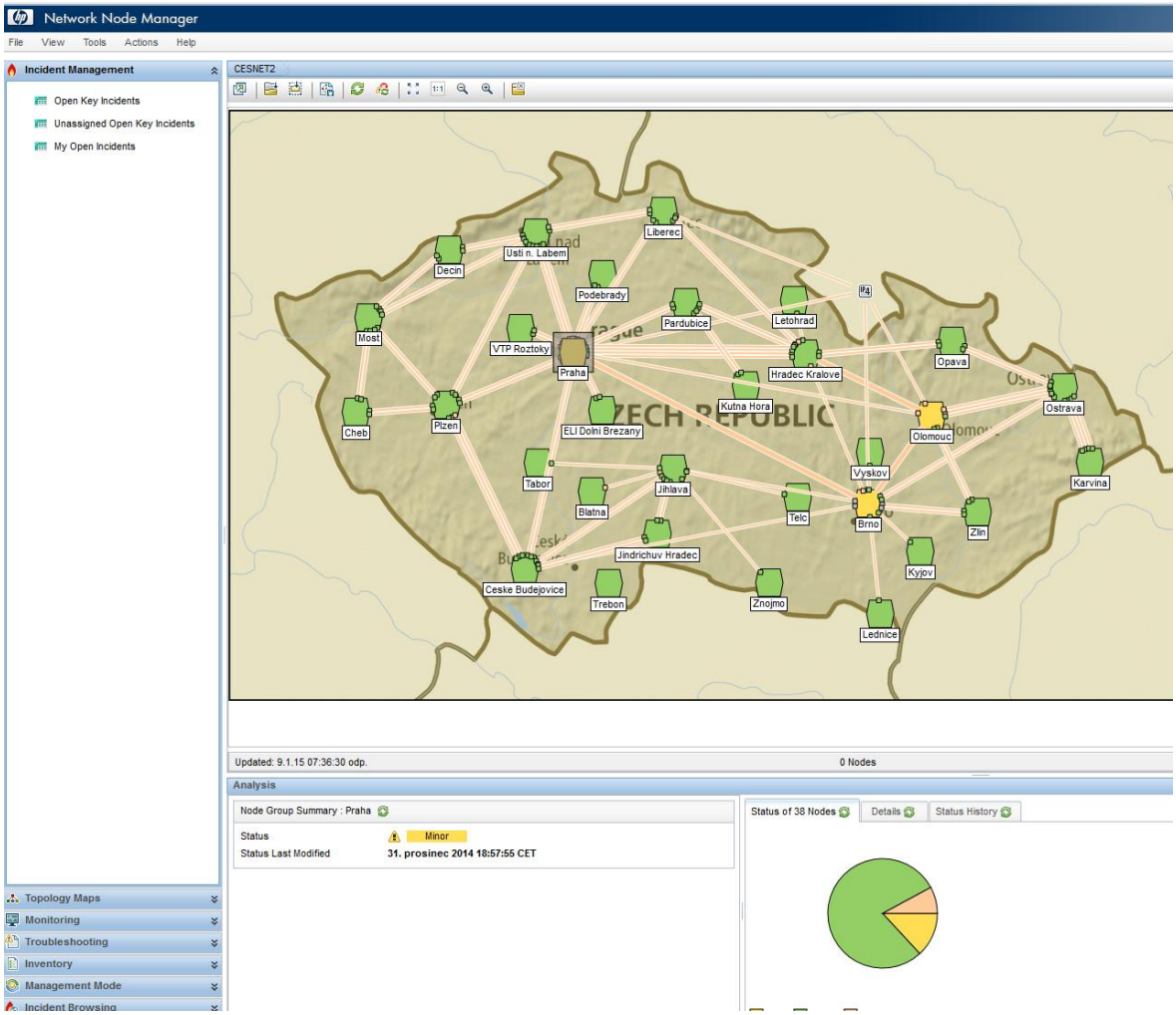
4.1.1.2 Grafické prostředí Network Node Manageru

Po zadání adresy, na které je umístěn NNM je zobrazena přihlašovací obrazovka.



Obrázek 9: Přihlašovací obrazovka NNM. Screenshot CESNET

Po přihlášení je na obrazovce viditelná souhrnná mapa sítě a její uzly. Zde je pak možno přepínat mezi různými pohledy, jako je přehled incidentů nebo různými mapami. Po rozkliknutí uzlů se můžeme dostat hlouběji do zvoleného uzlu a zde již vidíme jednotlivé zařízení sítě. Každá takováto akce se ale zobrazí v nové záložce. V praxi pak může být otevřeno větší množství záložek, které zpomalí běh nástroje. Proto je doporučeno postupně nepotřebné záložky zavírat a v ideálním případě nechat zobrazenou jenom jednu, hlavní záložku s celkovým přehledem.



Obrázek 10: Prostředí NNM s incidenty. Screenshot CESNET

4.1.1.3 Obsluha Network Node Manageru

Pro zobrazení stavu sítě používá NNM tři pohledy:

- Mapy
- Tabulky
- Přehled incidentů

Každý z těchto pohledů je specifický, proto jejich kombinace zajišťuje lepší přehled o stavu sítě a kvalitu informace potřebné pro monitoring.

Pohled	Výhody	Nevýhody
Mapy	Větší přehled nad situací Lehčí zjištění příčiny problému nebo zasažených uzlů	Barva uzlu nám nedokáže říct, co přesně se stalo
Tabulky	Jednoduše tříditelné pomocí vybraného pole Detailnější než pohled pomocí mapy	Barva uzlu nám nedokáže říct, co přesně se stalo
Přehled incidentů	Každý incident je detailně zobrazen Incidenty mohou být tříděny pomocí atributů	Těžké priorizovat zprávy Není možné mít větší přehled nad situací, a proto je těžké určit priority

Tabulka 1: Přehled pohledů v NNM

(8)

Následující tabulka zobrazuje seznam barev stavů užitých v Network Node Manageru

Barva stavu	Popis stavu
	Unknown (neznámý)
	Normal (normální)
	Warning (varování)
	Minor (méně vážný)
	Major (vážný)
	Critical (kritický)
	Disabled (vypnutý)
	No status (bez stavu)

Tabulka 2: Barvy a stavy v NNM

Příklad: když je mapa počátečním zdrojem pro monitoring

Pohled mapy je užíván k počátečnímu pohledu. Když uzel změní barvu, je operátorem otevřen přehled incidentů pro více detailů.

Tento pohled dává komplexní přehled nad stavem sítě a operátor může ihned určit, v jaké oblasti incident nastal. Nedá nám však již detailnější pohled na to co se stalo.

Příklad: když je přehled incidentů výchozím zdrojem pro monitoring

U tohoto případu, když nastane incident, operátor ihned vidí, na jakém zařízení a co vzniklo za problém. Bez pohledu mapy ale nezjistí, jaký má incident dopad na síť.

Tento pohled se dá lehce filtrovat pro větší přehlednost. Jsou k dispozici dva filtry. Časový, kde je na výběr posledních pět minut, poslední hodina, posledních osm hodin, poslední den, poslední tři dny, poslední týden a poslední měsíc. Lze vybrat i možnost zobrazení všeho bez časového filtru.

Druhým filtrem je filtr uzlů. Díky němu se může zobrazit pouze vybraný uzel.

Tyto filtry se dají kombinovat, takže například můžeme zobrazit všechny trvající incidenty v uzlu v Praze za poslední měsíc. Incidenty, které trvají více, jak měsíc se v tomto pohledu nezobrazí.

V případě mapy, můžeme rozkliknout daný postižený uzel pro více informací. Tím se dostaneme k přehledu portů, IP adres, rozhraní, instalovaných karet a jiných podrobností o daném uzlu. Z těchto informací může operátor určit, na jakém místě problém vznikl, ale ne již jeho příčinu.

Z přehledu incidentů se také můžeme dostat do přehledu postiženého uzlu a zobrazit stejné informace jako při výchozím pohledu mapy.

Nejlepší způsob monitorování je kombinací mapy a přehledu incidentů. V praxi je tak vidět nejenom hrubý stav sítě, ale i podrobnější informace o případných incidentech.

4.1.2 Icinga

Icinga se v mnohém liší od HP Network Node Manageru. Zatímco NNM se primárně zabývá sledováním stavu jednotlivých rozhraní, ip adres atd. daného zařízení, které tvoří síť, Icinga sleduje primárně stav služeb a serverů připojených k té samé síti. Samozřejmě může také sledovat i síťové prvky a jejich rozhraní.

4.1.2.1 Konfigurace Icingy

Zde je uveden příklad instalace a konfigurace Icingy na systému Ubuntu

Instalace:

Nejprve přidáme PPA Icingy do balíčkového manageru

sudo add-apt-repository ppa:formorer/icinga

Poté je potřeba aktualizovat apt balíčkovou databázi

sudo apt update

A nakonec nainstalujeme Icingu a MySQL

sudo apt install icinga icinga-doc icinga-idoutils mysql-server libdbd-mysql mysql-client

Zde je seznam následujících výzev a doporučení jak na ně odpovědět:

Konfigurace MySQL: Vložit nové MySQL uživatelské heslo root.

PostFix konfigurace: Vybrat "Internet Site"

Konifugrace icinga-cgi: Vložit "icingaadmin" uživatelské heslo (přihlášení k přístupu do Icingy).

Konfigurace icinga-common: Vložit "No" pro zpřístupnění externích příkazů

Konfigurace icinga-idoutils: Vložit "Yes" pro konfiguraci databáze pro icinga-idoutils s dbconfig-common

Konfigurace icinga-idoutils: vybrat "mysql" jako databázový typ.

Konfigurace icinga-idoutils: Vložit MySQL root heslo

Konfigurace icinga-idoutils: Vložit nové icinga-idoutils databázové heslo

Toto je tedy postup instalace Icingy. Poté je ještě potřeba nastartovat Apache HTTP server, na kterém poběží webové rozhraní Icingy.

Poté je už jen nutné nastartovat Icingu a Apache:

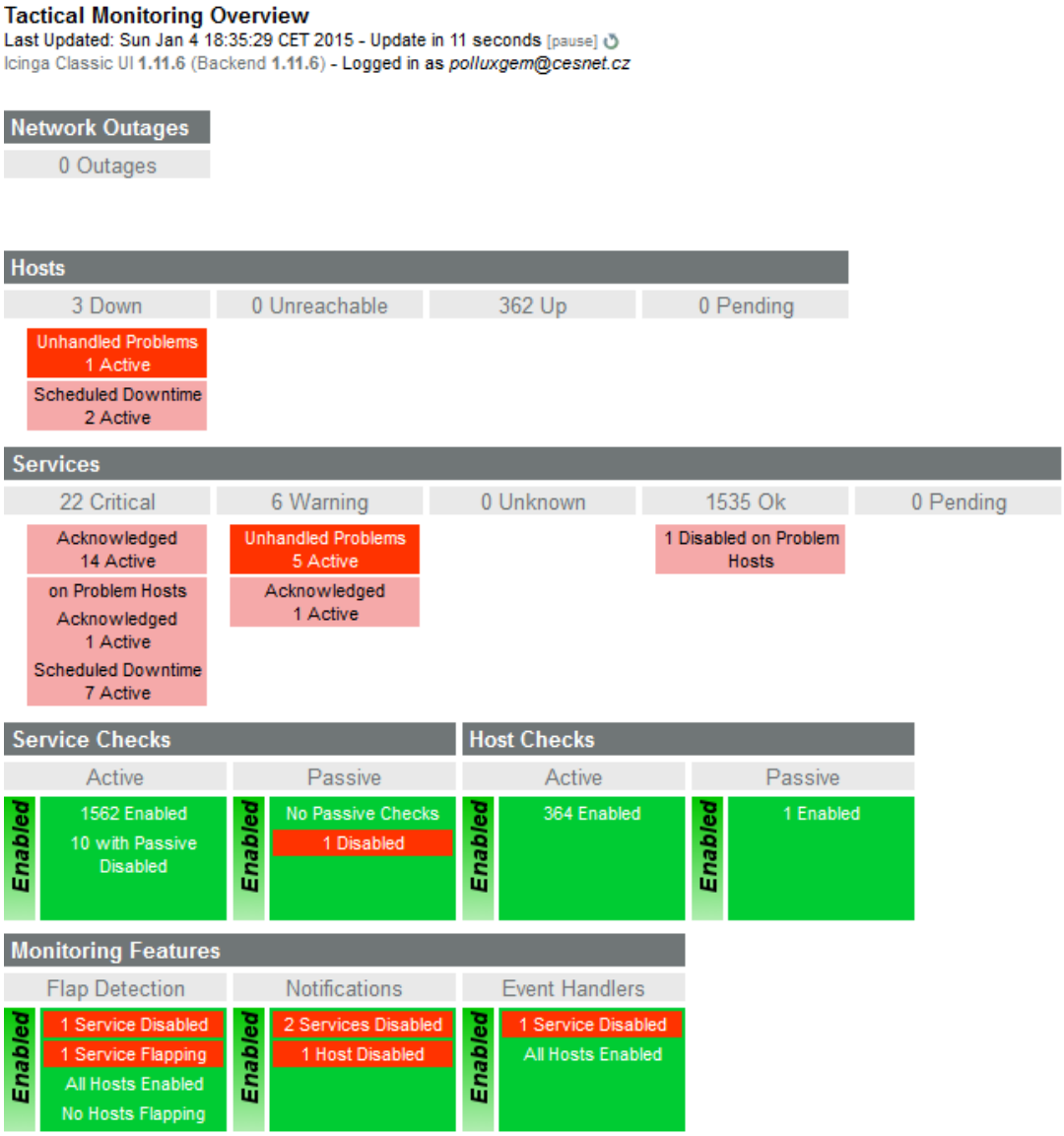
$ /etc/init.d/icinga start

$ /etc/init.d/apache2 start

(13)

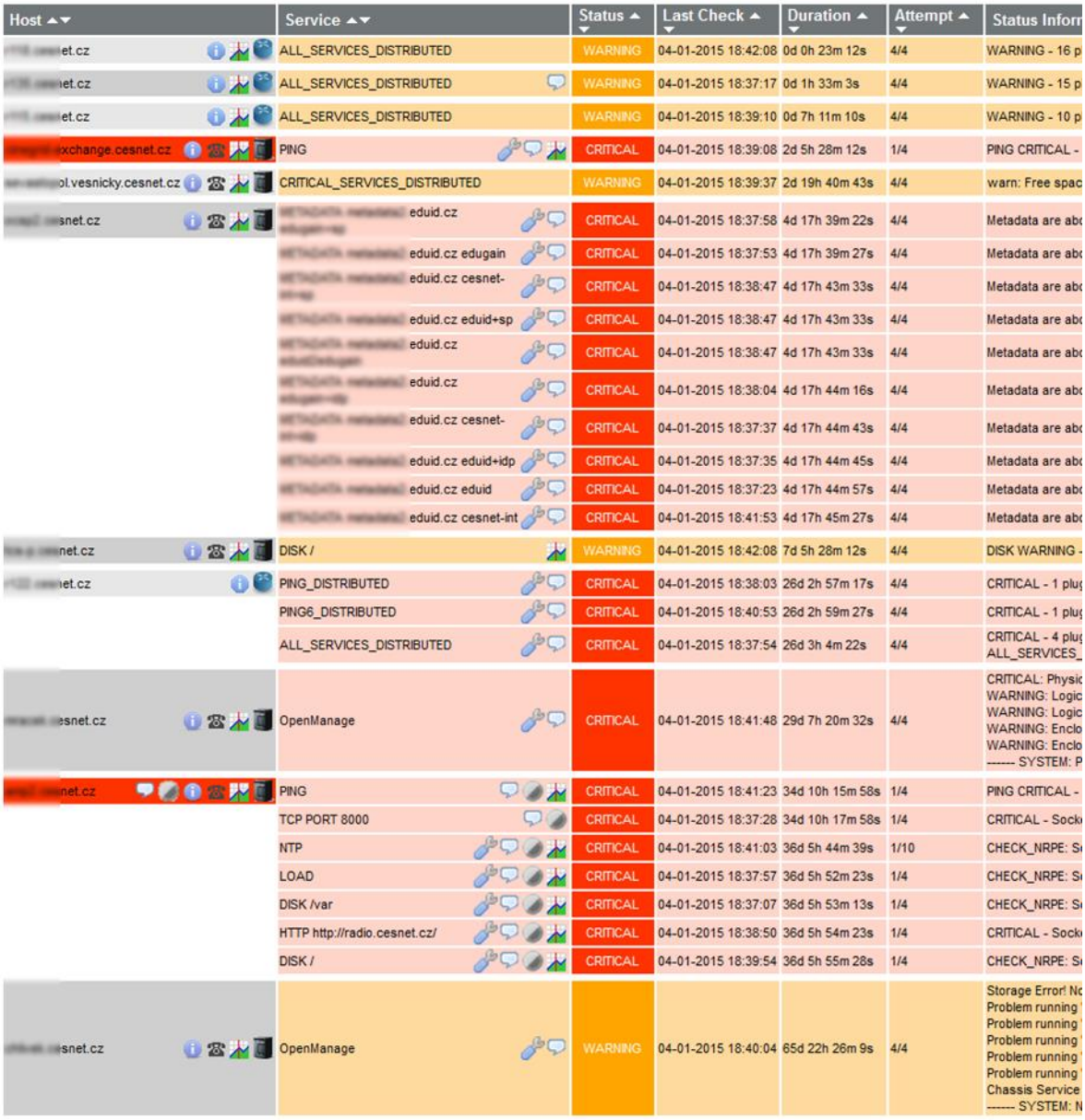
4.1.2.2 Grafické prostředí Icingy

Na úvodní obrazovce, která se zobrazí po spuštění webového rozhraní, je takzvané „Tactical Monitoring Overview“. Zde je zobrazen základní stav serverů, služeb a stav jejich testování. Tento pohled je v podstatě zbytečný. Mnohem lepší je zobrazení „Service problems“, kterému je věnován prostor dále.



Obrázek 11: Tactical monitoring overview. Screenshot CESNET

Pro rychlé zobrazení detailnějších informací ohledně incidentů slouží položka „Service Problems“. V tomto přehledu jsou zobrazeny všechny nastalé incidenty včetně těch, kterých si již správce nebo operátor všiml a u nichž vyplnil možnost tzv. Acknowledge.



Host	Service	Status	Last Check	Duration	Attempt	Status Inform
[redacted]et.cz	ALL_SERVICES_DISTRIBUTED	WARNING	04-01-2015 18:42:08	0d 0h 23m 12s	4/4	WARNING - 16 p
[redacted]net.cz	ALL_SERVICES_DISTRIBUTED	WARNING	04-01-2015 18:37:17	0d 1h 33m 3s	4/4	WARNING - 15 p
[redacted]et.cz	ALL_SERVICES_DISTRIBUTED	WARNING	04-01-2015 18:39:10	0d 7h 11m 10s	4/4	WARNING - 10 p
[redacted]xchange.cesnet.cz	PING	CRITICAL	04-01-2015 18:39:08	2d 5h 28m 12s	1/4	PING CRITICAL -
[redacted]ol.vesnicky.cesnet.cz	CRITICAL_SERVICES_DISTRIBUTED	WARNING	04-01-2015 18:39:37	2d 19h 40m 43s	4/4	warn: Free spac
[redacted]snet.cz	[redacted] eduid.cz	CRITICAL	04-01-2015 18:37:58	4d 17h 39m 22s	4/4	Metadata are abo
	[redacted] eduid.cz edugain	CRITICAL	04-01-2015 18:37:53	4d 17h 39m 27s	4/4	Metadata are abo
	[redacted] eduid.cz cesnet-	CRITICAL	04-01-2015 18:38:47	4d 17h 43m 33s	4/4	Metadata are abo
	[redacted] eduid.cz eduid+sp	CRITICAL	04-01-2015 18:38:47	4d 17h 43m 33s	4/4	Metadata are abo
	[redacted] eduid.cz	CRITICAL	04-01-2015 18:38:47	4d 17h 43m 33s	4/4	Metadata are abo
	[redacted] eduid.cz	CRITICAL	04-01-2015 18:38:04	4d 17h 44m 16s	4/4	Metadata are abo
	[redacted] eduid.cz cesnet-	CRITICAL	04-01-2015 18:37:37	4d 17h 44m 43s	4/4	Metadata are abo
	[redacted] eduid.cz eduid+idp	CRITICAL	04-01-2015 18:37:35	4d 17h 44m 45s	4/4	Metadata are abo
	[redacted] eduid.cz eduid	CRITICAL	04-01-2015 18:37:23	4d 17h 44m 57s	4/4	Metadata are abo
	[redacted] eduid.cz cesnet-int	CRITICAL	04-01-2015 18:41:53	4d 17h 45m 27s	4/4	Metadata are abo
[redacted]net.cz	DISK /	WARNING	04-01-2015 18:42:08	7d 5h 28m 12s	4/4	DISK WARNING -
[redacted]et.cz	PING_DISTRIBUTED	CRITICAL	04-01-2015 18:38:03	26d 2h 57m 17s	4/4	CRITICAL - 1 plug
	PING6_DISTRIBUTED	CRITICAL	04-01-2015 18:40:53	26d 2h 59m 27s	4/4	CRITICAL - 1 plug
	ALL_SERVICES_DISTRIBUTED	CRITICAL	04-01-2015 18:37:54	26d 3h 4m 22s	4/4	CRITICAL - 4 plug ALL_SERVICES_
[redacted]esnet.cz	OpenManage	CRITICAL	04-01-2015 18:41:48	29d 7h 20m 32s	4/4	CRITICAL: Physic WARNING: Logic WARNING: Logic WARNING: Enclo WARNING: Enclo ------ SYSTEM: P
[redacted]net.cz	PING	CRITICAL	04-01-2015 18:41:23	34d 10h 15m 58s	1/4	PING CRITICAL -
	TCP PORT 8000	CRITICAL	04-01-2015 18:37:28	34d 10h 17m 58s	1/4	CRITICAL - Sock
	NTP	CRITICAL	04-01-2015 18:41:03	36d 5h 44m 39s	1/10	CHECK_NRPE: S
	LOAD	CRITICAL	04-01-2015 18:37:57	36d 5h 52m 23s	1/4	CHECK_NRPE: S
	DISK /var	CRITICAL	04-01-2015 18:37:07	36d 5h 53m 13s	1/4	CHECK_NRPE: S
	HTTP http://radio.cesnet.cz/	CRITICAL	04-01-2015 18:38:50	36d 5h 54m 23s	1/4	CRITICAL - Sock
	DISK /	CRITICAL	04-01-2015 18:39:54	36d 5h 55m 28s	1/4	CHECK_NRPE: S
[redacted]snet.cz	OpenManage	WARNING	04-01-2015 18:40:04	65d 22h 26m 9s	4/4	Storage Error! No Problem running Problem running Problem running Problem running Problem running Chassis Service ------ SYSTEM: N

Obrázek 12:Prostředí Icingy s incidenty. Screenshot CESNET

Vážné incidenty se označují červenou barvou a mají status CRITICAL. U těchto incidentů je většinou potřeba reagovat neprodleně. Tento stav může způsobit řada událostí.

Například se může jednat o:

- výpadek serveru či služby
- výpadek portu na síťovém prvku
- překročení povolené teploty na zařízení
- překročení povolené hranice zatížení procesoru síťových prvků
- a další

Méně závažné incidenty se označují oranžovou barvou a mají status WARNING. U těchto incidentů je potřeba dbát zvýšené pozornosti a popřípadě je řešit. Mají nižší prioritu než ty, které mají status CRITICAL. Lehce ale mohou přejít na status CRITICAL. Proto se nedoporučuje je ignorovat.

Například se může jednat o:

- blížící se překročení povolené teploty na zařízení
- docházení místa na disku
- o něco větší než obvyklé zatížení procesoru
- a další

4.1.3 Cisco Transport Controller

Cisco Transport Controller je primárně určen ke konfiguraci a sledování stavu optických sítí. Je to mocný nástroj, ve kterém se dá konfigurovat téměř každý aspekt optického spoje, jako je například vlnová délka atd.

Okno CTC se objeví po tom, co se uživatel přihlásí do ONS 15454[11]. Okno obsahuje položky v menu, panel nástrojů a rozdělení na vrchní a spodní část. Vrchní část poskytuje informace o stavu vybraného objektu a zobrazení aktuálního pohledu. Spodní část poskytuje záložky a subzáložky pro konfiguraci a pohled na ONS 15454.

[11] ONS 15454 je multiservisní platforma, která poskytuje funkci více síťových prvků v jedné platformě.

Přehled barev CTC karet

Grafická část CTC v reálném čase zobrazuje stav fyzické karty nebo slotu za pomocí těchto barev:

Barva karty	Stav
Šedá	Slot není propagován; není nainstalovaná žádná karta
Fialová	Slot je propagován; není nainstalovaná žádná karta
Bílá	Slot je propagován; je nainstalovaná funkční karta
Žlutá	Slot je propagován; je detekován menší problém
Oranžová	Slot je propagován; je detekován vážný problém
Červená	Slot je propagován; je detekován kritický problém

Tabulka 3: Stav karty nebo slotu podle barvy

Síťový pohled

Síťový pohled poskytuje přehled o dané síti v geografickém přehledu. Grafická část zobrazuje obrázek na pozadí, což může být například mapa republiky a na ní proložené ONS ikony. Administrátor tento pohled nastaví, pokud chce, aby každý uživatel viděl stejný síťový pohled.

Linky zobrazující DCC spoje mezi uzly může nabývat zelené barvy pro aktivní, nebo šedé barvy pro chybu. Linky také mohou být plné (okruh tudy může být routován), nebo přerušované (okruh nemůže být routován skrze tuto linku).

(14)

Barva	Alarmy
Zelená	Žádné alarmy
Žlutá	Nezávažné alarmy
Oranžová	Vážnější alarmy
Červená	Kritické alarmy
Šedá s „Uknown#“	Uzly se poprvé inicializují. CTC zobrazuje Unknown#, protože ještě nezjistil jméno uzlu.

Tabulka 4: Barvy linek označující stav spojů

Síťový pohled – záložky a subzáložky

Záložka	Popis	Subzáložky
Alarms	Seznam aktuálních alarmů v síti	---
Conditions	Seznam současných stavů v síti	---
History	Poskytuje historii síťových alarmů obsahující datum, typ a závažnost	---
Circuits	Vytváří, maže, edituje, filtruje a vyhledává síťové okruhy	---
Provisioning	Poskytuje seznam uživatelů, profily alarmů, BLSR, přehled okruhů	Security, Alarm Profiles, BLSR, Overhead Circuits
Maintanance	Zobrazuje typ zařízení a stav každého uzlu v síti; Zajišťuje možnost stažení nové verze softwaru	Software

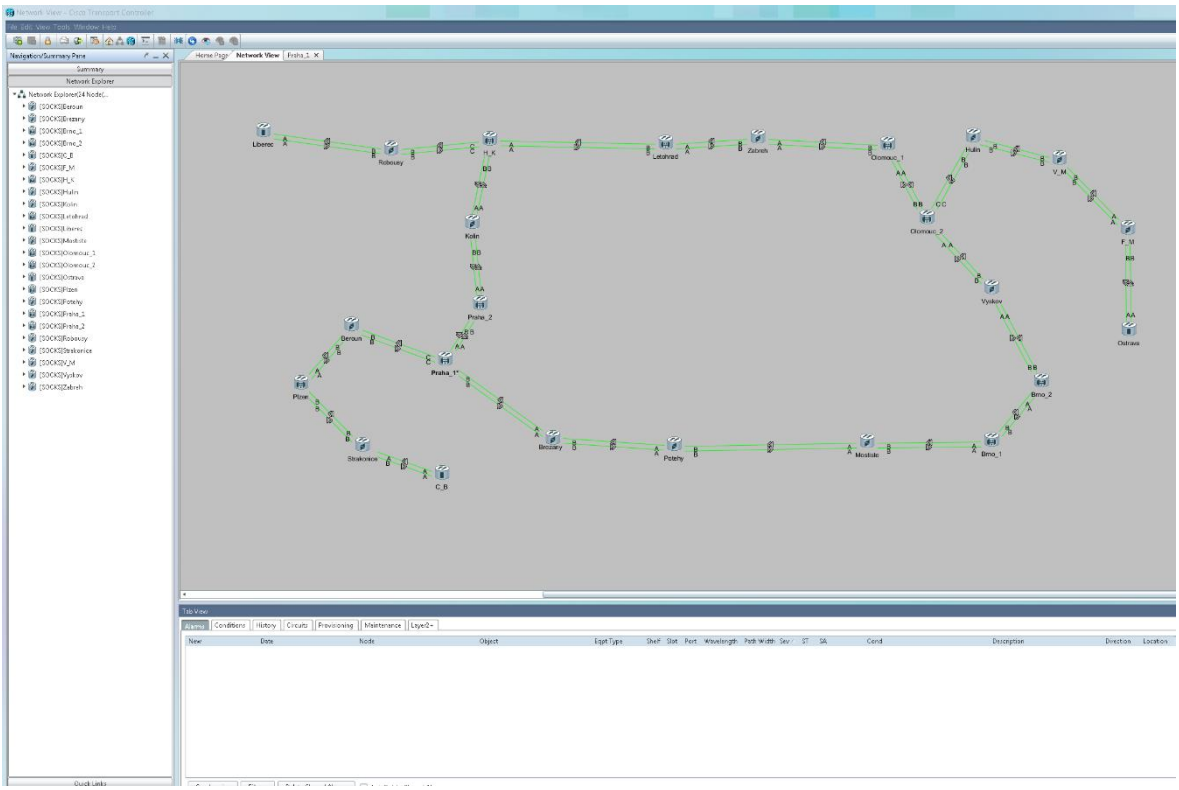
Tabulka 5: Přehled záložek s subzáložek v CTC

(14)

Pohled karet (Card view)

Pohled karet poskytuje informace o individuálních ONS kartách. Tento pohled zobrazuje porty na kartách a jejich stavy. V přehledu stavů je zobrazen název uzlu, slot, počet alarmů, typ karty, typ zařízení a stav karty.

Nástroj CTC obsahuje mnohem více možností a konfigurací, ale to se již dostáváme mimo oblast monitoringu.



Obrázek 13: Prostředí CTC. Screenshot CESNET

5 Zhodnocení výsledků

Pro potřeby CESNETu je použito řešení s kombinací nástrojů Cisco Transport Controller, HP Network Node Manager a Icinga.

Pro rozvržení nástrojů na obrazovkách je vhodné použít následující řešení:

HP Network Node Manager: Pohled mapy 80% jedné obrazovky. Napravo od něj přehled incidentů, pro snadnější orientaci v nových incidentech. Tento pohled bude nastaven na zobrazení critical incidentů bez časového omezení a řazen od nejnovějších, které budou nahoře, po nejstarší. Toto rozložení zajistí jednoduchý a přehledný pohled na stav uzlů. V mapě vidíme, v jaké oblasti se incident stal. To nám pomůže v posouzení, jaký má daný výpadek rozsah.

K detailnějšímu přehledu o stavu sítě pak bude sloužit seznam incidentů. To nám pomůže rozlišit stav, kdy se stanou dva a více incidentů v jednom a tom samém uzlu. Takovou situaci v mapě nerozlišíme. Museli bychom stále otevírat uzly a kontrolovat, zda nepřibyl nějaký jiný incident.

Icinga: Pohled nastavený na Service problems. Tento pohled je zvolen proto, jelikož kdybychom zvolili pouze Unhandeled services, nebyli bychom si vědomi, kdy daná služba či síťový prvek obnovily správnou činnost. Tento pohled je vhodné nastavit na řazení od nejnovějších incidentů nahoře po nejstarší dole. Pokud ale v Service problems bude příliš mnoho incidentů a stane se tak nepřehledným, je vhodné přepnout na zobrazení Unhandeled problems. V tomto zobrazení ale není doporučeno zůstávat delší dobu. Operátor by pak po chvíli přišel o přehled nad stavem prvků a služeb.

Cisco Transport Controller: U tohoto nástroje je doporučeno mít v horní polovině obrazovky kartu Network view, kde bude mapa sítě s jejími uzly. V dolní polovině je pak vhodné použít kartu Alarms, kde budou chronologicky vypsány jednotlivé problémy s optickými propoji.

Tímto zobrazením se docílí toho, že operátor nejdříve uvidí dlouhý červený nebo žlutý řádek s alarmem a v návaznosti na to i změnu barvy uzlu na mapě. Při prvním pohledu je pak již jasné, v jaké oblasti se stala chyba a napoví, co může být její příčinou.

Kombinace těchto nástrojů pokrývá všechny možné scénáře, které se mohou v síti vyskytnout.

V následujících tabulkách je několik scénářů, které se mohou v oblasti sítí vyskytnout a reakce jednotlivých nástrojů.

Scénář pád portu na síťovém prvku

Nástroj	Reakce
Cisco Transport Controller	Bez reakce
Network Node Manager	Změna stavu portu na Down a červené barevné označení portu, případně uzlu
Icinga	V seznamu incidentů se objeví nová Critical položka označená tak, jako je aktivní síťový prvek. V informacích o stavu se dá najít, který port spadl a jeho popis.

Tabulka 6: Scénář pád portu

U tohoto problému je nutné nejprve vyhodnotit jeho závažnost. Pád neoznačeného portu, který nemá větší význam pro síť, není nutné řešit bezprostředně. Většinou se jedná o odpojený port síťovým technikem, který ale nebyl administrativně vypnutý.

Pád serveru

Nástroj	Reakce
Cisco Transport Controller	Bez reakce
Network Node Manager	Zčervenání uzlu a označení jako down. V případě pohledu incidentů nová položka s označením zařízení a se stavem Critical.
Icinga	Stav Critical služby PING a označení nedostupnosti ve sloupci host červenou barvou.

Tabulka 7: Scénář pád serveru

Tento problém je většinou nutné řešit bezodkladně. Může postihovat důležité prvky sítě a proto je mu nutné věnovat zvýšenou pozornost.

Pád služby na serveru

Nástroj	Reakce
Cisco Transport Controller	Bez reakce
Network Node Manager	Bez reakce
Icinga	V seznamu incidentů se zobrazí nová Critical položka označená tak jako server. V informacích o službě se dá najít, jaká služba spadla.

Tabulka 8: Scénář pád služby

U tohoto případu je nutné postupovat podle informací, které dodal administrátor serveru. Některé výpadky služeb jsou pravidelné, například v rámci údržby.

Varování na problém se službou na serveru

Nástroj	Reakce
Cisco Transport Controller	Bez reakce
Network Node Manager	Bez reakce
Icinga	V seznamu incidentů se zobrazí nová Warning položka označená tak jako server. V informacích o službě se dá najít, o jakou službu se jedná.

Tabulka 9: Scénář problém se službou

Zde se postupuje podle informací dodaných administrátorem serveru.

Přerušení trasy mezi uzly

Nástroj	Reakce
Cisco Transport Controller	Zčervenání propoje mezi uzly, případně zčervenání uzlu. Nová hláška v logu alarmů
Network Node Manager	Zčervenání uzlu a označení portu jako down. V případě pohledu incidentů nová položka s označením portu, kterým je trasa připojena.
Icinga	V závislosti na konfiguraci. Nová Critical položka u které je ve sloupci Status information popsán spadlý port na zařízení.

Tabulka 10: Scénář přerušení trasy

V případě této situace je nutné okamžitě reagovat. Jedná se o problém s velkou prioritou.

Pád aktivního zařízení v síti (předpokládáme router nebo switch)

Nástroj	Reakce
Cisco Transport Controller	Záleží na důležitosti zařízení. Pokud pád ovlivní napojení optických propojů, projeví se zčervenáním propoje mezi uzly, případně zčervenání uzlu. Nová hláška v logu alarmů
Network Node Manager	Zčervenání uzlu a označení stavu jako Critical
Icinga	Stav Critical služby PING a označení nedostupnosti ve sloupci host červenou barvou.

Tabulka 11: Pád aktivního zařízení

Ve většině případů se jedná závažný incident, existují však případy, kdy Network Node Manager špatně načte aktivní prvek, který byl již dříve odstraněn z nějaké starší konfigurace, a chybně tak hlásí jeho přítomnost a nedostupnost.

Z těchto příkladů je patrné, že jedině kombinace všech tří nástrojů dává kompletní pohled o stavu sítě. Pokud bychom používali jen dva nebo dokonce jeden z nich, mohlo by se stát, že síťovému operátorovi některá událost unikne.

6 Závěr

Tato práce se zabývala přehledem a představením práce s různými nástroji pro monitoring sítě. Ukázala důležitost těchto nástrojů u každého většího poskytovatele síťových služeb. Jako příklad byla vybrána firma CESNET, z. s. p. o., ve které jsou tyto nástroje používané v běžné praxi. Autor v této firmě čerpal zkušenosti s prací s nástroji pro sledování sítě a zhodnotil jejich význam v konkrétních situacích. Doporučil také, jak tyto nástroje používat v praxi. Vyzdvihl ideální způsob použití pro co nejefektivnější sledování konkrétního stavu sítě. V práci je dále uvedeno praktické rozložení uživatelského rozhraní nástrojů. Pro každý nástroj totiž existuje více možností, jak informace o síti zobrazit. Některé zbytečně zahlcují operátora, nebo mu naopak nedávají pravdivý přehled o síti.

Všemi těmito postřehy autor ukázal na důležitost stálé služby, který tyto nástroje kontroluje a ovládá. U menších sítí postačují automatické zprávy, které nástroje generují. U větších sítí je již však doporučeno zřídit stálou službu, která bude vykonávat nepřetržitý dohled nad těmito nástroji. Může tak zareagovat okamžitě po nastalé události, která může vést k omezení provozu sítě nebo k výpadkům serveru.

7 Bibliografie

1. Začínáme s monitoringem sítě. *Samuraj-cz.com.* [Online] http://www.samuraj-cz.com/clanek/zaciname-s-monitoringem-site/.

2. Příhoda, Petr. [Online] http://phoenix.inf.upol.cz/esf/ucebni/poc_site.pdf.

3. *Network monitor software and windows development tools.* [Online] http://www.monitortools.com/.

4. Cloud monitoring. [Online] http://forpsicloud.cz/cloud-monitoring/vlastnosti.

5. Network diagnostic utilities. *ManageEngine.* [Online] http://www.manageengine.com/products/oputils/help/diagnostics/diagnostics_tools.html.

6. Bruey, Douglas. SNMP: Simple? Network Management Protocol. [Online] http://www.rane.com/note161.html.

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

8. VILEMAITIS, Marius. *HP Network Node Manager 9: getting started.* Birmingham, U.K. : Packt Enterprise, 2011. 9781849680851.

9. Alwayn, Vivek. *Optical Network Design and Implementation.* místo neznámé : Cisco Press, 2009. 1587141507.

10. Jamrich, Marián. Nagios: monitorovanie počítačovej siete. *Root.* [Online] 15. 12 2010. http://www.root.cz/clanky/nagios-monitorovanie-pocitacovej-siete/.

11. Štrauch, Adam. Icinga: monitorování sítí a serverů. *Root.cz.* [Online] 13. 05 2011. [Citace: 06. 06 2014.] http://www.root.cz/clanky/icinga-monitorovani-siti-a-serveru/.

12. What does Icinga have that Nagios doesn't? *Icinga.org.* [Online] [Citace: 06. 06 2014.] https://www.icinga.org/about/nagios/feature-comparison/.

13. Mehta, Viranch. *Icinga network monitoring monitor complex and large environments across dispersed locations with Icinga.* Birmingham, UK : Packt Pub, 2013.

14. Cisco Systems, Inc. *Cisco ONS 15454 Reference Manual* . San Jose : Cisco Systems, Inc., 2008.

8 Seznam použitých obrázků a tabulek

Obrázek 1: Schéma monitorování sítě. Zdroj http://www.samuraj-cz.com/ 18

Obrázek 2:Networkd Node Manager. Screenshot CESNET 21

Obrázek 3: HP OpenView. Screenshot CESNET 21

Obrázek 4:Cisco Transport Controller. Screenshot CESNET 23

Obrázek 5: Nagios. Screenshot http://www.nagios.com/ 25

Obrázek 6: Icinga. Screenshot CESNET 26

Obrázek 7: Schéma rozpoznávacích módů. Zdroj: HP Network Node Manager 9 28

Obrázek 8: Instalace NNM. Zdroj: HP Network Node Manager 9 30

Obrázek 9: Přihlašovací obrazovka NNM. Screenshot CESNET 31

Obrázek 10: Prostředí NNM s incidenty. Screenshot CESNET 32

Obrázek 11: Tactical monitoring overview. Screenshot CESNET 37

Obrázek 12:Prostředí Icingy s incidenty. Screenshot CESNET 38

Obrázek 13: Prostředí CTC. Screenshot CESNET 42

Tabulka 1: Přehled pohledů v NNM 33

Tabulka 2: Barvy a stavy v NNM 34

Tabulka 3: Stav karty nebo slotu podle barvy 40

Tabulka 4: Barvy linek označující stav spojů 41

Tabulka 5: Přehled záložek s subzáložek v CTC 41

Tabulka 6: Scénář pád portu 44

Tabulka 7: Scénář pád serveru 45

Tabulka 8: Scénář pád služby 45

Tabulka 9: Scénář problém se službou 46

Tabulka 10: Scénář přerušení trasy 46

Tabulka 11: Pád aktivního zařízení 47

9 Seznam použitých zkratek

RSS *Rich site summary* (formát xml pro lepší přehled o novinkách v html)

IIS *Internet Information Services* (softwarový webový server)

FTP *File Transfer Protocol* (protokol pro přenos souborů)

SQL *Structured Query Language* (strukturovaný dotazovací jazyk)

IP *Internet Protocol* (základní protokol pracující na síťové vrstvě)

SNMP *Simple Network Management Protocol* (protokol sloužící potřebám správy sítě)

DNS *Domain name system* (systém doménových jmen)

XML *Extensible Markup Language* (rozšiřitelný značkovací jazyk)

HTML *HyperText Markup Language* (značkovací jazyk pro tvorbu webových stránek)

CPU *Central Processing Unit* (centrální procesorová jednotka)

WMI *Windows Management Instrumentatation* (rozhraní přes které procházejí notifikace a upozornění)

IPMI *Intelligent Platform Management Interface* (subsystém, který poskytuje možnosti pro monitoring)

IDS *Instrusion Detection System* (systém pro odhalení průniku)

IPS *Intrusion Prevention System* (systém prevence průniku)

NNM *Network Node Manager* (nástroj pro sledování sítě)

VLAN *Virtual Local Area Network* (virtuální síť)

MSSP *Managed Security Service Provider* (síťové bezpečnostní služby o které se stará poskytovatel)

CTC *Cisco Transport Controller* (nástroj pro sledování sítě)

ID *Identity* (Identita)

GUI *Graphical User Interface* (grafické uživatelské prostředí)