Monitorování aktivních prvků počítačové sítě

Monitoring of computer network components

Bc. Zdeněk Habrman

Diplomová práce
2013

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2012/2013

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Zdeněk Habrman**
Osobní číslo:	**A11481**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Informační technologie**
Forma studia:	**kombinovaná**
Téma práce:	**Monitorování aktivních prvků počítačové sítě**

Zásady pro vypracování:

1. **Seznamte se s principy a možnostmi dohledových systémů.**
2. **Analyzujte dostupná řešení na trhu.**
3. **Zaměřte se na systémy, které pracují pomocí standardních protokolů (např. SNMP, ICMP).**
4. **Implementujte vybrané řešení na počítačovou síť.**
5. **Vyhodnoťte výsledky monitorování.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **HUCABY, Dave, Steve MCQUERRY a Andrew WHITAKER. Cisco router configuration handbook. 2nd ed. Indianapolis, IN: Cisco Press, 2010, xxii, 641 s. ISBN 978-1-58714-116-4.**
2. **MCQUERRY, Steve, David JANSEN a Dave HUCABY. Cisco LAN switching configuration handbook. 2nd ed. Indianapolis, Ind.: Cisco Press, 2009, xx, 333 s. ISBN 978-1-58705-610-9.**
3. **SOSINSKY, Barrie. Mistrovství - počítačové sítě: [vše, co potřebujete vědět o správě sítí]. Vyd. 1. Brno: Computer Press, 2010, 840 s. ISBN 978-80-251-3363-7.**
4. **COLE, Eric, Ronald L KRUTZ a James W CONLEY. Network security bible. 2nd ed. Indianapolis: Wiley Publishing, 2009, xliv, 891 s. ISBN 978-0-470-50249-5.**
5. **DONDICH, Taylor. Network Monitoring with Nagios [online]. 1st ed. Sevastopol: O'Reilly, 2006.**

Vedoucí diplomové práce: **Ing. Jiří Korbel, Ph.D.**
Ústav počítačových a komunikačních systémů

Datum zadání diplomové práce: **22. února 2013**

Termín odevzdání diplomové práce: **22. května 2013**

Ve Zlíně dne 22. února 2013

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. Mgr. Roman Jašek, Ph.D.
ředitel ústavu

ABSTRAKT

Tato práce se zabývá možnostmi a principy dohledových systémů. Analyzuje systémy používané v dnešní době a to hlavně systémy používající standardní protokoly SNMP a ICMP. Implementuje vybraný systém na univerzitní počítačovou síť a prezentuje výsledky monitorování této sítě.

Klíčová slova: monitoring, open source, počítačová síť, SNMP, ICMP, Cacti, Nagios, Zabbix, graf, PHP, SQL, apache server, přepínač, Cisco

ABSTRACT

This thesis is aimed to possibilities and principles of monitoring systems. Analyzes systems used nowadays. Especially systems use standard protocols SNMP and ICMP. Implements selected system on the university computer network and presents the monitoring results of this network.

Keywords: monitoring, open source, computer network, SNMP, ICMP, Cacti, Nagios, Zabbix, graph, PHP, SQL, apache server, switch, Cisco

Chtěl bych poděkovat vedoucímu práce panu Ing. Jiřímu Korbelovi, Ph.D. A to nejenom za cenné rady a příkladný přístup, ale především za jeho čas, věnovaný této práci.

Tuto práci bych chtěl věnovat své ženě Lucii a svému synu Ondřejovi.

Motto:

„Chcete-li vybudovat velký podnik, vybudujte nejdříve sebe.“

Tomáš Baťa

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

Informační technologie na nás dýchají na každém kroku. Ráno nás budí chytrý telefon, kterým nám později sdělí, v kolik nám jede autobus či vlak do práce, a jaké má zpoždění. V práci se snad již každý potká s nějakou formou IT. Ať je to osobní počítač na email, PLC co ovládá nějaký stroj, či čipová karta pro výdej obědů. Prostě jsme si tak nějak zvykli, že mnoho takových služeb funguje, jsou přínosné a dá se na ně spolehnout. Jelikož nic není bezchybné, tak se občas setkáme, že něco nefunguje. Je nás nejspíš mnoho, které už někdy nechala technika na holičkách, a to vždy v době, kdy to nejméně potřebujeme. Čím vícekrát nás služby obslouží a čím rychleji jsou opětovně v chodu, tím je považujeme za spolehlivější. Spolehlivost je vlastnost, díky které se ke službě častěji vracíme nebo ji považujeme za samozřejmou. Monitoring je nástroj, kterým tuto spolehlivost podstatně zvyšujeme.

Hlavní rozdíl mezi „pádem“ monitorované a nemonitorované sítě je v čase zotavení sítě po jejím krachu. U monitorované sítě víme, kdy vypadla (s přesností na interval testování) a co nám přestalo fungovat. Čili reagujeme ihned po výpadku a přesně tam, kde je potřeba. Za to u sítě bez dohledového systému začneme problém řešit, až na něj náhodou narazíme nebo nás na něj při nejhorším upozorní uživatel. Po-té ještě musíme samozřejmě zjistit, co se nám porouchalo. A to nám zabere také trochu času.

V případě monitorované sítě se v mnoha případech stává, že uživatel ani nezjistí, že nastal nějaký problém. A to nejen proto, že má správce sítě nemalý a tak cenný náskok, ale také ví, co za problém má odstraňovat.

Další velkou výhodou monitoringu je statistika. Ta může vyhodnocovat například, jak často je daná služba nedostupná, vytíženost jednotlivých spojení a procesorů. Výstupem pro přehlednost bývá nejčastěji grafy, které správce vyhodnocuje. Takovým typickým výstupem může být graf vytíženosti routeru při špičce. Kdy se může stát, že ač procesor není vytížen, tak odchozí linka je přetížena. Tudíž správce ví, kde přesně je problém a může navrhnout řešení v podobě nového připojení nebo omezení počtu uživatelů s připojením do internetu.

Čím rozsáhlejší síť, tím je dohledový systém nutnější. Je nutné vybrat ten správný pro danou síť, neboť každý systém je trochu jiný. Vybraný systém se aplikuje na danou síť pro získání dohledu a jasných výsledků.

I. TEORETICKÁ ČÁST

1 DOHLEDOVÉ SYSTÉMY

Systémy, jejichž prvotním účelem je sledovat stav počítačové sítě a prvků. Mezi jejich další neméně důležité funkce patří také záznam jednotlivých stavů a upozornění v případě výjimečné situace. Toto upozornění by mělo obsahovat tolik informací, aby bylo ihned jasné, co se přesně stalo. Je možné upozornit pomocí emailu či sms.

Lze nejen upozornit, ale také provést určitou akci při splnění podmínek. Například při nedostupnosti webové služby se restartuje webový server. Při takové konfiguraci dělá některé úkony (restart služby nebo zařízení, změna konfigurace zařízení atd.) dohledový systém namísto administrátora. To je nejen komfortní, ale také to snižuje čas zotavení.

Jako nejzákladnější vlastnost se bere ukládání stavů a jejich zpětné zobrazení. S tím je spjatá tvorba přehledných grafů s definovatelnými časovými rozpětími. Velmi dobrá vlastnost je více zobrazených informací v jednom grafu, například jak se mění v průběhu dne odezva serveru při různém vytížení jak spojení tak serveru samotného.

Systém lze nainstalovat na různé operační systémy s různou hardwarovou náročností. Dohledové systémy mají spoustu další funkcí. Některé jsou potřeba v domácí a některé ve firemní síti. Musí se tedy vybrat ten správný systém a správně jej nakonfigurovat.

1.1 Metody monitorování

Tedy jakým způsobem se získávají informace o daném subjektu. Při zjišťování parametrů sítě či aktivních prvků se může požít metoda aktivní či pasivní. Co se týče zjišťování stavu nebo statistik o zařízení máme také dvě možnosti. První je, že zařízení poskytuje tyto informace pomocí standardního protokolu a nazývá se ***bez agenta***. Při druhé metodě se nasadí na zařízení program „agent“, který získává informace o zařízení a posílá je monitorovacímu serveru. Této metodě se říká ***s agentem***.

Aktivní monitoring

Aktivní monitorování je umělé „vypouštění“ testových dat do sítě za účelem zjistit parametry sítě. Tato testovací data se po té zachycují na vybraném bodě a vyhodnocuje se například zpoždění, propustnost či ztrátovost. Při testování maximální zátěže se mohou částečně či úplně omezit uživatelé sítě. Je to většinou jednorázová sonda, ale může se i opakovat v pravidelných intervalech.

Nevýhody této metody spočívá v navyšování zátěže sítě testovacími daty. Simulace bývá od reality často velice odlišná, neboť simulace zátěže více uživateli s nepřebernou různorodostí dat je velice obtížná. Dosažený výsledek bude od reality vždy odlišný.

Pasivní monitoring

Při pasivním monitorování se neposílají do sítě testovací pakety, ale vyhodnocují se časové a objemové charakteristiky uživatelského provozu. Pasivní monitorování neovlivňuje uživatelský provoz a může sledovat charakteristiky, které jsou aktivním monitorováním nezjistitelné. Například jaký je objem a dynamika volné kapacity v síti, které aplikace uživatelů mají největší nároky na kapacitu sítě nebo zda v síti dochází k bezpečnostním útokům. (Ubik, 2006)

Kromě čistě aktivního nebo pasivního monitorování jsou i metody využívající kombinace obou přístupů (vhodné například pro měření ztrátovosti), metody zpracovávající data získaná z komponentu síťové infrastruktury (např. Pomocí SNMP nebo protokolu Netflow) a měření sledující stav koncové stanice (např. Pomocí rozhraní PAPI). (Ubik, 2006)

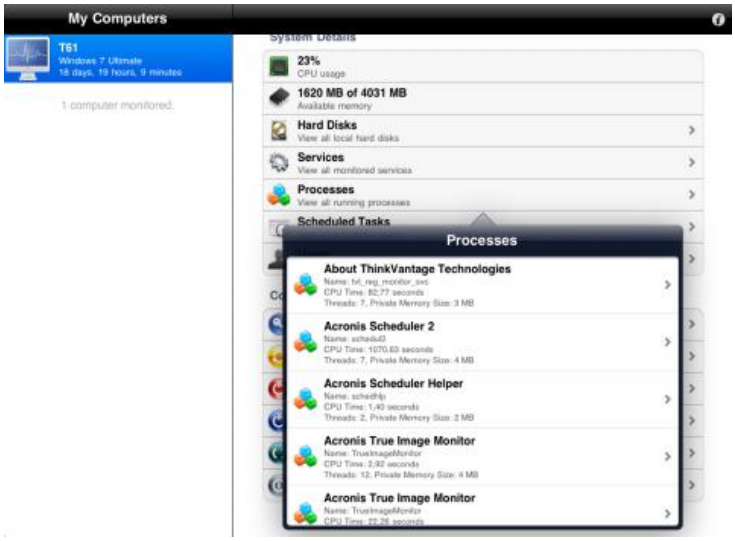
1.2 Druhy použití dohledových systémů

Dohledový systém je program, který plní svůj účel, na který byl naprogramován. Každý tento systém má jinou filozofii, jiné poselství. Je jich nepřeberné množství. Vzniká tedy potřeba je rozlišit pro správný výběr.

1.2.1 Lokální

Pouze shromažďují data o požadovaných stavech. Jedná se o výhradně sledování „co se zaplo či vyplo“ nebo „jak to jede rychle“. Tyto dohledové systémy se používají výhradně jen pro přehled a jsou částečně reprezentovány v každém OS.

Dále také program sledující počet otevřených portů, vytíženost procesů, zatížení síťového spojení, momentální rychlost zápisu na pevné disky. U takových jednoduchých systémů nebývá samozřejmostí delší náhled historie průběhu.



Obrázek 1: PC Monitor – sledování PC (Polzer, 2010)

1.2.2 Síťové

Systémy spojené výhradně s monitorováním síťových prvků a toků. Základní systémy se spokojí s detekcí zapnutý/vypnutý pomocí odpovědí na ping (ICPM echo). Detailnější rozbor vytíženosti jednotlivých linek, portů a samotných aktivních prvků poskytují ty lepší systémy. Ke spolehlivému fungování je nezbytná znalost topologie sítě, celé struktury sítě, nastavený přístup k těmto prvkům (povolené porty na firewallu, skupiny SNMP atd.).

Takovéto systémy využívají buď statistický přístup jako je technologie Netflow nebo dotazový protokol SNMP.

Používání Netflow je vhodné z řady důvodů. Můžeme sledovat zatěžování sítě v čase a plánovat rozšiřování kapacity nebo lepší využití stávajících prostředků. Zároveň můžeme údaje z Netflow použít pro analýzu bezpečnostních hrozeb, například detekovat Denial of Service (DoS) útoky. (Bouška, 2009)

Když se podíváme více do hloubky, jak funguje SNMP komunikace, tak je to velmi jednoduché. SNMP má přesně daný formát paketu, jehož aplikační část (4. vrstva dle TCP/IP modelu) je schematicky zobrazena na obrázku. Je zde vidět rozdělení na hlavičku, která obsahuje určení použité *verze SNMP* a *community string*, a *uživatelská data*, která se označují jako SNMP PDU (Protocol Data Unit). Datová část je složena z určení *SNMP operace*, *čísla dotazu* pro svázání mezi dotazem a odpovědí, případného *chybového kódu* a *ukazatele na objekt*, kde k chybě došlo, a *variable bindings*, což je svázání OID a odpovídající hodnoty. Protože se můžeme najednou ptát na více hodnot, tak *variable bindings* se může vyskytovat vícekrát za sebou pro různé OID. (Bouška, 2009)

1.2.3 Komplexní

Jedná se o universální monitorovací systém. Lze pomocí agentů či různých rozšíření (ať už programové či skriptové) monitorovat prakticky cokoliv v síti a jakýkoliv parametr. Tyto systémy jsou hardwarově náročnější. Vrací nám to pěknými přehledy zapnutých zařízení či služeb, přehlednými grafy datových toků (vstupních, výstupních).

Tyto systémy umožňují nejen sledovat vytíženost portů, služeb, serverů, ale také za splnění podmínek může zastat funkci administrátora. Jsou-li nastavená přístupová práva SNMP skupiny, kterou se na zařízení přistupuje, je schopen systém restartovat samostatnou službu a v případě neobnovení služby i restartovat samotné zařízení. Testovaní nemusí probíhat výhradně přes protokol SNMP, ale i přes TCP/IP, http, ftp atd. Záleží přímo na testované službě.

Ty z nejlepších se dokážou distribuovat. Pokud je již síť rozsáhlá, má nejen příliš mnoho zařízení, ale také mnoho sledovaných parametrů je lepší sbírat informace na několika bodech v síti a ty pak přeposílat do centrální databáze, ze které se data zobrazují.

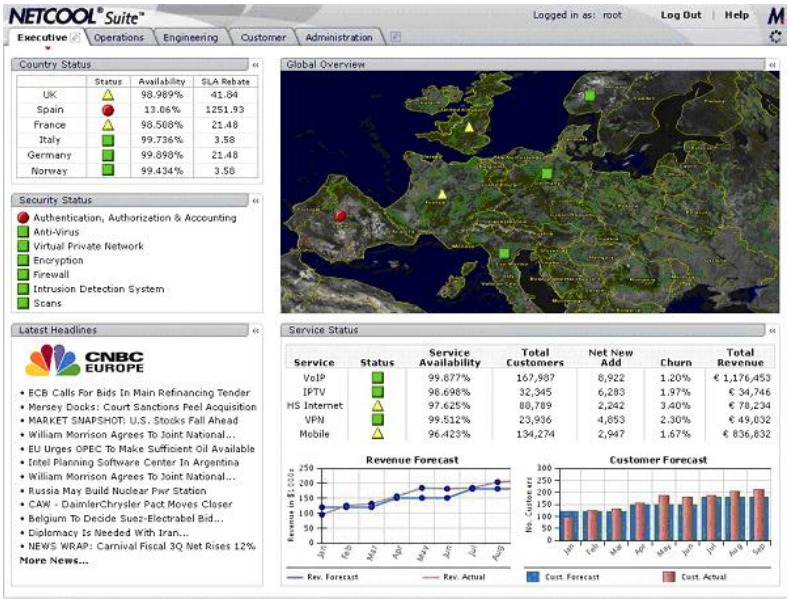
K zobrazení stavů, grafů, nastavení atd. používají většinou webové stránky. Nejspíš pro univerzálnost (zobrazí se na PC, tabletech či chytrých telefonech) a nezávislost na OS (Windows, Linux, Max OS atd.).

Produkty zdarma jsou často značně univerzální a se širokými možnostmi konfigurace. Vyžadují však také hlubší znalosti pro nastavení, protože některé konfigurace znamenají psaní vlastních skriptů. Výhoda je, že máme komplexní prostředí (které zahrnuje třeba konfiguraci, dashboard, zpracování grafů) a na míru nastavujeme pouze určité šablony pro získávání dat. Oproti tomu komerční produkty většinou nainstalujeme na pár kliknutí a monitorování rozchodíme během pár minut. Stačí znát adresy zařízení, a jaké údaje na nich chceme monitorovat. Většinou jsou zde připraveny šablony pro jednotlivé oblasti. To nám ovšem zároveň omezuje možnosti použití. Samozřejmě nic není pouze bílé nebo černé, takže i do komerčních aplikací můžeme dopisovat vlastní skripty. A nalezneme i volně šiřitelné systémy, které jsou připravené na nejběžnější nasazení. (Bouška, 2009)

1.2.4 Profesionální

Tivoli Netcool je software vhodný pro poskytovatele služeb. Nabízí software pro správu, pro monitorování a řízení kritických služeb, aplikací a síťových systémů. Tivoli Netcool

pomáhá poskytovatelům řízení bezdrátových a kabelových služeb. Poskytovatelé internetových služeb mohou čelit dnešním výzvám a dodat řešení odpovídající požadavkům. Vysoce škálovatelné a rychle nasaditelné, Tivoli Netcool software poskytuje end-to-end služby. Řízení, izolace a automatizace pomáhá poskytovatelům služeb pracovat efektivněji. (IBM, 2013)



Obrázek 2: Ukázka IBM Tivoli Netcool

Jakýkoliv produkt této kategorie nezná hranici svých možností. Nezná hranice lokální sítě, aneb dokáže monitorovat rozsáhlé sítě napříč kontinentem. Monitorování jakýkoliv parametrů či kteréhokoliv zařízení je naprostou samozřejmostí. Školení administrace systému, helpdesk, rozsáhlé fórum. To vše je k dispozici za peníze tomu všemu odpovídající. Většina profesionálních poskytovatelů si ceny chrání, respektive jsou ochotny sdělit cenu až při konkrétní nabídce. Na webové stránce *www.softwarehouse.de* se nachází nabídka licence pro IBM Program Tivoli pro přístupovou bránu a to za cenu 30876,93 Euro včetně daně (800 tisíc Kč). Nagios XI nabízí neomezenou Enterprise Edition za 6495$ (130 tisíc Kč).

1.2.5 Hardwarové

Problémem pasivního monitorování je potřeba zpracování velkého objemu dat v reálném čase. Páteřní linky současných sítí mají standardně kapacitu 10 Gb/s. Monitorování tak velkého objemu dat je potřeba rozdělit mezi hardware a software. Specializované hardwarové monitorovací adaptéry provádějí operace na nižších vrstvách komunikace v síti, jako je sledování časových a objemových charakteristik paketu i jejich klasifikace

podle protokolu nebo jiných údajů. Potom následuje zpracování již menšího objemu dat na vyšších úrovních komunikace. Tím muže být výpočet dlouhodobých statistik nebo rozpoznávání aplikací a možných bezpečnostních útoků podle obsahu vybraných filtrovaných paketu. (Ubik, 2006)

Například společnost INVEA-TECH a.s. dělá COMBO FPGA karty (FlowMon sondy), které umožňují nejen reálné sledování rychlých linek.

FlowMon sondy jsou na rozdíl od směrovačů s podporou Netflow schopny zaznamenat v reálném čase každý paket, a to i na linkách s propustností 10 Gb/s. Navíc jsou to zařízení neviditelná na L2 i L3 vrstvě, a tak jsou chráněny před útoky hackerů. Jedná se o mobilní zařízení, a proto je lze umístit do libovolného bodu v síti. Umožňuje:

- detailně monitorovat síťový provoz v reálném čase
- získat informace typu kdo komunikoval s kým, kdy, kolik se přeneslo dat, pomocí které služby atd.
- předcházet výpadkům a zahlcením sítě
- efektivně dohlížet na síť a zjednodušit správu sítě pro administrátory
- zvýšit bezpečnost sítě odhalením vnějších i vnitřních útoků
- sledovat aktivity uživatelů i aplikací (služeb), dohlížet nad využitím Internetu
- určit kritická místa sítě a optimalizovat její infrastrukturu

(INVEA-TECH a.s., 2013)

1.2.6 Speciální

Monitorovací systému mohou mít i specifická použití. S rostoucím rozšířením Internetu do firem, roste i problém s využitím lidských zdrojů. Zvyšují se požadavky na sledování činnosti uživatelů. Hlavním úkolem dohledových systémů v tomto případě je sledování aktivit na jednotlivých portech, záznam spuštění a vypnutí jednotlivých programů atd.

Velkým působištěm dohledových systémů je monitorování připojených klientů do sítě zaměřené na sledování stáhnutých dat a následným omezením rychlosti (FUP). Není to samozřejmě jediný úkol těchto systémů. Sledují taktéž výpadky uzlů, plní další služby komplexního systému. Mohou být rozšířeny i o další funkce například fakturace jako ISPadmin.

Obrázek 3:Ukázka z dohledového systému ISPadmin

Poslední dobou velice rozšířené sociální sítě si také vysloužili své monitorovací systémy. Ty ale převážně slouží pro vyhledávání jednotlivých řetězců či monitorování aktivit uživatelů.

2 PROTOKOLY

2.1 Internet Protokol

Je implementován na síťové vrstvě, je stavový a nespojovaný. Ač počítá se stoprocentním doručení paketů, neklade žádné nároky na druh spojení. To se odráží ve schopnosti komunikovat tímto protokolem přes různé typy sítí (s možností přepnutí trasy). Momentálně existují 2 verze protokolu, které mohou běžet současně na jednom počítači (dual-stack), nejsou ale navzájem kompatibilní.

Mezi nevýhody patří zejména to, že když nějaká přenosová technologie dokáže poskytnout "něco navíc", protokol IP to nedokáže využít. Příkladem může být technologie ATM, která dokáže podporovat tzv. kvalitu služeb a různým druhům provozu garantovat požadované parametry přenosu. Protokol IP však s ničím takovým nepočítá, a je-li implementován nad technologií ATM, její přednosti nedokáže využít. Mezi výhody "minimalistické koncepce" protokolu IP patří zejména skutečnost, že je možné jej implementovat snad nad každou fyzickou přenosovou technologií (neboli přenosovou technologií spadající do vrstvy síťového rozhraní). (Peterka, 2011)

IPv4

První verze IP. Dnes pořád převažující standart. Samotná adresa zabírá 32 bit. Skládá se ze čtveřice čísel oddělené tečkami (tzv. IP adresa). Každé toto číslo může mít hodnotu od 0 až 255. Při svém vzniku se jevilo jako dostatečné řešení, masový rozmach Internetu, ale ukázal opak. Před zavedením vyšší verze IP se ošetřil vyčerpání IPv4 třemi způsoby:

- Beztřídní směřování mezi doménami
- Podsítě s proměnlivou délkou masky
- Maskování podsítí

IPv6

Protokol neřeší jen problém nedostatku adresního prostoru. Má automatickou konfiguraci (funkce NDP – Neighbor Discovery Protocol), zdokonalené směrování (obsahuje funkce pro zajištění úrovně služeb QoS – Quality of Service) a vylepšené zabezpečení. Snaha autorů byla, aby většina protokolů vyšších vrstev fungovali beze změn stejně jako s IPv4. Adresní prostor má 128 bitů. Záhlaví má pevnou velikost.

2.2 TCP

Nejpoužívanější transportní protokol dnešní doby. Vychází ze standardu RFC 793. Řídící mechanismus protokolu zajišťuje, že se data přenesou nepoškozené a sestaví ve správném pořadí. Je zde několik řídicích příkazů ovlivňujících jak množství dat v paketech, tak vysílací frekvencí těchto paketů. Tento protokol je hojně využíván při prohlížení webových stránek, programy pro přenos souborů či doručení elektronické pošty.

Autoři tohoto protokolu měli na paměti nespolehlivost sítě a na úkor výkonnosti (mnoho režijních úkonů) dbali na to, aby tuto nespolehlivost eliminovali. Struktura paketu TCP může vypadat následovně:

<table>
<tr><th>Bity</th><th>4</th><th>8</th><th>12</th><th>16</th><th>20</th><th>24</th><th>28</th><th>32</th></tr>
<tr><td>0</td><td colspan="4">zdrojový port</td><td colspan="4">cílový port</td></tr>
<tr><td>32</td><td colspan="8">číslo sekvence</td></tr>
<tr><td>64</td><td colspan="8">potvrzovací číslo</td></tr>
<tr><td>96</td><td>offset dat</td><td colspan="2">rezervo-váno</td><td colspan="2">příznaky</td><td colspan="3">okénko</td></tr>
<tr><td>128</td><td colspan="5">kontrolní součet</td><td colspan="3">urgentní ukazatel</td></tr>
<tr><td>160</td><td colspan="8">volby (volitelné)</td></tr>
<tr><td>192</td><td colspan="8">data</td></tr>
</table>

Obrázek 4: Struktura TCP paketu (Sosinsky, 2010)

2.2.1 Princip

Hlavním principem je vytvoření virtuálního spojení mezi dvěma body (systémy, síťovými uzly). Přičemž tyto body jsou stále, ale cesta se může měnit. Body jsou definovány IP adresou a číslem portu. Před zahájením každé transakce musí proběhnout takzvané „potřesení rukou“ neboli třícestné zahájení spojení (three-way handshake):

I. Zahajitel spojení pošle druhému požadavek na synchronizaci (příznak *SYN*)
II. Příjemce odpoví s příznaky *SYN* a *ACK*. Zároveň dojde k výměně čísla sekvence (ISN – Initial Sequence Number). Toto číslo je každé spojení jiné a dochází k jeho změně.

III. Zahajitel tohoto spojení odpoví zprávou s pouze *ACK* příznakem. Tímto je stvrzeno spojení a oba koncové body nazýváme sockety.

Po tomto „potřesení rukou“ již probíhá výměna dat. Definice takového spojení je IP adresa příjemce, port příjemce, IP adresa odesílatele, port odesílatele. (Sosinsky, 2010)

2.3 UDP

Protokol ze skupiny internetových protokolů, který je založen na bezstavovém spojení. Koncové body tohoto spojení se nazývají datagramové sockety a data, co putují mezi nimi, se nazývají datagramy. Virtuální spojení je založeno na využívání portů a umožňuje tak multiplexování, což je souběžné posílání datových toků paralelními procesy. Přijaté datagramy se ihned extrahují, bez ohledu na pořadí, či zda se nějaké datagramy ztratily. Díky tomu je tento protokol mnohem rychlejší než TCP, ale není zase vhodný při potřebě stoprocentního doručení paketů.

UDP protokol se používá pro kratší a většinou všesměrové zprávy (např. DNS, DHCP, RIP, SNMP, hlasové a audiovizuální aplikace, atd.). Je to logické, neboť ztráta jednoho obrazového rámečku nám ze subjektivního hlediska moc nevadí.

Na Obrázek 5 je vidět jednoduchý formát datagramu UDP. Při srovnání s paketem TCP (Obrázek 4) je vidět úspora v režii už ve struktuře.

Bity	4	8	12	16	20	24	28	32
0	zdrojový port				cílový port			
32	délka				kontrolní součet (volitelně)			
64	data							

Obrázek 5: Struktura UDP datagramu (Sosinsky, 2010)

2.4 Porty

Transportní protokoly TCP i UDP používají abstraktní veličinu zvanou port, který slouží k založení internetového socketu na obou koncových bodech komunikace. Když data dorazí do svého cíle, prozkoumá se jejich zdrojová adresa, zdrojový port, cílová adresa a cílový port. Existuje úmluva definující přiřazení čísel portů různým typům datové

komunikace. Spravuje ji organizace zvaná IANA (Internet Assigned Numbers Authority, tedy autorita pro přiřazování čísel v Internetu). (Sosinsky, 2010)

Tato organizace má na svých webových stránkách seznam všech portů. Samostatný a nezávislý správce svých portů je počítač sám. Existují speciální procesy pro monitorování a vedení záznamů o portech.

Porty jsou rozděleny do 3 skupin:

Název skupiny	*Rozsah*	*popis*
Známe porty	0 – 1023	Spravuje přidělení IANA. Používají je standardní protokoly jako je FTP, HTTP, SSH atd.
Registrované porty	1024 – 49151	Výrobci, skupiny (průmyslové či obchodní), jedinci či organizace si mohou tyto porty registrovat u organizace IANA, která je má také na starosti.
Dynamické a privátní porty	49152 – 65535	Nepřiřazené a porty volně k používání. Také zde se nachází porty, které se náhodně přidělují během spojení pro zvýšení bezpečnosti. Ty se taky někdy nazývají „pomíjivé“ (angl. Ephemeral).

Tabulka 1: Rozdělení portů do skupin

Pro úplnost a přehlednost je následující tabulka přiřazení jednotlivým protokolů (TCP a UDP) a jednotlivých portů (pouze vybrané).

Číslo	*TCP*	*UDP*	*Význam*
0	Ano	Ano	Vyhrazeno
1	Ano	Ano	Multiplexor služeb na TCP portech
2	Ano	Ano	Utility pro správu
20	Ano	Ano	FTP – port určen pro tok dat
21	Ano	Ano	FTP – port určen pro příkazy
22	Ano	Ano	SSH (pro vzdálené přihlašování)
23	Ano	Ano	Telnet

38	Ano	Ano	Protokol vzdáleného přístupu (Remote Access Protocol)
161	Ano	Ano	SNMP protokol
162	Ano	Ano	Události SNMP protokolu (traps)
170	Ano	Ne	Síťová služba (PostScript po síti)
513	Ne	Ano	Protokol Who

Tabulka 2: Přiřazení jednotlivých portů významům (Sosinsky, 2010)

2.5 SNMP

Spolu s neustále se zvyšující komplexností sítí nabývá potřeba rozkrývat, administrovat a řídit zařízení v síti na důležitosti. Pro splnění těchto potřeb byl v rámci organizace IETF (International Engineering Task Force) navržen protokol SNMP (Simple Network Management Protocol). Jedná se o protokol aplikační (sedmé) vrstvy, který se postupem času stal nejoblíbenějším nástrojem pro správu síťových systémů. (Sosinsky, 2010)

Chápat se dá jako sytém SNMP, který má těchto pět prvků:

- **Síťový protokol SNMP** – Protokol umožňuje komunikaci mezi zařízením a speciálním softwarem a to prostřednictvím SNMP v TCI/IP sítích.
- **Řízené objekty** – Ty objekty, které se spravují. Např.: routery, přepínače, tiskárny atd.
- **Agenti** – Softwarová část běžící na řízených objektech. Ta shromažďuje data o objektu samotném a o síťové komunikaci. Tyto data nabízí pomocí dotazů protokolu SNMP.
- **Báze MIB (Management Information Base) –** Kompletní informace o řízených objektech ve formě databáze. Většina dat je určena pouze pro čtení, ale existují i data, které je možné měnit (proměnné řídícího objektu). Důraz je kladen hlavně na snadnou rozšiřitelnost databáze. Obsah jednotlivých objektů je dán typem tohoto objektu. SNMP neurčuje žádné povinný typ atributů, co musí každý prvek obsahovat. Dokonce ani neurčuje, které atributy musí být proměnné. SNMP určuje způsob uložení (soubory MIB) a definuje způsob poskytnutí pro uživatele.
- **Konzola –** V tomto softwaru se tvoří dotazy a sbírají data. Komunikuje přes SNMP protokol.

Verze protokolu jsou:

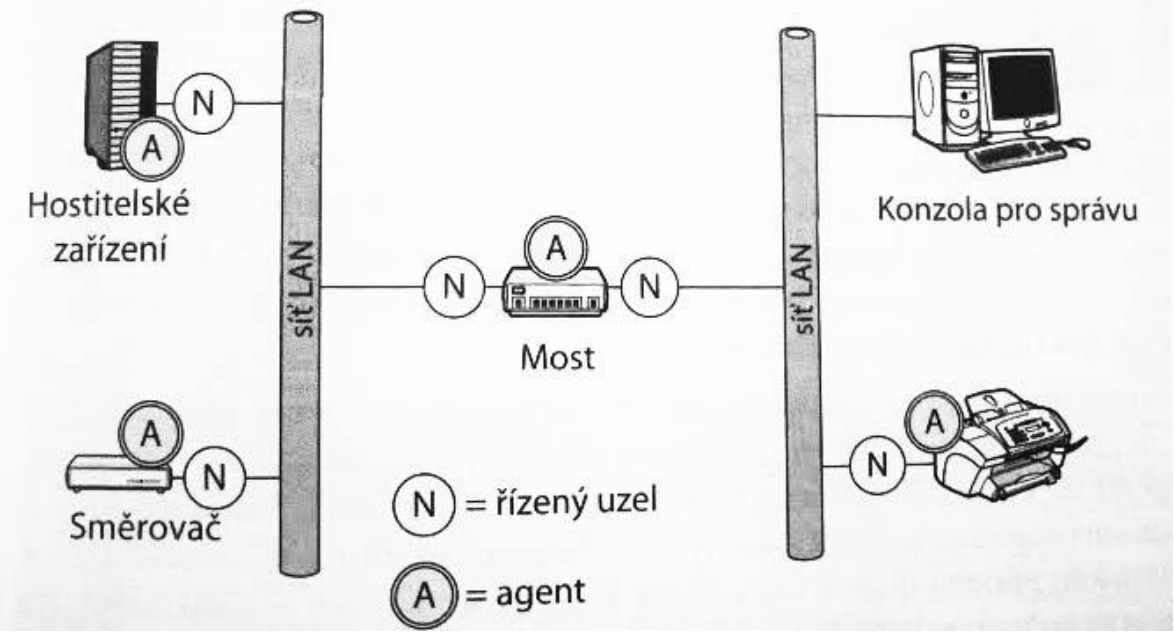
SNMPv1 – Prvotní verze protokolu. Slabá bezpečnost.

SNMPv2c – Vychází z první verze. Jsou zde přidány další datové typy a struktury. Není kompatibilní s verzí č. 1 (rozdílný formát zpráv a operací). Přidána kontrola doručení zprávy (ošetření ztrátovosti paketu pomocí UDP protokolu).

SNMPv3 – Rozšířeno o zabezpečení (šifrování) a vzdálenou konfiguraci.

2.5.1 Princip

Základem jsou SNMP příkazy odeslané směrem k řízeným objektům (respektive uzlům). Konzole tyto příkazy posílá a sbírá odpovědi od agentů. Odpovědi ukládá, aby byly později k nahlédnutí uživateli. Uživatel může řízené objekty konfigurovat přes konzolu a to pomocí SNMP příkazů. Jednoduchý příklad použití je na Obrázek 6.



Obrázek 6: Příklad správy pomocí SNMP protokolu

2.6 ICMP

ICMP (Internet Control Message Protocol) je protokol definující zprávy, které si systémy v síti IP zasílají jako požadavky nebo reakce na události při přenosu dat. Je velmi důležitý pro řízení provozu a zahlcení sítě, slouží k signalizaci korektního doručení paketů i požadavků na jejich opětovné zaslání a kontrolu směrování. Expirace parametru životnosti (TTL – Time To Live) IP paketů je jednou událostí, která má následek zaslání chybové zprávy ICMP. Pro správné fungování protokolu IP musí systémy podporovat zprávy

ICMP. Korektní chování ICMP je nutnou podmínkou pro bezchybnou komunikaci v sítích IP. Existují přitom dvě verze tohoto protokolu, jedna určená pro IPv4 a druhá pro IPv6. (Sosinsky, 2010)

ICMP je nespolehlivý formát přenosu, neboť ICMP zprávy se vždy vlezou do jednoho datagramu a není tedy nutné ověřovat doručení. IANA na svém webu také rozepisuje jednotlivé typy hlášek. Pro ukázku zobrazíme vybrané i rozdíly mezi verzemi (ICMPv4 a ICMPv6):

Typ	Jméno	Popis
0	Echo Reply	Odpověď na výzvu k odezvě (příkaz PING)
3	Destination Unreachable (ICMPv4)	Např. Cílový hostitel, port, protokol je nedostupný. Atd.
	Time Exceeded (ICMPv6)	Čas vypršel
4	Source Quench (ICMPv4)	Žádost o snížení toku (zahlcení sítě)
	Parameter problem (ICMPv6)	Problém s parametrem
8	Echo	Výzva k odezvě (příkaz PING)
11	Time Exceeded	TTL paketu vypršela na cestě
13	Timestamp	Žádost o časové razítko
14	Timestamp Reply	Odpověď (na Typ 13) na časové razítko
15	Information Request	Žádost o informace
16	Information Reply	Odpověď (na Typ 15) na žádost o informace

19	Reserved (for Security)	Rezervováno pro zabezpečení
20-29	Reserved (for Robustness Experiment)	Rezervováno pro testování odolnosti vůči výpadkům
40	Security failures	Selhání zabezpečení
255	Reserved	Rezervováno pro budoucí informační zprávy ICMPv6

Tabulka 3: Typy zpráv ICMP (IANA, 2013)

3 VYBRANÁ PROGRAMOVÁ ŘEŠENÍ

Samotná naprogramovaná řešení monitorovacích systémů se od sebe velice liší. Jak v nárocích na operační systém, tak možnostmi nastavení, přívětivostí instalace a nastavení. Dnes existuje opravdu široká škála těchto programů. Třeba od velkých korporací jako je IBM (IBM Tivoli Netcool), Cisco (CiscoWorks LAN Management Solution) a Microsoft (Microsoft System Center Operations Manager). Jedná se profesionální, ale drahá řešení. Levnější variantou jsou placené programy např.:Zenoss, PacketTrap, WhatsUp Gold. Tyto programy mají taktéž vysokou úroveň. Řešení pro malou firmu stojí například u WhatsUp Gold přes tisíc dolarů a to se nesmí ještě zapomenout na práci administrátora. Existují také volně dostupné programy jako Cacti, Nagios a Zabbix. Ty ač jsou zdarma, tak se vyznačují vysokou kvalitou a širokou škálou použití i vyspělými funkcemi. Většinou je k nim připojená veliká komunita, která velice ráda při problémech poradí. Jedná se tedy o zajímavou alternativu v monitoringu aktivních prvků.

3.1 Cacti

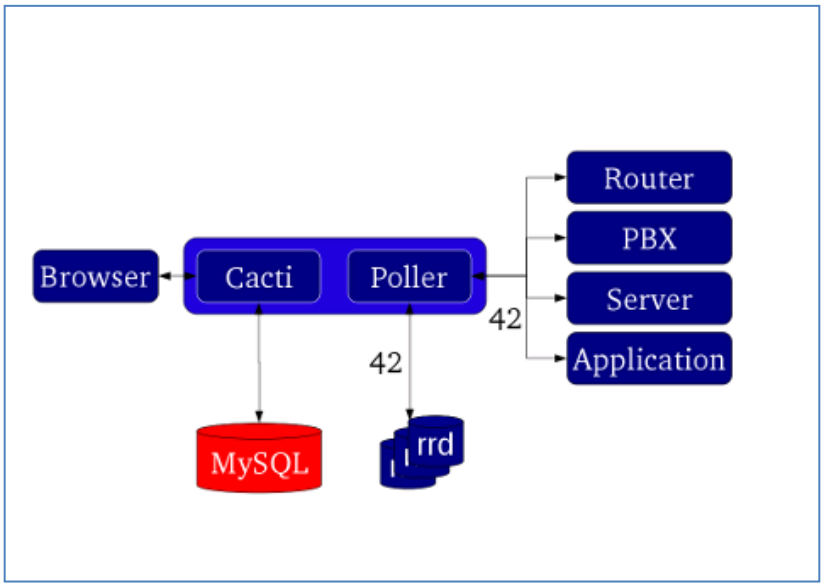
Cacti je postaveno na RRDtoolu, který ukládá a načítá všechny nezbytné informace pro vytváření grafů z MySQL databáze. Je kompletně napsán v PHP. Aby bylo schopno zpravovat grafy, zdroje dat a Round Robin Archives v databázi, Cacti udržuje vytěžování data. Je zde také podpora SNMP pro užití v přenosových grafech s MRTG. (The Cacti Group, Inc., 2004-2012)

3.1.1 Jádro a princip

Pro běh systému je zapotřebí webová služba umožňující PHP a také databáze MySQL. Tři části operací jsou rozděleny do získání, uložení a zobrazení.

O získávání dat se stará Poller, který se nastaví pro pravidelné spouštění. Může využívat pro sběr dat jak PHP prostředky, skripty a nebo pluginy. Jakmile je přidán zdroj dat, tak je automaticky obsluhován v nastavených intervalech, který lze modifikovat.

Data se mohou uložit do MySQL databáze, anebo je zpracuje RRDtool do kompaktních souborů (viz. Obrázek 7).



Obrázek 7: Princip Cacti (The Cacti Group, Inc., 2004-2012)

K zobrazení dat se používá RRDTool s svými bohatými možnostmi. Základní zobrazení grafů je pomocí šablon (*Graph Templates*) automaticky sřetězenými se šablonami datovými (zdroje dat).

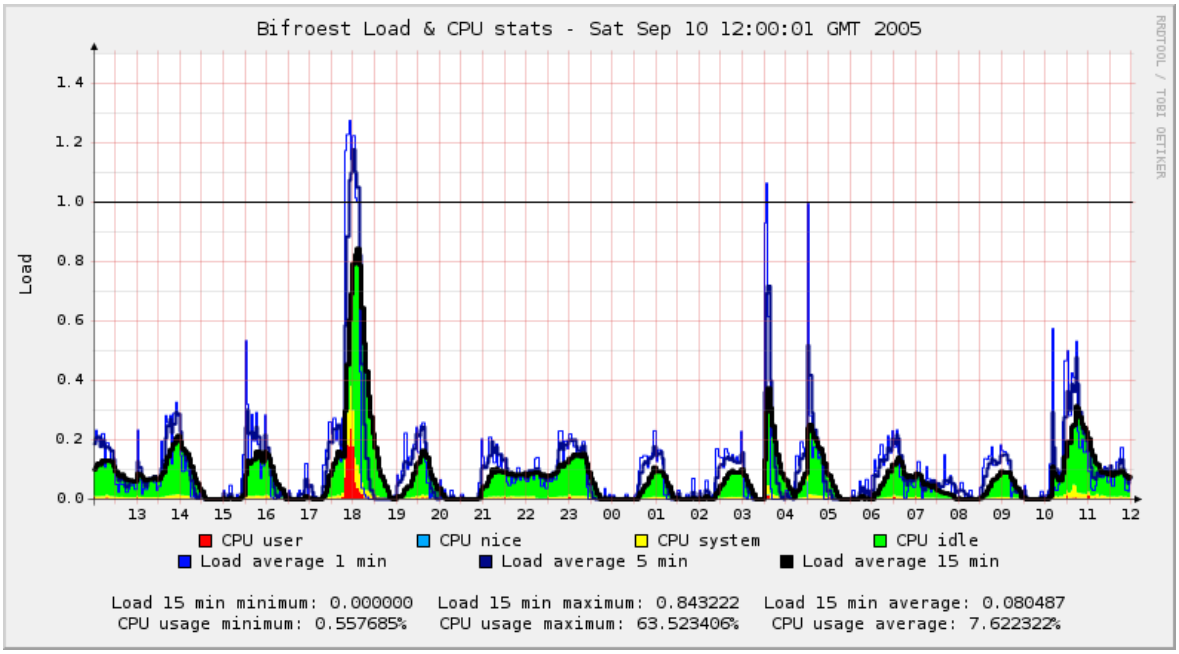
Jakmile je jeden nebo více datových zdrojů definován, může být graf RRDtool vytvořen. Cacti umožňuje vytvořit téměř jakýkoliv představitelný RRDtool graf s využitím všech standardních typů RRDtool grafů a konsolidačních funkcí. Výběr barvy pozadí a funkce automatické textové výplně také pomáhají při tvorbě grafů, aby byl tento proces jednodušší. Nejen, že můžete vytvořit základní RRDtool grafy v Cacti, ale existuje mnoho způsobů, jak je zobrazovat. Spolu se standardními „zobrazení seznamu“ a „režim náhledu“, je tam „stromový pohled“, který umožňuje, aby se grafy zobrazily na hierarchicky stromově pro organizační účely. (The Cacti Group, Inc., 2004-2012)

3.1.2 RRDTool

Jedná se o open source nástroj, který byl vyvinut na zpracování časově závislých informací (teplota prostředí, tok vody, spotřeba elektřiny, vytížení procesoru, síťový tok atd.). Zakládá se na systematickém a účinném zpracování dat. Tato data umí taky analyzovat neboli rychle vytvářet přehledné grafy za definovaný časový úsek.

Při sledování stavu systému, je vhodné, aby byly tyto údaje k dispozici v konstantním časovém intervalu. Bohužel, systém nemusí být vždy schopen načítat data v přesný čas, který je požadován. Proto RRDtool umožňuje aktualizovat soubor protokolu kdykoliv budete chtít. To bude automaticky interpolovat hodnotu datového zdroje na nejnovější

oficiální časový slot (interval) a psát tyto interpolované hodnoty do protokolu. Původní hodnota, kterou jsme zadali, je tak dobře uložena a bere také v úvahu při interpolací další položku protokolu. (Oetiker, 2009)



Obrázek 8: Příklad grafu z RRDtoolu

3.1.3 Rozšíření

Co použitelnost Cacti dále zvyšuje, jsou Pluginy. Na nasazení pluginů je nejprve nutné nainstalovat Plugin Architecture. Instalace pluginů už je potom jen otázkou nakopírování patřičných souborů na správné místo a zapsání názvu pluginu do konfiguračního souboru. Pluginy jsou ke stažení na adrese cactiusers.org. (Macek, 2009)

Tyto pluginy vytváří silná komunita kolem projektu Cacti a dodávají tomuto systému všestrannost a umožňují i profesionální použití. Následuje tabulka s vybranými pluginy:

Architecture	Nutný plugin pro provoz ostatních pluginů
BackUP	Umožní kompletní archivaci dat a nastavení i na vzdálený disk
Discovery	Najde zařízení s podporou SNMP, které ještě není sledováno
MACtrack	Zobrazí klienty na jednotlivých přepínačích (určí z CAM tabulek)
Manage	Umožňuje vzdálenou správu serverů a dalších zařízení.
NCP	Určený pro propojení s programem Nagios. Lze tímto pluginem

	využívat jeho data a funkce.
Realtime	Nahlížení grafů „naživo“
Reports	Umí rozesílat v nastavitelných intervalech grafy přes email
Thold	Hlídá námi navržené hranice hodnot u jednotlivých prvků
Uptime	Pokud sledované zařízení splní námi dané podmínky, umí toto zařízení restartovat přes SSH.
Weathermap	Vytváří grafické rozložení sítě

Tabulka 4: Nejpopulárnější pluginy Cacti a jejich význam

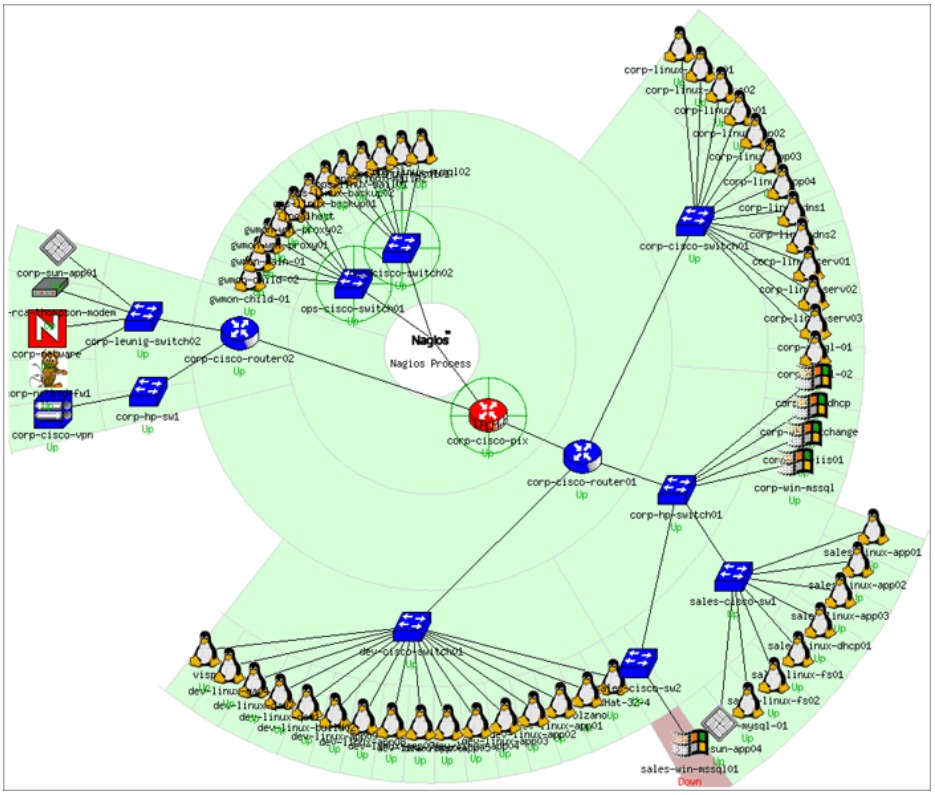
3.1.4 Uživatelský přístup

Umožňuje vytvořit pro každého uživatele svůj profil, ke kterému se budou vázat i jiné grafy. Například by jeden správce mohl sledovat vytížení serverů a uživatelských stanic, druhý by pak sledoval dostupnost a vytíženost sítě a jejich prvků. Tento prvek dává velké možnosti v prezentaci samotného monitoringu.

3.2 Nagios

Patří mezi nejoblíbenější dohledové systémy, to potvrzuje několik nezávislých anket na internetu a mnoho firem, zaměřených na monitoring sítě, využívá právě Nagios. Jedná se o open source řešení pro monitorování, které poskytuje spolehlivě pro stovky tisíc organizací po celém světě. Nagios open source se skládá z různých Nagios projektů.

Nagios dovoluje sledovat funkce velkého množství různých zařízení a služeb; nepatří-li mezi standardní vybavení metoda testování vašeho zařízení, lze systém jednoduše o tuto specifickou metodu rozšířit. Systém byl navržen na Linuxu jako open source software, monitorovat lze prakticky vše, včetně počítačů s operačními systémy Linux, UNIX, Windows, přes telefonní ústřednu až po fyzikální veličiny. V případě výpadku monitorovaného zařízení nebo služby, systém dokáže poslat prostřednictvím mailu nebo GSM upozornění správcům sítě či samostatně provést některou z předem definovaných akcí - restart problémové služby apod. Systém je možno rozšiřovat prostřednictvím uživatelských funkcí (pluginů), a lze tak monitorovat velké množství zařízení, služeb, definovat vlastní monitorovací postupy a reakce na různé stavy. (ORTEX spol. s r.o, 2010)



Obrázek 9: Ukázka programu Nagios

3.3 Nagios XI

Jedná se rozšíření open source Nagios pro podnikovou sféru. Je to tedy placená verze. Rozdíl oproti bezplatné verzi popisuje Nagios Enterprises:

Nad rámec základních IT je monitorování zařízení produktem Nagios XI. Jedná se o monitorování na podnikové úrovni a pohotovostní řešení, které poskytuje organizacím rozšířený pohled na jejich IT infrastrukturu. Chrání také před problémy ovlivňující kritické obchodní procesy. Nagios XI poskytuje organizacím tyto vlastnosti:

- výkonné webové rozhraní
- výkonné a kapacitní plánovací grafy
- ovládací panely
- zobrazení
- konfigurační webové GUI
- průvodce nastavením
- pokročilý správce nastavení
- pokročilá správa uživatelů
- specifické předvolby oznámení pro uživatele

- non-stop provoz
- rozšiřitelná architektura
- databáze pro administraci webu

3.4 Zabbix

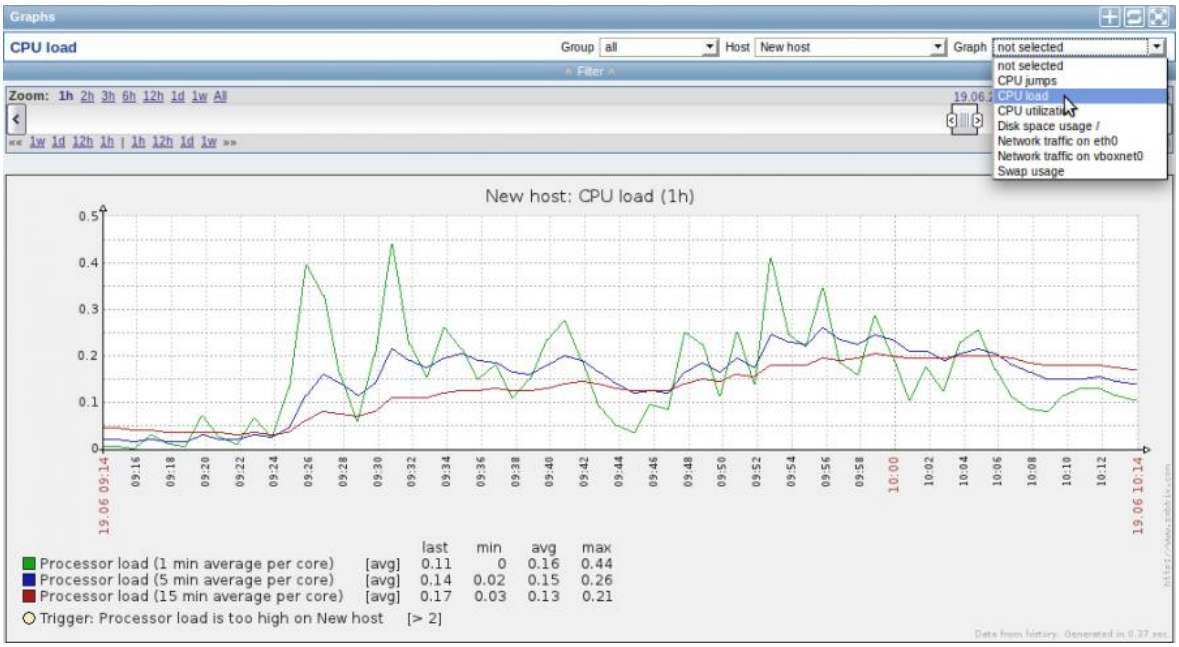
Zabbix slouží k monitorování aktivních síťových prvků (PC, servery, tiskárny, modemy, přepínače, UPS, atd.), které jsou připojeny do počítačové sítě. Metody pro sledování a zjišťování informací jsou různé. Počínaje jednoduchým ICMP echo request (ping) přes použití složitějších metod SNMP (Simple Network Management Protocol), IPMI (Intelligent Platform Management Interface), JMX (Java Management Extensions). Je možné použít také k monitoringu SSH/Telnet nebo použití agenta, který je dostupný pro většinu dnes používaných operačních systémů. Při použití agenta je možné monitorovat informace o stavu hardware (operační paměť, procesor, úložné zařízení, atd.), ale také systémové informace a stav běžících služeb. V neposlední řadě je možné integrovat do prostředí vlastní externí skripty nebo využít API, a vytvořit si tak vlastní testy. Pomocí API lze také komunikovat s jinými nástroji. Co se týká počtu dohlížených zařízení, dle tvůrců, je možné monitorovat přes 100 000 hostů a provádět tak 1 000 000 vyhodnocení za minutu, což je pochopitelně závislé na systémových zdrojích serveru, na kterém je dohledový systém provozovaný. Zabbix může pracovat distribuovaně, což znamená, že v různých vzdálených lokalitách běží Zabbix v režimu proxy a data se následně přenáší na centrální server. To je vhodné pro velmi robustní a rozsáhlé sítě s velkým počtem zařízení. Dohledový systém je přístupný z webového rozhraní, které slouží zároveň i jako administrační prostředí pro správu a vyhodnocení dat. (Antonín Kolísek, 2013)

Údaje uváděné ZABBIX SIA:

- automatické zjišťování serverů a síťových zařízení
- low-level zjišťování
- distribuované monitorování s centralizovanou správou web
- podporu pro dotazování a odchytu mechanismů
- serverový software pro Linux, Solaris, HP-UX, AIX, FreeBSD, OpenBSD, OS X
- vysoce výkonné nativní agenti (klientský software pro Linux, Solaris, HP-UX, AIX, FreeBSD, OpenBSD, OS X, Windows NT4.0 Tru64/OSF1, Windows 2000, Windows 2003, Windows XP, Windows Vista)
- monitorování bez agenta

- bezpečná autentizace uživatele
- flexibilní uživatelská oprávnění
- webové rozhraní
- flexibilní e-mail oznamování předdefinovaných událostí
- pohled na sledované zdroje na vysoké úrovni
- audit logování

(ZABBIX SIA, 2001 - 2013)



Obrázek 10:Ukázka grafů v Zabbixu (Antonín Kolísek, 2013)

3.5 WMI

Jedná se o rozšíření modelu CIM (Common Information Model) od firmy Microsoft. WMI je forma úložiště, které obsahuje informace o řízených objektech. Umožňuje správu těchto dat pomocí svého rozhraní API (pokračování modelu WDM – Windows Driver Model). Na jednom místě tedy naleznete jak informace o objektech, tak zde i zadáváte příkazy a konfigurujete dané objekty. Existují tři druhy zadávání příkazů: VBScript, PowerShell nebo příkazový řádek. (Sosinsky, 2010)

Tento systém je velice bohatý na správu. Lze také spravovat velké množství zařízení, ale technologie je specifická pro prostředí Windows.

3.6 FlowMon

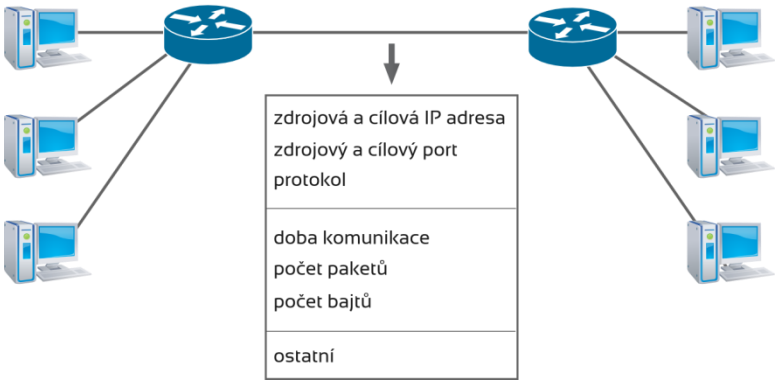
Kompletní řešení pro monitorování sítí na základě IP toků (technologie Netflow/IPFIX). Řešení FlowMon zahrnuje výkonné autonomní sondy pro všechny typy sítí až do rychlosti 100 Gb/s, kolektory pro uložení, zobrazení a analýzy síťových statistik a další rozšiřující moduly s přidanou funkcionalitou – v podobě např. pokročilého reportingu, monitorování HTTP provozu a mnoha dalšího. Řešení FlowMon je také možné rozšířit o bezpečnostní systémy pro detekci anomálií a nežádoucího provozu, které jsou postaveny na permanentním vyhodnocování chování sítě a jejích změn (NBA – Network Behavior Analysis) a díky tomu přináší výrazné zvýšení bezpečnosti sítě.

Získané statistiky o provozu na síti jsou nezbytné pro zlepšení zabezpečení sítě, odhalování a řešení problémů, účtování a fakturace za přenesená data na sdílených linkách, plánování kapacit linek, monitorování uživatelů a služeb či optimalizaci síťového toku.

3.6.1 NetFlow

NetFlow technologie efektivně poskytuje měřící základ pro klíčovou sadu aplikací, včetně účetnictví síťového provozu, účtování sítě založené na použití, sledování aplikace a uživatele, profilování, síťové plánování a analýzy, odchozí marketing a datové sklady pro oba poskytovatele služeb a podnikovým zákazníkům. (Caligare, 2011)

NetFlow je v současnosti nejrozšířenější průmyslový standard pro měření a monitorování počítačových sítí na základě IP toků. Tok je v terminologii NetFlow definován jako sekvence paketů se shodnou pěticí údajů: cílová/zdrojová IP adresa, cílový/zdrojový port a číslo protokolu. Pro každý tok je zaznamenávána doba jeho vzniku, délka jeho trvání, počet přenesených paketů a bajtů i další údaje. NetFlow statistiky vytvořené nad IP provozem poskytují informace o tom kdo komunikoval s kým, kdy, jak dlouho, jak často, nad kterým protokolem a kolik bylo přeneseno dat. (INVEA-TECH a.s., 2013)



Obrázek 11: Ukázka principu technologie NetFlow

3.6.2 IPFIX

Internet Protocol Flow Information Export (IPFIX) byl vytvořen pracovní skupinou IETF na základě potřeby společného, univerzálního standardu pro export informací o IP tocích. Standard IPFIX definuje, jak jsou informace o IP tocích formátovány a přenášeny z exportéru na kolektor. Dříve byla velká řada operátorů datových sítí odkázána na proprietární standard NetFlow společnosti Cisco popisující export informací o síťových tocích. (INVEA-TECH a.s., 2013)

II. PRAKTICKÁ ČÁST

4 ZHODNOCENÍ A VÝBĚR SYSTÉMU

Monitorovací program pro univerzitu by měl být:

- Nezávislý na OS serveru a stanic
- Hardwarově nenáročný a neúměrně nezatěžovat síť
- Snadno rozšiřitelný
- Funkční, přehledný a uživatelsky přívětivý
- Uživatelově orientovaný

K těmto parametrům se přidá cenová nabídka a možná výkonová rozložitelnost.

Velkou předností by byla implementace pomocí nějakého programovacího jazyka, který se vyučuje na univerzitě. Za předpokladu, že bude k dispozici jeho zdrojový kód (aspoň pluginů).

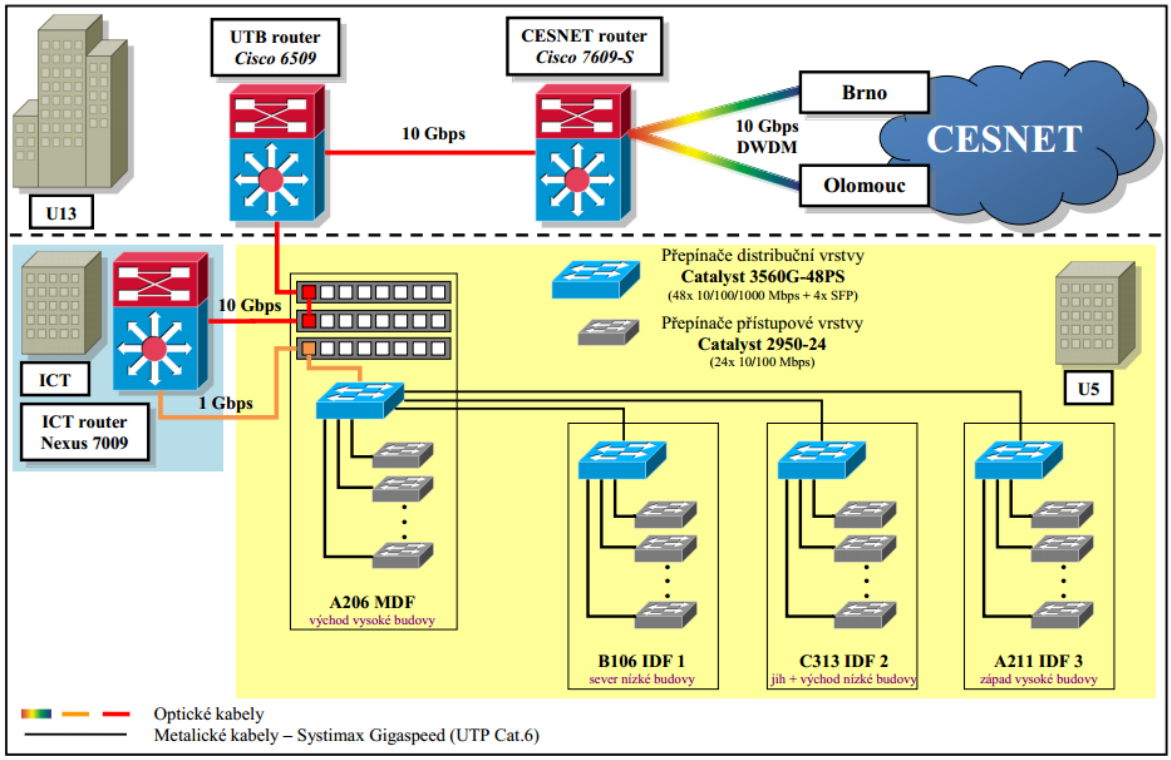
Ke komunikaci se zařízeními se musí používat všeobecně známé a používané protokoly například ICMP či SNMP.

K ukládání dat se jeví vhodný nějaký databázový systém, neboť ty jsou velice výkonné. Nejspíše by byla vhodná nějaká odnož SQL.

Tyto parametry splňují z vybraných systémů pouze Zabbix, Nagios a Cacti. Zbývající systémy jsou buď placené a demoverze s omezenými možnostmi se pro diplomovou práci nehodí.

4.1 Počítačová síť budovy U5

Počítačová síť v budově U5 Univerzity Tomáše Batě ve Zlíně je poměrně rozsáhlá (viz Obrázek 12). Jsou zde použity spolehlivé přepínače od firmy Cisco, známé svou kvalitou. Ty jsou dělány na velké zatížení, kterému během pracovního dne musí čelit. V budově se nachází mnoho počítačových učeben a spousta studentů se připojuje pomocí školní wifi sítě.



Obrázek 12: Aktuální struktura počítačové sítě budovy U5 a její připojení k Internetu

Monitoring se zaměří na páteřní přepínače (přepínače distribuční vrstvy) a také na přepínače ke koncovým stanicím a VoIP telefonům (přepínače přístupové vrstvy).

Tudíž monitorovací systém by měl zvládat mnoho zařízení a být kompatibilní s produkty Cisco. To opět splňují všechny tři systémy.

4.2 Hardwarová náročnost

Ve školní síti jsem dostal k dispozici server s dostatečnou konfigurací:

Procesor	Intel® Xeon® @ 2,13GHz
Paměť	6,00 GB
Disk	500 GB
OS	Windows Server 2008 R2 Standart 64bit

Tabulka 5: Konfigurace školního serveru

Sestavení serveru je velice solidní s dostatečnými parametry na monitoring rychlé sítě s mnoho zařízeními. Pro zjednodušení správy serveru je vhodné, aby monitorovací systém šel nainstalovat přímo na Windows Server, jelikož systém Windows je majoritním systémem UTB.

Název systému	Podporované OS serveru
Cacti	Linux, Unix, Windows
Nagios	Linux, Unix
Zabbix	Linux

Tabulka 6: OS pro monitorovací systémy

Z podporovaných operačních systémů pro server systému pouze Cacti podporuje Windows.

Žádný systém neurčuje minimální konfiguraci stroje. Stačí, pokud na stroji běží podporovaný OS, a pak běží i dohledový systém. Výkonnost stroje začíná být důležitá až při počtu sledovaných parametrů. Nějaký výpočet velikosti operační paměti, rychlosti procesoru nebo počtu jader žádný neuvádí.

4.3 Zobrazení, ovládání a podpora systému

Dnešní trendy jsou tablety a chytré telefony. Dá se očekávat, že ke kontrole systému bude docházet i z takových zařízení. Ale zároveň by mělo být komfortní i na běžné obrazovce.

Přehlednost a intuitivnost se ocení již v průběhu instalace.

Jako nejvhodnější zobrazení průběhů stavů se nabízí grafy. Grafy by měli být modifikovatelné. Jak časová osa, tak rozsah. Funkce zoom v takovém případě je neocenitelná. Volba barvy pro každý sledovaný parametr pomáhá ke zrychlení orientace ve velkém množství grafů. Sdružování více parametrů do jednoho grafu, ulehčí případné dokazování vazby těchto parametrů.

Případný export dat do univerzálního souboru se také cení.

U neplacených programů obecně se podporou nemyslí klasický helpdesk, ale je to komunita lidí komunikující převážně přes oficiální fórum. Což napomáhá při hledání řešení problémů. Pokud je komunita dostatečně veliká, je většinou vzniklý problém již vyřešen ve fóru nebo se řešení přinejmenším rýsuje.

U všech tří systémů jsou grafy a ovládání velice podobné. Co se týče komunit je vítězem Nagios, ale oba mu šlapou na paty.

4.4 Výsledná volba

Při zaměření na bezplatné řešení se výběr omezí na 3 produkty. Všechny tři jsou si velice podobné ve všech parametrech. Jejich porovnání výkonnosti není bez nainstalování zcela objektivní. Cacti pak jako jediné poskytuje server i pro Windows. To je hlavní argument pro volbu tohoto dohledového systému.

Cacti vyhovuje ve všech parametrech a v mnohých je i převyšuje. Jednak je to open source. Umí standardní protokoly a ukládá do MySQL a RRA archivů. Umí exportovat data do CSV souborů. RRDtool vykresluje velice přehledné grafy a nabízí funkci zoom pro každý graf. Výkonnost školního serveru pro Cacti by stačilo pro několik tisícovek sledovaných parametrů. Webové rozhraní je také vhodné pro moderní platformy, jakou je například tablet nebo chytrý telefon.

Vhodnost Cacti by se mohla ocenit i při výuce, jelikož Perl skripty neznají hranic. Také PHP snese spoustu úprav a vylepšení.

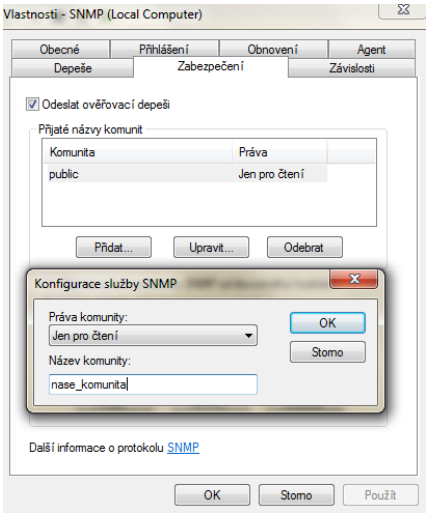
5 INSTALACE A IMPLEMENTACE CACTI

5.1 Konfigurace Windows Serveru

Jedná se „čistou“ instalaci Windows Serveru 2008 R2 verze Standart. Windows aktualizujeme, kvůli bezpečnosti.

Dále je potřeba nahrát SNMP služby. To se najde v *Ovládací panely\Všechny položky Ovládacích panelů\Programy a funkce*, tam se klikne na odkaz *Zapnout nebo vypnout funkce systému Windows*. Tento odkaz nás nasměruje do *Server manageru*, ve kterém se klikne na *Features* a *přidat Features*. Zde se vybere *SNMP služba* a potvrdí se tlačítkem *Další* a *Install*.

Je také potřeba tuto službu nakonfigurovat. *Start\Služby* kde se vyhledá *SNMP služba*, na kterou se klikne pravým tlačítkem myši a zvolí se *vlastnosti*. V záložce *Zabezpečení* v sekci *Přijaté názvy komunit* se klikne na *Přidat*. Práva komunity se nastaví na Jen pro čtení a název komunity na *nase_komunita* a potvrdíme dvakrát.



Obrázek 13: nastavení komunity

Diskusní fórum komunity Cacti doporučuje vypnout službu SNMP při instalaci. Vyvolá se nabídka *služby SNMP* ve *Službách* a zvolí se *zastavit*.

5.2 Instalace komponent a Cacti

Instalace všech komponent není potřeba, zda již jsou nainstalovány, nebo jsou-li k dispozici jejich alternativy. Existují také balíčky jako je wamp, xamp nebo EasyPHP, které již obsahují většinu komponent a zbylé si stačí stáhnout z oficiálního webu. Nebo je

možné stáhnout jednotlivé komponenty zvlášť a nakonfigurovat je podle návodu z oficiálního webu Cacti.

Možností je spousta. Nejprve byla snaha postupovat podle oficiálního webu Cacti a poskládat komponenty podle návodu. Zde několikrát nastal problém s jednotlivými verzemi komponent a nějaké nekompatibility s danou verzí Cacti. Tento problém je neduh komunitního softwaru, což je vykoupeno cenou. Rozhodlo se stáhnout kompletní balíček Cacti verze 0.8.8a vyvinutý přímo komunitou Cacti. Ten obsahuje *Apache server 2.2.22, PHP 5.3.17, MySQL Server 5.5, RRDtool 1.4.4, Spine* a *Net-snmp 5.6.1.1-1.win32*. Jedná se o jeden exe soubor velikosti 201 MB. Nejen, že odpadá nutnost shánět kompatibilní verze, ale také nutnost mnohých nastavení převážně *Apache, PHP* a *MySQL*.

Instalace probíhá dle Windows zvyklostí s těmito volbami:

- *Apache server* (je možnost použít IIS od Microsoftu, musí být ale nainstalované před touto instalací)
- *Cacti & Dependencie, Plugins, Optional Templates*
- *Zvolí se místo instalace C:*

Výpis konečných složek:

- *C:\Apache2\htdocs\Cacti*
- *C:\Spine*
- *C:\Program Files\MySQL\MySQL Server 5.5*
- *C:\Net-SNMP*
- *C:\PHP*
- *C:\RRDTool*

Zobrazí se heslo pro *MySQL* uživatele *root* a pro *administrátora Cacti*. Tím daná instalace končí.

5.3 Konfigurace Cacti a komponent

I přes jednoduchou instalaci je minimální konfigurace nezbytná.

Pluginy

Ve složce *C:\Apache2\htdocs\cacti\plugins* se nalézají předinstalované pluginy. Pokud by se potřebovala další či aktualizace nalezneme je na *http://docs.cacti.net/plugins*. Tyto pluginy se rozbalí (ze zip formátu) do výše uvedené složky.

PHP

Pro správnost časového pásma se udělá malá úprava jednoho souboru.

Otevře se soubor *C:/php/php.ini* v poznámkovém bloku a upraví se:

date.timezone=”Europe/Prague”

Konfigurace Windows

Start\Ovládací panely\Všechny položky Ovládacích panelů\Systém zde se klikne na *Upřesnit nastavení systému*. Otevře se okno *Vlastnosti systému* v záložce *Upřesnit*. Klikne se na *upřesnit proměnné*. V oblasti *Systémové proměnné* se zkontrolují proměnné:

- **MIBDIRS** s hodnotou C*:\PHP\Extras\mibs*
- **PHPRC** s hodnotou *C:\PHP*

Apache

Zkontroluje se toto nastavení v souboru C:\Apache2\conf\httpd.conf

LoadModule php5_module „c:\php\php5apache2_2.dll“

AddType application/x-httpd-php .php

PHPIniDir „C:\php“

DirectoryIndex index.php index.html index.htm

Net-SNMP

Spustí se ve složce *C:\Net-SNMP* soubory *registeragent.bat* a *registertrapd.bat* s administrátorskými právy. Tím se zaregistruje net-snmp jako agent služby snmp.

Komunita také doporučuje zkontrolovat nastavení souboru *C:\Apache2\htdocs\Cacti\include\config.php* a to tyto řádky:

$database_type = „mysql“;

$database_default = „cacti“;

$database_hostname = „localhost“;

$database_username = „cactiuser“;

$database_password = „cactipw“;

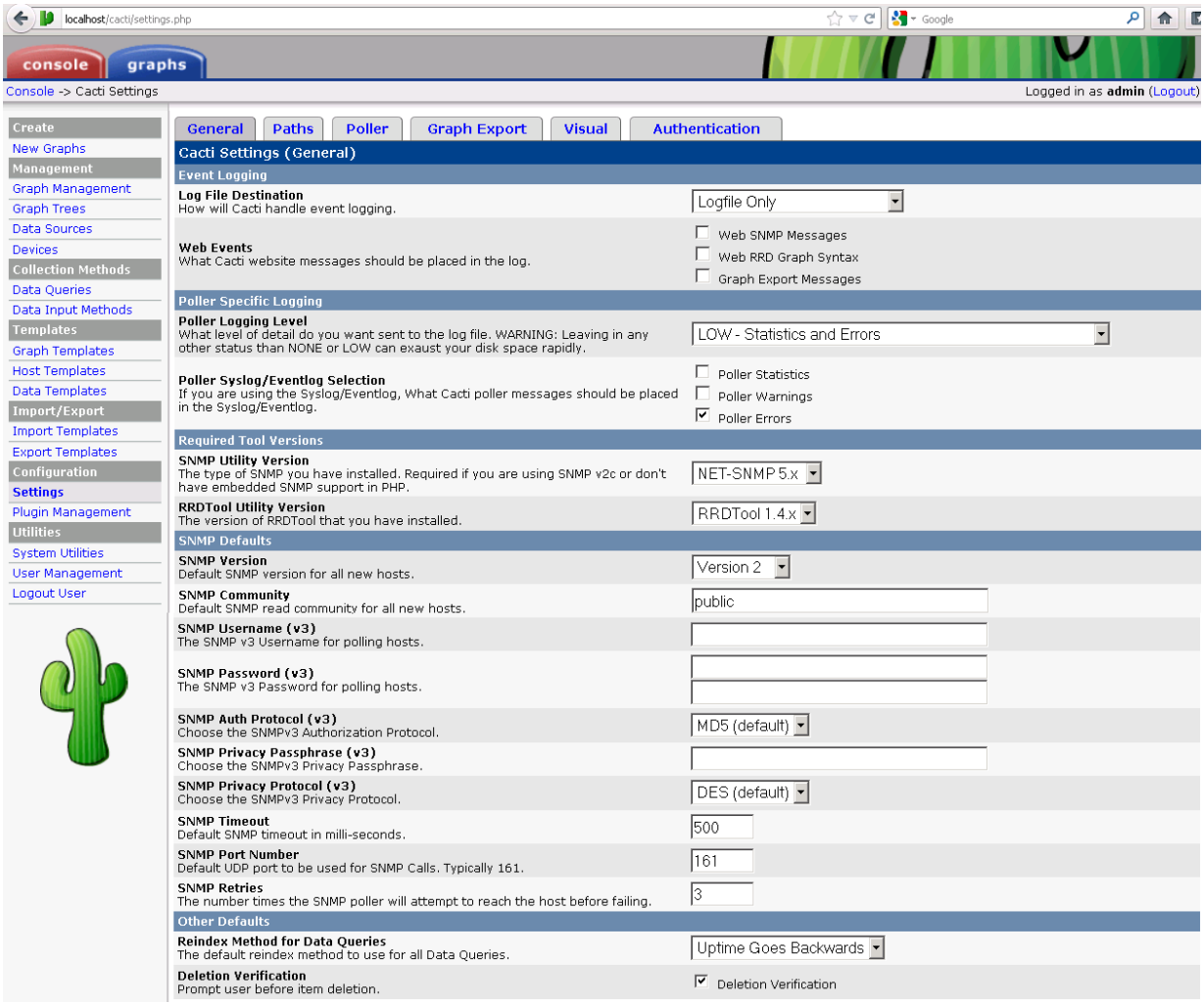
$database_port = „3306“;

$database_ssl = false;

5.4 Konfigurace ve webovém rozhraní

Po restartu serveru se zadá adresa *http://localhost/cacti/* do prohlížeče. To je výchozí adresa pro program.

Po přihlášení se zobrazí úvodní webového rozhraní. Prozatím jsou v nabídce dvě záložky *Console* a *Graphs*. Záložka *Console* slouží pro nastavování grafů, přidávání objektů a vůbec kompletního nastavení Cacti. Záložka *Graphs* slouží pouze pro zobrazení grafů.



Obrázek 14: webové rozhraní Cacti s defaultním nastavením

5.4.1 Cacti Console Settings

Prvotní záložkou v *Console/Settings* je záložka *General*. Jedná se o základní nastavení aplikace.

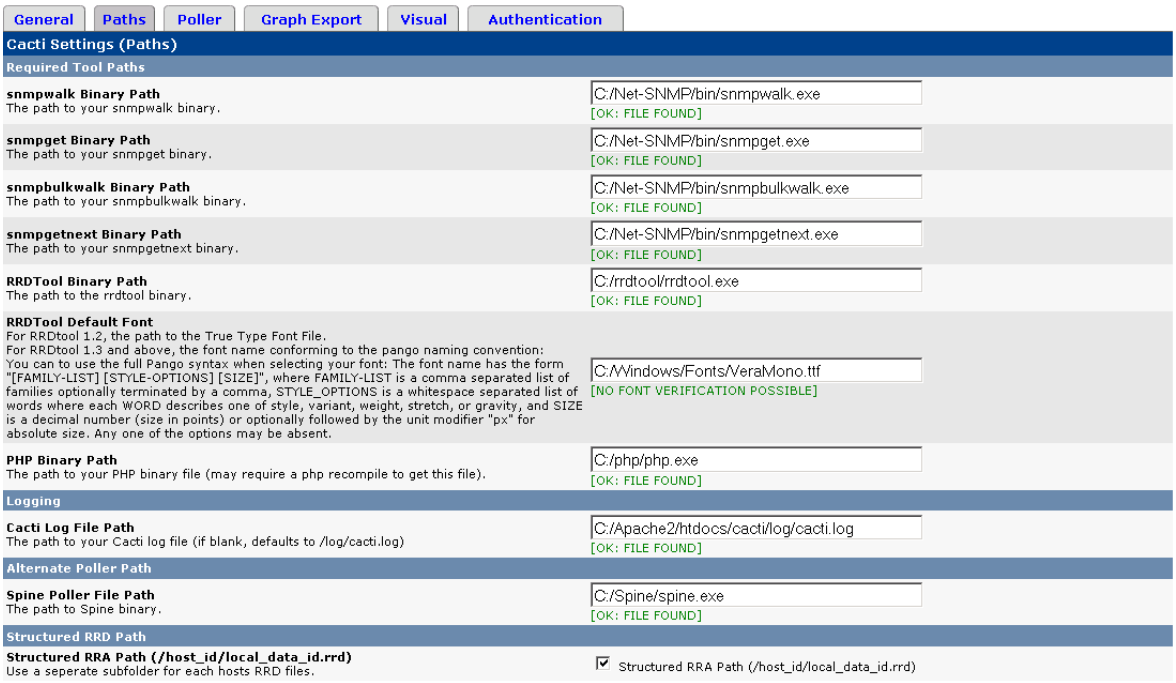
Event Logging – se ponechá původní nastavení

Poller Specific Logging – toto nastavení bychom změnili v případě nějakých chyb programu. Dá se nastavit i zaznamenávání na úrovni *Debug*, což je velmi podrobné zaznamenávání všech činností programu.

Required Tool Version – musí být nastaveno na správnou verzi jak *net-snmp* (5.x) tak *RRDtool* (1.4.x).

SNMP Defaults – Toto je výchozí nastavení pro tento protokol. Nastaví se *SNMP Version* na Version 1 a *SNMP Community* se vyplní textem *nase_komunita*.

Druhá záložka *Paths* se zabývá nastavení cest pro komponenty Cacti. Pokud je cesta k souboru dobře nastavena, po uložení se vypíše zelené hlášení [OK: FILE FOUND]. Zajímavou, a pro více zařízení nezbytnou volbou, je Structured RRD Path, což nařídí strukturované ukládání souborů RRA do složek po zařízeních.



Obrázek 15: Nastavení cest ke komponentům Cacti

Druhou je záložka *Poller*, kde se nastavují parametry výkonovému souboru poller.php čili procesu zjišťující námi požadované informace.

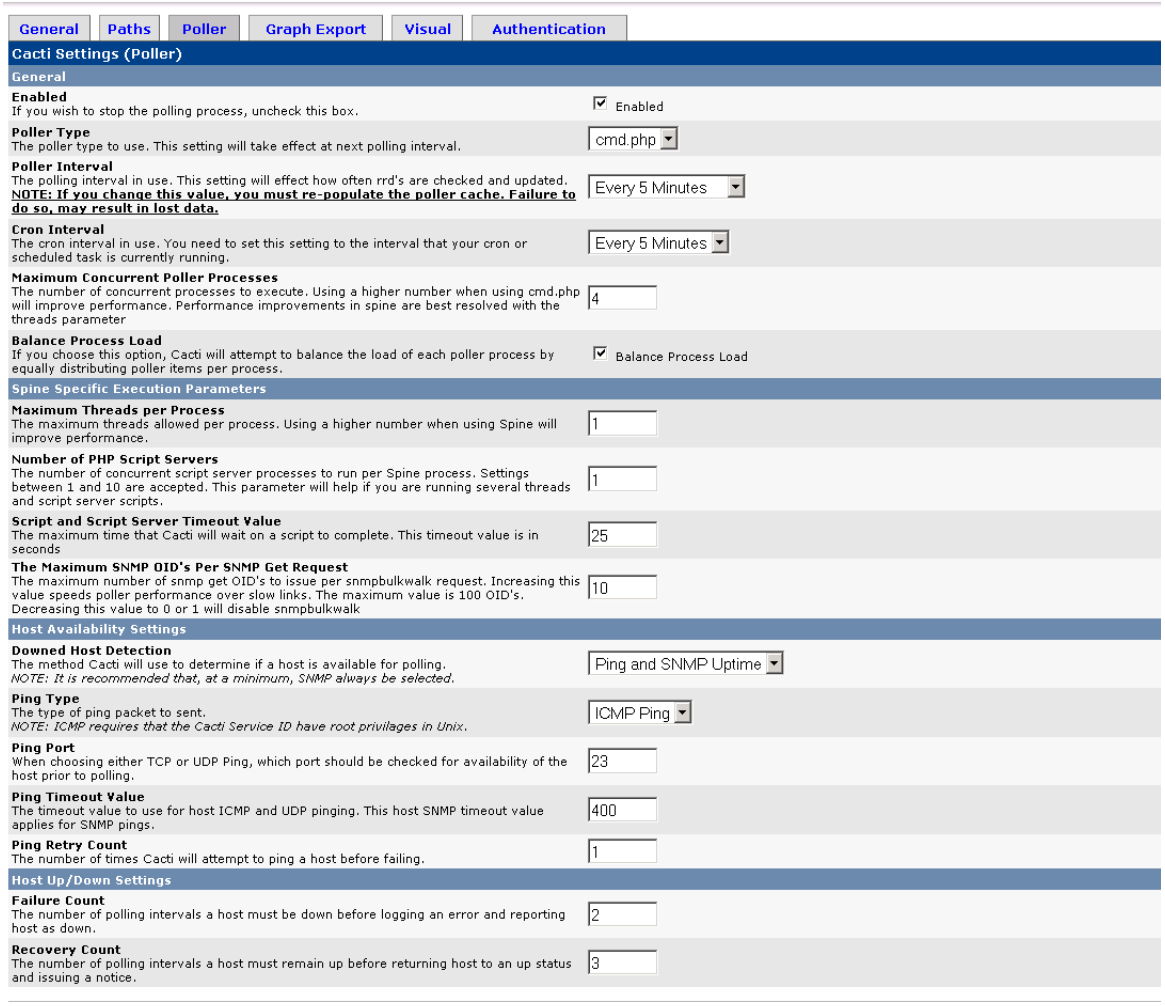
Proces lze deaktivivovat vykřížkováním *Enabled* v prvním řádku nastavení. Další položka určuje druh procesu a to mezi *cmd.php* (využívá systémový příkazový řádek, nejčastější a také doporučováno komunitou) a *spine* (obslužný program napsaný v jazyku C). *Poller Interval* a *Cron Interval* se ponechá na 5 minut. Takové nastavení poskytuje data každých pět minut, což je dostačující pro naše účely a zároveň zbytečně nezatěžuje sít. Znamená to

taky, že celá obslužná část (doba kdy poller zjišťuje data ze zařízení) nesmí překročit pěti minutový interval (na komunitním webu jeden uživatel uváděl, že zvládá monitorovat přes 1600 zařízení v tomto intervalu). *Maximum Concurrent Poller Processes* se ponechá 4 (zvyšuje se pouze při potřebě zvýšení výkonu). A *Balance Process Load* ponecháme zaškrtnuté.

Jelikož se používá cmd.php není potřeba se zabývat *Spine Specific Execution Parameters*.

Za to *Host Availability Settings* je velice důležité nastavení. Jedná se hodnoty, které se budou předvyplňovat u každého nově přidaného zařízení. Jedná se tedy o defaultní hodnoty. *Downed Host Detection* se nastaví na *Ping and SNMP Uptime*, čili se bude vyhodnocovat přístupnost jak přes Ping tak přes SNMP protokol. *Ping Type* se nastaví *ICMP Ping*. Zbývající *Ping Port, Ping Timeout Value, Ping Retry Count* se ponechají v původním nastavení.

Host Up/Down Settings se ponechají v rozumném prvotním nastavení, kdy zařízení je označeno za vypnuté při dvou nezodpovězených pingách a označeno za zapnuté při třech ping odpovědích v pořádku.



Obrázek 16: Nastavení obslužného procesu poller

5.4.2 Instalace pluginů

Bez pluginů by se mohli pouze vykreslovat jednoduché grafy ke sledovaným prvkům v zařízení. Za použití pluginů se stává z Cacti komplexní monitorovací nástroj.

V předchozích verzích Cacti (nižší než 0.8.8) se musel první instalovat Plugin Architecture. V nynějších verzi *Cacti 0.8.8a* je již součástí a to verze 3.1.

Správa pluginů je velmi přehledná a pohodlná. Vše se obsluhuje v *Console/Plugin Management*. Po kliknutí na tento odkaz se nám objeví správce pluginů.

Plugin Management (Cacti Version: 0.8.8a, Plugin Architecture Version: 3.1)

Search: Rows: Default Go Clear

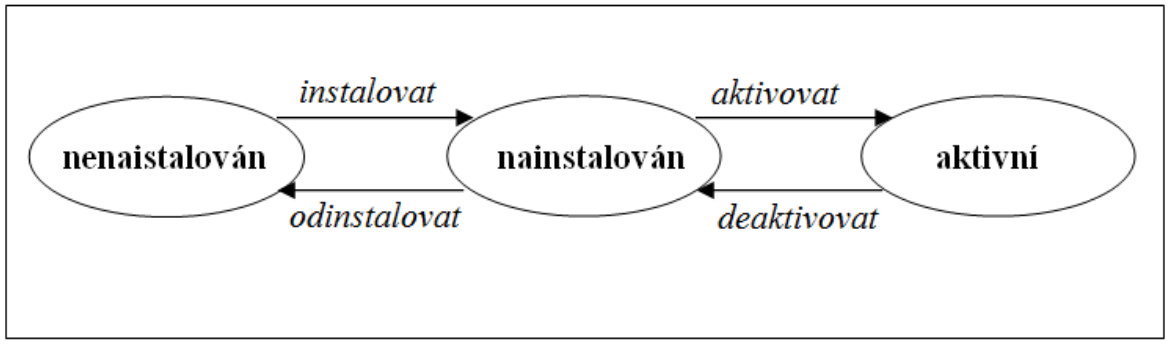
<< Previous Showing Rows 1 to 30 of 31 [1,2] Next >>

Actions	Name	Version	Load Order	Description**	Type	Status	Author
	Autom8	0.36		Automate Cacti Tasks	General	Not Installed	Reinhard Scheck
	Clog	1.7		Cacti Log View	General	Not Installed	Larry Adams
	Slowlog	1.3		Cacti MySQL Slow Log Viewer	General	Not Installed	The Cacti Group
	Aggregate	1.01		Create Aggregate Graphs	General	Not Installed	Reinhard Scheck
	Cycle	2.3		Cycle Graphs	General	Not Installed	The Cacti Group
	Dsstats	1.4		Data Sources Statistics	System	Not Installed	The Cacti Group
	Monitor	1.3		Device Monitoring	General	Installed	Jimmy Conner
	Mactrack	2.9		Device Tracking	General	Not Installed	Larry Adams
	Docs	0.4		Documents	General	Not Installed	Jimmy Conner
	Errorimage	0.2		Error Images	General	Not Installed	Jimmy Conner
	Flowview	1.1		FlowView	General	Not Installed	Jimmy Conner
	Settings	0.71		Global Plugin Settings	System	Active	Jimmy Conner
	Hmib	1.4		Host MIB Tool	General	Not Installed	The Cacti Group
	Remote	0.1		Host Remote Console Utility	General	Not Installed	The Cacti Group
	Boost	5.1		Large Site Performance Booster	System	Not Installed	The Cacti Group
	Loginmod	1.0		Login Page Mod	Old PIA	Disabled	Jimmy Conner
	Mikrotik	1.0		MikroTik Switch Tool	General	Not Installed	The Cacti Group

Obrázek 17: Správce pluginů v Cacti

Pluginy jsou uspořádány v tabulce a mohou se seřadit podle toho, co se uzná uživatel za vhodné. Zobrazeny jsou všechny pluginy nahrány ve složce *C:\Apache2\htdocs\cacti\plugins*. Jsou zde sloupce:

- *Actions* – kliknutím na symboly v tomto sloupci se pluginy instalují, odinstalují, aktivují a deaktivují.
- *Name* – jméno pluginu
- *Version* – verze nahraného pluginu
- *Load Order* – zatížení pluginu
- *Description* – zkrácený popis pluginu
- *Type* – druh pluginu (většina se dělí na systémové a obecné)
- *Status* – Stav (nenainstalován, instalován, aktivní)
- *Author* – autor pluginu



Obrázek 18: Přepínání statusů pluginů

Pokud se přidá plugin (je na mysli jeho aktivace), tak ve většině případů přibude i nová záložka vedle Console a Graphs.

Obrázek 19:Ukázka záložek aktivních pluginů

Aggregate

Plugin na souhrn grafů. V některých případech je vhodné některé veličiny zobrazit v jednom grafu, což nám umožňuje tento plugin.

Discover

Počítačová sít není nic pevně daného. Neustále se vyvíjí, mění. Stejně jako jeho prvky se taky obměňují. Tento plugin dokáže vyhledávat nové prvky, které umí protokol snmp a jsou v nastavené podsíti.

Monitor

Umožní přehled všech zařízení, nad kterými zobrazí datum čas, ke které se zobrazení vztahuje. Každé zařízení představuje jednu ikonku určité barvy – zelená zapnuté (*Up*), červená vypnuté (*Down*), oranžová zotavuje se (*Recovering*).

Při najetí kurzoru na ikonku se zobrazí základní statistika.

Settings

Plugin rozšiřující možnosti nastavení Cacti jako DNS a MAIL.

Thold

Zkráceně Thresholds (Prahové hodnoty). Jeden z nejužitečnější pluginů. Umožní nastavení jak upozorňovacích (warnings), tak kritických (Alert) hodnot a to jak spodní tak vrchní hranice. Aby bylo možné takové sledování nastavit je nutné zařízení sledovat a danou veličinou sledovat v grafu. Samozřejmostí je také nastavení emailové účtu.

5.5 Další nastavení

Po aktivaci je nutné dokonfigurovat další nastavení.

Záložka Mail/DNS se věnuje nastavení dle svého názvu. V první oblasti *Emailing Options* se vyplní testovací email (na který se dá zaslat testovací email), *Mail Services* se bude provozovat pomocí *SMTP*. Dále se vyplní, od koho se budou emaily odesílat „cacti@localhost“ a jméno „Cacti“. *Word Wrap* se ponechá nezměněno.

Do *SMTP Options* se do *hostname* vyplní lokální IP adresa (serveru) a *port* se doplní standardní 25.

DNS Options není nutné vyplňovat. Doplnili se veřejné google dns servery *8.8.8.8* a *8.8.4.4*.

V záložce *Misc* se upraví pouze oblast *Discover*. *Subnet(s) to scan* se vyplní všechny podsítě, které se mají sledovat. *DNS server* je nejlépe vyplnit lokální. *Ping Method* se použije ICMP. *SNMP Communities,* zde se uvedou všechny komunity, které se používají v nadaných zařízeních. V našem případě se vyplní *nase_komunita*. *Poller Frequency* je dostačující každých 12 hodin.

5.6 Spuštění pravidelného polleru

Poller.php se musí spouštět pravidelně. Využije se součásti každého Windows, a to *Plánovače úloh* (*Task Scheduler*).

Instalátor již událost vytvořil, je dobré ale zkontrolovat hlavní parametry. Události se jmenuje Cacti, a pokud se na ni klikne, tak se otevře na záložce *Obecné*. Zde je nutné, aby se v *oblasti zabezpečení* zakřížkovalo *Spustit nezávisle na přihlášení uživatele* a *Spustit s nejvyššími oprávněními.*

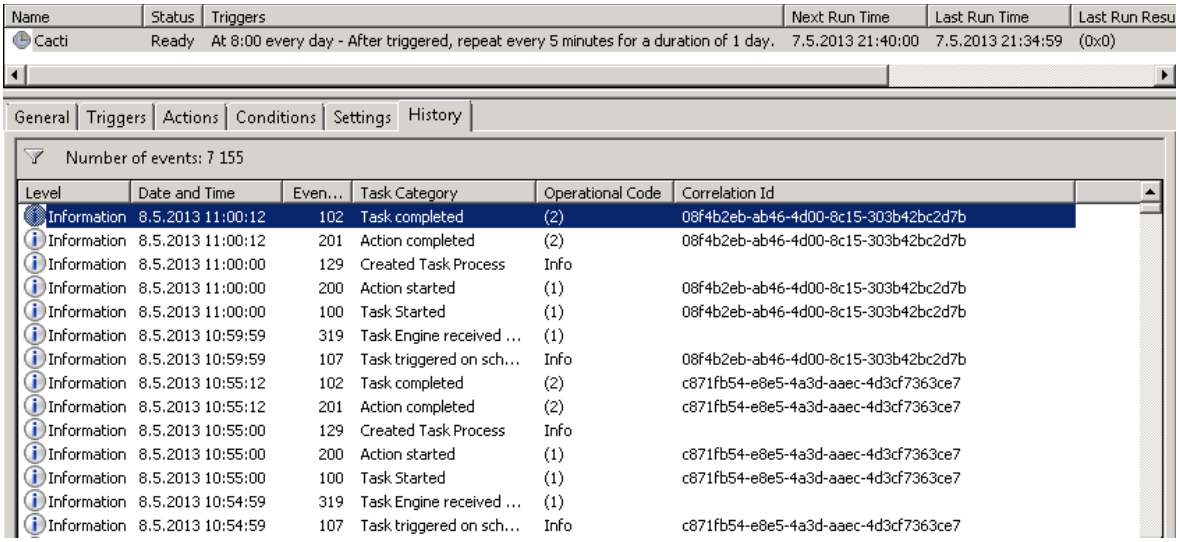
V záložce *Aktivační události* se nastavují podmínky spouštění události. V našem případě je to Začátek úlohy: *Podle plánu*. Nastaví se *denně*. Upřesněné nastavení je *opakování úlohy 5 min* trvání *1 den*. *Povoleno* se zakřížkuje. Tímto se nastaví spouštění této události každých pět minut pořád dokola.

Záložka *Akce* se zabývá tím, co se bude během vzniku události dělat. V našem případě se jedná o *Akci: Spustit program*. Program je *C:\PHP\php.exe* s argumentem *C:\Apache2\htdocs\cacti\poller.php* a spouštět v *C:\Apache2\htdocs\cacti*.

V další záložce se pouze odkřížkuje *Spustit úlohu pouze při připojení k napájení*.

Záložkou *Nastavení* se volí poslední možnosti pro událost. Zakřížkováno se nechá pouze *Povolit spuštění úlohy na požádání* a *Při selhání úlohy znovu spustit každých* 5 minut a *Počet pokusů o restartování* nastavit na 3 krát. Pravidlo pro kolizi úloh je *Zastavit stávající instanci.*

Celé nastavení se potvrdí tlačítkem OK. V pravém sloupci Plánovače úloh *Akce* se klikne na *povolení historie všech úloh*. Tím se získá lepší přehled o průběhu události.



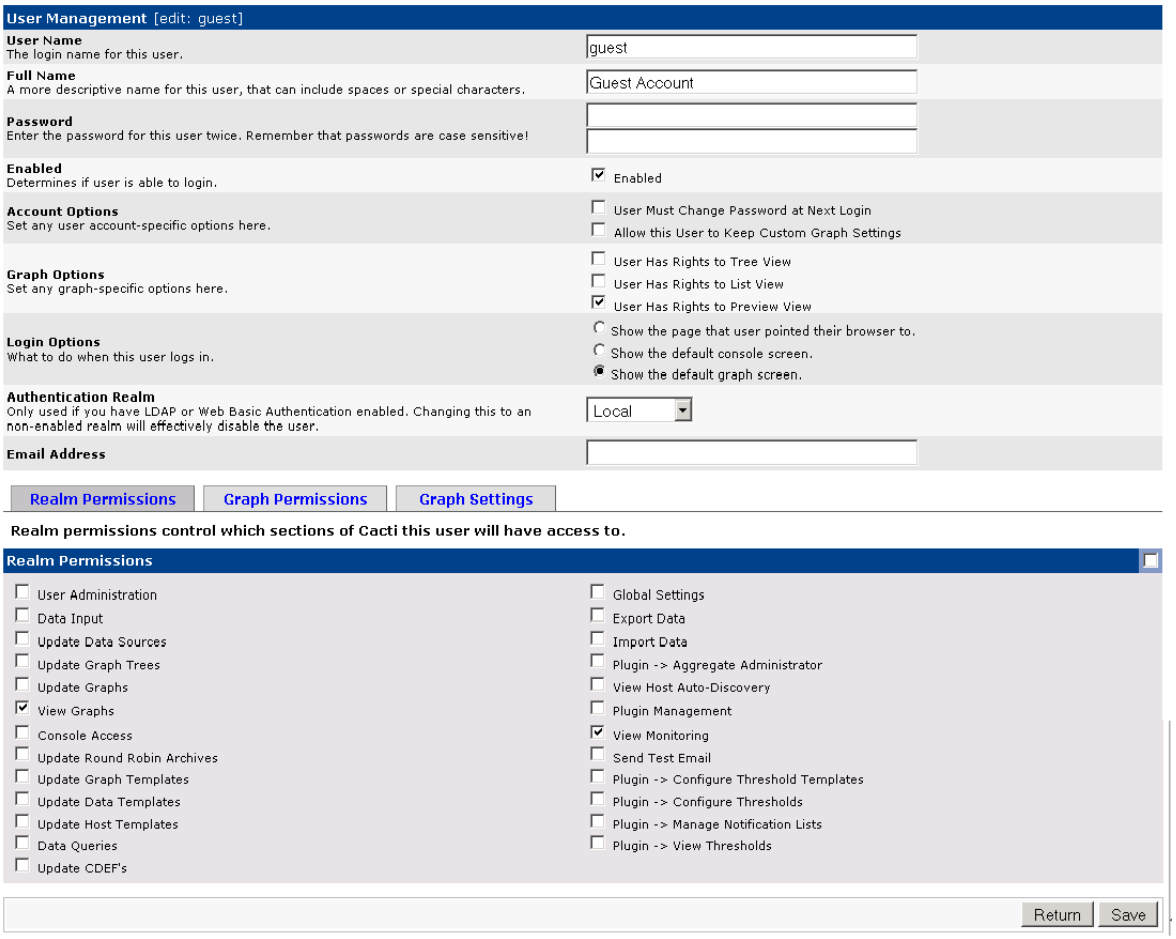
Obrázek 20: Ukázka historie události

5.7 Správa uživatelů

V Cacti se nastaví uživatelé a jejich práva velice snadno. Vše se nastavuje v *Console/User Management*. Zde se klikne na účet guesta a změní se jeho nastavení.

Zakřížkuje se *Enabled*, tím se povolí účet guesta. *Account Options* se zcela odkřížkují, neboť zabezpečení guesta není potřeba. V *Graph Options* se zakřížkuje pouze políčko *User Has Rights to Preview View*.

V *Realm Permissions* se ponechá pouze *View Graphs* a *View Monitoring*.



Obrázek 21: Nastavení uživatele guest

5.8 Prvotní přidání hosta

Přidání prvního hosta bývá zpravidla hostitel (stroj, na kterém Cacti běží). Tento host bývá defaultně již vytvořen, ale lepší je, jej vytvořit znovu a dle vlastní konfigurace.

Seznam všech přidaných zařízení se nalézá pod *Console/Devices*. Tady se smaže původní zařízení a přidá se nové zařízení, stisknutím *Add*.

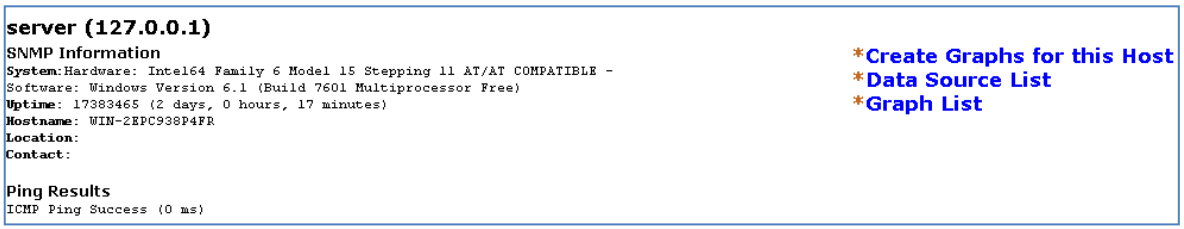
Vyplní se kompletní list nastavení zařízení. *Description* se vyplní jako jméno prvku, čili „server“. *Hostname* je IP adresa zařízení. V *Host Template* se zvolí, dle které šablony se pro zařízení mají přiřadit šablony grafů a datové dotazy (*Data Queries*). Pro server se zvolí šablona *Windows 2000/XP host*. *Number of Collection Threads* nemá vliv na sběr dat pomocí cmd.php.

Availability/Reachability Options vychází z *Host Availability Settings*, tudíž se může přeskočit.

SNMP Options je konkrétní SNMP nastavení daného zařízení. V případě serveru je *SNMP Version* verze číslo 2 (*Version 2*). Do SNMP Community se vepíše název komunity, která je na serveru nastavena (nase_komunita). *SNMP Port*, *SNMP Timeout* a *Maximum OID's Per Get Request* se ponechá v původním nastavení.

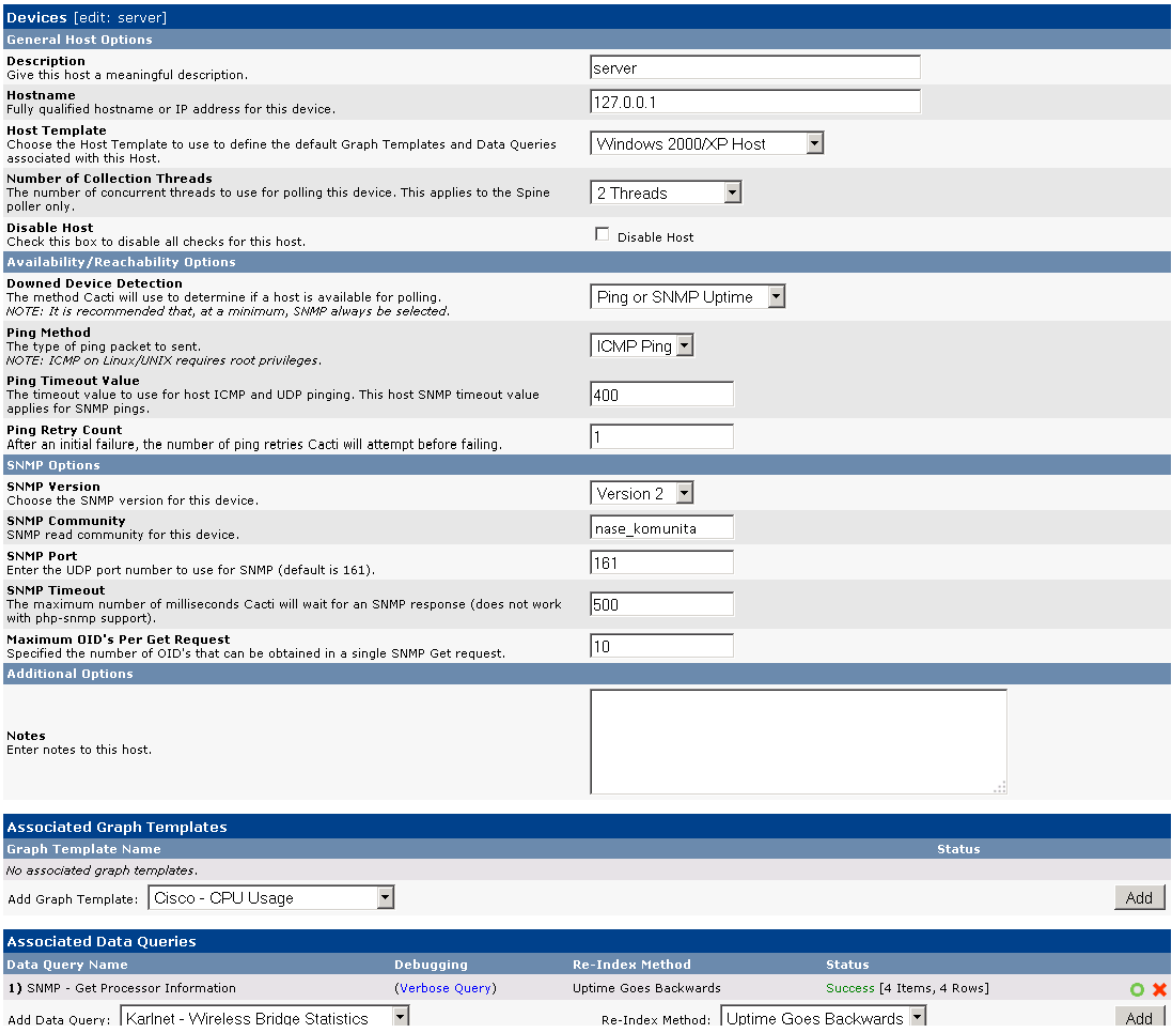
Volbu potvrdíme tlačítkem *Create*.

Po obnovení stránky přibudou, při správné konfiguraci SNMP, Informace o zařízení a hodnota ICMP pingu.



Obrázek 22: Informace o zařízení ze SNMP

Jelikož se bude zobrazovat jen vytížení jednotlivých procesorů, musí se upravit *Associated Graph Templates* (připojené grafické šablony) a *Associated Data Queries* (připojené datové dotazy). Ponechá se pouze *SNMP – Get Processor Information* v sekci *Associated Data Queries*.



Obrázek 23: Kompletní nastavení prvního zařízení – serveru

V horní části se klikne na **Create Graphs for this Host*. Zobrazí se nabídka připojených grafických šablon a datových dotazů. Vyberou se všechny (čtyři) procesory a klikne se na tlačítko *Create*.

Na další obrazovce se pouze volba potvrdí.

5.9 Přidání sledovaných přepínačů

Vychází se ze struktury sítě (Obrázek 12) a pojmenují se distribuční přepínače (modré) jako *paterni switch 1-4* a přístupové přepínače (šedé) jako *ucebnovy switch 1-43*.

5.9.1 Vytvoření šablony

Pro vylepšení grafu s odezvou ping se z webu *http://docs.cacti.net/templates* stáhne *graph template advanced_ping_alt*. Ten se rozbalí na disku ze zipu. V Cacti v *Console* se klikne na odkaz *Import Templates*. V prvním řádku se klikne na procházet a najde se

z rozbalených souborů (ze stáhnutého zip archivu) xml soubor. Po-té se volba potvrdí tlačítkem *Import*.

Pro usnadnění přidávání zařízení se vytvoří dvě šablony. Klikne se *Host Templates* a *Add*. Zadá se název *Cisco router paterni*, kterému se přidá v *Associated Graph Templates*: *Cisco – CPU Usage* a *PING – Advanced Ping ALT*. Ve *Associated Data Queries* se přidá *SNMP – Interface Statistics*.

Druhá šablony *Cisco router ucebnovy* nebude akorát obsahovat v *Associated Graph Templates*: *Cisco – CPU Usage*.

5.9.2 Samotné přidání zařízení

V *Console/Devices* se klikne na *Add*.

Vyplní se jméno zařízení dle pojmenování ustanovené v bodě 4.2 a IP adresu prvku. Po té se přiřadí vytvořenou šablonou (*Cisco router paterni* či *Cisco router ucebnovy*). Dále se zaškrtne *Monitor Host* (bude se objevovat v záložce Monitor) a *Thold Up/Down Email Notification* se zvolí *Global list*. Zbytek je již předvyplněn z předchozího nastavení Cacti. Volba se potvrdí tlačítkem *Create*.

Obrázek 24: SNMP a Ping informace o páteřním přepínači

Opět se načtou snmp informace ze zařízení (Obrázek 24), jako v prvním případě. Nyní se klikne pouze na **Create Graphs for this Host*. Zakřížkuje se políčko na řádku *Graph Template Name* a tím se zakřížkují všechny přiřazené grafové šablony a potvrdí se tlačítkem *Create*.

Dále se Cacti zeptá na parametry jednotlivých šablon. Pro *PING – Advanced Ping ALT* je to počet pignutí. Jelikož se plánuje monitorovat hodně zařízení, zvolilo se místo původního čísla dvacet raději pět pingů a protokol ICMP. U šablony *Cisco – CPU Usage* se volí pouze barva pro graf. Ponechá se defaultní červená.

Takto jednoduše se přidá a je sledován další aktivní prvek v síti. Stejně se přidaly čtyři páteřní (distribuční) a čtyřicet tři učebnových (přístupových) přepínačů.

5.9.3 Vytvoření šablony pro upozornění

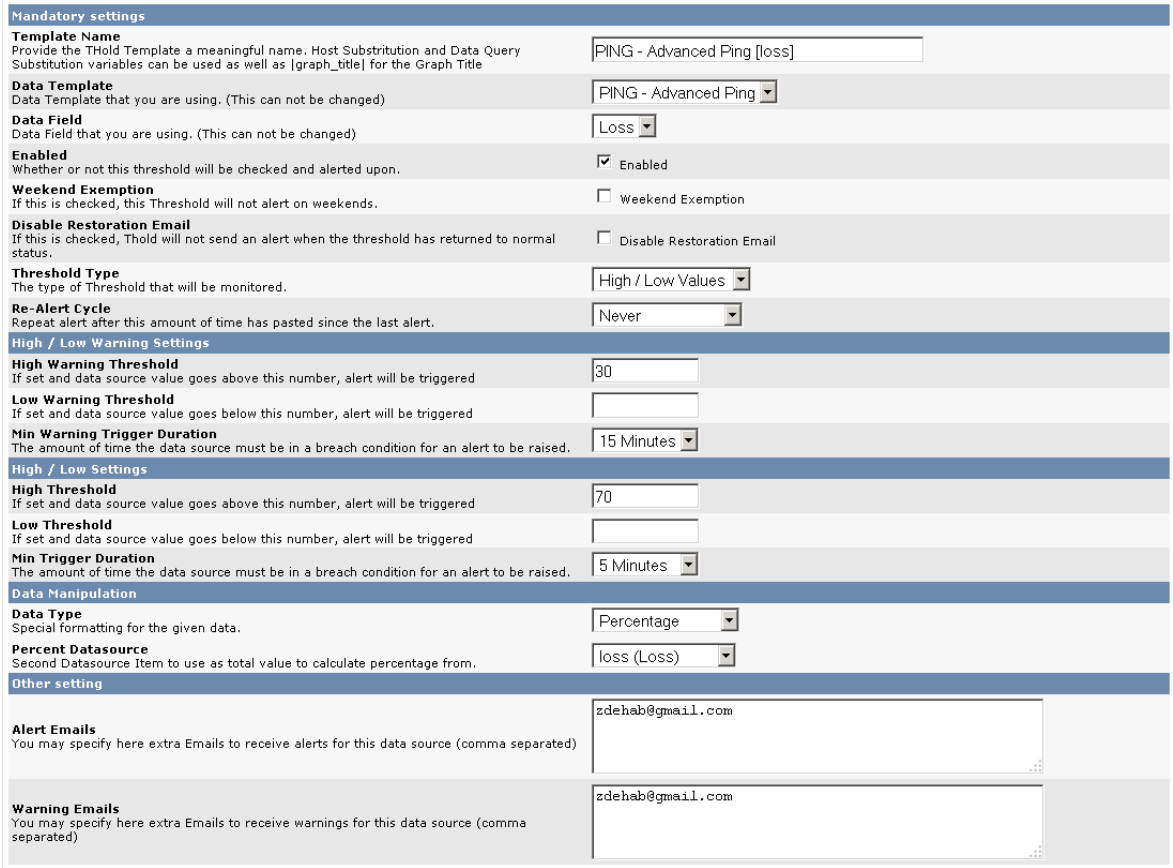
Cacti to označuje jako *Threshold Templates* (plugin Thold). Klikne se tedy na *Console/Threshold Templates* a dále na *Add*.

Zobrazí se *Threshold Template Creation Wizard***.** Zde jako *Data Template* se zvolí *PING – Advanced Ping* a následně *Data Source* se dá *loss (Loss)* a potvrdí se tlačítkem *Create*.

Mandatory settings se ponechají tak jak jsou a upraví se následující prvky: *High Warning Threshold* = 30, *Min Warning Trigger Duration* = 15 minutes, *High Threshold* = 70, *Min Trigger Duration* = 5 minutes, *Data Type* = Percentage, *Percent Datasource* = loss (Loss).

Do *Alert a Warning emails* se doplní všichni, kdo chce být o vzniklé události informován.

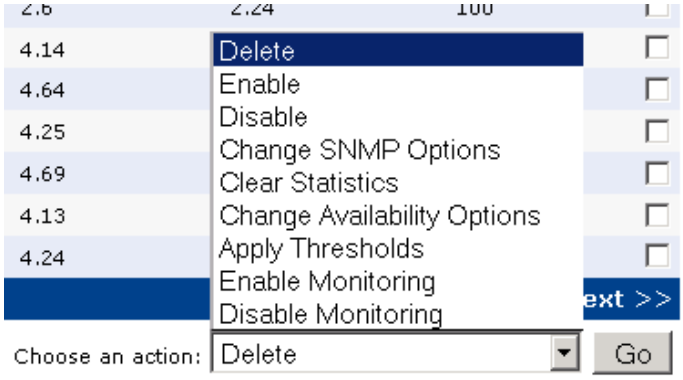
Toto nastavení slouží k zaslání varovného emailu při dvou z pěti (je více než 30%) ztracených ping, a to při trvání třech pětiminutových intervalech. Alarmový email je zaslán při opakovaném překročení 4 ztracených ping (přesáhne 70%).



Obrázek 25: Detail nastavení šablony pro Thold pluginu

5.9.4 Nastavení upozornění

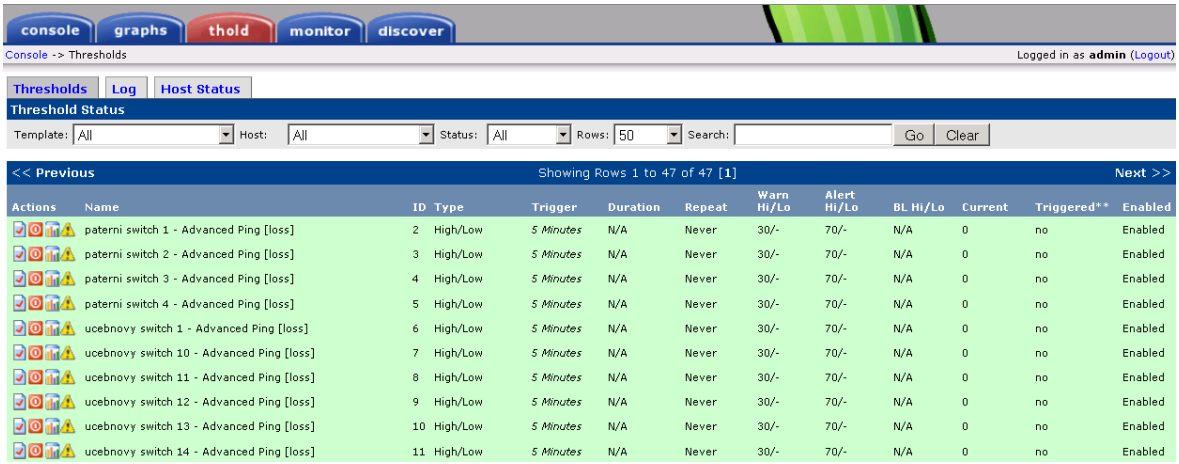
V *Console/Devices* se označí všechna zařízení a vyvolá se nabídka úplně vpravo dole.



Obrázek 26: Nabídka akcí pro označená zařízení

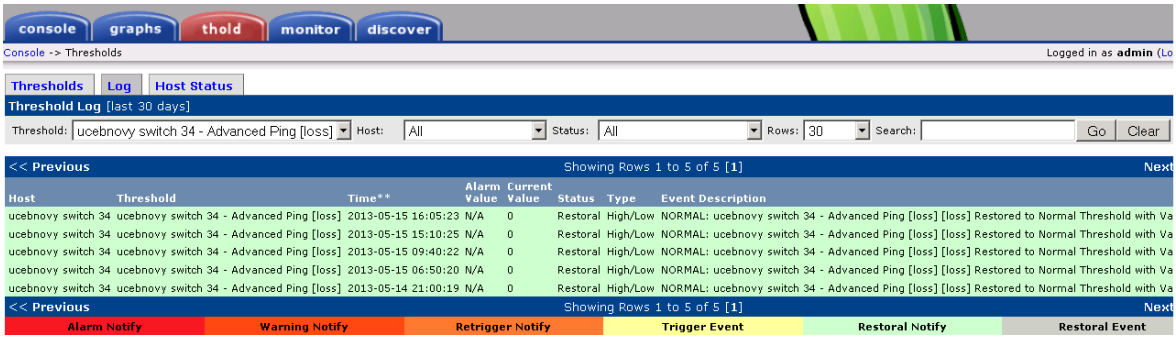
Vybere se *Apply Thresholds* a potvrdí tlačítkem *Go*. Zobrazí se výpis, který obsahuje všechna označená zařízení. Tento seznam se ztvrdí tlačítkem *Continue*.

Jelikož se vytvořila pouze jedna šablona Tholdu, přiřadí se automaticky. Zkontrolovat, editovat, vypínat a zapínat se dělá vše přehledně v záložce Tholdu.



Obrázek 27: Přehled všech nastavený varování v Tholdu

Pro lepší zpětnou dohledatelnost událostí lze vypsat historii ke každému alarmu. Z tohoto výpisu lze vyvodit nejproblematičtější zařízení.

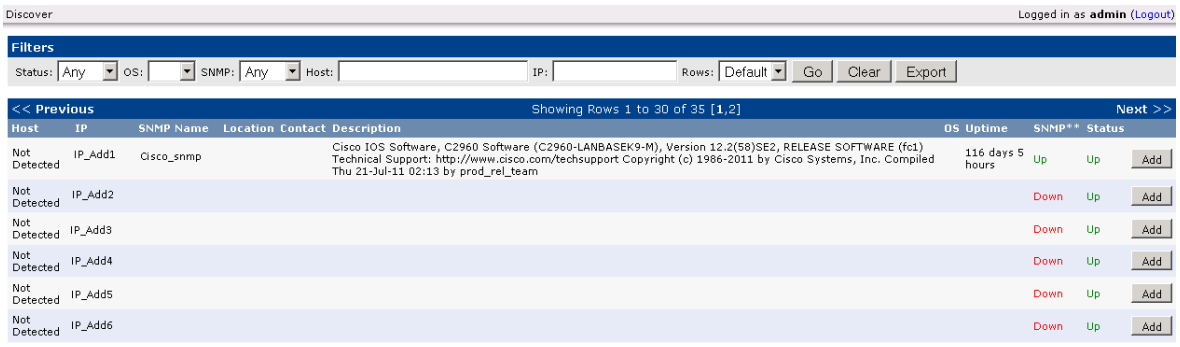


Obrázek 28: Historie alarmů učebnového switche č.34

5.9.5 Plugin Discover

Dle nastavení četnosti se plugin spouští po ukončení polleru. Prohledají se všechny podsítě nakonfigurovány v *Console/Cacti Settings/Misc*. Nalezené zařízení se zobrazí v záložce *Discover*. Zobrazí se i zařízení, které nemají přístupné snmp informace.

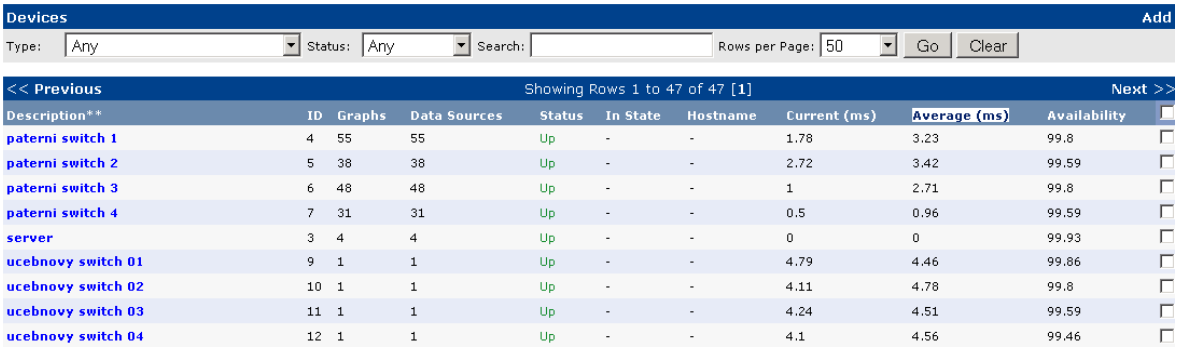
Zařízení se přidá jednoduše kliknutím na tlačítko *Add*. Dále se pokračuje jako v klasickém přidání nového zařízení.



Obrázek 29: Nalezená zařízení pluginem Discover

6 VÝSLEDKY MONITOROVÁNÍ

Mezi funkce dohledového systému patří statistika dostupnosti prvků. Jsou to přehledná a jasně hovořící data. Úvodní celkové statistiky dostupnosti (*Availability*) a průměrného pingu (*Average*) se tvoří automaticky v *Console/Devices*.



Devices Add

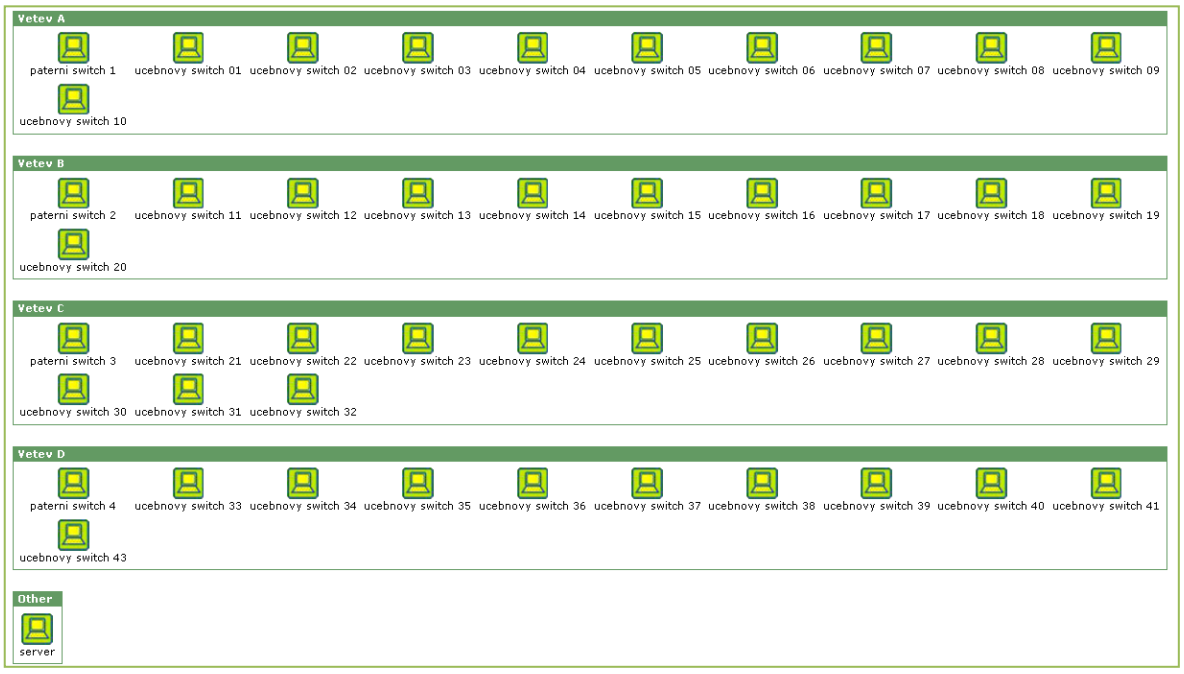
Type: Any Status: Any Search: Rows per Page: 50 Go Clear

<< Previous Showing Rows 1 to 47 of 47 [1] Next >>

Description**	ID	Graphs	Data Sources	Status	In State	Hostname	Current (ms)	Average (ms)	Availability
paterni switch 1	4	55	55	Up	-	-	1.78	3.23	99.8
paterni switch 2	5	38	38	Up	-	-	2.72	3.42	99.59
paterni switch 3	6	48	48	Up	-	-	1	2.71	99.8
paterni switch 4	7	31	31	Up	-	-	0.5	0.96	99.59
server	3	4	4	Up	-	-	0	0	99.93
ucebnovy switch 01	9	1	1	Up	-	-	4.79	4.46	99.86
ucebnovy switch 02	10	1	1	Up	-	-	4.11	4.78	99.8
ucebnovy switch 03	11	1	1	Up	-	-	4.24	4.51	99.59
ucebnovy switch 04	12	1	1	Up	-	-	4.1	4.56	99.46

Obrázek 30: Základní přehled a statistiky zařízení

Pro lepší přehled se zařízení uspořádala do stromu dle fyzické struktury (Obrázek 12). Přehledné strukturované zobrazení se nachází v záložce *Monitor*. Při najetí kurzoru na prvek se zobrazí jeho základní statistika.



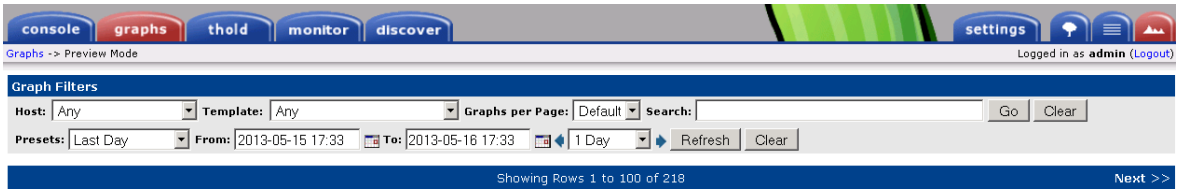
Obrázek 31:Stromové zobrazení v pluginu Monitor

6.1 Grafy

Grafy se v Cacti dají vytvořit prakticky na cokoliv. Sledovala ping dostupnost serveru, všech distribučních a přístupových přepínačů. U serveru se navíc sledovalo vytížení

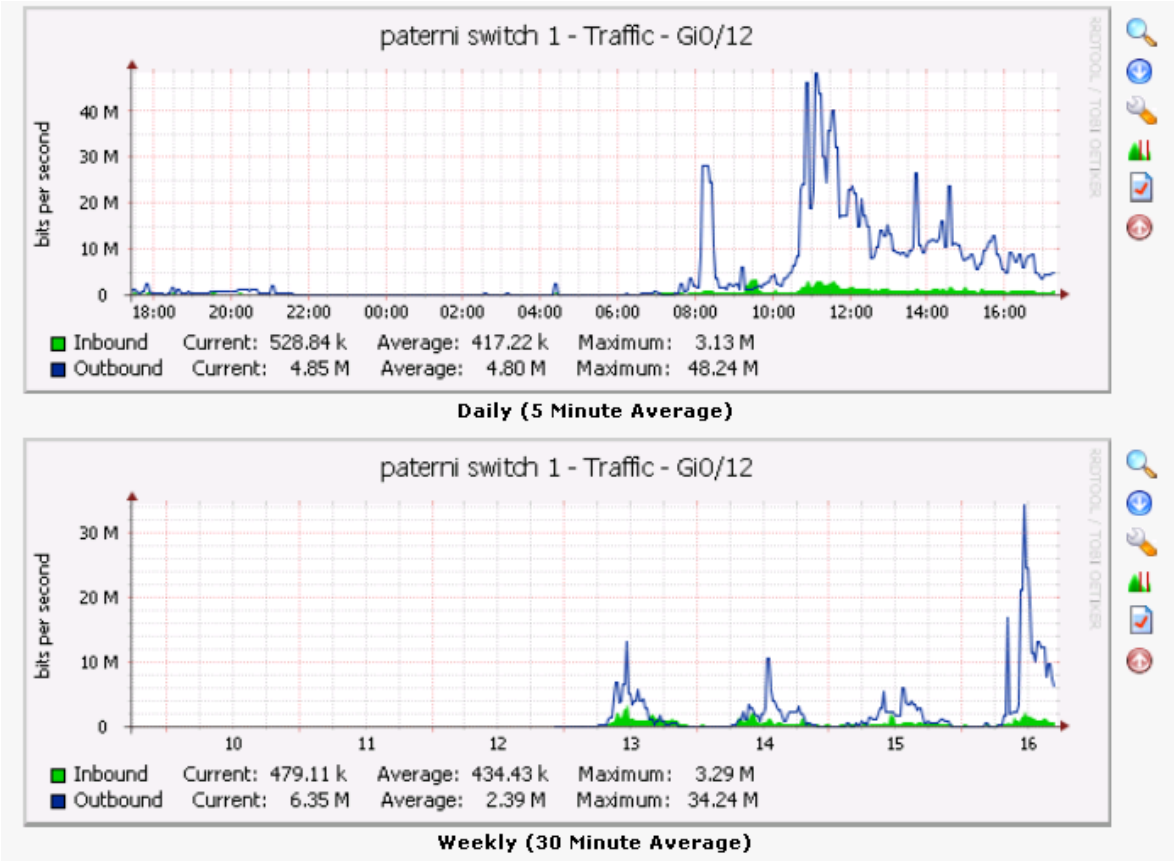
procesorů. U distribučních (páteřních) přepínačů se sledovalo ještě vytížení CPU a datové přenosy jednotlivých portů. Několikrát se ocenila funkce zoom, dostupná u každého grafu.

Při sledování více parametrů u mnoho zařízení se vytvoří spousta grafů. Hledání toho pravého grafu bez filtrace je nemyslitelné. Cacti má velice propracované navádění na grafy. Může se filtrovat dle hosta, šablony nebo vyhledávat graf přímo. Dá se nastavit přesné časové rozmezí, které nás zajímá.

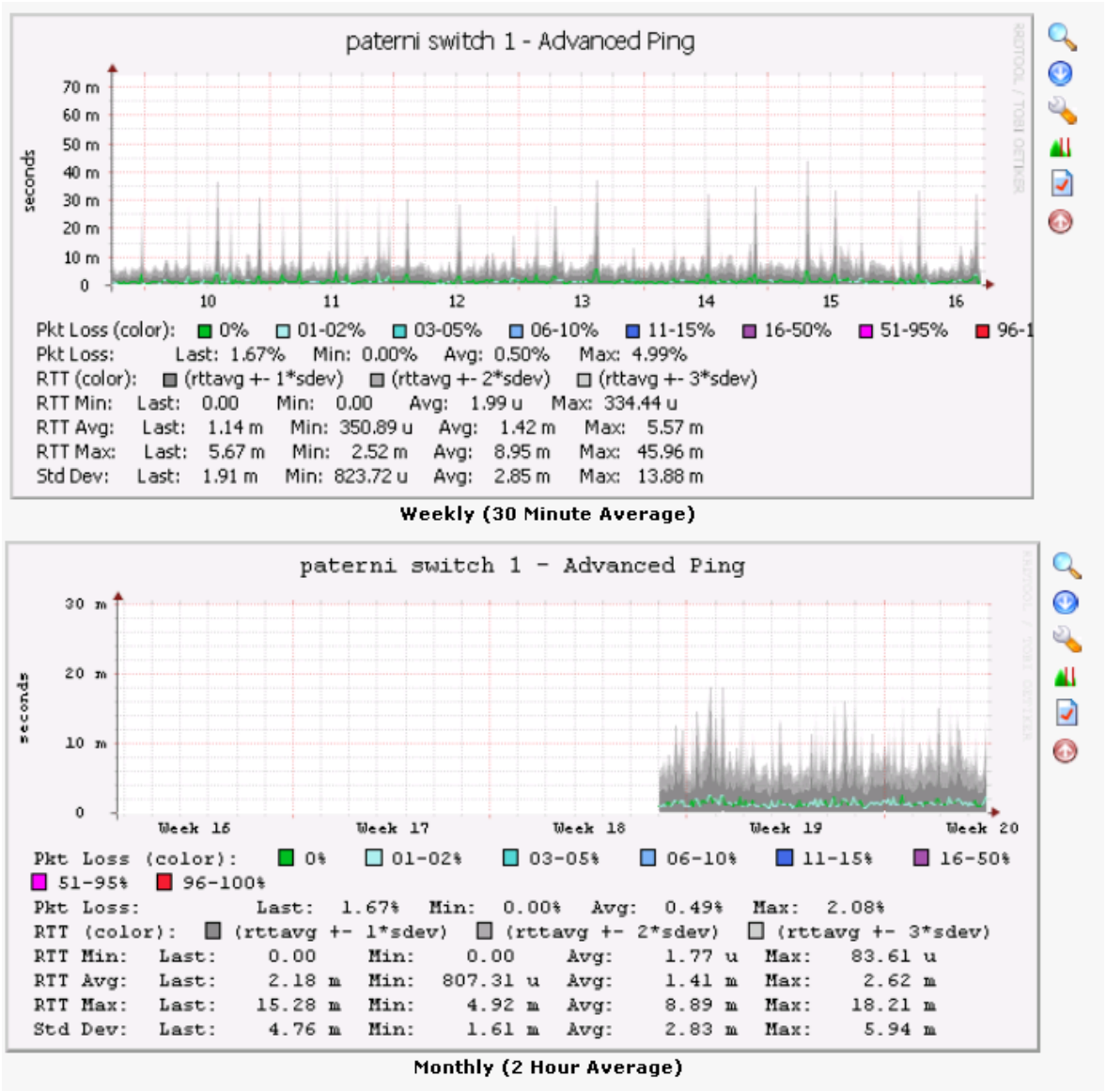


Obrázek 32: Filtrační a časové možnosti u grafů v Cacti

Po kliknutí na zobrazený graf se přesměruje na základní nastavení grafu a zobrazí se 4 grafy s předdefinovanými časovými úseky (den, týden, měsíc a rok). Dva z nich jsou na Obrázek 33 a Obrázek 34.

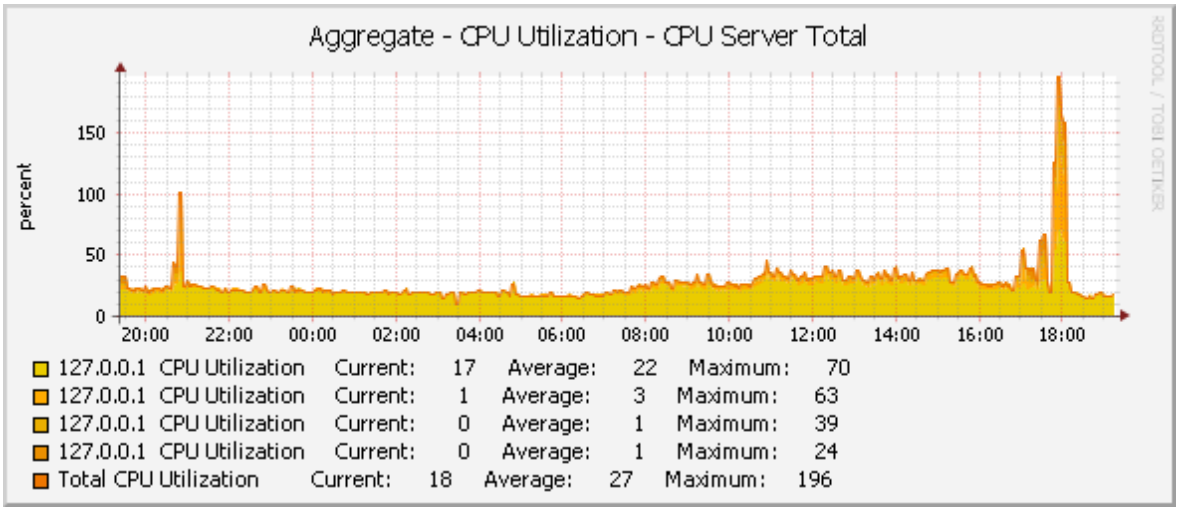


Obrázek 33: Grafy přenosu dat v čase na 12.portu páteřního přepínače č.1



Obrázek 34:Grafy a statistiky pingu páteřního switche č.1

Na sledování vytížení procesoru serveru se využil plugin *Aggregate*, tudíž se ze čtyř udělal jeden graf.



Obrázek 35: Plugin Aggregate a celkové využití procesorů serveru

6.1.1 Graph Management a Graph Trees

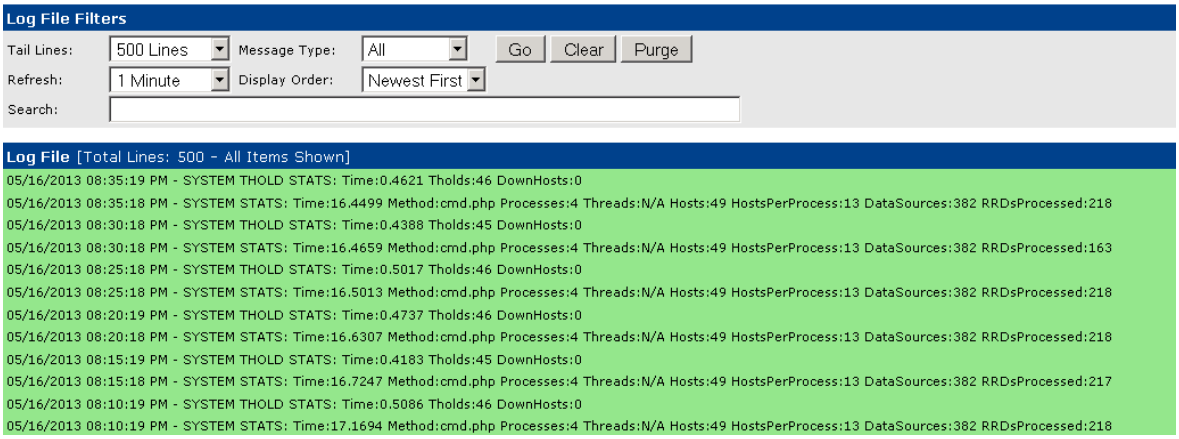
Graph Management slouží pro správu všech grafů, které se v Cacti vytvoří. Tyto grafy lze mazat nebo editovat. Dále je zde možnost vybrané grafy spojovat díky pluginu *Aggregate*. Vytvořit grafy bez šablony pro jakékoliv přidané zařízení. Klikne se pouze na tlačítko *Add* a zvolí se, co zobrazíme.

V *Graph Trees* se zařízení uspořádají do stromové struktury. V případě většího počtu zařízení to zpřehlední připojení či návaznosti zařízení.

Obrázek 36: Část stromového uspořádání prvků v Graph Trees

6.2 Vytížení serveru

Velice užitečné informace se nalézají v Cacti logu (*Console/Utilities/View Cacti Log File*). Zde se vypisují podle nastavené úrovně hlášky programu. Spolu se správcem úloh lze určit výsledné zatížení serveru dohledovým systémem.



Obrázek 37:Výpis Cacti logu

Správce úloh při běhu polleru ukazuje vytížení 100% všech čtyřech jádrech. Čas běhu polleru je okolo 16,5 sekundy při 382 parametrech. To při pěti minutovém intervalu je

$$vytíženost = \frac{t_{procesu}}{t_{periody}} \times 100 = \frac{16{,}5}{300} \times 100 = 5{,}5\%$$

Což znamená, že tato konfigurace by byla schopná zvládnout přes 6000 parametrů. To je hodně vysoké číslo a pokrylo by celou síť UTB (6 fakult + knihovna).

Odesílané emailové upozornění mělo na vytížení serveru nepodstatný vliv.

ZÁVĚR

Dohledový systém má primární úkol monitorovat stavy zařízení a sítě. Tyto stavy se musí zaznamenávat a upozornit v nestandardních situacích. Dnešní dohledové systémy umí komunikovat od tiskáren přes přepínače až po servery. Monitorování nekončí jen u samotných zařízení, ale můžou se sledovat jejich služby či procesory. Prakticky se monitorovat dá cokoliv.

Celá řada systémů je dostupná na různé druhy operačních systémů. Velké rozdíly jsou nejen v jejich ceně ale v provedení. Samotnou skupinou jsou profesionální řešení od velkých korporací IBM atd. Tato řešení jsou spojené spíše s lepšími službami (školení, podpora) a programovým provedením. Jsou ale vykoupeny podstatně vyšší cenou.

Nenarazil jsem na ani jeden produkt, který by neuměl komunikovat standardními protokoly SNMP nebo ICMP. Tyto protokoly jsou brány jako základní kámen každého dohledového systému.

Pro monitorování se zvolila univerzitní síť Fakulty aplikované informatiky. Jedná se vysokorychlostní počítačovou síť tvořenou čtyřmi distribučními a čtyřiceti třemi přístupovými přepínači. Všechny jsou od špičkového výrobce Cisco.

Jako aplikovaný dohledový systém se vybralo Cacti. Open source systém, který jako jediný byl možný provozovat na Windows. To bylo velice důležité při výběru, neboť byl k dispozici Windows Server 2008 R2. Mezi další plus tohoto systému patří velké monitorovací možnosti, široká škála šablon a velká aktivní komunita. Rozšiřitelnost sytému je také nezanedbatelná, neboť pluginy se mohou volně upravovat či vytvářet nové.

Na „svobodný“ systém je velmi přehledný a pohodlný. Tvoří velice pěkné grafy, se kterými se dobře pracuje. Ocení se například spojení několika grafů do jednoho, funkce zoom grafů nebo nespočet šablon. Dále se nastavilo emailové upozorňování na výpadky zařízení a vyhledávání nových zařízení v podsíti.

S nulovými náklady se povedlo aplikovat dohledový systém na část univerzitní sítě. Věřím, že by systém mohl plnit svoji funkci s minimální správou a to velice dobře. Možnosti pro rozšíření dohledu jsou také veliké. Své uplatnění by mohl najít i v několika předmětech vyučovaných na UTB.

ZÁVĚR V ANGLIČTINĚ

The monitoring system has the primary task of monitoring the device status and network. These conditions shall be recorded and noted in defined situations. Today's monitoring systems can communicate with the printer through the switch to servers. It cannot be monitor only device itself, but can be watch their services or processors. It can be monitored more that things.

Numerous systems are available in different kinds of operating systems. Large differences not exist only in their cost but also in performance. Alone group are professional solutions from large corporations like IBM, etc. These solutions are rather associated with better services (training, support) and program itself. But they are redeemed substantially higher price.

I have not find even one product that cannot communicate by standard SNMP or ICMP. These protocols are considered as the cornerstone of any monitoring system.

Space for monitoring was chosen computer network of the Faculty of Applied Informatics. There is a high-speed computer network consisting of four distribution switches and forty three access switches. All of them are from top producer of Cisco.

There was applied monitoring system Cacti. Only this open source system was possible to run at Windows. It was very important in the selection because there is available Windows Server 2008 R2 for this thesis. The other pluses of this system are lot of monitoring templates, a wide range of templates and a huge activities of community. Scalability of the system is not also negligible, because plugins are able to modify or create new ones.

On the "open source" system is very easy and comfortable. It forms a very nice graphs which works very well. For example it can be praised aggregate of graphs, the possibility of zooming graphs or countless templates. Furthermore, has set an email notification system of downtimes. Also was done settings for searching of new devices on the subnet.

It was successfully applied the monitoring system of the university network without investment. I believe that the system could perform its function with minimal administration and it very well. Options for extending of monitoring are also very possible. Its application could also be found in several subjects taught at UTB in Zlín.

CITOVANÁ LITERATURA

Caligare. 2011. www.caligare.com. *Netflow Definition.* [Online] Caligare, 2011. [Citace: 11. květen 2013.] http://www.caligare.com/netflow/netflow.php.

Antonín Kolísek. 2013. linuxsoft.cz. *Dohledový systém Zabbix.* [Online] linuxsoft.cz, 11. únor 2013. [Citace: 2013. květen 2013.] http://www.linuxsoft.cz/article.php?id_article=1963. ISSN 1801-3805.

Bouška, Samuraj - Petr. 2009. Začínáme s monitoringem sítě. *samuraj-cz.com.* [Online] samuraj-cz.com, 1. září 2009. [Citace: 13. květen 2013.] http://www.samuraj-cz.com/clanek/zaciname-s-monitoringem-site/.

—. 2009. Zařízení v síti pod kontrolou. *samuraj-cz.com.* [Online] samuraj-cz.com, 21. září 2009. [Citace: 13. květen 2013.] http://www.samuraj-cz.com/clanek/zarizeni-v-siti-pod-kontrolou/.

IANA. 2013. *IANA - Internet Assigned Numbers Authority.* [Online] IANA - Protocol Registries, 2013. [Citace: 7. duben 2013.] http://www.iana.org/protocols.

IBM. 2013. Tivoli Netcool Software for Service Providers. *IBM.com.* [Online] IBM.com, 2013. [Citace: 1. květen 2013.] http://www-01.ibm.com/software/tivoli/solutions/service-provider/.

INVEA-TECH a.s. 2013. Monitorování v reálném čase. *invea.cz.* [Online] INVEA-TECH a.s., 2013. [Citace: 13. květen 2013.] http://www.invea.cz/sitova-reseni/monitorovani-v-realnem-case.

—. 2013. NetFlow/IPFIX. *invea.cz.* [Online] INVEA-TECH a.s., 2013. [Citace: 12. květen 2013.] http://www.invea.cz/sitova-reseni/netflow/ipfix.

Macek, Petr. 2009. Cacti: vše důležité v jednom monitoru. *root.cz.* [Online] root.cz, 31. březen 2009. [Citace: 12. duben 2013.] http://www.root.cz/clanky/cacti-vse-dulezite-v-jednom-monitoru/. ISSN 1212-8309.

Oetiker, Tobias. 2009. RRDtool - About RRDtool. *RRDtool.* [Online] OETIKER+PARTNER AG, 2009. [Citace: 14. duben 2013.] http://oss.oetiker.ch/rrdtool/.

ORTEX spol. s r.o. 2010. NAGIOS - MONITOROVACÍ A DOHLEDOVÝ SYSTÉM. *http://web.ortex.cz/.* [Online] ORTEX spol. s r.o, 2010. [Citace: 14. květen 2013.] http://web.ortex.cz/sluzby/nagios.aspx.

Peterka, Jiří. 2011. IP - Internet Protocol. *archiv článků a přednášek Jiřího Peterky.* [Online] 2011. [Citace: 19. květen 2013.] http://www.earchiv.cz/anovinky/ai1843.php3.

Polzer, Jan. 2010. maxiorel.cz. *pc monitor sledujte stav pocitace z ipadu iphone nebo androida.* [Online] Maxiorel.cz, 14. prosinec 2010. [Citace: 13. květen 2013.] http://www.maxiorel.cz/pc-monitor-sledujte-stav-pocitace-z-ipadu-iphone-nebo-androida. ISSN 1802-470X.

Sosinsky, Barrie. 2010. *Mistrovství - počítačové sítě.* Brno : Computer Press, a.s., 2010.

The Cacti Group, Inc. 2004-2012. Cacti® - the complete rrdtool-based graphing solution. *Cacti®.* [Online] The Cacti Group, Inc., 2004-2012. [Citace: 14. duben 2013.] http://www.cacti.net.

Ubik, Sven. 2006. Trendy v monitorování vysokorychlostních pocítacových sítí. *Sdělovací Technika.* [Online] CESNET, z.s.p.o., 2006. [Citace: 21. březen 2013.] http://www.ist-lobster.org/publications/articles/sdel_tech.pdf. ISSN 0036-9942.

ZABBIX SIA. 2001 - 2013. Zabbix - The Enterprise-class Monitoring Solution for Everyone. *Homepage of Zabbix* . [Online] ZABBIX SIA, 2001 - 2013. [Citace: 12. květen 2013.] http://www.zabbix.com.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AIX	Advanced Interactive eXecutive
API	Application Programming Interface
atd.	a tak dále
CAM	Content Addressable Memory
CIM	Common Information Model
CPU	Central Processor Unit
CSV	Comma-separated values
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
ftp	File Transport Protocol
FUP	Fair Use Policy
HP-UX	Hewlett-Packard UniX
http	HyperText Transfer Protocol
IANA	Internet Assigned Numbers Authority
IETF	Internet Engineering Task Force
IP	Internet Protokol
IPFIX	Internet Protocol Flow Information Export
IPMI	Intelligent Platform Management Interface
IT	Informační technologie
JMX	Java Management Extensions
LAN	Local Area Network
MIB	management information base
MRTG	Multi Router Traffic Grapher
NBA	Network Behavior Analysis
NDP	Neighbor Discovery Protocol

OID	Object Identifier
OS	operační systém
PAPI	Performance Application Programming Interface
PC	Personal computer
PDU	Protocol Data Unit
PHP	Hypertext Preprocessor (původně Personal Home Page)
ping	Packet InterNet Groper
PLC	Programmable Logic Controller
QoS	Quality of Service
RFC	Request for Comments
RIP	Routing Information Protocol
RRDTool	Round-robin database tool
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
TTL	Time To Live
tzn	tak zvaně
UDP	User Datagram Protocol
VoIP	Voice over Internet Protocol
WDM	Windows Driver Model
WMI	Windows Management Instrumentation

SEZNAM OBRÁZKŮ

SEZNAM TABULEK