Vysoká škola ekonomická v Praze
Fakulta informatiky a statistiky
Vyšší odborná škola informačních služeb v Praze

ZDENĚK ČEJKA

Monitoring serverů s operačním systémem FreeBSD, jeho aplikací a služeb

BAKALÁŘSKÁ PRÁCE

2007

Zadávací list

PROHLÁŠENÍ

Prohlašuji, že jsem bakalářskou práci na téma Monitoring serverů s operačním systémem FreeBSD a jeho aplikací a služeb zpracoval samostatně a použil pouze zdrojů, které cituji a uvádím v seznamu použité literatury.

V Praze dne 26. srpna 2007

_ _ _ _ _ _ _ _ _ _ _ _ _ _

Zdeněk Čejka

PODĚKOVÁNÍ

Děkuji tímto paní Mgr. Ladě Vronkové za odborné vedení a rady při zpracování bakalářské práce, za metodickou pomoc, konzultace a připomínky, které mi poskytla.

OBSAH

ANOTACE

V této práci na téma Monitoring serverů s operačním systémem FreeBSD, jeho aplikací a služeb bude provedo nastavení služeb Apache, MySQL, Courier-IMAP, Postfix a ProFTPd a jejich monitoring. Sledovábу budou také čísti systému nezbytné k jeho chodu.

Práce je rozdělěna do dvou částí: nastavení monitorovaných služeb a aplikací a samotného monitoringu.

Nastavení služeb je členěno do kapitol. Každé službě je věnována jedna. V těchto kapitolách je zahrnuto jak nastavení službeb, tak jejich popis a funkce.

Část věnovaná monitoringu přináší informace o výstupních datech. Posuzován bude význam výstupů a jejich správné čtení. V této části budou uvedeny případné chyby ve výstupech a jejich řešení. Dále zde bude prezentována interpretace výstupů s ohledem na její různé formy.

KLÍČOVÁ SLOVA

FreeBSD, monitoring, periodic, MySQL, SSH, Postfix, Apache, Courier-IMAP, MRTG, UNIX, cron

1 ÚVOD

Počítače se staly součástí života moderní společnosti. Prakticky každá myslitelná věc v oblasti techniky je řízena počítačem nebo alespoň mikroprocesorem. Internet se jako médium zapsal do podvědomí všech počítačově gramotných lidí i velké části negramotných. Nepřeberné množství informací, které poskytuje, je vykoupeno velkým množstvím útoků jak na osobní počítače, tak servery a rozmanitost těchto forem nezná hranic.

Vyhledávání na internetu, prezentování firem, inzerce a mnoho dalších je bráno s jakousi samozřejmostí. Na provoz těchto služeb jsou kladeny nároky jak softwarového, tak hardwarového charakteru. Záleží pouze na klientovi, pro jak náročné řešení se rozhodne.

Každý systém má své výhody a nevýhody. Většina operčních systémů je založena nebo spíše odvozena od systému UNIX. Je jich však nepřeberné množství a každá vývojová větev je zaměřena na konkrétní problém. Některé se orientují na maximální přenositelnost, další na bezpečnost a jiné zase na flexibilitu a uživatelský komfort. Ale i zde platí pravidlo, že když je jedna věc oblíbená a uživatelsky přínosná v jednom systému, je okamžitě začleněna do ostatních. Při tom je ale nutno dbát na licenční politiku určitého systému a řídit se jejím ustanovením.

Cílem mé práce je nastavení služeb a aplikací na serverech s operačním systémem FreeBSD a monitoring jeho služeb a procesů. Popisována bude jak konfigurace jednotlivých služeb, která je převážně individuální, tak celková kontrola logů a správná funkčnost. Budu se snažit zjistit, zda výstupy zasílané emailem a poskytované grafickým nástrojem MRTG opravdu poskytují veškeré potřebné informace o stavu systému. Pokud je nebudou poskytovat v plně očekávané míře, bude nutné stanovit možnost nápravy.

První část se věnuje stručné historii tohoto operačního systému. Každý operační systém má svůj vývoj. Může se štěpit do různých větví a částečně přebírá klady i zápory svého „rodiče“. Z historie se dají také odvodit příkazy a syntaxe používané v konzoli.

Další kapitola bude zahrnovat nastavení a popis služeb, které mají být monitorovány. Správná konfigurace je velice důležitá a zajišťuje funkčnost systému. Budu se věnovat pouze stěžejní části těchto nastavení a kompletní výpis příslušných

konfiguračních souborů bude uveden v přílohách. Do své práce záměrně zahrnuji pouze ty konfigurační soubory, které se vztahují k monitoringu a správě aplikací a služeb, ostatní jsou vynechány.

V kapitole zaměřené na samotný monitoring bude popisován a vysvětlován význam emailových zpráv zasílaných správci systému. Využívají se jak služby poskytované samotným systémem, tak skripty, které do systému začleněny nejsou a musely být napsány separátně. U každého výstupu budou popisovány vlastnosti a význam řádků nebo pouze celkový význam výstupu. V případě grafického vykreslování pomocí Multi Router Traffic Grapher budou údaje zkoumány v delším časovém úseku.

V závěru bych rád zhodnotil kvality výstupů s ohledem na poskytované informace, jejich přehlednost, srozumitelnost a dostatečnost. Shrnu případné chyby a nedostatky jednotlivých typů monitoringu a jejich vzájemné koexistence.

2 HISTORIE

Jako nejoblíbenější a nejznámější z rodiny BSD-like operačních systémů je FreeBSD. Tento systém má řadu výhod. Pružnost a univerzálnost je jeho obrovským kladem. Jako jeden z mála UNIXových systémů obsahuje i Linuxové API, takže lze, i když s určitým omezením, spouštět aplikace psané pro Linux. Další hodnotnou devizou tohoto systému je velice propracovaný systém portů (ports). Jelikož FreeBSD je systém, který se instaluje/kompiluje ze zdrojových kódů, je většina aplikací zanesena do ports a z toho se potom kompilují s nastavením optimálním pro tento systém. Je zde možné si případná nastavení upravit podle svého přání.

Operační systém FreeBSD vychází ze systému UNIX. Jeho vývoj byl velice zajímavý. V době, kdy nebyl jednotný operační systém, měl každý počítač svůj vlastní, často vzájemně nekompatibilní. Některá data bylo nutné zadávat znovu. S nárůstem počtu uživatelů, kteří si chtěli nechat zpracovat data na počítači, se zvyšovali i nároky na systém.

Firmy AT&T, MIT a General Electric přednesly své požadavky na nový operační systém a v roce 1965 v Bell Labs byl založen projekt s názvem Multiplexed Information and Computing Service (Multics).

Multics byl sice schopen práce, ale nedělal to, pro co byl vyvíjen - například podporu více uživatelů. Dalším problémem bylo, že každá s podílejících se stran měla trošku jinou představu o konečném produktu. Ke všemu ještě přispěl pocit Bell Labs, že Multics by byl drahý, a tak byl projekt v roce 1969 zastaven.[1]

Dalším mezníkem ve vývoji Unixu byla paradoxně počítačová hra. Programátorem byl Ken Thompson, zaměstnanec Bell Labs, a nesla název Space Travel. Původní verze byla napsána pro systém Multics. Po určité době ji však Ken Thompson přepsal pro počítač GE 632 se systémem GECOS.[2]

---

[1] ŽÁK, Karel. *Historie OS UNIX* [online]. c2001, poslední revize 28. 6. 2001 [cit. 2007-05-20]. <http://www.root.cz/clanky/historie-os-unix/>.

[2] ŽÁK, Karel. *Historie OS UNIX* [online]. c2001, poslední revize 28. 6. 2001 [cit. 2007-05-20]. <http://www.root.cz/clanky/historie-os-unix/>.

GE 632 byl však velice velký a drahý, proto se spolu s Dennisem Ritchiem snažili najít menší a levnější variantu. Jejich představu splňoval DEC PDP-7. Mezi jeho hlavní výhody patřil subsystém pro ladění aplikací (debut subsystem), podpora operací s plovoucí čárkou a také daleko lepší terminál, než ten, který nabízel GE 632.

Po hře následovalo v létě roku 1969 napsání filesystému, který implementoval Thompson. Dalším krokem bylo naprogramování základních utilit pro kopírování, mazání a přemisťování editovaných souborů, a hlavně základního interpretoru příkazů. Vše bylo stále tvořeno pro GECOS a transformováno na PDP-7, což však nemělo dlouhého trvání a po čase se tento nový systém osamostatnil. Brian Kernighan proto navrhl dát systému jméno, a to znělo Unix (slovní hříčka na Multics). [3]

Pro UNIX bylo typické, že jádro systému nebyl obsažen shell. Veškeré takovéto programy se osamostatnily.

Společnost Bell Labs v Unixu viděla životaschopný projekt a v roce 1970 byl stávající počítač DEC PDP-7 již zastaralý, tak se rozhodli se zakoupit novější DEC PDP-11.

Pro vývoj Unixu mluvil také fakt, že měl být využíván uvnitř organizace. Byl tedy nasazen v patentovém oddělení Bellových laboratoří.

První oficiální prezentace Unixu proběhla 15. - 17. října 1973 na "The Symposium on Operating Systems Principles, IBM Thomas J. Watson Research Center, Yorktown Heights, New York". [4]

V roce 1976 se UNIX dostal i na univerzitu Berkley v Kalifornii. Tato větev se pojmenovala BSD. Systém dostal řadu vylepšení, jako byl například tisk, quoty a asi nejznámější je editor vi. Systém se upravoval, ale pořád v jeho kódu byly věci, které podléhaly licenci a nebyly volně šiřitelné. To vyústilo ve verzi 386BSD, která byla kompletně přepsána pro architekturu x86 a tím se zbavila všech částí, které podléhaly komerční licenci.

---

[3] ŽÁK, Karel. *Historie OS UNIX* [online]. c2001, poslední revize 28. 6. 2001 [cit. 2007-05-20]. <http://www.root.cz/clanky/historie-os-unix/>.

[4] ŽÁK, Karel. *Historie OS UNIX* [online]. c2001, poslední revize 28. 6. 2001 [cit. 2007-05-20]. <http://www.root.cz/clanky/historie-os-unix/>.

Projekt FreeBSD začal v roce 1993 jako soubor neoficiálních patchů pro 386BSD. Stáli za tím Nate Williams, Rod Grimas a Jordan Hubbard.[5]

Verze 1.0 vyšla v prosinci roku 1993. Byla založena na 4.3BSD-Lite („Net/2“). Některé součásti byly převzaty z 386BSD a Free Software Foundation. [6]

Zatím současná verze je 6.1, která vyšla v květnu roku 2006. Ta obsahuje několik zásadních změn v kernelu, zlepšení hardwarové podpory a nové síťové prvky.

FreeBSD je také portován na různé počítačové architektury, jako jsou například 64-bitové procesory od AMD (x86_64) a Intelu (IA-64), Digital Alpha/AXP nebo Sun UltraSPARC.

Jak z předchůdců FreeBSD, tak z něho samého, se postupem času začaly vyvíjet další systémy. Minimalistickou distribucí je například m0n0wall, která slouží primárně jako router či firewall. Pro desktopové řešení je zde PC-BSD a DesktopBSD. Obě tyto distribuce se zaměřují na co možná nejlepší uživatelský komfort a maximální nahrazení operačního systému Microsoft Windows. Live distribuce založené na FreeBSD nesou název FreeSBIE a Frenzy live CD.

Dalším operačním systémem založeným na FreeBSD je Mac OS X od firmy Apple. Ten je ale plně upraven na míru hardwaru používaném na jejich strojích.

Od FreeBSD se také oddělili vývojáři, kteří nesouhlasili se strategií multiprocesorové synchronizace použité ve verzi 5 a založili projekt s názvem DargonflyBSD. Posledním společným dílem byla verze 4.8, na které je DargonflyBSD postaven.

---

[5] HUBBARD, Jordan. *A Brief History of FreeBSD, FreeBSD Handbook* [online]. Last revision 14.5.2007 [cit. 2007-05-20]. < http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/history.html>.

[6] HUBBARD, Jordan. *A Brief History of FreeBSD, FreeBSD Handbook* [online]. Last revision 14.5.2007 [cit. 2007-05-20]. < http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/history.html>.

3 ZÁKLADNÍ/ÚVODNÍ NASTAVENÍ

Všechny servery byly v počátku holé, tj. bez operačního systému. K instalaci bylo použito CD se systémem FreeBSD NET install. Veškerý základní software, nutný k plnohodnotnému běhu systému na zvoleném stroji, byl natažen z mirrorů/zrcadel v průběhu instalace.

Základní nastavení serveru probíhá v serverovně. Zahrnuje především nastavení SSH deamona pro vzdálenou správu, firewallu a lokální konfigurace v podobě hostname, IP adres a aktualizace portů (ports). V této fázi je též možno nakonfigurovat jádro systému (kernel) a optimalizovat ho pro konkrétní stroj a jeho hardware. Není to ale nezbytné, jelikož GENERIC neboli výchozí jádro v sobě obsahuje podporu veškerých standardních ovladačů. Kompilaci jádra lze provést i následovně, ale v případě neúspěchu bude následovat cesta do serverovny.

Dodatečné instalace a nastavení konkrétních služeb probíhá přes SSH připojení. Používá se k tomu buď klasický SSH terminál, program zvaný PuTTy nebo jiné obdobně fungující aplikace. To je odvozeno od systému, ze kterého probíhá přihlašování.

Pro samotný monitoring jsou důležité takzvané logy. Jsou to převážně textové soubory obsahující informace o stavu systému, chováni aplikací a jejich chybových hlášení. Každá aplikace zapisuje data do svého separátního logu. Co všechno má být zaznamenáváno a po jak dlouhou dobu se určuje při konfiguraci aplikace. K těmto informacím by ale neměl mít přístup každý uživatel systému, jelikož mohou obsahovat citlivá data a ty pak lze náležitě zneužít.

Důležitá je také rotace logu. To znamená, že po určité době nebo určitém objemu dat je soubor přejmenován a v některých případech i zabalen, aby se ušetřilo místo na disku. Přejmenovává se zpravidla pomocí koncovek za názvem souboru např. starý http.log se bude jmenovat http.log.0.

3.1 NEJČASTĚJŠÍ ÚTOKY

Monitoring služeb běžících na serveru je důležitou součástí jeho správné funkčnosti. Za předpokladu správné konfigurace, vyvstává otázka nežádoucích útoků a prolomení přístupu u vnější sítě. Jedná se především o DoS (Denial of Service), útok hrubou silou (Brute Force Attack) a slovníkový útok.

3.1.1 DoS (Denial of Service)

Denial of Services jsou útoky snažící se znepřístupnit určitou službu, počítač nebo celou síť. V překladu DoS znamená odmítnutí služby.

Cílem těchto útoků nejsou dostatečně zabezpečené sítě, ale přístupové zdroje. Tím se sítě stávají pro ostatní nedostupné. Pro společnost působící převážně na internetu může způsobit tato blokace vážný problém nebo finanční ztráty. Pokud by tento výpadek byl dlouhodobějšího charakteru, mohl by mít pro společnost katastrofální následky.

Jak uvádí David Budai, cituji: "*DoS útoky je možné rozdělit podle několika parametrů. Jsou v podstatě charakterizovány jako pokusy útočníka znemožnit využívaní služeb napadeného cíle ostatními uživateli, což může zahrnovat:*

- *zahlcení sítě nebo přístupové linky, což znemožní přístup uživatelů k dané službě nebo serveru;*
- *zahlcení serveru takovým množstvím požadavků, že nebude schopen reagovat na požadavky regulérních uživatelů;*
- *zneužití bezpečnostní chyby a následné odstavení serveru."* [*7*]

V případě zahlcení sitě se hovoří o obsazení přenosové kapacity nebo o tzv. záplavových DoS útocích. Je to jednoduchá a velmi účinná metoda. Jejím cílem je vygenerovat tak velký provoz, který zahltí přístupovou linku oběti. Linka tak nebude

---

[7] BUDAI, David. *Nevyzpytatelné a nebezpečné útoky typu DoS* [DigiWeb, online]. 19.07.2007. [cit. 2007-07-30]. <http://digiweb.ihned.cz/c6-10053280-21651030-i00000_d-nevyzpytatelne-a-nebezpecne-utoky-typu-dos>

mít možnost komunikovat s okolím a reagovat na požadavky, protože její kapacita bude vyčerpaná.

Dnešní velké servery jsou však k internetu připojeny velmi rychlými linkami, takže k jejímu zahlcení by musely požadavky zasílat až statisíce počítačů současně. I to je samozřejmě možné, pokud se využije distribuovaný DoS útok (DDoS). Snadnými cíli tady ovšem mohou být malé servery nebo obyčejní uživatelé.

Naštěstí existují určitá opatření, která mohou riziko takového napadení snížit. Správci serverů mají samozřejmě dostupné podrobné informace k jejich zabezpečení. Z těch základních postupů lze jmenovat alespoň tyto:

- *vhodně nastavený firewall*
- *pravidelné záplatování systému*
- *vypnutí nepoužívaných a nepotřebných služeb*
- *použití systému IDS (Intrusion Detection Systém), tedy systému detekce narušení [8]*

3.1.2 Útok hrubou silou a slovníkový útok

Útok hrubou silou je metoda zjištění hesla pomocí velkého počtu kombinací znaků. Útočník zkouší všechny kombinace klíče. Pro příklad uvádím citaci pana Rohledera: "*Uveďme příklad pro heslo s 6 písmeny. Máme 96 tisknutelných znaků. Procesor Pentium 133 zvládne vyzkoušet přibližně 2.400 klíčů za sekundu. Pro vyzkoušení všech možností klíče tedy potřebuje 96^6/1.000=326.149.079 sekund, což je 3.774 dní. Ubráním jednoho písmene zmenšíme čas potřebný k dešifrování 96násobně. Navíc je algoritmus dešifrování snadno paralelizovatelný. Jak je vidět, prohledání celého stavového prostoru pro 6písmenné heslo může trvat na jediném počítači asi 10 let. Ale pro 5písmenné heslo je to pouze 39 dní.*" [9]

---

[8] BUDAI, David. *Nevyzpytatelné a nebezpečné útoky typu DoS* [DigiWeb, online]. 19.07.2007 [cit. 2007-07-30]. <http://digiweb.ihned.cz/c6-10053280-21651030-i00000_d-nevyzpytatelne-a-nebezpecne-utoky-typu-dos>

[9] *Citace: D. Rohleder. Bezpečnost v systémech UNIX. Zpravodaj ÚVT MU. ISSN 1212-0901, 1997, roč. VII, č. 4, s. 14-16.*

Slovníkový útok je modifikací útoku hrubou silou. Tímto postupem se omezí počet prohledávaných klíčů. Slovníkový útok může slavit úspěch tam, kde uživatelé spoléhají na snadno zapamatovatelná hesla, a proto volí běžná slova, případně je doplňují číslicemi. K tomu se používá wordlist (seznam všech běžných slov v daném jazyce) a z něho se zkoušejí všechna slova, případně jejich modifikace, zda se neshodují s hledaným heslem.

Jak nejvhodněji zamezit těmto útokům? Odpověď se přímo nabízí. Dostatečně nastaveným firewallem, vhodnou konfigurací SSH deamona a použitím hesla, které má vice jak 6 znaků a není jednoduché. Je dobré volit heslo, které si můžeme zapamatovat nějakou memotechnickou pomůckou *např. 2Brn2B? (To be or not to be?).* [10]

Dále je dobré promyslet si, jaké služby bude nutné povolit a jak systém uzpůsobit, aby prováděl to, co měl a neponechával otevřená zadní vrátka pro nežádoucí průnik.

3.2 SSH (SECURE SHELL)

SSH je služba, která pomocí šifrovaného přenosu dat umožňuje bezpečnou komunikaci mezi dvěma počítači. Zabezpečení je řešeno převážně pomocí RSA nebo DSA soukromého a veřejného klíče nebo pouze autentifikací stávajícího systému.

V současné době je SSH dostupný ve dvou verzích, SSH-1 a SSH-2. Tyto verze nejsou navzájem kompatibilní a je dobré se při konfiguraci a nastavováni rozhodnout pro jednu z nich. SSH-2 s sebou přináší zvýšení bezpečnosti výměny klíčů a zpřísnění kontroly integrity dat.

Veškerá vzdálená správa serverů tedy probíhá přes SSH. Je tedy nutné zajistit minimální zneužitelnost vhodným nastavením konfiguračního souboru SSH služby (deamona) a zároveň firewallu, který běží na všech počítačích.

Nastavení SSH se provádí v souboru `/etc/ssh/sshd_config` a výsledná konfigurace vypadá asi takto:

---

[10] *Citace: D. Rohleder. Bezpečnost v systémech UNIX. Zpravodaj ÚVT MU. ISSN 1212-0901, 1997, roč. VII, č. 4, s. 14-16.*

Nastavení portu pro komunikaci s sshd. Je možno zvolit jakýkoliv jiný volný port.

```
Port 22
```

Zde se určuje, jaká verze SSH se má použít. Použití verze 2 je však výhodnější.

```
Protocol 2
```

Je dobré si promyslet, jestli budeme používat IPv4, IPv6 nebo oboje. Jelikož IPv6 není ještě zdaleka tak rozšířena, nemá smysl ji nastavovat.

```
AddressFamily inet
```

Nastavení adresy pro SSH, na které má poslouchat. Pokud by byl systém nastaven na několik veřejných IP adres, dovoluje nám SSH zadat jejich rozsah nebo je určit přímo.

```
ListenAddress 82.208.36.174
```

Kvůli větší bezpečnosti se mohou definovat uživatelské skupiny, které mají přístup k přihlášení přes SSH. Uživatelé jiných než definovaných skupin jsou blokováni. Na stejném principu funguje parametr `AllowUsers`, který vymezuje přímo jednotlivé uživatele. Nemá smysl povolovat skupiny a zároveň uživatele.

```
AllowGroups wheel
```

Zakázání přihlášení superuživatele (root) je dalším bezpečnostním opatřením. Uživatel root má veškerá práva v systému. Pro potencionálního útočníka je obtížnější zjistit heslo běžného uživatele a následně potom superuživatele. Neméně důležitý je také fakt, že při povoleném přihlašovaní root, nelze zjistit, kdo kdy se jako root přihlásil.

```
PermitRootLogin no
```

Ověřování pomocí veřejného a soukromého klíče je bezpečnější než pomocí klasického hesla. Útočník by musel získat privátní klíč a ještě heslo, které je požadováno pro jeho použití.

```
PubkeyAuthentication yes
```

Jelikož pro ověřování přihlášení uživatele je použito klíčů, je ověření pomocí klasického hesla zbytečné. Pokud však dojde ke ztrátě klíče nebo zapomenutí fráze, nelze se jinak do systému vzdáleně přihlásit a je nutná návštěva serverovny a vygenerování nového klíče.

```
PasswordAuthentication no
```

Všechny služby a uživatelé nemající heslo jsou potencionálním bezpečnostním rizikem pro celý systém. Zamezení přihlášení bez hesla tento prvek eliminujeme.

```
PermitEmptyPasswords no
```

Tato konfigurace je plně postačující a detailnější nastavování není potřeba. Samozřejmě, že konfiguraci lze kdykoliv upravit nebo rozšířit. Vše se odehrává za běhu systému pouze s restartováním SSH deamona. Po novém načtení konfiguračního souboru se změny projeví až při následujícím spojení.

3.3 PF – PACKET FILTER (FIREWALL)

Zařízení, která slouží k zabezpečování a řízení provozu, se nazývají firewally. Určují pravidla při komunikaci mezi sítěmi. Slouží jako jejich kontrolní bod. Firewally získávají informace o stavu spojení a kontrolují protokoly.

Firewally lze dělit na dva základní typy:

3.3.1 Aplikační brána

Aplikační brána pracuje na aplikační vrstvě a střeží jednotlivé aplikace. Veškerá komunikace probíhá prostřednictvím zástupných (proxy) serverů. Uživatelé přistupují ke službám prostřednictvím těchto proxy serverů transparentně nebo pomocí upravených klientů.

Petr Bezděk popisuje komunikaci mezi klienty a servery takto, cituji: *“Komunikace mezi serverem a klientem vypadá následovně: klient chce kontaktovat server, místo toho kontaktuje proxy server na firewallu a ten dále komunikuje se skutečným serverem dle daných pravidel.*

+ možnost autentizace na úrovni uživatelů
+ není potřeba zasahovat do jádra
- nutnost úpravy aplikací
- nutnost zvláštního programu pro každou aplikaci [11]

[11] Bezděk, Petr. FreeBSD firewall – IPFW [online]. 29. 4. 2003 [cit. 18.7.2007], <http://www.fi.muni.cz/~kas/p090/referaty/2003-jaro/skupina10/fw-bsd.html>

3.3.2 Paketový filtr

Paketový filtr pracuje na síťové vrstvě. Jeho úkolem je zkoumat hlavičky u každého paketu a podle seznamu pravidel se rozhodnout, jak s daným paketem naložit. Může daný paket zahodit, anebo pustit k dalšímu zpracování.

Podle Petra Bezděka jsou výhody a nevýhody následující, cituji:

+ není potřeba upravovat aplikace

+ rychlost, většina operací se odehrává uvnitř jádra

+ nenáročný, lze vyrobit firewall na jedné disketě

- autentizace jen podle IP adres či čísla portů [12]

Packet Filter (PF) používaný v systému FreeBSD je portován z operačního systému OpenBSD. Je dílem Daniela Hartmeira, který se také podílí na vývoji systému OpenBSD. Packet filter je součástí systému FreeBSD až od verze 5.x.

Předchozí verze FreeBSD měly možnost používat dvou firewallových systémů - nativního ipfw, které bylo implementováno jako hack přímo do zpracování netinet packetů, a ipf, které bylo importováno a používalo generickou abstraktní vrstvu takzvaný PFIL. S importem OpenBSD firewallu pf, který také využívá PFIL, bylo rozhodnuto přepsat ipfw, aby používal PFIL framework. [13]

Spolu s Packet Filterem v systému přibyl traffic shaper ALTQ, který dříve existoval jako separátní patch.

Samotný firewall byl v mnohém vylepšen. Umožňuje definovat takzvané množiny pravidel, se kterými pak lze manipulovat jako s celkem, umí filtrovat pakety podle jailů (jakési polo-virtuální stroje, které FreeBSD používá pro oddělení různých procesů), dále jsou zde antispoof pravidla a ověřování validity zdroje paketu. Sledování procesů je již možné zachytit i formou množin a tabulek.

---

[12] Bezděk, Petr. FreeBSD firewall – IPFW [online]. 29. 4. 2003 [cit. 18.7.2007], <http://www.fi.muni.cz/~kas/p090/referaty/2003-jaro/skupina10/fw-bsd.html>

[13] Divácký, Roman. *Networking ve FreeBSD řady 5* [root.cz, online]. 20. 9. 2004 [cit. 20. 7. 2007]. <http://www.root.cz/clanky/networking-ve-freebsd-rady-5/>

Ve FreeBSD (od verze 4.1) existuje mechanismus KQUEUE, který zajišťuje O(1) implementaci pollingu na různé události. V jednoduchosti nahrazuje O(n) select/poll O(1). Ve verzi FreeBSD 5 byla podpora systému KQUEUE zahrnuta i na stav ethernetové linky. Tohoto využijí především routovací démony hlídající, která linka je v provozu a která ne.[14]

Pro povolení Packet Filteru při startu systému je nutné upravit soubor `/etc/rc.conf` přidáním řádku:

```
pf="YES"
```

Aby se předešlo kompletnímu restartu systému, lze pf spustit příkazem

```
/etc/rc.d/pf start
```

Probírány a vysvětlovány budou pouze stěžejní části nastavení. Kompletní konfigurační soubor pf.conf je uveden v příloze.

Nejvíce útoků na SSH probíhá ze zahraničních serverů. Z toho důvodu je povoleno přihlášení do systému z českých IP adres. Po zavedení tohoto pravidla v pf se snížil počet slovníkového útoku a útoku hrubou silou o 90%. Toto pravidla se sice dá obejít použitím nějakého proxy serveru nacházejícího se v České republice, ale takových jedinců, kteří s tímto omezením počítají, není mnoho.

```
table <czech_net> persist file "/etc/pf.czech_net.table"
pass in log on $ext_if proto tcp from <czech_net> to $ext_addr_1 port $ext_ssh_1 \
       flags S/SA keep state \
       (max-src-conn 5, max-src-conn-rate 3/30, overload <ssh_bruteforce> flush
       global)
```

Jsou zde definovány i povolené porty. Pokud nějaká služba či aplikace vyžaduje vlastní port nebo byl u stávajících služeb definován port jiný než standardní, je nutné ho přidat do seznamu povolených portů. V opačném případě by byl firewallem odfiltrován. Samozřejmě, že nastavení se vztahuje pouze na vstupní porty. Výstupní porty jsou ponechány otevřené všechny.

```
ext_tcp_0_inports="{ 21, 25, 80, 110, 143, 443, 993, 995 }"
```

Pro větší bezpečnost je možno definovat i IP adresy, které budou mít přístup povolen nebo zakázán. Lze zde vymezit jak samostatné IP adresy, tak jejich rozsah.

---

[14] Divácký, Roman. *Networking ve FreeBSD řady 5* [root.cz, online]. 20. 9. 2004 [cit. 20. 7. 2007]. <http://www.root.cz/clanky/networking-ve-freebsd-rady-5/>

Soubor `pf.goodguys.table` označuje IP adresy, kterým je umožněna komunikace na všech portech. Oproti tomu `pf.badguys.table` veškerou komunikaci striktně zakazuje.

```
table <goodguys> persist file "/etc/pf.goodguys.table"
table <badguys> persist file "/etc/pf.badguys.table"
```

Kompletní konfigurace PF je v `/etc/pf.conf` viz příloha 1.

3.4 MYSQL

MySQL je relační databázový systém typu DBMS (database managment system) šířený jako OpenSource. Byl vytvořen švédskou firmou MySQL AB. Jeho hlavními autory jsou Michael Widenius a David Axmark.

Každá databáze v MySQL je tvořena z jedné nebo více tabulek, které mají řádky a sloupce. Obdobně je tomu například u Microsoft SQL a jiných SQL databází. Systém MySQL je využíván v C, C++, Java, Perl, PHP, Python, Tcl, Visual Basic, .NET.

Jelikož se v počátku tento systém specializoval na výkon a rychlost, postrádal spoustu důležitých implementací, např. triggery, úložné procedury a pohledy. Od verze 5.0 však již většinu těchto věcí obsahuje.

MySQL sice tvoří nezbytnou část celého systému, ale jeho konfigurace je ve skrze jednoduchá. Systém nabízí několik přednastavených konfiguračních souborů, které se nacházejí v adresáři `/usr/local/share/mysql/` a jmenují se:

```
my-huge.cnf
my-innodb-heavy-4G.cnf
my-large.cnf
my-medium.cnf
my-small.cnf
```

Výběr je prakticky jen na našem uvážení a způsobu využívání databáze. Pro systém obsahující malý počet databází a dat nemá smysl volit stejnou konfiguraci jako pro velké. Konfigurační soubor je samozřejmě možné kdykoliv pozměnit a upravit, takže nemusíme být zaskočeni případným počtem zvyšujících se požadavků na MySQL server.

Následovné upravení souboru `/etc/rc.conf`:

```
mysql_enable="YES"
```

zajistí, že se databázový systém MySQL spustí po startu systému a není nutné jej spouštět ručně.

Spuštěním příkazu `/usr/local/etc/rc.d/mysql-server start` se spustí MySQL a není nutno restartovat celý systém.

3.5 POSTFIX

Postfix je MTA (mail transfer agent) a byl vytvořen jako alternativa k velice rozšířenému Sendmailu. Je jeho plnohodnotnou náhradou a změny se nedotknou funkcí ostatních aplikací.

Jako agent MTA Postfix přijímá a odesílá zprávy elektronické pošty přes síť protokolem SMTP. Nezajišťuje komunikaci přes POP ani IMAP. O to se stará jiný program např. Courier s IMAP rozšířením.

Postfix je řešen jako modulární systém. Procesy, které nevyužíváme, se dají jednoduše vypnout. Tím se zabrání jejich zneužití.

Po instalaci Postfixu je nutné vyřadit z činnosti stávajícího emailového agenta Sendmail. To se provede upravením `/etc/rc.conf`:

```
postfix_enable="YES"
sendmail_enable="NO"
sendmail_submit_enable="NO"
sendmail_outbound_enable="NO"
sendmail_msp_queue_enable="NO"
```

Vlastní konfigurace postfixu se odehrává v souborech `main.cf` a `master.cf`. Zde se definují veškeré proměnné. Jelikož bude využíván MySQL pro virtuální mailboxy, je nutné vytvořit dodatečné soubory, které nám budou uchovávat přístupové údaje do sql databáze. To se docílí úpravou následujících řádků v main.cf:

```
virtual_alias_maps = mysql:/usr/local/etc/postfix/mysql_virtual_alias_maps.cf
virtual_minimum_uid = 1001
virtual_gid_maps = static:1001
virtual_uid_maps = static:1001
virtual_mailbox_base = /usr/local/virtual
virtual_mailbox_domains =
mysql:/usr/local/etc/postfix/mysql_virtual_domains_maps.cf
virtual_mailbox_limit = 51200000
virtual_mailbox_maps = mysql:/usr/local/etc/postfix/mysql_virtual_mailbox_maps.cf
virtual_transport = virtual
virtual_create_maildirsize = yes
virtual_mailbox_extended = yes
virtual_mailbox_limit_maps =
mysql:/usr/local/etc/postfix/mysql_virtual_mailbox_limit_maps.cf
virtual_mailbox_limit_override = yes
```

```
virtual_maildir_limit_message = Sorry, the user's maildir has overdrawn his disk
space quota, please try again later.
virtual_overquota_bounce = yes
relay_domains = mysql:/usr/local/etc/postfix/mysql_relay_domains_maps.cf
```

Po vytvoření souboru s příslušným obsahem se zajistí propojení emailového systému s MySQL:

„`user`“ určuje uživatele, pod kterým se hlásíme do databáze,

„`password`“ heslo pro uživatele postfix,

„`hosts`“ adresu sql serveru

„`dbname`“ databází, do které přihlášení směřuje

a „`query`“ dotaz, který se má vykonat.

```
/usr/local/etc/postfix/mysql_virtual_alias_maps.cf :
user = sys_mail_postfix
password = heslo
hosts = localhost
dbname = sys_mail
query = SELECT goto FROM alias WHERE address='%s' AND active = 1
```

```
/usr/local/etc/postfix/mysql_virtual_domains_maps.cf :
user = sys_mail_postfix
password = heslo
hosts = localhost
dbname = sys_mail
query = SELECT domain FROM domain WHERE domain='%s'
```

```
/usr/local/etc/postfix/mysql_virtual_mailbox_limit_maps.cf :
user = sys_mail_postfix
password = heslo
hosts = localhost
dbname = sys_mail
query = SELECT quota FROM mailbox WHERE username='%s'
```

```
/usr/local/etc/postfix/mysql_virtual_mailbox_maps.cf:
user = sys_mail_postfix
password = heslo
hosts = localhost
dbname = sys_mail
query = SELECT maildir FROM mailbox WHERE username='%s' AND active = 1
```

Obsah předchozích souborů je velice podobný. Liší se pouze v dotazu prováděném v SQL databázi. Bohužel bez těchto nastavení by výsledná konfigurace nebyla kompletní.

Jestliže klient, pro kterého je server spravován se rozhodne využívat služeb zabezpečeného SMTP, bude následovat úprava následujících řádků v souboru `main.fc`:

```
smtp_use_tls = yes
smtp_tls_note_starttls_offer = yes
smtpd_use_tls = yes
smtpd_tls_key_file = /usr/local/etc/ssl_cert/roxy.refresh.cz.pem
smtpd_tls_cert_file = /usr/local/etc/ssl_cert/roxy.refresh.cz.pem
smtpd_tls_loglevel = 1
smtpd_tls_received_header = yes
smtpd_tls_session_cache_timeout = 3600s
smtpd_tls_auth_only = yes
tls_random_source = dev:/dev/urandom
```

V případě použití zabezpečeného protokolu je nutné vygenerovat příslušné klíče programem OpenSSL. Je to program, který implementuje Secure Socket Layer (SSL v2/v3) a Transport Layer Security (TLS v1). Vlastní vygenerování klíčů se provede příkazem:

```
openssl req -new -x509 -nodes -out roxy.refresh.cz.pem -keyout roxy.refresh.cz.pem
-days 3650
```

Úplný výpis ze souboru `main.cf` je uveden v příloze 2.

Soubor `master.cf` obsahuje konfigurace systémových deamonů programu Postfix. Jak již bylo řečeno, Postfix je svou strukturou modulární a tudíž dovoluje spouštět pouze určité procesy. Ostatní zůstávají vypnuty.

Výchozí formát `master.cf` je následující:

- každá logická část určuje samostatnou Postfix službu. Služba je identifikovatelná pomocí jména a typu, kterým je popsána. Jestliže několik řádků popsuje stejné jméno služby a typ, platí pouze ten poslední.
- Prázdné a zakomentované (označené # na začátku) řádky jsou ignorovány.

Základní nastavení pro SMTP je

```
smtp      inet  n       -       n       -       -       smtpd
```

Ovšem přidáním řádku

```
       -o receive_override_options=no_address_mappings
```

docílíme zakázání normativního mapování adres.

Jelikož na serveru neběží žádné nestandardní aplikace, není nutné výchozí `master.cf` příliš měnit. Za zmínku stojí pouze povolení antivirového scanneru AMaViS přidáním řádku

```
-o content_filter=smtp-amavis:[127.0.0.1]:10024.
```

Kompletní výpis konfiguračního souboru `master.cf` je uvede v příloze 3.

3.6 COURIER-IMAP

Courier-IMAP je rychlý, škálovatelný IMAP server, který využívá emailové adresáře. Je využíván mnoha emailovými servery k jednoduché správě i několika stovek účtů. S vlastními vestavěnými IMAP a POP3 službami má prakticky neomezené množství různých kombinací nastavení. [15]

Při spojení s klientem, čeká na jeho přehlášení. Následně pohledává server, na kterém se příslušná schránka nachází a vytvoří spojení v jednom nepřerušovaném procesu.

Je to ten samý IMAP server, jenž je zahrnut v klasickém Courier mail serveru. Konfigurace je uzpůsobena tak, aby mohl běžet samostatně. Jeho služby využívají další mail servery, jako jsou Postfix, Exim nebo Qmail.

Nezbytnou součástí Courier-IMAP je jsou autentifikační knihovny courier-authlib a courier-authlib-mysql. Jejich kompilace proběhne automaticky s překladem courier-imap.

---

[15] SCHNEIDER, Roland <list-courier@serv.ch>, PRICE, Patrick <sysadmin@moment.net> - Courier Documentation, 30. 10 2006, <http://www.courier-mta.org/documentation.html>

Nastavení courier-authlib probíhá v adresáři `/usr/local/etc/authlib` úpravou nebo vytvořením souborů `authdaemonrc` a `authmysqlrc`.

Authdaemonrc slouží k nastavení autentifikačního deamona. Jelikož náš systém využívá pro ověřování data uložená v MySQL je důležité, aby soubor obsahoval

```
authmodulelist="authmysql"
```

Seznam veškerých možných autentifikací lze nalézt také na řádku

```
authmodulelistorig="authuserdb authvchkpw authpam authldap authmysql authpgsql"
```

Jak je vidět, lze také použít například databázový systém PosgreSQL nebo PAM ověřování. Ostatní nastavení mohou zůstat nedotčena. Za zmínku by ještě stála debuggovací služba. Tu je možno nastavit na 3 stavy:

`DEBUG_LOGIN=0` vypíná logování chybných hlášení,

`DEBUG_LOGIN=1` zapíná logování chybných hlášení,

`DEBUG_LOGIN=2` zapíná logování chybných hlášení a navíc vypisuje hesla do systémového logu.

Poslední možnost není kvůli bezpečnosti doporučována. Jde ji ovšem povolit za předpokladu ověřování hesel při prvotním nastavení.

Soubor `authmysqlrc` slouží k vlastní konfiguraci ověřování pomocí MySQL a má následující obsah:

```
MYSQL_SERVER         localhost
MYSQL_USERNAME       sys_mail_courier
MYSQL_PASSWORD       heslo
```

Konfigurační soubory pro Courier-IMAP jsou v adresáři `/usr/local/etc/courier-imap`. Měli bychom se rozhodnout, zda budeme provozovat POP3 i IMAP server nebo pouze jeden z nich.

POP3 (Post Office Protocol version 3) je protokol využívaný ke stahování emailových zpráv ze serveru na klienta. Pro své účely má vyhrazen TCP port 110. Přestože je pro něj běžné využívání nezabezpečeného přenosu hesel, podporuje současně několik autentifikačních metod ověřování přístupu k poštovní schránce. Jednou z metod je APOP. Využívá hashe MD5 k zabezpečení přenosu hesla od klienta na server. Lze také šifrovat celou zprávu využitím SSL nebo modernějšího TSL. K tomu je vyhrazen port 995.

Čtení zpráv je možno pouze po stažení ke klientovi. Připojení k serveru je ukončeno po stažení všech označených zpráv. Je obnoveno pouze za účelem vyzvednutí nových zpráv ze serveru.

IMAP (Internet Message Access Protocol) na rozdíl od POP3 je optimalizován pro dlouhodobé připojení k poštovnímu serveru. Zprávy se ze serveru stahují jen v případě jejich potřeby. Jsou na něm uchovány a leze je různě řadit do složek.

Velice často se používá v rozlehlých sítích. Jakmile jsou nové zprávy uloženy na server, lze k nim pomocí IMAP okamžitě přistupovat.

Výhody oproti POP3 například podpoře více klientů připojených k jedné schránce, rychlejší práce s velkými nebo mnoha e-maily nebo vyhledávání přímo na serveru. Standardní nastavení portu je na čísle 143 pro nešifrovaný přenos a 993 pro šifrovaný.

Jelikož FreeBSD nabízí upravené konfigurační soubory, lze je využít. Nesou názvy `imapd.dist imapd.cnf.dist imapd-ssl.dist` pro IMAP a `pop3d.dist pop3d.cnf.dist pop3s-ssl.dist` pro POP3. Z názvu těchto souborů stačí odstranit koncovku .dist.

Výjimku tvoří `imapd.cnf` a `pop3d.cnf`, které je ještě nutno upravit. Slouží k vygenerování X.509 certifikátu.

Tělo těchto dokumentů vypadá následovně:

```
RANDFILE = /usr/local/share/courier-imap/imapd.rand

[ req ]
default_bits = 1024
encrypt_key = yes
distinguished_name = req_dn
x509_extensions = cert_type
prompt = no

[ req_dn ]
C=CZ
ST=Czech Republic
L=Prague
O=Refresh, s.r.o.
OU=Webmaster Team
CN=roxy.refresh.cz
emailAddress=refresh@refresh.cz

[ cert_type ]
nsCertType = server
```

Pro spouštění courier-imap po startu počítače je nutné přidat následující řádky do /etc/rc.conf:

Spuštění authentifikačního deamona

```
courier_authdaemond_enable="YES"
```

Spuštění nešifrované služby IMAP

```
courier_imap_imapd_enable="YES"
```

Spuštění šifrované služby IMAP

```
courier_imap_imapd_ssl_enable="YES"
```

Spuštění nešifrované služby POP3

```
courier_imap_pop3d_enable="YES"
```

Spuštění šifrované služby POP3

```
courier_imap_pop3d_ssl_enable="YES"
```

Opět zde platí pravidlo, že pokud jsou nějaké služby nechtěné, stačí je z rc.conf odstranit nebo případně zakázat nastavením na NO. Zadáním následujících příkazů zajistíme spuštění jejich spuštění bez nutnosti restartu:

```
/usr/local/etc/rc.d/courier-authdaemond start
/usr/local/etc/rc.d/courier-imap-imapd.sh start
/usr/local/etc/rc.d/courier-imap-imapd-ssl.sh start
/usr/local/etc/rc.d/courier-imap-pop3d.sh start
/usr/local/etc/rc.d/courier-imap-pop3d-ssl.sh start
```

3.7 PROFTPD

ProFTPd vznikl z potřeby mít bezpečný a plně konfigurovatelný FTP server. Před započetím tohoto projektu byl velice rozšířená wu-ftp. I přes jeho vynikající kvalitu, měl velice chabé zabezpečení.

Mnoho lidí, včetně vývojářů pracujících nyní na ProFTPd, strávilo spoustu času opravováním těchto chyb a zahrnováním vylepšení do wu-ftp. Tato práce se nejevila jako efektivní a byl vznesen požadavek na kompletní přepsání zdrojového kódu a instrukcí pro lepší konfigurovatelnost. Byl vydán pod GPL licenci.

Jeho dokumentace je velice obsáhlá a konfigurační syntaxe jsou podobné struktuře, jakou využívá Apache. Má snadnou konfiguraci několika virtuálních FTP serverů. Jeho design je modulární, tudíž umožňuje spouštět podporu SSL/TSL, LDAP a

SQL jako samostatný modul. O jeho kvalitách také vypovídá plná připravenost přechodu na IPv6.

Konfigurace ProFTPd je uchována v souboru `/usr/local/etc/proftpd.conf`. Rozhodnutí, zda má server běžet jako samostatný proces nebo bude spouštěn pomocí inetd, je jen na našem uvážení. Výhodou nastavení jako samostatného procesu je okamžitý přístup k serveru přes port, na kterém naslouchá. V konfiguračním souboru je to zaneseno následovně:

```
ServerType                  standalone
```

Je také zádoucí zvolit vhodné jméno k jeho identifikaci.

```
ServerName                  "FTP daemon"
```

Pokud není vyžadováno anonymní připojení k FTP serveru a budu se přihlašovat pouze definovaní uživatelé prostřednictvím svých jmen a hesel je dobré celou sekci mezi <anonymous ~ftp> a </anonymous> smazat nebo případně zakomentovat.

Propojení s MySQL zajišťují následující řádky:

```
SQLAuthenticate             users*
SQLConnectInfo sys_ftp@localhost:3306 sys_ftp_proftpd SImk4LexSOxo PERSESSION
SQLAuthTypes                Crypt
SQLUserInfo                 users login passwd uid gid homedir shell
SQLHomedirOnDemand          off
```

Kompletní výpis z `proftpd.conf` je v příloze 4.

3.8 APACHE

Apache http server je softwarový webový server. Protože jeho kód je otevřený, byl portován do mnoha operačních systémů.

Roku 1993 na Illinoiské univerzitě byl započat projekt s názvem NSCA HTTPd. O rok později hlavní programátor Rob McCool opustil vývojářský tým a tím došlo ke zpomalení vývoje a v roce 1998 k úplnému zastavení. Jelikož již došlo k rozšíření serveru, spojila se malá skupinka webmasterů a snažila se stávající NSCA HTTPd upravovat a záplatovat. Z iniciativy Braina Behlendorfa a Cliffa Skolnicka vznikla emailová konference, ve které byly veškeré úpravy zaznamenávány a uchovávány. Následovalo kompletní přepsání zdrojových kódu a Apache2 již neobsahuje nic z původního NCSA HTTPd.

Úpravy nastavení se provádějí v `/usr/local/etc/apache2/httpd.conf`. Pro konfiguraci Apache je důležité nastavení IP adresy a portu, na kterém má server poslouchat. Pokud by nebyla zadána pevná IP adresa, znamenalo by to, že server poslouchá na všech dostupných adresách na určeném portu.

```
Listen 82.208.36.175:80
```

Nastavení emailové adresy správce se považuje za slušnost. Případné dotazy a připomínky ke správě serveru směřují na zadanou adresu.

```
ServerAdmin refresh@refresh.cz
```

V případě použití zabezpečeného serveru HTTPS se zahrne další konfigurační soubor do nastavení Apache. Jedná se o virtuální server běžící nad stávajícím, avšak využívající SSL. Pro tento fakt by měl být vygenerován příslušný certifikát sloužící k ověření serveru.

```
Include etc/apache22/vhosts_ssl/enabled/*.conf
```

Podle potřeby je možno vytvořit více virtuálních serverů zahrnutím jejich konfiguračního souboru do httpd.conf. Apache má mnoho různých možností nastavení a dá se upravit tak říkajíc na míru konkrétním požadavku.

Kompletní konfigurační soubor viz příloha 5.

3.9 DOKONČENÍ NASTAVENÍ SYSTÉMU

V předchozích kapitolách byly uváděny části konfiguračních souborů, které zajišťovali spojení s databází MySQL. Aby data mohla být ukládána do příslušné databáze a tabulky, je nutné je vytvořit a zajistit k nim přistup.

Celý emailový systém, tj. pro Postfix a Courier-IMAP, využívá společnou databázi, stačí provést následující příkazy v SQL:

```
CREATE DATABASE `sys_mail` DEFAULT CHARACTER SET utf8 COLLATE utf8_czech_ci;
GRANT SELECT ON `sys\_mail`.* TO 'sys_mail_postfix'@'localhost' IDENTIFIED BY
'heslo';
GRANT SELECT ON `sys\_mail`.* TO 'sys_mail_courier'@'localhost' IDENTIFIED BY
'heslo';
GRANT SELECT ON `sys\_mail`.* TO 'sys_mail_amavisd'@'localhost' IDENTIFIED BY
'heslo';
GRANT SELECT, INSERT, UPDATE, DELETE ON `sys\_mail`.* TO
'sys_mail_padmin'@'localhost' IDENTIFIED BY 'heslo';
```

Pro ProFTPd jsou SQL dotazy následující:

```
CREATE DATABASE `sys_ftp`;
GRANT SELECT ON `sys\_ftp`.* TO 'sys_ftp_proftpd'@'localhost' IDENTIFIED BY
'heslo';
```

Tímto by byla konfigurace aplikací a služeb ukončena. V některých případech postačilo výchozí nastavení nabízené systémem, jinde bylo nutno provést několik změn. Bylo dbáno na vylíčení funkčnosti jednotlivých aplikací a jejich vývoj. V celém systému lze provést ještě takzvaný hardening, to znamená kompletní zabezpečení systému, včetně oprav jádra a systémových prostředků, upravení přihlašovacích skriptů a dalších věcí. Vše je spolehlivě a přehledně popsáno na http://www.bsdguides.org/guides/freebsd/security/harden.php , tudíž bych případné zájemce o tuto problematiku odkázal sem.

4 MONITORING

K vlastnímu monitorování se využívá jak služeb na lokálním počítači, tak odezvy a hlášení z přidružených strojů. Díky tomu, že je systém nakonfigurován na rozesílání emailových zpráv, lze jej využít k přeposílání systémových hlášení a hlášení o chybách správci. Využívá se jak skriptů `/etc/periodic`, cronu, tak monitorovacího systému MRTG. Poslední jmenovaný není v základní nabídce systému obsažen, ale je možné ho přes porty (ports) doinstalovat.

Výstupy zasílané z periodic a cronu jsou textového charakteru. Výstupy z MRTG jsou grafické a zobrazují se pomocí služby Apache jako webové stránky. Textové výstupy poskytují informace pravidelně v určitých nastavených intervalech nebo při výskytu problému. Grafické výstupy poskytují souvislé informace o stavu v podobě grafů.

4.1 SKRIPTY PERIODIC

FreeBSD pomocí periodic spouští v určitou dobu programy provádějící pravidelnou údržbu systému. Příkaz periodic čte konfigurační soubor /etc/default/periodic.conf, resp. /etc/periodic.conf, pokud jsou nutné nějaké změny. Příkaz periodic je využíván k periodickému spouštění denních, týdenních atd. vlastních příkazů. [16]

Základní skripty pro periodic se nacházejí v /etc/periodic a jsou rozděleny podle času spouštění plus adresář obsahující security skripty. [17]

Z detailního pohledu na /etc/defaults/periodics.conf plyne zjištění, že periodic lze nastavit tak, aby prováděl důmyslné kontroly a funkce. Veškeré výstupy jsou zasílány uživateli root. Toto nastavení je možné změnit a to buď v tomto souboru nebo v /etc/mail/aliases. Skripty jsou spouštěny v pořadí podle jejich prefixu. Toto číslování

---

[16] BĚLKA, Jiří. *Začínáme bezpečně s FreeBSD (5)* [root.cz, online]. 20. 7. 2004 [cit. 2007-08-12]. <http://www.root.cz/clanky/zaciname-bezpecne-s-freebsd-5/>

[17] BĚLKA, Jiří. *Začínáme bezpečně s FreeBSD (5)* [root.cz, online]. 20. 7. 2004 [cit. 2007-08-12]. <http://www.root.cz/clanky/zaciname-bezpecne-s-freebsd-5/>

je používáno již od SystemV. Takže skripty s nižším prefixem jsou spouštěny dříve než skripty s vyšším.

Výpis z /etc/periodic.conf na serveru elsa.eurofinancial.cz je následující:

Provede příkaz pkg_version -v a zašle výsledek na email superuživatele (roota)

```
weekly_status_pkg_enable="YES"
```

Zaslaní emailu denních statistik gmirroru se používá pouze v případě, když je gmirror nastaven při instalaci systému. Jinak toto nastavení postrádá smysl a je možné ho buď vynechat, nebo zakázat změnou hodnoty na NO.

```
daily_status_gmirror_enable="YES"
```

Tato nastavení jsou úzce spjata s Postfixem. Zasílají informace o emailovém systému. Jak je patrné, jsou tyto statistiky zakázány.

```
daily_clean_hoststat_enable="NO"
daily_status_mail_rejects_enable="NO"
daily_status_include_submit_mailq="NO"
daily_submit_queuerun="NO"
```

Následující řádky se vztahují k samotnému systému FreeBSD a udávají různé statistiky vztahující se k portům a novým zařízením.

```
monthly_statistics_enable="YES"
monthly_statistics_report_devices="YES"
monthly_statistics_report_ports="YES"
```

Zde je povoleno zasílání změny tabulky nastavení Packet Filteru.

```
daily_status_security_pf_tables_enable="YES"
```

V závěru konfiguračního souboru nacházíme nastavení adresy pro lokální skripty. Pokud při instalaci nějakého programu či služby jsou vytvářeny periodic skripty, ukládají se právě do tohoto adresáře.

```
local_periodic="/usr/local/etc/periodic"
```

Výpis z `/etc/defaults/periodic.conf` viz příloha 6.

4.1.1 Daily run output

Daily run outup je výstup veškerých skriptů ve složce daily a povolených v /etc/defaults/periodic.conf `nebo v` /etc/periodic.conf.

Následující řádej je seznam odstraněných souborů ze složky `/var/preserve`, které nejsou 7 dni změněny nebo jinak upraveny. Pokud by se v této složce nacházely soubory vyhovující podmínkám pro jejich smazání, budou odstraněny a jejich seznam se objeví pod následujícím řádkem.

```
Removing stale files from /var/preserve:
```

Vymazání staré denní zprávy. Opět lze nastaví dobu, po které se má určitý soubor odstranit, nebyl-li změněn.

```
Cleaning out old system announcements:
```

Odstranění souborů z adresáře `/var/rwho`. Rhwo je obdobný příkaz jako who, ale vztahuje se na všechny stroje z lokální sítě. [18]

```
Removing stale files from /var/rwho:
```

Zazálohování souboru uživatelů a hesel a soubor skupin. Provádí se v případě, že se příslušné soubory změnily. Jedná se o rozdílové zálohy pomocí programu diff. Jak je vidět byl změněn jeden uživatel v souboru `/etc/passwd` a dvě skupiny v `/etc/groups`. Pokud by změny nebyly provedeny administrátorem, je tímto upozorněn.

```
Backup passwd and group files:
amanda.refresh.cz passwd diffs:
18a19
> _dhcp:(password):65:65::0:0:dhcp programs:/var/empty:/usr/sbin/nologin
amanda.refresh.cz group diffs:
22a23
> _dhcp:*:65:
25a27
> audit:*:77:
```

Zde je výpis kontroly syntaxí souboru `/etc/group`. Jak následující řádky napovídají, je vše v pořádku a soubor `group` neobsahuje žádnou chybu.

```
Verifying group file syntax:
/etc/group is fine
```

---

[18] FreeBSD Hypertext Man Pages [online]. 6. 6. 1993.
<http://www.freebsd.org/cgi/man.cgi?query=rwho&sektion=1>

Vytvoření zálohy souboru `/etc/mail/aliases` ve `/var/backup/`. Opět se provádí záloha jen v případě, že byl soubor pozměněn. Jak vyplývá z hlášení, byl zjištěn rozdíl mezi souborem `/etc/mail/aliases` a jeho záložní kopií. Následně potom se provedla synchronizace a záložní soubor byl upraven, aby odpovídal svému originálu. Kdyby si administrátor nebyl vědom provedených změn, jednalo by se s největší pravděpodobností o bezpečnostní problém.

```
Backing up mail aliases:
amanda.refresh.cz aliases diffs:
--- /var/backups/aliases.bak       Sun Jun 24 11:36:37 2007
+++ /etc/mail/aliases       Mon Aug 13 20:05:26 2007
@@ -26,6 +26,7 @@
 postmaster: root
  # General redirections for pseudo accounts
+_dhcp: root
 _pflogd: root
 bin:  root
 bind: root
```

Stav zaplnění disku se zjišťuje z příkazové řádky pomocí příkazu `df`. Aby vznikl náležitý přehled o stavu zaplnění disku, je nutné tento výpis dostávat pravidelně. Filesystem určuje část disku (partitions), 1K-blocks udává velikost oddílu disku v 1Kbyte bloků, Used označuje využité místo a Avail dostupné místo na diskovém oddílu. Sloupec s názvem Capacity vypisuje procentuální podíl zaplněného místa oproti celkové velikosti. Pokud se hodnota toho sloupce přibližuje k 100, je nutné provést kontrolu zaplnění a odstranit nechtěné nebo již přebytečné soubory. Výjimku tvoří řádek `devfs`. Je to proměnlivý souborový systém. To znamená, že vytváření nebo mazání údajů v `/dev` je závislé na dostupných zařízeních. Jeho hodnota je stále 100%. Sloupec `Mounted` on určuje místo připojení diskového oddílu.

```
Disk status:
Filesystem         1K-blocks      Used     Avail Capacity  Mounted on
/dev/mirror/gm0s1a    380654     63810    286392    18%    /
devfs                      1         1         0   100%    /dev
/dev/mirror/gm0s1f   8748416   3302988   4745556    41%    /usr
/dev/mirror/gm0s1d  25385516    698906  22655770     3%    /var
/dev/mirror/gm0s1e   2026030        20   1863928     0%    /tmp
/dev/mirror/gm0s2d 337795360 174057912 136713820    56%    /vol0
/dev/md0c            3045006    507986   2293420    18%    /vol0/jail/rain
devfs                      1         1         0   100%    /vol0/jail/rain/dev
```

Pod následujícím řádkem by byl výpis pouze v případě použití `dump` a `restore` pro vytváření záloh.

```
Last dump(s) done (Dump '>' file systems):
```

Následuje výpis statistik pro síťová rozhraní. Obdobného vstupu je možno dosáhnout provedením příkazu `netstat –in` z konzole. Z těchto údajů lze vyčíst nastavení IP adres pro jednotlivá síťová zařízení, přijaté a odeslané pakety a co je velice důležité chyby (jak při přijímání, tak odesílání) a kolize paketů. Při pohledu na následující výpis je zřejmé, že k žádným chybám ani kolizím nedošlo.

```
Network interface status:
Name    Mtu Network       Address              Ipkts Ierrs    Opkts Oerrs  Coll
nve0   1500 <Link#1>      00:e0:81:5f:5e:4a  3890767     0   321248     0     0
nve0   1500 192.168.123   192.168.123.2       309401     -   309348     -     -
bge0   1500 <Link#2>      00:e0:81:5f:5e:4b 244420939    0 299123636    0     0
bge0   1500 82.208.36/24  elsa               217787123    - 299291559    -     -
bge0   1500 82.208.36.71/ hosting             194405     -    41822     -     -
bge0   1500 82.208.36.72/ unassigned-82-208     8299     -        0     -     -
bge0   1500 82.208.36.73/ klub.soliver.cz       8127     -        0     -     -
lo0   16384 <Link#3>                          1692232     0  1692232     0     0
lo0   16384 fe80:3::1     fe80:3::1                0     -        0     -     -
lo0   16384 localhost.cod ::1                      0     -        0     -     -
lo0   16384 your-net      localhost          1435618     -  1435618     -     -
lo1   16384 <Link#4>                           323693     0   323693     0     0
lo1   16384 172.16.16.2/3 172.16.16.2        5700249     -   323693     -     -
tap0   1500 <Link#5>      00:bd:f8:4a:00:00  2043899     0  2120286     0     0
tap0   1500 10.111/24     10.111.0.10              0     -  2109443     -     -
```

Následuje statistika uptime (doba, po kterou systém běží bez restartu), aktuální počet přihlášených uživatelů a aktuální zátěž systému.

```
Local system status:
 3:01AM  up 82 days, 14:59, 0 users, load averages: 0.00, 0.00, 0.00
```

Pokud by nějaký email stále čekal ve frontě, bude jejich výpis zde. Jelikož tomu tak není, je zde pouze oznámení, že fronta je prázdná.

```
Mail in local queue:
Mail queue is empty
```

Kdyby nějaké maily zůstaly nevyřízené, byl by výpis následující

```
Mail in local queue:
-Queue ID- --Size-- ----Arrival Time---- -Sender/Recipient-------
D26B922B26     4140 Mon Aug 13 16:53:18  MAILER-DAEMON
                  (connect to defitem.com[209.167.25.58]: Operation timed out)
                                        LeslyeManley@defitem.com
```

```
86C69229EE     3284 Wed Aug 15 13:51:14  MAILER-DAEMON
                    (connect to kinom.com[222.122.63.8]: Operation timed out)
                                        qamass@kinomaniaki.com

-- 7 Kbytes in 2 Requests.
```

Pro detailnější výpis zabezpečení se používá vlastní skript, proto je zde pouze informace o této skutečnosti.

```
Security check:
    (output mailed separately)
```

V závěru daily run output je už jen výpis AXFR a IXFR, což se týká provozování vlastního DNS serveru BIND.

```
Checking for denied zone transfers (AXFR and IXFR):

-- End of daily output --
```

V daily run output je možné nastavit spouštění vlastních skriptů nebo přidat zbývající systémové, jako jsou výpisy ze souboru kalendáře, čištění disku a další. Samozřejmě, že se to týká věcí, které jsou používány nebo nainstalovány. Dostávat prázdné výpisy z neexistujících služeb je zbytečné.

4.1.2 Weekly run output

Tento výpis poskytuje týdenní informace o systému podle nastavení v `/etc/periodic.conf` a `/etc/defaults/periodic.conf`.

V poslední době se vyskytoval větší počet problémových SATA disků. Z tohoto důvodu byl napsán skript `smartctl.sh`, který provádí jednou týdně kontrolu disku přes jeho S.M.A.R.T. monitorovací systém. Jeho autorem je Miroslav Lachman a je vydán pod BEER-WARE LICENSE. Při problémech, které nastávaly na serverech roxy.refresh.cz a lite.eurofinancial.cz se tento skript velice osvědčil a poskytoval věrohodné a smysluplné informace. Celý skript viz příloha 7.

Výpis z weekly run output je následující.

```
Rebuilding locate database:

Rebuilding whatis database:

Check for out of date packages:
  clearsilver-python-0.10.4 needs updating (port has 0.10.5)
  mysql-client-5.0.41 needs updating (port has 5.0.45)
```

```
  mysql-server-5.0.41 needs updating (port has 5.0.45)
  neon-0.26.3 needs updating (port has 0.26.4)
  roundcube-0.1.20070303 needs updating (port has 0.1.20070608)
  subversion-1.4.3_2 needs updating (port has 1.4.4)

Checking S.M.A.R.T changes:

elsa.eurofinancial.cz changes for device /dev/ad4:
--- /var/log/smartctl__dev_ad4.today      Sat Jul 14 04:15:56 2007
+++ /tmp/security.3sUom95F  Sat Jul 21 04:15:57 2007
@@ -10,7 +10,7 @@
 Device is:        In smartctl database [for details use: -P show]
 ATA Version is:   7
 ATA Standard is:  ATA/ATAPI-7 T13 1532D revision 4a
-Local Time is:    Sat Jul 14 04:15:56 2007 CEST
+Local Time is:    Sat Jul 21 04:15:56 2007 CEST
 SMART support is: Available - device has SMART capability.
 SMART support is: Enabled

@@ -54,13 +54,13 @@
   5 Reallocated_Sector_Ct   0x0033  253  253  010   Pre-fail  Always   -         0
   7 Seek_Error_Rate         0x000f  253  253  051   Pre-fail  Always   -         0
   8 Seek_Time_Performance   0x0025  253  253  015   Pre-fail  Offline  -         0
-  9 Power_On_Hours          0x0032  100  100  000   Old_age   Always   -      4924
...
+195 Hardware_ECC_Recovered  0x001a  100  100  000   Old_age   Always   - 243715511
 196 Reallocated_Event_Count 0x0032  253  253  000   Old_age   Always   -         0
 197 Current_Pending_Sector  0x0012  253  253  000   Old_age   Always   -         0
 198 Offline_Uncorrectable   0x0030  253  253  000   Old_age   Offline  -         0
@@ -153,27 +153,27 @@

 SMART Self-test log structure revision number 1
 Num  Test_Description    Status                  Remaining  LifeTime(h) LBA_OFE
-# 1  Short offline       Completed without error       00%      4922         -
-# 2  Short offline       Completed without error       00%      4911         -
-# 3  Short offline       Completed without error       00%      4898         -
-# 4  Short offline       Completed without error       00%      4887         -
...
+#18  Short offline       Completed without error       00%      4911         -
+#19  Short offline       Completed without error       00%      4898         -
+#20  Short offline       Completed without error       00%      4887         -
+#21  Short offline       Completed without error       00%      4874         -

 SMART Selective Self-Test Log Data Structure Revision Number (0) should be 1
SMART Selective self-test log data structure revision number 0

-- End of weekly output --
```

Výstup ze skriptu `smartctl.sh` je velice obsáhlý, a proto byl zkrácen. Nemá smysl jej zde celý uvádět, protože se jedná o kompletní výpis testu prováděného pomocí `smartmontools`.

Do týdenního reportu může být zahrnuta ještě kontrola souborů, které nemají přiřazeno žádné uživatelské ID nebo případné skripty vlastní.

Jak se snižuje frekvence zasílání informací o systému, snižuje se s tím také závažnost zkoumaných informací. Z tohoto důvodu jsou veškeré důležité informace zasílány denně a případně lze snížit interval zasílání.

Kompletní výpis z `weekly run output` je obsažen v příloze 9.

4.1.3 Monthly run output

Jedním z dalších výstupů je monthly run output. Jedná se o měsíční výpis a je nejjednodušší. Poskytuje pouze výpis času přihlášení uživatelů do systému a odesílání statistik na www.bsdstats.org. Na tomto serveru jsou zaznamenávány informace o používání BSD-like operačních systémů.

Veškeré informace mají informativní charakter. Zda nedošlo k nežádoucímu průniku do systému, se dá částečně odhadnout, pomocí vysokého čísla času přihlášení. Ale pravděpodobnost, že by se to projevilo zde, je malá.

```
Doing login accounting:
       total             365.78
       dino-preschool.   115.52
       quip               81.39
       www.toxicita.cz    78.81
       www.darujvic.cz    31.92
       share.nejvic.in    28.34
       dynaspol.dev.co    15.19
       soliver.dev.cod     5.58
       www.seanet.cz       4.13
       aureliano           3.70
       www.wyschkof.co     0.81
       www.prutoky.cz      0.28
       freebsd.quip.cz     0.06
       fiallka.nejvic.     0.05
Posting monthly OS statistics to rpt.bsdstats.org Posting monthly device statistics
to rpt.bsdstats.org Posting monthly CPU statistics to rpt.bsdstats.org Posting
monthly ports statistics to rpt.bsdstats.org

-- End of monthly output --
```

Periodic poskytuje k měsíčnímu zaslání jen velice málo skriptů. Ostatní se dají doinstalovat pomocí portů (ports), jako například zasílání statistik na BSDStats.

4.1.4 Security run output

Pomocí security run output získáváme přehled o bezpečnostních dírách, počtu příhlášení, odmítnutých spojení a dalších bezpečnostních hlášení.

Obdobně jako daily run output je zasílán denně, jelikož tyto informace je důležité znát minimálně v tomto intervalu.

Pro názornost byly vybrány výstupy ze serverů grimm.quip.cz, elsa.eurofinancial.cz a retezat.tovarna.cz. Každý tento výpis obsahuje jisté odlišnosti, na které je dobré poukázat a vysvětlit proč se tomu tak děje.

Výpis ze serveru elsa.eurofinancial.cz je poměrně jednoduchý. V úvodu je kontrola potenciálně nebezpečných setuid souborů. Jedná se o soubory, které jsou kýmkoliv spustitelné s právy vlastníka souboru. Jsou zde vypisovány pouze rozdílové zálohy. Jestliže se od posledního security run output žádné suid soubory nezměnily, bude výpis prázdný.

```
Checking setuid files and devices:
ararat.tovarna.cz setuid diffs:
--- /var/log/setuid.today   Tue Jun  5 03:03:40 2007
+++ /tmp/security.vcgS9pKi  Tue Aug 14 03:04:09 2007
@@ -32,8 +32,8 @@
 588817 -r-sr-xr-x  1 root  wheel       3400 Jan 12 08:39:44 2007
/usr/libexec/pt_chown
 588860 -r-xr-sr-x  1 root  smmsp     583680 Jan 12 08:42:13 2007
/usr/libexec/sendmail/sendmail
 736188 -rwsr-xr-x  1 root  wheel     285580 Mar 27 11:36:31 2007
/usr/local/bin/screen
-597031 -rwxr-sr-x  1 root  maildrop  146742 Jun  4 13:40:06 2007
/usr/local/sbin/postdrop
-597032 -rwxr-sr-x  1 root  maildrop  152660 Jun  4 13:40:06 2007
/usr/local/sbin/postqueue
+589538 -rwxr-sr-x  1 root  maildrop  146813 Aug 13 20:59:18 2007
```

Následuje kontrola uživatelů s číslem 0. Standardně by tuto hodnotu měli mít pouze superuživatelé root a toor. Uživatel toor za normálních okolností nepoužívá. Má stejná práva jako root. Je využívám v případech, kdy z nějakého důvodu nefunguje přihlášení jako root. Přihlášením je myšleno zalogování se do konzole.

```
Checking for uids of 0:
root 0
toor 0
```

Systémový uživatel bez hesla znamená potenciální bezpečnostní riziko. Pravidelnou kontrolou lze odhalit případné vytvoření nových uživatelských účtu bez hesel, dohledání jejich práv a případné zakázání nebo vymazání. Z výpisu je patrné, že se v systému žádny účet bez hesla nenachází.

```
Checking for passwordless accounts:
```

Následuje výpis zamítnutých paketů u packet filteru. Jedná se pouze o statistické informace.

```
elsa.eurofinancial.cz pf denied packets:
+++ /tmp/security.uiEVyEZ6  Tue Aug 14 03:05:12 2007
+block drop in quick from <badguys> to any [ Evaluations: 2447140
+Packets: 0 Bytes: 0 States: 0 ] block drop in quick from <bruteforce>
+to any [ Evaluations: 2447140 Packets: 74 Bytes: 6988 States: 0 ] block
+drop in quick from <ssh_bruteforce> to any [ Evaluations: 2447066
+Packets: 9 Bytes: 468 States: 0 ] block drop quick inet6 all [
+Evaluations: 5393062 Packets: 597 Bytes: 42984 States: 0 ] block drop
+all [ Evaluations: 5392465 Packets: 720794 Bytes: 72280145 States: 0 ]
+block drop quick on bge0 inet from <reserved> to any [ Evaluations:
+5392465 Packets: 60 Bytes: 5796 States: 0 ] block drop quick on bge0
+inet from any to <reserved> [ Evaluations: 5286433 Packets: 11915
+Bytes: 3591635 States: 0 ] block drop in quick on ! bge0 inet from
+82.208.36.0/24 to any [ Evaluations: 5380490 Packets: 0 Bytes: 0
+States: 0 ] block drop in quick on ! bge0 inet from 82.208.36.71 to any
+[ Evaluations: 105972 Packets: 0 Bytes: 0 States: 0 ] block drop in
+quick on ! bge0 inet from 82.208.36.72 to any [ Evaluations: 105972
+Packets: 0 Bytes: 0 States: 0 ] block drop in quick on ! bge0 inet from
+82.208.36.73 to any [ Evaluations: 105972 Packets: 0 Bytes: 0 States: 0
+] block drop in quick inet from 82.208.36.70 to any [ Evaluations:
+5380490 Packets: 0 Bytes: 0 States: 0 ] block drop in quick inet from
+82.208.36.71 to any [ Evaluations: 2434485 Packets: 0 Bytes: 0 States:
+0 ] block drop in quick inet from 82.208.36.72 to any [ Evaluations:
+2434485 Packets: 0 Bytes: 0 States: 0 ] block drop in quick inet from
+82.208.36.73 to any [ Evaluations: 2434485 Packets: 0 Bytes: 0 States:
+0 ] block drop in quick on ! lo0 inet6 from ::1 to any [ Evaluations:
+2434485 Packets: 0 Bytes: 0 States: 0 ] block drop in quick on ! lo0
+inet from 127.0.0.0/8 to any [ Evaluations: 2434485 Packets: 0 Bytes: 0
+States: 0 ]
```

Podstatně důležitější informace poskytuje výpis špatných přihlášení. Pokud by docházelo ke slovníkovému útoku nebo útoku hrubou silou, projevilo by se to zde.

```
elsa.eurofinancial.cz login failures:
Aug 13 22:51:45 elsa sshd[19140]: Invalid user share.nejvic.in from 89.176.74.115
Aug 13 22:53:03 elsa sshd[19202]: Invalid user share.nejvic.in from 89.176.74.115
Aug 13 22:54:00 elsa sshd[19205]: Invalid user share.nejvic.in from 89.176.74.115
```

V předešlém příkladu se jistě nejednalo o nějaký útok. Následující výpisy naznačují, že se jedná o útok na neexistující uživatelská jména. Pro tento výpis bylo záměrně po nějakou dobu vyřazeno z provozu pravidlo packet filteru povolující přihlášení přes SSH pouze u českých IP adres. Jak se předpokládalo, útok začal několik minut po otevření přístupu v 1:31:17 a trval do 2:03:43 z IP 83.170.105.142. Další se objevil v 12:06:04 a trval do 14:45:50 z IP 195.56.172.196. Bylo zaznamenáno ještě několik menších útoků, ale tyto dva byly největší.

```
retezat.tovarna.cz login failures:
Aug 13 01:31:17 retezat sshd[33111]: Invalid user ftp from 83.170.105.142
Aug 13 01:31:18 retezat sshd[33113]: Invalid user ftpuser from 83.170.105.142
Aug 13 01:31:18 retezat sshd[33115]: Invalid user mail from 83.170.105.142
Aug 13 01:31:18 retezat sshd[33117]: Invalid user user from 83.170.105.142
Aug 13 01:31:19 retezat sshd[33119]: Invalid user mailer from 83.170.105.142
Aug 13 01:31:19 retezat sshd[33121]: Invalid user office from 83.170.105.142
Aug 13 01:31:20 retezat sshd[33123]: Invalid user service from 83.170.105.142
Aug 13 01:31:21 retezat sshd[33127]: Invalid user info from 83.170.105.142
Aug 13 01:31:21 retezat sshd[33129]: Invalid user mailtest from 83.170.105.142
Aug 13 01:31:22 retezat sshd[33131]: Invalid user admin from 83.170.105.142
Aug 13 01:31:22 retezat sshd[33133]: Invalid user secretariat from 83.170.105.142
Aug 13 01:31:23 retezat sshd[33135]: Invalid user xfs from 83.170.105.142
Aug 13 01:31:24 retezat sshd[33139]: Invalid user lp from 83.170.105.142
Aug 13 01:31:24 retezat sshd[33141]: Invalid user rpc from 83.170.105.142
Aug 13 01:31:24 retezat sshd[33143]: Invalid user rpcuser from 83.170.105.142
Aug 13 01:31:25 retezat sshd[33147]: Invalid user list from 83.170.105.142
Aug 13 01:31:26 retezat sshd[33149]: Invalid user irc from 83.170.105.142
Aug 13 01:31:26 retezat sshd[33151]: Invalid user vpopmail from 83.170.105.142
Aug 13 01:31:27 retezat sshd[33153]: Invalid user services from 83.170.105.142
Aug 13 01:31:28 retezat sshd[33159]: Invalid user carlos from 83.170.105.142
Aug 13 01:31:29 retezat sshd[33161]: Invalid user nscd from 83.170.105.142
```

V případě, že by spojení se serverem bylo odmítnuto, bude následovat výpis. V tom případě k žádnému odmítnutí nedošlo.

```
elsa.eurofinancial.cz refused connections:

Checking for a current audit database:
Database created: Mon Aug 13 02:40:01 CEST 2007
```

Většina aplikací se neobejde bez bezpečnostních chyb. Ty jsou ovšem aktualizovány v co možná nejkratším čase. Informace o chybách ve verzích balíčků jsou porovnávány z databází. U každé chyby je uvedena www adresa, která o ní podává informace.

Vypadá to asi takto:

```
Checking for packages with security vulnerabilities:

Affected package: php5-session-5.1.4
Type of problem: php -- multiple vulnerabilities.
Reference: <http://www.FreeBSD.org/ports/portaudit/f5e52bf5-fc77-11db-8163-
000e0c2e438a.html>

Affected package: php5-5.1.4
Type of problem: php -- multiple vulnerabilities.
Reference: <http://www.FreeBSD.org/ports/portaudit/f5e52bf5-fc77-11db-8163-
000e0c2e438a.html>

Affected package: php5-session-5.1.4
Type of problem: php -- multiple vulnerabilities.
Reference: <http://www.FreeBSD.org/ports/portaudit/7fcf1727-be71-11db-b2ec-
000c6ec775d9.html>

3 problem(s) in your installed packages found.

You are advised to update or deinstall the affected package(s) immediately.
```

Z požadavku na detailnější výpis z tabulek packet filteru byl Miroslavem Lachmanem napsán další skript s názvem pftables.sh. Skript každý den vypisuje IP adresy z definovaných tabulek (badguys, goodguys a bruteforce), pokud není určená žádná, vypisuje se ze všech. Získaná data ukládá do souborů v adresáři /var/log. Jeden soubor náleží jedné tabulce. Následující den provede tu samou činnost, porovná rozdíly pomocí programu diff, a pokud nastala změna oproti předchozímu dni, vypíše rozdíl a zašle ho emailem. V následujícím příkladu je patrné, že došlo ke změně v tabulce goodguys.

```
Checking content of PF tables:
No ALTQ support in kernel
ALTQ related functions disabled

elsa.eurofinancial.cz host changes in table goodguys    (total        4 IP):
--- /var/log/pf_table_goodguys.today      Sun Jun 24 03:04:48 2007
+++ /tmp/security.0Jm5sesX  Tue Aug 14 03:05:14 2007
@@ -1,3 +1,4 @@
    82.208.41.41
+   213.220.192.200
    213.220.192.218
    217.11.225.101

-- End of security output --
```

Stejně jako v předešlých výpisech je security run output možno doplnit o další vlastní skripty, případně je doinstalovat z portů. Bezpečnostní výpis je úzce spjat s výpisem denním a jsou generovány a zasílány současně.

4.1.5 MySQL error log

Skript `350.mysql_error_log.sh` není obsažen v periodic. Byl napsán z důvodu potřeby výpisu chybových hlášek MySQL a patří do denního výpisu periodic. Na rozdíl od ostatních skriptů zasílá zprávy separátně.

Jeho funkcí je vytvořit denně kopii mysql error logu. Porovnává současnou a předešlou verzi a rozdíl zasílá administrátorovi. Ne na všech serverech je nastavena rotace mysql logu, proto se výpisy ze serverů liší.

Na serveru amanda.refresh.cz vypadá tento výpis následovně:

```
Status information:

Current dir: /var/db/mysql/
Running threads: 2  Stack size: 196608
Current locks:
lock: 0xbb03224:
lock: 0xbb6ce24:
lock: 0xbbdca24:

Key caches:                             handler status:
Default                                 read_key:       771984
Buffer_size:      67108864              read_next:     5571032
Block_size:           1024              read_rnd             0
Division_limit:        100              read_first:       3241
Age_limit:             300              write:          764721
blocks used:           115              delete               0
not flushed:             0              update:              0
w_requests:              0
writes:                  0
r_requests:        1720527
reads:                 554

Table status:                           Alarm status:
Opened tables:       5701               Active alarms:   2
Open tables:          128               Max used alarms: 9
Open files:           189               Next alarm time: 464
Open streams:           0
```

Podle tohoto výpisu je zřejmé, že na serveru není žádná chyba a v závěru jsou uvedeny kompletní statistiky. K hlášení lock dochází právě při zmíněné rotaci logu

Na serveru retezat.cz přichází pouze chybové hlášky nebo rozdílové zprávy například:

```
070724  9:20:05 [ERROR] Slave: Error 'Duplicate entry '14ondo1nq68kaj5o9qu6cfiv37'
for key 1' on query. Default database: 'retezatcz'. Query: 'INSERT INTO
sessionValue(sessionId,value,timestamp,valid)
VALUES('14ondo1nq68kaj5o9qu6cfiv37','download|i:1;','1185261605','1185264005')',
Error_code: 1062
070724  9:20:05 [ERROR] Error running query, slave SQL thread aborted. Fix the
problem, and restart the slave SQL thread with "SLAVE START". We stopped at log
'indy-bin.000151' position 1047636548
```

Zde je vidět, že došlo ke špatné synchronizaci mezi primární a sekundární databází. Problém se řeší manuálně pomocí sql příkazů. Je nutné doplnit chybějící záznamy nebo případně smazat záznamy přebývající v sekundární databázi. Přesné řešení toho případu i s SQL dotazy je uvedeno v příloze 11.

4.2 SPOUŠTĚNÍ SKRIPTŮ POMOCÍ CRONU

Cron je *NIXový systémový nástroj, který spouští různé programy v předem definované době a v daném intervalu (jeho obdobou jsou naplánované úlohy ve Windows).

Pokud je rozhodnuto, že cron bude využívat více uživatelů, je dobré si promyslet, kteří získají přístup k této službě a kteří nikoliv. Standardně k němu mají přístup všichni uživatelé.

Pří omezení na určité uživatele, je jejich přístup vázán na soubory `/var/cron/allow` a `/var/cron/deny`. Jak již název napovídá, jedná se o soubory, kde se buď přístup povoluje, nebo zakazuje. Pokud je povolen přístup jen uživateli `pokus` a `pokus2`, napíší se do souboru `allow` jejich uživatelská jména. Každé na jeden řádek. Tím je všem ostatním uživatelům přístup ke cronu zakázán. Pokud má být výše uvedeným uživatelům přístup zakázán a ostatním povolen, uvedou se jejich uživatelská jména do souboru `deny`. Stejně jako u předchozího souboru se píše jeden uživatel na jeden řádek. Samozřejmě uvedená uživatelská jména by měla v systému existovat. Při neexistenci těchto souborů bude mít ke cronu přístup pouze root.

Mimo skriptů, které se mají spouštět, je důležitý také čas spuštění. Jelikož cron spouští definované aplikace vždy v předem určeném intervalu, nelze ho použít pouze

k jednorázovému spuštění. Minimální interval, po kterém je možno aplikaci znovu spustit je 1 minuta.

K nastavení časování slouží utilita crontab. Spravuje seznam úloh, které má cron vykonávat. Uživatelé si rovněž mohou definovat vlastní tabulky pro cron, ty jsou uloženy ve `/var/cron/tabs/jmeno_uzivatele` podle jména uživatele z `/etc/passwd`. Pro uživatelskou práci s crontab se používají příkazy `crontab -e` a `crontab -l` pro vypsání tabulky.

Systémová tabulka cron, `/etc/crontab`, se podobá uživatelským tabulkám, ale umožňuje definovat i uživatele, pod jehož privilegii daný proces poběží. Soubor `/etc/crontab` na svém začátku obsahuje definici proměnných prostředí a pak již tabulky pro procesy. Základní tabulka ve FreeBSD vypadá následovně:

```
# /etc/crontab - root's crontab for FreeBSD
# $FreeBSD: src/etc/crontab,v 1.32 2002/11/22 16:13:39 tom Exp $
SHELL=/bin/sh
PATH=/etc:/bin:/sbin:/usr/bin:/usr/sbin
HOME=/var/log
#minute hour  mday  month  wday  who      command
*/5     *     *     *      *     root     /usr/libexec/atrun
# Save some entropy so that /dev/random can re-seed on boot.
*/11    *     *     *      *     operator /usr/libexec/save-entropy
# Rotate log files every hour, if necessary.
0       *     *     *      *     root     newsyslog
# Perform daily/weekly/monthly maintenance.
1       3     *     *      *     root     periodic daily
15      4     *     *      6     root     periodic weekly
30      5     1     *      *     root     periodic monthly
# Adjust the time zone if the CMOS clock keeps local time, as opposed
# to UTC time.  See adjkerntz(8) for details.
1,31    0-5   *     *      *     root     adjkerntz –a
```

4.2.1 Reboot

Reboot počítače může být buď cílený, nebo samovolný. U cíleného je převážně z důvodů aktualizace celého systému nebo zamrznutí nějaké služby, jejíž znovu nastartování není možné provést přes SSH a která blokuje celý systém.

Samovolný reboot není tak častý a dochází k němu při výpadcích proudu v serverovně. Většina těchto serveroven má sice záložní napájení nebo agregáty generující elektrický proud, ale i ten může občas vysadit.

O těchto skutečnostech je administrátor informován pomocí emailu zasílaného přes cron. Příkaz k zaslání je zanesen v tabulce uživatele pomocí příkazu `crontab –e` následovně:

```
#minute       hour   mday   month  wday   command

@reboot echo "`hostname` rebooted, up at `date`" | mail -s "`hostname` rebooted, up at `date`" mail@zdenekcejka.net
```

Struktura emailu potom vypadá:

```
From: cejkon@amanda.refresh.cz
To: mail@zdenekcejka.net
Subject: amanda.refresh.cz rebooted, up at Mon Aug 13 20:38:02 CEST 2007
```

Podle těchto informací má administrátor možnost poznat, kdy konkrétně k rebootu došlo a pokud byl reboot nečekaný, kontaktovat osoby zodpovědné za správu serverhostingových místností.

4.3 MRTG (MULTI ROUTER TRAFFIC GRAPHER)

Každý server je monitorován jak pomocí textových zpráv zasílaných emailem, tak pomocí grafů zobrazujících vytížení služeb na serveru, procesoru, přístupu k webovému serveru Apache a mnoho dalších.

K tomuto měření a následnému zobrazování statistik se používá nástroj MRTG (Multi Router Traffic Grapher). Jedná se o monitorovací nástroj síly vytížení na síťových linkách. Jeho vlastnosti však umožňují monitorovat prakticky jakoukoliv službu běžící na serveru. Je napsán v PERLu. Jeho funkčnost není omezena na konkrétní operační systém, proto poskytuje stejně kvalitní výstupy na UNIX/Linux OS, Microsoft Windows i na Netware systémech.

Ukázka mužností MRTG bude prezentována na výstupech ze serveru retezat.tvarna.cz.

Na úvodní stránce je zobrazen přehled všech součástí systému, které se graficky monitorují. Každý graf v sobě skrývá odkaz, po jehož otevření následuje detailnější zobrazení. Veškeré intervaly jsou zobrazovány zpětně po určitou dobu tedy denně, týdně, měsíčně a ročně.

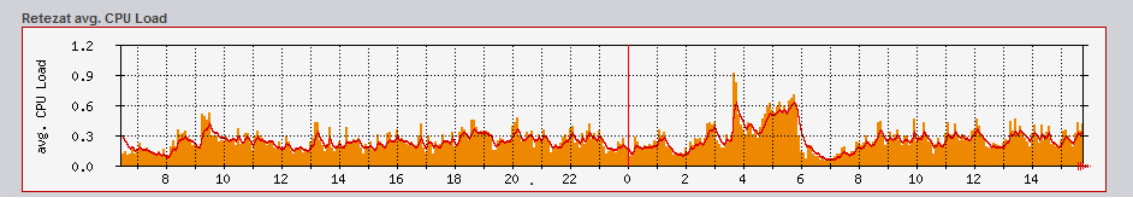
Veškeré informace je nutno porovnávat v určitém časovém horizontu. Časová posloupnost a provázanost s ostatními grafy poskytuje přehled o chování systému.

4.3.1 CPU

První graf zobrazuje vytížení procesoru. Při dlouhodobé vysoké zátěži procesoru se může jednat o kompilaci nebo nějaký proces pořád zůstává spuštěn, i když by neměl, a zabírá výkon procesoru. Zátěž není počítána v procentech, ale je udávána v LOAD.

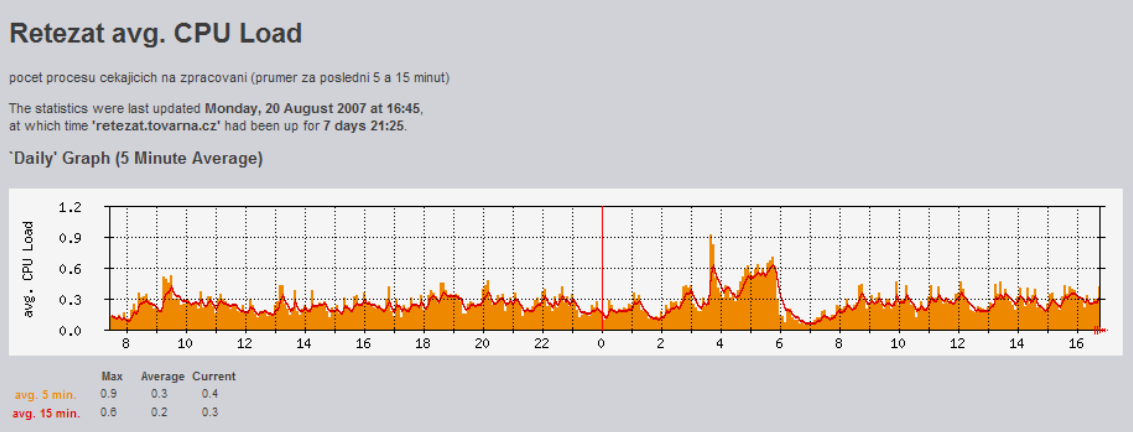
Load vyjadřuje množství práce, které systém právě provádí. Pokud tedy bude load činit 3,12, ude se jednat o 212% přetížení. Do toho čísla jsou v UNIXových systémech započítávány procesy, které právě využívají procesor nebo na něj čekají.

Zátěž serveru se tedy liší a nelze jednoznačně říct, jaký stav je správný. Tento fakt lze ozřejmit sledováním grafu v delším časovém úseku. U serveru elsa.eurofinancial.cz se pohybuje průměrný load CPU pod 1, kdežto na jiném serveru se může průměrný load pohybovat kolem 3.



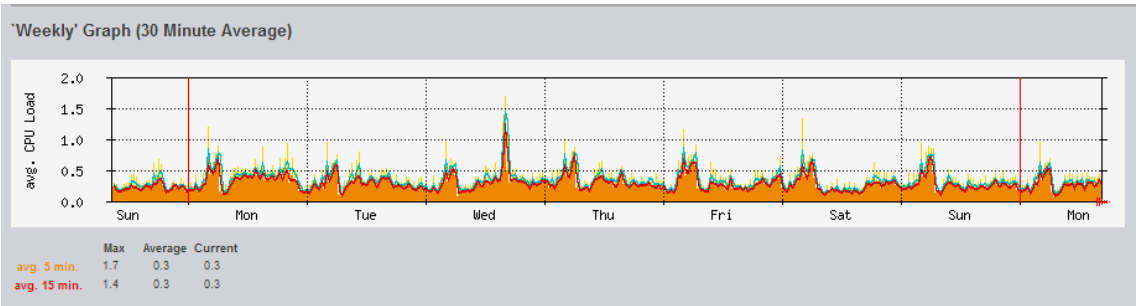
Detailní statistiky:

Denní statistika je totožná s grafem na úvodní stránce, ale poskytuje i popisky použitých barev na grafu.

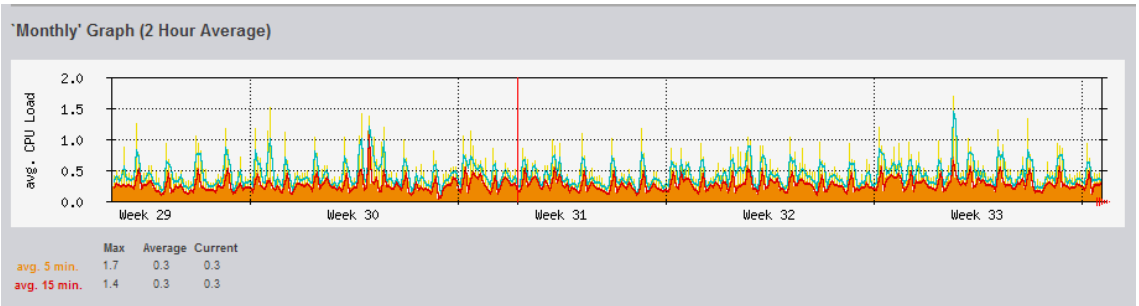


Týdenní výpis popisuje load procesoru v průběhu jednoho týdne. Na tomto výpisu je vidět, že vytížení procesoru se opakuje v pravidelných intervalech. Pokud by

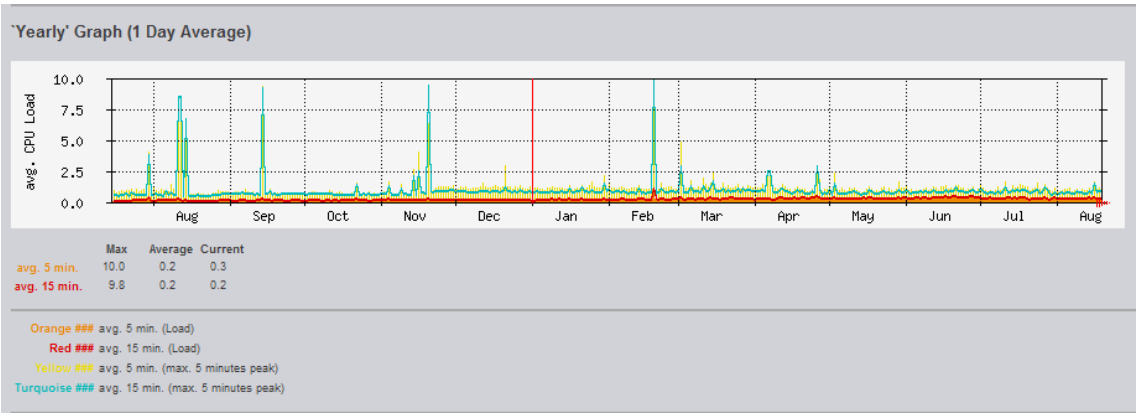
byl zaznamenán vyšší výkyv, je nutné prověřit prozkoumáním logů a zjistit, co se v té době dělo. V tomto případě se jednalo o kompilaci nové verze courier-imap serveru.



Měsíční graf je už převážně informativní. Zde z něj vyčíst, jak byl procesor vytížen v rozmezí jednoho měsíce.



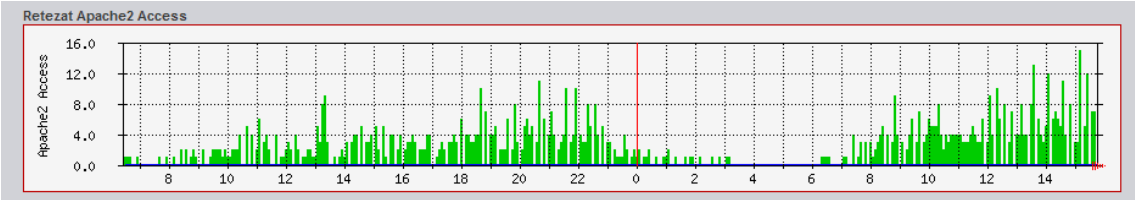
Roční výpis pouze sumarizuje všechny předešlé informace. Jak je patrné v létě minulého roku je vytížení procesoru vyšší než jindy. V té době probíhal upgrade systému a vysoký load způsobovalo kompilování aplikací.



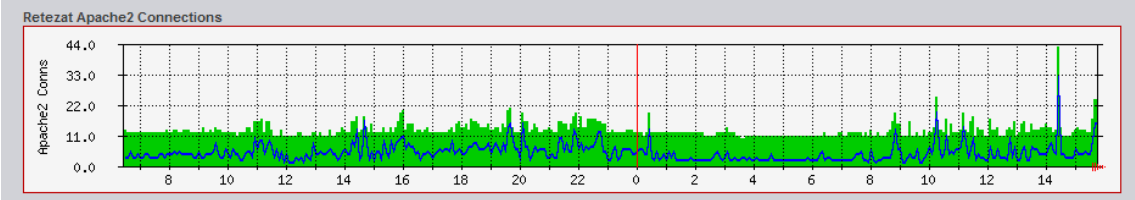
4.3.2 Apache2

Pro monitorování webového serveru Apache2 jsou použity dva grafy.

První nese název Retezat Apache2 Access. Zobrazuje počet požadavků přicházejících na server za dobu jedné vteřiny a datový přenos v MB/s.



Druhý má jméno Retezat Apache2 Connections. Jeho smyslem je podávat informace o počtu procesů Apache a počtu aktivních procesů.

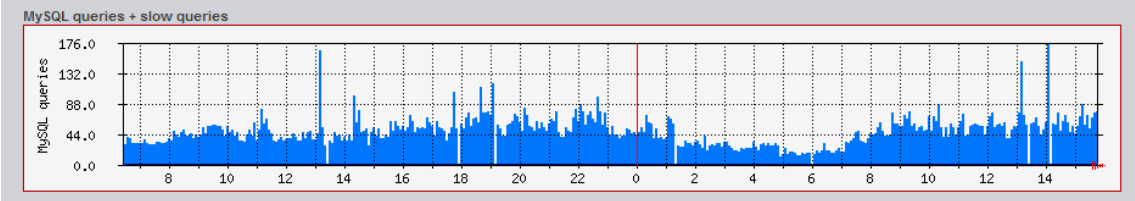


Detailním zobrazením se dá opět určit, v jakých intervalech se výkyvy pohybují. Sama o sobě jsou tato data zbytečná. Uchovávají se převážně z hlediska mapování minulých období. Z těchto dat je možné říci, že po určité době nebo po nasazení konkrétního projektu se vytížení Apache 2 zvýšilo či snížilo.

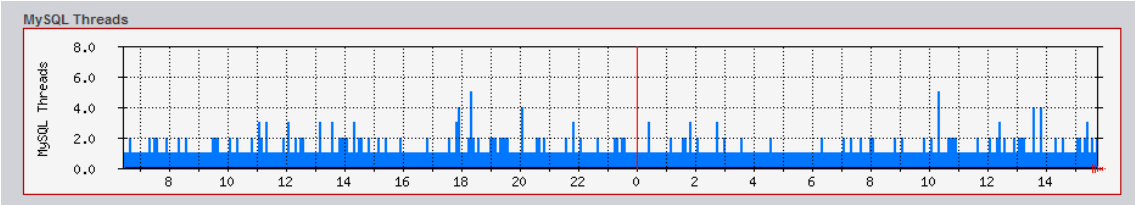
Kompletní statistika je uvedena v přílohách 13 a 14.

4.3.3 MySQL

Jako u Apache jsou pro MySQL použity dva grafy. První se vztahuje k počtu dotazů směřujících k databázi



a druhý k počtu vláken.

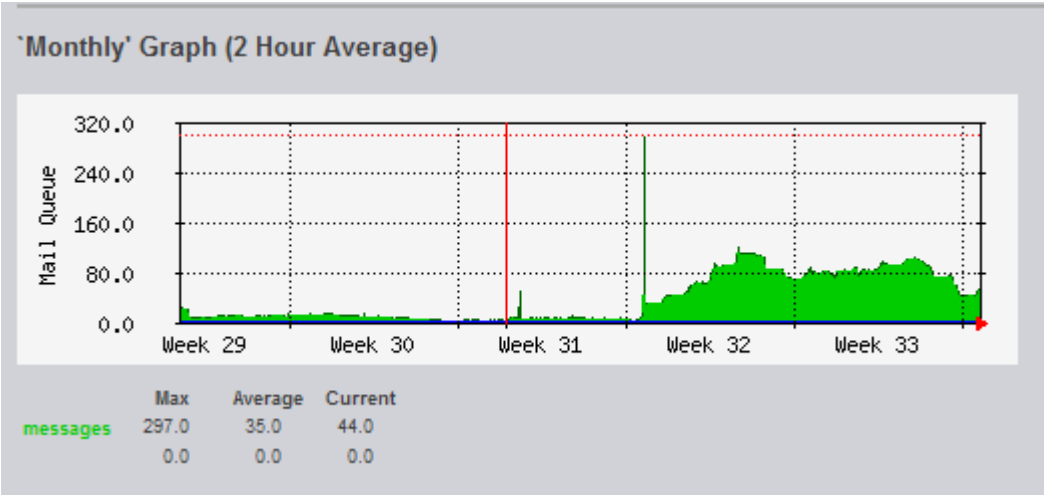


Při ročním porovnání (viz příloha 15 a 16 Yearly' Graph) je patrné, že počet dotazů stoupá, ale počet vláken v dubnu klesl. Nastalo tak v důsledku zvyšování počtů webových prostor a zároveň spuštění serveru ararat.tovarna.cz, na který se přesunuly veškeré emailové služby z retezat.tovarna.cz.

4.3.4 Mail Queue

Zobrazuje počet emailů, které čekají ve frontě na odeslání obdobně, jak to udává výpis poskytovaný daily periodic. Z grafického vyjádření lze vyčíst, kdy se zvýšil počet odesílaných emailů.

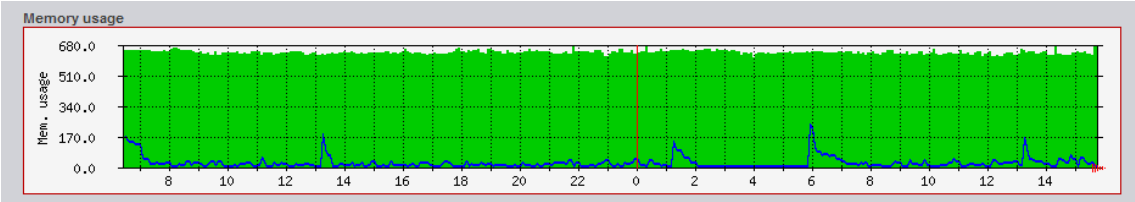
V tomto případě není uveden graf nacházející se na úvodní stránce serveru retezat.tovarna.cz, ale měsíční graf serveru roxy.refresh.cz.



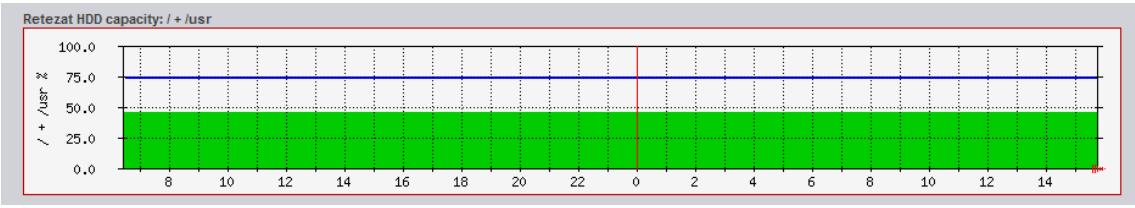
Je patrné, že ve 32. a 33. týdnu rapidně vrostl počet emailů ve frontě. V tomto případě se jednalo o spuštění nového mailinglistu. Pokud by se ale tento výkyv objevil bez sebemenších příčin, mohlo by se stát, že příslušný server rozesílá spam nebo je přes něj alespoň rozesílán.

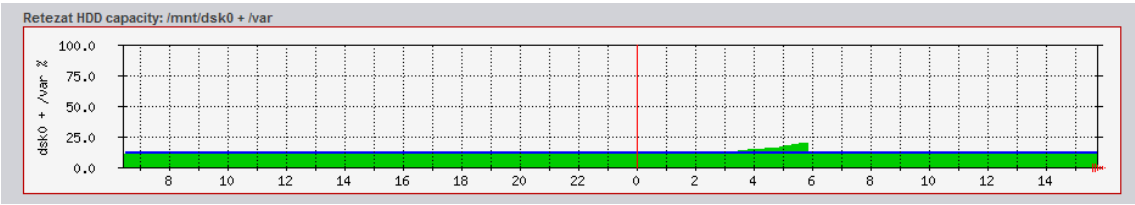
4.3.5 Systémové informace

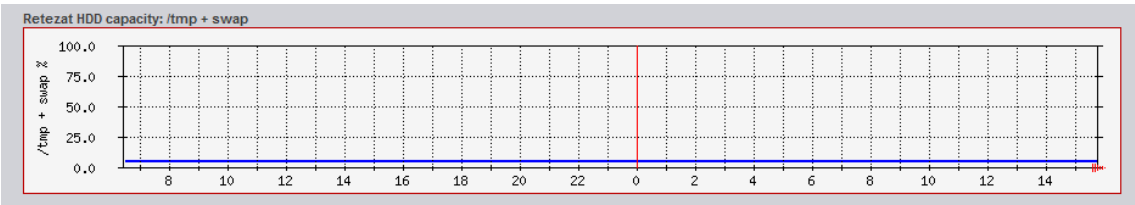
V úvodu informací o systému je možno nalézt informace o využití fyzické paměti.



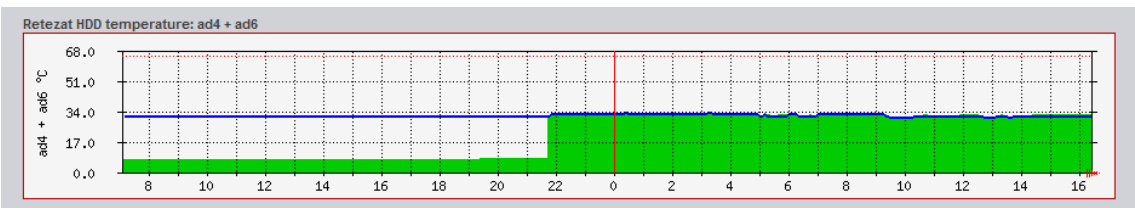
Následně je zobrazeno procentuální zaplnění diskových oddílů. Tato data jsou zasílána v denním výpisu skriptu periodic. Jsou sice podrobnější, ale z grafu lze naopak vyčíst, v jakém období se oddíly plnily a porovnat jejich přírůstky a úbytky. Obě tyto části tedy dávají lepší informace, jak z detailního tak časového pohledu.





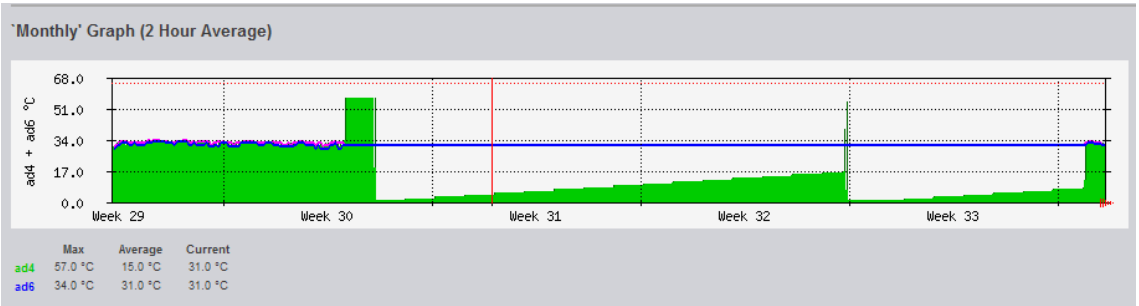


Pokud se jedná o disky, je nutné zachytit i jejich teplotu. K tomu slouží graf s názvem Retezat HDD temperature: ad4 + ad6.

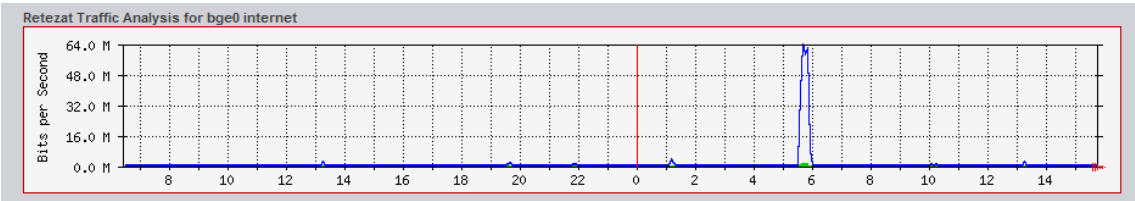


Jak je patrné z grafu, od 22. hodiny byl zaznamenáván veliký teplotní rozdíl mezi oběma disky. Jeden mel průměrnou teplotu okolo 8°C a druhý okolo 31°C.

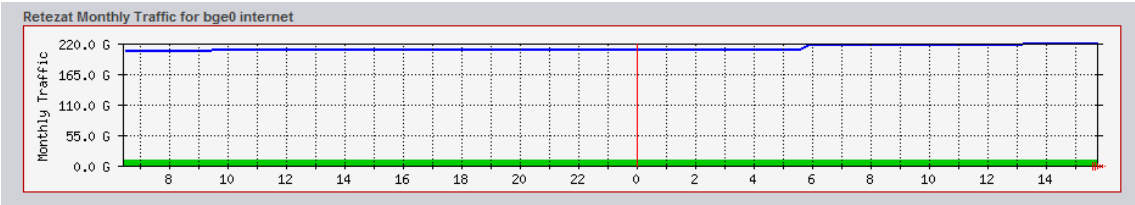
Z měsíčního grafu plyne, že problém nastal před třemi týdny. Byl způsoben nesprávnou funkcí deamona smartmontools. Řešením bylo update smartmontools na novou verzi a tím pádem došlo i k jeho restartu. Po těchto úkonech již vykreslování funguje.



Poslední zobrazovaným grafem je statistika síťových prvků. V základním přehledu jsou uvedeny dva grafy. První z nich udává aktuální přenosovou rychlost



a druhý objem dat přenesených v období jednoho měsíce. Po této době se data vynulují.



Kompletní přehled grafů zobrazovaných pomocí MRTG (Multi Router Traffic Grapher) viz přílohy 12-25.

5 ZÁVĚR

Monitoring serveru je individuální záležitost. Nejde obecně říci, co je postačující a co zbytečné. Pokud by přicházely data pouze v textové podobě, bylo by složité je správně roztřídit a zpětně dohledávat potředné informace. Pomocí grafického znázornění stavu systému je tento krok jednodušší. Takto koexistence zaručuje dostatečný přehled o chování jak běžících služeb a aplikací, tak celého systému.

V tomto případě jsem došel k závěru, že nastavení služeb je pro jejich základní správnou funkci dostatečné. Další specifikace využívaných služeb závisí na požadavku klienta. Případná donastavení nebo úpravy lze provádět bez závažnějších problémů za plného běhu systému. Důsledkem přenastavování mohou být chvilkové výpadky upravované služby, ale takováto opatření se většinou provádí v nočních hodinách za malého vytížení systému. Problémy mohou nastat při přechodu na novější verzi, kde jsou v určitých připadech použity odlišné syntaxe konfiguračního souboru, než ve verzi předešlé. Rozdíl v syntaxích může zapříčinit případné nespuštění služby nebo nesprávnou funkčnost. To se však stává velice zřídka. U některých aplikací lze použít výchozí konfigurační soubor nabízený operačním systémem pro usnadnění práce s nastavením a redukci případných chyb.

Při monitorování pomocí emailových zpráv se převážně využívá monitorovacích služeb poskytovaných systémem FreeBSD. V určitých případech služby neposkytují informace potřebné k detailnímu sledování, proto je nutné si některé skripty sám napsat nebo využít již vytvořených. U vypůjčených skriptů je potřeba dodržovat licence, pod kterými jsou napsány. Žádný z půjčených skriptů, použitých v popisovaném monitorovacím systému, nebyl komerčního charakteru a tudíž po svolení autora a dodržení podmínek příslušné licence, je šlo použít.

Nástroj pro grafické zobrazení Multi Router Traffic Grapheru (MRTG) poskytuje velkou variabilitu. Jeho funkce umožňují libovolné nastavení zobrazení sledovaných procesů podle uvážení administrátora. Výstupy je potřeba sledovat v delších časových úsecích - tedy dnech, týdnech nebo měsících. Při vykreslování dat se mohou vyskytnout i chyby, jak jsem ukázal na grafickém znázornění teploty disku v kapitole 4.3.5. To ovšem nezpůsobil MRTG vykreslující pouze data, která dostával. Problém spočíval v nesprávné funkci aplikace smartmontools, která poskytuje informace ze

S.M.A.R.T. (Self-Monitoring, Analysis, and Reporting Technology) rozhraní pro jednotlivé pevné disky.

Došel jsem k závěru, že při zavádění opatření na servery s operačním systémem FreeBSD nedochází k žádným potížím. Zasílaná data jsou interpretována v takové podobě, jakou lze najít v logu příslušné služby nebo aplikace. Problémy nastávají ve fázi nefunkčnosti poštovního serveru, který emaily s informacemi zasílá.

Jelikož zprávy přicházejí v určitém opakujím se cyklu, je možné tento problém ihned odhalit. Obdobný problém nastává u MRTG. Ten je vázán na webový server Apache, PHP a databázi MySQL. Při jejich jakékoliv nefunkčnosti nebo výpadku nelze dostat z MRTG smysluplná data. V tomto ohledu se nedá předpokládat žádné zlepšení a je nutné počítat s případnými problémy, které mohu nastat za běhu systému. K jejich odhalování monitorovací programy slouží.

6 SEZNAM ZDROJŮ

1. kolektiv autorů, oficiální dokumentace k FreeBSD <questions@FreeBSD.org>. 19. 8. 2006. <http://www.freebsd.org/docs.html>
2. LUCAS, Michael – FreeBSD ,Podrobný průvodce síťovým operačním systémem. Brno: ComputerPRESS, 2003
3. HILDEBRANDT, Ralf a KOETTER, Patrick – Postfix, Provozujeme poštovní server v Linuxu. Brno: ComputerPRESS, 2006
4. kolektiv autorů - PHP5, MySQL, Apache, Vytváříme webové aplikace. Brno: CompterPRESS, 2006
5. KABIR, Mohammed J. - Apache Server 2, Kompletní příručka administratora. Brno: ComuterPRESS, 2006
6. POŠMURA, Vlastimil – Apache, Příručka správce WWW serveru. Brno: ComputerPRESS, 2002
7. DELISLE, Marc - phpMyAdmin - efektivní správa MySQL. ZonerPress, 2004
8. SCHNEIDER, Roland <list-courier@serv.ch>, PRICE, Patrick <sysadmin@moment.net> - Courier Documentation, 30. 10 2006, <http://www.courier-mta.org/documentation.html>
9. LOWES, Mark. Proftpd - A User's Guide. c2001, 16. 5. 2007 <http://www.proftpd.org/localsite/Userguide/linked/userguide.html>
10. LYNCH, Patrick a kolektiv. Referenční manuál [online], 30. 10. 2006. <http://dev.mysql.com/doc/>
11. JOY, William. Manuálové stránky pro csh shell. http://www.mkssoftware.com/docs/man1/csh.1.asp , 30. října 2006
12. ŽÁK, Karel < zakkr@zf.jcu.cz>. *Historie OS UNIX* [online]. c2001, poslední revize 28. 6. 2001 [cit. 2007-05-20]. <http://www.root.cz/clanky/historie-os-unix/>.
13. HUBBARD, Jordan. *A Brief History of FreeBSD, FreeBSD Handbook* [online]. Last revision 14.5.2007. <http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/history.html>.
14. BUDAI, David. *Nevyzpytatelné a nebezpečné útoky typu DoS* [DigiWeb, online]. 19.07.2007. <http://digiweb.ihned.cz/c6-10053280-21651030-i00000_d-nevyzpytatelne-a-nebezpecne-utoky-typu-dos>

15. D. Rohleder. Bezpečnost v systémech UNIX. Zpravodaj ÚVT MU. ISSN 1212-0901, 1997, roč. VII, č. 4, s. 14-16.
16. *OpenSSH FAQ (Frequently asked questions)* [online]. 20. 9. 2005. <http://www.openssh.org/faq.html>
17. NORIS, Ivan <vix@deja-vix.sk>, *Príručka systémového administrátora, 1.9.2, kap 9. SSH (Secure Shell)* [online]. 2. 5. 2006, <http://deja-vix.sk/sysadmin/ssh.html>
18. MOURANI, Gerhard <gmourani@openna.com> *Securing and Optimizing Linux, RedHat Edition - A Hands on Guide* [online]. c2000, 17. 6. 2007. http://www.faqs.org/docs/securing/
19. KNIGHT, Joel. *PF: The OpenBSD Packet Filter* [online]. 21.5.2005. <http://www.openbsd.cz/faq/pf/index.html>
20. BEZDĚK, Petr <xbezdek@fi.muni.cz>. *FreeBSD firewall – IPFW* [online]. 29. 4. 2003. <http://www.fi.muni.cz/~kas/p090/referaty/2003-jaro/skupina10/fw-bsd.html>
21. YONGHYEON, Pyun <yongari@kt-is.co.kr>, LAIER, Max <mlaier@freebsd.org>. *FreeBSD packet filter (pf)* [online]. 9. 12. 2004. <http://pf4freebsd.love2party.net/>
22. YOCUM, Tim <tim@yocum.org>. *Postfix + TLS + SASL on FreeBSD* [online]. 22. 2. 2005. <http://yocum.org/faqs/postfix-tls-sasl.html>
23. *Postfix Configuration Parameters* [online]. 20. 7. 2007. <http://www.postfix.org/postconf.5.html>
24. BOXMAN, Jason <jasonb@edseek.com>. *Configuring Exim4 and Courier IMAP under Debian GNU/Linux* [online]. 19. 5. 2006. <http://edseek.com/~jasonb/articles/exim4_courier/courierimap.html>
25. LOWES, Mark. *Proftpd - A User's Guide* [online]. c2001, 23. 7. 2007. <http://www.proftpd.org/localsite/Userguide/linked/userguide.html>
26. BĚLKA, Jiří. *Začínáme bezpečně s FreeBSD (5)* [root.cz, online]. 20. 7. 2004. <http://www.root.cz/clanky/zaciname-bezpecne-s-freebsd-5/>
27. *FreeBSD Hypertext Man Pages* [online]. 6. 6. 1993. <http://www.freebsd.org/cgi/man.cgi?query=rwho&sektion=1>
28. *Tobi Oetiker's MRTG - The Multi Router Traffic Grapher*, 16. 8. 2007 <http://oss.oetiker.ch/mrtg/>

7 PŘÍLOHY

Příloha 1. pf.conf - konfigurační soubor Packet Filteru
Příloha 2. main.cf - konfigurační soubor aplikace POSTFIX
Příloha 3. master.cf - konfigurační soubor aplikace POSTFIX
Příloha 4. proftpd.conf - konfigurační soubor FTP serveru ProFTPd
Příloha 5. httpd.conf - konfigurační soubor aplikace Apache 2
Příloha 6. periodic.conf - konfigurační soubor služby periodic
Příloha 7. smartctl.sh - skript začleněný do týdenního výpisu periodic
Příloha 8. Daily run output
Příloha 9. Weekly run output
Příloha 10. Monthly run output
Příloha 11. Řešení problému synchronizace primární a sekundární MySQL databáze
Příloha 12. Úvodní výstup z MRTG
Příloha 13. Detailní výstup z MRTG pro Apache 2 Access
Příloha 14. Detailní výstup z MRTG pro Apache 2 Connections
Příloha 15. Detailní výstup z MRTG pro MySQL Queries
Příloha 16. Detailní výstup z MRTG pro MySQL Threads
Příloha 17. Detailní výstup z MRTG pro Mail Queue
Příloha 18. Detailní výstup z MRTG pro Využití paměti RAM
Příloha 19. Detailní výstup z MRTG pro Využití oddílu disku připojeného k / a /usr
Příloha 20. Detailní výstup z MRTG pro Využití oddílu disku připojeného k /mnt/dsk0 a /var
Příloha 21. Detailní výstup z MRTG pro Využití oddílu disku připojeného k /tmp a odkládací oddíl swap
Příloha 22. Detailní výstup z MRTG pro Uptime
Příloha 23. Detailní výstup z MRTG pro Výpis teploty disků
Příloha 24. Detailní výstup z MRTG pro Rychlost přenosu dat na zařízení bg0 (síťová karta)
Příloha 25. Detailní výstup z MRTG pro Objem přenesených dat na zařízení bg0 (síťová karta)

Příloha 1. pf.conf - konfigurační soubor Packet Filteru

MACROS

```
ext_if="ed0"  # actual external interface name i.e., dc0
ext_addr_0="192.168.1.10"   # primary IP of ext. interface (later allow SSH
connection from czech_net) - maintainance only
ext_tcp_0_inports="{ 21, 25, 80, 110, 143, 443, 993, 995 }"
ext_ssh_0="22"       # port on which sshd listen - restricted IPs
ext_addr_1="192.168.1.10"
ext_tcp_1_inports=""
ext_ssh_1="22"       # port on which sshd listen - all czech IPs
ext_addr="{" $ext_addr_0 $ext_addr_1 "}"
unfiltered="{ lo0 }"

## TABLES
table <reserved> { 172.16.0.0/12, 10.0.0.0/8, 127.0.0.0/8, 0.0.0.0/8,
169.254.0.0/16, 192.0.2.0/24, 204.152.64.0/23, 224.0.0.0/3 }
table <czech_net> persist file "/etc/pf.czech_net.table"
table <goodguys> persist file "/etc/pf.goodguys.table"
table <badguys> persist file "/etc/pf.badguys.table"
table <bruteforce> persist
table <ssh_bruteforce> persist

## OPTIONS
set timeout { interval 10, frag 20 }
set limit { states 10000, frags 5000 }
set optimization aggressive
set block-policy drop
set skip on $unfiltered

## NORMALIZATION
scrub in on $ext_if
scrub out on $ext_if no-df random-id min-ttl 24 max-mss 1492

## FILTER
pass in quick proto tcp from <goodguys> to any port $ext_ssh_0 flags S/SA keep
state
block in quick from { <badguys>, <bruteforce>, <ssh_bruteforce> } to any
block quick inet6 all
block
block quick on $ext_if inet from <reserved> to any
block quick on $ext_if inet from any to <reserved>

pass in log on $ext_if proto tcp from <czech_net> to $ext_addr_1 port $ext_ssh_1
flags S/SA keep state \
       (max-src-conn 5, max-src-conn-rate 3/30, overload <ssh_bruteforce> flush
global)
pass out quick on $ext_if inet proto icmp icmp-type 8 code 0 keep state
pass in quick on $ext_if inet proto icmp icmp-type 8 code 0 keep state
pass out on $ext_if inet proto udp keep state

pass out on $ext_if inet proto tcp from $ext_if to any flags S/SA modulate state
pass in on $ext_if inet proto tcp from any to $ext_addr_0 port $ext_tcp_0_inports
flags S/SA keep state
# passive FTP transfer - highports
pass in on $ext_if inet proto tcp from any to $ext_addr_0 port 55000 >< 56000 keep
state
```

Příloha 2 - main.cf - konfigurační soubor aplikace POSTFIX

```
queue_directory = /var/spool/postfix
command_directory = /usr/local/sbin
daemon_directory = /usr/local/libexec/postfix
mail_owner = postfix
mydomain = $myhostname
myorigin = $myhostname
mydestination = $myhostname, localhost.$mydomain, localhost
unknown_local_recipient_reject_code = 550
mynetworks_style = host
smtpd_banner = $myhostname ESMTP $mail_name
debug_peer_level = 2
debugger_command = PATH=/bin:/usr/bin:/usr/local/bin:/usr/X11R6/bin
        xxgdb $daemon_directory/$process_name $process_id & sleep 5
sendmail_path = /usr/local/sbin/sendmail
newaliases_path = /usr/local/bin/newaliases
mailq_path = /usr/local/bin/mailq
setgid_group = maildrop
html_directory = no
manpage_directory = /usr/local/man
sample_directory = /usr/local/etc/postfix
readme_directory = no
virtual_alias_maps = mysql:/usr/local/etc/postfix/mysql_virtual_alias_maps.cf
virtual_gid_maps = static:2125
virtual_mailbox_base = /var/spool/domains
virtual_mailbox_domains = mysql:/usr/local/etc/postfix/mysql_virtual_domains_maps.cf
virtual_mailbox_limit = 51200000
virtual_mailbox_maps = mysql:/usr/local/etc/postfix/mysql_virtual_mailbox_maps.cf
virtual_minimum_uid = 2125
virtual_transport = virtual
virtual_uid_maps = static:2125
virtual_create_maildirsize = yes
virtual_mailbox_extended = yes
virtual_mailbox_limit_maps =
mysql:/usr/local/etc/postfix/mysql_virtual_mailbox_limit_maps.cf
virtual_mailbox_limit_override = yes
virtual_maildir_limit_message = Sorry, the user's maildir has overdrawn his diskspace
quota, please try again later.
virtual_overquota_bounce = yes
relay_domains = mysql:/usr/local/etc/postfix/mysql_relay_domains_maps.cf
proxy_read_maps = $local_recipient_maps $mydestination $virtual_alias_maps
  $virtual_alias_domains $virtual_mailbox_maps $virtual_mailbox_domains
  $relay_recipient_maps $relay_domains $relocated_maps $transport_maps
  $virtual_mailbox_limit_maps
broken_sasl_auth_clients = yes
smtpd_sasl_auth_enable = yes
smtpd_sasl_local_domain = $myhostname
smtpd_sasl_security_options = noanonymous
#smtpd_sender_restrictions = permit_sasl_authenticated, permit_mynetworks
smtpd_recipient_restrictions =
       permit_mynetworks,
       permit_sasl_authenticated,
       reject_non_fqdn_sender,
       reject_non_fqdn_recipient,
       reject_unauth_destination,
       reject_unauth_pipelining,
       reject_invalid_hostname,
smtp_use_tls = yes
smtp_tls_note_starttls_offer = yes
smtpd_use_tls = yes
smtpd_tls_key_file = /usr/local/etc/ssl_cert/roxy.refresh.cz.key
smtpd_tls_cert_file = /usr/local/etc/ssl_cert/roxy.refresh.cz.crt
smtpd_tls_loglevel = 1
smtpd_tls_received_header = yes
smtpd_tls_session_cache_timeout = 3600s
smtpd_tls_auth_only = yes
tls_random_source = dev:/dev/urandom
local_transport = local
vacation_destination_recipient_limit = 1
message_size_limit = 10240000
```

Příloha 3 - master.cf - konfigurační soubor aplikace POSTFIX

```
# ==========================================================================
# service type  private unpriv  chroot  wakeup  maxproc command + args
#               (yes)   (yes)   (yes)   (never) (100)
# ==========================================================================
smtp      inet  n       -       n       -       -       smtpd
       -o receive_override_options=no_address_mappings
submission inet n       -       n       -       -       smtpd
       -o receive_override_options=no_address_mappings
       -o smtpd_enforce_tls=yes
       -o smtpd_client_restrictions=permit_sasl_authenticated,reject
smtps    inet  n       -       n       -       -       smtpd
       -o receive_override_options=no_address_mappings
       -o smtpd_tls_wrappermode=yes
       -o smtpd_client_restrictions=permit_sasl_authenticated,reject
pickup    fifo  n       -       n       60      1       pickup
cleanup   unix  n       -       n       -       0       cleanup
qmgr      fifo  n       -       n       300     1       qmgr
tlsmgr    unix  -       -       n       1000?   1       tlsmgr
rewrite   unix  -       -       n       -       -       trivial-rewrite
bounce    unix  -       -       n       -       0       bounce
defer     unix  -       -       n       -       0       bounce
trace     unix  -       -       n       -       0       bounce
verify    unix  -       -       n       -       1       verify
flush     unix  n       -       n       1000?   0       flush
proxymap  unix  -       -       n       -       -       proxymap
smtp      unix  -       -       n       -       -       smtp
relay     unix  -       -       n       -       -       smtp
       -o fallback_relay=
showq     unix  n       -       n       -       -       showq
error     unix  -       -       n       -       -       error
discard   unix  -       -       n       -       -       discard
local     unix  -       n       n       -       -       local
virtual   unix  -       n       n       -       -       virtual
lmtp      unix  -       -       n       -       -       lmtp
anvil     unix  -       -       n       -       1       anvil
scache   unix -      -      n      -      1      scache

maildrop  unix  -       n       n       -       -       pipe
  flags=DRhu user=vmail argv=/usr/local/bin/maildrop -d ${recipient}
old-cyrus unix  -       n       n       -       -       pipe
  flags=R user=cyrus argv=/cyrus/bin/deliver -e -m ${extension} ${user}
cyrus     unix  -       n       n       -       -       pipe
  user=cyrus argv=/cyrus/bin/deliver -e -r ${sender} -m ${extension} ${user}
uucp      unix  -       n       n       -       -       pipe
  flags=Fqhu user=uucp argv=uux -r -n -z -a$sender - $nexthop!rmail ($recipient)
ifmail    unix  -       n       n       -       -       pipe
  flags=F user=ftn argv=/usr/lib/ifmail/ifmail -r $nexthop ($recipient)
bsmtp     unix  -       n       n       -       -       pipe
  flags=Fq. user=foo argv=/usr/local/sbin/bsmtp -f $sender $nexthop $recipient
```

Příloha 4 - proftpd.conf - konfigurační soubor FTP serveru ProFTPd

```
ServerName                  "FTP daemon"
ServerType                  standalone
ServerIdent                 on     "FTPd"
DefaultServer               on
DeferWelcome                on
Port                        21
Umask                       022
MaxInstances                30
User                        nobody
Group                       nogroup
DefaultRoot   ~
AllowOverwrite                      on
AllowRetrieveRestart        on
AllowStoreRestart           on
RequireValidShell           off
ScoreboardFile       /var/run/proftpd.scoreboard
SystemLog            /var/log/proftpd/main.log
LogFormat awstats "%t       %h     %u     %m     %f     %s     %b"
ExtendedLog /var/log/proftpd/main.xferlog read,write awstats
TransferLog none
UseReverseDNS               off
IdentLookups                off
TimesGMT                    off
PassivePorts         55000 56000
<Limit SITE_CHMOD>
  #DenyAll
</Limit>
SQLAuthenticate                     users*
SQLConnectInfo                      sys_ftp@localhost:3306 sys_ftp_proftpd
SImk4LexSOxo PERSESSION
SQLAuthTypes                Crypt
SQLUserInfo                 users login passwd uid gid homedir shell
SQLHomedirOnDemand          off
<Global>
</Global>
<IfModule mod_tls.c>
       TLSEngine            on
       TLSLog               /var/log/proftpd/tls.log
       TLSRequired          on
       TLSRSACertificateFile
       /usr/local/etc/ssl_cert/roxy.refresh.cz.crt
       TLSRSACertificateKeyFile    /usr/local/etc/ssl_cert/roxy.refresh.cz.key
       TLSVerifyClient             off
</IfModule>
```

Příloha 5 - httpd.conf - konfigurační soubor aplikace Apache 2

```
ServerRoot "/usr/local"
Listen 192.168.1.10:80

LoadModule authn_file_module libexec/apache22/mod_authn_file.so
LoadModule authn_default_module libexec/apache22/mod_authn_default.so
LoadModule authz_host_module libexec/apache22/mod_authz_host.so
LoadModule authz_user_module libexec/apache22/mod_authz_user.so
LoadModule authz_dbm_module libexec/apache22/mod_authz_dbm.so
LoadModule authz_default_module libexec/apache22/mod_authz_default.so
LoadModule auth_basic_module libexec/apache22/mod_auth_basic.so
LoadModule auth_digest_module libexec/apache22/mod_auth_digest.so
LoadModule deflate_module libexec/apache22/mod_deflate.so
LoadModule log_config_module libexec/apache22/mod_log_config.so
LoadModule logio_module libexec/apache22/mod_logio.so
LoadModule expires_module libexec/apache22/mod_expires.so
LoadModule setenvif_module libexec/apache22/mod_setenvif.so
LoadModule ssl_module libexec/apache22/mod_ssl.so
LoadModule mime_module libexec/apache22/mod_mime.so
LoadModule status_module libexec/apache22/mod_status.so
LoadModule autoindex_module libexec/apache22/mod_autoindex.so
LoadModule negotiation_module libexec/apache22/mod_negotiation.so
LoadModule dir_module libexec/apache22/mod_dir.so
LoadModule alias_module libexec/apache22/mod_alias.so
LoadModule rewrite_module libexec/apache22/mod_rewrite.so
LoadModule php5_module        libexec/apache22/libphp5.so

<IfModule !mpm_winnt_module>
<IfModule !mpm_netware_module>
User www
Group www
</IfModule>
</IfModule>

ServerAdmin mail@quip.cz
ServerName quip.cz:80

#DocumentRoot "/usr/local/www/apache22/data"
DocumentRoot "/vol0/web/quip.cz/doc_root"
<Directory />
    AllowOverride None
    Order deny,allow
    Deny from all
</Directory>

<Directory "/vol0/web/quip.cz/">
    Options Indexes FollowSymLinks
    AllowOverride None
    Order allow,deny
    Allow from all
</Directory>

<IfModule dir_module>
    DirectoryIndex index.html index.cgi index.pl index.php index.xhtml
</IfModule>

<FilesMatch "^\.ht">
    Order allow,deny
    Deny from all
</FilesMatch>

ErrorLog /var/log/httpd-error.log

LogLevel warn
```

```
<IfModule log_config_module>
    LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\""
combined
    LogFormat "%h %l %u %t \"%r\" %>s %b" common
    <IfModule logio_module>
      LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\" %I
%O" combinedio
    </IfModule>
    CustomLog /var/log/httpd-access.log combined
</IfModule>

<IfModule alias_module>
    ScriptAlias /cgi-bin/ "/usr/local/www/apache22/cgi-bin/"
</IfModule>

<IfModule cgid_module>
</IfModule>

<Directory "/usr/local/www/apache22/cgi-bin">
    AllowOverride None
    Options None
    Order allow,deny
    Allow from all
</Directory>

DefaultType text/plain

<IfModule mime_module>
    TypesConfig etc/apache22/mime.types
    AddType application/x-compress .Z
    AddType application/x-gzip .gz .tgz
</IfModule>

<IfModule ssl_module>
SSLRandomSeed startup builtin
SSLRandomSeed connect builtin
</IfModule>

Include etc/apache22/Includes/*.conf

#    RewriteEngine       On
#    RewriteCond         %{HTTP_HOST}  !^www.quip.cz$
#    RewriteRule         ^/(.*)$ http://www.quip.cz/$1 [L,R=permanent]

Alias /pma "/usr/local/www/phpMyAdmin/"
    <Directory "/usr/local/www/phpMyAdmin/">
        Options none
       AllowOverride all
       Order allow,deny
       Allow from all
    </Directory>

Alias /mail "/usr/local/www/roundcube/"
    <Directory "/usr/local/www/roundcube/">
        Options none
        AllowOverride all
        Order allow,deny
        Allow from all
    </Directory>

Alias /mailadmin "/usr/local/www/postfixadmin/"
    <Directory "/usr/local/www/postfixadmin/">
        Options none
        AllowOverride all
        Order allow,deny
        Allow from all
    </Directory>
```

```
Alias /egroupware "/usr/local/www/data-dist/egroupware/"
    <Directory "/usr/local/www/data-dist/egroupware/">
        Options none
        AllowOverride all
        Order allow,deny
        Allow from all
    </Directory>


    php_value           error_reporting         2039
    php_admin_value     sendmail_from           web@quip.cz
    php_admin_value     upload_tmp_dir          /vol0/web/quip.cz/tmp
    php_admin_value     open_basedir
/vol0/web/quip.cz/:/usr/local/www/phpMyAdmin/:/usr/local/www/postfixadmin/:/usr/loc
al/www/roundcube/:/usr/local/etc/cups/
    php_admin_value     session.save_path       /vol0/web/quip.cz/tmp
    php_admin_flag      safe_mode               Off
    php_admin_value     safe_mode_include_dir
.:/usr/local/www/phpMyAdmin/:/usr/local/www/postfixadmin/:/usr/local/www/roundcube/
:/usr/local/etc/cups/
    php_admin_flag      register_globals        On

# PHP settings
Include etc/apache22/extra/httpd-php5.conf
# Server-pool management (MPM specific)
Include etc/apache22/extra/httpd-mpm.conf
# Multi-language error messages
Include etc/apache22/extra/httpd-multilang-errordoc.conf
# Fancy directory listings
Include etc/apache22/extra/httpd-autoindex.conf
# Language settings
Include etc/apache22/extra/httpd-languages.conf
# Real-time info on requests and configuration
Include etc/apache22/extra/httpd-info.conf
# Virtual hosts
#Include etc/apache22/extra/httpd-vhosts.conf
# Various default settings
Include etc/apache22/extra/httpd-default.conf
<IfDefine SSL>
# Secure (SSL/TLS) connections
Include etc/apache22/extra/httpd-ssl.conf
</IfDefine>
```

Příloha 6 - periodic.conf - konfigurační soubor služby periodic

```
# provedeni pkg_version -v a zaslani mailem
weekly_status_pkg_enable="YES"

# only if gmirror is used
daily_status_gmirror_enable="YES"

# postfix related
daily_clean_hoststat_enable="NO"
daily_status_mail_rejects_enable="NO"
daily_status_include_submit_mailq="NO"
daily_submit_queuerun="NO"

# BSDstats
monthly_statistics_enable="YES"
monthly_statistics_report_devices="YES"
monthly_statistics_report_ports="YES"

# PF tables changes
daily_status_security_pf_tables_enable="YES"
#daily_status_security_pf_tables_tables="goodguys badguys bruteforce
ssh_bruteforce"

# SMART changes
weekly_smartctl_changes_enable="YES"
#weekly_smartctl_changes_devices="/dev/ad4 /dev/ad6"
#weekly_smartctl_changes_flags="-a"
# added by mergebase.sh
local_periodic="/usr/local/etc/periodic"
```

Příloha 7 - smartctl.sh - skript začleněný do týdenního výpisu periodic

```
#!/bin/sh -
#
# Copyright (c) 2007  Quip
# All rights reserved.
#
# "THE BEER-WARE LICENSE" (Revision 44):
# quip at quip dot cz wrote this file. As long as you retain this notice
# you can do whatever you want with this stuff. If we meet some day, and
# you think this stuff is worth it, you can buy me a juice or non-alcoholic
# beer in return. Miroslav Lachman #

# show changes in S.M.A.R.T log of ATA/SATA/SCSI devices #
# Put this file in to /usr/local/etc/periodic/weekly/ and chmod it to 0544 #

if [ -r /etc/defaults/periodic.conf ]
then
       . /etc/defaults/periodic.conf
       source_periodic_confs
fi

. /etc/periodic/security/security.functions

rc=0

case "$weekly_smartctl_changes_enable" in
       [Yy][Ee][Ss])
       echo ""
       echo 'Checking S.M.A.R.T changes:'

       # devices are not defined, try to list available devices
       if [ -z "${weekly_smartctl_changes_devices}" ]
       then
              weekly_smartctl_changes_devices=` ls /dev/da? 2> /dev/null ; ls
/dev/ad? 2> /dev/null`
       fi

       if [ -n "${weekly_smartctl_changes_devices}" ]
       then
              # for each device
              for device in $weekly_smartctl_changes_devices
              do

       weekly_smartctl_changes_flags=${weekly_smartctl_changes_flags:-"-a"}

                     /usr/local/sbin/smartctl ${weekly_smartctl_changes_flags}
${device} | check_diff smartctl_`echo ${device} | sed 's~/~_~g'` - "${host} changes
for device ${device}:"
                     rc=$?
              done
       else
              echo 'You must define $weekly_smartctl_changes_devices as space
separated list of devices'
       fi;;

       *)  rc=0;;
esac

exit $rc
```

Příloha 8 - Daily run output

```
Removing stale files from /var/preserve:

Cleaning out old system announcements:

Removing stale files from /var/rwho:

Backup passwd and group files:

Verifying group file syntax:
/etc/group is fine

Backing up mail aliases:

Rotating accounting logs and gathering statistics:

Disk status:
Filesystem         1K-blocks     Used     Avail Capacity  Mounted on
/dev/mirror/gm0s1a    380654   160386    189816    46%    /
devfs                      1        1         0   100%    /dev
/dev/mirror/gm0s1f   2657570     6202   2438764     0%    /tmp
/dev/mirror/gm0s1e   7103150  4845090   1689808    74%    /usr
/dev/mirror/gm0s1d  30462636  3367230  24658396    12%    /var
/dev/mirror/gm0s2d 193862888 23468668 154885190    13%    /mnt/dsk0

Last dump(s) done (Dump '>' file systems):

Network interface status:
Name    Mtu Network       Address              Ipkts Ierrs    Opkts Oerrs  Coll
bge0   1500 <Link#1>      00:15:f2:e0:bb:e7 41916892     0 64268187     0     0
bge0   1500 82.208.36/24  retezat           25514083     - 64266244     -     -
bge0   1500 82.208.36.191 krizovatka.skaut. 14222873     -   125350     -     -
bge0   1500 82.208.36.192 retezat              49944     -        0     -     -
bge1   1500 <Link#2>      00:15:f2:e0:bb:e8     1198     0        1     0     0
bge1   1500 192.168.22    retezat.local            0     -        0     -     -
plip0  1500 <Link#3>                                0     0        0     0     0
lo0   16384 <Link#4>                           365919     0   365919     0     0
lo0   16384 fe80:4::1     fe80:4::1                0     -        0     -     -
lo0   16384 localhost.tov ::1                      0     -        0     -     -
lo0   16384 your-net      localhost           240563     -   240563     -     -
pflog 33208 <Link#5>                                0     0        0     0     0

Local system status:
 3:01AM  up 8 days,  7:41, 0 users, load averages: 0.50, 0.38, 0.34

Mail in local queue:
-Queue ID- --Size-- ----Arrival Time---- -Sender/Recipient-------
CD92F284262     5177 Fri Aug 17 11:04:00  tomas.slavik@google.com
                 (connect to tiscalli.cz[207.218.235.178]: Connection refused)
                                         lek.kras@tiscalli.cz

C749D2840C9     4657 Mon Aug 20 00:48:09  info@drill.cz
        (connect to elec-eng.leeds.ac.uk[129.11.133.104]: Operation timed out)
                                        H.J.Strangeways@elec-eng.leeds.ac.uk

-- 10 Kbytes in 2 Requests.

Security check:
    (output mailed separately)

Checking for denied zone transfers (AXFR and IXFR):

-- End of daily output --
```

Příloha 9 - Weekly run output

```
Rebuilding locate database:

Rebuilding whatis database:

Check for out of date packages:
  firebird-client-1.5.3 needs updating (port has 1.5.4)
  p5-Mail-SpamAssassin-3.2.1 needs updating (port has 3.2.1_1)
  p5-Net-DNS-0.60 needs updating (port has 0.61)
  php5-5.2.3 needs updating (port has 5.2.3_1)
  php5-bz2-5.2.3 needs updating (port has 5.2.3_1)
  php5-ctype-5.2.3 needs updating (port has 5.2.3_1)
  php5-curl-5.2.3 needs updating (port has 5.2.3_1)
  php5-dom-5.2.3 needs updating (port has 5.2.3_1)
  php5-xmlrpc-5.2.3 needs updating (port has 5.2.3_1)
  php5-xmlwriter-5.2.3 needs updating (port has 5.2.3_1)
  php5-xsl-5.2.3 needs updating (port has 5.2.3_1)
  php5-zlib-5.2.3 needs updating (port has 5.2.3_1)
  postfix-2.4.3,1 needs updating (port has 2.4.5,1)
  python-2.4.4,1 needs updating (port has 2.4,2)
  python24-2.4.4 needs updating (port has 2.4.4_1)
  python25-2.5_1 needs updating (port has 2.5.1)
  roundcube-0.1.20061207 needs updating (port has 0.1.20070608)
  strace-4.5.2 needs updating (port has 4.5.5)
  t1lib-5.1.1_1,1 needs updating (port has 5.1.1_2,1)
  vim-lite-7.1.39 needs updating (port has 7.1.55)

Checking S.M.A.R.T changes:

lite.eurofinancial.cz changes for device /dev/ad4:
--- /var/log/smartctl__dev_ad4.today      Sat Aug  4 04:20:46 2007
+++ /tmp/security.m1PGtS4t  Sat Aug 11 04:21:04 2007
@@ -9,7 +9,7 @@
 Device is:        Not in smartctl database [for details use: -P showall]
 ATA Version is:   7
 ATA Standard is:  Exact ATA specification draft version not indicated
-Local Time is:    Sat Aug  4 04:20:46 2007 CEST
+Local Time is:    Sat Aug 11 04:21:03 2007 CEST
 SMART support is: Available - device has SMART capability.
 SMART support is: Enabled

@@ -50,15 +50,15 @@
   3 Spin_Up_Time            0x0003 095 095 000  Pre-fail  Always    -      0
   4 Start_Stop_Count        0x0032 100 100 020  Old_age   Always    -      7
   5 Reallocated_Sector_Ct   0x0033 100 100 036  Pre-fail  Always    -      13
-  7 Seek_Error_Rate         0x000f 079 060 030  Pre-fail  Always    -     92455733
-  9 Power_On_Hours          0x0032 093 093 000  Old_age   Always    -      6885
+  7 Seek_Error_Rate         0x000f 079 060 030  Pre-fail  Always    -     94795106
+  9 Power_On_Hours          0x0032 092 092 000  Old_age   Always    -      7032
  10 Spin_Retry_Count        0x0013 100 100 097  Pre-fail  Always    -       0
  12 Power_Cycle_Count       0x0032 100 100 020  Old_age   Always    -       10
 187 Unknown_Attribute       0x0032 001 001 000  Old_age   Always    -       9450
 189 Unknown_Attribute       0x003a 100 100 000  Old_age   Always    -       0
-190 Temperature_Celsius     0x0022 065 058 045  Old_age   Always    -    672530467
-194 Temperature_Celsius     0x0022 035 042 000  Old_age   Always    -      35
-195 Hardware_ECC_Recovered  0x001a 048 042 000  Old_age   Always    -    149941908
+190 Temperature_Celsius     0x0022 066 058 045  Old_age   Always    -    672530466
+194 Temperature_Celsius     0x0022 034 042 000  Old_age   Always    -       34
+195 Hardware_ECC_Recovered  0x001a 051 042 000  Old_age   Always    -     67899027
 197 Current_Pending_Sector  0x0012 100 100 000  Old_age   Always    -       0
 198 Offline_Uncorrectable   0x0010 100 100 000  Old_age   Offline   -       0
 199 UDMA_CRC_Error_Count    0x003e 200 200 000  Old_age   Always    -       0
@@ -70,27 +70,27 @@

 SMART Self-test log structure revision number 1
```

```
 Num  Test_Description    Status                  Remaining  LifeTime(hours)
LBA_of_first_error
-# 1  Short offline       Completed without error       00%      6864         -
-# 2  Short offline       Completed without error       00%      6843         -
-# 3  Short offline       Completed without error       00%      6822         -
-# 4  Short offline       Completed without error       00%      6801         -
-# 5  Short offline       Completed without error       00%      6780         -
-# 6  Short offline       Completed without error       00%      6759         -
-# 7  Extended offline    Completed without error       00%      6739         -
-# 8  Short offline       Completed without error       00%      6738         -
-# 9  Short offline       Completed without error       00%      6717         -
-#10  Short offline       Completed without error       00%      6696         -
-#11  Short offline       Completed without error       00%      6675         -
-#12  Short offline       Completed without error       00%      6655         -
-#13  Short offline       Completed without error       00%      6633         -
-#14  Short offline       Completed without error       00%      6612         -
-#15  Extended offline    Completed without error       00%      6592         -
-#16  Short offline       Completed without error       00%      6592         -
-#17  Short offline       Completed without error       00%      6570         -
-#18  Short offline       Completed without error       00%      6550         -
-#19  Short offline       Completed without error       00%      6528         -
-#20  Short offline       Completed without error       00%      6508         -
-#21  Short offline       Self-test routine in progress 90%      6885         -
+# 1  Short offline       Completed without error       00%      7010         -
+# 2  Short offline       Completed without error       00%      6990         -
+# 3  Short offline       Completed without error       00%      6968         -
+# 4  Short offline       Completed without error       00%      6948         -
+# 5  Short offline       Completed without error       00%      6927         -
+# 6  Short offline       Completed without error       00%      6905         -
+# 7  Extended offline    Completed without error       00%      6886         -
+# 8  Short offline       Completed without error       00%      6885         -
+# 9  Short offline       Completed without error       00%      6864         -
+#10  Short offline       Completed without error       00%      6843         -
+#11  Short offline       Completed without error       00%      6822         -
+#12  Short offline       Completed without error       00%      6801         -
+#13  Short offline       Completed without error       00%      6780         -
+#14  Short offline       Completed without error       00%      6759         -
+#15  Extended offline    Completed without error       00%      6739         -
+#16  Short offline       Completed without error       00%      6738         -
+#17  Short offline       Completed without error       00%      6717         -
+#18  Short offline       Completed without error       00%      6696         -
+#19  Short offline       Completed without error       00%      6675         -
+#20  Short offline       Completed without error       00%      6655         -
+#21  Short offline       Self-test routine in progress 90%      7032         -

 SMART Selective self-test log data structure revision number 1
  SPAN  MIN_LBA  MAX_LBA  CURRENT_TEST_STATUS

lite.eurofinancial.cz changes for device /dev/ad6:
--- /var/log/smartctl__dev_ad6.today      Sat Aug  4 04:20:46 2007
+++ /tmp/security.zvtSX68N  Sat Aug 11 04:21:04 2007
@@ -9,7 +9,7 @@
 Device is:        Not in smartctl database [for details use: -P showall]
 ATA Version is:   7
 ATA Standard is:  Exact ATA specification draft version not indicated
-Local Time is:    Sat Aug  4 04:20:46 2007 CEST
+Local Time is:    Sat Aug 11 04:21:04 2007 CEST
 SMART support is: Available - device has SMART capability.
 SMART support is: Enabled

@@ -50,15 +50,15 @@
   3 Spin_Up_Time            0x0003 096 096 000    Pre-fail  Always       -       0
   4 Start_Stop_Count        0x0032 100 100 020    Old_age   Always       -       7
   5 Reallocated_Sector_Ct   0x0033 100 100 036    Pre-fail  Always       -       0
-  7 Seek_Error_Rate         0x000f 079 060 030  Pre-fail  Always    -    91056616
-  9 Power_On_Hours          0x0032 093 093 000  Old_age   Always    -       6880
+  7 Seek_Error_Rate         0x000f 079 060 030  Pre-fail  Always    -    93367871
+  9 Power_On_Hours          0x0032 092 092 000  Old_age   Always    -       7026
```

```
  10 Spin_Retry_Count        0x0013 100 100 097  Pre-fail  Always    -       0
  12 Power_Cycle_Count       0x0032 100 100 020  Old_age   Always    -       10
 187 Unknown_Attribute       0x0032 100 100 000  Old_age   Always    -       0
 189 Unknown_Attribute       0x003a 100 100 000  Old_age   Always    -       0
-190 Temperature_Celsius     0x0022 066 058 045  Old_age   Always    -  47900327970
-194 Temperature_Celsius     0x0022 034 042 000  Old_age   Always    -       34
(Lifetime Min/Max 0/21)
-195 Hardware_ECC_Recovered  0x001a 051 044 000  Old_age   Always    -    199879059
+190 Temperature_Celsius     0x0022 068 058 045  Old_age   Always    -  47900327968
+194 Temperature_Celsius     0x0022 032 042 000  Old_age   Always    -       32
+195 Hardware_ECC_Recovered  0x001a 052 044 000  Old_age   Always    -    109985690
 197 Current_Pending_Sector  0x0012 100 100 000  Old_age   Always    -       0
 198 Offline_Uncorrectable   0x0010 100 100 000  Old_age   Offline   -       0
 199 UDMA_CRC_Error_Count    0x003e 200 200 000  Old_age   Always    -       0
@@ -70,27 +70,27 @@

 SMART Self-test log structure revision number 1
 Num  Test_Description    Status                  Remaining  LifeTime(hours)
LBA_of_first_error
-# 1  Short offline       Completed without error       00%      6859         -
-# 2  Short offline       Completed without error       00%      6838         -
-# 3  Short offline       Completed without error       00%      6816         -
-# 4  Short offline       Completed without error       00%      6796         -
-# 5  Short offline       Completed without error       00%      6775         -
-# 6  Short offline       Completed without error       00%      6754         -
-# 7  Extended offline    Completed without error       00%      6735         -
-# 8  Short offline       Completed without error       00%      6733         -
-# 9  Short offline       Completed without error       00%      6712         -
-#10  Short offline       Completed without error       00%      6691         -
-#11  Short offline       Completed without error       00%      6670         -
-#12  Short offline       Completed without error       00%      6649         -
-#13  Short offline       Completed without error       00%      6628         -
-#14  Short offline       Completed without error       00%      6608         -
-#15  Extended offline    Completed without error       00%      6588         -
-#16  Short offline       Completed without error       00%      6586         -
-#17  Short offline       Completed without error       00%      6566         -
-#18  Short offline       Completed without error       00%      6544         -
-#19  Short offline       Completed without error       00%      6523         -
-#20  Short offline       Completed without error       00%      6503         -
-#21  Short offline       Self-test routine in progress 90%      6880         -
+# 1  Short offline       Completed without error       00%      7006         -
+# 2  Short offline       Completed without error       00%      6984         -
+# 3  Short offline       Completed without error       00%      6963         -
+# 4  Short offline       Completed without error       00%      6943         -
+# 5  Short offline       Completed without error       00%      6921         -
+# 6  Short offline       Completed without error       00%      6901         -
+# 7  Extended offline    Completed without error       00%      6881         -
+# 8  Short offline       Completed without error       00%      6880         -
+# 9  Short offline       Completed without error       00%      6859         -
+#10  Short offline       Completed without error       00%      6838         -
+#11  Short offline       Completed without error       00%      6816         -
+#12  Short offline       Completed without error       00%      6796         -
+#13  Short offline       Completed without error       00%      6775         -
+#14  Short offline       Completed without error       00%      6754         -
+#15  Extended offline    Completed without error       00%      6735         -
+#16  Short offline       Completed without error       00%      6733         -
+#17  Short offline       Completed without error       00%      6712         -
+#18  Short offline       Completed without error       00%      6691         -
+#19  Short offline       Completed without error       00%      6670         -
+#20  Short offline       Completed without error       00%      6649         -
+#21  Short offline       Self-test routine in progress 90%      7026         -

 SMART Selective self-test log data structure revision number 1
  SPAN  MIN_LBA  MAX_LBA  CURRENT_TEST_STATUS

-- End of weekly output --
```

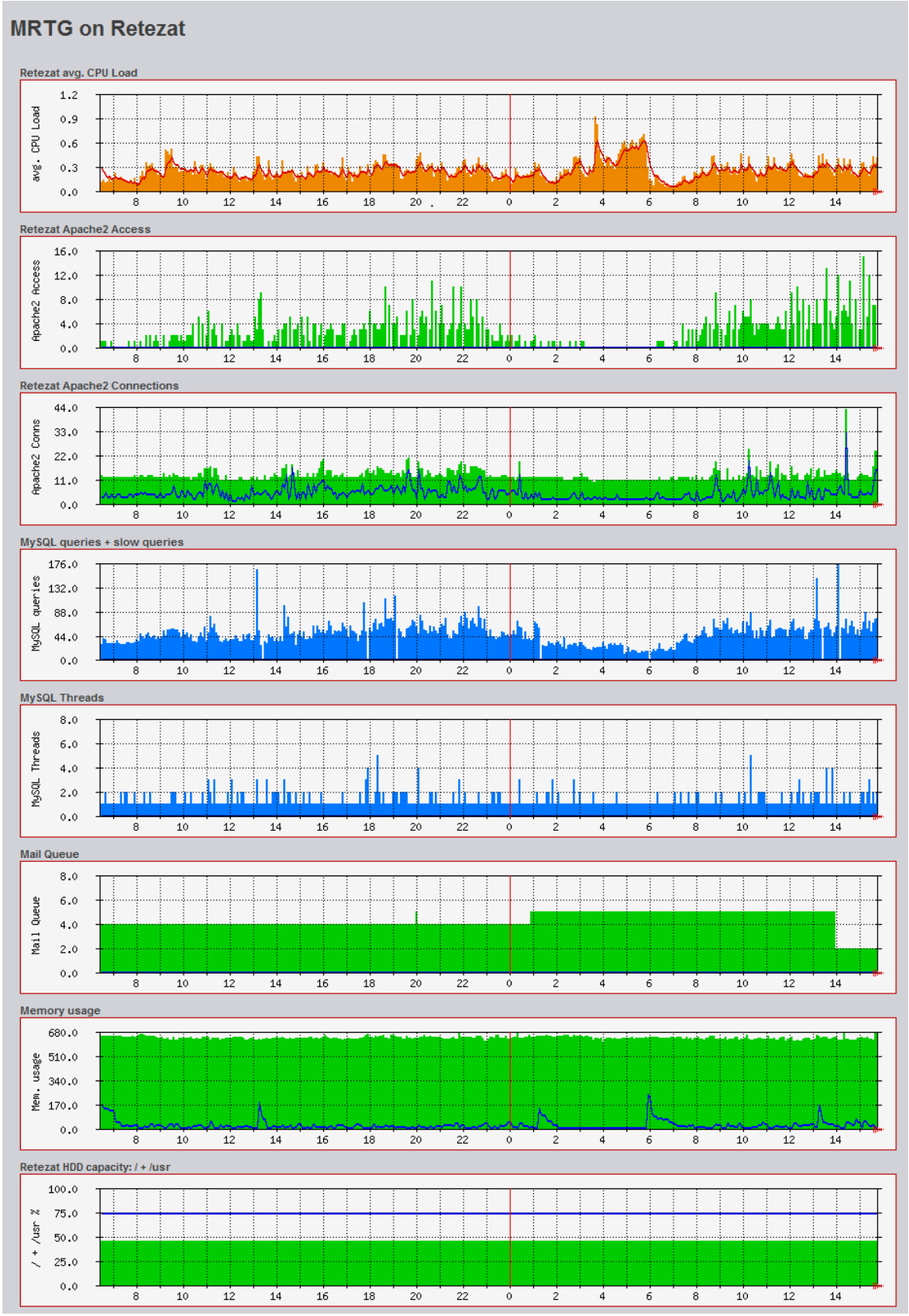
Příloha 10 - Monthly run output

```
Doing login accounting:
       total               96.15
       clientzone.euro     48.95
       www.eurofinanci     25.97
       java_datastorag      8.14
       dbcs.eurofinanc      6.40
       quip                 6.39
       aureliano            0.30
       blog.eurofinanc      0.00
       benefit.eurofin      0.00
Posting monthly OS statistics to rpt.bsdstats.org Posting monthly device statistics
to rpt.bsdstats.org Posting monthly CPU statistics to rpt.bsdstats.org Posting
monthly ports statistics to rpt.bsdstats.org

-- End of monthly output --
```

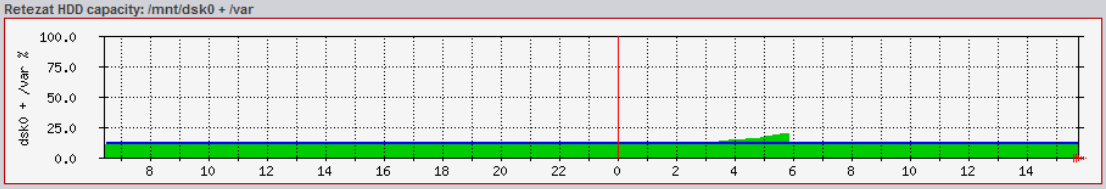
Příloha 11 - Řešení problému synchronizace primární a sekundární MySQL databáze

```
Na MASTER DB serveru

mysql> use retezatcz
Database changed
mysql> SELECT * FROM sessionValue WHERE
sessionId='14ondo1nq68kaj5o9qu6cfiv37';
Empty set (0.00 sec)

Na SLAVE DB serverech

mysql> use retezatcz
Database changed
mysql> SELECT * FROM sessionValue WHERE
sessionId='14ondo1nq68kaj5o9qu6cfiv37';
+---------------------------+---------------+------------+------------+
| sessionId                 | value         | timestamp  | valid      |
+---------------------------+---------------+------------+------------+
| 14ondo1nq68kaj5o9qu6cfiv37 | download|i:1; | 1185261542 | 1185264005 |
+---------------------------+---------------+------------+------------+
1 row in set (0.00 sec)

Takze je potreba smazat starou session ve SLAVE DB databazich

mysql> DELETE FROM sessionValue WHERE
sessionId='14ondo1nq68kaj5o9qu6cfiv37';
Query OK, 1 row affected (0.02 sec)

A na obou SLAVE DB serverech znovu spustit replikaci

mysql> SLAVE START;
Query OK, 0 rows affected (0.01 sec)

mysql> SHOW SLAVE STATUS;


root@retezat.tovarna.cz wrote:

>070724  9:20:05 [ERROR] Slave: Error 'Duplicate entry
>'14ondo1nq68kaj5o9qu6cfiv37' for key 1' on query. Default database:
>'retezatcz'. Query: 'INSERT INTO
>sessionValue(sessionId,value,timestamp,valid)
>VALUES('14ondo1nq68kaj5o9qu6cfiv37','download|i:1;','1185261605','11852
>64005')', Error_code: 1062
>070724  9:20:05 [ERROR] Error running query, slave SQL thread aborted.
>Fix the problem, and restart the slave SQL thread with "SLAVE START".
>We stopped at log 'indy-bin.000151' position 1047636548
>
>
>
```

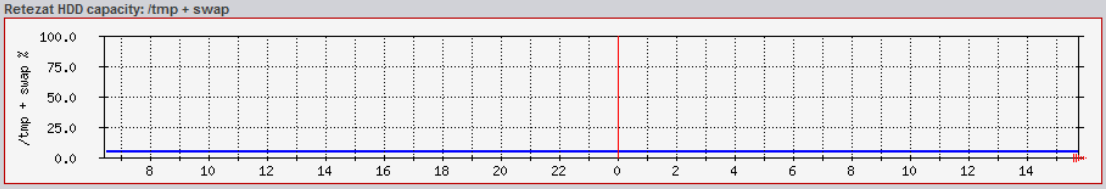
Příloha 12 - Úvodní výstup z MRTG



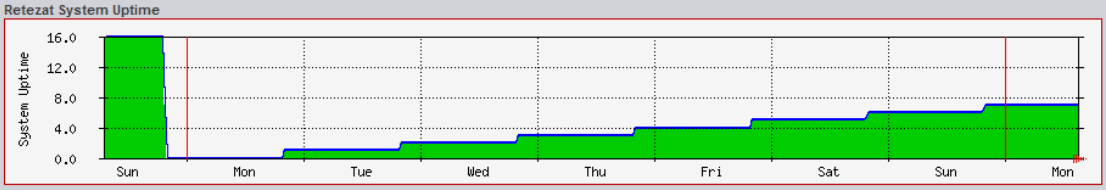
Retezat HDD capacity: /mnt/dsk0 + /var



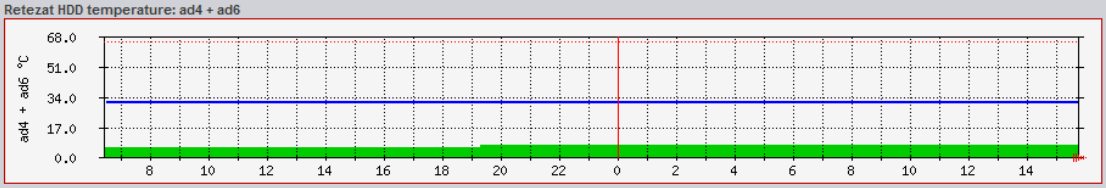
Retezat HDD capacity: /tmp + swap



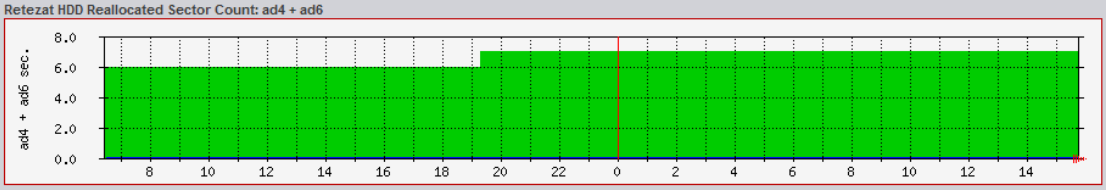
Retezat System Uptime



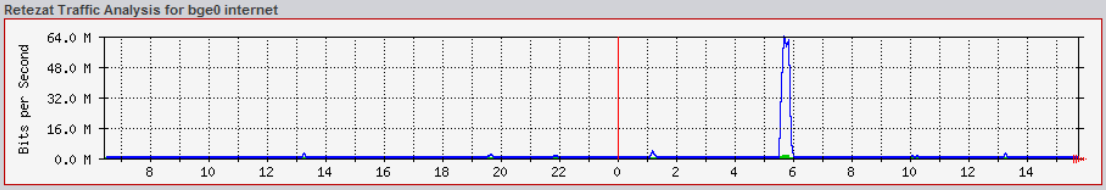
Retezat HDD temperature: ad4 + ad6



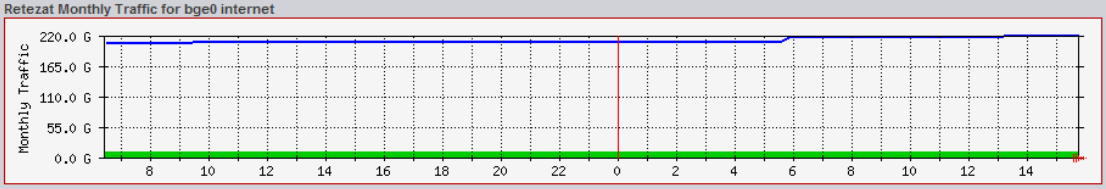
Retezat HDD Reallocated Sector Count: ad4 + ad6



Retezat Traffic Analysis for bge0 internet



Retezat Monthly Traffic for bge0 internet



MRTG MULTI ROUTER TRAFFIC GRAPHER
version 2.15.0
Tobias Oetiker <tobi@oetiker.ch>
and Dave Rand <dlr@bungi.com>

Příloha 13 - Detailní výstup z MRTG pro Apache 2 Access

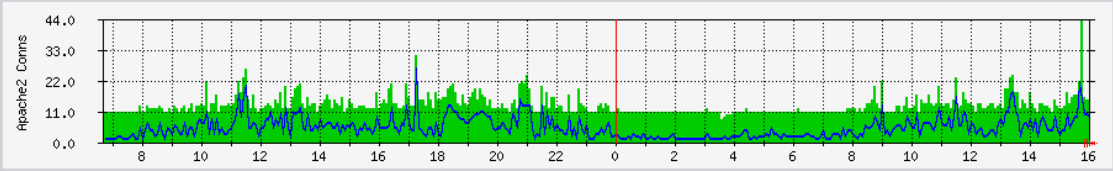
Příloha 14 - Detailní výstup z MRTG pro Apache 2 Connections

Retezat Apache2 Connections

pocet procesu/childu Apache a pocet aktivnich procesu

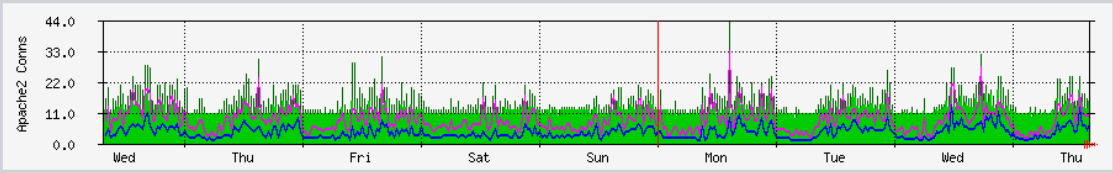
The statistics were last updated **Thursday, 23 August 2007 at 16:00**,
at which time **'retezat Apache'** had been up for **1 days, 20:00:25**.

`Daily' Graph (5 Minute Average)



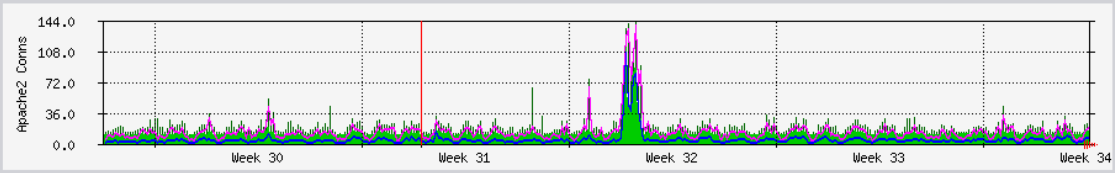
	Max	Average	Current
proc. count	44.0	13.0	15.0
busy workers	26.0	5.0	9.0

`Weekly' Graph (30 Minute Average)



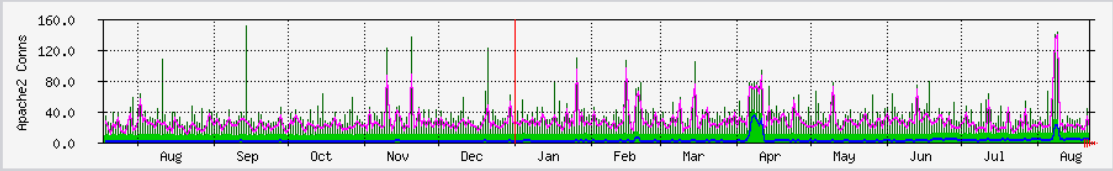
	Max	Average	Current
proc. count	44.0	12.0	15.0
busy workers	33.0	4.0	7.0

`Monthly' Graph (2 Hour Average)



	Max	Average	Current
proc. count	144.0	13.0	15.0
busy workers	138.0	4.0	7.0

`Yearly' Graph (1 Day Average)



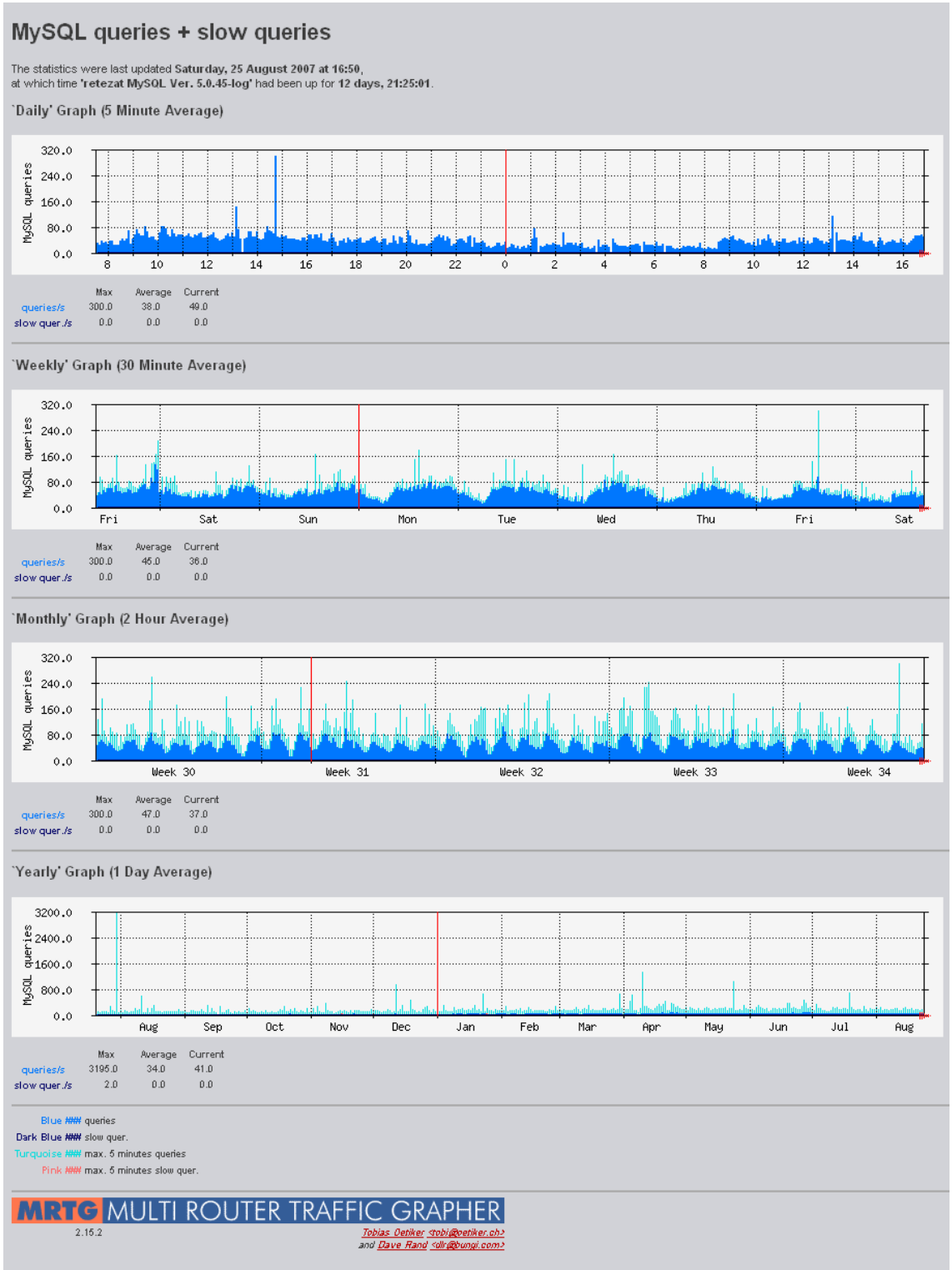
	Max	Average	Current
proc. count	152.0	11.0	13.0
busy workers	138.0	2.0	4.0

GREEN ### proc. count
BLUE ### busy workers
DARK GREEN ### Maximal 5 Minute Incoming Traffic
MAGENTA ### Maximal 5 Minute Outgoing Traffic

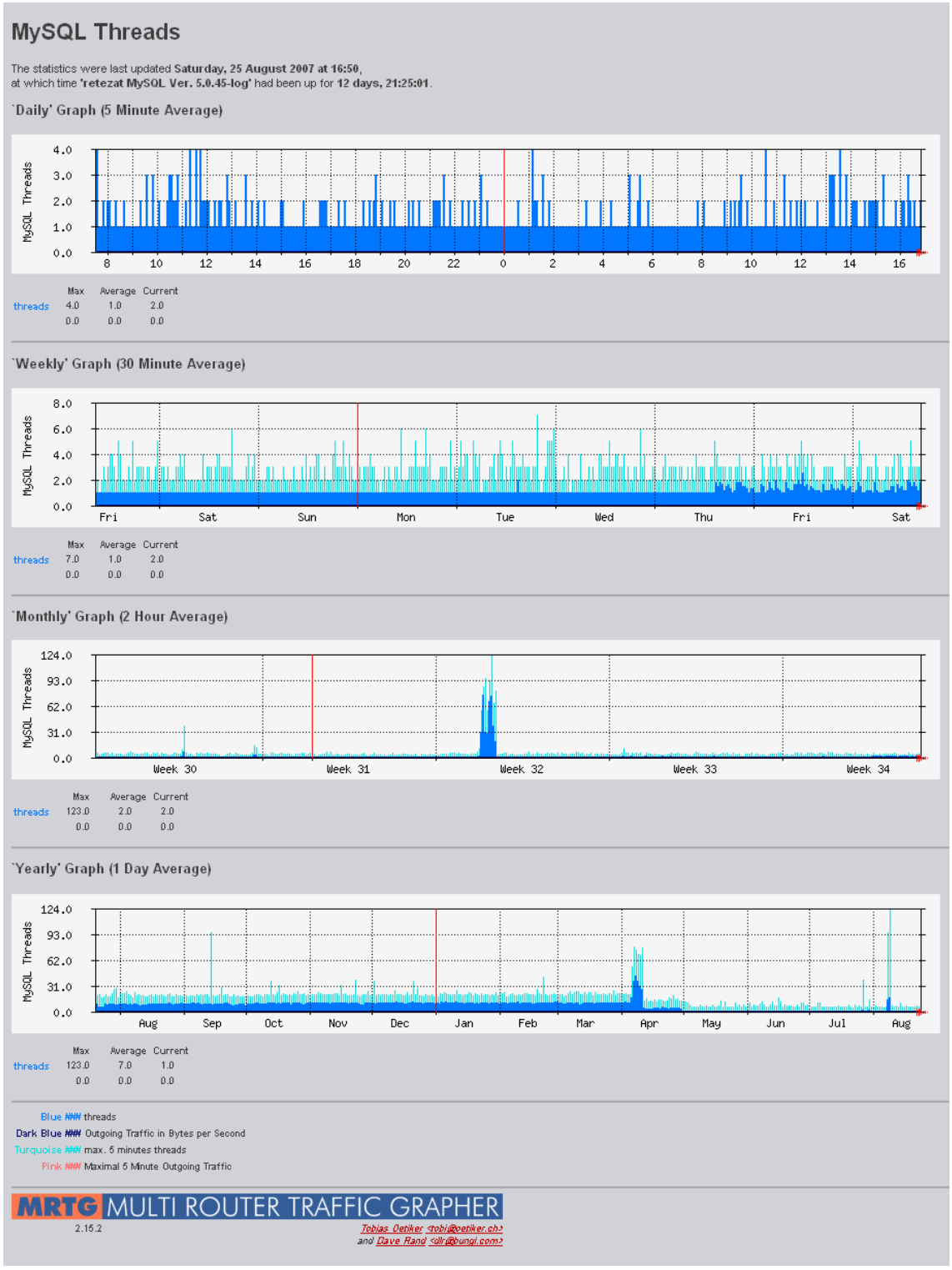
MRTG MULTI ROUTER TRAFFIC GRAPHER
2.15.2

Tobias Oetiker <tobi@oetiker.ch>
and Dave Rand <dlr@bungi.com>

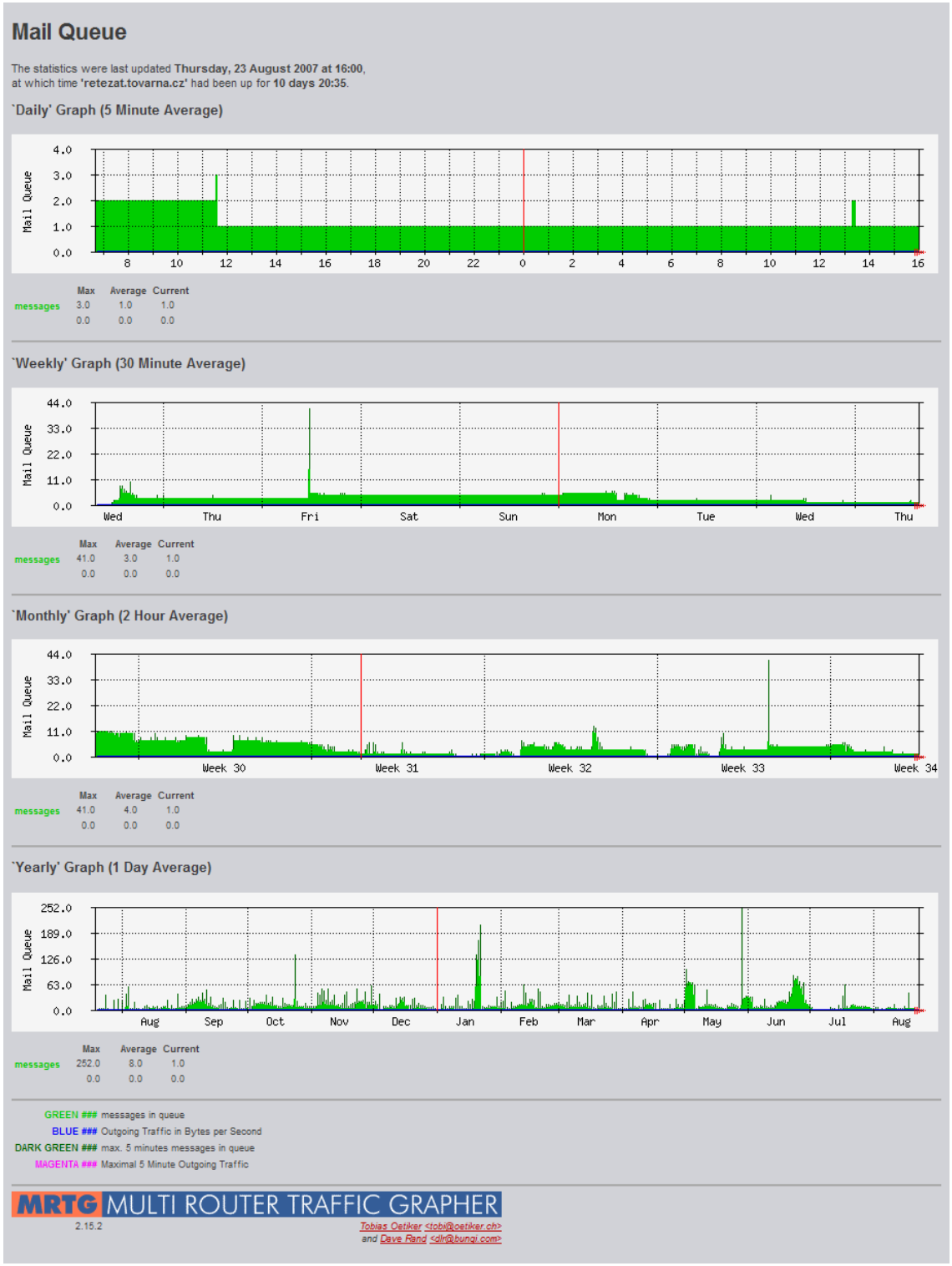
Příloha 15 - Detailní výstup z MRTG pro MySQL Queries



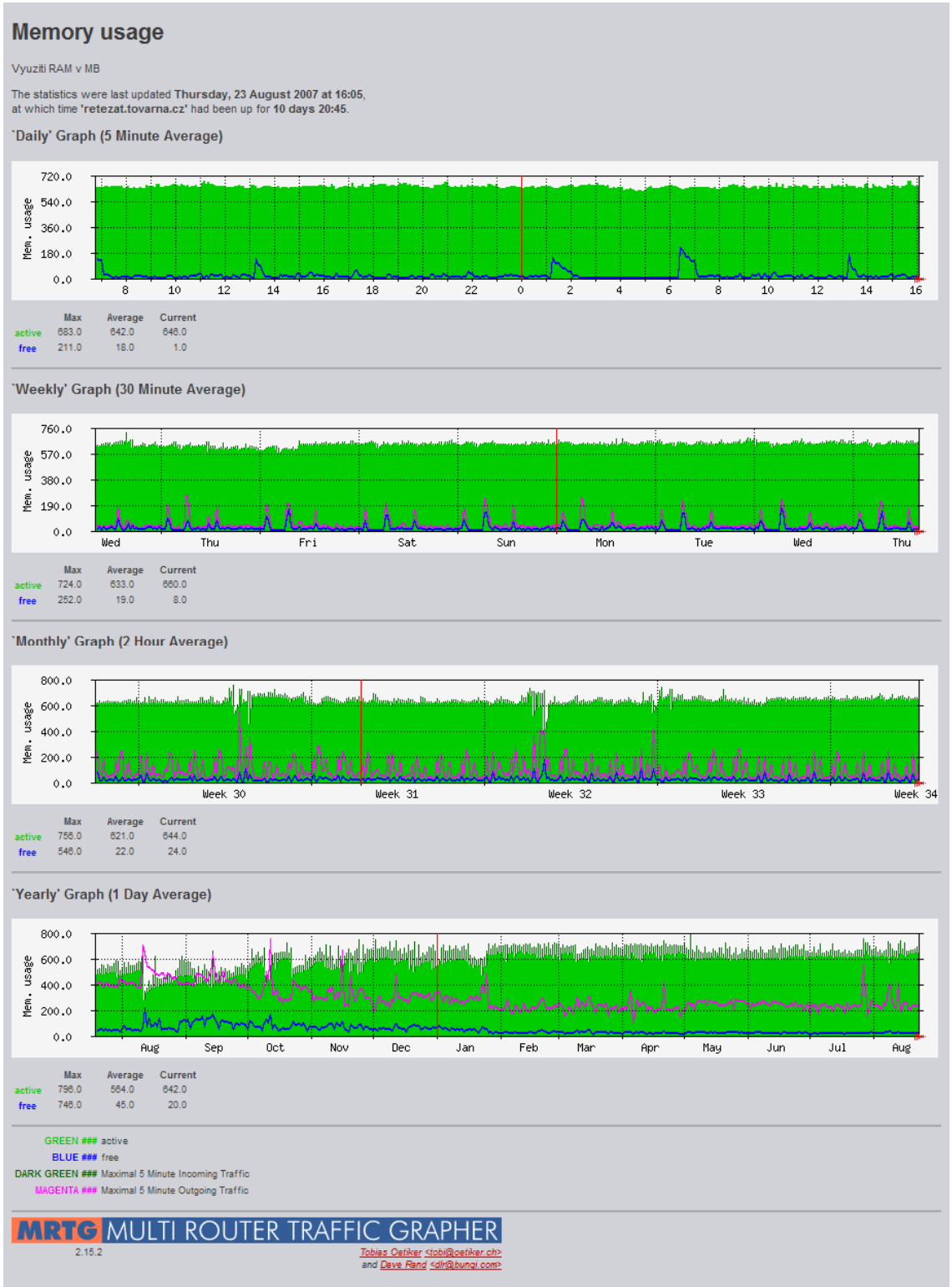
Příloha 16 - Detailní výstup z MRTG pro MySQL Threads



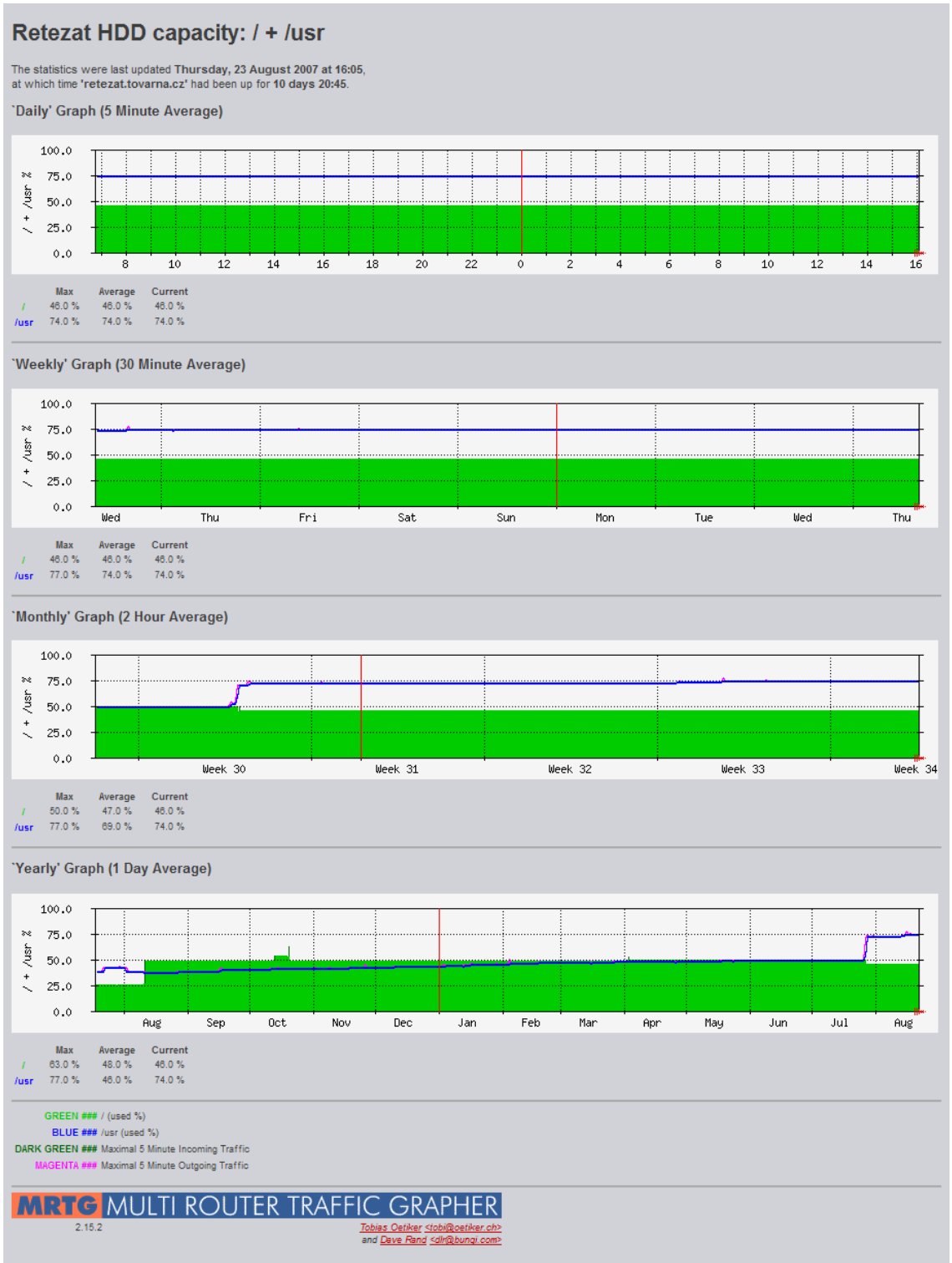
Příloha 17 - Detailní výstup z MRTG pro Mail Queue



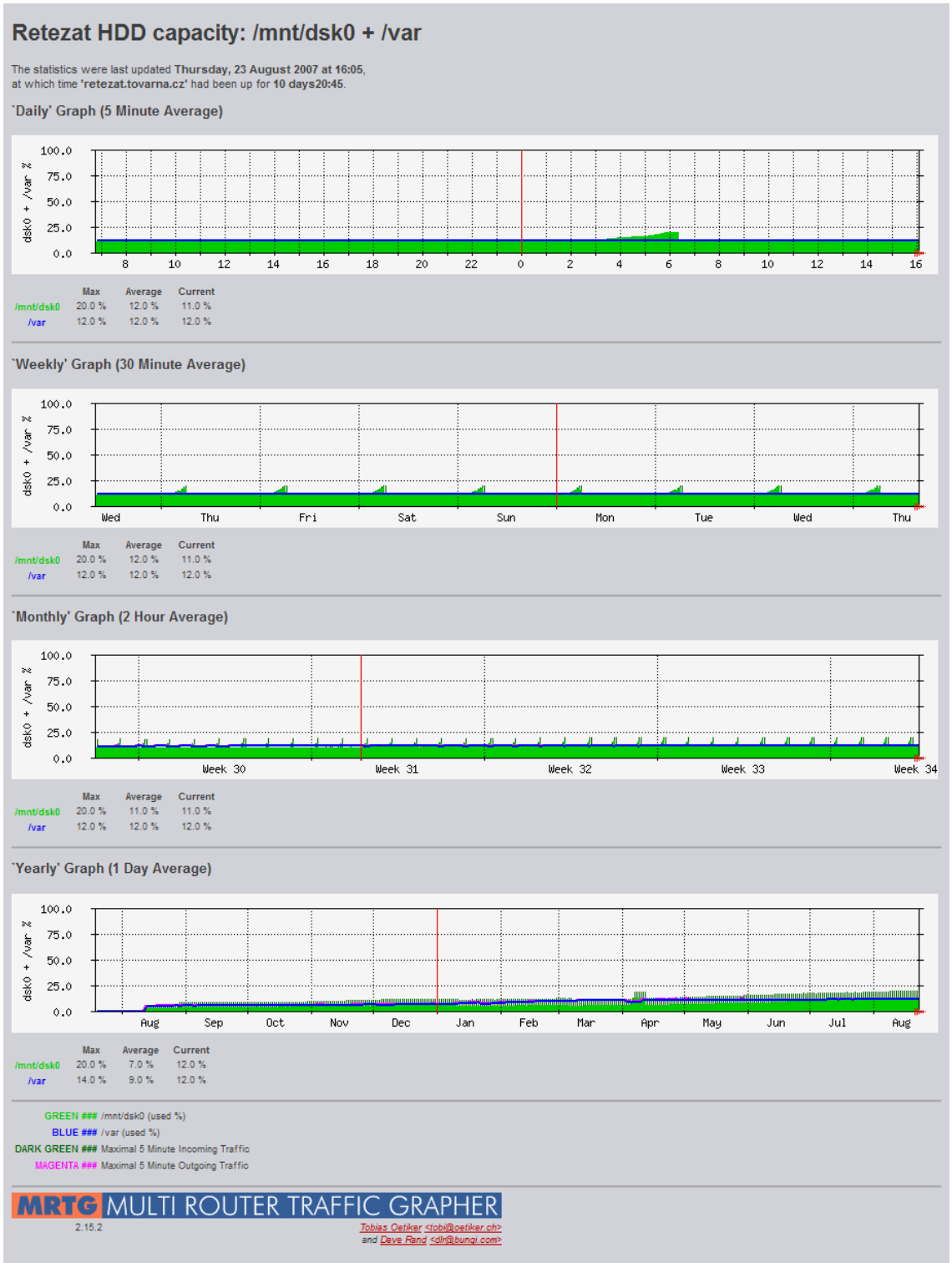
Příloha 18 - Detailní výstup z MRTG pro Využití paměti RAM



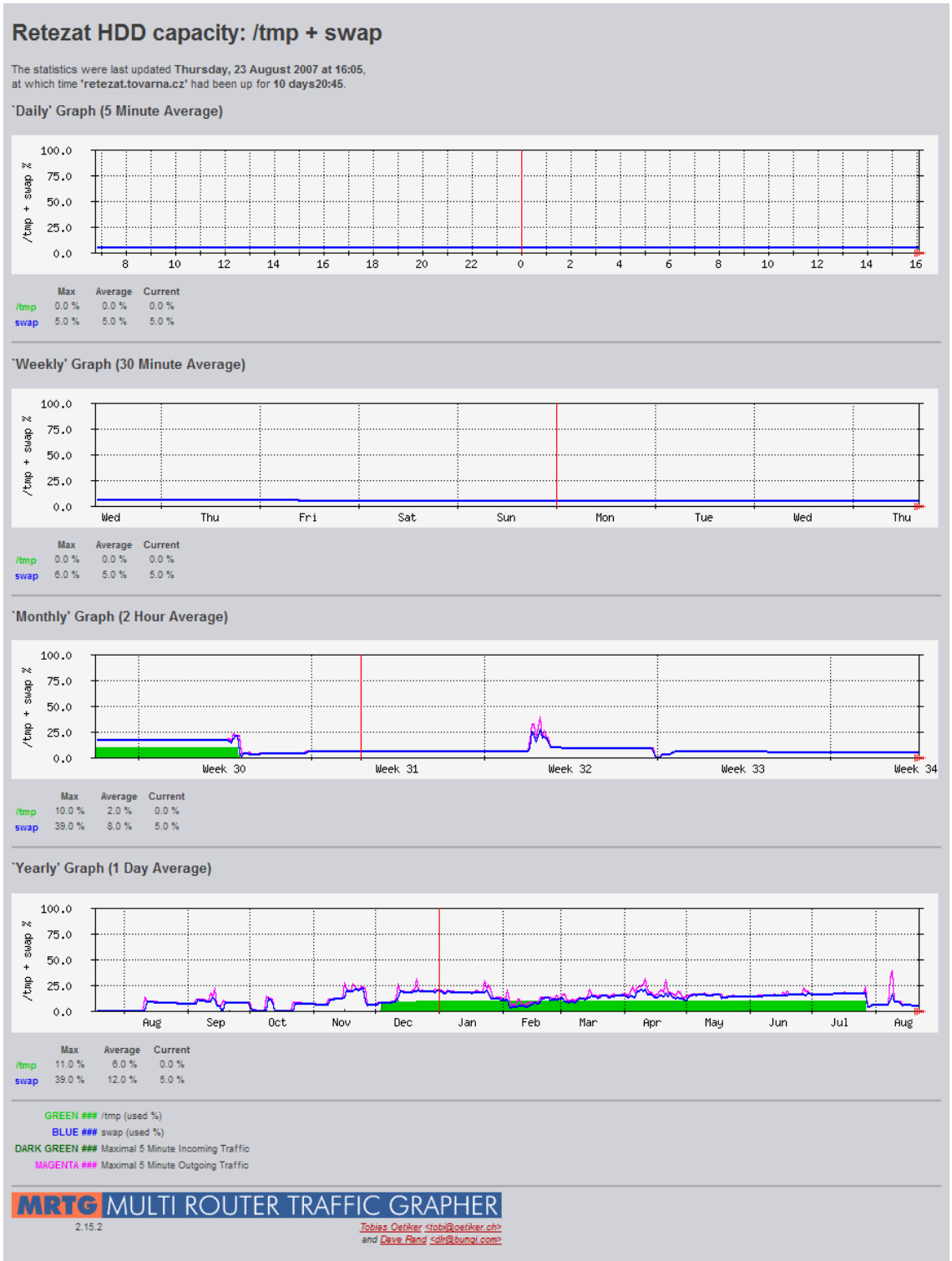
Příloha 19 - Detailní výstup z MRTG pro Využití oddílu disku připojeného k / a /usr



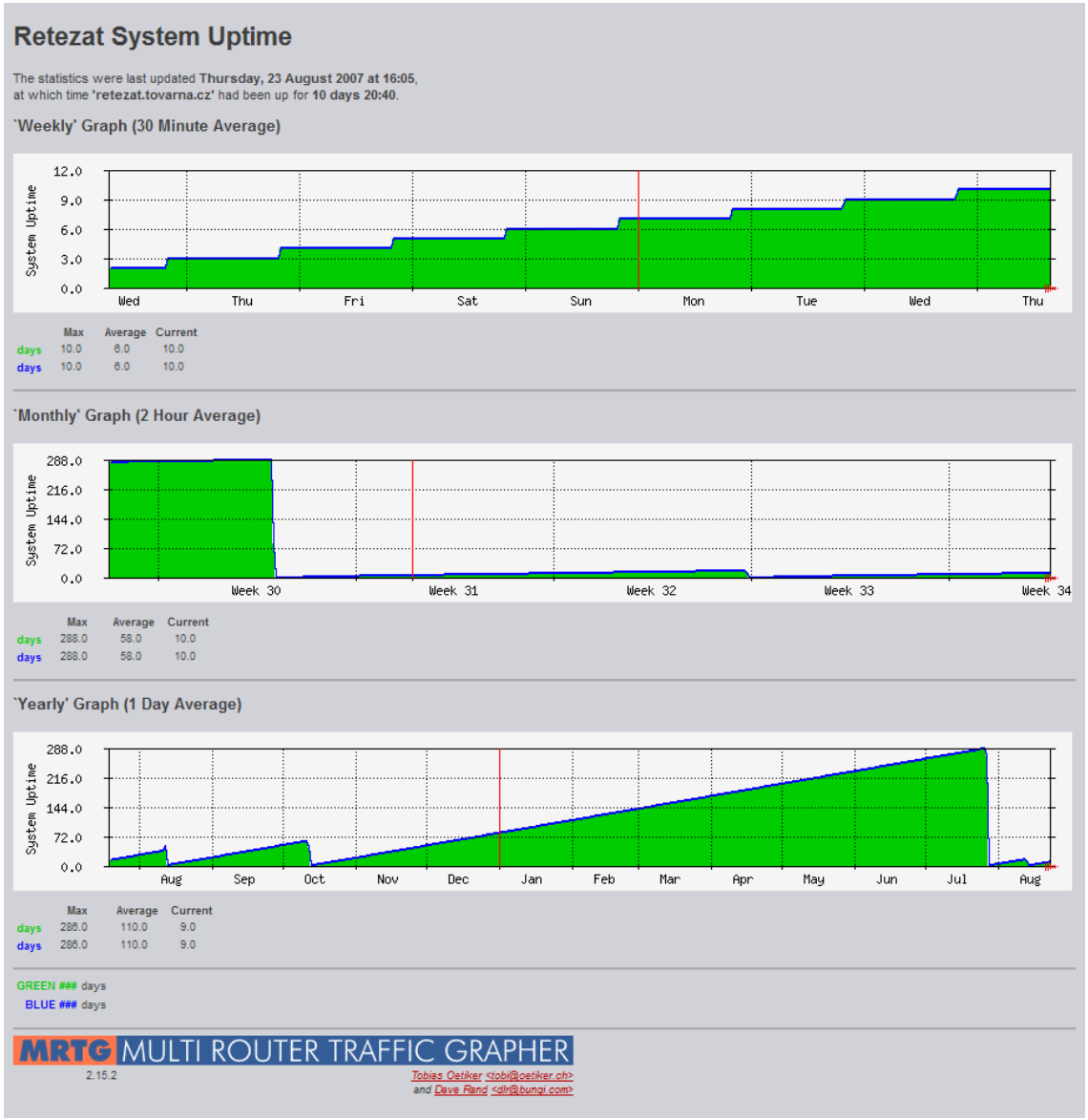
Příloha 20 - Detailní výstup z MRTG pro Využití oddílu disku připojeného k /mnt/dsk0 a /var



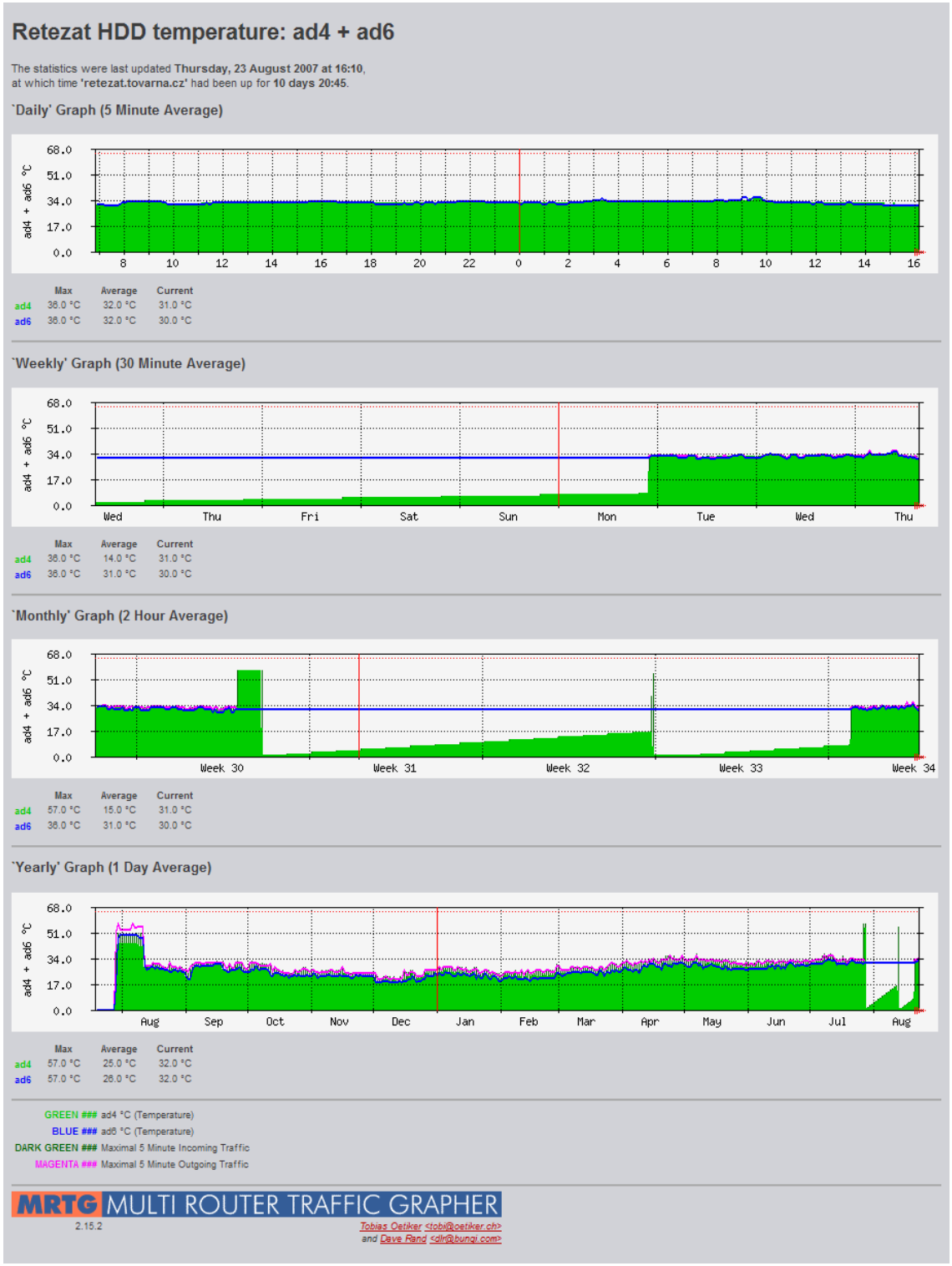
Příloha 21 - Detailní výstup z MRTG pro Využití oddílu disku připojeného k /tmp a odkládací oddíl swap



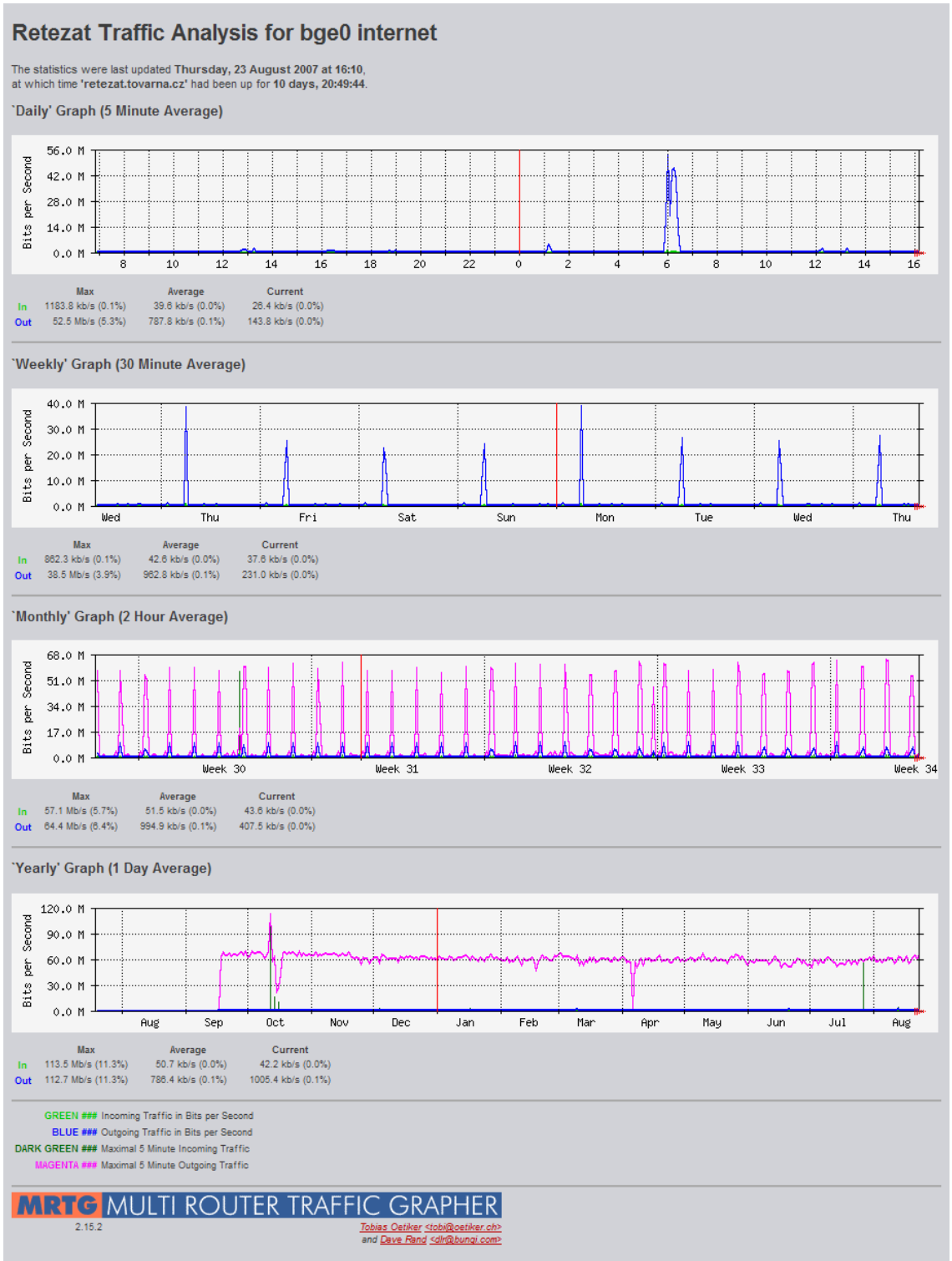
Příloha 22 - Detailní výstup z MRTG pro Uptime



Příloha 23 - Detailní výstup z MRTG pro Výpis teploty disků



Příloha 24 - Detailní výstup z MRTG pro Rychlost přenosu dat na zařízení bg0 (síťová karta)



Příloha 25 - Detailní výstup z MRTG pro Objem přenesených dat na zařízení bg0 (síťová karta)