VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INFORMAČNÍCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INFORMATION SYSTEMS

SROVNÁNÍ SYSTÉMŮ PRO SLEDOVÁNÍ PROVOZU POČÍTAČOVÝCH SÍTÍ

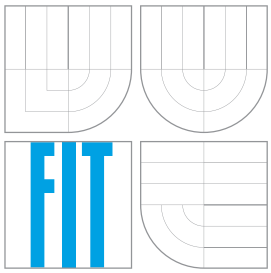
BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE
AUTHOR

LUKÁŠ VOZDECKÝ

BRNO 2007

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INFORMAČNÍCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INFORMATION SYSTEMS

SROVNÁNÍ SYSTÉMŮ PRO SLEDOVÁNÍ PROVOZU POČÍTAČOVÝCH SÍTÍ

COMPARISON OF SYSTEMS FOR MONITORING OF COMPUTER NETWORKS

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — LUKÁŠ VOZDECKÝ
AUTHOR

VEDOUCÍ PRÁCE — Ing. RUDOLF ČEJKA
SUPERVISOR

BRNO 2007

Zadání bakalářské práce/3458/2006/xvozde03

Vysoké učení technické v Brně - Fakulta informačních technologií

Centrum výpočetní techniky

Akademický rok 2006/2007

Zadání bakalářské práce

Řešitel: **Vozdecký Lukáš**
Obor: Informační technologie
Téma: **Srovnání systémů pro sledování provozu počítačových sítí**
Kategorie: Počítačové sítě

Pokyny:

1. Seznamte se s problematikou sledování provozu počítačových sítí a dostupnosti služeb.
2. Vyhledejte a vyzkoušejte různé monitorovací systémy, jako jsou např. Nagios, Zabbix nebo BigSister.
3. Zjistěte možnost jejich nasazení z hlediska potřeb v reálném provozu.
4. Zhodnoťte jednotlivé systémy a navrhněte nejlepší řešení.

Literatura:

- Projekt Nagios (http://nagios.org/)
- Projekt Zabbix (http://www.zabbix.org/)
- Projekt BigSister (http://bigsister.graeff.com/)

Při obhajobě semestrální části projektu je požadováno:

- Splnění bodů 1 a 2.

Podrobné závazné pokyny pro vypracování bakalářské práce naleznete na adrese http://www.fit.vutbr.cz/info/szz/

Technická zpráva bakalářské práce musí obsahovat formulaci cíle, charakteristiku současného stavu, teoretická a odborná východiska řešených problémů a specifikaci etap (20 až 30% celkového rozsahu technické zprávy).

Student odevzdá v jednom výtisku technickou zprávu a v elektronické podobě zdrojový text technické zprávy, úplnou programovou dokumentaci a zdrojové texty programů. Informace v elektronické podobě budou uloženy na standardním paměťovém médiu (disketa, CD-ROM), které bude vloženo do písemné zprávy tak, aby nemohlo dojít k jeho ztrátě při běžné manipulaci.

Vedoucí: **Čejka Rudolf, Ing.**, CVT FIT VUT
Datum zadání: 1. listopadu 2006
Datum odevzdání: 15. května 2007

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
Fakulta informačních technologií
Ústav informačních systémů
612 66 Brno, Božetěchova 2

L.S.

doc. Ing. Jaroslav Zendulka, CSc.
vedoucí ústavu

LICENČNÍ SMLOUVA
POSKYTOVANÁ K VÝKONU PRÁVA UŽÍT ŠKOLNÍ DÍLO

uzavřená mezi smluvními stranami

1. Pan

Jméno a příjmení: **Lukáš Vozdecký**
Id studenta: 84105
Bytem: Foltýnova 9, 635 00 Brno
Narozen: 18. 07. 1983, Brno
(dále jen "autor")

a

2. Vysoké učení technické v Brně

Fakulta informačních technologií
se sídlem Božetěchova 2/1, 612 66 Brno, IČO 00216305
jejímž jménem jedná na základě písemného pověření děkanem fakulty:

.....
(dále jen "nabyvatel")

Článek 1
Specifikace školního díla

1. Předmětem této smlouvy je vysokoškolská kvalifikační práce (VŠKP):
bakalářská práce

Název VŠKP: Srovnání systémů pro sledování provozu počítačových sítí
Vedoucí/školitel VŠKP: Čejka Rudolf, Ing.
Ústav: Centrum výpočetní techniky
Datum obhajoby VŠKP: .....

VŠKP odevzdal autor nabyvateli v:
tištěné formě počet exemplářů: 1
elektronické formě počet exemplářů: 2 (1 ve skladu dokumentů, 1 na CD)

2. Autor prohlašuje, že vytvořil samostatnou vlastní tvůrčí činností dílo shora popsané a specifikované. Autor dále prohlašuje, že při zpracovávání díla se sám nedostal do rozporu s autorským zákonem a předpisy souvisejícími a že je dílo dílem původním.
3. Dílo je chráněno jako dílo dle autorského zákona v platném znění.
4. Autor potvrzuje, že listinná a elektronická verze díla je identická.

Článek 2
Udělení licenčního oprávnění

1. Autor touto smlouvou poskytuje nabyvateli oprávnění (licenci) k výkonu práva uvedené dílo nevýdělečně užít, archivovat a zpřístupnit ke studijním, výukovým a výzkumným účelům včetně pořizování výpisů, opisů a rozmnoženin.
2. Licence je poskytována celosvětově, pro celou dobu trvání autorských a majetkových práv k dílu.
3. Autor souhlasí se zveřejněním díla v databázi přístupné v mezinárodní síti:
   - ☒ ihned po uzavření této smlouvy
   - ☐ 1 rok po uzavření této smlouvy
   - ☐ 3 roky po uzavření této smlouvy
   - ☐ 5 let po uzavření této smlouvy
   - ☐ 10 let po uzavření této smlouvy

   (z důvodu utajení v něm obsažených informací)
4. Nevýdělečné zveřejňování díla nabyvatelem v souladu s ustanovením § 47b zákona č. 111/ 1998 Sb., v platném znění, nevyžaduje licenci a nabyvatel je k němu povinen a oprávněn ze zákona.

Článek 3
Závěrečná ustanovení

1. Smlouva je sepsána ve třech vyhotoveních s platností originálu, přičemž po jednom vyhotovení obdrží autor a nabyvatel, další vyhotovení je vloženo do VŠKP.
2. Vztahy mezi smluvními stranami vzniklé a neupravené touto smlouvou se řídí autorským zákonem, občanským zákoníkem, vysokoškolským zákonem, zákonem o archivnictví, v platném znění a popř. dalšími právními předpisy.
3. Licenční smlouva byla uzavřena na základě svobodné a pravé vůle smluvních stran, s plným porozuměním jejímu textu i důsledkům, nikoliv v tísni a za nápadně nevýhodných podmínek.
4. Licenční smlouva nabývá platnosti a účinnosti dnem jejího podpisu oběma smluvními stranami.

V Brně dne: .....

.....

Nabyvatel

.....

Autor

Abstrakt

Práce se zabývá srovnáním tří open–source Linux/Unix aplikací Nagios, Zabbix, Big Sister sloužících k monitorování stavu a služeb počítačové sítě. Pro každou aplikaci je uveden stručný princip konfigurace a sledování sítě. Pro srovnání je použit seznam akcí a problémů, se kterými se lze v běžném provozu setkat nejčastěji. Pro jednotlivé aplikace je pak naznačen způsob řešení, včetně konkrétního postupu v dané aplikaci.

Klíčová slova

Nagios, Zabbix, Big Sister, jak monitorovat počítačovou síť, nástroje pro monitorování počítačové sítě

Abstract

This thesis is comparison of three open–source Linux/Unix network monitoring applications Nagios, Zabbix, Big Sister. Every application is described according to its basic fundamentals. The comparison is done through managing series of tests based on real environment experience. Solution to these problems and specific procedure differencies are described for each application.

Keywords

Nagios, Zabbix, Big Sister, how to monitor computer network, network monitoring tools

Citace

Lukáš Vozdecký: Srovnání systémů pro sledování provozu počítačových sítí, bakalářská práce, Brno, FIT VUT v Brně, 2007

Srovnání systémů pro sledování provozu počítačových sítí

Prohlášení

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně pod vedením pana Ing. Rudolfa Čejky. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

. . . . . .
Lukáš Vozdecký
10. května 2007

Obsah

Kapitola 1

Úvod

Rozvoj počítačových technologií je do značné míry ekvivalentní pojmu rozvoj počítačových sítí a jejich údržba. Počítačové služby jsou zřídka poskytovány a využívany jiným způsobem než prostřednictvím počítačové sítě. Kvalita služeb je tak přímo úměrná efektivnímu monitorování síťového provozu.

Problematikou práce je porovnání tří nejrozšířenějších open-source aplikací pro monitorování síťových prvků Nagios, Zabbix a Big Sister. Jsou uvedeny obecné informace o způsobu konfigurace a fungování jednotlivých aplikací včetně obecné struktury konfiguračních souborů i konkrétních příkladů.

Podat přesný popis všech atributů jednotlivých aplikací není cílem této práce. Informace tohoto typu jsou detailně probrány zde [5, 6, 3]. Studium a používání této dokumentace je doporučeno paralelně se studiem této prací. Zároveň je předpokládáno alespoň letmé seznámení se s problematikou sledování provozu počítačových sítí.

Stěžejním bodem práce je soubor nejčastějších akcí, se kterými se osoba pověřená správou a monitorováním sítě může setkat v praxi. Mezi tyto akce patří různá nastavení v souvislosti s notifikací o nedostupnosti služeb. Dále pak specifikace různých monitorovacích intervalů pro různé služby s ohledem na aktuální stav, ve kterém se daná služba nachází. V poslední řadě pak podrobnější monitorování vzdálených stanic.

Tyto úkony jsou stejné pro každou aplikaci, a jsou zpracovány v závěrečných kapitolách jednotlivých sekcí. Přístup a efektivita jejich řešení jsou pak hlavním kritériem při srovnání monitorovacích aplikací.

Obecné aspekty monitorovacích aplikací, které nebylo možné zařadit a porovnat v rámci jednotlivých systémů, jsou dodatečně zmíněny v závěrečné kapitole Srovnání Nagios, Zabbix a Big Sister. Zároveň je zde upozorněno na podstatné rozdíly jednotlivých aplikací a z nabízených řešení doporučeno to nejefektivnější.

Kapitola 2

Nagios

2.1 Prerekvizity

Monitorovácí aplikace Nagios je open-source k dispozici na http://www.nagios.org. Provoz vyžaduje následující komponenty

- **OS typu Linux/Unix**
- **Nagios-plugins**

  Jedná se o několik skriptů nebo binárních souborů, které jsou samostaně schopny vyhodnotit dostupnost určité služby a výsledek předat hlavní aplikaci.
- **Web server**

  Doporučen Apache s podporou gd knihovny Thomase Boutella verze 1.6.3 nebo novější (požadováno pro stavovou mapu a trendy CGI).
- **NRPE**

  Nagios agent pro monitorování vzdálených stanic s OS typu Linux/Unix.
- **NSClient++**

  Nagios agent pro monitorování vzdálených stanic s OS typu Windows. K dispozici na http://sourceforge.net/projects/nscplus.

Podrobnější informace k této problematice viz [5].

2.2 Konfigurace

2.2.1 Server

Serverové rozhraní Nagios je konfigurováno prostřednictvím několika textových souborů. Veškeré změny v konfiguračních souborech si vyžadují restart procesu, aby nabyly platnosti.

Hlavní konfigurační soubor
Základním prvkem konfigurace je hlavní konfigurační soubor, který je předáván při spuštění programu jako parametr. První skupinou dat jsou cesty k ostatním konfiguračním souborům, log souboru a stavovému souboru (obsahuje data popisující výsledky monitorování, která jsou projektována na webové rozhraní). Další skupinou nastavení je povolení nebo zakázání určitých aspektů monitorování (notifikace, externí příkazy).

Makro soubor
Obsahuje uživatelem definovaná makra, která lze použít např. v definici příkazu. Jak se makra používájí je objasněno zde [5].

Soubory s objekty monitorování
Obsahují data, která se vztahují k tomu, co se bude monitorovat. Lze zde definovat a popsat tyto základní typy objektů:

- **Služby –** `service`

  Vztahují se vždy k nějakému objektu typu stanice a popisují jeho vlastnosti (zátěž procesoru, volné místo na pevném disku) nebo jím poskytované služby (ftp, http).

- **Skupina služeb –** `servicegroup`

  Skupina objektů typu služba.

- **Stanice –** `host`

  Fyzické zařízení na síti, ke kterému se vztahují vybrané služby nebo jich využívá.

- **Skupina stanice –** `hostgroup`

  Skupina objektů typu stanice.

- **Kontakt –** `contact`

  Osoby, na jejichž kontaktní adresu (email, telefonní číslo) bude doručena notifikace.

- **Skupina kontaktů –** `contactgroup`

  Skupina objektů typu kontakt.

- **Příkazy –** `command`

  Obsahují volání programu nebo skriptu, ktera budou spuštěny v rámci monitorovací nebo notifikační akce (např. notifikace pomocí emailu, použije k rozeslání zprávy program mail, tělo zprávy bude obsahovat informace o monitorované službě. V syntaxi Nagiosu bude toto reprezentováno jedním příkazem `notify-by-email`).

- **Časový úsek –** `timeperiod`

  Určuje dobu, po kterou budou stanice a služby monitorovány a rozesílány notifikace.

CGI konfigurační soubor
Webové rozhraní Nagios je konstruováno prostřednictvím CGI skriptů. V konfiguračním souboru jsou uloženy informace o umístění html souborů, o zavedení autentizovaného přístupu a další data podobného charakteru.

2.2.2 Agent

Agent Nagios (NRPE, NSClient++) je konfigurován jedním textovým souborem. Neobsahuje žádná data podobná konfiguračním souborům serverové části aplikace. Nejdůležitějšími udáji je seznam IP adres Nagios serverů, se kterými má agent povoleno komunikovat.

2.3 Monitorování provozu

Soubory s objekty monitorování obsahují struktury (typy objektů) jejichž součástí jejichž součástí jsou nagios-pluginy, což znamená, že konkrétní typ objektu (stanice, služba) jsou monitorovány prostřednictvím tohoto pluginu.

2.3.1 Kontrola stanic

Kontroly stanic jsou prováděny v rámci sktruktury Stanice v Souborech s objekty monitorování. Monitorování je v případě Kontroly stanic plně řízeno Nagiosem.

Význam Kontroly stanic spočívá v otestování dostupnosti zařízení, pokud libovolná Kontrola služby vrátí status non-OK, tzn. zda je cílové zařízení vůbec k dispozici, zda má smysl provádět na tomto zařízení další s ním asociované Kontroly služeb.

2.3.2 Kontrola služeb

Kontroly služeb jsou prováděny v rámci sktruktury Služba v Souborech s objekty monitorování. Kontroly služeb jsou hlavní prostředek pro monitorování sítě.

Struktura Služba obsahuje zejména tyto položky. Služba se vztahuje k zařízení v `host_name`, plugin je uveden v `check_command` a může vyžadovat další parametry. Položka `contact_groups` určuje skupinu uživatelů, která obdrží případné notifikace. Seznam a popis všech položek struktury zde najít v [5].

2.4 Použití v praxi

Interval monitorování
Vyhodnocení statutu služby (dostupná – OK, nedostupná – CRITICAL) probíhá na základě několika pokusů s různými časovými intervaly mezi jednotlivými pokusy. Pro některé služby je vhodné použít delší časovou prodlevu, větší počet opakování, pro jiné tomu může být naopak. Položka `max_check_attempts` určuje počet pokusů (počet spuštění pluginu `check_ftp`), po kterých bude status vyhodnocen jako CRITICAL. Mezi pokusy je interval `retry_check_interval` minut. Pokud bude služba vyhodnocena jako OK, další testování následuje za `normal_check_interval` minut.

```
define service{
        host_name                       localhost
        service_description             ftp-localhost
        check_period                    24x7
        max_check_attempts              4
        normal_check_interval           5
        retry_check_interval            1
        contact_groups                  admins
```

```
        notification_interval           960
        notification_period             24x7
        notification_options            w,u,c,r
        check_command                   check_ftp
        }
```

Timeout
Maximální doba, po kterou se bude testování služby (Kontrola služby) pokoušet o úspěšný dotaz pluginem, je v hlavním konfiguračním souboru položka `service_check_timeout`. Standartně je tato hodnota nastavena 10*s*. Timeout lze měnit i přímo jako parametr pluginu, pokud je podporován.

Notifikace
Položka `contact_groups` ve struktuře Služba určuje skupinu kontaktů, kterým se budou zasílat notifikace o stavu služby.

```
define service{
        host_name                       localhost
        service_description             Current Load
        contact_groups                  admins
        ...
        }
```

Kontakt ze skupiny kontaktů ma ve své struktuře emailovou adresu, příkazy pro jednotlivé notifikace `service_notification_commands`, `host_notification_commands` a omezení příjmu určitých druhů výpadku `service_notification_options`, `host_notification_option`.

```
define contactgroup{
        contactgroup_name               admins
        alias                           Nagios Administrators
        members                         nagios-admin
        }

define contact{
        contact_name                    nagios-admin
        alias                           Nagios Admin
        service_notification_period     24x7
        host_notification_period        24x7
        service_notification_options    w,u,c,r
        host_notification_options       d,r
        service_notification_commands   notify-by-email
        host_notification_commands      host-notify-by-email
        email                           nagios-admin@localhost
        }
```

Tělo příkazu, formát zprávy a aplikace, která zasílá notifikaci je specifikována ve struktuře Příkaz v `command_line`.

```
define command{
command_name host-notify-by-email
command_line /usr/bin/printf "%b" "***** Nagios @VERSION@ *****\n\n
             Notification Type: $NOTIFICATIONTYPE$\nHost: $HOSTNAME$
             \n State: $HOSTSTATE$\nAddress: $HOSTADDRESS$\nInfo:
             $HOSTOUTPUT$\n\nDate/Time: $LONGDATETIME$\n"
             | @MAIL_PROG@ -s "Host $HOSTSTATE$ alert for
             $HOSTNAME$!" $CONTACTEMAIL$
         }

define command{
         command_name notify-by-email
         ...
         }
```

Notifikace s ohledem na hierarchii sítě
Při složitější topologii sítě, kdy některé její prvky tvoří podsítě a jsou dostupné(status UP) přes prvky typu router apod., je neefektivní přijímat notifikace o nedostupnosti(status DOWN) služeb na počítačích v podsíti, pokud je samotná podsíť (resp. router, spojující podsíť se zbytkem sitě) nedostupná. Položka `parents` ošetřuje tuto situaci. Pokud je stanice Router1 DOWN, je stanici Pc1 přiřazen místo statutu DOWN, status UNREACHABLE. Položka `notification_options` pak umožňuje regulovat zasílání notifikací, v tomto případě není přítomna podmínka na zaslání notifikace při statutu UNREACHABLE(u).

```
define host{
        host_name               Pc1
        parents                 Router1
        alias                   Web Server
        address                 192.168.1.5
        check_command           check-host-alive
        max_check_attempts      10
        notification_interval   120
        notification_period     24x7
        notification_options    d,r
        }
```

Testování dostupnosti služeb při nedostupnosti stanice
Pokud libovolná Kontrola služby vrátí non-OK status,provede se příkaz `check-host-alive`, který je zodpovědný za zjištění statusu zařízení. Dokud `check-host-alive` nevrátí status OK, nebude se Nagios pokoušet monitorovat služby na daném zařízení.

Flapping
Nagios podporuje speciální ošetření stavu, kdy stanice nebo služba mění svůj stav velmi často. Více o této problematice v dokumentaci [5].

Monitorování vzdálených stanic
Získání privátních informací (zátěž CPU) ze vzdálených stanic zajišťuje v prostředí Nagios agent (NRPE pro Linux/Unix, NSClient++ pro OS Windows), který musí běžet na vzdáleném počítači.

Spolu s NRPE musí být na vzdálené stanici nainstalovány nagios-pluginy. Volání příkazu na vzdálené stanici ze serveru se provádí prostřednictvím speciálního `check_nrpe` pluginu. Struktury v konfiguračním soubou na straně serveru vypadají takto.

```
define service{
          host_name            remotehost
          service_description Current Users
          check_command        check_nrpe!check_users
          ...
          }

define command{
          command_name check_nrpe
          command_line /usr/local/nagios-plugins/check_nrpe
                       -H $HOSTADDRESS$ -c $ARG1$
          }
```

Pro Windows je třeba nainstalovat NSClient++, postup je analogický, pouze místo `ckeck_nrpe` pluginu se použije plugin `ckeck_nt`.

Vzdálené služby lze testovat přes vzdálené připojení SSH pluginem `check_by_ssh`, který nevyžaduje agenta na vzdálené stanici. Princip je podobný jako u výše uvedených pluginů, syntaxe použití je však jiná. Pro přesný popis více na [5].

Obsluha událostí

Obsluha události dovoluje spustit v okamžiku problému uživatelem vytvořený skript, který by se měl pokusit službu opravit např. restartovat službu. Architektura Nagios automaticky definuje, kdy je takový skript spuštěn. Nejprve se pokusí spustit skript v okamžiku předposledního testování služby (test v pořadí `max_check_attempts - 1`) než je proveden poslední test před vyvoláním notifikace. A pak ještě jednou pokud poslední test (test v pořadí `max_check_attempts`) selže. Pokud od této chvíle služba přetrvává v CRITICAL stavu bude skript volán jednou za `normal_check_interval` dobu. Obsluha události musí být povolena v hlavním konfiguračním souboru v `enable_event_handlers` i u samotné služby `event_handler_enabled`.

Následující konfigurací se pomocí skriptu script-restart-ftd Nagios pokusí restartovat FTP službu způsobem popsaným výše. Cesta ke skriptu a jeho indentifikátor je definován ve struktuře typu Command.

```
define service{
         host_name                  localhost
         service_description        ftp-localhost
         max_check_attempts         4
         event_handler              restart-ftp
          event_handler_enabled      1
         ...
         }

define command{
         command_name restart-ftp
         command_line /usr/local/nagios-scripts/script-restart-ftp
         }
```

Rozšíření: Existují příkazy, které lze předat Nagiosu z jiných aplikací (např. prostřednictvím CGI rozhraní lze předat příkaz, který na specifickou dobu zruší všechny kontroly služeb týkající se počítače pc1). Příkaz se zapíše do souboru nagios.cmd, který je Nagiosem kontrolován jednou za `command_check_interval` sekund (lze nastavit v hlavním konfiguračním souboru). Seznam již vytvořených příkazů a jejich syntaxe je k dispozici v [5].

Možnosti webového rozhraní
Nagios nelze primárně konfigurovat prostřednictvím webového rozhraní tzn. nelze měnit obsah konfiguračních souborů, přidávat nové stanice nebo služby. U monitorovaných služeb však lze např. plánovat jejich provádění, vypnout/zapnout obsluhu události nebo notifikaci.

Tvorba vlastních testovacích skriptů a aplikací
Nagios podporuje tvorbu nových a modifikaci stávajících pluginů. Více zde [5, 4].

Kapitola 3

Zabbix

3.1 Prerekvizity

Monitorovácí aplikace Zabbix je open-source k dispozici na http://www.zabbix.org. Provoz vyžaduje následující komponenty

- **OS typu Linux/Unix**
- **Apache**

  Verze 1.3.12 nebo novější.
- **MySQL (nebo PostgreSQL)**

  Verze 3.22 MySQL nebo novější. Versze 7.0.2 PostgreSQL nebo novější. MySQL nebo PostgreSQL knihovny.
- **PHP**

  Verze 4.0 nebo novější jako Apache modul.
- **PHP GD nebo GD2 modul**

  Nutné pro zobrazení grafů a map, podpora PNG grafického formátu.

Podrobnější informace k této problematice zde [6].

3.2 Konfigurace

3.2.1 Server

Serverová část Zabbix využívá pro základní nastavení konfigurace jeden konfigurační soubor. Soubor neobsahuje data, která bezprostředně souvisí s konfigurací monitorovaní. Konfigurační data se týkají nastavení přístupu k databázi, umístění logovacího souboru atd.

3.2.2 Webové rozhraní

Konfigurace elementů týkajících se samotného monitorovaní probíhá výhradně přes webové grafické rozhraní v sekci Configuration.

Nastavení informačních parametrů je v podsekci General (Users, Housekeeper, Working Time) Lze ponechat implicitní, je podobné i pro různé typy sledovaných sítí.

Základní konfigurace, zajišťující monitorování libovolné služby nebo stroje na síti, lze provést konkrétním nastavením v podsekcích Hosts, Items, Triggers, Actions. Notifikaci zajistí nastavení v Media Types, Media, Users.

Sekce Maps, Graphs, Screens zprostředkovávají výstup monitorování do uživatelsky pohodlného formátu. Sekce Screens umožňuje nakombinovat několik grafů vedle sebe a celou síť tak je možné sledovat na jedné obrazovce.

Configuration → Hosts
V této sekci lze objekty v síti zanést do Zabbixu a zajistit tak jejich sledování. Nová stanice se do systému přidá vyplněním formuláře, pomocí kterého lze stanici přiřadit i další atributy. Lze použít speciální šablonu (Link with template), která podle povahy stroje (OS Windows nebo Unix, poštovní server, databázový server) automaticky zavede služby, které se pro daný typ předpokládají.

Configuration → Items
Items jsou způsob, jak do monitorovacího systemu přidat nový element (co a kde má být monitorováno). Zabbix obsahuje několik předdefinovaných Items, které se vážou ke skupine zvolené v Configuration → Hosts pomocí Link with Template. Pokud nechceme monitorovaný objekt zařadit do žádné již předdefinované skupiny, musí se mu Items přiřadit samostatně. Pro přidávání Items je potřeba nastavit uživateli práva v Configuration → Users.

Configuration → Triggers
Pomocí několika proměnných a operátorů lze sestavit výraz, který vrací TRUE, FALSE nebo UNKNOWN. Proměnné v tomto případě představují návratové hodnoty monitorovaných elementů (návratové hodnoty z Items).

Configuration → Actions
Actions využívá Triggers k vygenerování akce, kterou je zpravidla notifikace (email, SMS zpráva) nebo vykonaní vzdáleného příkazu.

Configuration → Users → Media
Nastavení emailové adresy pro zasílání notifikací. V sekci Configuration → General → Media Types je potřeba nastavit totéž a specifikovat typ notifikace (email, SMS).

3.2.3 Agent

Zabbix Agent proces je nutný na všech monitorovaných stanicích včetně serveru. Omezené množství služeb lze provést i bez agenta. Konfigurační soubor obsahuje standartní náležitosti (IP adresu serveru a další).

3.3 Monitorování provozu

Monitorování Zabbix spočívá ve vytvoření dostatečného množství Triggers (jejichž základ tvoří jeden nebo více Items) a jejich použití v Actions pro notifikace. Vizuálně lze sledovat stav sítě

a služeb v sekci Monitoring. Po události Trigger se prochazí všechny Actions a testuje se zda byly splněny i dodatečné podmínky (jméno počítače, stupeň důležitosti události a další). Pokud ano, dojde k odeslaní zprávy, jejíž formát a obsah je součástí Actions formuláře.

Monitorovaný element (Items) může být několika různých typů. Typ se definuje při tvorbě elementů v Items ve formuláři Create Item.

Simple Checks
Nevyžadují na monitorované stanici běžícího agenta. Používají se k monitorovani služeb, které slouží zejména ostatním objektům v síti (ftp, http).

Internal checks
Jedná se o monitorování interních dat zabbixu (např. počet Triggers nebo Items).

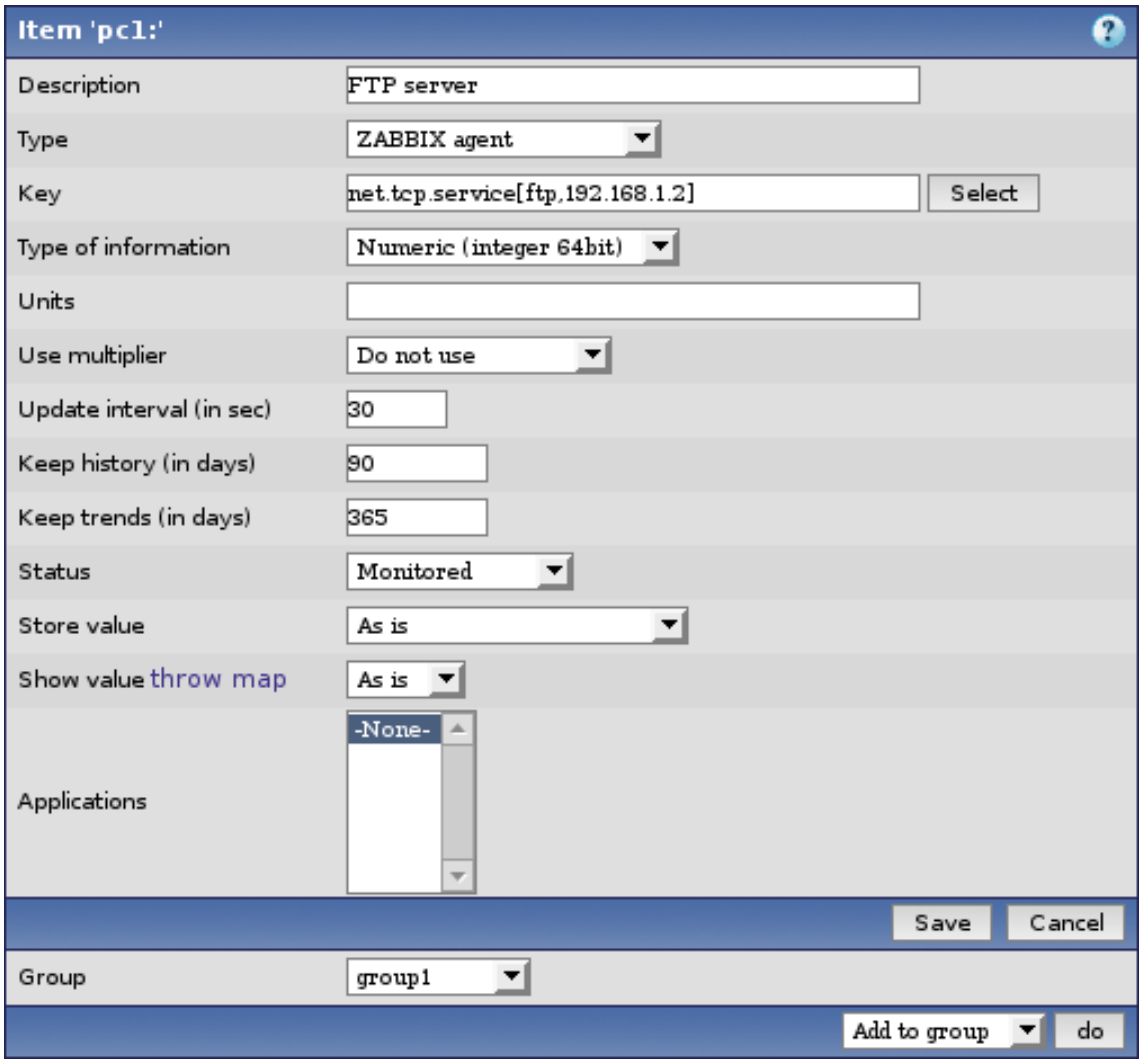
Aggregated checks
Dotazy směřují přímo na databázi zabbixu, ve které jsou uloženy data získaná monitorováním (např. prostřednictvím Simple checks, Agent checks). Na monitorované stanici není vyžadován běžící agent proces.

Agent checks
Umožňují získat private data z monitorovaných počítačů (Volné místo na pevném disku, zátěž CPU). Vyžadují běžící proces zabbix agent, který se liší podle povahy OS.

SNMP checks
Sbírá data od snmp agentů, zabbix musí být nakonfigurován s podporou snmp, viz [6].

3.4 Použití v praxi

Interval monitorování
Při vytvoření nové Item lze v poli Update Interval specifikovat čas(s), po uplynutí této doby se Zabbix bude pokoušet získat novou hodnotu (znovu otestovat službu).



Zabbix provádí automaticky otestování dostupnosti na bázi příkazu ping. V konfiguračním souboru zabbix_server.conf lze pro všechny stanice nastavit interval `PingerFrequency`.

Pokud tento příkaz neuspěje, dostává se stanice do stavu UNREACHABLE. Prostřednictvím položky `UnreachableDelay` určuje frekvenci(s), s jakou se pokoušet o opětovné spojení se stanicí. Hodnota by měla být menší než `PingerFrequency`.

Po uplynutí doby `UnreachablePeriod` se stanice dotane do stavu UNAVAILABLE. Frekvenci, znovu se spojit se stanicí ve stavu UNAVAILABLE, lze opět specifikovat v `UnavailableDelay`. Zde je vhodné nastavit delší dobu než `PingerFrequency`, je málo pravděpodobné, že bude stanice v brzké době dostupná, menší frekvence tak sníží zátěž systému.

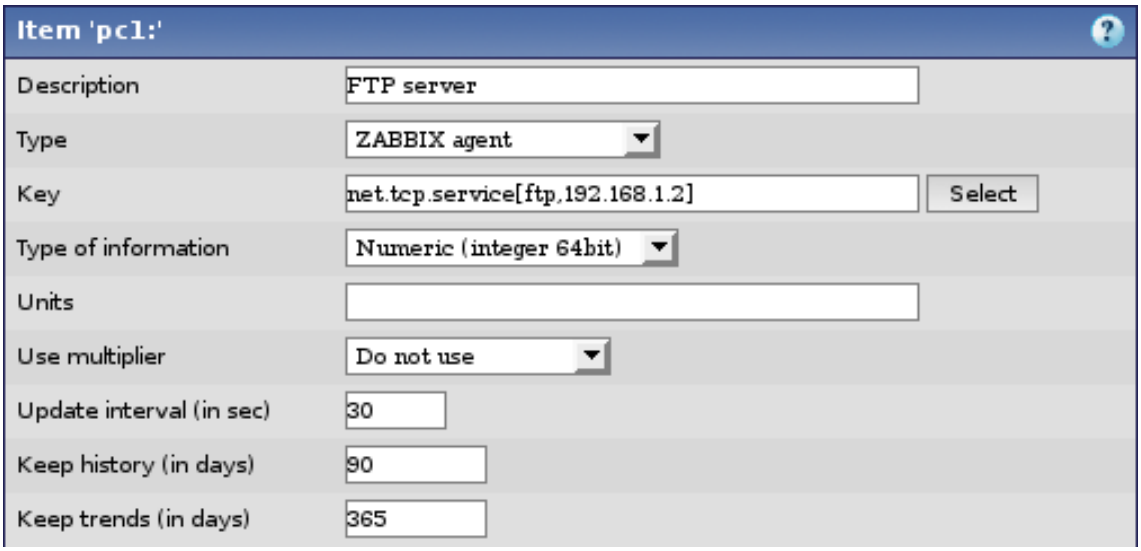
```
#Frequency of ICMP pings.
PingerFrequency=30
```

```
#After how many seconds of unreachability treat a~host as unavailable
UnreachablePeriod=45

#How often check host for availability during the unreachability period
UnreachableDelay=15

#How often check host for availability during the unavailability period
UnavailableDelay=60
```

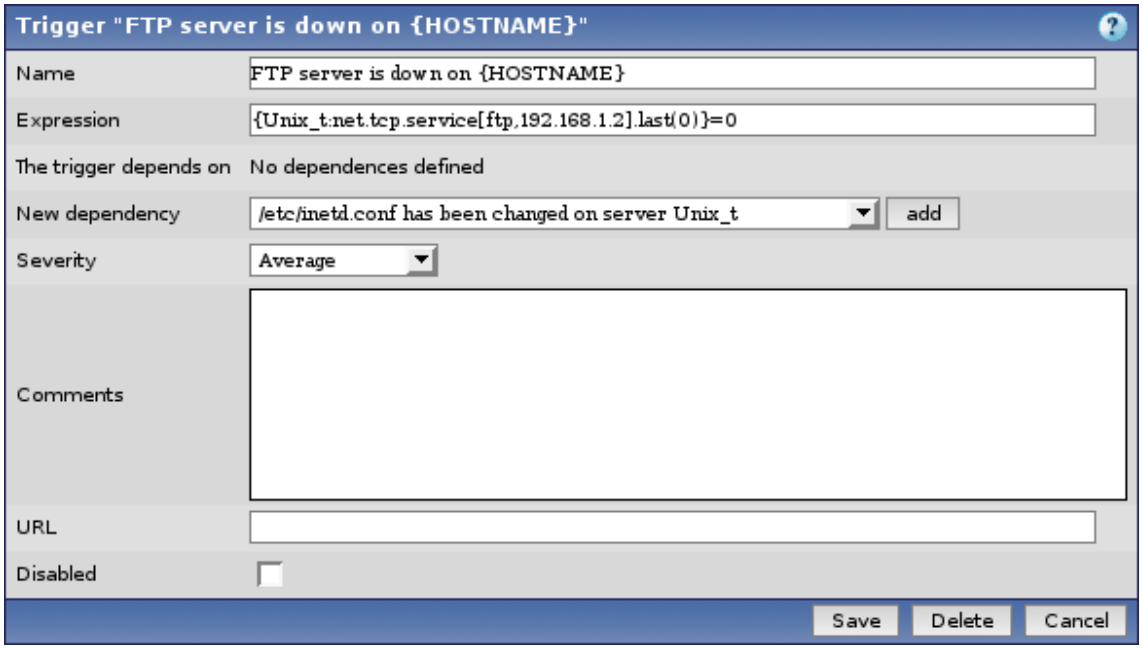
Timeout
Maximální doba, po kterou se bude Zabbix server čekat na agenta až doručí zprávu o stavu sledované služby, jinak vrácí neúspěch.

```
#Specifies how long we wait for agent (in sec)
#Must be between 1 and 30
Timeout=5
```

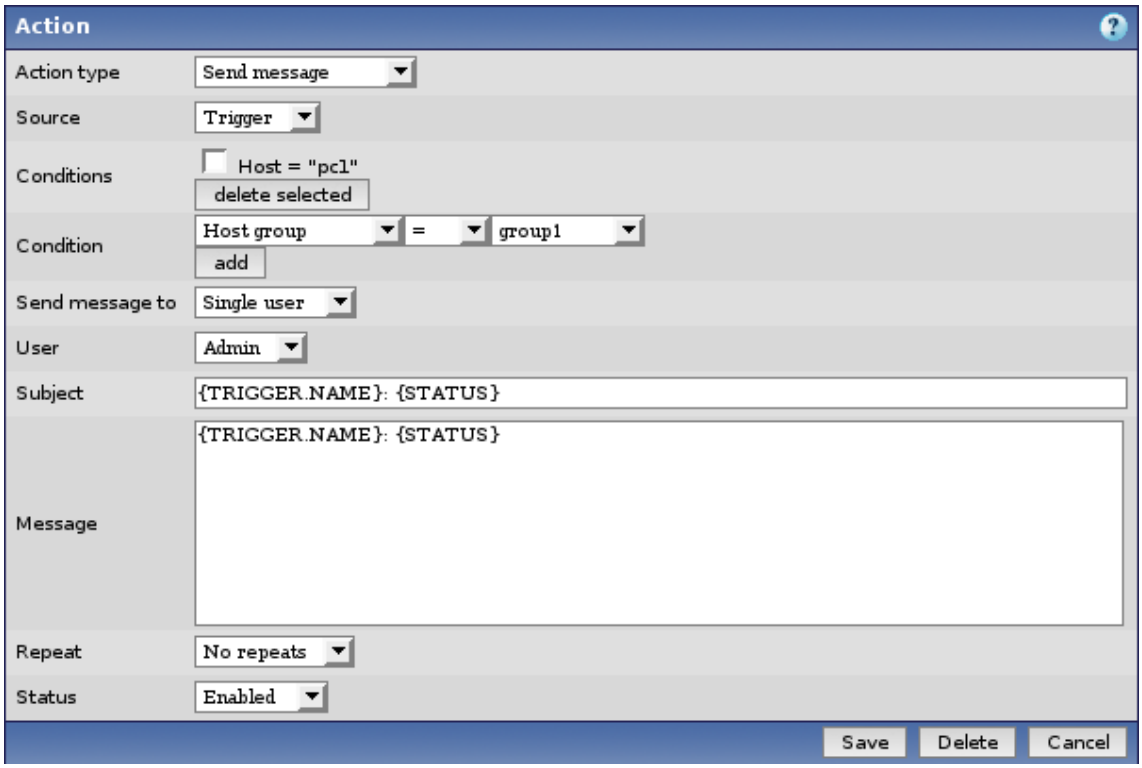
Notifikace
Pro monitorování služeb na lokálním počítači je vytvořena následující Item přes Configuratin → Items → Create Item.



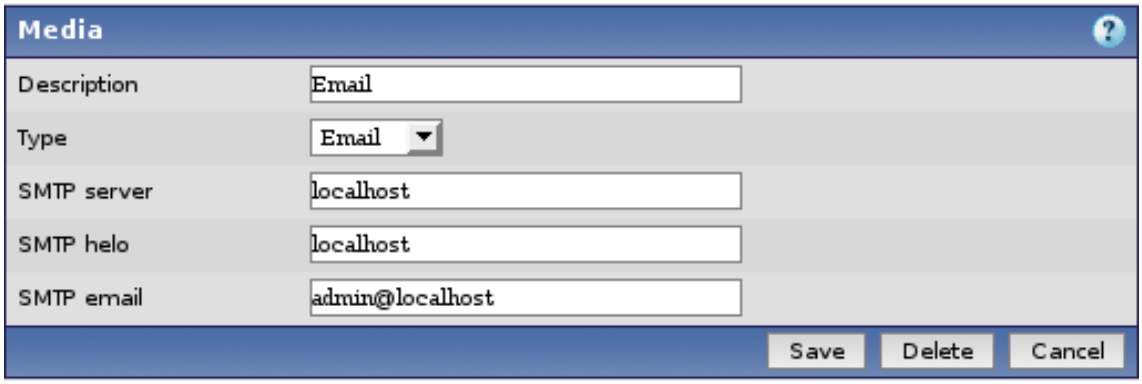
Je vytvořen Trigger přes Configuration → Triggers → Create Trigger. Následující Trigger se spustí pokud Item v těle Triggeru vrátí FALSE.



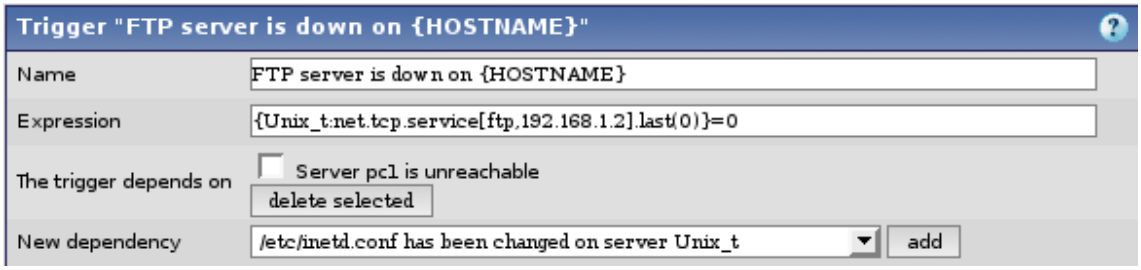
a vyvolá akci Configuration → Actions → Create Action.



kde IP adresa pc1 je 127.0.0.1, zpráva bude zaslána uživateli Admin, jeho emailová adresa se nastavuje v Configuration → User → Media. Rozesílání pošty prostřednictvím Zabbixu se nastavuje v Configuration → General → Media Types.



Notifikace s ohledem na hierarchii sítě
Notifikace je v Zabbixu řešena prostřednictvím Triggers, po jehož spuštění (splnění podmínek) následuje adekvátní odezva. V nastavení Triggeru lze položkou `New dependancy` přidat několik dalších Triggerů, které specifikují omezení pro spuštění. Ke spuštění Triggeru nedojde, pokud některý z Triggerů v `The Trigger depends on`, již byl spuštěn. Nedojde tak k zaslání redundantní notifikace.



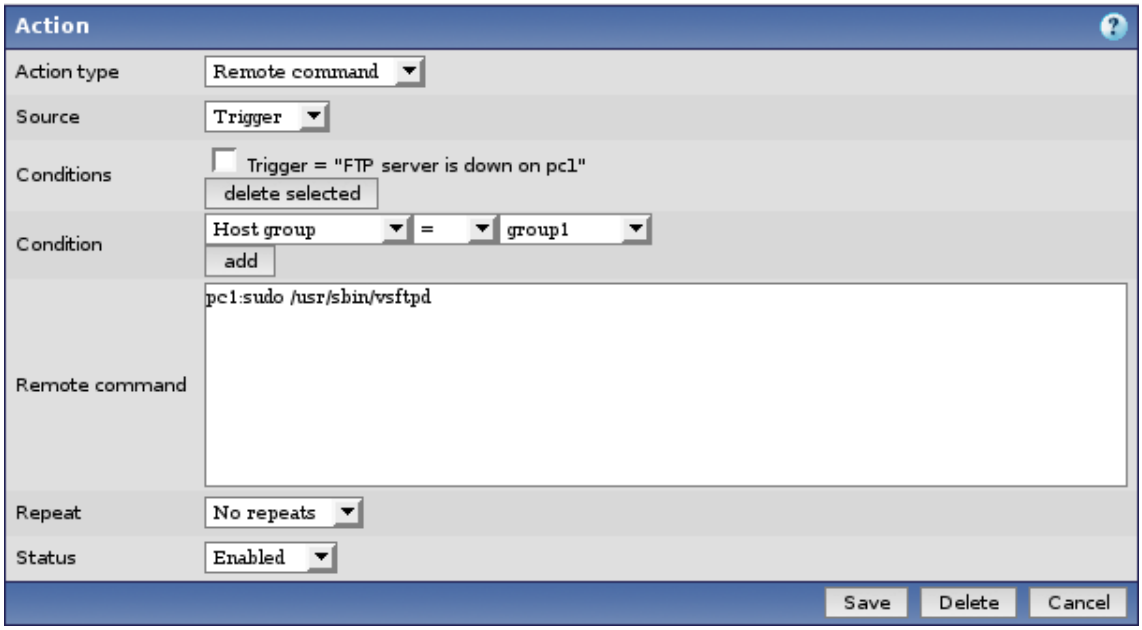
Testování dostupnosti služeb při nedostupnosti stanice
Zabbix neumožňuje ihned automaticky otestovat dostupnost stanice, při nedostupnosti některé z jeho služeb. Po určitou dobu tak dochází k redundantnímu spouštění testovacích skriptů.

Flapping
Automatická detekce stavu flapping není v Zabbix přítomna. Pomocí složitějších Trigger konstrukcí lze docílit podobného efektu, ale výsledek není příliš efektivní.

Monitorování vzdálených stanic
Získání privátních informací (Zátěž CPU) ze vzdálených stanic zajišťuje v prostředí Zabbix výhradně zabbix agent, který musí běžet na vzdáleném počítači. Při vytváření Items, týkajících se lokálních dat na vzdáleném počítači, není potřeba žádného specifického postupu. V tomto případě se postupuje stejně jako u Items týkajících se lokálního počítače.

Obsluha událostí
Obsluha události dovoluje spustit v okamžiku problému uživatelem vytvořený skript, který by se měl pokusit službu opravit např. restart služby.

V Configuration → Actions lze nové Action přiřadit typ Remote Command, která nejčastěji v reakci na nějaký Trigger může provést na stanici libovolný příkaz. V zabbix_agentd.conf je potřeba Remote Commands v `EnableRemoteCommands` povolit.



Možnosti webového rozhraní
Stanice a služby jsou v prostředí Zabbix konfogurovány výhradně prostřednictvím webového rozhraní. Konfigurační soubory stanic a služeb v textové podobě nejsou podporovány.

Tvorba vlastních testovacích skriptů a aplikací
Zabbix podporuje tvorbu nových a modifikaci stávajících testovacích aplikací. Více zde [6].

Kapitola 4

Big Sister

4.1 Prerekvizity

Monitorovácí aplikace Big Sister je open-source k dispozici na http://bigsister.graeff.com/. Provoz vyžaduje následující komponenty

- **OS typu Linux/Unix/Windows**

  Distribuce pro OS typu Linux/Unix vyžaduje perl interpreter 5.6 nebo novější.

- **Web server**

  Doporučen Apache.

Podrobnější informace k této problematice zde [3].

4.2 Konfigurace

4.2.1 Server

Struktura konfiguračních souborů je sestavena z několika pravidel, která se aplikují postupně od začátku souboru. Pravidlo sestává z masky, která identifikuje objekt (počítač, skupina počítačů v síti, uživatel) a akce, která se má aplikovat pokud objekt, který právě komunikuje se serverem (např. monitorování hlasí nedostupnost) vyhovuje masce. Veškeré změny v konfiguračních souborech si vyžadují restart procesu, aby nabyly platnosti.

bb_event_generator.cfg
Soubor bb_event_generator.cfg obsahuje pravidla s maskou počítač + služba a adekvatní akci, jejíž soucastí je zaslaní notifikace na uvedenou emailovou adresu.

permissions
Soubor permissions obsahuje pravidla definujicí klientské počítače, které mohou komunikovat se serverem a s jakými omezeními.

bb-display.cfg
Soubor bb-display.cfg umožňuje měnit formu zobrazení monitorovaných dat přes webové rozhraní.

notify.cfg
Umožňuje při vyvolání akce mail, rozšířit tuto akci o skript, který zašle zprávu i na jiné zařízení, pozn. lze provést i v bb_event_generator.cfg.

uxmon-net
Konfigurační soubor obsahující data vztahující se k monitorování, první část masky identifikuje stanici a její službu, následují parametry testování.

4.2.2 Agent

BigSister agent používá jeden konfigurační soubor (přesněji jeden typ, souborů může být více) uxmon-net. Pokud jsou k monitorování použity příkazy využívající root oprávnění (např. icmp protokol) musí být uxmon-net přejmenován na uxmon-asroot (monitorovací testy jsou spuštěny s root právy).

4.3 Monitorování provozu

Konfigurační soubor uxmon-net má následující strukturu

- pomocí klíčového slova DEFAULT lze nastavait parametry služeb, typ protokolu, typ operačního systému atd. počítači, skupině počítačů, službě.

  ```
  DEFAULT frequency=1 ping
  ```

  Kdykoliv bude volána služba ping, bude interval kontroly 1 minuta.

- pomocí klíčového slova DESCR lze nastavit typ prostředí (OS) pro daný počítač nebo skupinu počítačů

  ```
  DESCR features=unix,linux localhost
  ```

  OS počítače localhost je kategorie linux, unix (může mít vliv na některé služby, informace o OS se zobrazí v grafickém rozhraní)

- skupina záznamů definujicí služby a jejich parametry, které se mají na uvedených počítačích monitorovat.

  ```
  192.168.1.1 frequency=2 type=ext2 diskfree
  myhost      proto=icmp            ping
  ```

Pro identifikaci zařízení ze použít IP adresu nebo DNS jméno. Následuje seznam parametrů a jméno služby (resp. skriptu) Seznam vytvořených skriptů, možných parametrů a použití, viz [3].

- záznam, udávající adresu Big Sister serveru, kam budou směrovány veškerá data získaná monitorováním. Na tomto počítači pak lze data zobrazit přes webový prohlížeč

```
192.168.1.10     bsdisplay
```

4.4 Použití v praxi

Interval monitorování
BigSister má nastavenou předdefinovanou hodnotu testovat každou službu jedenkrát za 5 minut. Tuto hodnotu lze pro konkrétní služby upravit pomocí parametru frequency.

```
192.168.1.8 frequency=1 ping
localhost   frequency=5 disk
```

Timeout
Maximální doba, po kterou se bude BigSister server čekat na agenta až doručí zprávu o stavu sledované služby, je 15 minut. Poté bude u služby status NO STATUS REPORT, indikující neúspěšné spojení s agentem. Tuto hodnotu nelze konfigurovat.

Notifikace
Notifikační masky jsou součástí souboru bb_event_generator.cfg. Implicitně je pro zasílaní zprávy použit program sendmail. Nejjedodušší maska pro zásílání notifikací o všech monitorovaných službách na všech stanicích má podobu

```
*.*   mail=admin@localhost
```

Do masky lze přidat další parametry, specifikující prodlevu mezi dalšími upozorněními, vazbu na dostupnost stanice atd.

```
router.ping delay=0 repeat=0 mail=admin@pc1
```

Pokud chceme k zaslání notifikace použít jiný způsob než klasický email, lze pomocí parametru `pager` a speciálního pravidla `PAGER` filtrovat notifikace a použít k jejich rozeslání skript sms-sender-script. Eventuálně i přeposlat dalším kontaktům.

```
*.* mail=admin1@pc1 pager=sms-sender
PAGER{$pager eq "sms-sender"} pager=sms-sender-script mail=admin1@pc1
```

Notifikace s ohledem na hierarchii sítě
Podmínky pro evokování notifikácí se upraví v konfiguračním souboru bb_event_generator.cfg. Parametr `check` obsahuje podmínku, na které závisí zaslání notifikace.

Podmínka sestává z otestování dalších služeb na síti (např. je ping na hlavní router v podsíti OK, je ping na počítač, na kterém běží monitorovaná služba OK). Pokud je podmínka TRUE dojde k zaslání notifikace. Parametr delay definuje čas od výpadku služby do okamžiku kdy dojde k zaslání notifikace. Zároveň pokud podmínka v `check` není v tomto intervalu alespoň jednou splněna dojde k zrušení notifikace (ping na router je zpočátku OK, po chvíli se ale přestane ozývat).

```
*.ftp delay=10 check="$host.conn" mail=admin@pc1
```

Testování dostupnosti služeb při nedostupnosti stanice
Big Sister neumožňuje ihned automaticky otestovat dostupnost stanice, při nedostupnosti některé z jeho služeb. Dochází tak k redundantnímu spouštění testovacích skriptů.

Poznámka: Big Sister povoluje v konfiguračním souboru uvést pouze DNS jméno, IP adresa není povinná (narozdíl od aplikací Nagios a Zabbix). To může vést k neopodstatněnému hlášení o nedostupnosti služeb, kde příčinnou je manipulaci s DNS záznamy.

Flapping
Automatická detekce stavu flapping není v Big Sister přítomna.

Monitorování vzdálených stanic
Získání privátních informací (Zátěž CPU) ze vzdálených stanic zajišťuje v prostředí Big Sister výhradně big sister agent, který musí běžet na vzdáleném počítači. Při vytváření služeb, týkajících se lokálních dat na vzdáleném počítači, není potřeba žádného specifického postupu. Postupuje se jednotně jako u služeb týkajících se lokálního počítače (ke specifikování vzdáleného počítače stačí pouze IP adresa nebo DNS jméno).

Obsluha událostí
Big Sister neumožňuje přiřadit obslužný skript při výpadku služby. Výjimkou je speciální obslužný skript při notifikaci.

Možnosti webového rozhraní
Big Sister nelze primárně konfigurovat prostřednictvím webového rozhraní tzn. nelze měnit obsah konfiguračních souborů, přidávat nové stanice nebo služby. U monitorovaných služeb lze vypnout/zapnout monitorování – status DISABLED.

Tvorba vlastních testovacích skriptů a aplikací
Big Sister podporuje tvorbu nových a modifikaci stávajících pluginů. Více zde [1, 2].

Kapitola 5

Srovnání Nagios, Zabbix a Big Sister

Rozdíly mezi jednotlivými aplikacemi by měli být patrné již z předcházejícíh kapitol. Zde jsou zmíněna témata obecnější povahy, jejichž vypovídající hodnota nemusí být objektivní.

Architektura používající Triggers je univerzálnější než řešení Nagios a Big Sister, které mají pro notifikace a vzdálené příkazy dva specifické způsoby. Triggers jsou obecné řešení, které lze použít pro vyvolání notifikace i vzdáleného příkazu. Navíc lze kombinovat několik návratových hodnot sledovaných služeb, vytvořit mezi nimi závislosti a tomuto celku přiřadit jednu notifikaci a obsluhu události.

Pohled na monitorovaná data prostřednictvím webového grafického rozhraní je u Zabbixu nejkvalitnější. V Zabbixu je možné vytvořit speciální pole grafů (sekce Screens) a mít dobrý přehled o stavu sítě. Grafické nástroje v Nagios a Big Sister podobných kvalit nedosahují, navíc nejsou součástí standartní instalace a jsou k dispozici až v rámci MRTG nebo RRDTool (zavedení je popsáno v [5],[3]).

Použitelnost dokumentace je důležitý faktor reprezentující software. Ze všech tří aplikací je přístup vývojového týmu Nagiosu nejkvalitnější. Zéjmena struktura dokumentace, ale i přístup k prezentaci a podpora softwaru na internetových stránkách. Vývoj nových verzí aplikací je u Nagios a Zabbix velmi produktivní, oproti tomu vývoj Big Sister stagnuje a není perspektivní.

Ná základě výsledků v této práci lze za nejefektivnější variantu považovat kombinované monitorování Nagios a Zabbix. Zabbix díky vysoce přehlednému a přizpůsobivému grafickému rozhraní k tomu má nejlepší předpoklady. Nagios je oproti ostatním vysoce konfigurovatelný z hlediska monitorování služeb a má implementováno množství funkcí, které v ostatních aplikacích nejsou k dispozici. Čehož lze využít zejména při monitorovaní rozsáhlé sítě.

Kapitola 6

Závěr

Kapitoly práce se snaží pokrýt hlavní rozdíly mezi monitorovacími aplikacemi Nagios, Zabbix a Big Sister. Jednotlivé sekce lze studovat nezávisle a pro studium za účelem porovnání a výběru jedné ze tří aplikací je tento postup i doporučen.

Perspektivní rozšíření tohoto projektu by bylo možné dvěma směry. Zaměřit se na další drobné odlišnosti, které již však nenachází tak hromadné uplatnění v praxi. Jedná se například o rozšíření notifikace (eskalace a závislosti – Nagios), podrobnější analýzu dat, kde se pracuje nejen s návratovou hodnotou testování služby (nepř. v úvahu se bere nejen hodnota ping testu OK/non-OK, ale i čas odezvy, velikost množství paketů) nebo použití tzv. pasivního monitorování, kdy vzdálené aplikace provedou kontrolu služby a výsledek zasílají monitorovací aplikaci.

Druhý směr zahrnuje analýzu monitorovacích sytémů ve velkých sítích – 100 a více stanic. Zde je výhodné zavést distribuované monitorování (přímou podporu má Nagios) a lze již rozlišit, zda některé konfigurační rozhraní netrpí nedostatky přílišné časové náročnosti na údržbu.

Literatura

[1] WWW stránky. Big sister - tvorba vlastních příkazů 1.
http://www.joerg.cc/PDFs/devel-2005-08-15.pdf.

[2] WWW stránky. Big sister - tvorba vlastních příkazů 2.
http://bigsister.graeff.com/plugins.html.

[3] WWW stránky. Big sister dokumentace.
http://www.joerg.cc/html/bigsis/index.html.

[4] WWW stránky. Nagios - tvorba vlastních příkazů.
http://nagiosplug.sourceforge.net/developer-guidelines.html.

[5] WWW stránky. Nagios dokumentace. http://nagios.sourceforge.net/docs/3_0/.

[6] WWW stránky. Zabbix dokumentace. http://www.zabbix.com/documentation.php.