BIG SISTER

SYSTEM MONITORINGU SIECI DLA LINUX/UNIX I WINDOWS

Michał (traq) Żuchowski

traq@shl.pl

INSTALACJA BIG SISTER

1. Wymagania:
   - Prel: SNMP, GD, Net::SMTP, LWP::UserAgent and URI, Crypt::SSLeay - http://www.cpan.org
   - RRDTool - rysownie wykresów - http://eestaff.ethz.ch/~oetiker/webtools/rrdtool
   - Apache z obsługą cgi
   - SMTP

2. Dystrybucja w formie pakietów rpm i deb, oraz kodu źródłowego

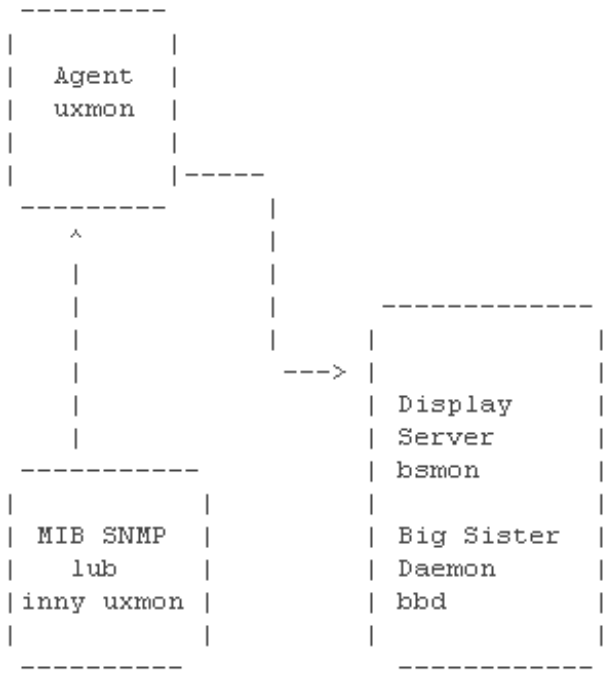
3. Instalacja "ze źródeł":

   - ściągnąc źródła z http://bigsister.graeff.com
   - rozpakować i ./configure --prefix=/usr/local/bs && make && make install
   - w przypadku instalacji samego agenta uxmon:

./configure --prefix=/usr/local/bs && make && make install-agent && make install-modules

ARCHIKTEKTURA BIG SISTER

- Agent
- Big Sister Daemon
- Display Server



1. Uruchamianie daemona uxmon

- w systemie v /etc/rc.d/init.d/bigstser start/stop/restart
- w systemie bsd prefix/bin/bb_start start/stop/restart

2. Konfiguracja daemona uxmon: perfix/adm/uxmon-net

Przykładowa configuracja

```
DEFAULT     community=public frequency=1 perf=5    ALL
DEFAULT     version=1 proto=udp                    rpc
DEFAULT     proto=icmp                             ping

DESCR       features=unix,linux                    localhost

localhost   load memory cpuload
localhost   warn=5% fail=1% disk
localhost   interface=eth0 speed=100Mb/s network
localhost   syslog
localhost   proc=rlinetd procs
localhost   proc=sshd procs
localhost   proc=httpd procs
localhost   proc=proftpd procs
localhost   proc=mysqld procs
localhost   proc=mksd procs
localhost   proc=named procs
localhost   proc=master procs
localhost   proc=amavisd procs
localhost   proc=oidentd procs
localhost   users

213.195.190.30  bsdisplay
include include_checks.
```

3. Inne wybrane ciekawe fukcje uxmon:

ftp - sprawdza dostępność usług ftp
http - sprawdza dostępność usług http
realhttp - sprawdza dokładnie konkretny andres url
ping - zarówno icmp jak i udp
mailq - kolejka poczty
smtp - sprawdza dostępność usług smtp
ssh - sprawdza dostępność usług ssh
mysql - monitoring bazy mysql
oracle - monitoring bazy oracle
pop3 - sprawdza dostępność usług pop3
ups - monitoring ups
snmp - popbiera informacje z MIB SNMP urządzeń np: Cisco

4. Testy i ich modyfikacja

- Główny plik konfiguracyjny: prefix/etc/tests.cfg
- Definicje testów znajdują się w kat. prefix/etc/ i prefix/etc/testdef

Przykładowe testy:

CPUperf monitor

<cut>

```
"idle_yellow:int:Minimum % the CPU must be idle unless yellow status is reported (default: 15)",
"idle_red:int:Minimum % the CPU must be idle unless red status is reported (default: 10)",
"item:string:column name we should report the results under (default: cpu)"
"perf:int:time in minutes between sending performance data (0 for no performance data)";
  init {
    instance import idle_yellow;
    instance import idle_red;
    instance set idle_yellow if( ${idle_yellow}, ${idle_yellow}, 15 );
    instance set idle_red if( ${idle_red}, ${idle_red}, 10 );
    instance import item report_item;
    instance set report_item if( ${report_item}, ${report_item}, "cpu" );
    instance set id 1;
    instance import perf perf_frequency;
    instance set firstpass 1;
  }
```

</cut>

syslog

```
var/adm/messages,/var/log/messages,/var/adm/syslog/syslog.log:
lefault                         green   0       messages looks fine     msgs
lefault                         green   0       no errors logged        disk
 bsmon:                         green   0       ignore
:nd_request: I/O error.*\((.*)\)        red             20      $1 disk error   disk
:/O error                       red             20      I/O error               disk
 [^\s]+): file system full      red     20      $1 fs full              disk
:u.*failed for ([^\s]+)         yellow  20      su failed for $1
:u: FAILED SU .to ([^\s]+). ([^\s]+)    yellow  60      su $1 failed for $2
:u: .to ([^\s]+). ([^\s]+)      clear   0       su $1 failed for $2
:u :.*1 ([^\s]+)                yellow  20      su failed for $1
:csi.*error                             red     15      scsi error              disk
iotice                          yellow  15      notice
arning                          yellow  15      warning
eed.*maintenance                yellow  30      need maintenance
atal                            yellow  15      fatal error
```

<cut>

1. Konfiguracja: prefix/adm/bb-display.cfg

```
%Port 1984
%Option -ImmediateHTML +KeepGroups +StartOK -DNS
%Autojoin new NEW
%Autojoin all_hosts ALL
%Autojoin all UNIVERSE

%Groups
flash  SIEC-OSIEDLOWA
moon   SIEC-OSIEDLOWA
cache  SIEC-OSIEDLOWA
bramka SIEC-OSIEDLOWA

%skin static_lamps techie
%Logskin static_lamps techie
%Page top Cala_siec
%title Cala_siec
%refto none
%itemref html
%sort severity
%table ALL

%Section Sieci_wedlug_podzialu:
%Page osiedlowa Siec_osiedlowa
%title Siec_osiedlowa
%refto none
%itemref html
%sort severity
%table SIEC-OSIEDLOWA

%Section Mapy_sieci
%skin static_lamps techie
%Logskin static_lamps techie
%title Mapa_sieci_osiedlowej
%Page mapa_osiedl Mapa_sieci_osiedlowej
%image adm/display_map.cfg
%refto none
%itemref html
%sort severity
%select <green
```

%table SIEC-OSIEDLOWA

%Frameset index top Big_Sister

2. Imagemaps

- Konfiguracja: prefix/adm/display_map.cfg

Przykładowy plik konfiguracyjny:

```
template       www/pic/serwerownia-posesja.png

red          www/skins/default/red.gif
yellow        www/skins/default/yellow.gif
green        www/skins/default/green.gif
purple       www/skins/default/purple.gif


at           305,160 cache.conn
at           180,160 moon.conn
at           40,160 bramka.conn
at           458,160 flash.conn
at           355,12 83.238.41.190.conn
at           79,12 10.10.100.120.conn
at           59,284 ap4.conn
at           44,382 ap5.conn
at           460,284 ap6.conn
at           460,382 ap7.conn

dump          www/pic/map.png
```

ALARMY

1.Plik konfiguracyjny prefix/adm/bb_event_generator.cfg

2. Przykład pliku konfiguracyjnego:

```
flash.msgs      down=never up=never
*.conn  prio=40 down=yellow up=green delay=1 norepeat=20 keep=1 mail=alarm repeatprio=10 msgmax=60
*.procs prio=40 down=yellow up=green delay=1 norepeat=20 keep=1 mail=alarm repeatprio=10 msgmax=60
*.cpu   prio=40 down=yellow up=green delay=1 norepeat=20 keep=1 mail=alarm repeatprio=10 msgmax=60
*.net   prio=40 down=yellow up=green delay=1 norepeat=20 keep=1 mail=alarm repeatprio=10 msgmax=60
*.disk  prio=40 down=yellow up=green delay=1 norepeat=20 keep=1 mail=alarm repeatprio=10 msgmax=60
```

3. Inne ciekawe opcje:

flash.* {daytime 17:00-07:00} down=never

Denerwujemy Tomka ;)

*.SIEC-OSIEDLOWA{weekday Sat,Sun} mail=lenyo@gnu.univ.gda.pl

4. Możemy również tworzyć raport pod kątem SLA - temat rzeka na ew. warsztaty.

ZARZĄDZANIE ZA POMOCĄ TELNET LUB BSADMIN

1. Składnia telnet:

telnet adres-serwera port polecenie obiekt.parametr

2. Składania bsadmin:

bsadmin -d adres-serwera polecenie obiekt.parametr

3. Przykłady:

telnet jakis.server.com 1984 remove flash.*

bsadmin -d jakis.server.com remove flash.*

4. Wybrane polecenia:

join - przyłącza do grupy obiekt sieciowy

leave - usuwa z grupy obiekt sieciowy

displayname - ustawia nazwę wyświetlaną dla obiektu sieciowego

savelogs - rotacja i zapis logów

remove - usuwa albo jakiś parametr monitorowany, albo w przypadku obiekt.* usuwa cały obiekt z bazy wyświetlania

BEZPIECZEŃSTWO

1. Dostęp do DISPLAY SERVER na port 1984 jest realizowany poprzez
   plik: prefix/adm/permissions

2. Składnia

   kto-ma-mieć-dostęp => do-jakiej-funkcji (+,-)

3. Przykładowe możliwości konfiguracji:

   - wszyscy mają dostep: host .* => +all
   - dana klasa adresowa ma dostęp: host 10.10.*.* => +all
   - dana domena ma dostęp: host .*.gnu.univ.gda.pl => +all
   - dana klasa adresowa ma dostęp tylko do przekazaywania swojego statusu:
     host 192.168.*.* => +status
   - blokujemy wszystko: name .* => -all

4. Wybrane funkcje:

   status - przekazywanie statusu
   gropuing - możliwość grupowania i usuwania z grup obiektów sieciowych
   all - obejmuje wszystkie opcje
   archiving - archiwizacja logów
   authenticate - kto może się autoryzować

5. Tunelowanie połączeń przez ssh:

ssh -l user -n display-server -L 10192:localhost:1984 sleep 600

W pliku uxmon-net należy podmienić linię określającą serwer na:

localhost port=10192 bsdisplay

LINKI

Strona domowa projektu

http://bigsister.graeff.com/bigsister.html

Dokumentacja on-line

http://www.joerg.cc/html/bigsis/index.html

Big Sister Instalation Howto

http://bigsister.graeff.com/pdoc/INSTALL.html