ubuntu - Nove funkcije #14515

syslog ng

10.06.2008 17:37 - Ernad Husremović

Status:	Zatvoreno	**Početak:**	10.06.2008
Prioritet:	Normalan	**Završetak:**	
Odgovorna osoba:	Ernad Husremović	**% završeno:**	0%
Kategorija:		**Procjena vremena:**	0.00 sat
Ciljna verzija:			

Opis

http://blog.assaydepot.com/2007/7/29/setup-a-central-logging-server-using-splunk-syslog-ng-and-named-pipes-on-ubuntu

Historija

#1 - 10.06.2008 18:04 - Ernad Husremović

ruby syslog testni client

root@monitor:~/test# cat syslog_client.rb

```
require 'syslog'

Syslog.open('pppd', Syslog::LOG_PID | Syslog::LOG_NDELAY, Syslog::LOG_FTP)

Syslog.log(Syslog::LOG_NOTICE, "Serial link appears to be disconnected.")
Syslog.log(Syslog::LOG_CRIT, "the sky is falling in %d seconds!", 10)
```

root@monitor:~/test# vi syslog_client.rb

```
Jun 10 18:01:57 monitor pppd[3778]: Serial link appears to be disconnected.
Jun 10 18:01:57 monitor pppd[3778]: the sky is falling in 10 seconds!
```

#2 - 10.06.2008 18:04 - Ernad Husremović

- Status promijenjeno iz Novo u Dodijeljeno

- Odgovorna osoba postavljeno na Ernad Husremović

#3 - 10.06.2008 18:09 - Ernad Husremović

slanje alarmu filterisanih syslog poruka

/etc/syslog-ng/syslog-ng.conf

destination

```
destination alarm_alert_script {program ("/usr/local/bin/syslog_alarm_alert.rb"); };
```

filter

```
filter internet_disconnect {
 program("pppd") and
        match ("Serial link appears to be disconnected");
};
```

log povezuje source, filter i destinaciju

```
log {
       source(s_all);
       filter(internet_disconnect);
       destination(alarm_alert_script);
};
```

alarm opet čita syslog poruku, i šalje je monitor-u

root@monitor:~/test# cat /usr/local/bin/syslog_alarm_alert.rb

```
#!/usr/bin/ruby

# read lines from stdin and put to the alarm

lines=""
while line=gets
  lines += line
end

require 'drb'
monitor = DRbObject.new nil, "druby://monitor.bring.out.ba:9010"

put "lines = #{lines}"
monitor.process_syslog(7, lines)
```

#4 - 10.06.2008 18:11 - Ernad Husremović

da bi imali kompletnu sliku navešču Analaze.rb dio koji handlira ovu poruku:

```
class Analyze
...

        def process_syslog( level, message)
                @@log.debug("syslog event: #{level} : #{message}")
                if level >= 3
                        #asterisk_send_sms_all("#{level} : #{message}")
                        asterisk_send_sms("061141311", "#{level} : #{message}" )
                end
        end

end
```

#5 - 10.06.2008 18:16 - Ernad Husremović

da li ručno dolazi poruka ?

root@monitor:~/test# echo "pppd test" | /usr/local/bin/syslog_alarm_alert.rb

```
lines = pppd test
```

root@monitor:~/ruby# tail /var/log/monitor.log

```
D, [2008-06-10T18:15:43.556867 #24340] DEBUG -- : send_sms 061141311  7 : pppd test
```

dolazi super

#6 - 10.06.2008 18:48 - Ernad Husremović

ahaaaaa

http://linux.derkeiler.com/Mailing-Lists/SuSE/2008-01/msg03323.html
[opensuse] Any one tried in syslog-ng a "program() destination driver"?

- From: "Carlos E. R." <robin.listas@xxxxxxxxxxxxxx>
- Date: Wed, 30 Jan 2008 17:10:59 +0100 (CET)

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

(repost after my unsubscribe by server)

Hi,

I'm trying to get a program executed or do something when certain message
is logged. I'm trying the following in syslog-ng:

filter f_router_got_ip { host("router") and match("Received valid IP address from server"); };

destination router2 { file("/var/log/router2"); };
log { source(ext); filter(f_router_got_ip); destination(router2); };

This does work, I get the expected entry in /var/log/router2. However, if I try this, per the documentation:

destination routerip { program("/usr/local/syslog-askandlogrouterip"); };
log { source(ext); filter(f_router_got_ip); destination(routerip); };

The destination program (a script) never runs. According to the documentation, the program should be loaded only once right at the start:

program()

This driver executes the specified program with the specified arguments and sends messages to the standard input (stdin) of the child.

The program() driver has a single required parameter, specifying a program name to start. The program is executed with the help of the current shell, so the command may include both file patterns and I/O redirection, they will be processed.

Declaration:
program(commandtorun);

Note

Ovo je ključno: **The program is executed once at startup, and kept running until**

#7 - 10.06.2008 18:58 - Ernad Husremović

evo konačne verzije sylog-ng ruby skripte

root@monitor:~# cat /usr/local/bin/syslog_alarm_alert.rb

```
#!/usr/bin/ruby

require 'drb'

# read lines from stdin and put to the alarm
# The program is executed once at startup, and kept running until

while line = gets

  monitor = DRbObject.new nil, "druby://monitor.bring.out.ba:9010"

  puts "line = #{line}"
  monitor.process_syslog(7, line)

end
```

evo klijenta

root@monitor:~/test# cat syslog_client.rb

```
require 'syslog'

Syslog.open('pppd', Syslog::LOG_PID | Syslog::LOG_NDELAY, Syslog::LOG_FTP)

Syslog.log(Syslog::LOG_NOTICE, "Serial link appears to be disconnected.")
Syslog.log(Syslog::LOG_CRIT, "the sky is falling in %d seconds!", 10)
Syslog.close
```

root@monitor:~/test# ruby syslog_client.rb

root@monitor:~/test# ps ax

```
  PID TTY      STAT   TIME COMMAND
    1 ?        Ss     0:00 init [2]
11849 pts/0    S      0:00 /bin/sh -c /usr/local/bin/syslog_alarm_alert.rb      <<<<<<<<<<<<<<<<<<< skripta va
zda aktivna
11850 pts/0    S      0:00 /usr/bin/ruby /usr/local/bin/syslog_alarm_alert.rb
11851 ?        Ss     0:00 /sbin/syslog-ng -p /var/run/syslog-ng.pid
11956 pts/0    R+     0:00 ps ax
24323 ?        Ss     0:00 sshd: root@pts/1
24325 pts/1    Ss+    0:00 -bash
```

```
24340 pts/1    Sl     0:01 /usr/bin/ruby /root/ruby/analyze_drb.rb
24341 pts/1    Sl     0:01 /usr/bin/ruby /root/ruby/starter.rb
26333 ?        Ss     0:00 /usr/sbin/sshd
26356 ?        Ss     0:00 /usr/sbin/cron
26378 ?        Ss     0:00 /usr/bin/perl /usr/share/webmin/miniserv.pl /etc/webmin/miniserv.conf
26386 ?        Ss     0:00 vzctl: pts/0
26387 pts/0    Ss     0:00 -bash
```

to je to

#8 - 10.11.2008 11:26 - Ernad Husremović

- Status promijenjeno iz Dodijeljeno u Zatvoreno

na sve servere sada postavljamo syslog-ng