PRELUDE SIEM - Bug #625

Filtering plugin smtp

09/30/2015 04:11 PM - Thierno DIOP

Status:	Closed	**Start date:**	09/21/2015
Priority:	Urgent	**Due date:**	
Assignee:	Antoine LUONG	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			
Resolution:			

Description

Hello,

I try to configure prelude-manager to send me one email when a force brute attack has detected.
But if i reboot prelude-manager, i have cf (host1.png).And its will be down after a few secondes.
My configuration is (cf host.png).

I need your help!!

Thank you.

History

#1 - 09/30/2015 04:41 PM - Thierno DIOP

- File host.png added

- File host1.png added

Thierno DIOP wrote:

> Hello,
>
> I try to configure prelude-manager to send me one email when a force brute attack has detected.
> But if i reboot prelude-manager, i have cf (host1.png).And its will be down after a few secondes.
> My configuration is (cf host.png).
>
> I need your help!!
>
> Thanks you.

#2 - 09/30/2015 05:02 PM - Antoine LUONG

- Category deleted (idmef)

- Status changed from New to Assigned

- Assignee set to Antoine LUONG

Hello,

Please provide information about the OS you are using and the installation method (from source or packages).

Regards

#3 - 09/30/2015 05:12 PM - Thierno DIOP

I use CentOS 6.7. I installed packages with yum install.
So I had no errors during installation.

Regards

#4 - 09/30/2015 05:23 PM - Antoine LUONG

You should then install the **prelude-manager-smtp-plugin** package from the repository.

#5 - 10/01/2015 09:36 AM - Thierno DIOP

Ok i installed this plugin and i have not the message that was displayed when I rebooted prelude-manager (cf host1.png).
Everything seems Ok but after a few secondes prelude-manager, prelude-lml and prelude-correlator will be down . And when i commented the smtp section, it will be ok. You can see my smtp configuration:

[smtp]
sender = admin@xxxxx.fr
smtp-server = smtp.xxxxx.fr
subject = Alert: $alert.classification.text
template = /etc/prelude-manager/smtp-template/mail.template1

dbtype = mysql
dbname = xxxxxx
dbuser = xxxxxx
dbpass = xxxxxx
dbhost = localhost

correlated-alert-template = /etc/prelude-manager/smtp-template/mail.template1

#6 - 10/01/2015 09:57 AM - Antoine LUONG

You seem to have forgotten the **recipients** configuration parameter.

#7 - 10/01/2015 11:12 AM - Thierno DIOP

I configured the recipients parameter but I always have the same.

[smtp]
sender = admin@xxxxx.fr
recipients = recep@gmail.com
smtp-server = smtp.xxxxx.fr
subject = Alert: $alert.classification.text
template = /etc/prelude-manager/smtp-template/mail.template1

dbtype = mysql
dbname = xxxxxx

dbuser = xxxxxx
dbpass = xxxxxx
dbhost = localhost

#8 - 10/01/2015 11:51 AM - Antoine LUONG

Please stop the prelude-manager service and post the output of the command 'prelude-manager --debug'.

#9 - 10/01/2015 12:01 PM - Thierno DIOP

- File out1.png added

- File out2.png added

Please check the joint files out1.png and out2.png

#10 - 10/01/2015 12:17 PM - Antoine LUONG

Are you sure you uncommented the [smtp] section in the configuration file?

#11 - 10/01/2015 01:30 PM - Thierno DIOP

Sorry I thought it was already done. So now i uncommented this and i have

01 Oct 13:25:45 (process:6258) INFO: Subscribing Normalize to active decoding plugins.
01 Oct 13:25:45 (process:6258) INFO: server started (listening on 127.0.0.1 port 4690).
01 Oct 13:25:45 (process:6258) INFO: Subscribing db[default] to active reporting plugins.
01 Oct 13:25:45 (process:6258) INFO: SMTP: connection to smtp-xxxx.fr succeeded.
01 Oct 13:25:45 (process:6258) INFO: Subscribing SMTP[test] to active reporting plugins.
01 Oct 13:25:45 (process:6258) INFO: Subscribing Debug[default] to active reporting plugins.
version: <empty>
heartbeat:
analyzer(0):
analyzerid: 2999950199843006
name: prelude-manager
manufacturer: http://www.prelude-ids.com
model: Prelude Manager
version: 1.2.6
class: Concentrator
ostype: Linux
osversion: 2.6.32-573.7.1.el6.x86_64
node:
category: unknown (0)
location: Le Mans
name: My IDS Snort
address(0):
category: ipv4-addr (7)
address: 127.0.0.1
process:
name: prelude-manager
pid: 6258
path: /usr/bin/prelude-manager
create_time: 01/10/2015 13:25:45.258706 +02:00
heartbeat_interval: 600
additional_data(0):
meaning: Analyzer status
type: string (0)
data: starting
additional_data(1):
meaning: Analyzer SHA1
type: string (0)
data: 6aecc7d9304249a1d45d15c53e90b9856bf5d98a

#12 - 10/01/2015 03:44 PM - Antoine LUONG

So it seems to be working... For further configuration-related questions please use the forum User.

#13 - 10/01/2015 03:57 PM - Thierno DIOP

it seems to work but it not working because after starting prelude-manager, it will be out of service.
Ok no problem, i will use the forum user for further questions.

#14 - 10/01/2015 05:05 PM - Antoine LUONG

Are you saying the manager in debug mode stopped working immediately after the output #625-11?

#15 - 10/01/2015 05:30 PM - Thierno DIOP

I meant that when i uncommente the [smtp] section in the configuration file and i start prelude-manager,
it seems to work. But after a few secondes it will be down.

Now everything works good. I get an email when there are a brute force attack. but in every 10 minutes,
I am obliged to restart the servers prelude-manager, prelude-lml and prelude-correlator.
What you thinks about??

#16 - 05/30/2016 07:05 AM - Thomas ANDREJAK

- Status changed from Assigned to Closed

It should be solved in 3.0 version of libPrelude / prelude-manager.

Files

host.png	14.2 KB	09/30/2015	Thierno DIOP
host1.png	50.2 KB	09/30/2015	Thierno DIOP
host.png	14.2 KB	09/30/2015	Thierno DIOP
host1.png	50.2 KB	09/30/2015	Thierno DIOP
out2.png	16.6 KB	10/01/2015	Thierno DIOP
out1.png	78.6 KB	10/01/2015	Thierno DIOP