Prelude-LML - Bug #229

Fix format when checking apache logfile(s)

06/01/2007 03:34 PM -

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Yoann VANDOORSELAERE	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:	0.9.10.1		
Resolution:	fixed		

Description

Here is a small fix for prelude-lml.conf when checking Apache logfiles, to get rid of the annoyed "cannot match" log entries.

```
--- prelude-lml.conf.orig       Mon May 21 16:11:45 2007
+++ prelude-lml.conf    Fri Jun  1 15:30:56 2007
@@ -73,7 +73,7 @@
 #
 [format=apache]
 time-format = "%d/%b/%Y:%H:%M:%S"
-prefix-regex = "^(?P<hostname>\S+) - - \[(?P<timestamp>.{20}) \[+-].{4}\] "
+prefix-regex = "^(?P<hostname>\S+) - \S+ \[(?P<timestamp>.{20}) [+-].{4}\] "
 file = /var/log/apache2/access_log
```

Regards,

Robin Gruyters

Associated revisions

Revision 81e740c7 - 07/16/2007 10:22 AM - Yoann VANDOORSELAERE

Fix typo in Apache regexp: thanks to andre@vandervlies.xs4all.nl for
pointing this out. Refs #229.

git-svn-id: file:///home/yoann/dev/prelude/git/nok/SVN/prelude-lml/trunk@9684 09c5ec92-17d4-0310-903a-819935f44dba

History

#1 - 06/02/2007 10:44 AM - Yoann VANDOORSELAERE

- Status changed from New to Assigned

Hello Robin,

Could you provide a sample Apache log that make the current *prefix-regex* fail?

Regards,

#2 - 06/06/2007 01:20 PM -

Sure:

```
10.8.0.132 - account [06/Jun/2007:13:14:47 +0200] "REPORT /svn/brainz/!svn/vcc/default HTTP/1.1" 200 147 "-" "
SVN/1.4.3 (r23084) neon/0.25.5"
```

and

```
10.8.0.132 - - [06/Jun/2007:13:08:19 +0200] "PROPFIND /svn/demos/BeNeXt/trunk HTTP/1.1" 401 401 "-" "SVN/1.4.3
 (r23084) neon/0.25.5"
```

```
10.8.0.131 - - [06/Jun/2007:13:19:49 +0200] "GET /horde HTTP/1.1" 301 228 "-" "Mozilla/5.0 (Windows; U; Window
s NT 5.1; en-US; rv:1.8.1.4) Gecko/20070515 Firefox/2.0.0.4"
```

Regards,

Robin

#3 - 06/06/2007 01:41 PM - Yoann VANDOORSELAERE

- Status changed from Assigned to Closed

- Resolution set to fixed

(In r9557) Include patch from Robin Gruyters <r.gruyters@yirdis.nl>, to fix
Apache formating when Apache logname or user is set. Fix #229.

#4 - 07/13/2007 08:08 PM -

I think this is still wrong. It should read ' [+-].{4}\] " on line 76 (as stated in Robin Gruyters orginal remarks).

The '\[' renders to a 'No match'.....

```
71   #
72   # Sample configuration for apache:
73   #
74   [format=apache]
75   time-format = "%d/%b/%Y:%H:%M:%S"
76   prefix-regex = "^(?P<hostname>\S+) \S+ \S+ \[(?P<timestamp>.{20}) \[+-].{4}\] "
77   file = /var/log/apache2/access_log
78
79
```

#5 - 07/13/2007 08:19 PM -

<Sigh> Must use wikiformatting...

The code (prelude-lml.conf.in: 9557) says:

```
71 #
72 # Sample configuration for apache:
73 #
74 [format=apache]
75 time-format = "%d/%b/%Y:%H:%M:%S"
76 prefix-regex = "(?P<hostname>\S+) \S+ \S+ \[(?P<timestamp>.{20}) \[+-].{4}\] "
77 file = /var/log/apache2/access_log
78
79
```

<pre>

#6 - 07/16/2007 10:22 AM - Yoann VANDOORSELAERE

(In r9684) Fix typo in Apache regexp: thanks to andre@vandervlies.xs4all.nl for pointing this out. Refs #229.

#7 - 04/29/2009 02:48 PM - Yoann VANDOORSELAERE

- Project changed from PRELUDE SIEM to Prelude-LML

- Category deleted (generic)

- Target version deleted (0.9.10.1)