Suricata - Support #2790

rule_perf.log repeating the same results
01/23/2019 05:13 PM - Bryant Smith

Status: Closed
Priority: Normal
Assignee: 
Category: 
Affected Versions: 4.1.2
Label: 

Description
I just recently notice that the rule_perf.log file has been repeating the exact same results for a rule alert. I have my yaml file configured to NOT append and I also have the json output disabled. The file is overwritten but always with 6 outputs of the same event. I also have Suricata 4.0.6 install on the same VM running Ubuntu 18.04.1 LTS without this issue.

alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"Testing Signature and Rule Perf";flow:established,to_server;content:"/forum.ghp";http_uri;sid:11111;rev:1;)

1. rule profiling

rules:
1. Profiling can be disabled here, but it will still have a
2. performance impact if compiled in.
   enabled: yes
   filename: rule_perf.log
   append: no

---------------------------------------------------------------------
---------------------------------------------------------------------
<table>
<thead>
<tr>
<th>Num</th>
<th>Rule</th>
<th>Gid</th>
<th>Rev</th>
<th>Ticks</th>
<th>% Checks</th>
<th>Matches</th>
<th>Max Ticks</th>
<th>Avg Ticks</th>
<th>Avg Match</th>
<th>Avg No Match</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>11111</td>
<td>1</td>
<td>1</td>
<td>12404</td>
<td>100.00</td>
<td>1</td>
<td>12404</td>
<td>12404.00</td>
<td>12404.00</td>
<td>0.00</td>
</tr>
</tbody>
</table>

---------------------------------------------------------------------
---------------------------------------------------------------------
<table>
<thead>
<tr>
<th>Num</th>
<th>Rule</th>
<th>Gid</th>
<th>Rev</th>
<th>Ticks</th>
<th>% Checks</th>
<th>Matches</th>
<th>Max Ticks</th>
<th>Avg Ticks</th>
<th>Avg Match</th>
<th>Avg No Match</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>11111</td>
<td>1</td>
<td>1</td>
<td>12404</td>
<td>100.00</td>
<td>1</td>
<td>12404</td>
<td>12404.00</td>
<td>12404.00</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---------------------------------------------------------------------
---------------------------------------------------------------------
<table>
<thead>
<tr>
<th>Num</th>
<th>Rule</th>
<th>Gid</th>
<th>Rev</th>
<th>Ticks</th>
<th>% Checks</th>
<th>Matches</th>
<th>Max Ticks</th>
<th>Avg Ticks</th>
<th>Avg Match</th>
<th>Avg No Match</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>11111</td>
<td>1</td>
<td>1</td>
<td>12404</td>
<td>100.00</td>
<td>1</td>
<td>12404</td>
<td>12404.00</td>
<td>12404.00</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---------------------------------------------------------------------
---------------------------------------------------------------------
<table>
<thead>
<tr>
<th>Num</th>
<th>Rule</th>
<th>Gid</th>
<th>Rev</th>
<th>Ticks</th>
<th>% Checks</th>
<th>Matches</th>
<th>Max Ticks</th>
<th>Avg Ticks</th>
<th>Avg Match</th>
<th>Avg No Match</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>11111</td>
<td>1</td>
<td>1</td>
<td>12404</td>
<td>100.00</td>
<td>1</td>
<td>12404</td>
<td>12404.00</td>
<td>12404.00</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Date: 1/23/2019 -- 10:08:37. Sorted by: number of checks.

<table>
<thead>
<tr>
<th>Num</th>
<th>Rule</th>
<th>Gid</th>
<th>Rev</th>
<th>Ticks</th>
<th>%</th>
<th>Checks</th>
<th>Matches</th>
<th>Max Ticks</th>
<th>Avg Ticks</th>
<th>Avg Match</th>
<th>Avg No Match</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>11111</td>
<td>1</td>
<td>1</td>
<td>12404</td>
<td>100.00</td>
<td>1</td>
<td>1</td>
<td>12404</td>
<td>12404.00</td>
<td>12404.00</td>
<td>0.00</td>
</tr>
</tbody>
</table>

### Date: 1/23/2019 -- 10:08:37. Sorted by: number of matches.

<table>
<thead>
<tr>
<th>Num</th>
<th>Rule</th>
<th>Gid</th>
<th>Rev</th>
<th>Ticks</th>
<th>%</th>
<th>Checks</th>
<th>Matches</th>
<th>Max Ticks</th>
<th>Avg Ticks</th>
<th>Avg Match</th>
<th>Avg No Match</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>11111</td>
<td>1</td>
<td>1</td>
<td>12404</td>
<td>100.00</td>
<td>1</td>
<td>1</td>
<td>12404</td>
<td>12404.00</td>
<td>12404.00</td>
<td>0.00</td>
</tr>
</tbody>
</table>

### Date: 1/23/2019 -- 10:08:37. Sorted by: max ticks.

<table>
<thead>
<tr>
<th>Num</th>
<th>Rule</th>
<th>Gid</th>
<th>Rev</th>
<th>Ticks</th>
<th>%</th>
<th>Checks</th>
<th>Matches</th>
<th>Max Ticks</th>
<th>Avg Ticks</th>
<th>Avg Match</th>
<th>Avg No Match</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>11111</td>
<td>1</td>
<td>1</td>
<td>12404</td>
<td>100.00</td>
<td>1</td>
<td>1</td>
<td>12404</td>
<td>12404.00</td>
<td>12404.00</td>
<td>0.00</td>
</tr>
</tbody>
</table>

#### Suricata 4.1.2 Build====

```
./configure --prefix=/opt/suricata-4.1.2 --sysconfdir=/opt/suricata-4.1.2/etc/ --localstatedir=/opt/suricata-4.1.2/var/ --enable-luajit \
--with-libnss-libraries=/usr/lib --with-libnss-includes=/usr/include/nss/ --with-libnspr-libraries=/usr/lib \
--with-libnspr-includes=/usr/include/nspr --with-libluajit-includes=/usr/local/include/luajit-2.0/ \
--with-liblua-libraries=/usr/lib/ \
--enable-profiling \
--enable-rust
```

This is Suricata version 4.1.2 RELEASE

Features: PCAP_SET_BUFF AF_PACKET HAVE_PACKET_FANOUT LIBCAP_NG LIBNET1.1

HAVE_HTP_URI_NORMALIZE_HOOK PCRE_JIT HAVE_NSS HAVE_LUA HAVE_LUAJIT HAVE_LIBJANSSON PROFILING TLS MAGIC RUST

SIMD support: SSE_4_2 SSE_4_1 SSE_3

Atomic intrinsics: 1 2 4 8 16 byte(s)

64-bits, Little-endian architecture

GCC version 7.3.0, C version 199901

compiled with _FORTIFY_SOURCE=2

L1 cache line size (CLS)=64

thread local storage method: __thread

compiled with LibHTP v0.5.29, linked against LibHTP v0.5.29

Suricata Configuration:

AF_PACKET support: yes
eBPF support: no
XDP support: no
PF_RING support: no
NFQueue support: no
NFLOG support: no
IPFW support: no
Netmap support: no
DAG enabled: no
Napatech enabled: no
WinDivert enabled: no

Unix socket enabled: yes
Detection enabled: yes
Libmagic support: yes
libnss support: yes
libnspr support: yes
libjansson support: yes
liblzma support: yes
hiredis support: no
hiredis async with libevent: no
Prelude support: no
PCRE jit: yes
LUA support: yes, through luajit
libluajit: yes
libgeoip: no
Non-bundled htp: no
Old barnyard2 support: no
Hyperscan support: no
Libnet support: yes
liblz4 support: yes

Rust support: yes
Rust strict mode: no
Rust debug mode: no
Rust compiler: rustc 1.30.0
Rust cargo: cargo 1.30.0

Install suricatasc: yes
Install suricata-update: no

Profiling enabled: yes
Profiling locks enabled: no

Development settings:
Coccinelle / spatch: no
Unit tests enabled: no
Debug output enabled: no
Debug validation enabled: no

Generic build parameters:
Installation prefix: /opt/suricata-4.1.2
Configuration directory: /opt/suricata-4.1.2/etc/suricata/
Log directory: /opt/suricata-4.1.2/var/log/suricata/

--prefix /opt/suricata-4.1.2
--sysconfdir /opt/suricata-4.1.2/etc
--localstatedir /opt/suricata-4.1.2/var
--datarootdir /opt/suricata-4.1.2/share

Host: x86_64-pc-linux-gnu
Compiler: gcc (exec name) / gcc (real)
GCC Protect enabled: no
GCC march native enabled: yes
GCC Profile enabled: no
Position Independent Executable enabled: no

CFLAGS -g -O2 -march=native -I${srcdir}/../rust/gen/c-headers
PCAP_CFLAGS -I/usr/include
SECCFLAGS

History
#1 - 01/23/2019 05:35 PM - Victor Julien
The outputs are not the same. They are each sorted by a different column. Not very useful with a single rule, but I think it's not worth adding an exception for just a single rule.

#2 - 01/23/2019 05:55 PM - Bryant Smith
Well I'm an idiot. All I had to do was read the next few lines in the yaml file. Sorry about that and thanks for pointing it out.

1. Sort options: ticks, avgticks, checks, matches, maxticks
#sort: avgticks

#3 - 01/23/2019 07:15 PM - Victor Julien
- Tracker changed from Bug to Support
- Status changed from New to Closed

Files

<table>
<thead>
<tr>
<th>File</th>
<th>Size</th>
<th>Date</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018-9059.pcap</td>
<td>5.93 KB</td>
<td>01/23/2019</td>
<td>Bryant Smith</td>
</tr>
</tbody>
</table>