Reg : Time field of exporter flows

Lavanya Singaravelan <lavanya.singaravelan@tatacommunications.com>
Fri 20/12/2019 13:50
To: Sriram Ramanujam <sriram.ramanujam@tatacommunications.com>

Hi Sriram,

Regarding the date field, as mentioned in the discussion we had yesterday

Most of the IPFIX exporter, exported their time stamps with element 152 and 153

152 flowStartMilliseconds – absolute timestamp of first packet of flow in milliseconds
153 flow start millisecond – absolute timestamp of last packet of flow in milliseconds

But in the Cisco, the time stamp of the field was sent in elements 21 and 22

According to IPFIX RPC:

21 flowEndSysUpTime – number of milliseconds since the device restarted. Relative time of last packet of flow
22 flowStartSysUpTime - number of milliseconds since the device restarted. Relative time of first packet of the flow

Since the time is relative 21 and 22 requires another field which has device start time to give the absolute time of first and last packet of the flow
160 systemInitTimeMilliseconds – absolute time when the device configured with ipfix restarted
The systemup time is sent in element **160** from Cisco exporter but nfdump cannot read element 160.

Based on this issue : https://github.com/phaag/nfdump/issues/36

Then I checked the export fields and their corresponding export-id in Cisco router
And I was able to see 152 and 153 in export-id

```
timestamp absolute first                :   152
timestamp absolute last                 :   153
```

Again I changed the configuration for flow record as below

```
collect timestamp absolute first
collect timestamp absolute last
```

And now I'm able to get the correct time stamps for first and last packet of the flow with a precision of milliseconds

```
Date first seen          Duration Proto      Src IP Addr:Port           Dst IP A$
2019-12-20 11:11:24.387     0.000 ICMP    192.168.56.106:0      ->   192.168.56.$
2019-12-20 11:11:24.411     0.000 ICMP    192.168.56.106:0      ->   192.168.56.$
2019-12-20 11:11:24.423     0.000 ICMP    192.168.56.106:0      ->   192.168.56.$
2019-12-20 11:11:24.431     0.000 ICMP    192.168.56.106:0      ->   192.168.56.$
2019-12-20 11:11:24.443     0.000 ICMP    192.168.56.106:0      ->   192.168.56.$
2019-12-20 11:11:25.627     0.000 ICMP    192.168.56.106:0      ->   192.168.56.$
2019-12-20 11:11:25.639     0.000 ICMP    192.168.56.106:0      ->   192.168.56.$
2019-12-20 11:11:25.651     0.000 ICMP    192.168.56.106:0      ->   192.168.56.$
2019-12-20 11:11:25.659     0.000 ICMP    192.168.56.106:0      ->   192.168.56.$
2019-12-20 11:11:25.671     0.000 ICMP    192.168.56.106:0      ->   192.168.56.$
2019-12-20 11:11:26.483     0.000 ICMP    192.168.56.106:0      ->   192.168.56.$
2019-12-20 11:11:26.491     0.000 ICMP    192.168.56.106:0      ->   192.168.56.$
2019-12-20 11:11:26.503     0.000 ICMP    192.168.56.106:0      ->   192.168.56.$
2019-12-20 11:11:26.515     0.000 ICMP    192.168.56.106:0      ->   192.168.56.$
```

I'll further test with resetting the time of the router clock

Thanks and Regards,
Lavanya Singaravelan