Prelude Correlator - Bug #374

Prelude Correlator Memory Usage

04/06/2010 07:35 PM - James Chapple

Status:	Closed	**Start date:**	04/06/2010
Priority:	Normal	**Due date:**	
Assignee:	Thomas ANDREJAK	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			
Resolution:			

Description

When a system with Prelude Correlator acts as a relay to another system with Prelude Correlator, the second system will consume excessive amounts of memory, generate excessive sql records, and sometimes crash. The specific conditions were as follows:
Machine A runs a Manager with no Correlator, Prewikka, and relays all events to machine B
Machine B runs a Manager, Correlator, Prewikka, and relays only medium/high events and heartbeats to machine C
Machine C runs a Manager, Correlator, and Preiwkka.
30 connection attempts are sent to machine C in a short period of time and are logged by iptables. Prewikka on machine A shows the 30 events. After the timer expires, Prewikka on machine B shows the 30 events, and an Eventscan correlated event. Shortly thereafter Prewikka on machine C shows the Eventscan. After another timer period for an Eventscan expires, significant activity occurs on machine C and a second Eventscan appears. Attempting to view this in Prewikka hangs. Examination of the Prelude_Address table shows over 100,000 records generated from the second Eventscan generated on machine C. A subsequent test generating 150 events instead of 30 consumed over 2GB memory in the Prelude Correlator, causing the entire system to hang.

History

#1 - 05/05/2010 11:35 AM - Yoann VANDOORSELAERE

Hi James,

Are you sure the events triggering the issue is an EventScan? I see how the issue might be triggered by an EventStorm or an EventSweep, but EventScan are tied to a single source/destination.

Additionnally, what version of Prelude-Correlator are you using?

Regards,

#2 - 05/31/2012 04:48 PM - Jean-Charles ROGEZ

- Project changed from PRELUDE SIEM to Prelude Correlator

#3 - 05/29/2016 04:51 PM - Thomas ANDREJAK

- Status changed from New to Closed

- Assignee set to Thomas ANDREJAK

No activity