PRELUDE SIEM - Bug #1082

Problem to register my IDS (Suricata) on Prelude OSS

04/12/2019 08:13 AM - Marc-Antoine delannoy

Status:	Assigned	**Start date:**	04/12/2019
Priority:	Normal	**Due date:**	
Assignee:	Antoine LUONG	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:	Prelude OSS 5.1.0		
Resolution:			

Description

Hi,
I have a problem to register my IDS (Suricata) on Prelude OSS. My IDS is on the same network but in a different CentOs VM. The prelude address is 192.168.0.2 and the IDS address is 192.168.0.3
I already installed from source : prelude-manager, prelude lml (not used), prelude-admin and libpreludedb. I configured the /usr/local/etc/prelude/default/client.conf
to change the server-addr=127.0.0.1 to server-addr=192.168.0.2
Same for prelude-manager.conf with listen = 192.168.0.2:5553
I verify the connection between my IDS and my Prelude with a ping.
Then I enter the command line on the prelude machine :
prelude-admin registration-server prelude-manager
and on the IDS :

prelude-admin register suricata "idmef:w admin:r" 192.168.0.2 –uid 1000 –gid 1500

I copy the one shot password but get this error message on my IDS :
Connecting to registration server (192.168.0.2 :5553)
Could not connect to 192.168.0.2 port 5553 : No route to host
So I scan my port and the number 5553 remains closed throughout all the process.
I may have missed a command line or configuration, so i reread the whole doc but I didn’t found anything about it.

Do you have any suggestions?

Thanks.

History

#1 - 04/12/2019 09:52 AM - Antoine LUONG

- Status changed from New to Assigned

- Assignee set to Antoine LUONG

Hello,

Did you check your firewall rules?

Regards

#2 - 04/12/2019 12:36 PM - Marc-Antoine delannoy

Thanks for your answer.
It's exactly the problem. I just have to use firewall-cmd command to solve it.
Sorry I thought prelude was in charge of opening the port. which is obviously not possible for security reasons.

Thank you.
Regards,

Marc-Antoine Delannoy