Nagios

Configuring a Linux Server to Send Netflow Data on Nagios Network Analyzer 2024

Considerations

In all of the following examples, we will be sending UPD traffic on a specific uncommon port. This means that firewall issues are something to keep in mind (local firewall rules are automatically created). Also, each individual Netflow source will need to be sending the data on a different port, so you will need to be aware of which ports are currently being used for existing Netflow sources when adding new sources.

Configuring A Linux Server To Send Information

Open a terminal session to your Linux server, CentOS 8 users will first need to enable the PowerTools repository:

yum config-manager --set-enabled powertools

Everyone will need to run the following commands as the root user:



The script will install fprobe. It is an application, that allows the server to record its network activity in Netflow format and send it to Nagios Network Analyzer.

Nagios

www.nagios.com

Nagios

To start fprobe type the following command and press Enter (remember to replace <interface> with the actual interface name, the <NetworkAnalyzer server> with the IP of the remote machine, the <port> with the actual port number you are sending data to):

fprobe -i <interface> <NetworkAnalyzer server>:<port>

For example:

fprobe -i eth0 10.25.5.70:9915

This should be sufficient for most cases. If you have two Ethernet interfaces, you will have to modify your command. To view the usage, run from the command line:

man fprobe

To start fprobe on system boot, run the following command:

```
echo '/usr/local/sbin/fprobe -i <interface> <NetworkAnalyzer server>:<port>'
>> /etc/rc.local
```

For example:

echo '/usr/local/sbin/fprobe -i eth0 10.25.5.70:9915' >> /etc/rc.local

That completes the configuration for exporting Netflow data from a Linux server.

<u>N</u>agios

www.nagios.com

© 2024 Nagios Enterprises, LLC. All rights reserved. Nagios, the Nagios logo, and Nagios graphics are the servicemarks, trademarks, or registered trademarks owned by Nagios Enterprises. All other servicemarks and trademarks are the property of their respective owner.

<u>Nagios</u>

Create Nagios Network Analyzer Source

You are now ready create a Source within Nagios Network Analyzer to receive the exported Netflow data. For information about how to create a Source in Nagios Network Analyzer refer to the following document:

Understanding Sources And Sourcegroups In Network Analyzer

Juni	ce - centos15 🔤	play View: Default	(All Data)					© F	unning (PID: 27013
A Summar	ry Reports O Queries	Percentile Calculator							
Graph using	Logarithmic O Linear		View bandwidth	graph and top talkers for th	Date Rar	nge 👤	06/13/2017 1	1:16 - 0	6/13/2017 14:09
		Selec	Bandwidt	h Graph	legend				≡
95.4 M		00.00		show on the graph doing the	logona				
9.5 M									
976.6 K —									
510.010									
97.7 K —									
9.8 K —	11:30 11:45	12:00	12:15 12:30	12:45	13:00	13:15	13:	30	13:45
				Time					
			Bytes	Packets Bytes/Sec					
			Bytes	Packets Bytes/Sec					
			Bytes	Packets Bytes/Sec					
S	Destination IP	% Bytes	Source IP	Packets Bytes/Sec	Dest.		Src. Port	% Bytes	
(ers	Destination IP 10.25.5.13	% Bytes 60.0	Source IP	Packets Bytes/Sec	Dest. Port	% Bytes	Src. Port	% Bytes 68.9	
alkers	Destination IP 10.25.5.13 0.0.0.0	% Bytes 60.0 14.4	Source IP 10.25.13.33 56.47.98.68	Packets Bytes/Sec	Dest. Port 55591	% Bytes 30.1	Src. Port 80 5666	% Bytes 68.9 6.5	
5 Talkers	Destination IP 10.25.5.13 0.0.0 10.25.5.93	% Bytes 60.0 14.4 8.3	Source IP 10.25.13.33 56.47.98.68 10.25.11.13	Packets Bytes/Sec % Bytes 73.2 14.4 4.1	Dest. Port 55591 55595	% Bytes 30.1 29.2	Src. Port 80 5666 46720	% Bytes 68.9 6.5 6.2	
p 5 Talkers	Destination IP 10.25.5.13 0.0.00 10.25.5.93 239.255.250	% Bytes 60.0 14.4 8.3 7.5	Source IP 10.25.13.33 56.47.98.68 10.25.11.13 10.25.5.1	% Bytes/Sec % Bytes 73.2 14.4 4.1 3.6	Dest. Port 55591 55595 1900	% Bytes 30.1 29.2 10.3	Src. Port 80 5666 46720 137	% Bytes 68.9 6.5 6.2 1.9	
Top 5 Talkers	Destination IP 10.25.5.13 0.0.0 10.25.5.93 239.255.255.250 10.25.5.1	% Bytes 60.0 14.4 8.3 7.5 3.8	Source IP 10.25.13.33 56.47.98.68 10.25.11.13 10.25.5.1 10.25.18.1 10.25.18.1	% Bytes/Sec % Bytes 73.2 14.4 4.1 3.6 3.0	Dest. Port 55591 55595 1900 5666	% Bytes 30.1 29.2 10.3 6.4	Src. Port 80 5666 46720 137 1900	% Bytes 68.9 6.5 6.2 1.9 1.8	

Here is an example of the Source that was created for the Linux server added in the previous step.

<u>N</u>agios

www.nagios.com

© 2024 Nagios Enterprises, LLC. All rights reserved. Nagios, the Nagios logo, and Nagios graphics are the servicemarks, trademarks, or registered trademarks owned by Nagios Enterprises. All other servicemarks and trademarks are the property of their respective owner.