## Purpose

This document describes how Sources and Source Groups work and what they are in Nagios Network Analyzer.

#### **Understanding Sources**

A Source in Nagios Network Analyzer is the data collector. Whether it be sFlow or NetFlow, the Source is the same. Sources require a unique name and port to bind to. They create their own directory to store data and have what is called a data lifetime that determines the length of time the granular data is stored. The longer the data lifetime, the more disk space is going to be consumed.

#### **Data Lifetime**

Data lifetime was created to reduce the amount of disk space used by Sources. Granular flow data is stored for each Source you create in a directory and database files. These files can grow extremely large and fast. In order to combat the effects of requiring 10TB of disk space every month for a single Source in extreme conditions we created data lifetime.

What data lifetime does is, once data reaches the cutoff point (standard is set to 24 hours) the data is compressed, and only minimal aggregated information (such as bandwidth) is saved for viewing in graphs and other areas of the web interface. If you want longer granular data, you can set the data lifetime to longer, just be aware of the disk size requirements will vary depending on the amount of flows that are received.

#### **Source Groups**

A Source Group is a Group of one or more Sources. Grouping Sources allows you to see traffic trends on a larger scale. No extra disk space is used when you create a Source Group. These Groups do not collect any data but share the data collected by each individual Source. Because of how Source Groups work, a Source Group's data lifetime is only as long as the shortest data lifetime of a Source in the Group.

www.nagios.com



Page 1 of 12

## **Creating A Source**

In the following steps you will need to know the network port that your device will be sending flow data on. The following documentation provides steps on certain types of devices.

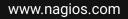
- Configuring Switch And Routers To Send Netflow Data To Network Analyzer
- Configuring A Linux Server To Send Netflow Data To Network Analyzer
- Installing And Configuring Windows Netflow Exporters For Network Analyzer

You can configure the devices before or after creating a Source, there is no specific requirement.

- 1. In Nagios Network Analyzer, select **Sources** from the navigation bar.
- 2. Click the Create Source button.

Nagios" Network Analyzer"							in 👤 nagiosadmin	
Das	hboard Sources Source	Groups Views Reports	Querles Ale	rting	,	leip Administration	1 Log Out	
Sources								
Sou	Sources							
Full list of	all sources in your system. Only	viewable sources are shown.						
Search by source name						۹		
Status	Source Name	Traffic last 30 minutes		Disk Usage	Data Lifetime	Flow Type	Actions	
No sourc	es currently exist.							

- 3. The Create Source screen will appear. Populate the following fields and selections.
  - o Source Name Must be unique and is not editable after creation.
  - Sender IP Address(es) This is an optional list of the IP address(es) of the device(s) sending flow information.
  - **Listening Port** Must be unique and over port 1024. This is the network port that the device(s) sending flow information will be received on.
  - **Incoming Flow Type** Select the flow type, either **sFlow** or **NetFlow** (including anything that is formatted as NetFlow).
  - **Raw Data Lifetime** As explained <u>earlier</u> in this document, it is the data lifetime for granular data.





Page 2 of 12

- **Disable abnormal behavior checks** Check the box if you want to disable the display of abnormal traffic on the **Dashboard**.
- Advanced Settings Click the Advanced Settings link to show the Data Directory option.
  - Data Directory Instead of using the default data directory (/usr/local/nagiosna/var/) to store the flow data, you can specify an alternate folder. The directory requires nna:users as the owner/group and the permissions of 775 granted to that folder. When the Source is created, it will create a subfolder using the Source name inside the directory given.

	ke sure you set up the source to send flow data to your NNA of you specify below to receive data.
Source Name*:	Firewall Public
	Must be unique. Name of the flow data collector. Used in back-end file system. Use a nice name that is easily associated with the flow data sending device.
Sender IP Address(es):	192.168.25.1
	Optional. Use this to internally show what IP address(es) of switches, routers, o servers are sending to this source.
Listening Port*:	9914
	Must be unlique. Port that the flow data is received on for this source. Multiple switches, routers, and servers can send to one port.
Incoming Flow Type:	NetFlow •
Raw Data Lifetime:	Use NetFlow If you're using a device that supports NetFlow, /Flow, IPFIX, etc.
	The length of time you want granular flow data to be stored on your server, recommended 24hr period saves disk space. More into.
	Disable abnormal behavior checks (removes from front page)
	Advanced Settings

4. Click the **Create Source** button when you have finished populating the fields and making selections.

www.nagios.com



5. The Source will be created and will be displayed on the **Sources** page with the status of running.

Sources								
Full list of all sources in your system. Only viewable sources are shown.  Create Source Search by source name								
Status	Source Name	Traffic last 30 minutes	Disk Usage	Data Lifetime	Flow Type	Actions		
0	Firewall Public o	No Data	1.3M	8 Weeks	NetFlow	Stop • Delete		

6. Clicking on the Source Name will bring up the details page of the Source with the **Summary** tab selected by default. It will take at least 15 minutes before the graph appears and 5 minutes before any data appears under the **Top 5 Talkers**.

Source - Firewall Public Display View:	Default (All Data)	Create	Running	(PID: 5237)	Stop Resta
Summary Reports O Queries al Percontile Calculator			Manage Views	▶ Edit	Bemove
aph using 💿 Logarithmic 🔿 Linear		View	bandwidth graph and top talkers for t	Last 24	Hours
Policy of control of	Bandwidth Graph				≡
	t the types of data to show on an	e graph using ure iegend			
93G					
93.G					
93.G		he Langer	unternet		
93.G		MULANA	umhund		1.11

Here is the Source after it has been running for over a day:

Destination IP	% Bytes	Source IP	% Bytes	Dest.		Src. Port	% Bytes
150.101.126.93	21.0	150.101.126.93	18.6	Port	% Bytes	53	37.1
2001:44b8:3132:25:10:25:2:1	11.0	192.168.25.254	10.9	53	14.9	80	6.8
192.168.25.254	10.1	192.231.203.132	10.5	80	11.1	443	2.9
192.231.203.132	4.6	2001:44b8:1::1	7.4	443	10.8	123	2.9
192.168.25.80	3.6	192.231.203.3	6.6	123	3.0	0	2.6
				5900	1.8		

www.nagios.com



Page 4 of 12

## **Stopping / Starting A Source**

Stopping a Source will stop the Source from collecting data that is being sent to it from the sender. The sender will still be sending data, unless you do something to stop it. Starting and stopping a source can be done two ways.

1. Navigate to the Sources page and use the Start and Stop links in the Actions column.



2. Navigate to the **Sources** page and click on the Source Name to bring up the details page of the selected Source. Use the **Start** and **Stop** buttons in the top right corner.



## **Editing A Source**

Editing a Source can be done on the details page of the selected Source. Click the **Edit** link in the top right corner to access the available options. These options are the same as those presented in the <u>Creating a Source</u> section and will not be explained again here.



www.nagios.com



Page 5 of 12

#### **Deleting A Source**

Deleting a Source is a destructive process and all data relating to the Source will be lost. Deleting a Source can be done two ways.

1. Navigate to the **Sources** page and use the **Delete** link in the **Actions** column.

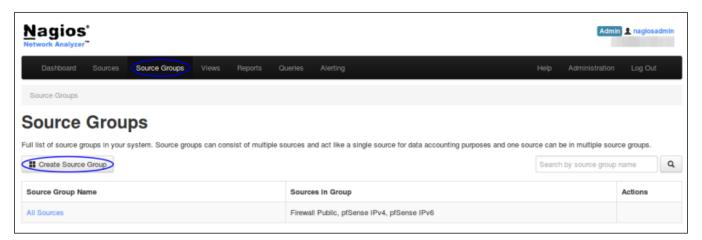
Flow Type	Actions
NetFlow	Stop Delete

2. Navigate to the **Sources** page and click on the Source Name to bring up the details page of the selected Source. Use the **Remove** link in the top right corner.



#### **Creating A Source Group**

- 1. In Nagios Network Analyzer, select Source Groups from the navigation bar.
- 2. Click the Create Source Group button.



www.nagios.com



Page 6 of 12

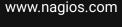
- 3. The Create Source Group screen will appear. Populate the following fields and selections.
  - Provide a name for the Source Group.
  - Select the Sources you want to add to the Group from the Available Sources column on the left. Use the arrow button to move them to the Sources in Group column on the right. You can add as many Sources as you want to a single Source Group.

	ource Group	up. Fill out all informs	Non bolow	
You will need to add one	or more source(s) to a sourcegro	up. Pill out all informa	ation below.	
Source Group Name*:	pfSense IPv4 and IPv6			
	Available Sources	Source	ces in Group	
	Firewall Public		ense IPv6	< >
Raw Data Lifetime:	Same lifetime as the source with	the shortest raw dat	a lifetime.	
Create Source Gro	Cancel			

- 4. Click the **Create Source Group** button when you have finished selecting all of the Sources.
- 5. The Source Group will be created and will be displayed on the **Source Groups** page. All of the Sources associated to the Source Group are listed in the Source Groups table.

Source Group Name	Sources In Group	Actions
All Sources	Firewall Public, pfSense IPv4, pfSense IPv6	
pfSense IPv4 and IPv6	pfSense IPv4, pfSense IPv6 (Change)	Delete

A Source Group does not "start" or "run" like a Source. The Source Group only displays data collected by the Sources associated with that Source Group.



Page 7 of 12

## **Editing A Source Group**

Editing a Source Group can be done on the details page of the selected Source Group. Click the **Edit** link in the top right corner to access the available options. These options are the same as those presented in the <u>Creating a Source Group</u> section and will not be explained again here.

Sources: pfSense IPv4, pfSense IPv6					
🗲 Edit	Remove				

#### **Deleting A Source Group**

Deleting a Source Group only removes the Group itself, it does not do anything destructive to the Sources that are in the Source Group. Deleting a Source Group can be done two ways.

1. Navigate to the **Source Groups** page and use the **Delete** link in the **Actions** column.



2. Navigate to the **Source Groups** page and click on the Source Group Name to bring up the details page of the selected Source Group. Use the **Remove** link in the top right corner.

Sources: pfSense IPv	/4, pfSense IPv6
6.5.0	<b>*</b> •
Edit	Remove

www.nagios.com

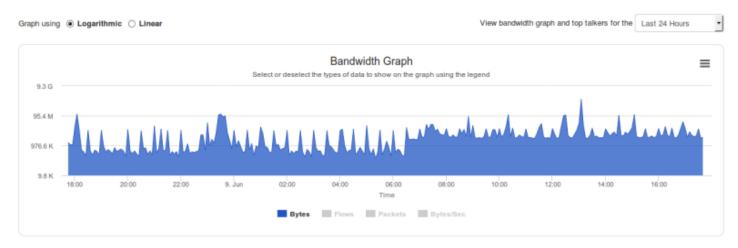


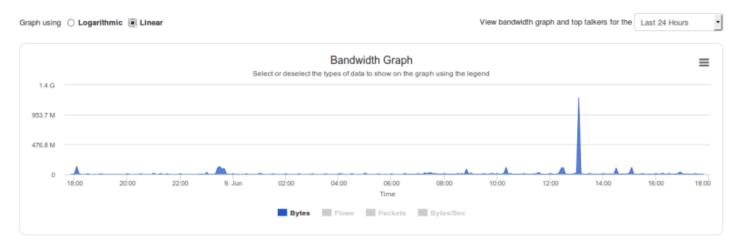
#### Sources / Source Groups Details

When viewing a Source or a Source Group, many of the features available are common to both. This section will explore what is available on these pages.

#### **Summary Tab**

The Summary tab provides a **Bandwidth Graph** and a **Top 5 Talkers** table. The **Bandwidth Graph** has two views that can be selected: **Logarithmic** and **Linear**.





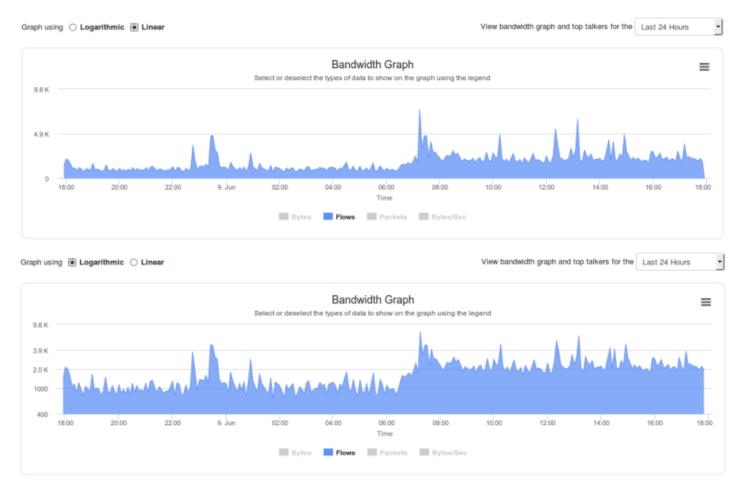
The two screenshots were taken one after the other, so the data they are generated from is identical. As you can see, the **Linear** view is a more realistic view of the traffic flow (when looking at bytes), however, a large peak can prevent you from seeing the overall trend of the traffic.

www.nagios.com



Page 9 of 12

You can also enable/disable **Bytes**, **Flows**, **Packets**, and **Bytes/Sec** on the graph by clicking on the legend. Here are the **Logarithmic** and **Linear** graphs but this time **Flows** was selected:



You can see that with these examples the overall trend on each graph is very similar.

You can change the time period of the **Bandwidth Graph** by making a selection from the drop-down list in the top right corner of the graph.

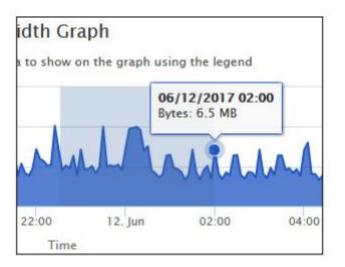
View bandwidth graph and top talkers for the	Last 24 Hours	2	
	Last 24 Hours		
	Last 2 Days		
	Last Week Last Month		
legend			

www.nagios.com

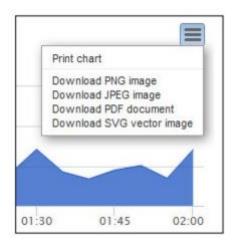


Page 10 of 12

You can also zoom in on a specific time period by dragging the mouse cursor over the time period that you want to focus on.



Export the graph by clicking the **Chart context menu** icon in the top right corner of the graph.



#### **Reports and Queries Tabs**

The **Reports** and **Queries** tabs are explained in more detail in the following documentation:

- Understanding And Using Network Analyzer Reports
- Understanding And Using Custom Queries In Network Analyzer

www.nagios.com



Page 11 of 12

#### **Percentile Calculator Tab**

The percentile calculator is used to calculate the bandwidth usage based on the flow data collected. Please refer to the **How is this calculated** link under the **Percentile Calculator Tab** for a detailed explanation.

Here is an example for a month's time period.

Time frame: 05/01/2017 00:00 to 06/01/2017 00:00	Select Data Type: Bps	Percentile: 95 Calculate
95th Percentile Calculation ⊖ Print ⊖ PDF Generated for 05/01/2017 00:00 to 06/01/2017 00:00		
8429.00 7024.17 5619.33 4214.50 2809.67 1404.83 0.00 Samples	Data sample size:5 minutesNumber of samples:892995th Percentile:21.910 Bps	

## Views

You will also notice that there are selections for views on the screens you have been navigating. Views are used to define specific data retention settings which are different to the source they are applied to. More detailed information on this topic is located in the <u>Understanding And Using Views In</u> <u>Network Analyzer</u> documentation.

## **Finishing Up**

This completes the documentation on understanding Sources and Source Groups in Nagios Network Analyzer. If you have additional questions or other support-related questions, please visit us at our Nagios Support Forum, Nagios Knowledge Base, or Nagios Library:

Visit Nagios Support Forum

Visit Nagios Knowledge Base

Visit Nagios Library

www.nagios.com



Page 12 of 12