



Purpose

This document describes what Sources and Source Groups are and how they work within Nagios Network Analyzer. You will learn how to create new Sources, start and stop Sources, and create new Source Groups.

Target Audience

This document is intended for use by network administrators who want to setup and use 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.

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.

On the menu bar navigate to **Sources**.



Admin nagiosadmin

Dashboard **Sources** Source Groups Views Reports Queries Alerting Help Administration Log Out

Sources

Sources

Full list of all sources in your system. Only viewable sources are shown.

Create Source



Status	Source Name	Traffic last 30 minutes	Disk Usage	Data Lifetime	Flow Type	Actions
No sources currently exist.						

Click the **Create Source** button.

Populate the following fields and selections.

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 - This is explained previously in this document, it is the data lifetime for granular data.

Disable abnormal behavior checks - Check the box if you want to disable the display of abnormal traffic on the Dashboard.

Advanced Settings

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 sub-folder using the Source name inside the directory given.

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

Create Source

When adding a new source, make sure you set up the source to send flow data to your NNA installation IP address at the port you specify below to receive data.

Source Name*:
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):
Optional. Use this to internally show what IP address(es) of switches, routers, or servers are sending to this source.

Listening Port*:
Must be unique. Port that the flow data is received on for this source. Multiple switches, routers, and servers can send to one port.

Incoming Flow Type:
 Use NetFlow if you're using a device that supports NetFlow, jFlow, IPFIX, etc.

Raw Data Lifetime:
 The length of time you want **granular flow data** to be stored on your server, recommended 24hr period saves disk space. [More info.](#)

Disable abnormal behavior checks (removes from front page)

[Advanced Settings](#) ^

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

Sources

Full list of all sources in your system. Only viewable sources are shown.

[Create Source](#)

Status	Source Name	Traffic last 30 minutes	Disk Usage	Data Lifetime	Flow Type	Actions
✔	Firewall Public	No Data	1.3M	8 Weeks	NetFlow	Stop • Delete

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 graph appears and 5 minutes before any data appears under the Top 5 Talkers. Here is the Source after it has been running for over a day:

Sources / Source - Firewall Public

Source - Firewall Public

Display View: ✔ Running (PID: 5237)

[Summary](#) [Reports](#) [Queries](#) [Percentile Calculator](#) [Manage Views](#) [Edit](#) [Remove](#)

Graph using Logarithmic Linear View bandwidth graph and top talkers for the

Bandwidth Graph

Select or deselect the types of data to show on the graph using the legend

Top 5 Talkers

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

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:

On the main Source page using the links under the **Actions** column.

Flow Type	Actions	Flow Type	Actions
NetFlow	Stop Delete	NetFlow	Start Delete

On the selected Source page using the buttons in the top right corner.

Running (PID: 29579)
[Stop](#)
[Restart](#)
[Start](#)

[Manage Views](#)
[Edit](#)
[Remove](#)
[Manage Views](#)
[Edit](#)
[Remove](#)

Editing A Source

Editing a Source can be done when on the details page of the Source. Click the **Edit** link at the top right of the page and the options that can be updated will be presented. These options are identical to when creating the Source and hence will not be explained here.

Running (PID: 5237)
[Stop](#)
[Restart](#)

[Manage Views](#)
[Edit](#)
[Remove](#)

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:

On the main Source page using the links under the **Actions** column.

Flow Type	Actions
NetFlow	Stop Delete

On the selected Source page using the **Remove** link in the top right corner.

Running (PID: 29579)
[Stop](#)
[Restart](#)

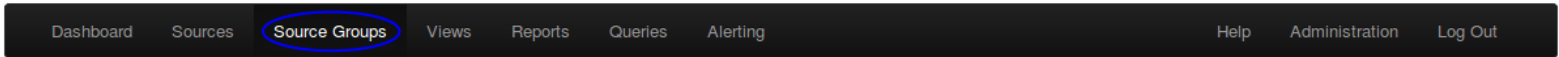
[Manage Views](#)
[Edit](#)
[Remove](#)

Creating A Source Group

On the menu bar navigate to **Source Groups**.



Admin naglosadmin



Source Groups

Source Groups

Full list of source groups in your system. Source groups can consist of multiple sources and act like a single source for data accounting purposes and one source can be in multiple source groups.

Create Source Group

Search by source group name



Source Group Name	Sources in Group	Actions
All Sources	Firewall Public, pfSense IPv4, pfSense IPv6	

Click the **Create Source Group** button.

Provide a name for the Source Group.

Select the Sources you'd like to place into the Group by selecting them from the left and use the arrow button to move them to right.

You can add as many Sources as you want to a single Source Group.

Once you have selected all of the Sources, click the **Create Source Group** button.

Create Source Group

You will need to add one or more source(s) to a sourcegroup. Fill out all information below.

Source Group Name*:

Available Sources

 Firewall Public


Sources in Group

 pfSense IPv4
 pfSense IPv6

Raw Data Lifetime: Same lifetime as the source with the shortest raw data lifetime.

Once created, the new Source Group will show up in the Source Groups list. 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 display data collected by the Sources associated with that Source Group.

Editing A Source Group

Editing a Source Group can be done when on the details page of the Source Group. Click the **Edit** link at the top right of the page and the options that can be updated will be presented. These options are identical to when creating the Source Group and hence will not be explained 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:

On the main Source Group page using the links under the **Actions** column.


Actions

[Delete](#)

Sources: [pfSense IPv4](#), [pfSense IPv6](#)

On the selected Source Group page using the **Remove** link in the top right corner.

 Edit

 Remove

Sources / Source Groups Details

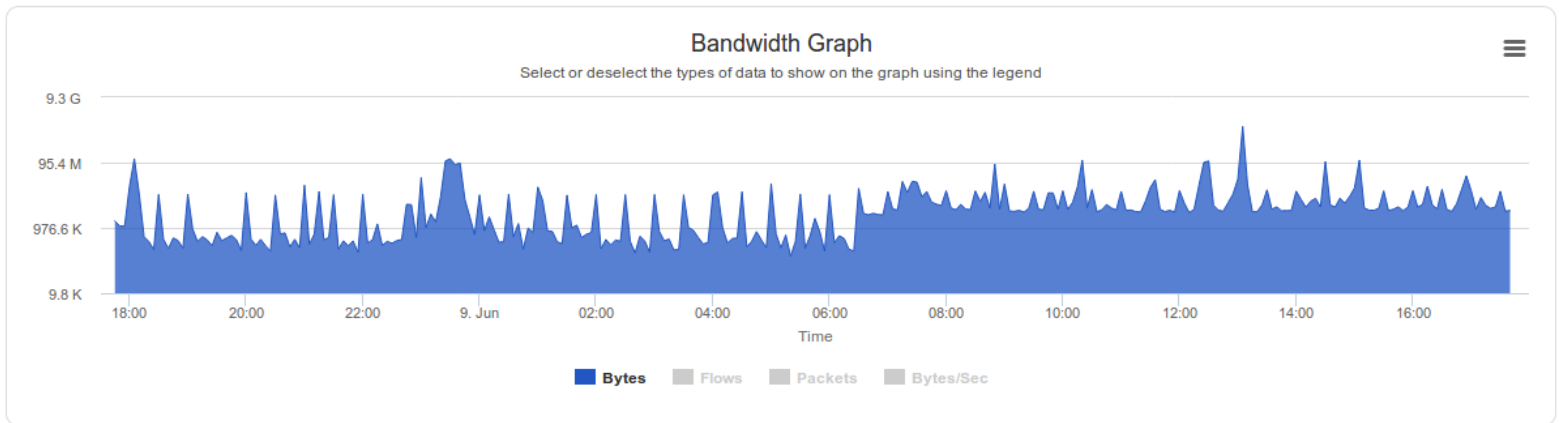
When viewing a Source or a Source Group, many of the features available are common to both. This section will explore what is available on these pages.

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**:

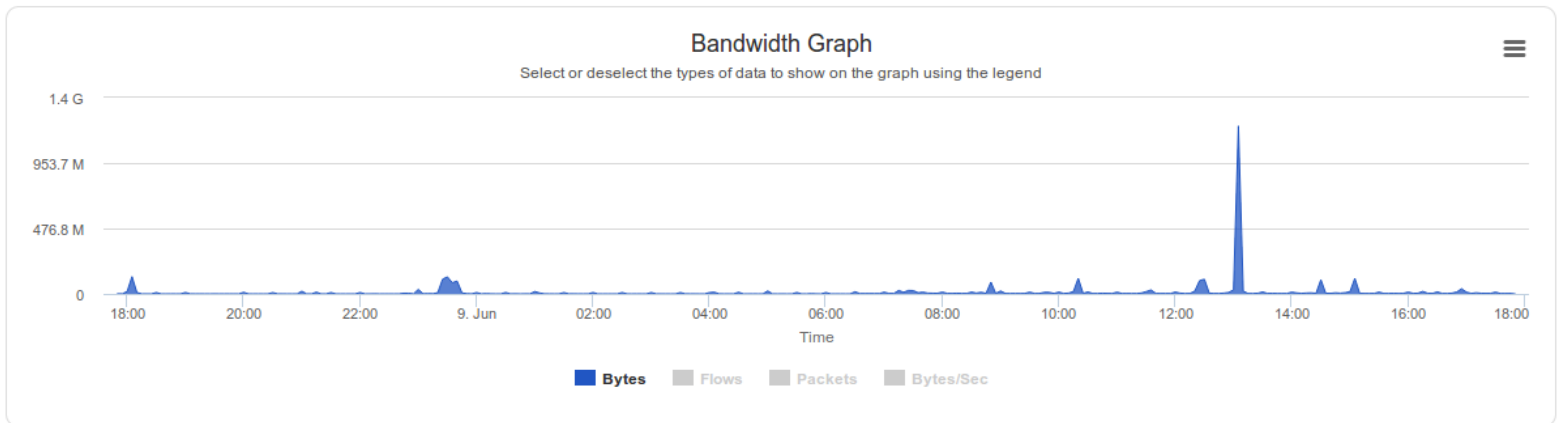
Graph using Logarithmic Linear

View bandwidth graph and top talkers for the Last 24 Hours



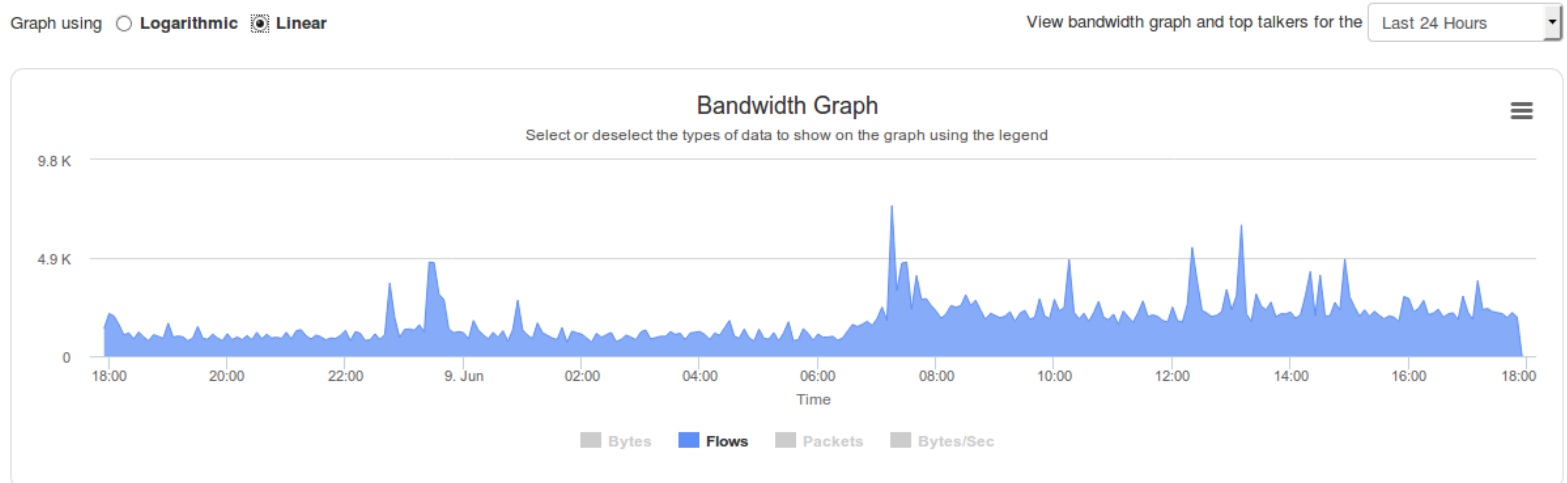
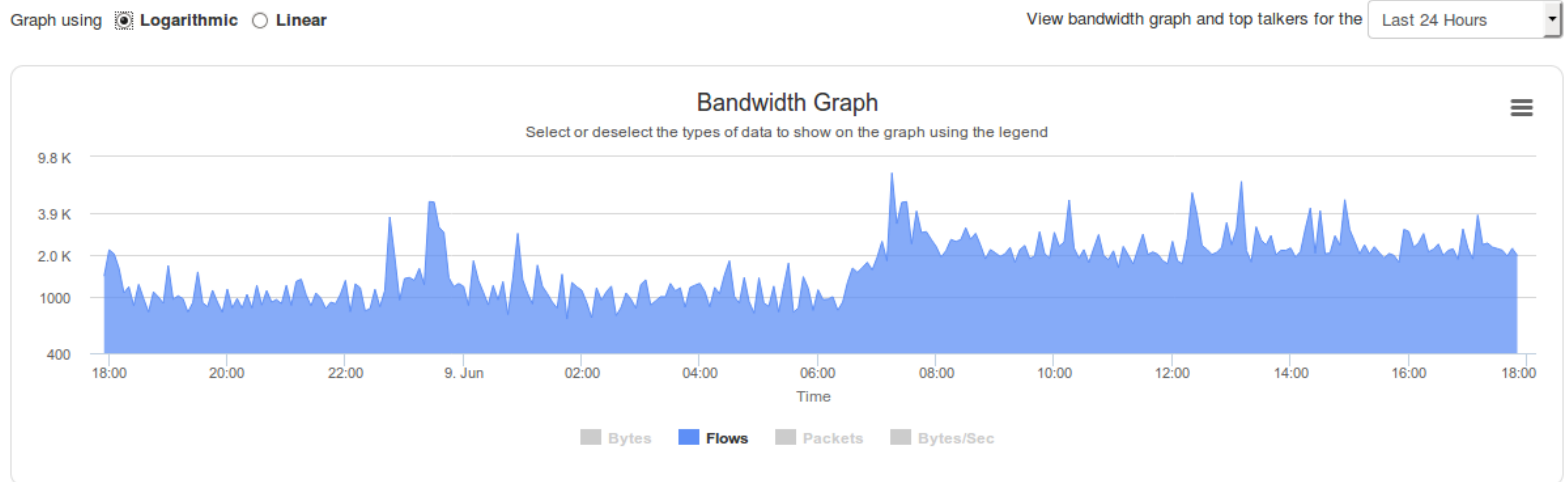
Graph using Logarithmic Linear

View bandwidth graph and top talkers for the Last 24 Hours



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.

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.

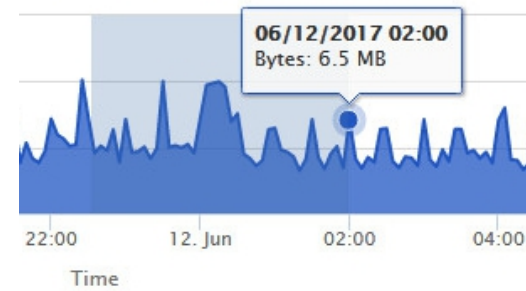
You can change the time period of the bandwidth graph by making a selection from the drop down list at the top right of the graph.



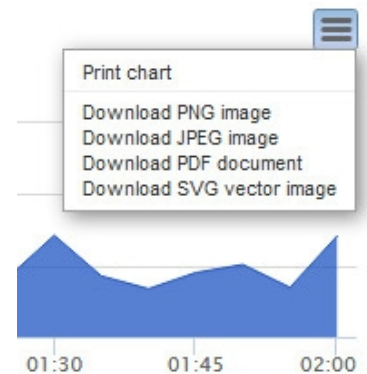
You can also zoom in on a specific time period by dragging the mouse cursor over the time period that you want to focus on.

Bandwidth Graph

Click to show on the graph using the legend



A graph can be exported by clicking the icon of three horizontal lines at the top right 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](#)

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 on the screen for a detailed explanation. Here is an example for a month time period.

Time frame: to Select Data Type: Percentile:

95th Percentile Calculation

Generated for 05/01/2017 00:00 to 06/01/2017 00:00



Data sample size: **5 minutes**

Number of samples: **8929**

95th 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 [Understanding And Using Views In Network Analyzer](#) documentation.

Finishing Up

This completes the documentation on 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 Forums:

<https://support.nagios.com/forum>

The Nagios Support Knowledgebase is also a great support resource:

<https://support.nagios.com/kb>