How To Understand Sources And Source Groups In Nagios Network Analyzer 2024

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.

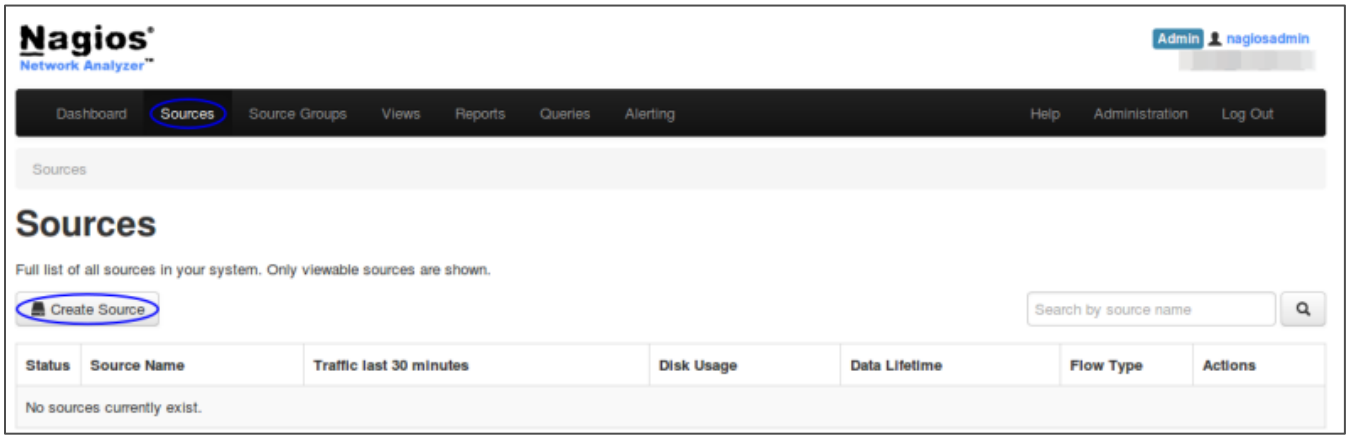
Creating A Source

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

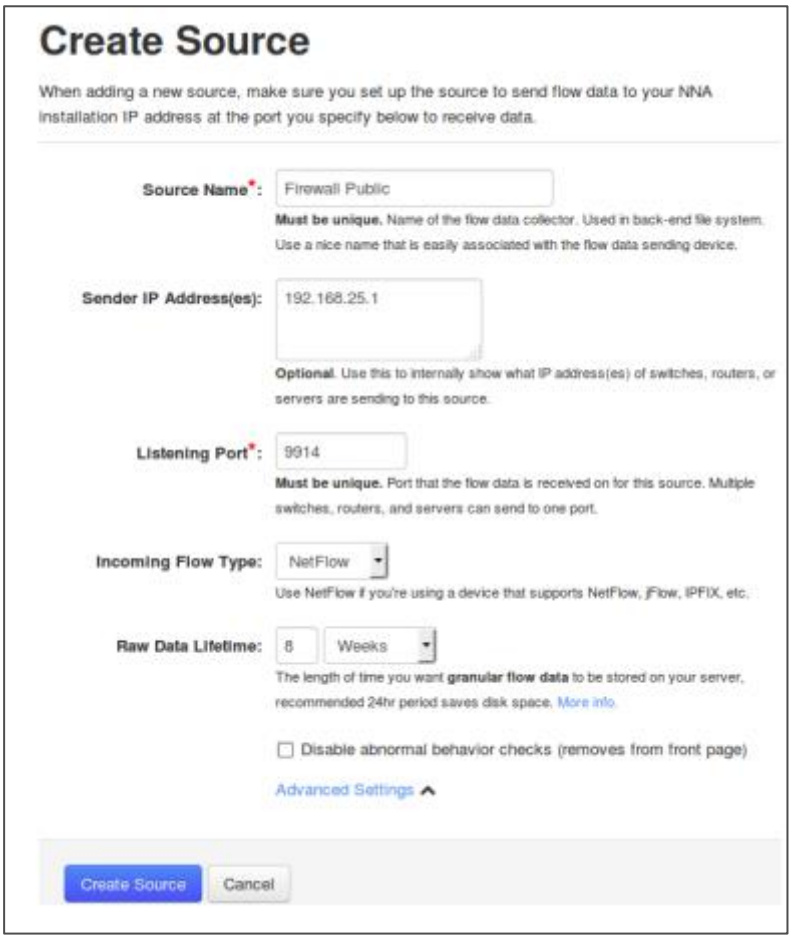
You can configure the devices before or after creating a Source, there is no specific requirement.

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



3. The **Create Source** screen will appear. 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** - As explained earlier 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** - 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.

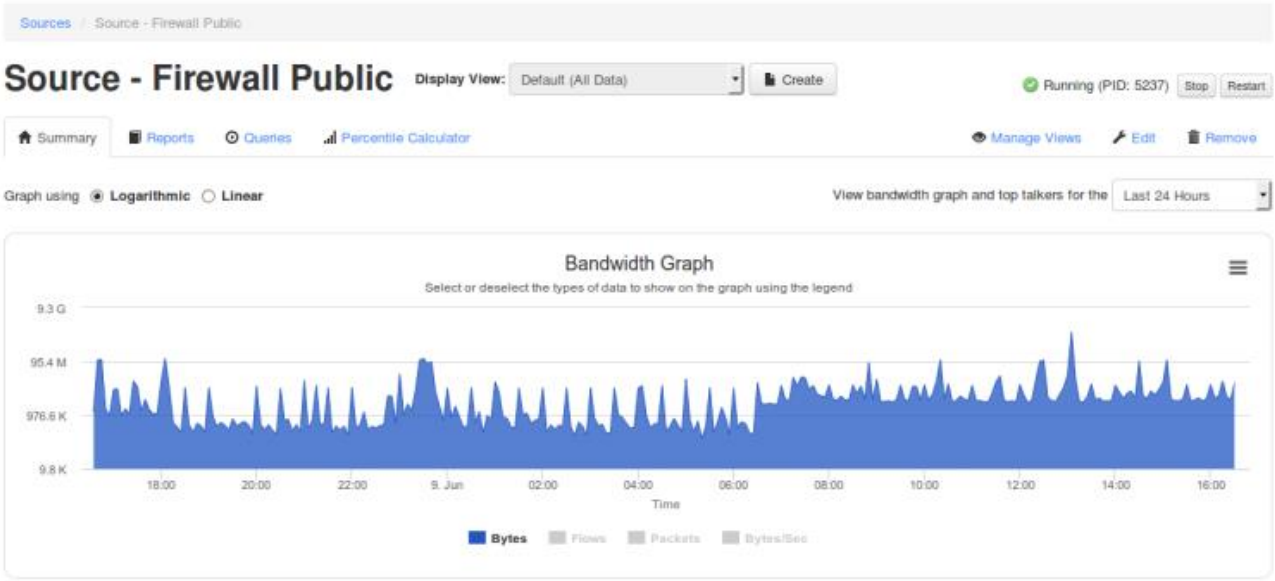


4. Click the **Create Source** button when you have finished populating the fields and making selections.

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

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**.

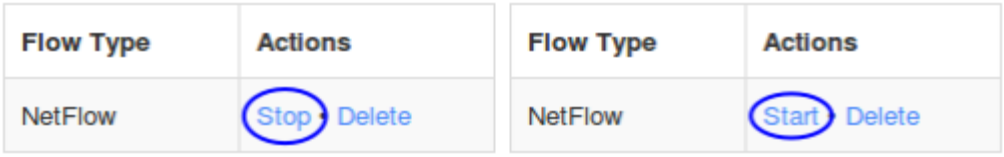
   Here is the Source after it has been running for over a day:



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.

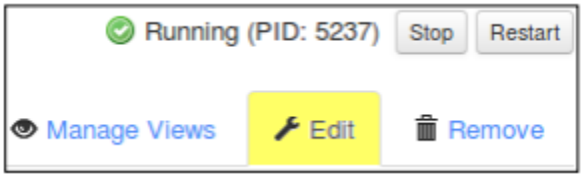
1. Navigate to the **Sources** page and use the **Start** and **Stop** links in the **Actions** column**.**



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 Creating a Source section and will not be explained again here.



Deleting A Source

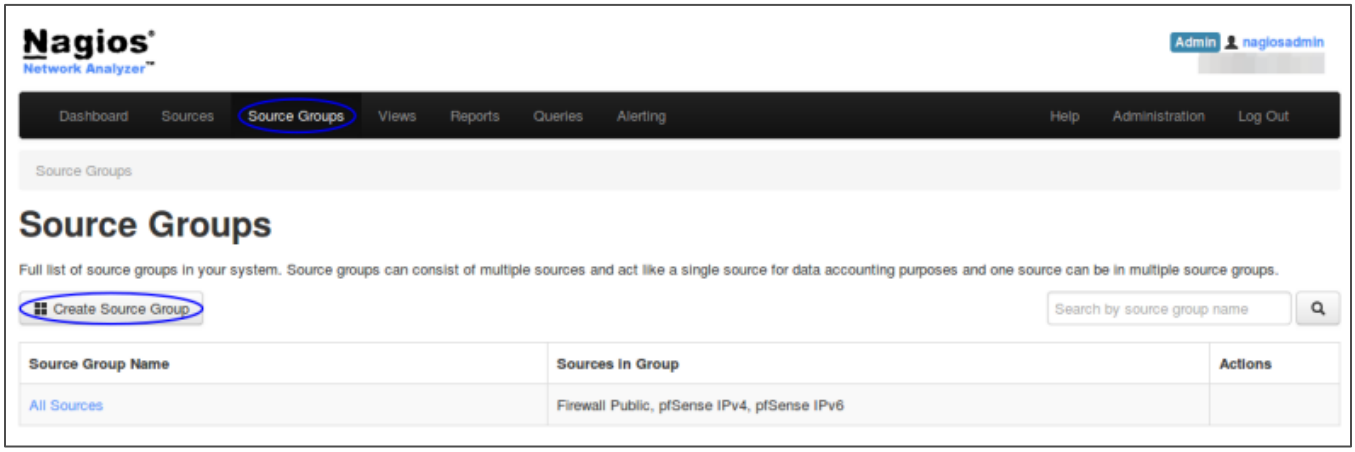
Deleting a Source is a destructive process and all data relating to the Source will be lost. Deleting a Source can be done two ways.

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

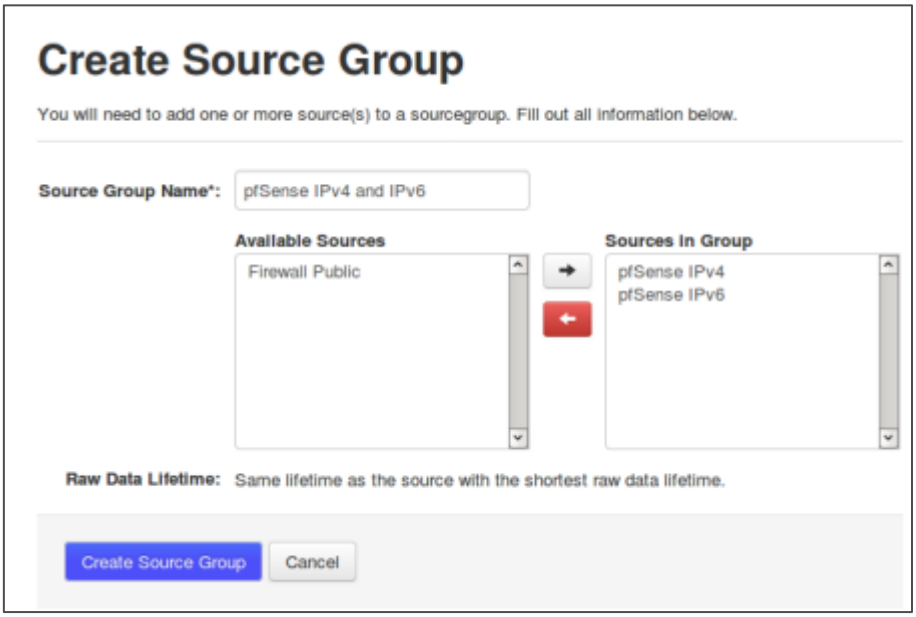
2. Navigate to the **Sources** page and click on the Source Name to bring up the details page of the selected Source. Use the **Remove** link in the top right corner.

Creating A Source Group

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



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.



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.

Editing A Source Group

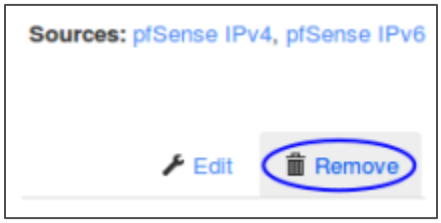
Editing a Source Group can be done on the details page of the selected Source Group. Click the **Edit** link in the top right corner to access the available options. These options are the same as those presented in the Creating a Source Group section and will not be explained again here.

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.

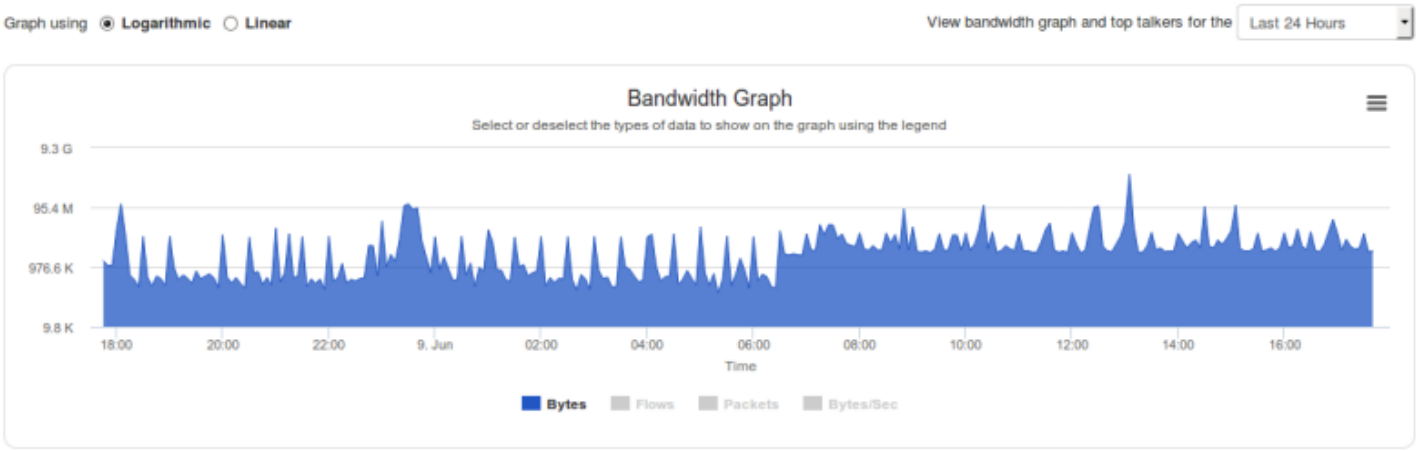


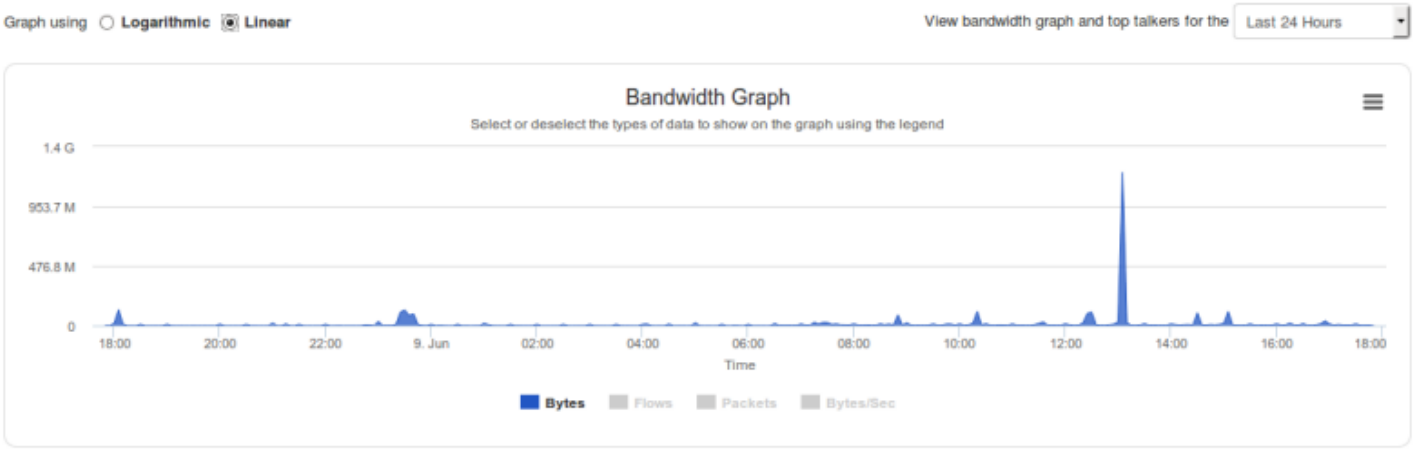
Sources / Source Groups Details

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**.

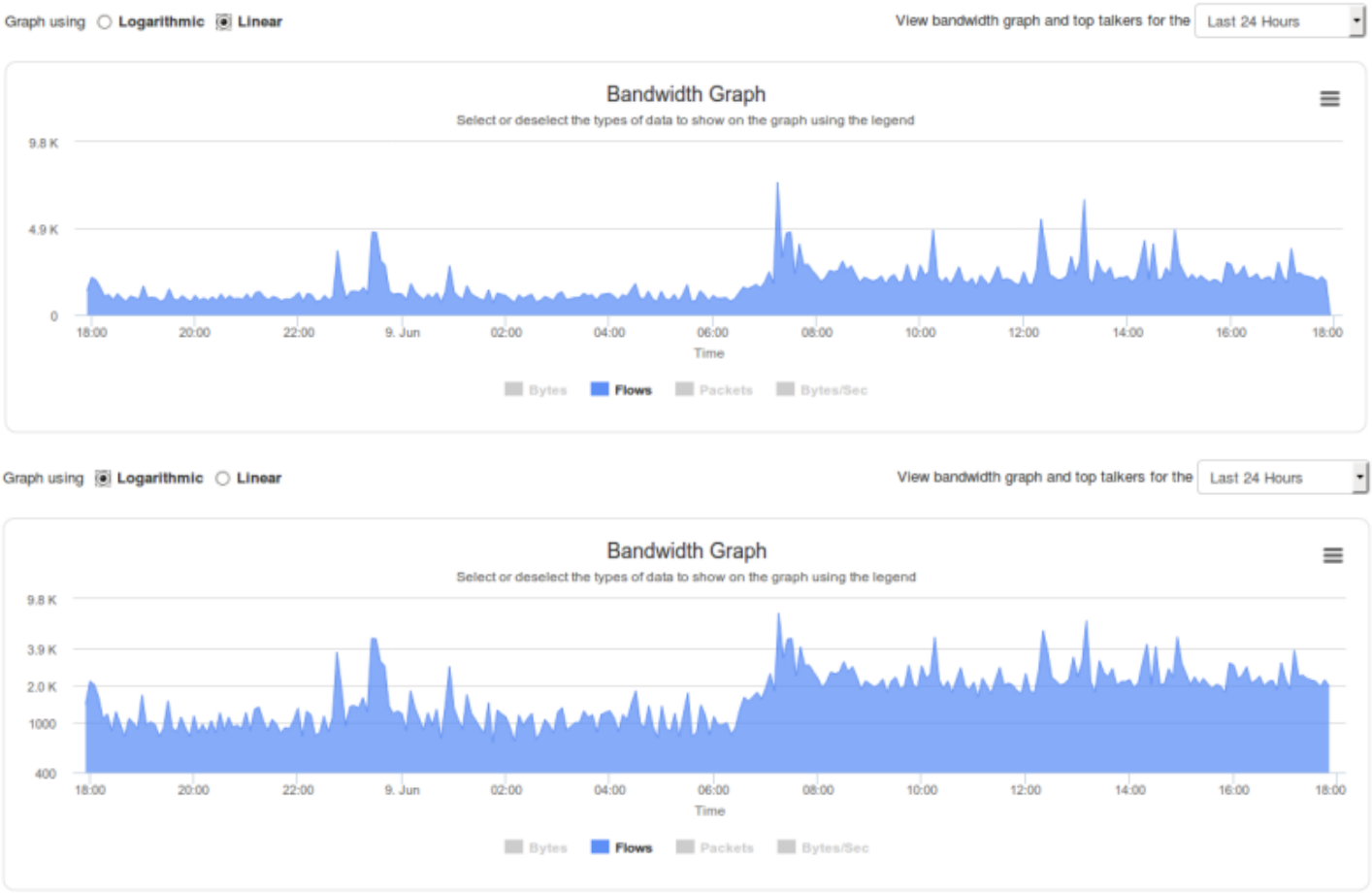




The two screenshots were taken one after the other, so the data they are generated from is identical. As you can see, the **Linear** view is a more realistic view of the traffic flow (when looking at bytes), however, a large peak can prevent you from seeing the overall trend of the traffic.

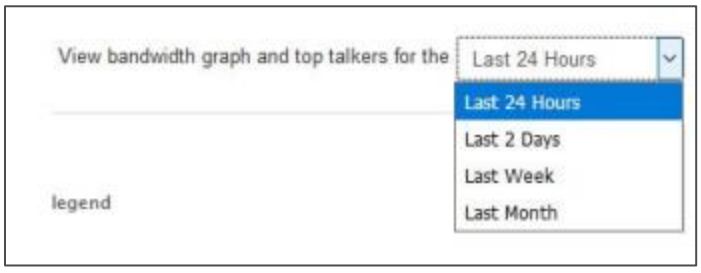
How To Understand Sources And Source Groups In Nagios Network Analyzer 2024

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:

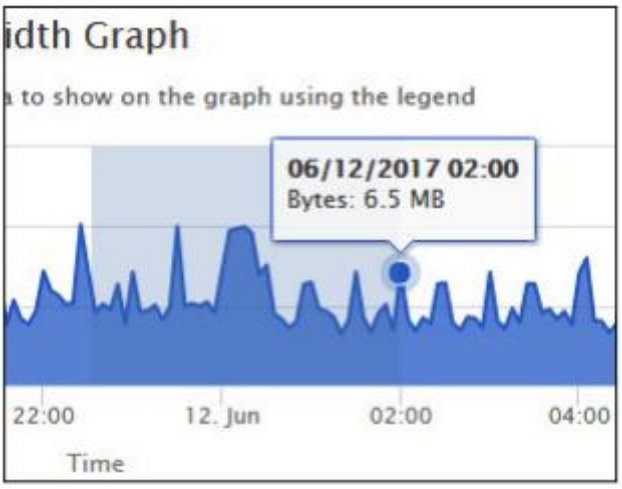


You can see that with these examples the overall trend on each graph is very similar.

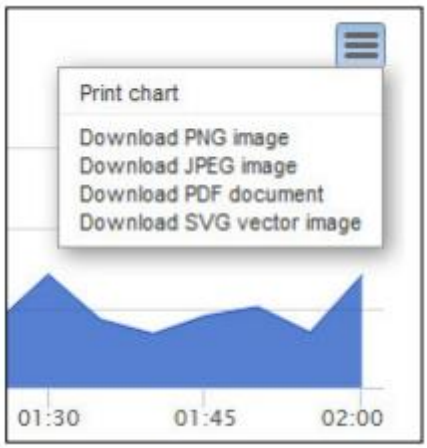
You can change the time period of the **Bandwidth Graph** by making a selection from the drop-down list in the top right corner of the graph.



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

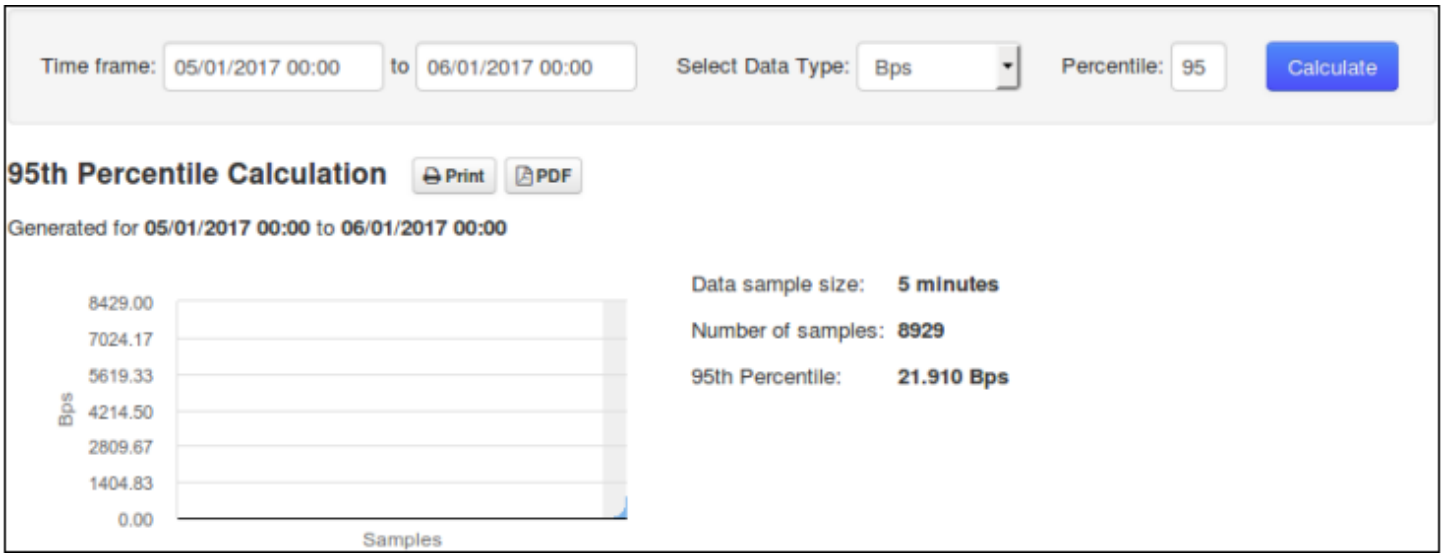
The **Reports** and **Queries** tabs are explained in more detail in the following documentation:

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

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.



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 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