Network Analyzer

Understanding And Using Reports

Purpose

This document describes how to understand, configure, and use Reports in Nagios Network Analyzer.

Target Audience

This document is intended for use by network administrators who want to integrate Nagios Network Analyzer reporting into their Network Analysis.

Considerations

This guide expects that you have a current and running installation of Nagios Network Analyzer, and that you have valid Netflow data with which to base your reports.

The Reports Menu

On the navigation menu in Nagios Network Analyzer click **Reports**.

You are presented with a list of available reports. The screenshot above shows the four reports that come

included in Nagios Network Analyzer. These reports are permanent and cannot be deleted (deleting will be discussed later).

Running A Report

A report can be run by clicking the **Run** link under the actions column. You are prompted to select a Source or Source group that you want to execute the report against. Once you click the **Run Report** button you will be taken to the Source or Source Group page with the results of the report just executed.

Run a Report   ✕

Select the source or sourcegroup to run the report on.

       ⦿ Source   ◯ Source Group

Run On: Firewall Public   ▾

                                       Cancel   Run Report ❯

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

Sources / Source - Firewall Public / Reports

Source - Firewall Public

Display View: Default (All Data) ▾ 📄 Create   ✅ Running (PID: 5237) Stop Restart

🏠 Summary   📋 Reports   ⊙ Queries   📊 Percentile Calculator   👁 Manage Views 🔧 Edit 🗑 Remove

Custom Report Saved Report   Top 5 Talkers By Destination Port (Last 24 Hours) *   ▾   Run Report ❯   📄 PDF

☰ Pie Chart   ⤢ dstport <=> srcip   ⤢ dstport <=> dstip   ⤢ dstport <=> srcport
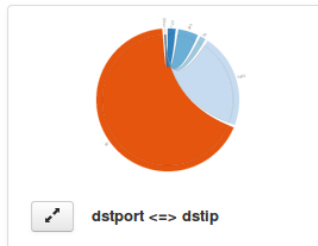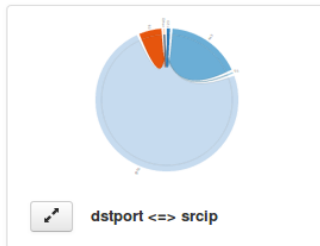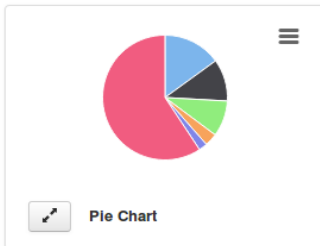
Top 5 Talkers By Destination Port (Last 24 Hours)

Displaying top 5 from **last 24 hours** grouping by **destination port** and ordering by **bytes**.

                                      ➚ External API   ⓘ Use Via HTTP

Start Date	End Date	Duration	Protocol	Destination Port	Flows	Flow %	Packets	Packet %	Bytes	Byte %	Packets/Sec	Bits/Sec	Bits/Packet
2017-06-08 11:02:16	2017-06-09 10:53:59	85903	any	53	136875	36.1	139138	21.1	10.25 MB	15.0	1	1000	77
2017-06-08 11:02:11	2017-06-09 10:53:07	85855	any	80	10779	2.8	74633	11.3	7.46 MB	10.9	0	728	104
2017-06-08 11:02:33	2017-06-09 10:52:06	85773	any	443	5560	1.5	57377	8.7	6.40 MB	9.3	0	625	116
2017-06-08 11:02:11	2017-06-09 10:53:33	85881	any	123	27746	7.3	29556	4.5	2.25 MB	3.3	0	219	79
2017-06-08 11:02:47	2017-06-09 10:34:06	84679	any	5900	5344	1.4	33653	5.1	1.48 MB	2.2	0	146	46

1295 Bandana Blvd N, St. Paul, MN 55108   sales@nagios.com   US: 1-888-624-4671   INTL: 1-651-204-9102

Nagios®   **www.nagios.com**

You can see that several charts are generated, you can click the icon on any chart to enlarge it. On some of the charts you can hover the mouse on a port/address and the chart will highlight the relationship with the other objects.

Underneath the charts is the detailed table of the results from the report. Some of the columns provide hyperlinks in the table of data, clicking these will execute a new query. In the screenshot on the previous page this is the Destination Port column.

There are some buttons on the page that provide the following functionality:

PDF   Turn the report into a PDF, this will be generated and opened in your web browser.

External API   This opens the raw report data into a web browser. The URL in the address bar has all the particular details about the report being run.

Use Via HTTP   This opens a modal that provides a URL *(what was used by the External API button)* and also an example of running the report using a CURL request.

Creating A Report

On the Reports page click the **Create Report** button.

A modal will appear providing a selection of options for creating the custom report. The options here are self-explanatory, except for **Limiter** which will be explained a bit later on.

Click the **Save** button to create the new report.

Create Custom Report   ✕

A custom report can be run on any source and is not linked to sources specifically. Use a limiter query to get data for specific ports or ips.

Report Name: Bytes - Top 10 - Last Week - Destination IP

Display top #: 10

Time Range: Last Week

Group By: Destination IP

Order By: Bytes

Limiter (Optional): ip 192.168.0.1

Cancel   Save

www.nagios.com

You will be returned to the reports page and the new report will now appear in the list.

☐	Bytes - Top 10 - Last Week - Destination IP	Run • Edit • Delete

Run the report to see if it generated the information you were after. In this example I have run the report against a Source Group and here is the table of information generated by the report:

Start Date	End Date	Duration	Protocol	Destination IP	Flows	Flow %	Packets	Packet %	Bytes	Byte %	Packets/Sec	Bits/Sec	Bits/Packet
2017-06-06 07:10:32	2017-06-06 16:34:38	33845	any	2001:44b8:3132:25:10:25:14:91	178	0.0	589486	2.7	707.92 MB	7.8	17	175458	1259
2017-06-02 22:43:28	2017-06-09 09:45:28	558120	any	2001:44b8:3132:25:10:25:14:51	149	0.0	467395	2.1	582.20 MB	6.4	0	8750	1306
2017-06-02 11:44:22	2017-06-09 11:33:34	604152	any	2001:44b8:3132:25:10:25:254:50	22462	0.8	813696	3.7	580.25 MB	6.4	1	8056	747
2017-06-08 07:13:31	2017-06-08 09:08:11	6880	any	2001:44b8:3132:25:7c83:ebf6:4d33:e6ed	653	0.0	375537	1.7	482.59 MB	5.3	54	588392	1347
2017-06-02 14:12:16	2017-06-08 17:34:13	530516	any	2001:44b8:3132:25:10:25:14:52	251	0.0	314027	1.4	419.48 MB	4.6	0	6632	1400
2017-06-02 11:46:57	2017-06-09 11:30:48	603831	any	2001:44b8:3132:25:10:25:5:70	8290	0.3	726896	3.3	388.08 MB	4.3	1	5391	559
2017-06-02 11:44:17	2017-06-09 11:31:11	604013	any	239.255.255.250	25460	0.9	947178	4.3	385.28 MB	4.2	1	5350	426
2017-06-02 17:16:45	2017-06-02 19:10:48	6843	any	2001:44b8:3132:25:250:56ff:feab:4bd9	108	0.0	256316	1.2	363.12 MB	4.0	37	445122	1485
2017-06-02 17:21:23	2017-06-02 18:57:00	5737	any	2001:44b8:3132:25:10:25:254:ab3a	117	0.0	248683	1.1	352.45 MB	3.9	43	515307	1486
2017-06-02 11:43:59	2017-06-09 11:33:59	604200	any	2001:44b8:3132:25:10:25:2:1	190568	6.7	392408	1.8	328.41 MB	3.6	0	4559	877

It's interesting to see that in a network of IPv4 and IPv6 addresses that IPv6 is the top of the list. With that in mind the next step shows you how to edit a report and will discuss using a Limiter.

Editing A Report

On the Reports page click the **Edit** link in the **Actions** column for the report you want to edit.

A modal will appear providing the same selection of options when you created the report.

The **Limiter** option allows you to use raw query syntax to make the report more granular. The raw query syntax is explained in the [Understanding And Using Custom Queries In Network Analyzer](#) documentation and hence will not be explained in detail here.

In this example the following limiter is going to be added:

```
net 10.25.0.0/16 OR net 2001:44b8:3132:25::/64
```

Click the **Save** button to update the new report. Now when the report is run the information returned is specific to the subnets that was defined by the limiter.

Start Date	End Date	Duration	Protocol	Destination IP	Flows	Flow %	Packets	Packet %	Bytes	Byte %	Packets/Sec	Bits/Sec	Bits/Packet
2017-06-06 07:10:32	2017-06-06 16:34:38	33845	any	2001:44b8:3132:25:10:25:14:91	178	0.0	589486	4.1	707.92 MB	9.2	17	175458	1259
2017-06-02 22:43:28	2017-06-09 09:45:28	558120	any	2001:44b8:3132:25:10:25:14:51	149	0.0	467395	3.3	582.20 MB	7.6	0	8750	1306
2017-06-02 12:01:27	2017-06-09 11:46:02	603874	any	2001:44b8:3132:25:10:25:254:50	22468	1.3	813625	5.7	580.19 MB	7.5	1	8059	747
2017-06-08 07:13:31	2017-06-08 09:08:11	6880	any	2001:44b8:3132:25:7c83:ebf6:4d33:e6ed	653	0.0	375537	2.6	482.59 MB	6.3	54	588392	1347
2017-06-02 14:12:16	2017-06-08 17:34:13	530516	any	2001:44b8:3132:25:10:25:14:52	251	0.0	314027	2.2	419.48 MB	5.4	0	6632	1400
2017-06-02 11:59:51	2017-06-09 11:43:52	603841	any	2001:44b8:3132:25:10:25:5:70	8295	0.5	727869	5.1	388.52 MB	5.0	1	5397	559
2017-06-02 17:16:45	2017-06-02 19:10:48	6843	any	2001:44b8:3132:25:250:56ff:feab:4bd9	108	0.0	256316	1.8	363.12 MB	4.7	37	445122	1485
2017-06-02 17:21:23	2017-06-02 18:57:00	5737	any	2001:44b8:3132:25:10:25:254:ab3a	117	0.0	248683	1.7	352.45 MB	4.6	43	515307	1486
2017-06-02 11:59:32	2017-06-09 11:48:59	604167	any	2001:44b8:3132:25:10:25:2:1	190156	11.3	392019	2.7	328.34 MB	4.3	0	4558	878
2017-06-06 20:55:19	2017-06-08 21:06:48	173488	any	2001:44b8:3132:25:10:25:10:1	9760	0.6	287679	2.0	219.80 MB	2.9	1	10627	801

As you can imagine, the Limiter expands the capabilities of the reports you can generate. Keep in mind that the more complex a limiter you have, the longer it can take to run a report.

Deleting Reports

On the Reports page you can delete reports individually by clicking the **Delete** link in the Actions column.
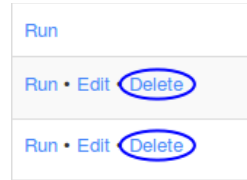
You can also delete multiple reports by checking the boxes in the left column and then clicking the **Delete** button above.

Running Reports via Source or Source Group

Reports can also be run directly from a **Source** or **Source Group**.

Click the reports tab and select a report from the drop down list.

Resolving Addresses To Hostnames

If you would like your reports to resolve the network addresses to hostnames you will neeed to enable this functionality. Navigate to **Administration** > **General** > **Global Settings**.

Here you can enable **Reports and Queries** and/or **Graphs**. Please ensure that your Nagios Network Analyzer server is correctly configured to DNS server(s) that can correctly resolve internal and external network addresses.

Finishing Up

This completes the documentation on understanding and using reports 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