netmon

6.1

Reporting Guide

Contents

Reports Explorer

To access the Netmon Reports Explorer, click the Reports button in the top toolbar. Netmon ships with a selection of built-in reports. These reports are customizable, can be saved for later re-use or run automatically on a user defined schedule.

Network Activity

The Network Activity Report allows you to query Netmon's network traffic database for any type of activity, for any host.

To run a Network Activity Report, open the Report Explorer by clicking the **Reports** link in the top toolbar.

1. Click the **New Report Builder** button in the Report Explorer. This will open the Report Builder Wizard. Choose *Network Activity Report* from the **Report Type** selection box.
2. If you plan to use this report later, enter a label that will be used to identify it in the **Label** text box.
3. Choose a **Source Interface** from the available drop-down box. You can select any of Netmon's built-in Local Packet Analyzers, or any NetFlow-enabled interface.
4. Determine which hosts are going to be included in your report by making a selection in the **Host(s)** drop-down box. You can choose from a variety of options here, including:
   a. **All Hosts:** All hosts with activity on the specified packet analyzer or Netflow interface.
   b. **Specific IP Address:** You can enter an IP address here to run a report for a specific host.
   c. **Keyword Search:** Hosts matching a keyword or character pattern.
   d. **Host Filter:** If you are using Host Filters, they will be available for selection here.
5. Determine what network traffic you're interested in. There are several available options here:

    a. **All Activity:** All network activity on the specified packet analyzer or Netflow interface.

    b. **Specific Protocol:** If you're looking for activity on a specific TCP or UDP port, choose this option, then enter the port number in the box that appears.

    c. **Traffic Filter:** If you are using Traffic Filters, they will be available for selection here.

6. Choose a maximum number of results to retrieve from the database in the **Limit Results** drop-down box.

7. Determine the order of results in the report by making a selection in the **Order Results By** drop-down box.

8. Click the **Next Step** button in the wizard dialog window.

9. Choose a reporting period from the available list. You can choose specific start and end times by selecting **Custom Range** from this list, which will then expose fields for start and end time.

10. If you want to run this report on a regular schedule, check the **Schedule this report to run automatically** box, and follow the instructions in *Saving and Scheduling Reports* on page 17.

11. Click the **Run Report Now** button.

Network Conversations

The Network Conversation Report allows you to examine network activity between two hosts, or two groups of hosts.

To run a Network Conversation Report, open the Report Explorer by clicking the **Reports** link in the top toolbar.

1. Click the **New Report Builder** button in the Report Explorer. This will open the Report Builder Wizard. Choose *Network Conversation Report* from the **Report Type** selection box.

2. If you plan to use this report later, enter a label that will be used to identify it in the **Label** text box.

3. Choose a **Source Interface** from the available drop-down box. You can select any of Netmon's built-in Local Packet Analyzers, or any NetFlow-enabled interface.

4. Determine which source hosts are going to be included in your report by making a selection in the **Host(s)** drop-down box. A source host is the originator of a connection or a request. You can choose from a variety of options here, including:

    a. **All Hosts:** All hosts with activity on the specified packet analyzer or Netflow interface.

    b. **Specific IP Address:** You can enter an IP address here to run a report for a specific host.

    c. **Keyword Search:** Hosts matching a keyword or character pattern.

    d. **Host Filter:** If you are using Host Filters, they will be available for selection here.

5. Determine which destination hosts are going to be included in your report by making a selection in the **Host(s)** drop-down box. A destination host is the recipient of a connection or a request, and typically delivers a payload of some kind in response. You can choose from a variety of options here, including:

    a. **All Hosts:** All hosts with activity on the specified packet analyzer or Netflow interface.

    b. **Specific IP Address:** You can enter an IP address here to run a report for a specific host.

    c. **Keyword Search:** Hosts matching a keyword or character pattern.

    d. **Host Filter:** If you are using Host Filters, they will be available for selection here.

6. Determine what network traffic you're interested in. There are several available options here:

    a. **All Activity:** All network activity on the specified packet analyzer or Netflow interface.

    b. **Specific Protocol:** If you're looking for activity on a specific TCP or UDP port, choose this option, then enter the port number in the box that appears.

    c. **Traffic Filter:** If you are using Traffic Filters, they will be available for selection here.

7. Choose a maximum number of results to retrieve from the database in the **Limit Results** drop-down box.

8. Determine the order of results in the report by making a selection in the **Order Results By** drop-down box.

9. Click the **Next Step** button in the wizard dialog window.

10. Choose a reporting period from the available list. You can choose specific start and end times by selecting **Custom Range** from this list, which will then expose fields for start and end time.

11. If you want to run this report on a regular schedule, check the **Schedule this report to run automatically** box, and follow the instructions in *Saving and Scheduling Reports* on page 17.

12. Click the **Run Report Now** button.

Web Traffic

The Web Traffic Report allows you to query Netmon's HTTP Request Plugin, which keeps track of URLs which have been requested from your network.

To run a Web Traffic Report, open the Report Explorer by clicking the **Reports** link in the top toolbar.

1. Click the **New Report Builder** button in the Report Explorer. This will open the Report Builder Wizard. Choose *Web Traffic Report* from the **Report Type** selection box.
2. If you plan to use this report later, enter a label that will be used to identify it in the **Label** text box.
3. Determine which hosts are going to be included in your report by making a selection in the **Host(s)** drop-down box. You can choose from a variety of options here, including:
   a. **All Hosts:** All hosts with activity on the specified packet analyzer or Netflow interface.
   b. **Specific IP Address:** You can enter an IP address here to run a report for a specific host.
   c. **Host Filter:** If you are using Host Filters, they will be available for selection here.
4. If you'd like to narrow results to a particular string or keyword match, enter it in the **Keyword Filter** text box.
5. Choose a maximum number of results to retrieve from the database in the **Limit Results** drop-down box.
6. Click the **Next Step** button in the wizard dialog window.
7. Choose a reporting period from the available list. You can choose specific start and end times by selecting **Custom Range** from this list, which will then expose fields for start and end time.
8. If you want to run this report on a regular schedule, check the **Schedule this report to run automatically** box, and follow the instructions in *Saving and Scheduling Reports* on page 17.
9. Click the **Run Report Now** button.

Uptime / Downtime

This report provides a summary of the availability of each of your monitored services and disks, for the time interval specified.

To run an Up/Downtime Report, open the Report Explorer by clicking the **Reports** link in the top toolbar.

1. Click the **New Report Builder** button in the Report Explorer. This will open the Report Builder Wizard. Choose *Up/Downtime Report* from the **Report Type** selection box.
2. Click the **Next Step** button in the wizard dialog window.

3. Choose a reporting period from the available list. You can choose specific start and end times by selecting **Custom Range** from this list, which will then expose fields for start and end time.
4. If you want to run this report on a regular schedule, check the **Schedule this report to run automatically** box, and follow the instructions in *Saving and Scheduling Reports* on page 17.
5. Click the **Run Report Now** button.

Reporting Bandwidth

Bandwidth Activity

A Bandwidth Activity Report plots bandwidth utilization for SNMP device interfaces, such as those found on routers, firewalls, switches and servers, for a given time interval.

Important Note: You can only run a Bandwidth Activity Report if you have enabled historical logging for an interface.

To run a Bandwidth Activity Report, open the Report Explorer by clicking the **Reports** link in the top toolbar.

1. Click the **New Report Builder** button in the Report Explorer. This will open the Report Builder Wizard. Choose *Bandwidth Activity Report* from the **Report Type** selection box.
2. If you plan to use this report later, enter a label that will be used to identify it in the **Label** text box.
3. Make a selection in the **Choose a Device** drop-down box.
4. Once you've selected a device, you can choose a monitored interface via the **Choose an Interface** drop-down box.
5. Click the **Next Step** button in the wizard dialog window.
6. Choose a reporting period from the available list. You can choose specific start and end times by selecting **Custom Range** from this list, which will then expose fields for start and end time.
7. If you want to run this report on a regular schedule, check the **Schedule this report to run automatically** box, and follow the instructions in *Saving and Scheduling Reports* on page 17.
8. Click the **Run Report Now** button.

Bandwidth Consumption

The Bandwidth Consumption Report allows you to measure total network activity for particular subnet(s) or IP range(s). This report is useful to identify the largest bandwidth consumers (and providers) on a particular monitored network. Before you run a Bandwidth Consumption Report, familiarize yourself with the following report parameters:

Source Network(s): This is the subnet or IP range you wish to measure. Every IP address in the selected range will be accounted for in the resulting report (assuming there is network activity for that address).

Network(s) to Exclude: Any activity between the source network(s) and the network(s) specified here is excluded from the reporting result. This feature is useful, for example, if you want to measure Internet-bound bandwidth for a subnet, while filtering out any local activities (i.e. activity which is switched internally, insidethe network border). Or, you may wish to filter out traffic which is destined to a particular branch office.

Traffic Filter: You can use traffic filters to limit the report result to a specific protocol or group of protocols by making a selection here. The default selection includes all network activity, regardless of protocol.

Order Results By: You choose to produce a report for each individual IP address selected as Source Network(s), or you can produce a report which summarizes the data for each network subnet/range.

To run a Bandwidth Utilization Report, open the Report Explorer by clicking the **Reports** link in the top toolbar.

1. Click the **New Report Builder** button in the Report Explorer. This will open the Report Builder Wizard. Choose *Bandwidth Consumption Report* from the **Report Type** selection box.
2. Choose a **Source Interface** from the available drop-down box. You can select any of Netmon's built-in Local Packet Analyzers, or any NetFlow-enabled interface.
3. If you're excluding any networks from the report results, make a selection in the **Mutual Exclusion Network(s)** drop-down selector.
4. Determine what network traffic you're interested in. There are several available options here:
   a. **All Activity:** All network activity on the specified packet analyzer or Netflow interface.
   b. **Specific Protocol:** If you're looking for activity on a specific TCP or UDP port, choose this option, then enter the port number in the box that appears.
   c. **Traffic Filter:** If you are using Traffic Filters, they will be available for selection here.
5. Enter your selection in the **Order Results By** selection box.

6. By default, Netmon will convert bytes transferred into kilobytes, megabytes and gigabytes. If you plan to do mathematical work on the results of this report, it's recommended to check off the **Return all values in raw bytes** option.
7. Click the **Next Step** button in the wizard dialog window.
8. Choose a reporting period from the available list. You can choose specific start and end times by selecting **Custom Range** from this list, which will then expose fields for start and end time.
9. If you want to run this report on a regular schedule, check the **Schedule this report to run automatically** box, and follow the instructions in *Saving and Scheduling Reports* on page 17.
10. Click the **Run Report Now** button.

Reporting Disk Activity

The Disk Activity Report allows you to plot disk utilization over a specified time interval. To run a Disk Activity Report, open the Report Explorer by clicking the **Reports** link in the top toolbar.

1. Click the **New Report Builder** button in the Report Explorer. This will open the Report Builder Wizard. Choose *Disk Activity Report* from the **Report Type** selection box.
2. If you plan to use this report later, enter a label that will be used to identify it in the **Label** text box.
3. Choose a monitored disk from the available list in **Choose a Disk/Partition** drop-down box.
4. Click the **Next Step** button in the wizard dialog window.
5. Choose a reporting period from the available list. You can choose specific start and end times by selecting **Custom Range** from this list, which will then expose fields for start and end time.
6. If you want to run this report on a regular schedule, check the **Schedule this report to run automatically** box, and follow the instructions in *Saving and Scheduling Reports* on page 17.
7. Click the **Run Report Now** button.

Reporting on Email Usage

Email Traffic Inspection

The Email Traffic Inspection Report provides details on non-encrypted email traffic across a monitored network. For each email that matches the filter critera, a line showing the sender,

recipient and subject is displayed. Further details for individual messages can be revealed by clicking the link labelled "Show" on a particular line. This will reveal full details about the email message — client and server IP, attachments, message size and headers.

Important Note: In order to run Email Traffic Inspection Reports you must enable the IMAP, POP3 and SMTP plugins for your sniffing interface in **Settings** > **Services & Plugins**.

To run an Email Traffic Inspection Report, open the Report Explorer by clicking the **Reports** link in the top toolbar.

1. Click the **New Report Builder** button in the Report Explorer. This will open the Report Builder Wizard. Choose *Email Traffic Inspection Report* from the **Report Type** selection box.
2. If you plan to use this report later, enter a label that will be used to identify it in the **Label** text box.
3. Determine which hosts are going to be included in your report by making a selection in the **Host(s)** drop-down box. You can choose from a variety of options here, including:
   a. **All Hosts:** All hosts with activity on the specified packet analyzer or Netflow interface.
   b. **Specific IP Address:** You can enter an IP address here to run a report for a specific host.
   c. **Host Filter:** If you are using Host Filters, they will be available for selection here.
4. If you'd like to narrow results to a particular string or keyword match, enter it in the **Keyword Filter** text box.
5. Choose the email message criteria to apply the keyword filter to in the **Search Type** drop-down box. For example, if you wanted to search for all emails that have your selected keyword in the subject line sent to or from "info@mydomain.com", you'd choose **Subject** from this list.
6. Choose a maximum number of results to retrieve from the database in the **Limit Results** drop-down box.
7. Click the **Next Step** button in the wizard dialog window.
8. Choose a reporting period from the available list. You can choose specific start and end times by selecting **Custom Range** from this list, which will then expose fields for start and end time.
9. If you want to run this report on a regular schedule, check the **Schedule this report to run automatically** box, and follow the instructions in *Saving and Scheduling Reports* on page 17.
10. Click the **Run Report Now** button.

Email Traffic Statistics

The Email Traffic Statistics Report provides a high-level summary of the non-encrypted email traffic across a monitored network. Broken down by the type of report output you select, you will see a summary of the e-mail messages sent and received, their acerage and total size for the selected report period.

In order to run an Email Traffic Statistic Reports you must enable the IMAP, POP3 and SMTP plugins for your sniffing interface in **Settings** > **Services & Plugins**.

To run an Email Traffic Statistics Report, open the Report Explorer by clicking the **Reports** link in the top toolbar.

1. Click the **New Report Builder** button in the Report Explorer. This will open the Report Builder Wizard. Choose *Email Traffic Statistics Report* from the **Report Type** selection box.
2. If you plan to use this report later, enter a label that will be used to identify it in the **Label** text box.
3. Make a selection in the **Report Type** drop-down box. Available options are:
   a. Address: A summary of emails sent and received by email address
   b. Client: A summary of emails sent and received by client IP
   c. Domain: A summary of emails sent and received by email domain
   d. Server: Summary of emails sent and received by server IP
4. If you'd like to narrow results to a particular string or keyword match, enter it in the **Keyword Filter** text box.
5. Click the **Next Step** button in the wizard dialog window.
6. Choose a reporting period from the available list. You can choose specific start and end times by selecting **Custom Range** from this list, which will then expose fields for start and end time.
7. If you want to run this report on a regular schedule, check the **Schedule this report to run automatically** box, and follow the instructions in *Saving and Scheduling Reports* on page 17.
8. Click the **Run Report Now** button.

Latency

The Latency Report analyzes all of the TCP Service Trackers, PING Service Trackers and Disks which have been configured in the Netmon Trackers console, and provides an average latency (in milliseconds) for each service, for the time interval specified.

Important Note: In order to run a Latency Report for a specific device/service, you first need to enable full historical logging for that device/service. By default, Netmon does not keep historical data for devices or services, for performance reasons.

To run a Latency Report, open the Report Explorer by clicking the **Reports** link in the top toolbar.

1. Click the **New Report Builder** button in the Report Explorer. This will open the Report Builder Wizard. Choose *Latency Report* from the **Report Type** selection box.
2. If you plan to use this report later, enter a label that will be used to identify it in the **Label** text box.
3. Select a Ping or TCP Service Tracker from the available list.
4. Click the **Next Step** button in the wizard dialog window.
5. Choose a reporting period from the available list. You can choose specific start and end times by selecting **Custom Range** from this list, which will then expose fields for start and end time.
6. If you want to run this report on a regular schedule, check the **Schedule this report to run automatically** box, and follow the instructions in *Saving and Scheduling Reports* on page 17.
7. Click the **Run Report Now** button.

OID Tracker

An OID Tracker Report allows you to examine historical values for any SNMP management object (OID) through Netmon's OID Tracker Service. Though this is a very simple report, it is extremely flexible and useful for a variety of tasks.

Important Note: In order to run a report for any OID Tracker, you must first ensure that the Enable Logging selection has been checked in the OID Tracker Manager.

To run an OID Tracker Report, open the Report Explorer by clicking the **Reports** link in the top toolbar.

1. Click the **New Report Builder** button in the Report Explorer. This will open the Report Builder Wizard. Choose *OID Tracker Report* from the **Report Type** selection box.
2. If you plan to use this report later, enter a label that will be used to identify it in the **Label** text box.
3. Select a tracked Object Identifier (OID) from the available list.
4. Click the **Next Step** button in the wizard dialog window.

5. Choose a reporting period from the available list. You can choose specific start and end times by selecting **Custom Range** from this list, which will then expose fields for start and end time.
6. If you want to run this report on a regular schedule, check the **Schedule this report to run automatically** box, and follow the instructions in *Saving and Scheduling Reports* on page 17.
7. Click the **Run Report Now** button.

URL Tracker

A URL Tracker Report allows you to evaluate the performance of websites and web applications. You can monitor the performance (latency) of URL request delivery, as well as accuracy (expected results returned) through the same report.

Important Note: In order to run a report for any URL Tracker, you must first ensure that the Enable Logging selection has been checked in the URL Tracker Manager.

To run a URL Tracker Report, open the Report Explorer by clicking the **Reports** link in the top toolbar.

1. Click the **New Report Builder** button in the Report Explorer. This will open the Report Builder Wizard. Choose *URL Tracker Report* from the **Report Type** selection box.
2. If you plan to use this report later, enter a label that will be used to identify it in the **Label** text box.
3. Select a URL Tracker from the available list.
4. Click the **Next Step** button in the wizard dialog window.
5. Choose a reporting period from the available list. You can choose specific start and end times by selecting **Custom Range** from this list, which will then expose fields for start and end time.
6. If you want to run this report on a regular schedule, check the **Schedule this report to run automatically** box, and follow the instructions in *Saving and Scheduling Reports* on page 17.
7. Click the **Run Report Now** button.

Port Scan

A Port Scan Report summarized the results of Netmon's background port scanning service, which probes hosts on your various network range(s) for open ports.

Netmon scans each host on your network range(s) every 2 hours, and records the results of its scan to the database. A port scan report shows all scanned hosts, along with the open ports for each host. Where possible, Netmon will attempt to identify the protocol using Port Labels.

To run a Port Scan Report, open the Report Explorer by clicking the **Reports** link in the top toolbar, then taking the following steps:

1. Click the **Port Scan Report** link in the **Permanent** Reports panel in the Report Explorer.
2. The report will appear in a few moments. There are no input parameters for this report.

Alert History

The Alert History Report displays a list of all email and pager alerts which have been generated across the entire Netmon system for the specified period of time. To run an Alert History Report, open the Report Explorer by clicking the **Reports** link in the top toolbar.

1. Click the **New Report Builder** button in the Report Explorer. This will open the Report Builder Wizard. Choose *Alert History Report* from the **Report Type** selection box.
2. If you plan to use this report later, enter a label that will be used to identify it in the **Label** text box.
3. Click the **Next Step** button in the wizard dialog window.
4. Choose a reporting period from the available list. You can choose specific start and end times by selecting **Custom Range** from this list, which will then expose fields for start and end time.
5. If you want to run this report on a regular schedule, check the **Schedule this report to run automatically** box, and follow the instructions in *Saving and Scheduling Reports* on page 17.
6. Click the **Run Report Now** button.

Netmon Login Activity

The Netmon Login Report displays a list of all Netmon login activity for the specified period of time. To run a Login Activity Report, open the Report Explorer by clicking the **Reports** link in the top toolbar.

1. Click the **New Report Builder** button in the Report Explorer. This will open the Report Builder Wizard. Choose *Netmon Login Report* from the **Report Type** selection box.
2. If you plan to use this report later, enter a label that will be used to identify it in the **Label** text box.
3. Click the **Next Step** button in the wizard dialog window.

4. Choose a reporting period from the available list. You can choose specific start and end times by selecting **Custom Range** from this list, which will then expose fields for start and end time.

5. If you want to run this report on a regular schedule, check the **Schedule this report to run automatically** box, and follow the instructions in *Saving and Scheduling Reports* on page 17.

6. Click the **Run Report Now** button.

Saving and Scheduling Reports

Saving a Report for Later Use

Most reports give you the option to specify a **Label** when they are being created in Report Builder. When this option is present, and a label is specified, Netmon will save your report parameters using the label you supply.

Working with Saved Reports

Saved reports appear in the **Saved Report Templates** section of the Report Explorer. You can re-run a saved report by clicking on it, which then brings up a Report Builder window with the pre-selected options you made previously.

You can also customize a saved report before you run it again, by changing the values in the available fields and drop-down menus.

Deleting a Saved Report

Saved reports can be removed by clicking the button next to the associated report in the **Saved Report Templates** section.

Generating Reports Automatically on a Schedule

Many reports can be configured to run automatically on a pre-defined recurring schedule, and be delivered by email. To accomplish this, take the following steps:

1. Check the **Schedule this report to run automatically** box in the **Report Parameters** stage of the Report Builder. This will expose additional fields which allow you to configure the schedule and email recipients.
2. Choose a **Scheduled Start Time**. This should be in a 4-digit, 24-hour format. (Examples: 02:30 or 16:00).
3. Choose a **Frequency**. Depending on the choice you make here, an **Every** selection may appear (i.e. if you choose "Weekly", to allow you to choose a day of the week).
4. Finally, make a selection in the **Notify on Completion** drop-down menu. This can be any Netmon user.