Syslog Analysis

Syslog Chart

EventLog Chart shows distribution of Syslog messages (logs) by severity:

- 1. Logs per bar (y-axis)
- 2. Time axis (x-axis)
- 3. Bar width
- 4. Zoom out



Chart shows number of logs in certain time chunks (1 minute, 1 day, 1 hour). Width of the chart bars and number of bars depends on the Time Window selected. See table below:

Time Window	Bar Width	Number of Bars
Last hour	30 seconds	120
Last 6 hours	5 minutes	72
Last 12 hours	5 minutes	144
Last day	15 minutes	96
Last week	1 hour	168
Last month	6 hours	120

Chart has two axis: numerical y-axis and time x-axis. Numerical axis shows the number of logs per bar. Time shown on the x-axis of the chart is the same time as set in the Time Window. Next to the Syslog Chart is the Severity Table in which you can select if Syslog messages of the certain severity will be displayed on the chart or not. Colors on the chart correspond with the colors of the Syslog Severity in the Severity Table.

On the EventLog Chart above you can see that one bar on the chart represents logs during 30 seconds (bar = 30 seconds).

Severity Table

Severity Table shows log distribution by severity, for the logs of selected severity that occurred in the selected Time Window. On screenshot to the right currently selected severity levels are 0, 1, 2 and 3. This means that Syslog chart and tables will show only logs with this severity levels. By clicking on the corresponding severity in the Severity Table you can switch on/off logs of that severity. Switched off severity is shown with a gray background and logs with that severity are not shown on the carts and graphs.

Severity	Logs	Distribution
0-Emergency	0	0.0%
1-Alert	969	1.3%
2-Critical	39	0.1 %
3-Error	71,679	98.6%
4-Warning	0	0.0%
5-Notice	0	0.0%
6-Informational	0	0.0%
7-Debug	0	0.0%
Total	72,677	

On this page:

- Syslog Chart
- •
- Severity Table Exporter Table and Chart •
- Syslog Table Syslog Filtering
- Additional Options

Exporter Table and Chart

Exporter	Logs	Distribution
.4.65	3,294	
.6.202	2,512	
.6.201	2,163	
.5.166	1,255	
.4.63	960	
.4.75	720	
.2.2	600	
Total	13,344	

Exporter Table shows log distribution by exporter, for the logs of selected severity that occurred in the selected Time Window. Top 7 exporters have a color assigned, while other exporters are grey and under Others on the pie chart. To see other exporters, scroll down the exporter list. Clicking on an exporter will show only logs for that exporter on the charts and table. By clicking on it again, you can switch back to see logs for all exporters.

Syslog Table

EventLog Table shows messages with selected severity (in Severity Table) that were received during time set in the Time Window. For each message Date, Exporter, Severity, Facility and Message content is displayed. Severity levels are shown with the corresponding color, as in the chart and Severity Table. Syslog Table can be filtered by Exporter, Severity, Facility and Message content. Note that the filters can be activated by selecting items in the Severity and Exporter Tables, as described above. To clear all filters, click the Clear button above the Syslog chart.

Date	Exporter .7.108. 4.75	Severity 0.1,2,3,4,5	Facility	Message
Jul 29 2013, 10:10:19.205	4.75	5 - Notice	10 - Security/Authorization	stunnet. LOG8(7682:3072637840): Connection closed: 11468 bytes sent to 555, 138 bytes sent to socket
Jul 29 2013, 18:18:17.494	7.106	4 - Warning	23 - Local Use 7	1373913. Jul 29 16:16:16:16:350FF-6-ERRICV: Received invalid packet: mismatch area ID, from backbone area must be virtual-linic but not found from
JJ 29 2013, 18:18:14:248	4.76	6 - Notice	10 - Security/Authorization	stunnet. LOG6(7582.3072637840): Post check: verification level is low; skipping check
Jul 29 2013, 18:16:14:244	4.75	5 - Notice	10 - Security/Authorization	stunnet. LOG6(7682:3072637840); xapi connected from 4.82:60074
Jul 29 2013, 10:16:07.465	7.106	4 - Warning	23 - Local Use 7	1373912. Jul 29 16 16:00: %JSPF-4-ERRR/LV: Received invalid packet: mismatch area ID, from backdone area must be virtual-link but not found from
3.4 29 2013, 10 15 57 495	.7.108	4 - Warning	23 - Local Use 7	1378611: Jul 29 16 15 56: WOSPF-& ERRROY: Received invalid packet: mismatch area ID, from backdone area must be virtual-link but not found from
Jul 29 2013, 10:15:47.472	.7.105	4 - Warning	23 - Local Use 7	1371612 Jul 29 16 16 46: StOSPF-4-ERRIFCY: Received invalid packet: mismatch area ID, from backbone area must be virtual-link but not found from
Jul 29 2013, 10:15:44.231	4.75	3 - Error	10 - Security/Authorization	stunnet LOG3(7682:3072637540): 55L_read: Connection reset by peer (154)
Jul 29 2013, 10:19:44.231	4.75	5 - Notice	10 - Security/Vuthorization	stunnet LOG6(7682:3072637840): Connection reset: 11425 bytes sent to 555, 138 bytes sent to socket
Page 1	4.75	5 - Notice	51, Secular/advantation	example 1 0/06/7689-9/2298/28a/tr Rost relative variabilities laws in inser skinning relative

Syslog Filtering

You can filter out unwanted logs based on log's severity, exporter, facility, date and time, and message content.

NetVizura EventLog has three main types of Syslog filters:

- quick filters: severity and exporters
- table filters
- time filters (Time Window)



Quick filters are activated/deactivated by clicking on the corresponding severity in the Severity Table, or clicking on the corresponding exporter in the Exporter table. Inactive severity/exporters are marked with gray color, while active severity/exporters are colored. Logs from inactive exporters and logs with inactive severity levels are not shown in the charts and tables, and are not counted in the on-screen statistics.

Activating/deactivating severity or exporter filters will:

- update Syslog Table filters for the corresponding exporter or severity level
- · refresh charts and Syslog Table,
- refresh statistics in the Exporter Table and Severity Table

(i) Filters and data in Syslog Table, Exporter Table, Severity table always match each other.

Figure 10: Using filters in Syslog Table shows Syslog Table and Severity Table, and you can see that the Severity filter in the table matches the active (colored) severity levels in the Severity Table.

Table filters are used to filter Syslog messages by log's severity, exporter, facility and message text body. To activate or change a filter simple type the value in the corresponding filter text field and press Enter. This will update the data on all chats and tables.

1



To filter out the logs based on the time and date, change the Time Window value by clicking on it and (1) choosing a value from the drop menu or (2) selecting from and to dates in the calendar. Updating the Time Window will update the data on all chats and tables.

Additional Options

- Refresh Data manually refresh data on charts and tables
 Clear filters clear all filters
- 3. Show Exporter Names show names of exporters (routers) instead of their IP address. These can be DNS names, or the ones you defined in the Settings/Devices page.

