SolarWinds

Understanding SolarWinds Charts and Graphs

Technical Reference
Copyright © 1995-2015 SolarWinds Worldwide, LLC. All rights reserved worldwide.

No part of this document may be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the written consent of SolarWinds. All right, title, and interest in and to the software and documentation are and shall remain the exclusive property of SolarWinds and its respective licensors.

SOLARWINDS DISCLAIMS ALL WARRANTIES, CONDITIONS OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON SOFTWARE AND DOCUMENTATION FURNISHED HEREUNDER INCLUDING WITHOUT LIMITATION THE WARRANTIES OF DESIGN, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT. IN NO EVENT SHALL SOLARWINDS, ITS SUPPLIERS, NOR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY EVEN IF SOLARWINDS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

The SOLARWINDS and SOLARWINDS & Design marks are the exclusive property of SolarWinds Worldwide, LLC and its affiliates, are registered with the U.S. Patent and Trademark Office, and may be registered or pending registration in other countries. All other SolarWinds trademarks, service marks, and logos may be common law marks, registered or pending registration in the United States or in other countries. All other trademarks mentioned herein are used for identification purposes only and may be or are trademarks or registered trademarks of their respective companies.

Understanding SolarWinds Charts and Graphs, Version 18, 2/24/2015
# Table of Contents

- **Understanding Orion Platform Charts and Graphs** ................................................................. 4
- **Charts and Graphs Definitions** .................................................................................................. 5
- **IT Management Data Types** ...................................................................................................... 6
  - Raw Vs. Cooked Data .................................................................................................................. 7
  - Absolute vs. Relative Data ......................................................................................................... 8
  - Data Sources ............................................................................................................................. 9
  - Data Collectors .......................................................................................................................... 10
    - Data Perspective ..................................................................................................................... 11
- **Interpreting Orion Data Charts and Graphs** ............................................................................ 12
  - Gauges ....................................................................................................................................... 12
  - Bar and Line Charts .................................................................................................................. 12
- **Comparing Data from Different Resources** ............................................................................ 15
  - Disparate Data Sources .............................................................................................................. 15
  - Graphing Differences Between Views .................................................................................... 15
  - Graphing Differences Within a Single View .............................................................................. 16
Understanding Orion Platform Charts and Graphs

SolarWinds products offer a rich variety of information on the health and performance of your IT systems. Some charts are very data rich and may be more difficult to understand what is represented.

This section focuses on more complex graphs available in the SolarWinds Orion Platform and includes a brief overview of some of the basics of IT management data, data sources, and other general information for understanding that data.
Charts and Graphs Definitions

Polled Data
Data retrieved from a device by polling the device, typically, this is automated and at regular intervals.

Ad-hoc Data
Data received without requiring a request. This is commonly accomplished by leaving a TCP or UDP port open and reserved for receiving data.

Chart
A graphical representation of datasets. Types of charts we use include pie charts, bar charts, area charts, and two dimensional x-y graphs.

Graph
For our purposes, a graph is a two dimensional data display comparing two data sets: a variable data set on the y-axis and an incremental dataset on the x-axis. Example: an interface utilization line graph mapping variable interface utilization on the y-axis against set time periods on the x-axis.

Absolute Data
Data that is independent of other data. Example: value returned by polling an interface out octet counter.

Relative Data
Data derived by comparing a data point to one or more other data points. Example: percent interface utilization represents the interface counter data relative to the maximum interface speed.

View
A web page displayed within a SolarWinds product.

Resource
A single element of a view, for example, a pie chart.
IT Management Data Types

Data is passed from managed devices to a Network Management System (NMS), such as NPM, as a stream of bits that are assembled into frames, packets and Protocol Data Units (PDUs). The exact method of decoding the bit streams to IT management data is beyond the scope of this paper. What is important here is to understand some of the properties of the data types. This will help you understand how the data can be used and some inherent limitations.

Below is a list of the most common data types used in network management.

<table>
<thead>
<tr>
<th>Data Type</th>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Counter</td>
<td>A 32 or 64-bit positive number with the maximum value depending on the bit size. (2^{32}-1 or 2^{64}-1). Counters increase in size until they reach their bit limit when they begin counting again at zero plus the remainder of the last counter update. This is known as counter rollover. Counters are used to count bits transmitted or received as well as other similar data. Example: an automobile’s odometer.</td>
</tr>
<tr>
<td>Gauge</td>
<td>A 32-bit number which may increase or decrease in value but not exceed 2^{32}-1. Gauges are used for data that varies upward and downward often, such as CPU load, but can also be used for static information like interface speed. Example: an automobile’s tachometer.</td>
</tr>
<tr>
<td>Integer</td>
<td>A 32-bit number typically used to indicate an object state, such as 1=up, 2=down, 3=unknown.</td>
</tr>
<tr>
<td>IP Address</td>
<td>32-bit dotted decimal for IPv4 or 128-bit hexadecimal for IPv6 indicating the IP address of a node.</td>
</tr>
<tr>
<td>Network Address</td>
<td>32-bit dotted decimal for IPv4 or 128-bit hexadecimal for IPv6 indicating a network or subnet.</td>
</tr>
</tbody>
</table>
Data Type | Properties
---|---
Object Identifier | Dotted decimal string indicating a position within a MIB.
Octet Strings | Byte strings used to indicate text or layer 2 addresses.
Time ticks | A 32-bit number used to measure time in 1/100ths of a second.

**Raw Vs. Cooked Data**

Some data is displayed as raw, unaltered data. A CPU gauge is a good example, displaying in the same value as was collected. For other data types, displaying raw data would be of little use.

For example, the number of bytes received on an interface is raw, counter data. In a polling cycle the NMS might receive a number such as 456723. All this number means is that since the interface counter was reset, or possibly rolled over, 456723 bytes of data passed through the interface. Displaying this data as– is using a gauge would be meaningless. This data must be processed before it can be shown as useful information. The result is sometimes known as cooked data. It is common to use both raw and cooked data in IT management.

The below table shows how polled interface utilization data is cooked into useful information.

<table>
<thead>
<tr>
<th>Poll Time (Seconds)</th>
<th>Raw Polled Data (Agent Counter Octets) Raw, Absolute</th>
<th>Data Delta (This poll minus last) Cooked, Absolute</th>
<th>x8 (Bytes to bits) Cooked, Absolute</th>
<th>Bits per second Cooked, Relative</th>
<th>Percent Utilization (1.544 Mbps) Cooked, Relative</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>2156</td>
<td>Null</td>
<td>Null</td>
<td>Null</td>
<td>Null</td>
</tr>
</tbody>
</table>
As shown in the table, raw data goes through four operations before it is readily usable information, the percent utilization of the T-1 interface.

**Absolute vs. Relative Data**

The above table contains two data types that are commonly confused with one another. The first four columns contain absolute data. In column three, the numbers are a result of subtracting a counter number from the latest counter number. The result is still an absolute count. The multiplication by 8 to convert units does not change the fact the data is just a count, and still absolute. The next calculation to bits per second creates a rate, which is relative data. Once data is relative, it remains relative unless the operation that converted it is reversed. In the last column, Percent Utilization, the data is relative.
Data Sources

Typically, the Network Management System (NMS) collects data either by actively polling devices for data or by passively listening for data on a reserved IP port. Simple Network Management Protocol (SNMP) polling and Windows™ Management Instrumentation (WMI) are common examples of polled data. SNMP trap and NetFlow are examples of passive data collection. SNMP polled data is obtained by the SNMP manager polling for specific data from an SNMP agent MIB on a managed device.

Both the NMS and managed device keep a copy of the Management Information Base (MIB). The MIB is similar to a file and folder structure for data stored on a hard drive. The MIB maps out where specific information is stored. MIBs consist of Object Identifiers (OIDs) that store data points. If more than one end object exists in an OID, the OID is appended with an index number. This structure is shown in the following example.

```
1.3.6.1.2.1.1          .3          .0
(RFC1213-MIB, mib-2)  object       instance
```

The SNMP agent on the managed device populates the agent’s MIB OIDs with the latest data in 10 seconds to one minute intervals, depending on the device and vendor’s SNMP implementation. In this case the data source is the SNMP MIB on the device’s SNMP agent. Other IT management data sources include flow exporters, such as NetFlow, WMI polling, API query responses, log exporters, SNMP traps, as well as telnet and SSH.

The following illustration shows IT management data sources, data types, and the data collector and how each of these communicates.
Data Collectors

Not all IT management collectors are Network Management Systems (NMS). Some are agents designed to perform tests or collect data and report the results back to the NMS. These agents provide two services to the NMS: they allow distributed data collection and they offload some of the collection and aggregation work for the NMS.
Data Perspective

Some data NMSs collect is perspective dependent and some is perspective independent. For example, consider an ICMP ping request sent from the NMS to a managed device. The information we retrieve at the NMS tells us the round trip time between the NMS and a managed device. If that managed device were to move to a different location across a lengthy WAN connection, the path to the device would change and so would the ping response time. Now consider a server sending log information to the NMS. An important part of log information is the time the logged event occurred, which is recorded in the timestamp field of the log message. The exact time the log server received the message is not critical. Moving a log server or log exporter will have no effect on the log data received.
Interpreting Orion Data Charts and Graphs

This section examines the data displays from various SolarWinds Orion Platform products and discuss what is represented in the data. We look at the data representations used and note what is common between products.

Gauges

One important property of gauge data is that each new data point can be larger or smaller than the previous data point. Gauge data is often shown on a gauge as raw, or unaltered, data. Some people assume that gauge displays are real-time, but SolarWinds Orion gauges are not real-time. They reflect the data from the last polling cycle.

Bar and Line Charts

Bar charts and line charts such as the in/Max/Average graphs are used extensively in several SolarWinds Orion products. These graphs show a large amount of information in a single resource. Consider the following interface graph as an example.
This graph shows all the data available since the first of the month to the end of the month. Each bar represents a data interval. The interval used for this graph is one day. The chart shows the light green bars to indicate the maximum data rate seen during each sample interval. This gives a data range for each interval, which means that each bar represents multiple polled data points.

The ranges in each bar are averaged and shown by the blue line running through them. The average is calculated by averaging all the data points in each sample period.

The trend line is calculated using a method called a least squares fit. The 95th percentile line indicates the level at which 95% of all data on the chart is at or below.

Now let’s examine what can happen when you alter the dataset’s time scope and interval periods. Click the Edit button from the top right corner of the graph to change the time period for the data and the sample interval. You may also find the link to the chart editor in the View Options drop-down menu.
As of NPM 10.2, the graphing engine only connects dots when it can verify the data points are from separate polls and only creates range bars when there is more than one polled data point within a sample interval. The range bars at the right side of the graph are a result of using the Poll Now button several times in the Node Details page. This created “rapid polling”, giving the graphing engine the ability to have multiple polled data points in the last graphing intervals. To better understand what causes this type of graphing issue, consider the following timeline.

This is an arbitrary example of a graphing and polling conflict to help explain an issue that causes scattered graph data and does not reflect the exact situation shown in the earlier Orion graph. The sample intervals are shown as red lines, starting out at time = 0 and continuing every 5-minutes for the 1- hour period. Each sample interval represents a request from the graphing engine for new data from the Orion database at a particular time. The SNMP polling period is set to 9 minutes. The first SNMP polled data the graphing engine considers is whatever is in the Orion database at time = 0. The first SNMP polling happens at time = 2 and then every 9 minutes thereafter. Any time there is more than one graphing interval within a single polling period there is no new data and so the reply to the graphing engine’s request is null. This creates gaps in the data and prevents connecting the minimum and maximum, data points with a line.
Comparing Data from Different Resources

People often compare from different views, such as an NPM interface traffic graph with an NTA top applications stacked area chart. While this can be a valid method for determining more information about a particular resource, you need to be aware of some pitfalls.

Disparate Data Sources

When comparing resources you must consider the sources of the data displayed. You may compare an interface utilization graph from NPM with a NetFlow resource for the same interface in the same time period. Although we might assume at first that these should be the same, they are often different.

Consider that the NPM data source is all traffic as recorded on the device’s SNMP agent and polled by NPM every 9 minutes, but, the NetFlow traffic is only IP traffic as recorded by the device’s NetFlow exporter. This data is exported to the NTA module every minute. There are two opportunities for the data to differ here:

1. The data counted by an SNMP interface counter has different criteria than the data counted by a NetFlow collector
2. The data collection time periods vary by a factor of 9.

While many times these two types of data will be roughly similar, there is opportunity for them to differ significantly. You should make sure that the two graphs you are comparing are using the same data period, intervals and that the Y-axis is set to the same units for both graphs.

Graphing Differences Between Views

Another issue that can make the data seem invalid is comparing resources with different criteria. Again if one compares an NPM interface utilization with a Top 5 applications graph in NTA the two will not align. The issue here is that the NPM interface graph is showing the total amount of data to cross that interface and the NTA graph is showing only traffic for the top 5 IP applications.
Graphing Differences Within a Single View

The most common place for finding graphing differences in a single view is comparing an NTA Top X Endpoints resource with any other NTA Top X resource for the same period. Typically, the top endpoints resource shows twice the traffic of the other resource. This is because the top endpoints are both top receivers and top talkers. All of the data associated with an endpoint is summed to calculate the total data for an endpoint. Knowing that the data is counted both to and from the endpoint, we would expect the data to be double.