Traverse Network Flow Integration

Advanced root-cause analysis solution

Dashboard-to-flow Drill-down

Traverse supports integration with network flow and packet level data collection tools to provide seamless drill-down from service, system and device level monitoring views to flow information to support troubleshooting and analysis. The flow data provides details on the network traffic between hosts, enabling quick identification of impacted services, trouble areas, and problem sources.

Network routers and switches can be configured to export conversation records for traffic passing through them to a 'flow collector.' These records consist of the source and destination IP address information, as well as the source and destination ports. Based on this information, it is possible to find out the total traffic between two hosts and the type of application that is generating the traffic.

When service performance problems are detected, operations personnel can quickly analyze the flow data to identify abnormal traffic volume and traffic type that might be causing the performance degradation. Supported protocols that provide the required flow data are NetFlow, sFlow, cflowd, and J-Flow.

Top-N Destinations and Sources

From the various devices status views, a user can drill down and invoke the network flow view to identify top-N destinations and sources of traffic.
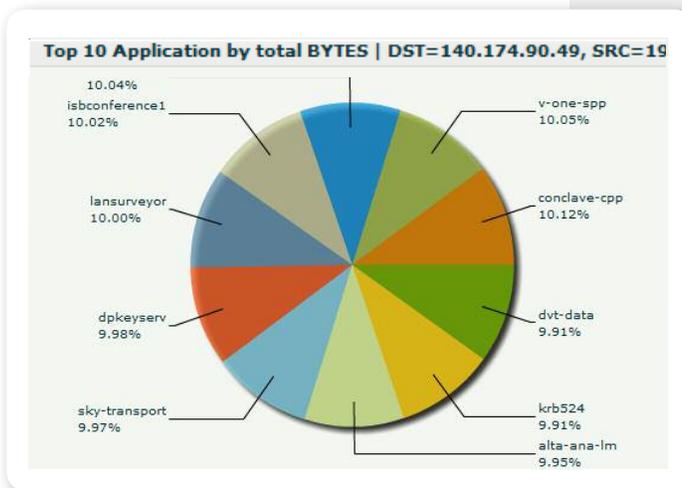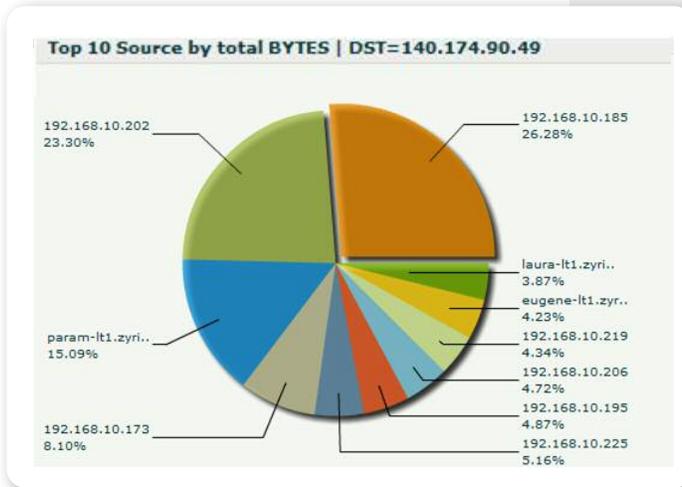
Top 10 Destination by total BYTES

IP Address	bytes
75.52.125.78	3532634071
140.174.90.49 (zyrion.com)	142540771
98.210.99.98 (c-98-210-99-98.hsd1.ca.comcast.net)	123293653
76.220.36.65 (76-220-36-65.lightspeed.sntcca.sbcglobal.net)	89647330
173.243.50.185 (173-243-50-185.ip.mozyops.net)	35444211
69.253.168.219 (c-69-253-168-219.hsd1.nj.comcast.net)	34165692
69.107.65.121 (adsl-69-107-65-121.dsl.pltn13.pacbell.net)	24623212
173.194.25.13	18804712
216.115.212.30 (216-115-212-30.expertcity.com)	6754455
216.115.214.54 (216-115-214-54.expertcity.com)	5994075

The user the can specify the time period for which flow analysis is to be performed, the metric of interest (e.g. bytes, packets, flows) and the number of sources or destinations to include in the analysis. The flow data can be displayed as a matrix, column chart or pie chart.

In addition, the specific applications for a given source can be viewed, as well as the history of the traffic generated by a particular application.

Viewing Network-wide Flow Analysis Data

In the most common mode of use, data is displayed for a single source or destination device. But users can reset the views in the network flow analysis console to have the scope of data be expanded to the entire network. This provides a network-wide view of the top-N sources, destinations, or applications. Users can then click through to get detailed device data as described earlier.

Top 10 Source by total BYTES | DST=140.174.90.49

- 192.168.10.202 — 23.30%
- 192.168.10.185 — 26.28%
- laura-lt1.zyri.. — 3.87%
- eugene-lt1.zyr.. — 4.23%
- 192.168.10.219 — 4.34%
- 192.168.10.206 — 4.72%
- 192.168.10.195 — 4.87%
- 192.168.10.225 — 5.16%
- 192.168.10.173 — 8.10%
- param-lt1.zyri.. — 15.09%

Top 10 Application by total BYTES | DST=140.174.90.49, SRC=19

- 10.04%
- isbconference1 — 10.02%
- v-one-spp — 10.05%
- lansurveyor — 10.00%
- conclave-cpp — 10.12%
- dpkeyserv — 9.98%
- dvt-data — 9.91%
- sky-transport — 9.97%
- krb524 — 9.91%
- alta-ana-lm — 9.95%

Solution Architecture

To enable network flow analysis integration in Traverse, the following components need to be configured:

- Traverse Data Collection Engines
- Traverse Flow Analysis Engine (flowqueryd)
- NetFlow Collector (3rd party or Traverse pre-integrated collector)
- Router or switch that exports flow records

The network flow analysis integration in Traverse is extremely flexible and can be easily extended to integrate with many different network flow data collectors. This is done through customizing the flowquery daemon to query flow data from different collector components. The data collection queries the network flow data from the flowquery daemon, which fetches the data from the flow collector and returns it to the data collection engine. Traverse then processes and displays this data.

Visual Correlation Capabilities

In addition to providing network flow to aid problem and root-cause analysis at a detailed level, Traverse provides the ability to view a correlation histogram to identify sources of service degradation at a higher-level. This enables isolating problem areas to drill deeper, if desired, initiate flow analysis.
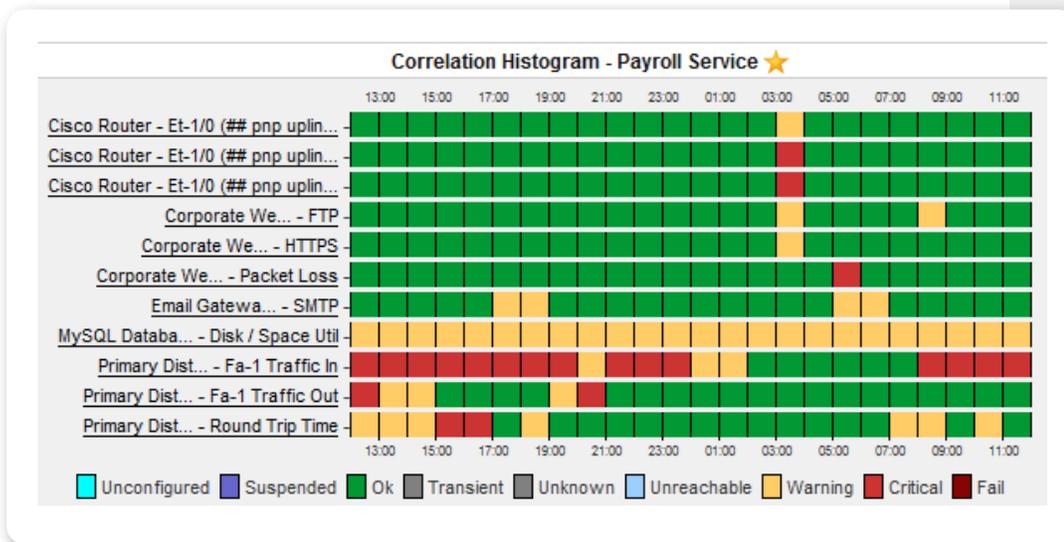
ABOUT TRAVERSE

Traverse is a next-generation monitoring solution from Kaseya, a global software solution provider with over 10,000 customers globally. Traverse's patented technology offers a distributed, scalable monitoring platform with rich data analytics and unified cloud & network management. Traverse allows enterprises and Managed Service Providers to optimize their IT operations with faster mean time to resolution for slow or failed IT services within their infrastructure. Customers leveraging Traverse include the Fortune 100 as well as small-sized and medium-sized businesses worldwide. For more information, visit **www.traverse-monitoring.com**