Performance Log Appliance (PLA)

The SevOne Performance Log Appliance (PLA) is the only solution on the market that automatically correlates real-time network and IT performance metrics with log events in a single integrated solution. Whether you need to analyze web application traffic, troubleshoot a rogue process behind rising CPU usage, or investigate a surge in firewall connections, the SevOne PLA provides you with greater visibility of root cause while eliminating the time-consuming practice of manually searching logs and self-correlating data points.

"SevOne will be the first to truly integrate log data into an enterprise-class, carrier-grade performance management system."

-Jim Frey
Vice President of Research
Enterprise Management Associates

Key Benefits

- Automatically correlate real-time performance metrics with log data
- Improve visibility of root cause of performance degradation
- Decrease time to troubleshoot and repair known issues
- Receive proactive alerts of customer and end user behavioral trends
- Understand the impact of configuration changes on application performance

Why Log Data?

The applications, systems, and infrastructure that run your business generate massive volumes of unstructured log data. This log data contains a definitive record of all user transactions, customer behavior, machine behavior, security threats, fraudulent activity, and more. Unstructured data presents a challenge to properly categorize and to mine for intelligence. However, when unstructured log data can be collected and organized by a performance-based log analytics platform like SevOne, log data provides an incredibly valuable resource for understanding the behavior of your users, customers, applications, and network and IT infrastructure.

While traditional performance data such as SNMP and IP SLA metrics tells you when spikes, anomalies, and outages occur, logs provide additional insight by revealing who or what caused the issue. Consider router monitoring:

Router Performance Metrics:

- Interface In/Out Stats
- CPU & Memory Utilization
- UP/Down
- ACL activity

Router Log Analytics:

- NAT tables
- Policy Utilization
- User Login
- Configuration Changes
- Error codes
- Operational Message Codes

Combining performance metrics with log analytics allows you to answer questions such as, "Did my recent configuration change alter CPU or memory utilization?" and, "Why is our Internet link mostly denied traffic?"

Beyond Log Search

SevOne improves operational intelligence by alerting users to unique and unusual data patterns, rather than expecting you to manually search for them.

Traditional Log Search products provide users a tool to search large volumes of machine generated data in order to troubleshoot known issues. However, there are problems with this approach:

- You need to know a performance issue exists
- You need to know what to look for in the logs
- You may need to learn a complex query language in order to maximize use of the tool
- You need to manually correlate infrastructure issues with service availability and response time problems on your own

SevOne advances the field of Log Analytics by moving beyond traditional Log Search. With little or no input or configuration on your behalf, the SevOne PLA extracts log data in real-time and correlates it to performance events, making search an unnecessary step in your process. It increases your application performance visibility by providing single-click drill-down from related data such as SNMP metrics to NetFlow records to SysLog files.

While other vendor products expect you to find the needle in the haystack, the SevOne PLA removes the hay and shows you what's left that's important.

Use Cases for Log Performance

The following examples illustrate the value of Performance Log Analytics with the SevOne PLA:

- **Why can't I make a VoIP call from the conference room?**
  Using SevOne, you confirm there is VoIP traffic in the conference room, but users complain they are unable to make calls. Drilling into the associated logs, you reveal that the firewall access list is set to deny VoIP traffic.

- **There's a drop in the number of firewall connections, what happened?**
  SevOne alerts you to a change in the number of firewall connections that appears to be an anomaly. Drilling into the logs for that period reveals a configuration change that negatively impacted user access.

- **I made a configuration change or implemented a new policy. How did it impact the performance of my infrastructure?**
  Working in reverse, you implement the change and then use SevOne to monitor its impact on your infrastructure by monitoring the traditional performance metrics alongside any unexpected aberration in log activity.

- **How can I better understand a particular application's capacity?**
  You use SevOne to compare the number users or IPs connected to a service to the health of the infrastructure supporting that service, including CPU and memory of the server. Having a clearer understanding of the application's capacity allows you to better forecast the impact of your future end user or customer growth on a particular application or service.

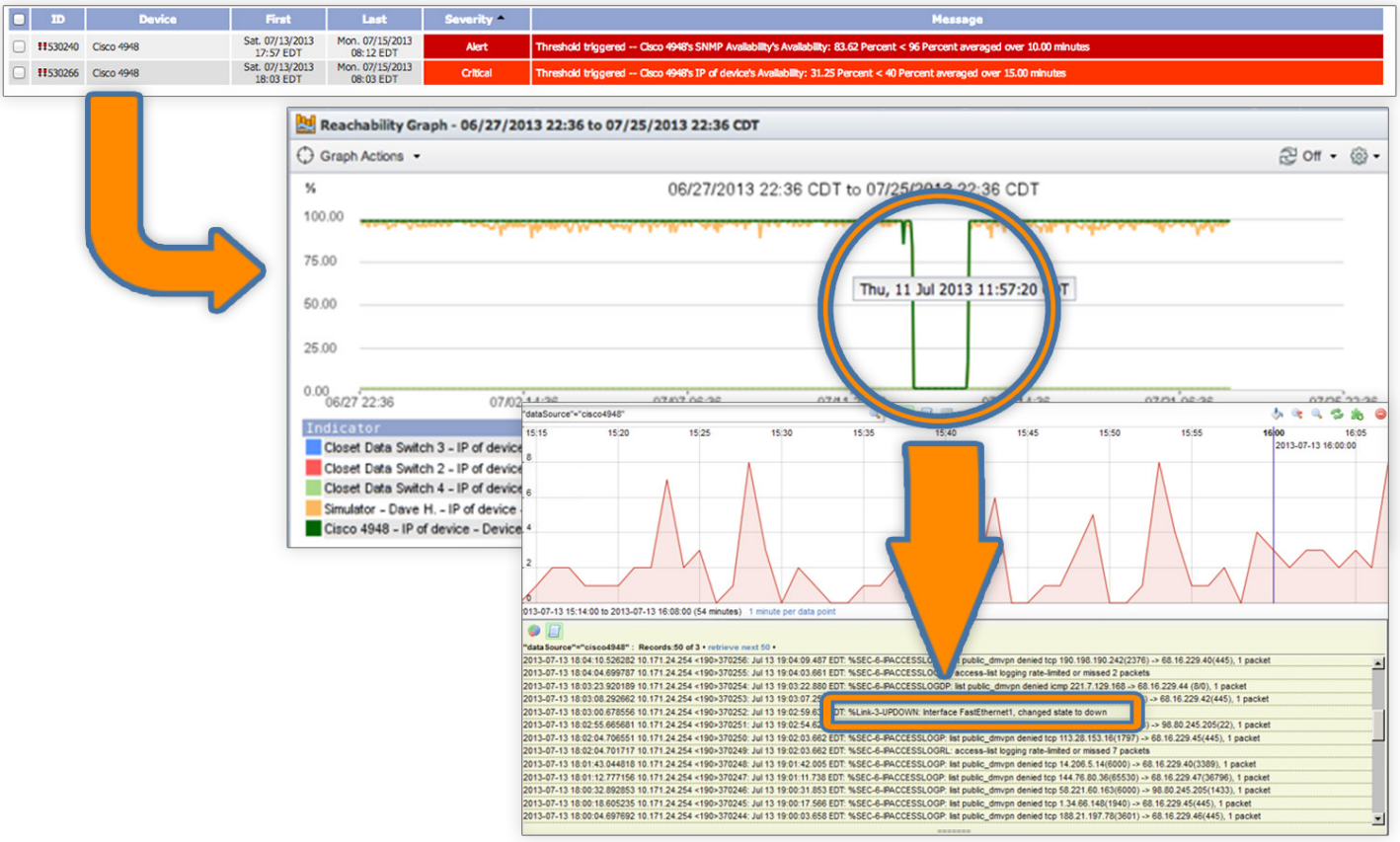
- **I need to purge users of my VPN system to free up space, but who do I remove?**
  You receive an alert from SevOne that memory for your VPN system is trending beyond capacity. You may have thousands of users configured to access your VPN, so you need to determine who no longer (or infrequently) accesses the system. Using SevOne, you report on the record of the audit logs to reveal candidates you can safely purge.

You Don't Know What You Don't Know

Performance issues in your network and IT environment often go undetected because your log search solution does not handle threshold-based alerts or understand trend pattern correlation. If your log solution does allow for threshold-based alerts, it is most likely not real-time (handled after the parsing) and the system bases alerts on static thresholds that are nothing more than best guesses of acceptable performance ranges.

Unlike other log search and SIEM tools, SevOne automatically baselines "normal" performance for every metric it collects – including logs – and triggers alerts any time performance deviates from expected behavior in your environment.

In addition, the SevOne PLA alerts when the first occurrence of a log appears. If you've never seen a particular log alert before, you will want to know about it so you can take action. For example, if your environment generates more than a million log messages every minute, how would you detect an error code from a router reboot in its first occurrence? With the SevOne PLA, you receive an automatic alert the first time such a log appears, allowing you to address the issue before it happens repeatedly and interrupts the operation of your network.



If the number of unique IP addresses or users accessing a particular application drops below normal expectations, it may be indicative of a poorly configured firewall rule or router change that has blocked those users. The SevOne PLA allows you to drill down from the alert to the logs to see if a change occurred during that timeframe.

Why SevOne?

SevOne cost-effectively scales with the largest of enterprise and service provider networks while still generating reports in seconds, not minutes or hours. The underlying distributed architecture of SevOne, in conjunction with a Log Analytics solution designed by the original founders of LogLogic, makes SevOne the platform of choice for proving the performance of the network and predicting potential performance issues before they impact end users or customers.

- **Raw log history** – maintain 180 days of uncompressed, raw log data for forensics search and drill down in reports
- **Drag and drop -** avoid complex written search queries in favor of drag and drop simplicity… with the same results
- **Time savings -** view integrated reports of performance metrics and log data that save you time during security and compliance audits
- **Best practices –** incorporate best practice (ITIL) and compliance regulations (PCI, FISMA, NERC) for a better IT operations management toolkit
- **Speed of log visualization –** gain real-time access to visualizations of log data, with the ability to cost effectively scale your log performance management solution

About SevOne

Founded in 2005, SevOne is headquartered in Wilmington, Delaware. SevOne provides the world's most scalable performance monitoring platform to the world's most connected companies. SevOne's patented architecture, the SevOne Cluster™, leverages distributed computing to effectively collect millions of key performance indicators and to provide proactive alerts when performance deviates from normal. SevOne's platform provides a single source of truth for future-ready customers including global enterprises, finance and healthcare companies, CSPs, MSPs and MSOs.