SevOne

White Paper

10 Key Factors for Selecting a Network Performance Management Solution

Why Network Performance Management

Maintaining optimal network performance is increasingly critical in today's business climate, with the convergence of all business applications and communications on the same network infrastructure. Network managers are facing increasingly dynamic, convoluted, and multi-tenant environments, with end points going mobile, server and application infrastructure being virtualized and distributed, and the introduction of cloud-based applications. This demands that even closer attention be paid to network performance in order to cost effectively and proactively deliver and ensure service levels. The business runs on the network, so if the network has a problem, the business is directly affected.

Selecting the right Network Performance Management (NPM) solution can be a very challenging exercise. The incumbent or legacy solutions have been built via acquisition and integration of separate products, which have disparate operating systems, databases, and even separate user interfaces. Many NPM tools provide application response time via packet capture and inspection, but they don't scale across the network. With both enterprise and service providers in mind, here are 10 key factors that organizations need to consider when selecting an NPM solution.

10 Key Factors in your NPM Selection

1. Architecture for Scale

Network performance management solutions must scale their collection and reporting functions to meet ever increasing network size and speed requirements. The scalability bottleneck in most solutions is the central reporting server. No matter how big a server is used, it can never scale to keep up with the demands of an increasing number of data collectors and storage and reporting demands. The larger the system deployment, the slower a report can take to generate.

NPM solutions that are based on peer-to-peer architecture principles remove these scalability limits, since each peer system acts as both a collector and a reporter. In a peer-to-peer architecture, all peers are aware of which device is being monitored by each peer, and can appropriately route data requests. Thus multiple systems can work together on one report in parallel, effectively multiplying the power of a single reporter. Scaling a peer-to-peer implementation simply requires adding additional peer systems.

2. Ease of Deployment

Most network performance management solutions are based on a server software model, in which the complete solution consists of one or more servers that host the NPM software. From an implementation and time to value standpoint, this can be problematic. In order to successfully deploy an NPM solution, network administrators must finish a complex process of provisioning servers with operating systems, building databases, provisioning offline storage, agent deployments, and then continuously manage all of these component systems as a solution.

An appliance-based solution is vastly simpler and less costly to deploy and maintain. All of the components required to perform data collection, monitoring, reporting and other tasks are pre-built into well tuned, simple to rack and install appliances. Within tens of minutes, the system can discover devices and begin monitoring thousands of network elements. Implementations of appliance based solutions can be done so quickly that in some cases significant problems have been detected in the first few hours of operation. The time to first report and therefore the time to business value is an important consideration from both a financial and operational standpoint.

3. Ease of Use

Network managers will get more value from a solution that is easy to use and that quickly produces meaningful reports. So how quickly and efficiently can operations staff troubleshoot problems? How much time does it take to isolate and convince the owner of the problem (mean time to isolate)? Are there limits to how many users are supported, and can business users retrieve their own performance reports? How application-aware is the reporting and troubleshooting?

Speed and accuracy of reporting is a significant factor in a network performance management solution's ease-of-use. A web-based console is the simplest to launch and use, and it can be easily integrated with existing customer-facing portals. A web-based console can also provide unlimited access to as many users as desired, reducing the mean time to isolate and hand off problems, and reducing ad-hoc report requests on IT operations staff by providing direct access for clients and business unit leaders.

4. Real-Time Visibility (at Scale)

Not only must a network performance management solution be easy to use, but it also must provide complete system-wide visibility, and to a broad set of users. This includes getting real-time visibility of the performance levels of all crucial IT devices, without compromise, across the entire network, server, and application infrastructure. Another key capability is being able to identify the applications and their delivery infrastructure and their impact on the network.

An all-in-one solution can collect and monitor the key performance indicators for all device types, identify applications, and generate reports for the complete and global IT infrastructure. The broadest data collection technology is agentless, meaning that no additional software is required to be installed. Solutions that require packet data capture and inspection cannot cost effectively scale across an enterprise or service provider network, and are inherently limited in the amount or the granularity of data that can be retained.

5. Automated Baselines

Many service-impacting network events are caused by changes in utilization levels, memory leaks and other abnormalities. From the Gartner *Hype Cycle for IT Operations Management, July 2010, "*Clients should look for network performance management products that not only track performance, but also automatically establish a baseline measurement of "normal" behavior for time of day and day of week, dynamically set warning and critical thresholds as standard deviations off the baseline, and notify the network manager only when an exception condition occurs."

Specific baselining and alerting technology can address business hour timeframes and time zone differences to reduce false positive alerts. Additionally, real-time oriented solutions enable operators to baseline network performance at intervals of minutes, whereas most legacy products can only calculate baselines hourly. This tighter time interval provides more proactive monitoring and analysis in addition to reducing the level of exposure to false positives.

6. Monitoring Efficiency

A key benchmark for performance management should be the "monitored elements-to-administrator ratio" or the amount of IT infrastructure elements monitored divided by the number of operations staff required. The most effective IT organizations and service providers track and optimize these types of ratios. An all-in-one solution provides the best workflow integration and application awareness; an appliance-based solution is more efficient to deploy and manage. For example, an organization had been monitoring approximately 400,000 elements with a client/server software solution. After replacing it with an all-in-one appliance solution, that same organization is now monitoring over two million elements with the same number of IT staff.

Finally, the ability to support multi-tenant environments provides further economies of scale for service provider oriented organizations. With fast time to value and less disparate monitoring systems to maintain on an ongoing basis, an all-in-one solution approach delivers a faster return on investment and a decreasing cost per element business model.

7. Integrated Workflows

A network administrator or engineer needs to quickly navigate from high-level status to detailed views of network performance data. Workflows need to be intuitive and reporting granular, with traffic analysis by application type, identification of source and destination users, and problem detection down to the individual indicator level.

For example, a solution using NetFlow data can automatically resolve what type of traffic was associated with a specific interface for a specific alarm. This capability of SNMP to NetFlow integration allows for faster troubleshooting and traffic analysis. Most network performance management solutions have difficulty automating this function.

8. Consolidation of Tools

Most network performance management solutions can collect and report on all types of network data from SNMP to NetFlow and IP SLA latency tests. One system should be able to support all networks and device types, with multiple workflows and roles, from troubleshooting to planning and analysis. Further, an all-in-one system can also monitor the server and application infrastructure, enabling an end-to-end view for troubleshooting and analysis. Client or users from business units should be able to easily view their own pertinent performance reports.

These best-of-breed solutions distinguish themselves from the legacy “Big 4” solutions by uniformly supporting all device types and all collection technologies and methods, including third-party data. This enables legacy server and application monitoring and reporting tools to be eliminated, saving additional maintenance and operations costs.

9. OSS Integration

Once a performance management solution is implemented, the next challenge is to integrate it within the data center in such a way that it provides the most complete, precise and meaningful representation of the organization’s network performance. The best-of-breed performance management solutions not only deploy and integrate effectively from data collection and reporting standpoints, but provide an open architecture for integrating with upstream fault management and trouble ticketing systems. Besides the ability to sending and receiving trap notifications, the Manager-of-Managers operators can “launch-in-context” instant reports when they are troubleshooting an event or outage and need detailed performance data.

10. Future Proof Solution

Choosing a solution that is “future-ready” requires all of the above capabilities. The solution must be easy to deploy and use, scale without limits, scale with increasing cost efficiency, easily support new device types, provide real-time visibility, automate and integrate multiple workflows, and support all user personas. Look for a solution with a peer-to-peer distributed architecture, plug-in device support and collection capability, and a unified reporting framework.

About SevOne

SevOne, Inc. delivers the industry’s fastest, most scalable, and comprehensive real-time network monitoring, troubleshooting and performance reporting solution. SevOne created a proprietary, next-generation distributed technology, called the SevOne Cluster™, that combines the cutting edge principles behind peer-to-peer sharing and big data clusters to scale smoothly so that millions of network elements, across all monitoring technologies, can be monitored and provide a single view to the user. Hundreds of customers, including the top cable companies in North America, wireless network and managed service providers, and top financial services institutions rely on SevOne. Visit www.sevone.com.