Realtime
publishers

The Essentials Series: Network Troubleshooting and Problem Identification

Isolating Network vs. Application Problems

sponsored by
solarwinds

by Greg Shields

SUPER-CHARGE YOUR NETWORK WITH SOLARWINDS ORION POWER PACK!

The **Orion Power Pack** combines three of our most popular products to take your network management to the next level!

- **Orion NPM** delivers comprehensive fault and performance management across multi-vendor networks of any size.
- **Orion APM** extends Orion NPM's powerful monitoring capabilities to applications and servers.
- **Orion NTA** provides deep visibility into network traffic behavior and trends by leveraging NetFlow, J-Flow and sFlow data.

solarwinds

Copyright Statement

Isolating Network vs. Application Problems

“The network is slow today” is without a doubt one of the most disliked phrases heard by network administrators. The network has become a dumping ground for problems that originate as often as not from servers and applications as from the network. Thus, one of the biggest jobs of the network administrator is to defend their network from being labeled the cause of today’s problem. Because slow environment performance is often first—and often incorrectly—attributed to the network, rapid triage and problem isolation is critical to the administrator’s workload.

> ✎ In the case of this author, the story of the “blame game” between network and applications is no better told than at a previous employer. There, an actual scoreboard was set up in one of the IT offices. On one side was labeled *“It is the network.”* On the other was *“It is the server.”* Over time, assigning points to one or the other column became a regular last step in problem resolution. Examples like this are prevalent in IT environments everywhere. They foster a competitive team spirit amongst members of IT while encouraging everyone to make sure their team wasn’t the culprit.

All things being equal, problems in the IT environment occur just as regularly within its applications as within the network itself. Often, impact from network conditions combines with application behaviors to manifest into the problem of the day. Because of this, it is critical to avoid technology and monitoring silos between IT teams. When the network team can view performance and other information related to servers and applications, they can apply their network-based troubleshooting knowledge to a resolution. Conversely, when server and application teams have the ability to peer into network statistics, they gain the ability to relate what they see and know within their domains.

Common Problems in IT

The best way to illustrate the need for cross-team problem identification is through a series of examples. Tools available to network administrators today have the ability to pierce the long-standing divide between “the network” and “the application,” giving the troubleshooting administrator a more-complete set of data to work with.

As a first example, one common problem occurs when network performance itself is the source of the IT problem. In this case, the tick mark goes into the *“It is the network”* column. For situations like these, the first sign of trouble often arrives when users experience slowdowns in application performance. Here, calls to the service desk fill out a picture that email traffic or working with files is not performing to usual standards. In this case, the server or application team may be the first group to be contacted to resolve the problem. If that team can rely on only performance counters native to the systems and applications themselves, they are not likely to find the problem’s resolution on their own. Instead, should they have access to see easy-to-understand traffic flow analysis data from the network side, they may be able to quickly isolate the problem to the network domain. Resolution may not be within their skill set, but general knowledge combined with heads-up visualizations gives them the information they need to redirect the issue to those that can.

A second example is the case in which the network is performing to specifications but an application or database residing on top of that network is experiencing problems. In this case, either team may be dispatched to isolate and resolve the problem. Either team has their domain-specific set of tools at hand to triage the problem—for example, WMI for Windows systems and applications, SNMP for network devices, and so on. Yet due to the complexity of the problem neither group of tools alone can sufficiently come to a resolution. Only through the combination of network statistics alongside those sourcing from servers and applications can a resolution be found. On the network side, that resolution may start with traffic flow analysis, followed by a deeper packet inspection to identify that perhaps the conversation itself between application client and server is the ultimate source of the problem.

> ✎ When the network, server, and application teams all view a common monitoring interface, they gain a greater ability to share information, see the problems and issues that relate to other teams, and work together more effectively. For this reason, today's best-in-class monitoring platforms are not limited to monitoring network components exclusively. Instead, they aggregate the best data from all sources to gain an overall picture of the IT environment.

Common Ways to "Tell the Difference"

Most often, simply identifying the source of the problem takes 80% of the time required to fix it. Thus, leveraging tools that speed the problem identification process greatly improves the efficiency of IT. Narrowing the possible options to one or more problem domains means that the most appropriate IT personnel can be assigned to its resolution.

Considering the previous examples, it can be argued that more data is generally preferred to less when troubleshooting IT problems. When network teams have the ability to pull system-based or application-based information, they gain a better vision of the overall IT environment. Yet the quality of that data is important as well. Not all types of monitoring are useful for troubleshooting all problems. To maximize the information available for troubleshooting administrators, an effective network monitoring tool should include some or all of the classes of monitoring explored in the following sections.

Network Device Metrics Collection

Network device metrics provide information about the system resources on each individual device. These metrics are critical in ascertaining whether a resource overuse problem is a central cause of a reduction in performance. Collecting and reporting on network devices helps the troubleshooting administrator quickly identify whether the device is a source of the problem or the problem lies within the network traffic or application communication itself. Virtually all network monitoring tools include the ability to gather and report on these statistics, most commonly through SNMP.

Server Metrics Collection

Essentially all network monitoring products include the ability to look at network device counters, but not all have the ability to do the same with servers that reside on that network. Although the technology for pulling these metrics has been available for many years, the long-held organizational boundaries between “network” and “server” responsibilities have resulted in these metrics not being gathered by many monitoring products. Yet, as discussed earlier, there is value to IT in aggregating server- and application-based metrics with network device metrics. Network administrators gain the ability to view the impact of network conditions on servers and applications, while server administrators can easily see how their applications are affecting the network.

Application Status and Event Collection

Server metrics illuminate one part of the picture, but their performance-focused information is not complete without the additional detail gained through application status and event collection. Capturing status information—up or down—of applications helps IT teams identify when servers and the network are up but their residing applications are not. Lacking this detailed level of information, it is difficult for troubleshooting teams to quickly isolate the cause of a problem. For example, a server may be operational and responding to a low-level ping request, but its residing application may no longer be functioning. Including this detailed information alongside traditional metrics enables teams to quickly isolate the problem and proceed to a resolution.

Transaction Timing Measurements

Even with the information gathered using the previously mentioned methods, there remains a class of problems that are still difficult to identify. These problems occur when the user’s experience degrades, but does so in ways that are difficult for traditional metrics to capture. Consider the situation in which a user is working with a Web-based application that involves multiple servers. A problem within that multi-server system may manifest as a significant slowdown to the user but not impact system counters, application availability, or even result in the creation of a log event. However, the user is experiencing a legitimate problem with the system.

In this case, the most effective way to measure the user’s experience is through the measurement of network transactions between the elements of that system. Transaction measurements provide a way to determine when and where the user is experiencing delays in their interaction with the system. Analyzing transaction timing over an extended period of time provides a way to determine how the application is responding in comparison with previous measurements. Transaction measurements are sometimes augmented with the ability to submit synthetic or “test” transactions to the application as a way to measure timing against a known result.

Alerting and Notification

A common feature in almost all network monitoring platforms, alerting and notification capabilities are necessary to warn administrators when conditions change in the IT environment. Although alerting features are common, there are major differences between products in the level of detail in alerts as well as granularity in administrator targeting. Effective network monitoring tools enable the ability for rich targeting of administrators based on the type and source of problems. Also important are the mediums supported for alert submission, with better products including support for more and different alerting mediums.

Important also is the data sent to the administrator as part of the alert. Inefficient monitoring solutions alert administrators regarding changes in environmental status. Without the right level of tuning, administrators can be overloaded with alerts as situations occur. The right monitoring solution will alert administrators in real-time with actionable information regarding the situation, while reducing alerts to the minimum necessary.

Auto-Remediation

In mature environments where the configurations are well known, effective documentation and workflows are in place, and the environment is properly baselined, a good monitoring solution can enhance the problem resolution process by solving known problems automatically. Auto-remediation is the process whereby known problems are resolved automatically as they occur. Examples of problems that work well with auto-remediation are network services that require restarting, devices that require resetting, or even the full repopulation of config files in the case of outages. Auto-remediation activities require a network monitoring solution that is aware of environment conditions and has the logic in place to complete an action when a predetermined condition occurs.

Isolating Problems Requires the Work of All IT Teams

The traditional boundaries between what was considered the purview of the “network team” and the “applications team” are steadily blurring. With applications spanning multiple servers in multiple network locations, determining the source of IT problems whether network or application requires the cooperation of both groups of people. As the complexity of the IT environment grows over time, teams must work together to resolve issues as they occur.

A critical assistance to this task is the aggregation of otherwise siloed monitoring needs into a centralized network monitoring solution that is accessible by everyone. Through the process of integrating data from the network and applications halves, both teams gain the necessary information they need to do their jobs effectively.

That process of doing one’s job effectively is important. Article 3 in this series will talk about the five configuration management tasks commonly handed to network administrators. That article will discuss not only the tasks but also tools that make the completion of those tasks much easier.