Essential IT Monitoring: Seven Priorities for Network Management

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper
Prepared for SolarWinds

March 2015

EMA™

IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

Essential IT Monitoring: Seven Priorities for Network Management

Table of Contents

Essential IT Monitoring:
Seven Priorities for Network Management

Essential IT Monitoring

The enabling of comprehensive visibility into all essential technology configurations, performance, and status is fundamental to achieving effective enterprise IT management. To achieve this consolidated view, these monitoring practices must cross multiple management disciplines, and each organization will have a unique set of requirements that will define which disciplines align most appropriately with their business. Therefore, EMA recommends the adoption of management solutions that are modular and fully integrated, allowing each organization to select the most appropriate combination of administrative resources to establish a complete view of its distinctive support stack from a "single pane of glass."

EMA's series of Essential IT Monitoring *white papers identifies key elements enterprises must target in particular management disciplines in order to rapidly identify and resolve issues and to optimize performance across IT infrastructures. Readers are advised to adopt integrated automated monitoring solutions that bring visibility to all the identified elements in the topic areas most applicable to their IT implementation.*

Monitoring Priorities for Network Management

If applications and services are the lifeblood of today's IT-enabled enterprises, then the network is the circulatory system that connects and delivers them. Monitoring the health and performance of your network has long since passed the "nice-to-have" stage and is now considered truly mission-critical. But where should you start? What are the most important aspects of network monitoring, from a practices and tools perspective?

It may help to start by considering how networks are perceived within today's connected organizations. Systems administrators think of networks as plumbing that connects their servers and storage. Application developers think of networks as a cloud—a nebulous means to reach their end users and little more. IT end users simply know the network is what connects them to IT resources so they can do their job. The help desk knows it is a checklist item of likely sources of issues. And everyone all around, usually thinks of the network first when something's not working.

While some will deploy monitoring simply to exonerate the network, there's a much greater opportunity at play. Because the network is the connecting fabric of IT, it is also an ideal location from which to understand the overall health and activity of the systemic whole of the IT infrastructure, including connected resources, users, and customers.

Enterprise Management Associates (EMA) conducts regular field research and dialogue with network engineering and management practitioners across organizations small and large, public and private, domestic and international. Over the years, EMA has identified a number of specific network monitoring practices that yield directly recognizable advantages and results both for network managers as well as broader IT Operations. Following is a detailed assessment of the top seven priorities that EMA advocates for best practices in network monitoring. These do not have to be addressed in the order presented, though the first is an important foundational step that all others must follow.

NETWORK MONITORING TECHNOLOGY ESSENTIALS

Most network monitoring utilizes SNMP (Simple Network Management Protocol) as a primary method for communicating between network devices and management tools. An SNMP agent is available on most every IP-based network device in the marketplace today.

The available SNMP information and commands offered by a network device are defined via a MIB (Management Information Base). Many MIBs are based on IETF standards, but many more are specific to individual equipment vendors and/or specific product types and models.

Network monitoring tools will use SNMP to receive and interpret traps (asynchronous notifications), gather state or statistical information via regular polling, and take actions on the device by setting values of certain key MIB variables.

Priority 1: Get the network under management.

Getting started is often the hardest part, but in this case it may be the easiest. In order to establish effective network monitoring, the first step is to figure out which devices comprise the network and which critical resources are connected to it and by it. You can't manage what you don't know is out there, and EMA has heard countless stories of surprises resulting from initial (or even ongoing) network discovery. Start by selecting a network monitoring product. Some are simple and some are sophisticated, but they all allow the collection of network device information for bringing devices under management.

The most basic approach to populating your monitoring tool involves manual definition of managed devices through the entry of IP addresses and essential security information such as SNMP community strings. Many tools also offer the ability to import device information in bulk, often from a spreadsheet or CSV file, to accelerate the process. But manual techniques will commonly leave gaps because unknown devices will remain unknown after the population process.

A better approach is to use autodiscovery features, whereby the monitoring tool will scan the network, find the devices for you, and automatically populate your monitoring tool. Getting the best out of autodiscovery does depend on conformity of and consistency in SNMP community strings so that the algorithms can properly find and include device details that you will want to monitor. If possible, it is also useful at this stage to define the topological relationships between devices. This helps during subsequent engineering and troubleshooting processes when it is important to recognize paths across the network. Some autodiscovery algorithms will do this automatically, by examining Address Resolution Protocol (ARP), routing, switch forwarding, and related tables via the SNMP interface, or by using discovery protocols such as Link Layer Discovery Protocol (LLDP) or Cisco Discovery Protocol (CDP).

Next, think beyond standard network devices. There are a number of critical connected resources that should also be incorporated as part of the initial monitoring push, including the following:

- **Network-Enabling Resources –** Network-enabling resources, such as Domain Name Service (DNS) and Active Directory (AD) servers, as well as IP address management systems such as Dynamic Host Control Protocol (DHCP), should be defined or discovered and added. These services are critical to basic network functionality, and when any of them stops functioning properly, network and application health and performance suffers. For instance, if AD authentication is not occurring because the server is down, users will not be able to access their Exchange email.
- **Network Security Elements –** Network security elements such as firewalls and Intrusion Detection/Prevention Systems (IDS/IPSs) will commonly sit inline as part of the network path.
- **Critical Connected Application Servers –** Critical connected application servers are important, too. You want to know that those systems are up, and at the very least that their network interface cards (NICs) are functioning properly so they can access the network without problems.

Priority 2: Define device groupings and relationships.

Once all network components have been found and brought under management, the next step is to organize the elements to be monitored. This essential step allows network monitoring teams to designate the relative importance of each component, according to specific characteristics of the organization and the managed infrastructure. Basically, the goals of this step are to link the monitored network to the organization that it connects and supports and to define the relationships and dependencies among these devices.

A monitoring tool that maps dependencies will be critical when a network operations team is responding to service degradations and interruptions. Most network monitoring tools will alert the network operations team about every device that has lost connectivity. If a single interface fails on a switch, that failure can have a cascading effect on multiple switches and servers that rely on it for connectivity to the rest of the network. The network operations center (NOC) might receive dozens of critical alerts that are tied to a single interface failure. This alert overload can often obscure the underlying problem and slow down the mean time to resolution (MTTR). Therefore, network monitoring tools that understand network dependencies and are more efficient with their alerting can be very valuable.

There are three types of grouping approaches that EMA finds to be most common and useful across settings both large and small, and using them helps to answer the what, where, and who of problem isolation and management. Following are some key types:

- **Device Type –** Network managers most often start with views into the managed network that bring together devices by category, such as routers, switches, and access points. This approach to grouping facilitates inventory management, device administration, and general health assessments. Enterprises with large wireless LAN deployments will derive value from device type groupings, as wireless access points are increasingly becoming the primary network access layer. The ability to distinguish between wired and wireless devices and to understand the relationships and dependencies between them will be critical to network operations. Device type groupings will often be the place to figure out precisely what is the source of a problem under investigation.
- **Geographical –** For any organization that has more than one operating location, a geographical or site-based grouping of monitored devices is perhaps the most easily understandable way of looking at the network. This answers the question of where problems have occurred. Graphical topology map views fill this need and are often used as a primary display in the NOC as a visual guide to operations status. It is also very helpful for quickly isolating the scope and impact of any problem. Additionally, Many network managers will assemble these geographical maps manually, which can be an error-prone process. However, some network monitoring tools use geolocation and discovery techniques to automatically assemble maps of the wired and wireless network, removing human error from the equation.
- **Organizational –** The most direct technique for relating network monitoring information to the connected community is to group network elements in terms of which part of the business or organization they serve. This addresses the question of who is impacted by any issue or problem. There will be a lot of overlap here when considering core devices, but this is key to recognizing, and accurately communicating with, end-user and line-of -business communities, whether for regular status reporting or during a troubleshooting and recovery scenario.

Priority 3: Prioritize availability monitoring.

The next step and priority is to define which devices, groups, and/or sites are to be designated as most critical to the organization. Any time one of these switches or ports is down unexpectedly, it's likely that access to important applications has been interrupted or, at best, impaired. These will be the network components that will be assigned the highest priority for sustained monitoring—when any of these elements or locations suffers an availability incident, they will receive priority attention from the operations staff.

Network availability monitoring gathers events, commonly in the form of SNMP traps or other asynchronous notifications, combined with regular "heartbeat" checks on device/component health and status, commonly via SNMP polling. Any events received or any atypical test results will be translated into alerts or alarms within the network monitoring system. Those alerts and alarms are then assigned relative priority, often ranging in severity from "informational" to "critical." Critical alerts indicate severe impairment of networking function and, usually, loss of connectivity, whereas major alerts may represent impairment but no loss of connectivity, and so on down the line. Most network management platforms include features for automatically notifying operations personnel of high-priority or critical alerts, via email, text, or other means—even social media.

Prioritized availability monitoring involves setting up alert/alarm severity definitions as well as escalation processes to be used as part of everyday operational monitoring. Typically, focus is put on handling the most critical availability issues—the ones where connectivity has been lost. But it also makes sense to set up priority notification and escalation for the most mission-critical network devices, network-enabling services, and network-connected resources. This helps operations teams recognize not only whether or not the network is operational, but also if the broader IT infrastructure and ecosystem are being served adequately. The work an organization has done in defining groupings and relationships among network devices will pay off here as it will help the network team identify which devices are most important to the overall health and performance of the infrastructure. If the monitoring tool has a solid understanding of infrastructure dependencies, the process of defining alert and alarm definitions will be far simpler.

> Prioritized availability monitoring involves setting up alert/alarm severity definitions as well as escalation processes to be used as part of everyday operational monitoring.

Priority 4: Add device-level performance monitoring.

With availability monitoring in hand, network managers can turn towards the next major set of challenges: recognizing and managing the performance of the network. The objective here is to move beyond being able to answer the question, "Is the network up?" and on to "Is the network meeting performance and throughput expectations?" The most common mechanism for this is to expand availability-oriented SNMP polling to collect a broad range of health and activity metrics from network devices on a periodic basis. That data is then archived in a historical database so that trends can be identified and "normal versus abnormal" activity revealed.

From a tools perspective, performance monitoring requires a scalable polling engine for gathering large volumes of metrics, together with a sufficiently high-performing database and reporting features. In large managed environments, multiple polling engines and multiple databases may be required, and they will need to work in a fully integrated fashion so that data can be pulled from all sources during reporting and analysis activities.

Based on EMA research and practitioner dialogue, following are a set of essential areas to focus upon for establishing device-level network performance monitoring:

- **Monitoring Device Resources –** Collecting metrics on current levels of device resources, such as CPU usage, memory usage, power levels, and temperature, reveals a detailed view of the operational capacity and health of each device.
- **Monitoring Ports/Interfaces –** By harvesting counters such as packets, octets, discards, and errors both coming into and going out of each logical and physical interface, it is possible to recognize congestion issues as well as operational viability of many touchpoints that comprise the connectivity fabric.

- **Setting Performance Thresholds –** Default performance alerts/alarms should be configured to watch for extreme high values in monitored metrics across all devices, such as interface utilization or device CPU exceeding 90%, and should be tuned more finely for critical/essential devices and resources. This provides indications to network managers that network links may be approaching saturation, before the network begins to fail.
- **Identifying Trends –** Your monitoring system should provide reports on performance metrics over time so that you can recognize trends over weeks or months, or even over the past year. This provides network engineering with the data necessary to accurately plan capacity and gives network managers the ability to recognize changes in usage patterns or quality indicators that warrant proactive mitigation. The system should have the analytical capacity to predict and alert on capacity issues before they lead to a service interruption. For instance, if the CPU on a router has risen from 50% to 70% over a three-month period, the tool should be able to predict when the utilization rate will hit 90%, a point at which network engineering will need to upgrade the device.

Priority 5: Get change under control.

When it comes to stability and performance of the network, the number one enemy is unplanned change or unintended consequences of change. Consequently, an essential aspect of monitoring networks for both performance and health must include recognition of changes being made to the network or occurring within the network. For instance, a routing change can break a network path between sites; a network QoS tag could be misconfigured and starve a latency-sensitive application like VoIP of necessary priority delivery; or a firewall rule change could block access to a critical application. Having change indicators on hand can significantly accelerate both troubleshooting and remediation of problems.

> An essential aspect of monitoring networks for both performance and health must include recognition of changes being made to the network or occurring within the network.

There are two techniques for integrating change awareness into network monitoring. The first involves finding and capturing change indicators and adding them into the primary monitoring platform and process. These indicators can often be found in the form of device traps or notifications (sometimes via application programming interface). Another good source is log files, which capture and record the exact change made, the time it was made, and often who made it.

The second important approach to establishing control over change is to leverage the ability of network change and configuration management (NCCM) tools to automatically scan devices, compare their configurations to expected norms, and report variances. This latter approach can help reveal potential problem sources while also providing the added value of assuring policy and regulatory compliance. NCCM tools may be available as a module that works directly with your network monitoring platform, which will be easiest to integrate into monitoring practices, or they may be standalone, in which case a bit more effort will be needed to incorporate change indicators and scan results.

Priority 6: Add application awareness.

With the network layer well in hand and being monitored for availability, performance, and change, network managers can turn their focus to adding the crown jewel of monitoring—application awareness. The objective here is to understand exactly what is traveling over the network and from where to where it is traveling, in what volumes, and at what times. This is the touchpoint between a network and the served organization, yielding direct insight into the applications and services that the network is entrusted to deliver. It also represents one of the most direct opportunities for recognizing how individuals as well as groups utilize and gain value from the network.

To get started, it is essential to deploy agents, probes, or tools that can measure and report application flow activity, or that can harvest that data from where it already resides. A common technique is to harvest NetFlow/sFlow/JFlow/IPFIX records that are generated by network devices and document application flows. This data can also be gathered via active synthetic testing with features such as Cisco's IP SLA, from log files on systems and devices. The most direct view into application awareness is through the inspection of packets as they traverse network links. Packet-monitoring tools can often automatically identify application flows and measure application and network response times. Each approach to application awareness has its strengths and its costs, and EMA advocates using a mix of techniques in order to establish the broadest and richest possible application visibility while staying within an acceptable total cost envelope.

EMA advocates using a mix of techniques in order to establish the broadest and richest possible application visibility.

With application-aware data incorporated into the monitoring process, measures can be taken to leverage it in a manner similar to using device-based performance data as outlined above. Network managers will want to set thresholds in order to be notified of unexpected spikes or high levels of activity of any individual application or any individual end user. Unexpectedly low levels of activity may also be of interest, as they may indicate impaired application or transaction activity.

Most application-aware approaches will also provide some means of measuring and monitoring end-user response times, which serve as a proxy for user experience. Monitoring and setting thresholds for lengthy response times is an important technique for recognizing disruptions affecting the end-user community, whether or not the end users are rooted in the network. This measure alone brings network monitoring directly into the fold as part of broader cross-domain, service-oriented operations and is consistent with strategic shifts that EMA has been documenting within the IT management function.

Finally, as with device-based performance monitoring, network managers should identify and tune thresholds so that alerts are raised against the most mission-critical applications on a timely basis, allowing faster response and restoration when issues arise.

Priority 7: Integrate and communicate.

The full value of network monitoring cannot be fully realized without sharing and collaborating, both across the IT infrastructure team and beyond it. Since the network is the fabric connecting IT-empowered organizations, it represents a strategic viewpoint for understanding the ebb and flow of activity and health of the IT function in the eyes of those who rely upon IT for their daily tasks and work. That viewpoint is a powerful one that, when effectively shared, can facilitate improved planning, smoother rollouts, and better collective understanding of operations between IT and their customers.

Based on the broad range of management systems that EMA studies and covers, as well as research findings in best practices in cross-domain operations management, the following are recommended focus areas for integration and sharing of information into and from the network monitoring function:

- **Help Desk and Trouble Ticketing –**Connecting the network monitoring system to a trouble-ticketing platform, and/or directly to a help desk management system, provides a direct link for tracking issues as they arise, viewing the steps that have been taken to remedy them, in the final dispensation. Time-based escalation procedures can also be automated for network issues using the features in these systems to provide a better experience for IT's customers.
- **Systems and Application Monitoring –** The network connects systems to end users or to other systems to deliver application and service traffic. By aligning network monitoring with monitoring

of systems and applications, IT operations teams can correlate indicators and events to recognize dependencies and accelerate identification of root causes. This may involve using another layer of management technology to serve as a central consolidation point, or it may be possible within the core network management platform, if that system has been designed to incorporate data from other domains.

- **Security Monitoring and Management** – Many of the technologies and data sources used for network security monitoring are the same as those used for network operations monitoring. Issues recognized within the network may, at times, actually reflect security threats. Open sharing of activity and issues found by the network monitoring team with the security team can greatly accelerate incident assessment and remediation. As with systems and applications, this may involve forwarding events or data to a central security event and information management (SEIM) platform, or it may be an integral capability of the network monitoring system.
- **Line of Business and End Users** – Finally, we cannot forget those the network serves. Providing a means for reporting or exposing current network health, availability, and even performance status to senior executive leadership and even down to end users can be very helpful in managing expectations and proving value delivered. Essential here is the ability to focus reporting on that portion of the infrastructure that is relevant to a user, group of users, or line of business so that they are not bothered with information that is not pertinent to their needs.

EMA Perspective

Many will say that network management is a mature, even mundane, set of technologies and practices today. However, EMA research and ongoing dialogues yield evidence to the contrary: While network management techniques are widely understood, they are often not applied in a consistent or effective manner. Sometimes this is due to growing pains—small shops that cobble together some open source with some scripts but find that the resulting approach doesn't keep pace with the demands of monitoring a growing network. Other times, the issue is fragmentation due to organizational size, where various teams have purchased the tools they need without considering the big picture or leveraging existing in-house capabilities. The result of either situation is an inefficient process, with gaps in visibility, a slow response to problems, and no ability to get ahead.

By building out network monitoring based on the practices and priorities listed here, network managers and operators can move away from a frenetic and reactive operations mode and towards a more proactive, strategic position. Start by getting your network under management, by aligning and grouping network resources according to organizational priorities, and by establishing and prioritizing availability monitoring. Follow that with performance monitoring, integrated change awareness, and application awareness to achieve the highest degree of visibility and control. And finally, share the results for the greatest and most lasting synergy.

> By building out network monitoring based on the practices and priorities listed here, network managers and operators can move away from a frenetic and reactive operations mode and towards a more proactive, strategic position.

SolarWinds is a provider of IT management technologies that cover a broad range of the network monitoring needs discussed here. At the core is **Network Performance Monitor** (NPM), which provides discovery, grouping, availability monitoring, performance monitoring, and alerting. Its grouping functionality now features automatic geolocation for advanced network mapping and grouping of wired and wireless infrastructure. NPM overlays these maps with performance data, which provides visual displays of wireless heat maps and Layer 2 and Layer 3 link utilization. Wireless heat maps are especially useful for WLAN troubleshooting and capacity planning.

SolarWinds has recently enhanced the operational efficiency of NPM with the addition of topology-aware and dependency-aware alerting. For instance, if a single device failure is responsible for a degradation or loss of service across multiple other devices, NPM has the intelligence to send the NOC a single prioritized alert rather than countless individual alerts that would overwhelm the network operations team. NPM has also gained the ability to provide forecasting and capacity planning alerts and reporting. SolarWinds has automated NPM's ability to analyze performance trends and warn the engineering team about capacity issues on the individual components of critical devices, including CPU, memory, and interface bandwidth.

On the application-awareness side of network monitoring, SolarWinds has added continuous packet monitoring to NPM. This deep-packet inspection feature provides application-aware network performance monitoring, including automatic application identification coupled with network and application response times. Together with SolarWinds **NetFlow Traffic Analyzer** (NTA), which can identify which users, applications, and protocols are consuming the most bandwidth, NPM is able to deliver a mix of techniques for application awareness in an enterprise's network management toolset. While SolarWinds NPM can also solve and cover some aspects of change awareness, **Network Configuration Manager** (NCM) can complete those functional needs. Other SolarWinds products are able to track and accommodate monitoring of essential network-connected resources such as **servers and applications**, **DHCP/DNS servers**, **virtualized infrastructure**, and **storage arrays**. And finally, the SolarWinds solution comes with a powerful complement of dashboard and reporting features that can be readily adopted for collaborative and information sharing needs.

About SolarWinds

SolarWinds (NYSE: SWI) provides powerful and affordable IT management software to customers worldwide from Fortune 500 enterprises to small businesses. SolarWinds' approach is consistent across all market segments – focusing exclusively on IT Pros and striving to eliminate the complexity that they have been forced to accept from traditional enterprise software vendors. SolarWinds delivers on this commitment with simplicity through products that are easy to find, buy, use and maintain while providing the power to address any IT management problem on any scale. Additional information on SolarWinds can be found at **http://www.solarwinds.com/**.

Additional Reading

For information on optimal monitoring practices in other management disciplines, please see other white papers in the EMA *Essential IT Monitoring* series:

Essential IT Monitoring: Five Priorities for Cross-Domain IT Management

Essential IT Monitoring: Ten Priorities for Systems Management

Essential IT Monitoring: Five Priorities for Security Management

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals and IT vendors at www.enterprisemanagement.com or blogs.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook or LinkedIn.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com
2770v2.031915