PAESSLER

How to Choose The Right Network Monitoring Solution

White Paper

PRTG NETWORK MONITOR

Author: Thomas Timmermann, BD Manager at Paessler AG
Published: June 2012 - Last Update: April 2014

Table of Contents

Introduction

A high performance network is a basic 'must have' for a functioning IT infrastructure in any company. To ensure smooth business procedures, all processes should run without complications, including the internal and external communication between various company locations, as well as with clients and partners. Malfunctions and failures in operational processes easily result in loss of time, as well as financial loss. A network monitoring software which constantly monitors processes in the network, performs analysis and alerts IT personnel as soon as an error occurs or critical values are exceeded is highly recommended in order to keep track of the availability, performance and bandwidth usage in an IT network. Network monitoring enables the administrator to intervene quickly, even remotely, if he or she is not on location.

Of course, every company has different requirements for a network monitoring solution, and as the market offers numerous different tools and solutions, careful selection of a suitable solution is a must. This white paper shows the various options a network solution can offer, if the right criteria are considered in the decision making process.

Why Network Monitoring?

More and more companies are integrating network monitoring solutions in their IT concepts. Around-the-clock monitoring pays for itself in several areas: it provides enormous time savings and supports administrators in planning resources, as well as optimizing the company network.

MORE TIME FOR ESSENTIALS

A monitoring solution generally proves itself through early recognition and reporting of errors, malfunctions and exceeded thresholds, and thus enables immediate intervention. In addition, IT personnel no longer have to keep constant watch over all network components, including servers, desktop computers, applications, traffic, etc. As such, the monitoring system saves in two ways on valuable time, which the administrator can use effectively for other tasks. This relates to the current client survey by Paessler AG: 90% of the 724 clients surveyed indicated that they are saving significant time resources through the network monitoring solution PRTG Network Monitor: 43% realize time savings of three working hours per week.

ADDED SECURITY

A monitoring solution also contributes significantly to the security of a network. If the solution reports a sudden jump in CPU usage or if traffic values suddenly differ significantly from the norm, this can be an important hint for the IT staff of possible malware or phishing attacks. Network monitoring software can be easily integrated into existing security concepts that have virus scanners, firewalls, etc., to provide additional security.

... CONTROL IS BETTER

Network monitoring solutions offer IT personnel more control over their field of responsibility through comprehensive monitoring of the entire network infrastructure and immediate alerts. The IT team has the network under constant observation and is provided with detailed insight into network processes and the usage of individual resources. The current status and other detailed information are available at any time. As several solutions provide remote access or smartphone apps, the administrator can even take care of his or her network when they are not on location. This significantly reduces the stress factor for the entire IT department: as long as no alert has been reported, the personnel can assume everything is working smoothly.

INCREASE POTENTIAL

Reliable trend analysis can be created from the network monitoring software's comprehensive data collection. This gives IT personnel deeper insight into their network and enables them to discover and realize optimization potential well in advance. For example, determining actual bandwidth usage allows IT to plan and provide the needed resources more systematically, which, especially for virtualization projects, is an important factor. Beyond this, the administrator can use this information to guarantee observation of the Service Level Agreements (SLAs).

FINANCIAL SAVINGS

As professional network monitoring solutions with large functional ranges are being offered for reasonable prices, these solutions put little stress on IT department budgets while offering high potential for saving time and resources. They also prevent significant financial losses caused by delayed failure identification. While selecting a solution, it is important to ensure that the manufacturer provides a transparent licensing model. This prevents the user from having to buy necessary functions as separate add-ons.

Network monitoring solutions ensure quick reactions by reporting error messages in time and, thus, eliminate down time significantly, if not completely. Analysis of the actual network status makes it possible for IT personnel to account for weak spots or usage peaks and to adjust, replace or cut these out accordingly before they lead to serious impairment of business processes.

" PRTG is the most comprehensive and cost-effective solution we've used. Beyond network monitoring, it's a change management solution. We can look at historical data for every sensor and make configuration changes right from our desktop. It definitely allows us to operate more efficiently, which is especially important with our small staff."

Greg Graeff, Associate Director of Information Technology, Point Park University

Classification of Network Monitoring Solutions

Every company, and therefore every network, has different requirements for monitoring software. A large number of solutions have been developed in order to cover these requirements as completely as possible. This multiplicity of options has lead to the market becoming more complicated. In spite of this, solutions can be categorized into four main types.

OPEN SOURCE SOFTWARE

In consideration of their IT department's often slim budget, many companies opt for open source software, with the hope of setting up a quick, inexpensive solution. At first glance, these systems offer significant advantages, as they are usually customizable and can be used with no license cost. A closer look, however, usually shows that the disadvantages outweigh the benefits. The above average effort required for implementation and configuration, as well as the often limited range of functions, are drawbacks that cannot be ignored. For the most part, only basic functions are integrated, which are not capable of detailed network monitoring. The lack of responsible manufacturers is another problem: product support is generally provided by the community and is correspondingly unreliable, often leaving the user to solve problems and answer questions themselves.

INTRODUCTORY MONITORING SOLUTIONS

Those with serious interest in long-term, reliable network monitoring can use inexpensive introductory solutions as a first step. While these also offer only a limited function range, they at least provide a foundation – bandwidth monitoring using SNMP or availability control via Ping. Because of its reduced range, this type of software is suitable for smaller networks or for an introduction into network monitoring. If monitoring should be expanded, a transition to a solution with higher performance and more extensive monitoring becomes necessary.

"SPECIALISTS"

Monitoring systems directed toward specific areas within the network, for example bandwidth measurement using Packet Sniffing, fall into this category. This specialization ensures high performance in that area, but is not appropriate for extensive, across-the-board monitoring. "Specialists" are generally used by equally specialized companies for monitoring high-performance cables or networks, often in combination with broader solutions.

ENTERPRISE NETWORK MANAGEMENT SOFTWARE

In enterprise network management solutions, monitoring systems are usually just a building block within a much broader concept. Due to higher license costs and complex installations, these solutions are generally of little interest for medium-sized companies. Besides this, these systems are not focused on network monitoring and cannot compete with independent network monitoring solutions in functionality and usability.

"ALL-IN-ONE" MONITORING SOLUTIONS

The growing importance of professional network monitoring has lead to "all-in-one" network monitoring solutions. These offer various general monitoring functions, as well as special features for individual sub-areas. For example, these solutions control conventional protocols like SNMP, Packet Sniffing and flow protocols for bandwidth monitoring. They also provide a wide selection of monitoring sensors and protocols (SQL, FTP, HTTP, Exchange, POP3, virtual servers, etc.). This product type can generally be installed quickly and simply, and often comes with professional, reliable manufacturer support. Another advantage: the solutions can be adjusted to growing network structures through scalable licenses, and the acquirement costs are manageable. All the same, the price ranges from 500 EUR to 50 000 EUR and higher – one more reason to analyze the actual requirements within a company to avoid running into unnecessary investments.

Selection Criteria for a Suitable Network Monitoring Solution

Several basic factors, besides the cost of the solution, should be considered in the decision making process, which consider the given infrastructure as well as the characteristics of potential solutions.

Those making these decisions must be absolutely certain on two points: which requirements they have for the system, and for which area of application the solution is needed.

FIGURE:

One solution to monitor the entire IT-infrastructure spread over several, distributed networks.
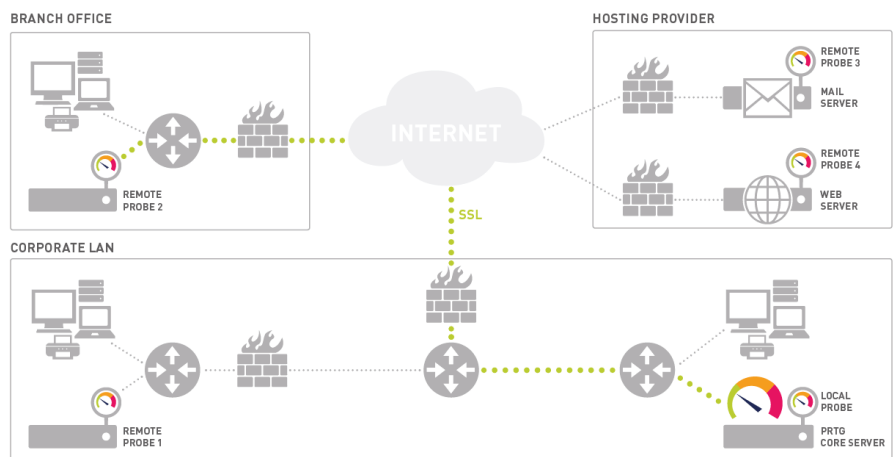
SIMPLIFICATION

The basic function of network monitoring software should be to provide the administrator with the time needed for other useful tasks instead of having to keep a permanent eye on the infrastructure and all connected systems. In other words: the solution works automatically after a simple installation,so that it creates space instead of creating more work for the IT personnel.

KNOW THE REQUIREMENTS

The selection of an appropriate network monitoring system generally complies with, the size of the network and the scenarios to be controlled. These scenarios include, for example, servers, switches, workspace computers, as well as the connections between these and the connection to external locations and the Internet. Two important areas that should be monitored in every company are the website and email communication. With the former, it is important that general performance and individual components, like shops or forms, are monitored in addition to mere response times. Monitoring systems are especially helpful for internationally operating companies to check and optimize response times for requests from various countries. Monitoring software supports the IT department in observing the availability of POP3 and IMAP servers for email traffic. It also helps to discover delivery errors by analyzing the entire delivery process, from sending to receipt of an email, using test mails.

A lack of monitoring experience often results in only identifying limited options of monitoring application in advance. Besides this, networks grow, increasing the demand for monitoring. It is advantageous to choose a solution that can grow according to the demand. To help remove insecurities before purchase, the user should be provided with a full-scale test version, which he or she can purchase after a successful and satisfactory trial run, and that can be used without interruption or reinstallation. Should problems arise during application of the test system, this is the perfect opportunity to test the manufacturer support, so that productive operation can run as free of complications as possible.
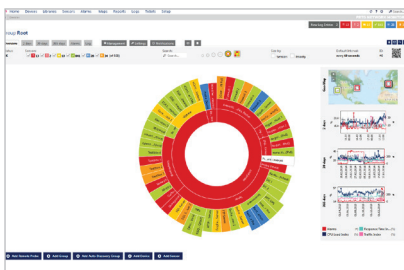
FIGURE:
Email round trip sensors ensure the end-to-end
delivery of emails.
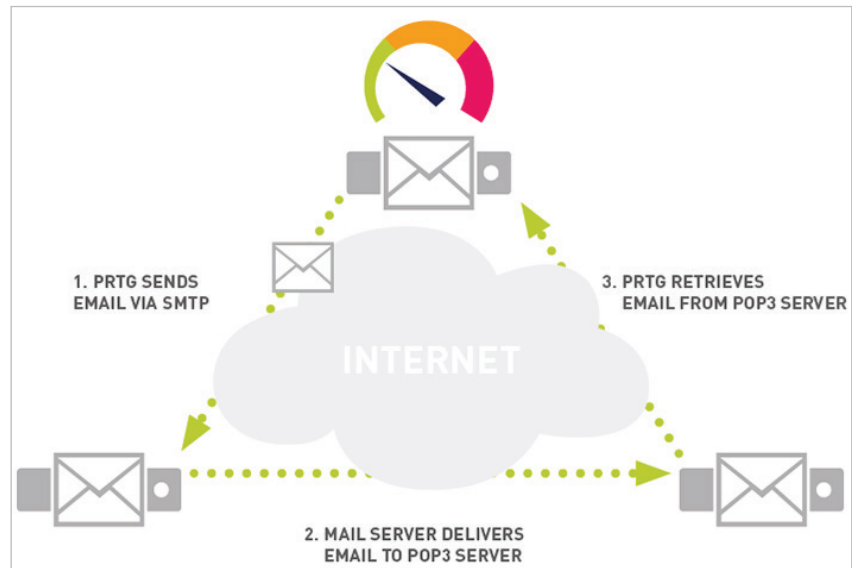
TECHNICAL "MUST-HAVES"

FIGURE:
The PRTG Sunburst View gives a fast overview
about the status of the entire network.

Bandwidth, usage and availability monitoring belong to the core elements of a monitoring solution's technical requirements. It is important to watch for extensive support of the most common protocols and technologies, like WMI, NetFlow, sFlow, jFlow, Packet Sniffing and SNMP, for example, as most networks are extremely heterogeneous IT landscapes. Comprehensive monitoring is possible through coverage of the most popular protocols. It is also advantageous to have optional remote monitoring available for multiple locations or distributed networks. This is sometimes even a component of particular service packages or licenses.
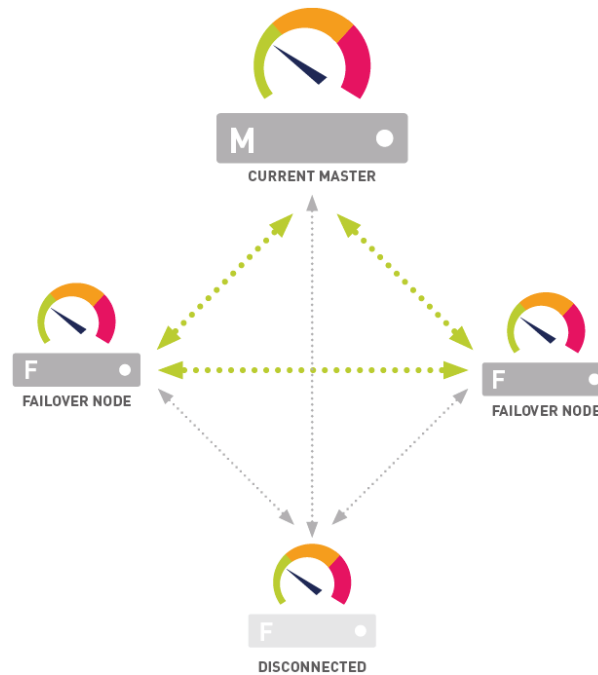
A good network monitoring software offers the administrator information about performance of bandwidth and availability in the form of clear, detailed graphs, reports and lists. It also archives all data so IT staff can maintain a long-term overview and make improvements or changes according to recognizable trends. This establishes the foundation of professional network management.

Alarms are an important function for relieving IT personnel as they alert the responsible administrator of existing errors, reached or crossed thresholds or devices that have crashed. With most solutions, these alarms can be tailored to suit the company's needs, so that the administrator can be reached per email, text message or pager notification, Syslog, HTTP request; or the problem can be rectified automatically with executable .exe files. This creates security and ease for the responsible personnel. It should be possible to define dependent actions for alarms as well: if a solution reports a server crash, for example, the applications that are connected to this server will not generate their own independent reports. This eliminates floods of redundant alarms.

An integrated cluster function provides increased security with regard to possible downtimes of the monitoring system. This feature enables parallel monitoring through multiple instances of the software. If one or more of these instances fail, the remaining, functional instances will take over their tasks and continue monitoring without interruption. This protects the user from software failure and guarantees optimal network performance.

Following the course of the ever-growing cloud computing concept and the increased use of virtualized systems, the network monitoring solution should also offer the corresponding options for monitoring these systems. A selection of different sensor types that are designed specifically for application in virtual environments is beneficial here, for example, for VMWare, Microsoft hyper-V, Parallels Virtuozzo Container or Amazon Elastic Compute Cloud (EC2).

ADVANTAGES IN USABILITY AND SERVICE

It goes without saying that a network monitoring service should be user-friendly with clear, comprehensible menus and intuitive operation. In addition, the user interface must be constructed flexibly and designed for use as, for example, a Windows, Web or mobile interface. As a general rule, automatic network recognition after installation should be a standard feature of the solution. A solution available in the national language is convenient but not necessarily a requirement.

When working with charts and reports, administrators profit from customizing structures and composition to fit their unique demands, as this enables quicker access to more frequently used analyses, for example. In most cases, single devices can be combined into groups, to create a clear overview of the network. Some solutions offer predesigned templates for an overview of the software and hardware components, which can be customized as needed. IT personnel can often choose between summary and detail views.

Before the final decision for a specific monitoring system is made, the company should examine the terms and conditions very carefully. Manufacturers that offer transparent costs with simply structured licensing models are especially appealing. Another plus factor is integrated upgrade options,in case the network expands in the future. This ensures that companies are armed for future tasks. A monitoring solution can earn further points with manufacturer support and further information in the form of user manuals, etc., in the appropriate language.

Summary

A network monitoring solution presents a highly advantageous supplement to a network's infrastructure and provides relief for the IT department on one hand, and is able to reveal previously unrecognized optimization possibilities on the other. It can only be used to its full potential, however, if it is attuned to the requirements of the network. Thus, companies on the lookout for the perfect system should take enough time to test and compare without buying the first solution they find. The following checklist specifies the most important criteria and questions that should be considered in advance.

Checklist for Selection of Network Monitoring Software

✔ What should the monitoring system be able to accomplish? How large is the existing network? Are there already concrete plans for expansion that should be considered in planning? Do upgrade options make the solution future proof?

✔ Should comprehensive monitoring be performed over the entire network, or should only specific areas be monitored?

✔ Is a test version of the monitoring solution available that, in a best-case scenario, can be adopted directly into productive operation after a successful test period without reinstallation?

✔ Which protocols and technologies support the solution regarding bandwidth and availability monitoring? Are these sufficient for the company's requirements? Is centralized monitoring of distributed locations possible?

✔ Which data is collected by the solution? How are these evaluated? Are graphs, reports, etc. customizable? Is there a long-term data archive that would provide the foundation for a trend analysis?

✔ How does the solution alert responsible persons in case of emergency? Is this configurable?

✔ Is the solution's structure user-friendly? Can it be operated intuitively? Are individual settings possible (e.g.: customized user interfaces)? Is the interface designed so that it functions in the operating system, browser and on mobile devices?

✔ Is the solution available in the required languages? Does the manufacturer provide sufficient support? Are other information sources (user manuals, blogs and/or forums) available?

✔ How transparent is the manufacturer's pricing policy? Do the licensing models fit the company requirements?

PRTG Network Monitoring

- Easy to Use
- Reliable Operation
- Simple and Fair Licensing
- Your Entire Network at a Glance
- All-in. No Add-ons. No Extra Costs.
- Long-term Planning and Optimization

ABOUT PAESSLER AG

Paessler AG leads the industry in providing the most powerful, affordable and easy-to-use network monitoring and testing solutions. The company's suite of just-right software products deliver peace of mind, confidence and convenience for businesses of all sizes – from Small Office/Home Office (SOHO) to large enterprises, including more than 70% of the Fortune 100 companies. Based in Nuremberg, Germany, Paessler's global reach includes more than 150,000 active installations of its products. Founded in 1997, Paessler AG remains a privately held company and is recognized as both a member of the Cisco Solution Partner Program and a VMware Technology Alliance Partner.

Freeware and Free Trial versions of all products
can be downloaded from www.paessler.com/prtg/download.

Paessler AG · www.paessler.com · info@paessler.com