How to Choose the Right Network Monitoring Solution

White Paper

wanstor

Contents

wanstor

Introduction

A high performance network is a basic '*must have*' for a functioning IT infrastructure in any company.

To ensure the business runs smoothly, all IT 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 IT operational processes result in lost staff productivity, higher operational costs and poor customer satisfaction.

A network monitoring software solution which constantly monitors processes in the network, performs analysis and alerts IT personnel as soon as errors occur or critical values are exceeded is highly recommended for IT departments to keep track of the availability, performance and bandwidth usage in an IT network.

Of course, every company has different requirements for a network monitoring solution, and as the market offers numerous solutions, careful selection of a suitable solution for your business is a must.

This white paper shows the various options a network monitoring solution can offer, if the right criteria are considered in the decision making process.

wanstor

Why Network Monitoring?

More and more companies are integrating network monitoring solutions in their IT concepts as they want greater control, visibility and a proactive approach in their day to day IT management.

As well as the operational benefits for the IT department, network monitoring pays for itself in several other areas; it provides enormous time savings for IT staff as they can identify and rectify any problems early with minimal disruption to the business.

It also assists in supporting IT administrators when planning resources for patches, upgrades and improvements to networks internal to or maintained by the organisation.

More time for essentials

A network monitoring solution generally proves itself through early recognition and reporting of errors, malfunctions and exceeded thresholds, and enables the IT department to take immediate action.

Additionally, IT staff no longer have to keep a constant watch over all network components, including servers, desktop computers, applications, traffic and so on.

As the monitoring system is set up to alert IT staff when things go wrong or may go wrong. This means the right network monitoring solution saves valuable staff time, which they can use for other more important tasks.

A recent survey by Paessler (2016) showed that 90% of 724 existing customers indicated significant time saving for IT staff was a key consideration in their purchase of a network monitoring solution.

Additional Security

A monitoring solution also contributes significantly to network security. If solutions report a sudden jump in CPU usage or traffic values show sudden variance, this provides hints to IT staff of possible malware or phishing attacks.

Network monitoring software can be easily integrated into existing security concepts that have virus scanners, firewalls and such, to provide additional security.

Greater control

Such solutions offer IT personnel enhanced control over their estates through comprehensive monitoring of network infrastructure and immediate alerts. Teams have the network under constant observation providing detailed insight into network processes and individual resource usage.

Current status and other detailed data are always available with remote access and mobile apps meaning administrators can manipulate networks when off-site, significantly reducing stress for the entire IT department with 24 hour access to network monitoring tools.

Increased Potential

Reliable trend analysis can be created from the network monitoring software's comprehensive data collection, giving IT personnel deeper insight into their network and enabling them to discover and realise optimisation 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 observance of Service Level Agreements (SLAs).

Financial Savings

Network monitoring solutions have matured significantly in last three years, with large functional ranges being offered for reasonable prices.

This means IT departments can now access best-in-class network monitoring solutions for a fraction of the price they were paying previously.

As the network monitoring market has matured so swiftly, it is recommended IT departments review their network monitoring supplier to whether they are receiving value for money in terms of original purchase and to see if the solution covers all requirements, as data, devices and operating systems change and grow in capability.

Network monitoring solutions can also provide financial savings to a business when they are operational. They can for example help to minimise financial losses caused by delayed failure identification, ensure quicker reactions to reporting error messages and if issues are identified early can eliminate down time significantly.

Classification of Network Monitoring Solutions

Every company, and therefore every network, has different requirements for network monitoring software.

A large number of solutions have been developed by PRTG and Wanstor to cover as many customer requirements as possible.

However, as other providers have started gaining ground in offering a selection of solutions, this means that customers are quite often confused about what is available and what they need.

PRTG and Wanstor can advise your business on what is required and why your company needs a particular solution, so as to avoid overinvestment in licencing or packages or, worse, purchasing entirely the wrong solution.

Despite the network monitoring market offering more choice than ever before the solutions can still be categorised four main types:

Open source, ***Specialists***, ***Enterprise*** and ***All in One***.

Open Source Software

For many IT departments budgets are under increasing pressure. As a result, 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 customisable and can be used with no license cost. A closer look, however, usually reveals 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.

Additionally, a lack of product support is generally provided by the community and advice given has sadly in many cases proved to be unreliable, often leaving the IT department to solve problems and answer questions themselves.

wanstor

All-in-One Monitoring Solutions

The growing importance of professional network monitoring has led to *all-in-one* network monitoring solutions. These offer various general monitoring functions, as well as special features for individual sub-areas - they can control conventional protocols like SNMP, Packet Sniffing and flow protocols for bandwidth monitoring, also providing a wide array of monitoring sensors and protocols (SQL, FTP, HTTP, Exchange, POP3, virtual servers & more).

These solutions can often be installed quickly and easily with professional, reliable manufacturer support, another advantage being the solution is adjustable to growing network structures through scalable licenses, making acquirement costs manageable.

Introductory Monitoring Solutions

Those with a 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 this reduced range, such software is suitable for smaller networks or for an introduction to network monitoring. If the solution must cover a wide variety of machines and bandwidth, 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 specialisation ensures high performance in that area, but is not appropriate for extensive network monitoring.

“Specialists” are generally used by equally specialised 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 building blocks 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.

Selection Criteria for Network Monitoring Solutions

Several basic factors, besides cost of the solution, should be considered when deciding on a network monitoring solution.

For example, the IT department need to think about their existing and planned future IT infrastructure, where problems may occur and what applications need to be maintained, deployed and retired and the associated impact on the network.

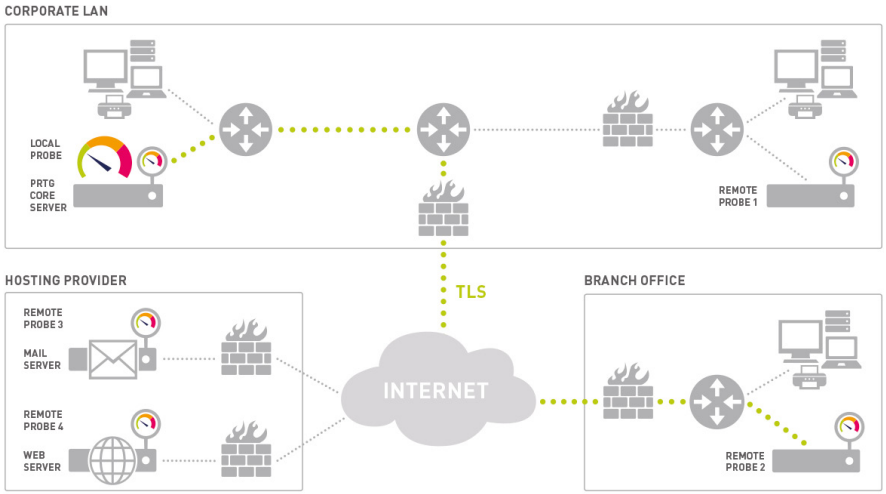

figure 1 : One solution is to monitor the entire IT infrastructure spread over several distributed networks

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 should work automatically after a simple installation, so that it creates time instead of work for the IT department.

Know the requirements

The selection of an appropriate network monitoring system generally complies with size of the network and scenarios to be controlled. These may include servers, switches and workspace computers, as well as network between these and out to external locations and the internet.

Two important areas to be monitored in every organisation are website and email communication. With the former, it's important that general performance and individual components such as shopping areas or forms are monitored in addition to response times.

wanstor

Network monitoring systems are invaluable to companies operating across different geographic regions when analysing and optimising response times from different locations.

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 analysing the entire delivery process, from sending to receipt of an email, using test mails.

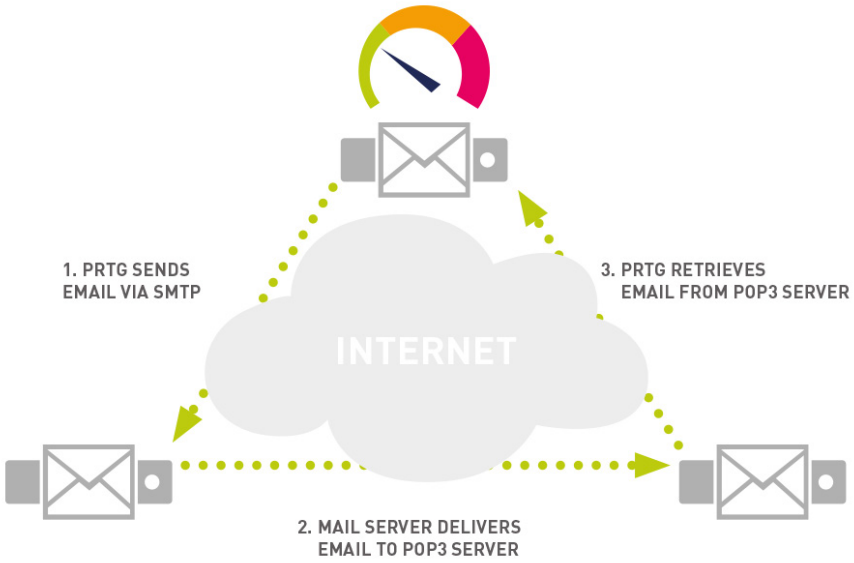

figure 2 : Email round trip sensors ensure the end-to-end delivery of emails

A lack of monitoring experience often results in identifying only limited options of monitoring application in advance. Besides this, networks grow, increasing demand for monitoring. It is advantageous to choose solutions that grow according to 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 trial manufacturer support, so that productive operation can run as free of complications as possible.

Technical '*Must-Haves*'

Bandwidth, usage and availability monitoring are 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 solution offers IT staff information about performance of bandwidth and availability in the form of clear, detailed graphs, reports and lists.

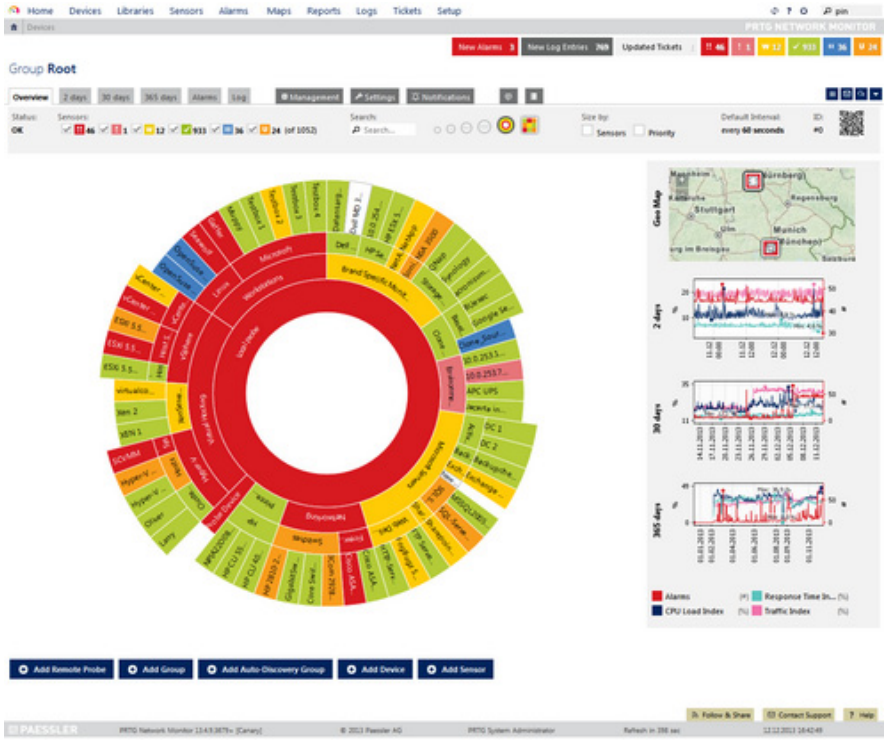

figure 3 : Sunburst view gives a fast overview covering the status of an entire network

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 IT staff, alerting active administrators to existing errors, broken thresholds or device issues. With most solutions alarms can be tailored to suit individual needs so administrators can be reached by email, text message or pager notification, Syslog or HTTP request.

Alternatively, the problem can be rectified automatically with executable files, creating security and ease for responsible parties.

Additionally, IT staff must be able to define dependent actions for alarms as well; if the solution reports a server crash, for example, applications that are connected to this server should not generate independent reports, eliminating floods of redundant alarms.

Integrated cluster functions provide increased security with regard to possible downtimes of the monitoring system by enabling parallel monitoring through multiple instances of the software.

If one or more of these instances fail, the remaining, functional instances assume control and continue monitoring without interruption, protecting users from software failure and guaranteeing 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).

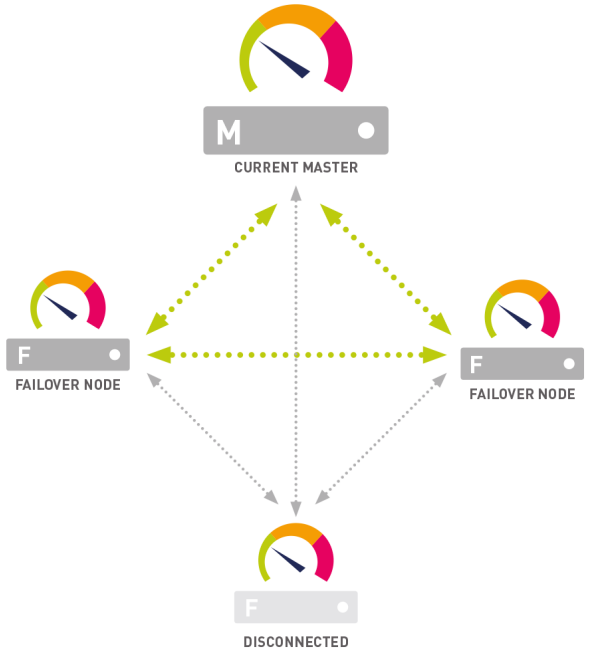

figure 4: The integrated cluster function of PRTG assures continuous monitoring

It goes without saying that a network monitoring service should be user-friendly with clear menus and intuitive operation. Additionally, the user interface should be designed with the user in mind and be available on different types of devices.

As a general rule, automatic network recognition after installation should be a standard feature of the solution. When working with charts and reports, administrators should be able to customise 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 customised as needed.

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 usually a best fit for medium and large sized organisations.

They should also offer a number of upgrade options in case the network expands in the future and have manufacturer support in place at all times.

wanstor

Checklist for the 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?
- Which protocols and technologies support the solution regarding bandwidth and availability monitoring? Are these sufficient for the company's requirements?
- Is centralised monitoring of distributed locations possible?
- What data is collected by the solution?
- How are these evaluated? Graphically or numerically?
- Is there a long-term data archive that would provide the foundation for a trend analysis?
- How does the solution alert personnel in case of emergency?
- Is the solution's structure user-friendly and can it be operated intuitively?
- Does the manufacturer provide sufficient support? (user manuals, blogs and/ or forums) available?
- How transparent is the manufacturer's pricing policy?
- Does the licensing models fit the company requirements?

Summary

A network monitoring solution presents a real cost and time saving opportunity for companies who have complex IT infrastructures. A companies IT infrastructure can only be used to its full potential, when it is attuned to the requirements of the network.

Therefore companies should test a range of network monitoring solutions before they make a final decision to make sure the solution is the right fit for their company both now and in the future. When testing a solution they should consider cost, time, risk and quality of a solution before making an investment.

Wanstor are a trusted independent provider of IT infrastructure services to businesses across the UK. We provide our customers with highly available technology platforms and 24 x 7 IT support. This enables our own customers to deliver a great IT experience to theirs.

Wanstor's partnership with Paessler extends over a decade, with high levels of technical competencies and a wealth of real-world expertise, our customers receive real technical and commercial value from our network monitoring services.

For more information about network monitoring solutions please contact us on **0333 123 0360** or email us at **info@wanstor.com** and one of our network monitoring experts will give you a call back.

Wanstor | 124-126 Borough High Street | London | SE1 1LB |

info@wanstor.com

wanstor