

# Overcoming everyday IT issues with network monitoring solutions

A guide for IT professionals

# Contents

- + Everyday network questions
- + Network needs at a glance
- + Ensuring quality network performance and security
- + Keeping basic systems running
- + Wanstor network monitoring services

# Everyday network questions

On a normal day as an IT system administrator, your colleagues, supervisors, and customers constantly ask for answers to common questions. At Wanstor we often find these questions frequently fall into three categories:

## Network Needs At A Glance

- + Why are my applications so slow and what happened to my apps last night when I left my computer on?
- + When are you going to upgrade our hardware to solve these issues?
- + Why doesn't my Outlook receive any emails?
- + Why do I receive alerts about downtimes of devices although my colleagues are already on a centralised maintenance/upgrade programme?

## Ensuring The Quality And Security Of Your Network

- + Are you sure that our network is really safe and no unauthorized person is accessing it?
- + How can we be sure that our server room equipment is safe from external threats?
- + Are you aware that our website is loading slow and customers are abandoning it at crucial stages in the buying process?
- + Why is the sound quality of phone calls so terrible over VOIP and video streams permanently affected by latency?

## Keeping Your Basic Systems Running

- + Why does our database perform so poorly every morning?
- + Why does my virtual machine crash so often?
- + Can you show me the status of all my different backup solutions at a glance?
- + Why do I always have to call you first when the toner of our printer is empty?

IT Managers need to address these questions quickly and in a comprehensive way to keep users and business trust. In this whitepaper Wanstor's network monitoring experts will give practical advice about the tools you need in place to be able to give definitive answers to the above questions.



wanstor

# Your Network and its Needs at a Glance

## Gain early recognition of potential hardware issues and plan hardware upgrades

Your IT infrastructure needs to be constantly reviewed in order to make sure it is serving the business to the best of its ability. Questions the IT team often ask include:

- + Are there overloaded components, like CPU or memory?
- + Is the temperature of servers acceptable?
- + Are there Windows servers that restart occasionally during the night?
- + Are the IT team aware of issues as they arise or are they continuously missing information that something is wrong?
- + Do the IT team know when hard disks in their environment are near maximum capacity, when memory is running low, or need to be upgraded?
- + Do the IT team understand bandwidth usage and what is actually consuming most of the bandwidth to cause problems?

Knowing the answers to these questions will indicate when it might be time to invest in new hardware resources.

Wanstor works with PRTG to provide IT teams with detailed monitoring data and historical reports about all network components. By analysing these in depth network monitoring reports, IT teams can identify usage trends in order to predict when resources are going to run out or need upgrading.

The reports can also be set to warn the IT team with an immediate notification when something uncommon occurs, like a server outage or when certain values reach a defined threshold. This way, the IT team can take a proactive approach to problem solving before it becomes a business critical issue.

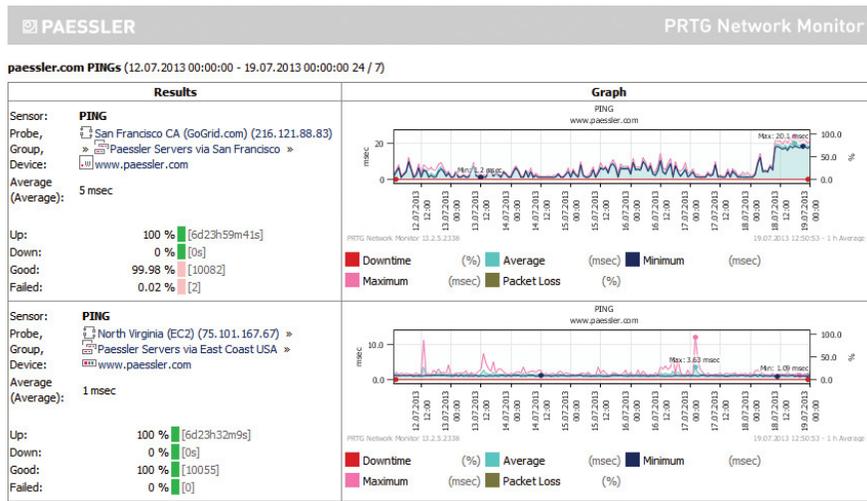


figure 1 : A report for ping sensors

## Automatically Reboot Failing Windows Services And Servers

When monitoring Windows services, if a service on a server fails, PRTG network monitoring tools can send relevant IT personnel a notification by SMS, email, etc. One of the most common methods for recovery is to manually reboot the whole server to get the failing service back online.

The same holds true for occasional system failures. In this case, Windows services will stop, PRTG network monitor recognizes this and sends a notification, prompting IT administrators to reboot. But, wouldn't it be even more efficient if the reboot could happen automatically?

At Wanstor we have worked with PRTG to develop an automated notification system. It simply creates a script that reboots services or the whole system and invoke it to an "Execute Program" notification.

Once configured, if a service or server is down for a defined time span, the script is executed and restarts the service or server automatically, with no intervention.

When monitoring specific Windows services via PRTG's WMI Service sensor, IT Administrators can choose an automatic restart option even if a service is not running.

## Eliminate Useless And Annoying Alerts During Planned Downtime

Sometimes it is necessary to take devices out of operation for maintenance and other issues. Or, perhaps the IT team need to shut down systems for the weekend or at night, or they do not want to be notified at certain times.

PRTG network monitor is designed to notify IT administrators in the event of an outage to maintain maximum system availability, but receiving alerts during planned system downtime is useless.

Manually pausing monitoring of certain sensors in a network is not worth the effort. Fortunately, PRTG have implemented a dedicated feature for maintenance and other planned downtimes.

For every group, device, or any other object, PRTG allows IT administrators to define schedules to limit monitoring time automatically.

This avoids false alarms and eliminates annoying notifications during planned downtime.

The screenshot shows the PRTG Network Monitor interface. At the top, there is a navigation bar with links for Home, Devices, Libraries, Sensors, Alarms, Maps, Reports, Logs, Tickets, and Setup. Below this is a breadcrumb trail: My Account > Schedules > Weekends [GMT+0100]. A status bar indicates 'New Log Entries: 3', '188', '4', '10', '331', '60', and '153'. The main content area is titled 'ScheduleWeekends [GMT+0100]' and has a 'Settings' button. Under 'BASIC SETTINGS', the 'Schedule Name' is 'Weekends [GMT+0100]'. The 'Edit Mode' is set to 'Use weekday/hour time table'. The 'Time Table (active time slots)' is a grid with columns for days of the week (All, Mo, Tu, We, Th, Fr, Sa, Su) and rows for time slots from 00:00 to 09:00. The 'All off' column shows 'off' for all time slots. The 'Sa' and 'Su' columns have checkmarks in all time slots, indicating monitoring is active on weekends. The 'All' column has checkboxes for each time slot, which are currently unchecked.

	All	Mo	Tu	We	Th	Fr	Sa	Su	All off
00:00	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00 off					
01:00	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	01:00 off					
02:00	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	02:00 off					
03:00	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	03:00 off					
04:00	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	04:00 off					
05:00	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	05:00 off					
06:00	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	06:00 off					
07:00	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	07:00 off					
08:00	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	08:00 off					
09:00	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	09:00 off					

figure 2 : Adjustable Schedules

# Ensuring the Quality and Security of Your Network

## Detect Security Issues In Your Network

How can any IT team be sure that the network they are responsible for operating is safe? At Wanstor we understand it is important that antivirus scanners are running on all computers and that they are up to date. We also understand that IT teams must run the latest version of Windows in order to have the latest security updates in terms of patch management.

However, even if your IT team takes great care and has deployed patch updates, antivirus and has a robust IT security policy in place, the reality is you are already under attack you just don't know it yet.

Quite often just examining some basic network behaviour will give the IT team the answers they are looking for. For example uncommon peaks in CPU usage and traffic can indicate a potential attack. PRTG network monitor can detect unusual network behaviour and switches the corresponding sensors to the "unusual" status, alerting IT teams that something may be wrong.

IT administrators can also manually check connections to the network: Are there connections through your firewall from unknown source addresses?

It is always wise to routinely analyse this via the Toplists feature of several traffic sensors to be on the safe side. Another helpful feature for security monitoring is the Similar Sensor Analysis, which can help to recognize strange interconnections between sensors.

PRTG monitors the overall security status like the antivirus software of a Windows computer with the WMI Security Centre sensor and Windows server updates with the WSUS Statistics sensor.



figure 3 : Analyzing connections via packet sniffer

## Keep Your Data Centre Safe

High temperatures, humidity, water leaks, floods, fire, smoke, brightness - there are all kinds of potentially harmful conditions that could damage your server room or data centre equipment. If the air conditioner has an outage, temperatures could quickly rise to a critical point and servers will soon overheat. Since they cannot just cool down automatically, it is important IT administrators are proactive rather than reactive.

Monitoring environmental values is important to make sure devices are safe. By monitoring several hardware sensors for temperature, humidity, etc., PRTG network monitoring solutions notify IT teams in the event of uncommonly high values. For example, if an APC sensor box measures more than 27°C, the applied SNMP Library sensor can show a warning status and notify you to take care of the issue. Perhaps the air conditioner is having a problem? With PRTG and a corresponding hardware sensor cable connected to the air conditioning unit, IT Administrators can check it easily from their computer.

In addition to environmental factors, unauthorized persons can have a critical impact on your infrastructure's security, and of course, should not have access to sensitive areas in the office. Using PRTG in combination with corresponding hardware sensors can help IT Administrators ensure that all observation cameras are running, that all doors and windows are locked, and alert them to any possible problems.



## Ensure Availability And Avoid Poor Performance Of Web Pages

Availability and loading times of web pages are a crucial for any organisation - every business needs its site to be reachable day and night with acceptable performance levels. For online retailers, it is extremely important that site requests work as expected.

If a buying process fails due to technical errors or browsing items on your page is a poor customer shopping experience, this may mean you are losing customers and potential revenue opportunities. The same is true if potential customers or employees browse to obtain information about your firm and the page is unacceptably slow.

PRTG network monitoring solutions helps avoid possible loss of earnings for your company by alerting IT teams immediately if anything goes wrong with their web page, or in the event of unusual behaviour such as slow performance.

Use the HTTP Full Web Page Sensor, for example, to monitor the loading time of the full page, or the HTTP Transaction sensor to measure loading times for performing transactions on an interactive web page. Or, add an HTTP Apache ModStatus Totals Sensor to monitor access and transferred data to identify traffic peaks at specific times. This helps IT teams to identify when it is time to provide more bandwidth.

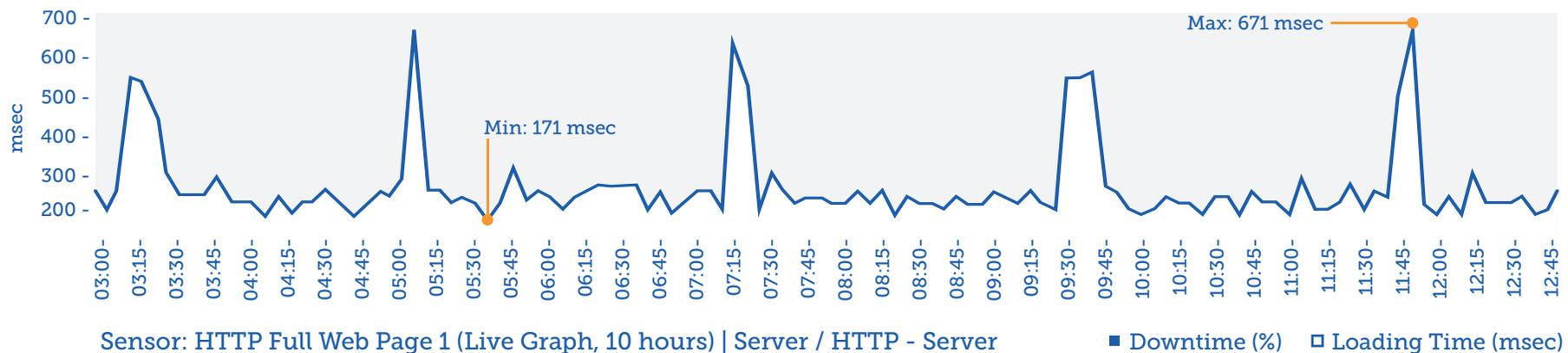


figure 4 : PRTG live graph for loading times of a web page

## Quality Of Service - Resolve Bad Sound/Picture Quality In VoIP And Video Streaming

When the sound quality of Voice over IP (VoIP) calls drops dramatically, or video streaming is interrupted frequently, IT teams need to investigate the relevant cause. Could it be jitter, packet loss, or packet delay variation of the network connection?

Both VoIP and video streaming services rely heavily on a steady stream of data packets, and quality of service suffers if UDP packets are not received in a timely fashion, lost or out of order.

PRTG network monitoring tools can help IT teams find those issues. With the out-of-the-box Quality of Service (QoS) sensor, IT teams can measure the quality of their network connection by sending UDP packets between two remote probes and analysing various network parameters.

IT Administrators can also monitor VoIP-relevant parameters through IP Service Level Agreement (SLA) results from Cisco devices as well.



# Keeping Your Basic Systems Running

## Troubleshoot Poor Database Performance

If database performance is low, IT Administrators need to assess the cause in order to optimize performance. Unfortunately, examining the reason for bad performance of SQL servers, for example, can be a painful task. PRTG's database maintenance support can help. For example, if SQL performance is low at specific times, this might be a result of overly high numbers of simultaneous user connections.

The WMI Microsoft SQL Server Sensors in PRTG can show you the number of user connections and the percentage of pages found in the buffer cache without having to read from disk. If PRTG indicates this number is too low, you can increase the amount of memory available to the SQL server. Or perhaps you send inefficient queries? PRTG measures the response time of queries and can check if the response value is the expected one.

## Resolve Unreliable Behaviour In Virtual Environments

It is important to continuously monitor virtual machines in highly flexible IT infrastructures where virtualization plays a major role. Problems with virtual machines can have several causes, and PRTG provides various sensors to detect and address these issues. Adding a VMware Virtual Machine Sensor to PRTG, allows IT Administrators

to monitor CPU and memory usage of virtual machines via SOAP, as well as the network speed of a single virtual machine. But what if speed is too slow or memory is overloaded on a VM? PRTG also enables you to monitor the host hardware, to detect immediately if problems with virtual machines originate in a host hardware failure.

For example, if the general status of your VMware host is anything other than "normal," the issue will be reported in the sensor message. Because of PRTG's dependencies feature, IT teams can quickly determine if a single VM or the hardware is causing the problem.

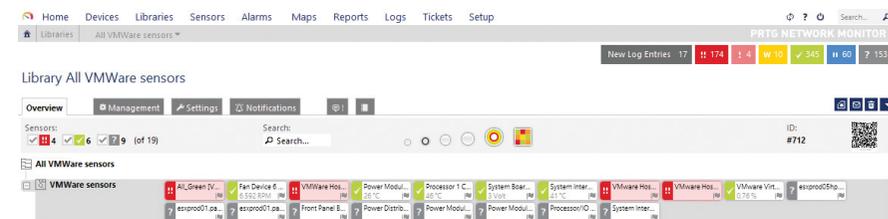


figure 5 : Analyzing connections via packet sniffer

## Ensure Backup Success Quickly And Easily

Virtualization backups. Operating system and complete image backups. SQL and Exchange backups. Tape and online backups. Even in small companies, maintaining an overview of all backups that run in the network can be difficult.

Most backup solutions send emails indicating their status every night, but it is impractical to analyse hundreds of emails every morning in order to identify potential backup problems.

Instead, PRTG sets parameters and alerts IT Administrators to any breaches. Simply configure backup software to send emails to a dedicated email account and then set up PRTG's IMAP sensor accordingly.

This way, PRTG keeps track of all your backups-and you save time while being confident that all backups succeeded.

## Eliminate Time-Consuming Printer Maintenance

As a system administrator, do you really want to waste time manually checking the status of the printers in your IT infrastructure every day? It's also annoying to be interrupted during concentrated work simply because of an empty paper tray in the printer on the floor above.

PRTG provides the solution: use the Windows Print Queue Sensor to monitor all jobs on a print server. If paper is running out, you receive an alert from PRTG and can react before colleagues start complaining. PRTG can even monitor hardware parameters of HP LaserJet printers with a natively available sensor.

The system can send a notification when the toner is low, or, even better, PRTG can automatically send an email to your supplier to bring new toners and exchange the old one.

With PRTG, you can eliminate printer status worries completely, so you can concentrate on more important work.

# Wanstor's Network Monitoring Services

For any business, just one minute of network downtime can result in a poor customer experience, lost revenue and seriously impact staff productivity. Wanstor understands that no two businesses are the same. We offer a range of network monitoring services so you can choose the right mix for your business. Our most popular network monitoring services include:



## Full Network Monitoring

Monitor every aspect of the network; PINGs, traffic, bandwidth, firewalls, routers and switches to make sure they have the right network infrastructure in place.



## Bandwidth Monitoring

Identify potential bandwidth capacity and overloads, and where shortages are happening.



## Hardware Monitoring

Allows the monitoring of all IT hardware at a glance - e.g. Computers, Printers, Servers, Hard Drives, Routers, and Switches.



## IP Monitoring

Allows the monitoring of all IP addresses in your network, even remote and on Virtual Machines.



## Update and Patch Monitoring

Makes sure updates and patch monitoring happens across all operating systems and applications.



## Database Monitoring

Enables datacenter teams to monitor availability, downtime, usage, alerts, Oracle SQL, MS SQL, MySQL, and PostgreSQL.



## Application Monitoring

Allows engineering teams to monitor SQL, exchange and server software, cloud and virtualised applications and other standard business applications.



## Wi-Fi Monitoring

Gives operational and IT teams access to what is happening across a Wi-Fi network, in terms of devices, load, traffic, signal strength, and last access.



## Network Monitoring Benefits

By having the right network monitoring solution in place IT departments can benefit from:

**Early recognition of potential hardware issues**, meaning a proactive approach to IT can take place saving engineering time and costs to repair in the future.

**Detect potential security threats earlier** and put in place anti-virus software and patch management to stop attacks before they harm the business.

**Enable the automation reboots** of computers and other hardware saving engineers time and effort in their daily roles.

**Make sure webpages are always available** and set up alerts if they start to run slowly so customers receive a great online presence whenever they visit your company online.

**Ensure your datacentre is running at the optimum temperature** and is safely accessed by the people at the right time.

**Make sure your business and guest Wi-Fi** has the right bandwidth and user experience wherever users are accessing the service.



# Wanstor Customers Using PRTG Network Monitoring Tools



# Summary

A network monitoring solution such as PRTG Network Monitor helps IT administrators to manage the challenges of everyday IT work. It 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.

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. By having the right network monitoring solution in place IT teams can keep track of the availability, performance and bandwidth usage across the IT network they are responsible for.

For more information about Wanstor's IT Network Monitoring services please contact us on **0333 123 0360**, email us at **info@wanstor.com** or visit us at **www.wanstor.com**.