



Setting Our Sights on Networks

Remote control monitoring software - detects errors and faults in networks and in network devices before anything catastrophic happens. Network Computing has tested four network monitoring products.

Things have moved on since we last tested network monitoring software. Network Computing has experienced completely revised user interfaces, many new functions and new prices. The bottom line is that the products have improved, but some presented deficiencies. The products included in this round of tests were »WhatsUp Gold 14.0« from Ipswitch, »OpManager 8.0« from ManageEngine, »PRTG Network Monitor 7.2« from Paessler and »Orion Network Performance Monitor 9.5« from Solarwinds.

Paessler PRTG Network Monitor 7.2

Network monitoring - simple and intuitive. In the case of Paessler's PRTG Network Monitor, this statement is no empty advertising claim. Network Computing's tests demonstrated that the product does exactly what the manufacturer promises. PRTG Network Monitor supplies live data about the current state of the network and its devices, as well as about long term network load trends. Thorough analyses help network professionals to optimally

configure data cables, routers, servers and other network components. The product is

extremely suitable for monitoring bandwidth, the availability of devices and the utilization of network resources. A particular feature of the software is that monitoring operations are not restricted to local networks or network segments, but also extend to complete enterprise networks, even if they consist of spatially separate segments. This is done using remote probes, which are not only used for monitoring spatially separate networks but can also be used, for example, for load distribution under CPU intensive processes such as packet sniffing or Netflow monitoring.

The remote probes allow users to utilize PRTG for a wide range of applications. For example, the software can be used to supervise customers' networks, to monitor

all branches of an organization or to monitor a company's distributed networks. Even if the networks to be monitored are complex, the use of PRTG Network Monitor is in no way complicated as all the monitoring operations require a single PRTG core server. The product can be scaled for up to 30,000 sensors per installation. That is good news for administrators, but the down side is that for various tasks, new servers, gateways and other devices have to be configured - not to mention what it all costs. As PRTG Network Monitor only has a few components, the installation and configuration of the product is straightforward. The »most« difficult decision the administrator has to take when carrying out the installation is the choice of language (German or English).



PRTG Network Monitor monitors complex, distributed networks with only one PRTG core server. One product installation supports up to 30000 sensors.

A setup assistant provides guidance through the setup process, which we think should take no more than two minutes (we haven't measured the actual time). Afterwards, a welcome assistant starts, which helps the administrator with registration / licensing and web server selection.

The product offers two graphical interfaces: a web and a Windows GUI. Network Computing could not attest that the interfaces (especially the web interface) of earlier versions of PRTG Network Monitor were as elegant and simple as the manufacturer claimed. However, as of version 7.2 at the latest, which was tested this time as beta software, this has changed. Both user interfaces are tidier and are now very easy to use and... Yes, elegant as well.

Especially the web interface really looks first class, and what is more important: it is now made very clear that there is an auto-discovery function available for networks and network devices. An earlier criticism was that some administrators only found the function after most of the work had already been done. Now it has a prominent position on the front page of the web application. It was obvious that we must click on it straight away ... and we were again pleasantly surprised: The local network discovery with an IP address range from 0 to 255 was instantaneous and flawless

Key Facts

PRTG Network Monitor 7.2



Manufacturer: Paessler

Category: Monitoring-Software

Price: 100 sensors US\$ 380.00

Enterprise Site Licence (unlimited number of sensors, probes and core servers) US\$ 8,500.00

Web: www.paessler.com

Plus / minus:

- + Complete package
- + Uncomplicated setup and simple configuration
- + Very good price-performance relationship

PRTG Network Monitor consists of two components: the PRTG server, for data storage and to act as a web server, as well as probes (one or many). The probes carry out the actual monitoring. They connect automatically to the server, download the required sensor configuration and begin monitoring. Data is transmitted to the server using SSL. It is the probes that initiate the connection. Even in the event of

a failure on the server or the connection to the server, monitoring continues. During the installation the program automatically creates the first »local« probe, which runs on the same computer as the PRTG core and monitors all the system sensors.

This single probe is sufficient for LAN monitoring if the monitoring is restricted to

a single location. Some configurations require multiple or external probes:

- Monitoring more than a single locality,
- Subdivision of a network into multiple LANs using firewalls (if the local sensor is not capable of monitoring through firewalls),
- Monitoring of systems in VPNs via public connections,
- Packet sniffing on another computer,
- Monitoring of Netflow data from another computer,
- When using CPU intensive sensors and thus associated performance limitations.

This is not a problem, as creating external probes with the »probe administrator« is quick and easy. The PRTG server is first set up to permit connections to external probes because, for security reasons, the default allows this only via the local host.

However, this setup takes next to no time. Sensors, device groups and devices are structured hierarchically by PRTG Network Monitor. This eases the task of the administrator and simplifies the configuration. For example, the administrator does not need to configure the login information for each device as this can be derived very easily from higher order entities such as groups or the root object.

What is the use of a monitoring product if nobody takes any notice when it has something to report? The PRTG Network Monitor now provides distinct acoustic and optical indications of new alarms, warnings and other messages. Someone failing to notice these signals would have to be both deaf and blind. On investigating a message or a selection of messages from a sensor, the program provides very good explanations regarding what individual values and the adjustable parameters actually mean. Here we can attest that the product is a role model.

Paessler has incorporated more than 500 improvements and modifications in version 7.2. Many of these improvements affect the user interface, including: Use of both GUIs on several computers, connection to PRTG core server via HTTP/HTTPS, display of device trees, an alarm list, maps and reports, comparison of live data and graphical historic data tables from two or more sensors. The new Windows GUI for the management of sensors is quicker and easier to operate, which is especially noticeable with large installations (500 sensors and above).

The product also contains more sensors than before. New additions are QoS, IP-SLA, Amazon Cloudwatch, Radius Server , Syslog , SNMP Trap and MS Exchange 2007 sensors, as well as sensors for servers running MS-Hyper-V, support for sFlow and Netflow 9 and also detailed monitoring of Exchange 2003.

Network monitoring - simple and intuitive. Paessler's PRTG Network Monitor 7.2 certainly fulfils these administrator requirements. The product is really easy to install, allows flexible use, provides good messages and explanations and is attractively priced. Not a single problem arose during the test.

Ipswitch WhatsUp Gold 14.0

WhatsUp Gold is a product that is widely used for monitoring in Windows and TCP/IP networks. The software runs network discovery, monitors network devices in real time, executes automatic actions if the status of a monitored device changes or a threshold value is exceeded, generates reports and alerts administrators. The product is highly scalable and offers extensive functionality.

However, before purchasing the product, one should consider thoroughly which functions are actually required and which

devices or networks are to be monitored as WhatsUp Gold is available in four editions. These editions vary in terms of performance, in their range of functions and, of course, in price. This makes selection difficult. Those looking for a product that is, for example, equivalent to PRTG Network Monitor cannot do much with the entry product WhatsUp Gold Premium as this does not support distributed monitoring. Those requiring more functionality must consider WhatsUp Gold MSP or the Distributed Edition and, of course, hand over more money.



The top ten views in WhatsUp offer administrators a good overview of the state of the network and the network devices

Let's take a look for a moment at the direct comparison with PRTG - as this is a comparative test after all. The setup for WhatsUp Gold requires considerably more time and planning. This is primarily because a Microsoft SQL Server has to be installed if one is not already available. At least the WhatsUp setup routine offers to install Microsoft SQL Server 2005 Express Edition if it fails to find any other SQL server. A

further issue is that the set up program initially only installs the WhatsUp Gold Central Site Edition and the Dashboard Screen Manager. To enable full use of the product on computers in remote locations, WhatsUp Gold Remote Site Edition also needs to be installed. This all seems so unnecessarily awkward but it could be made so easy - Paessler shows how it's done.

As soon as the software is running, it starts to find devices in the network. Network discovery was available in earlier versions and gave no reasons for complaint but further enhancements have also been made in version 14. The product comes with a new discovery console and a discovery web interface, as well as an improved discovery engine which correctly identifies network devices. The manufacturer states that the new discovery engine is up to four times faster than the old one. This cannot be tested, but it was found to be fast.

Administrators can also predefine the roles of devices, which means monitoring can be initiated more rapidly. The program offers numerous discovery options, including IP Address Range Scan, SNMP Smart Scan, Host-Data Import and scanning of individual devices. The IP Range and SNMP scans used in the test functioned reliably. Already during the discovery operation the program used active monitors to find, amongst other things, DNS, NNTP and TCP Echo Servers as well as applications communicating via protocols such as HTTP, HTTPS or POP3. The administrator can also immediately

select performance monitors, which the program uses during the scan process as well as later on.

The monitors provide the administrator with guidelines describing a range of actions which are to be carried out as soon as a device experiences an error. For example, when WhatsUp Gold identifies an error it sends an email message, plays a defined sound or opens a pop-up message on a selected computer.

WhatsUp Gold actively polls devices in the network to determine changes in status. For this purpose the program uses the pre-configured monitors or the monitors created by the administrator. Performance monitors observe device resources, such as discs, interfaces and memory. Regardless of the answers obtained by polling, WhatsUp Gold performs actions such as informing the administrator or restarting a service. A plus is the new alert center that consolidates alert notification displays and simplifies the management of message guidelines. In this way, administrators are always informed about what is happening within their network.

Key Facts

WhatsUp Gold 14.0

Manufacturer: Ipswitch

Category: Monitoring-Software

Price: between US\$ 2,425.50 (Standard Edition, up to 100 devices) and US\$ 11,695.50 (WhatsUp Gold Premium, up to 2500 devices, incl. WMI-capability).

Prices without optional plug-ins. Prices for more than 2500 devices on request.

Web: www.whatsupgold.com

Plus / minus:

+ Highly scaleable

+ extensive functionality

- Edition and add-on range offers flexibility but makes product selection more difficult

- Requires the Remote Site Edition in remote locations

However, the alert center does not provide as thorough explanations as the equivalent feature in PRTG Network Monitor. Ipswitch has added various new active monitors to its product, including monitors for APC-UPSs, Exchange-2007 and 010 (Beta 1), fans and network components, temperature, FTP and HTTP content. WhatsUp Gold now supports Cisco and Juniper Netscreen CPUs

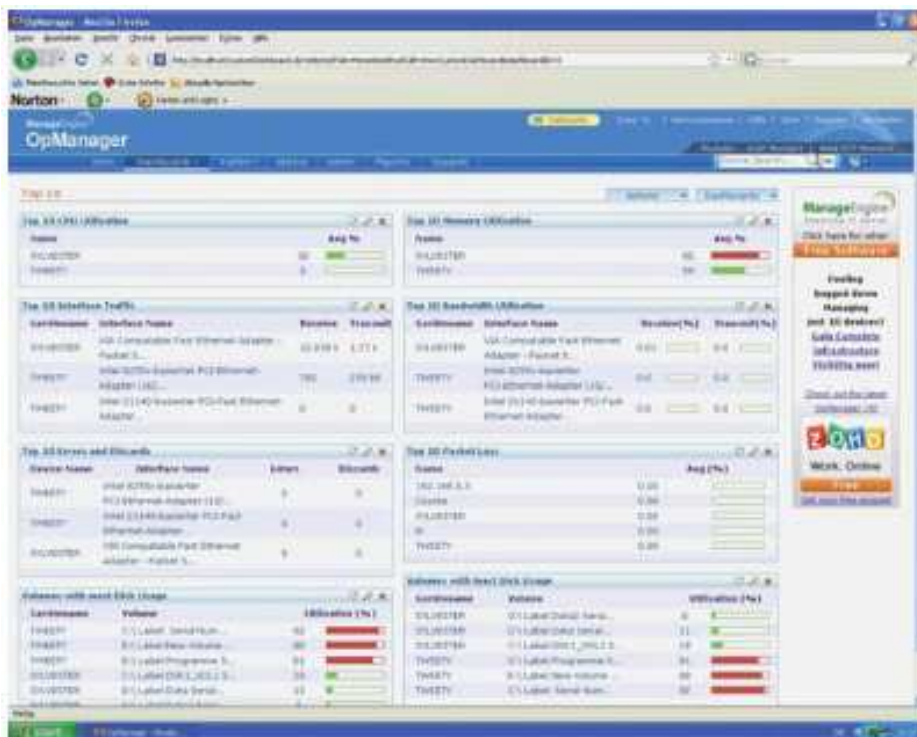
as well as memory performance monitors, Microsoft SQL Server 2008, Vmware-ESXi 3.0 and higher, Microsoft-HyperV Server 2008 sFlow and J-Flow. Various fixes have also been included. More functionality, such as bandwidth monitoring, VoIP monitoring and Layer 2/3 mapping are, as before, available as optional plug-ins.

ManageEngine OpManager 8.0

ManageEngine, as the name of the firm suggests, specializes in management applications. OpManager, the network monitoring software from this manufacturer, is the first choice of over 700,000 network administrators in 93 countries according to the supplier. It is, however, not our first choice.

very capable as regards monitoring networks, network devices and services, as well as being able to detect performance weaknesses, alert administrators and generate reports, but it is very difficult to set up the software to do exactly what an administration requires. There are a number of products that make things considerably easier for the user.

The product is on the whole efficient and



The web interface of OpManager uses widgets and is highly adaptable, but does not work flawlessly with every browser. It performed best with Mozilla Firefox

It is difficult enough to decide between all the OpManager editions on offer and to make selections from all the available add-ons and plug-ins. With ManageEngine it is not easy to determine which editions already contain the desired extensions. Thus it is not always possible to determine the total price. Naturally it is pretty cheap to get started - the simplest edition will monitor up to ten nodes for nothing (but for a maximum of ten nodes is probably unnecessary). On the other hand, for extensive features and for unlimited use in a WAN or for carrying out distributed monitoring, one needs to come up with at least 6495 dollars. This price is valid for monitoring up to 250 nodes. As before, it is

not entirely clear which add-ons and plug-ins this Enterprise Edition already contains or which extra ones have to be purchased. In order to be clear what we are talking about, the list of add-ons and plug-ins includes a Cisco IPSCA monitor, a WAN monitor (which is supported by Cisco IPSCA agents), a Netflow analyser and NCM plug-in, a VMware monitor, an Exchange 200/2003/2007, an active directory and a MS-SQL monitor.

The program setup for the test lasted around five minutes and required little input from the administrator. OpManager uses a Microsoft SQL server or MySQL as its database. The latter includes ManageEngine, which is a good thing.

Key Facts

Op-Manager 8.0

Manufacturer: ManageEngine

Category: Monitoring-Software

Price: US\$ 1,995.00 for Professional Edition (up to 100 devices), US\$ 27,995.00 for Deluxe Edition (up to 2000 devices). Prices without optional add-ons and plug-ins. Prices for more than 2000 devices on request.

Web: www.manageengine.com

Plus / minus:

+ Nice, highly adaptable user interface

- A lot of manual configuration required

- Incorrect device classification

After the starting the web client, the program wants to execute an auto-discovery. OpManager supports automatic discovery and smart classifications for devices and interface templates, mass imports and process templates. For the first discovery a little manual input is required. The administrator must, for example, choose the services to be discovered from a list including DNS, web, SQL, HTTP and POP, and then specify an IP range. The subsequent discovery process was very time

consuming and that was only for a sub-network with a range of 0 to 255. During the first discovery run, the system hung up for unknown reasons. In the second run the routine went right through to the end, discovered some devices, but not all, and falsely classified others. The software, for example, failed to find a WLAN access point, classified a routine incorrectly as a server and a switch as a desktop. These errors can be fixed, but other test candidates

demonstrated that such errors must never occur.

The generally visually pleasing and easy to use web client application uses Internet Explorer (Version 8 on the test machine) as standard. With this browser it does not run particularly fast. This was the least of the problems though. The application makes great use of widgets, which is ok in itself and allows the administrator, for example, to configure the interface as desired. However, a downside is that clicking on such a widget to open, for example, infrastructure snapshots, results in the view staying open for just a couple of seconds and then closing again. What is the best way to work? A test with Google Chrome looked to be promising at first, until it was found later that some of the windows were opened at the edge of the browser and the complete content of the window could thus not be seen. The button to close the window could not be reached in many cases. As moving a window or scrolling within it did not work, the use of Google Chrome was discontinued. Satisfactory results were only achieved with Firefox.

Without administrator intervention, OpManager initially monitors almost nothing. Nearly all the monitors have to be

Orion Network Performance Monitor 9.5

Orion Network Performance Monitor, in short Orion-NPM, is a tremendous package for which one must pay a tremendous price. That is not meant purely in terms of hard cash, but also relates to the complexity of the products and the patience required during setup. As the product description leads one to suppose, Orion NPM concentrates on monitoring network performance. If an administrator also wants to look at the performance of the network applications or manage the network configuration, a different product or module is required which naturally must be bought

initially configured and have devices assigned to them. Happily though, this process is simplified by using templates. Those who make the effort finally end up with a system with good fault management, performance and device monitoring. The program produces plenty of real time graph displays and historical reports about availability, utilization, response times and inventories. WAN monitoring is limited to the monitoring of availability of WAN links, as well as the provision of reports on performance analyses and capacity planning. An administrator can only obtain full functionality with the optional WAN monitor add-on.

The alarm system is basically alright although it is a bit sluggish. However, the program rarely provides information about alarms, adjustable parameters, etc. Administrators must have a good knowledge of the system in order to put the product to its best use.

During setup, German was selected as the language. This resulted in a mixture of English and German terms appearing in the user interface.

separately. Only with optional extras is Netflow traffic analysis, IP address management and IP-SLA management possible.

A standard installation is ok for monitoring up to 1000 nodes. The product is basically highly scalable even beyond that. That means that it grows in conjunction with the network. However, there is a price to pay for this scalability, which in this case means the installation of additional standby engines, numerous polling engines and/or additional web servers. For distributed networks with

adaptable as, for example, the version from ManageEngine, although other problems arose with this interface. As well as the two user interfaces, numerous other applications appear after installation in the Windows start menu which include options for adapting the Orion NPM installation or the maintenance of the database.

The alert system is flexible, worked flawlessly during the test and is relatively easy to use. As with other products, Orion NPM generated alerts when an event occurred or a threshold value was exceeded. Regarding the action to take in the case of alerts, the program offers many options, including the usual reporting options, automatic script or program execution and an escalation sequence. Configuring network alerts is no longer difficult. The product allows the administrator to define device dependency and to configure alerts

for related events and/or persistent states lasting over a defined period of time. With this feature the system can, for example, be adjusted so that it will not immediately create an alarm if CPU utilization exceeded 90 percent, especially if the higher utilization lasts for only five minutes. Version 9.5 of Orion NPM contains (free of charge as is emphasized by the manufacturer) a wireless poller for monitoring autonomous access points and their clients.

This allows the product to support wireless devices in the alert system, in reports and in top 10 lists. The product also supports Cisco Energywise Monitoring. In order to undertake energy management, the administrator must execute a few more additional operations: execute a readiness report, possibly update some IOS devices and then select energy guideline options.

Key Facts

Orion Network Performance Monitor 9.5

Manufacturer: SolarWinds

Category: Monitoring-Software

Price: 100 elements US\$ 2,475.00, unlimited elements US\$ 20,975.00.

Prices are without options such as Enterprise Operations Console or scalability engines.

Web: www.solarwinds.com

Plus / minus:

+ Flexible Alert System

- Lengthy setup

- Price

- In large distributed networks additional scalability engines may be required

Final Result

Monitoring suitable for enterprise networks does not have to be extremely expensive nor very complicated. With PRTG Network Monitor 7.2, Paessler provides a complete, highly scalable and user-friendly product at a price one usually associates more with entry level software. However, our test

showed that the price is deceptively cheap as, of all the products tested, PRTG Network Monitor 7.2 was in fact the most comprehensively equipped monitoring package and also the simplest to use. A simple and clear pricing scheme does not

conceal anything and facilitates product selection.

Of course, as with the other three products, the functionality on offer by PRTG was only achievable with the aid of a separate product, add-ons or plug-ins. In the best case, this only makes the installation, configuration and operation more difficult. What is worse is when, after large scale introduction of the product, it is found that the selected edition cannot undertake a critical task. »No problem«, many manufacturers would say. »For that we have our I-can-also-do-that plug-in«. Ok, what is perhaps required for the functionality is perhaps not a problem. But such plug-ins almost always cost money. And justifying doing so in retrospect, at a greater or lesser expense is certainly problematic for many IT experts.

From all these points of view we can only advise those who are looking for a good monitoring product to write PRTG Network

Monitor right at the top of the list of products to look at. For Network Computing this product is, as previously, still the »Reference«.

Except for Op-Manager, all four products tested ran smoothly after they were first installed and configured. The browser problem with OpManager was solved, and if the odd falsely classified device is a major error or not is a matter for each individual administrator. WhatsUp Gold, with options and add-ons, is equal to PRTG Network Monitor and is probably even better with the final layer of functionality added. However, the product is then very complex and more expensive. In direct comparison to PRTG, the price-performance relationship is not great. That is also the case with SolarWinds' Orion. For the price that SolarWinds is asking I would have expected a lot more.

dj@networkcomputing.de

Network Monitoring

Reportcard

	Weighting	Paessler PRTG Network Monitor 7.2	Ipswitch WhatsUp Gold 14.0	ManageEngine OpManager 8.0	SolarWinds Orion Network Performance Monitor 9.5
Features and functionality »out of the box«	25%	5	4	4	3
Ability of monitoring distributed networks	25%	5	5	4	3
Setup and configuration	20%	5	3	4	2
Usability	20%	4	4	4	3
Price	10%	5	4	3	1
Total result	100%	4,80	4,05	3,90	2,60
<p>A ≥4,3; B ≥3,5; C ≥2.5; D ≥1,5; E < 1,5; The ratings from A to C include a + or a - within their ranges</p> <p>Total results and weighted results are based on a scale from 0 to 5.</p>		A+	B+	B	C



TEST PROCEDURE – MONITORING SOFTWARE

The products were installed in a network containing a number of Windows server 2008 machines, an exchange server and an SQL server. The devices were connected in the network via fast Ethernet switches and a WLAN router, and a connection to the Internet was achieved using an ADSL router. The client machines operated with various operating systems such as Windows XP, Windows Vista and Linux. The services and protocols used by the network included TCP/IP, DNS, POP3, SMTP, IMAP, SNMP, HTTP, HTTPS and FTP.

After initial installation and configuration of the monitoring program, we let it investigate for a time to collect information about the installed services and protocols. Finally, threshold values were set and the actions to be performed were defined. It was investigated whether the program recognised and reacted as expected if threshold values had been exceeded, if there had been changes in system conditions and if drops in performance occurred. The items evaluated included the price-performance ratio, user friendliness and also how the product supported monitoring in a spatially distributed network.