A completely revised monitoring solution for corporate environments

Dr. Götz Güttich

Paessler has outfitted their network monitoring tool 'PRTG Network Monitor' with a new web GUI and an impressive selection of new functions. In our test, we looked at how the current version of the software works in operation, and at the advantages of the changes and new features in the software.

Paessler's PRTG is a tool used to monitor IT infrastructure. The solution is not only suited for use in local networks, but is designed to monitor WAN connections, websites, servers, URLS, etc. The product runs on a Windows system and collects usage data from the network components – that is, applications, computers and other network devices, like routers – without using agents. The systems that should be monitored are found and added to the PRTG database either automatically using a network scan, or they can be set up manually.

The monitoring tool saves all collected data for evaluation and analysis for one year. This time frame can, of course, be adjusted as needed.

PRTG's web GUI is the heart of the product. With this interface, administrators have constant access to the full service range of the monitoring solution, independent of the client system. They can manage their system, activate new monitoring components, create reports and analyze results, warnings and alarms.

Various network protocols are used to collect data, including jFlow, NetFlow, sFlow, SNMP, WMI, etc. PRTG also uses packet sniffing to keep an eye on traffic data. The monitoring itself is done using so-called 'sensors' – data evaluation routines that deliver information regarding statuses of specific services and systems. In total, Paessler's PRTG includes more than 180 types of sensors, which cover all normal network services. If an aspect cannot be covered by one of the existing sensors, the product offers easy-to-use interfaces – called custom sensors – to expand the monitoring routines.

Multiple sensors can work on a single monitored component (a server, for example), each of which has a specific task. Dependencies can be defined between the sensors. For example, a ping sensor checks whether the device in question is available, while other sensors (that only run when the ping sensor gives the OK) monitor parameters like the hard drive or RAM usage, CPU load, network traffic volume, the status of the installed anti-virus solution, or

the status of the HTTP service running on the server. In this way, PRTG determines that the administrator isn't swamped with error messages from all sensors if a system crashes; only the ping sensor will inform him that the system is not available. This improves clarity and significantly reduces the reaction time needed to solve the problem.

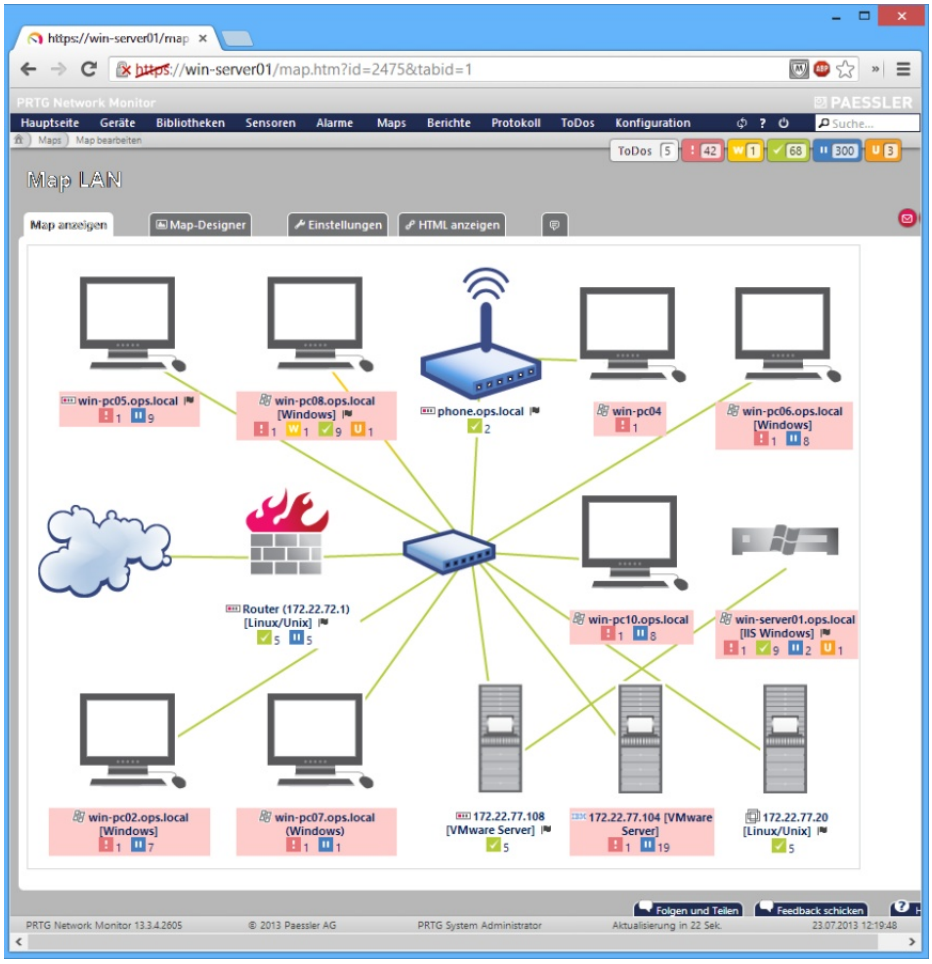
Sensors can be arranged in various ways to increase the clarity of the overview. These can be organized according to the associated device or according to type, day, category or priority.

For example, all CPU sensors in the network can be collected in a library, which allows staff comfortable monitoring of specific problem areas.

The sensors themselves contain channels, which provide detailed information on the related sensor. For a CPU load sensor, this might be the load of individual cores, for a network load sensor, this might be the outbound and inbound data traffic or the number of transferred packets.

Comprehensive ‘maps’ and the report, log and alarm functions round out PRTG’s service range. The maps enable IT staff to create customized overviews of their network. The entire network is displayed in a schema containing symbols and graphs, which represent the individual components. The maps can also contain background images that display, for example, where a specific computer or printer is located.
PRTG is available in Chinese, German, English, French, Japanese, Dutch, Spanish, Portuguese and Czech. Besides the web interface, a Windows application – which can be used to manage multiple PRTG installations – and apps – for Android and iOS – are also available for the product. A special mobile web interface is available for other mobile systems.

A PRTG installation can be distributed over multiple systems. The data is gathered using ‘probes’, which can run in diverse networks and can therefore gather information from remote servers as well as servers within the company headquarters.



If the administrator wishes, PRTG presents a graphic overview of the network after login; the start page can be freely defined

New Features

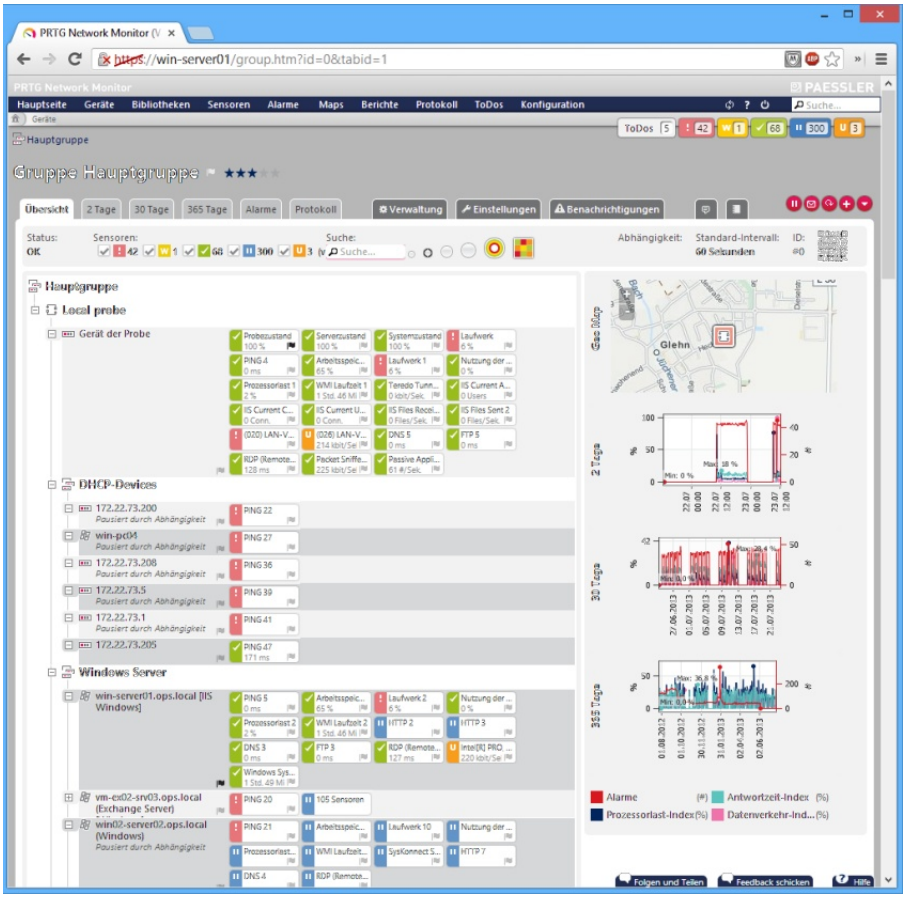
A new web interface and revamped mobile web GUI are some of the new features in the current PRTG version. The new web interface is a single page application (SPA) and works faster than the previous version, loading all settings in layer popups, so that users never lose the context of their work. The number of views has been increased as well, and an improved overview of the individual devices now contains an extra display for especially important sensors.
The page containing the overview of individual sensors has been reworked. The sensor data is now portrayed in a graph with a speedometer-like display. This not only shows the current sensor values, but also displays the thresholds defined for each entry. Even the dashboards including an overview page (more on that later) and the device tree have been revamped.

The page for comparing multiple sensor values has been expanded. Now, values from up to 32 different sensors can be compared over a time period of up to a year. This used to only be possible with two sensors. The Paessler Blog has been integrated in PRTG as well, and presents the newest changes via an RSS feed on the login screen. The mobile web GUI has been given a new look and feel and is now easier to read.

In addition to the improvements made in the interfaces, PRTG

IAITested

now runs on a 64-Bit operating system as a native application. The 64-bit PRTG version runs on servers with more than 6 GB RAM and eliminates the 3 GB barrier common to 32-bit



The device overview is the core of the monitoring tool

operating systems. This improves stability and performance for large installations. On top of this, further functions for analyzing similar sensors are available. This enables the monitoring solution to recognize similar sensor data automatically and display any 'hits' in the sensor overview. This feature works independent of the sensor type and is based on heuristic calculations. We'll cover that in more detail later. The new features also include a new Android app.

New Sensors

The current version of PRTG includes several new sensors. The first of these is the Passive Application Performance sensor. This sensor analyzes network application performance using packet sniffing and measures the timing between client queries and the respective server's response time.

The new hybrid sensors use Windows Performance Counters to query data from the target system and only use WMI as a fallback. This should improve performance and can be activated in the device settings. New sensors for hardware from Cisco, HP and Dell, as well as sensors for the Microsoft System Center Virtual Machine Manager (MSCVMM), diverse protocols, etc. have been added as well.

The Test

We installed PRTG on a 2012 Windows server with a 2.8 GHz quad-core, 4 GB RAM and 780 GB hard drive capacity. According to the manufacturer, the system runs on any hardware with the performance characteristics of a regular PC from 2007 or later. PRTG works on operating systems with all Windows client and server versions since Windows XP and the manufacturers recommend Google Chrome, Firefox, Safari or Internet Explorer from version 9 for the web browser.

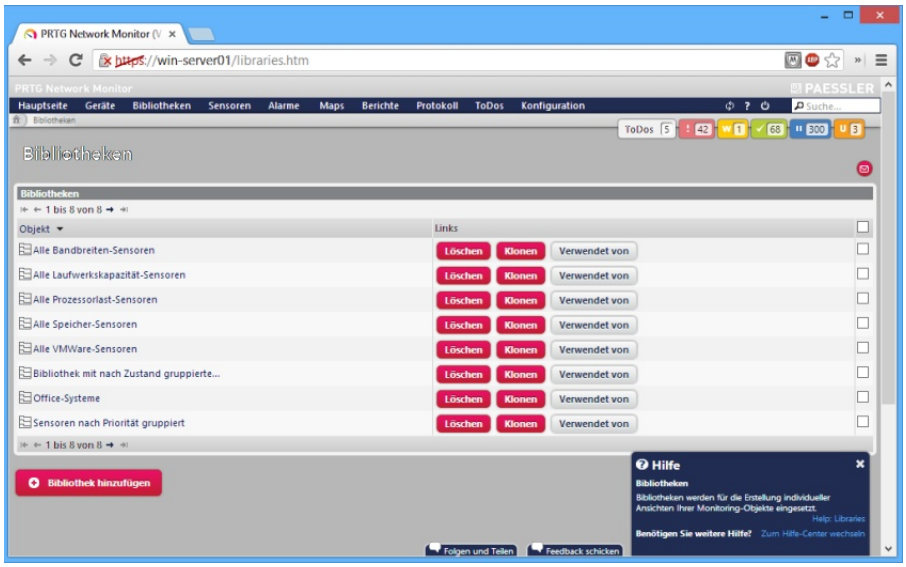
After installation, we executed a network search and added the systems in our heterogeneous test system to PRTG. We then let the solution collect data over a period of several weeks and introduced the product as a monitoring tool for our network. We used the device overview, the libraries, a variety of sensors, the maps and reports. We tested the alarm function and took a look at the logs and 'to do' lists. In all of these areas, we paid special attention to the new functions, giving them extra weight in the test.

Installation

Installing PRTG is as easy as downloading the setup file from the manufacturer's website and executing it on the future PRTG server. The installation runs using an assistant and doesn't present any insurmountable difficulties.

After completing the setup, a browser window opens automatically, displaying the so-called Configuration Guru. This helps the administrator to set up the solution. The Configuration Guru presents a total of ten steps, which can be executed individually or consecutively to create a functional initial

configuration. The administrator first sets up an administrator account to access PRTG and then logs in with his Windows user data. This login information will be used by PRTG to log in to the Windows computers that should be monitored, to query WMI data and the like. In the next step of the Wizard, login data for SNMP, VMWare/Xen servers, as well as Linux, Solaris and OS X systems can be entered as well. After completing these steps, the Guru offers to monitor the Internet connection. Here, the administrator just has to enter the standard gateway and the DNS server. The next configuration step helps to set up system monitoring in the LAN. The user can enter the addresses and/or names of the active directory or exchange servers. If necessary, it is also possible to enter names and IP addresses of additional servers, which PRTG then inserts into its database. Further steps help to configure monitoring for websites, online shops and cloud services (Dropbox, Facebook, Google search, Google Drive, Google Mail, iCloud, Microsoft Office 365, Salesforce, Skype and Twitter). Lastly, the Guru offers to search the network segments for devices. PRTG analyzes each device found and inserts the appropriate sensors. In our test, we tested this method using several sub-networks and noticed that the monitoring solution found all existing components and furnished each of them with the appropriate sensors. In some cases – for example, with our SQL server – we had to add some sensors manually, as the related machine was (correctly) recognized as a Windows computer and was assigned the typical Windows monitoring sensors accordingly, but was not assigned the SQL server sensors. In general, however, the Configuration Guru sets up an initial configuration that provides a solid foundation for IT staff to build on. Only in a few cases it is necessary to make manual corrections, which could also be processed using a template, if necessary.



Sensors that belong to a certain type can be grouped via the libraries

PRTG in Operation

After the Configuration Guru was finished, we first switched to the overview page. The PRTG interface features a menu bar at the top of the screen, which branches to the various subareas of the solution. The home page provides various overviews that display data in condensed form. Alarms, to-do lists, data from the most important sensors, a device tree, etc. are included on this page. Alternatively, the user can define any other page (e.g.: a map) as the home page, so that it appears directly after login.

The second menu item branches to the device overview. This shows all available network components in a tree structure with the respective sensors. Here, the user can view sensor data, combine sensors into groups (to improve clarity), and much more. A geomap shows where the currently selected devices are located.

Contrary to the overview, the ‘Libraries’ contain thematically sorted sensor collections, for example all bandwidth or memory sensors. Customized libraries can be set up to meet the administrator’s specific needs.

The sensor overview provides administrators with a list of all sensors in the network. Sensors can be added in this view as well, and important sensors can be marked as ‘favorites’. The sensors can be sorted according to groups or types, historical data and various lists can be displayed (with fastest and slowest systems, best availability, slowest websites and so on), and sensors can be compared with each other, as mentioned above.

The ‘Alarms’ menu item shows a list of all alarms that have occurred. Errors, warnings and unusual occurrences can be viewed here as well. The ‘Maps’, on the other hand, present the

graphic display of the network structure and the 'Reports' enable administrators to create or define reports. Paessler provides standard, preconfigured reports, presenting the fastest and slowest HTTP and Ping connections, an availability report and the like.

Important sensors are displayed large in the sensor overview for a device

Over the 'Log', the users see messages from PRTG. These can be filtered according to groups and status events or changes. The 'To-Dos' contain system messages that must be confirmed by the administrators. These include to-do lists, reports, automatic network searches and errors. For instance, PRTG uses this method to notify the administrator that a new sensor was created during an automatic network search.

Lastly, the 'Configuration' encompasses all options necessary for managing PRTG itself, such as software updates, schedules and a status page. The license management and the 'Chrome Desktop Notifications' are found here as well, over which messages can be displayed on the user's desktop (provided there is an active connection) via the Chrome browser. This functioned smoothly during our test.

New Web Interface Features

As previously mentioned, we paid special attention to the new functions in PRTG for this test. In light of that, the updated web interface was the most important portion of the test. The web interface is now a single page application (SPA), which is the newest generation of AJAX technology. When calling up new content on an SPA, the browser doesn't reload the entire page; only the required section is loaded. This reduces unnecessary computing time and accelerates working with the system. Because of the introduction of SPA, PRTG now displays all dialog fields for object settings as popup layers. That way, users no longer lose the focus of their work when performing actions like changing tags or adding notification triggers. Instead, after performing one of these tasks, they are immediately returned to the position they started in.

Paessler has also reworked the interface so that more information can be displayed in a smaller space. The majority of the changes are found in the sensor data display. Numbers and current sensor values are no longer presented in text form. Instead, graphical displays of the current live data are shown in the previously mentioned speedometer gauge. This makes it easier to differentiate between and manage the channels belonging to the sensors. The top of the sensor window now features a colored bar, which shows the status of the sensor at a glance (green, yellow, red, etc.).

The Netflow, sFlow, jFlow and packet sniffing sensors now have top lists. These provide information on the top 'talkers' in the network, the top connections and top logs. The data collected by these sensors are – just like the values of the other sensors – shown in a graphical display on the sensors overview page. The user can create customized top lists as well, based on IP addresses, ports, MAC addresses, logs, etc. The device overviews show the sensors belonging to a device in various sizes. The most

important sensors are shown larger than the others. To improve clarity, the colors of the graphs have been modified as well. The values displayed are now easier to identify.

server in another department displays a high processor load. These things aren't noticeable in daily operations, but may contribute important information when solving network problems.

The overview of individual sensors presents a broad spectrum of information to the administrator

Similar Sensors

The new heuristic sensor comparison examines all sensor data collected over the last 30 days and compares each sensor included in the system with every other sensor. This makes it easy to find correlations that aren't obvious at first glance. Similar sensors and their channels appear on an overview page in the sensor menu and on the affected sensor's page as well, so that the corresponding information catches the user's eye. For instance, this information may indicate that a high volume of data transfers always occurs on a switch at the same time that a

The similar sensor tool also gives IT staff the chance to remove redundant monitoring measures from their PRTG configuration.

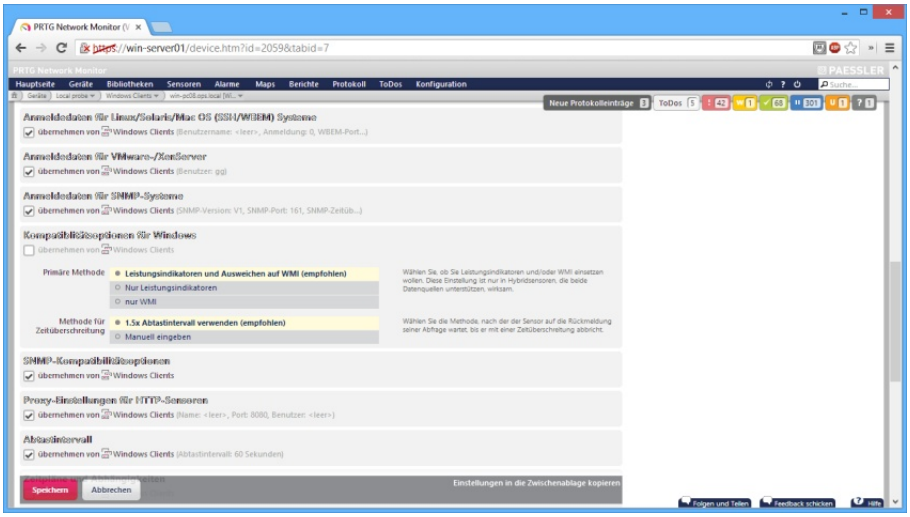
Further Innovations

With PRTG, it's always been possible to define certain sensors or devices as favorites and to include them in an overview with the most important components. This function has been expanded on in the current version. The 'favorite' status and priority can be modified at any time – in the device tree, for example. PRTG then uses this information to adjust the display size and order of the individual sensors for the device's overview page. This also ensures that administrators see the most interesting information first. Also worth mentioning: the Passive Application Performance sensor, which is still in Beta status. This sensor enables response time monitoring from servers and services where the IT department doesn't have access to the server or the client. Instead of reading out traffic and usage information from the device or service, the Passive Application Performance sensor uses the packet sniffer function to check all TCP packets that are sent to and from a server. This method determines how long the round trip takes for the TCP packet and uses those values to measure the performance of the service. The new sensor is suitable for use with various protocols, including IMAP, POP3, SMTP and SOAP.

Administrators who want to use these sensors must first determine that the PRTG server – or the corresponding packet sniffer – is able to see the related traffic. If it doesn't already run over the PRTG server or a connected probe, port mirroring can be used for this purpose. Administrators subsequently have the option to set up the sensor and define which TCP service should be monitored in the sensor settings. Each service can be defined in a row. The syntax for this is: "{IP-Address}:{Port}={Application name}"; for example: "172.22.72.1:80=Web Server". The sensor then creates several channels for each application entry and then presents the number of active connections, the number of dropped packages and the total number of analyzed packages, as well as the related average times up to the entry of

IAITested

ACK and request packets. The same applies for response times and the number of monitored connections.



Determine whether sensors should work with performance counters or WMI under 'Compatibility options for Windows' in the device settings

The sensor was easy to set up in the test and we don't think that any administrator could have trouble configuring the service entries. The sensor seems extremely useful to us. For example, it can be used to monitor external web or cloud services, which should not be burdened by the monitoring process.

PRTG for Android

The last important development is the app 'PRTG for Android'. This app is the new replacement for the old monitoring solution 'PRTGdroid' and arranges the sensor data hierarchically, just like the web interface. The user thus receives an easy-to-use and easy-to-navigate overview of all monitored components. A menu bar like the one in the web interface is included as well, allowing the user to switch quickly between pages for devices, libraries, sensors, alarms, maps, reports and other features. The data display automatically adjusts to the device's display size, so that as much information can be displayed as possible. This makes the app suitable for use on tablets and smartphones, which we were able to confirm in our test. A new notification system is available as well, which vibrates or uses ring tones to inform administrators of any problems in the network. The notifications can be adjusted to each user's requirements. If necessary, the user can even display the most important sensors as a widget on the home screen of the Android device.
The new app is not only designed to display sensor data, but can even be used for daily tasks. The solution enables users to search through network segments, change sensor priorities, confirm alarms and view graphs and reports. Libraries and maps can be used on the app as well. It is even possible to assign QR codes to racks, which can be scanned with the smartphone. The app then automatically opens the sensor data for the corresponding devices. In order to keep the data volume in check, the app only loads extensive graphs automatically if connected via WLAN. Otherwise, the user must first click on the desired information. This ensures that only essential information is loaded to keep potential roaming fees to a minimum. To complete the profile, Paessler also delivers a toolbox with the app, which the administrator can use to analyze the network connection using commands like ping and traceroute.

Conclusion

The new version of PRTG completely convinced us during our test. The tool's service range was always impressive, and now the web interface also provides a much better overview. It is not only much faster, but also presents the information required by each user in a clear and logical structure, which can be adjusted to accommodate the user's needs at any time. The speedometer display and graphical overviews, now integrated throughout the solution, are especially useful for providing clarity in operation.

The same goes for the Android software, which brings the majority of the solution's service range to mobile devices. With this app, administrators can react to problems and check the status of their network no matter where they are. The administrator is not restricted to the role of an onlooker, but can even actively change configurations. Further useful functions, such as the automatic sensor comparison or the passive service sensor for applications, complete the positive overall image of the product. Paessler has taken a great leap forward with the new version of its monitoring system, which should more than satisfy any system administrator.