The Entire Network in Sight

Dr. Götz Güttich

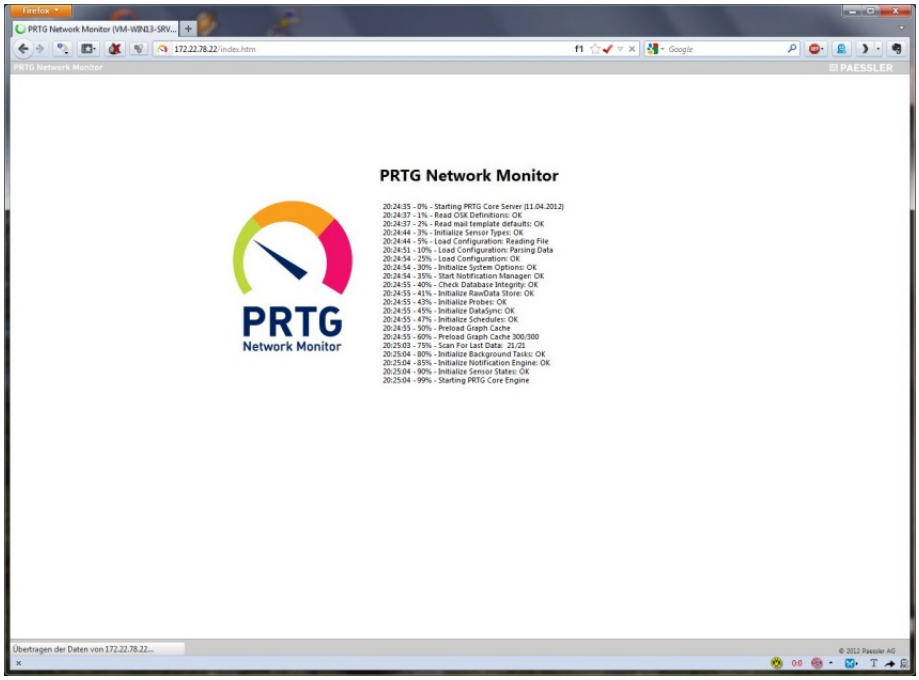
The PRTG Network Monitor by Paessler AG runs on Windows and collects data usage from computers, applications and other infrastructure components within the network. All information is stored in a central database and can be used at any time for comprehensive analyses. The tool administrator runs on a powerful web interface or a native Windows application. PRTG draws upon several different technologies for data collection, namely WMI, SSH, SNMP, NetFlow, jFlow and sFlow, as well as packet sniffing. IAIT took a look at the handling and performance of the solution in daily operations.

Paessler's PRTG Network Monitor proactively alerts administrators of issues in the network, thereby informing them of problems before they arise. The solution includes more than 130 sensor types, which are designed to monitor parameters such as the processor load of individual systems, free disk space and network interface utilization. Sensors are also available for network services, such as HTTP, SMTP, POP3, FTP, etc. The term 'sensor' is not to be taken literally in this context: PRTG works without agents – that is, without software components on the client systems that are being monitored. The sensors run on a central 'probe' (where necessary, multiple probes can be set up in the network) and, from there, query the clients' statuses regularly via the above-mentioned protocols, for example, WMI, SNMP or SSH. These findings are stored in the central database and can be used for extensive analyses, which can in turn be used to optimize the network. If any difficulties arise, PRTG is also able to send alerts via email, text message or pager, among other methods.

The license model is dependent on the number of sensors. Up to ten sensors are free of charge. Additional sensors can be bought as they are needed. With PRTG, all functions are included in every license, regardless of the license size. A 30-day test version is available with an unlimited number of sensors.

Architecture

PRTG operates using a core server that works with an Ajax Web interface. This interface constitutes the main management tool and offers the most extensive function range. A Windows administration tool called Enterprise Console is an alternative that offers a nearly complete range of functionalities (according to the manufacturer, 95%). A Mobile Web GUI, which provides data in an optimized form for mobile devices, is included as well.



The PRTG Network Monitor at startup

Apps for iOS and Android complete the palette of access options for the network monitoring system. The Android app (PRTG-droid) provides users with simple access to the Paessler software's mobile web interface and can inform administrators of any errors directly.

The iOS app (iPRTG) calls up the data from the web server via the API and displays them in native iPhone style. PRTG recommends Chrome and Firefox browsers for daily desktop use, and we even used Internet Explorer for the test, which worked perfectly.

Besides the Core Server, PRTG also uses probes, as mentioned above, which pull information from the clients. Multiple distributed probes can be used, if desired, and are especially useful when monitoring remote installations in addition to the local network, while still reviewing all information from a central position. Multiple PRTG installations can also be managed centrally using the Enterprise Console.

The sensors have so-called channels that can gather information on individual parameters. With memory sensors, for example, these are the total memory and available memory in percent.

Dependencies can be defined between sensors. This makes it possible to use both a Ping sensor and an HTTP sensor, for example, to monitor a web server. If the Ping sensor reports an error, the system will pause the corresponding HTTP sensor. This is beneficial because the HTTP service will not be available if the affected server is not responding over the network. The administrator thus only receives a single error message that indicates that the web server is not responding, not two. This improves clarity significantly, especially when monitoring systems with many sensors.

As a general rule, the sensors – according to the area of application – are very powerful. For example, not only is it possible to determine the fact that a webserver responds on request, but the IT administrator can configure the system in such a way that it queries specific content or even simulates a purchase in an online shop, in order to guarantee that the service is actually running as desired. If a website is hacked, for example, the web server still continues to work, although the shown contents might be completely different from those that the affected company actually intends to show. This can only be discovered if the monitoring software evaluates the web service's content as well as its response.

Custom scripts can be integrated as sensor types in PRTG at any time. All found data are saved for up to a year by default, and lon-

ger time spans can be set up as needed.

The Test

For our test, we installed version 12.2 of the PRTG Network Monitor on a Windows Server 2008 R2 system in our network and subsequently used the solution to monitor computers running Windows XP, Windows Server 2008, Windows 7, Windows Server 2008 R2, Red Hat and Fedora Linux, Ubuntu Linux, MacOS and Solaris. We also monitored diverse network components including, for example, Cisco switches and routers from Netgear and Lancom, and even included several websites, for example the IAIT website, and the online services Dropbox, Twitter and Skype in the monitoring as well. Because PRTG supports IPv6, we also monitored various systems using this protocol.

After installing the software and setting up the sensors we needed, we put special focus on monitoring our Exchange server and our virtualization environment (based on VMware). We examined the entire feature set of the monitoring software, including device trees, libraries, maps, reports and alarms. Last but not least, we used the app PRTGdroid for remote access to our installation.

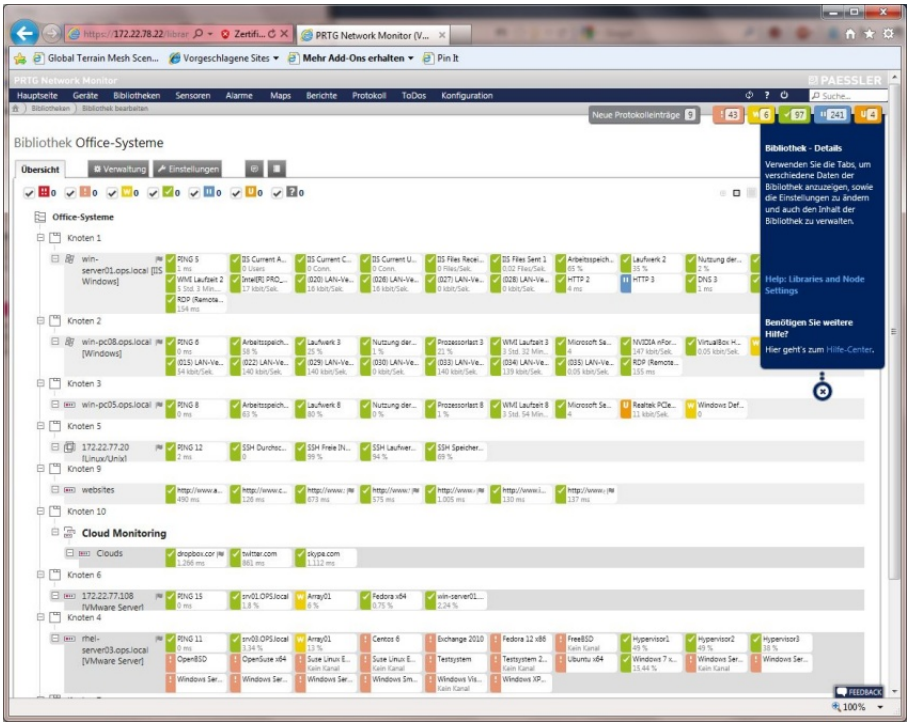
Installation

The ideal environment for the network monitor is an up-to-date Windows operating system on a dedicated host. Paessler recommends not installing the PRTG Network Monitor on a virtual machine for performance reasons.

A system with four GB RAM and a few hundred GB of available hard drive should be used for the best possible performance. The computer used for monitoring must be equipped with .NET Framework 4.0.

The installation of the product is controlled by the Wizard – just like any other Windows installation – and would pose no problems for any administrator. The administrator simply needs to choose the right language, enter his license key and define his mail account. A failover cluster can be set up later, if desired.

After completing the setup, the browser with the PRTG login screen opened on our system and we could log in to the monitoring product for the first time. Normally, the Configuration Guru appears at this point to support the administrator with the initial configuration of the system. However, because we used a Windows server with Internet Explorer and enhanced security configuration, we first had to add the PRTG page as a trusted site to ensure that the system displayed everything correctly.



The device overview presents users with the status of individual sensors

The Configuration Guru

The Configuration Guru helps administrators with basic PRTG configuration. In the first step, it suggests encrypting the access to the solution's web interface with SSL. The user is given the option to activate the SSL encryption or to skip this step. These options – executing the recommended task or skipping to the next step – are available for all steps with the Configuration Guru.

After setting up the SSL encryption, we set up our administrator password with the Configuration Guru's help and entered the credentials for the Windows systems – including our network domain. This step is mandatory, so that PRTG can access the appropriate computers to query information. Finally, the guru asked about credentials for SNMP, VMware and Xen, as well as Linux systems, and offered to monitor the Internet connection with Gateway and

DNS servers. The next step was to specify the servers that PRTG should keep an eye on in the network. For this, the guru offered us domain controllers, Exchange or other mail servers, as well as other servers, by name or address. We entered our domain controller and Exchange server, as we wanted to use a general network search in the PRTG environment to add our other systems later.

The server monitoring setup was completed, and it was time to set up monitoring for websites and online shops and to activate monitoring of cloud services, such as Google (search, drive and mail), Office 365, Salesforce, Dropbox, iCloud, Facebook, Twitter and Skype. Finally, the Configuration Guru ran the Network Auto-Discovery, an automatic network search for all systems in our LAN. This process instantly found all active components. With the VMware systems, PRTG also recognized that it was dealing with hosts of virtual machines (VMs), and immediately listed the VMs installed on these hosts as sensors.

Network Auto-Discovery

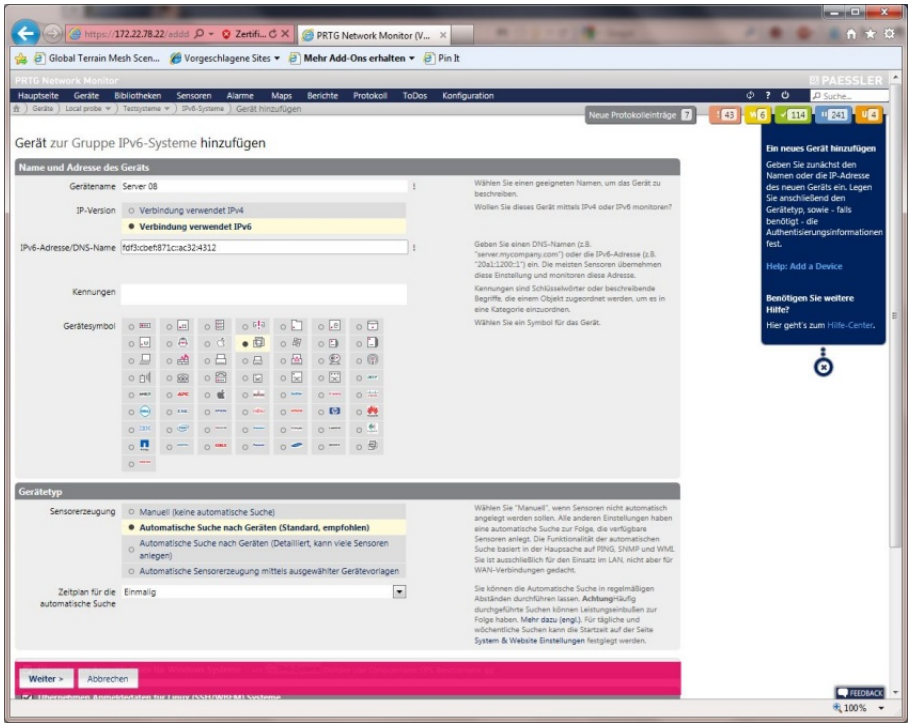
The automatic network search can be started manually at any time, or can be executed automatically according to a schedule. This search presents a sound method of keeping the configuration up to date and incorporating new systems in the PRTG environment. If a user would like to create a new group with all Windows servers, for example, all he has to do is create an automatic network search, select the appropriate probe, enter a group name and determine how the sensor creation should occur. There are four options: manual creation, automatic creation according to device, detailed automatic creation according to device (this method can create a lot of sensors) and sensor creation using device templates.

The last method is especially beneficial if multiple identical systems with specific components are part of the network. In most cases, normal automatic sensor creation is sufficient, and the sensors that are found can be added to manually if desired, for example with monitoring functions for specific server types.

The next step was to decide on a schedule for the auto-discovery and to specify the address range that should be searched. There are several options, namely Class C IP address ranges (IPv4), a list of individual IP addresses or DNS names (IPv4 or IPv6), a network address with a sub-network (IPv4) or IP with an octet range (IPv4). With these options, every administrator should be able to find something that suits his network.

As soon as the administrator enters the required information for the address range, he can activate name resolution using DNS, WMI or SNMP and skip the automatic search for the addresses of already recognized devices in order to speed up the process.

The final steps included entering the credentials for the Windows, Linux, VMware/Xen and SNMP systems, as well as settings and access information for the HTTP proxy. All of this information can be inherited from the existing configurations, so that auto discovery can use the credentials entered via the Configuration Guru, if applicable. The access rights determine which PRTG user accounts are granted access to the resulting objects of the current search. After the search is complete, the new sensors appear automatically in the device over-



Icons can be selected when adding devices, under which the devices will appear in the overview

view, which we will address in detail in a moment.

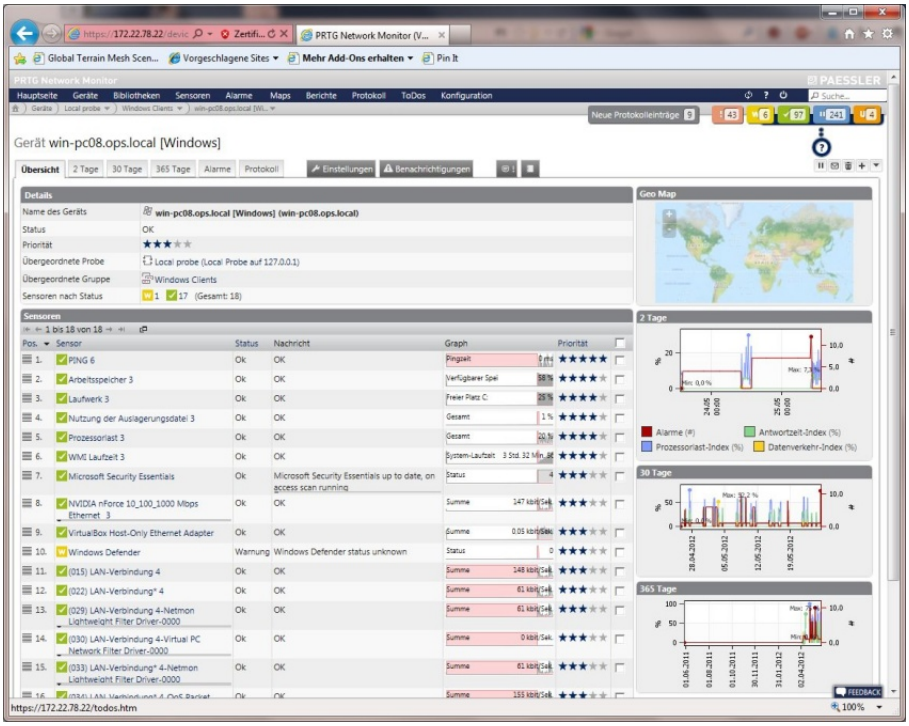
The Web Interface

Now that the installation and initial configuration were complete, we turned to the feature set of the monitoring tool. After logging in to the operating web interface, the administrator is shown a welcome screen, which presents the option to call up the Configuration Guru again, start the Network Auto-Discovery, switch to the device overview, download the Enterprise Console, install smartphone apps, call up the help function or contact support.

The top part of the configuration tool's window presents a menu bar, which leads directly to the most important entries, including the device overview, library, alarms, etc. Further options for the user are included under these main menus, which can be accessed by hovering the cursor over the menu titles.

The 'Home' menu, for example, contains four sub-entries leading to different overview pages. These – just like any other page – can be set as the homepage, if desired, and will then appear directly after login. The overview pages present a summary of data, containing the most important sensors (these can be marked as "favorites" by the user), the log, to-dos, alarms, warnings, groups, devices, sensors, sensors with the status "unusual" and recent log entries.

A sitemap containing all links available for the active user account is also available, as well as the option to call the mobile Web GUI and the above-mentioned welcome screen. The Home menu thus contains a wide range of options to configure the PRTG Network Monitor to deliver extensive information about the network directly after login.



The drill-down view of individual systems presents a list of all monitored services on the system

An in-depth, context-based help function is located on the right side, which explains nearly all of the available configuration options. This help is included on every page of the configuration tool.

The Device Overview

The second menu entry leads to the device overview mentioned above. This is the core of the Network Monitor and displays each monitored system with its sensors in a tree structure in the respective groups. Users can see where errors, warnings, etc. have occurred at first glance, as sensors with errors appear red, those with warnings are yellow, and problem-free sensors are shown in green. The device overview is not only for data display; remote probes as well as new groups, devices and sensors can be added as they become necessary. In addition, a geo map shows where each monitored system is located in the world, and overview charts display information regarding alarms, processor usage, data traffic and response times. In standard configuration, these overviews each show the status from the past two, 30 and 365 days.

Clicking on a group, computer or probe opens a corresponding drill-down overview. If a company has all Windows servers summarized to one group, for example, clicking on this group will only display the systems assigned to the group. In this way, IT staff is able to limit the display to individual computers or even single sensors.

If the system displays the data from a single computer, all sensors found on this computer are

displayed in a list. This list contains small charts, in addition to sensor-specific data including name and status, which show important information (e.g.: capacity utilization) at a glance.

The individual sensor display presents detailed information, including 2-day and 30-day overviews and live data. In addition, users can set sensor parameters and modify names, scanning intervals, priority (this determines the order of objects in list views) and access rights.

It is also possible to configure the sensors in such a way that they send notifications upon crossing certain thresholds or attaining certain statuses. If a sensor status is 'down', for example, a message can be sent to the administrator after a specific time period. Individual channels within the sensors can be assigned limits, and they can be configured to show up in charts and tables. Last but not least, administrators are able to insert comments here, and review the history of each sensor.

In addition to the points mentioned above, tabs are available in the device and group views, with which live data can be viewed in graphs and tables, and the history can be called up. Two-day, monthly and yearly overviews are available, as well as the option to query "historical" data according to freely definable time periods.

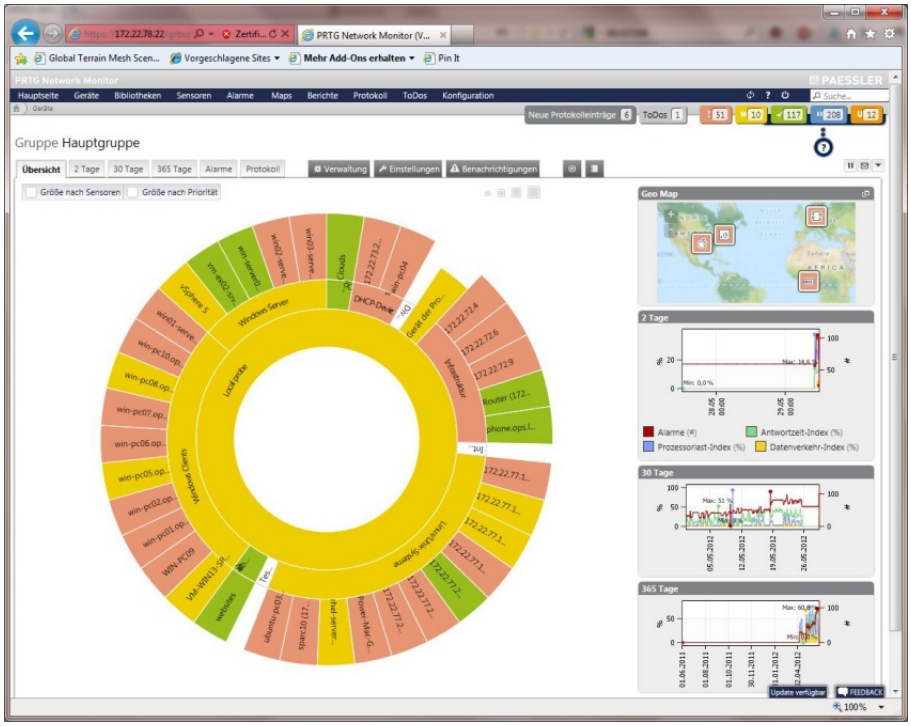
The menu item 'Management' is also available in the group and device overviews. Here, each user can arrange the sensors as he pleases using drag & drop.

In the settings tab, users can pause all sensors in a group or on a device and determine the type of sensor management (automatic, manual, etc.). It is also possible to change device credentials, define schedules and modify other parameters that were preset during the original network search. Tabs for creating notifications, entering comments and viewing the history complete the feature set for group and device configuration.

One more thing worth mentioning: the multi-edit function can be used to select and edit multiple objects in the sensor and device lists simultaneously. This is especially beneficial when configuring or pausing multiple sensors at once.

During the test, we noticed that administrating the network according to groups, devices and sensors helped us to keep a clear overview even when working in an environment with numerous components. On one hand, an alarm can be configured so that it is activated by an error anywhere within an entire computer group.

On the other hand, notifications can be set up in such a way that only a single sensor in a single system is recognized as a trigger. The alert and analysis options are thus minutely customizable to fit the requirements of specific situations and staff, without reducing the clarity of the entire system.



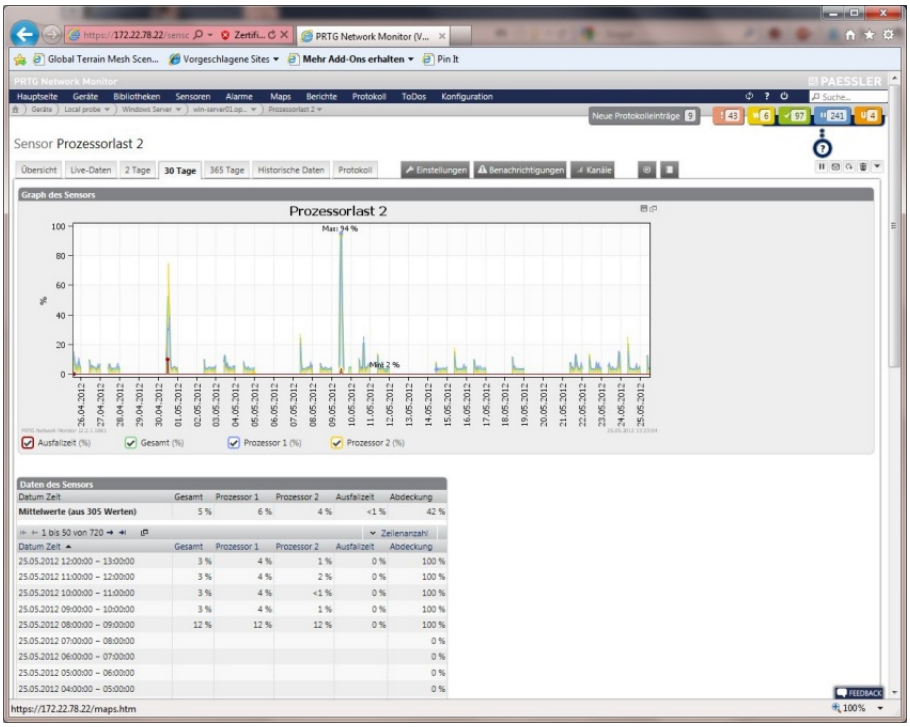
The 'sunburst view' provides information regarding the status of monitored components at a glance. The overview becomes more detailed as one moves outward, and individual systems pass on their status to the inside. This way, Paessler ensures that the inner ring, which represents the entire network, is only displayed error-free when none of the outer systems shows an error.

Libraries

Contrary to the device overview, libraries allow the user to create customized views according to various criteria. Environments that are listed in the device overview according to technical aspects, like operating systems or roles in networks, can be arran-

ged in such a way as to reflect the organizational structure of the company and its departments (marketing, accounting, IT, management, etc.). The individual library views can be generated and modified directly in the browser using drag & drop.

To insert a library, the user must simply enter a name and the access rights for the object; the library is then immediately available for further application. Existing libraries can be changed at any time. We had no difficulties working with libraries during the test.



The monitoring software presents the data and measurements for each sensor in a chart. Here, the CPU usage of a server is displayed over the time span of one month.

Sensors

The sensor overview comprises a list of all sensors with their statuses and a small chart, which displays capacity usage and other important information. When creating a new sensor, PRTG Network Monitor first asks the administrator if the sensor should belong to a new or an existing device, what the device symbol is, whether the connection runs over IPv4 or IPv6, what the credentials are and whether sensor creation should occur manually or via automatic search.

If the administrator decides for manual sensor creation, he can choose from an array of 131 predefined sensor types. Paessler offers categorized decision support to simplify this process.

The user can answer questions to find appropriate sensor types. These questions are: “Monitor what?” (availability/uptime, bandwidth/ traffic, speed/performance, CPU usage, disk usage, memory usage, hardware parameters, network infrastructure, custom sensors), “Target System Type?” (Windows, Linux/MacOS, Virtualization OS, File Server, Email Server, SQL Server), “Technology Used?” (Ping, SNMP, WMI, HTTP, SSH, packet sniffing, NetFlow, sFlow, jFlow). With the help of these categories, we were able to quickly and efficiently set up the sensors we needed to monitor our Exchange systems and our vSphere environment.

Various options are available in the Sensors menu to provide the user with an overview of the sensor data and results. These include top-10 lists for various attributes including “Best Availability”, “Fastest Ping”, “Worst Downtimes”, “Slowest Ping”, “Lowest Bandwidth Usage”, “Fastest Website”, etc. Overviews organized according to current status, uptime/downtime, group and type are available as well. It is even possible to compare sensors and view historical data. This provided us with very interesting insight in our network during our test.

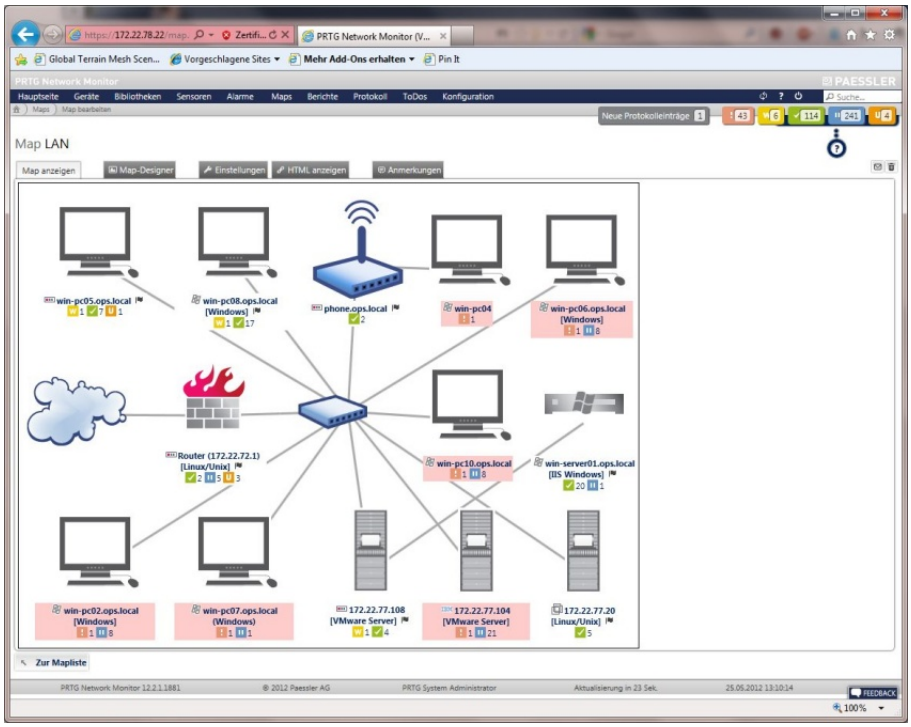
Alarms

The PRTG Network Monitor offers extensive alarm functions. The alarms can even be used to automate restarts and to execute Powershell scripts, batch files, and DLLs. PRTG also includes a list of current alarms and warnings. Hovering the mouse over the list (this applies for other overviews as well), the web interface blends in an overview window with the most important data and charts for the respective entry. This is very helpful when looking to attain a quick impression of multiple entries without having to open each one individually.

Maps

Maps offer a graphical network overview that can be enhanced with background images. A location map can be created for all computers in the building, for

example, on which the status of each system appears next to its location on the map. New maps can be created at any time and can even be published, so that third parties can gain access to



A network map set up as the homepage

the included information. A map is also an ideal option for the homepage that is presented directly after login. Maps can also be effortlessly integrated in external websites. Maps can be created – just like libraries – via drag & drop from the device tree.

Paessler provides additional symbols for the maps, which symbolize transparent components, like unmanaged switches, and external abstract systems, like the Internet. It's no problem to incorporate connections between individual systems in the map, either. We found one overview map of our LAN to be so useful in our test that we set it up as our homepage.

Reports

The monitoring system enables data and graphics to be combined in reports. One-time and recurring reports are both available. The time frame for which a report should be issued can be defined manually, and reports can be displayed as HTML, generated as PDFs and sent per email. Various reports are included in the software, like the "100 Fastest HTTP Sensors", "100 Slowest Ping Sensors", etc. Reports on bandwidth, CPU usage, memory usage, disk space and availability are available as well. All reports are fully customizable.

Reports can be saved and called up again at any time. The sensors that the report is based upon can be selected manually or according to tags. Selection by tag creates dynamic reports: if an administrator assigns one of these tags to a sensor or group, it will be included in the appropriate report.

To delete a component from the report, the administrator must simply delete the tag. Reports can also be created and sent out according to a predefined schedule. We encountered no difficulties here in our test.

Logs

PRTG displays its log in list form. The time frame and number of rows that should be displayed in the list of log entries can be specified at any time. All entries can be displayed, or they can be filtered according to group, system events or status change (ie: OK, down, paused/resumed, acknowledged or unusual).

To-Dos

The to-dos act as a notification service for the user. They include information that the administrator must confirm, including the availability of new program versions or activation of new sensors. The system also uses these to advise users of newly created reports.

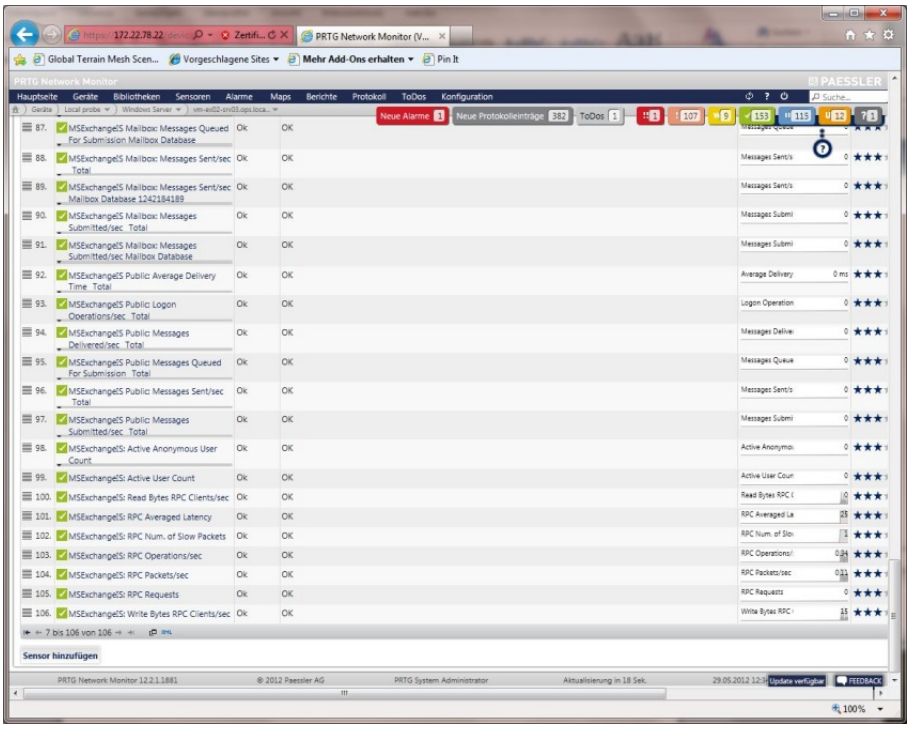
Setup

The Setup menu contains all entries for managing the PRTG Network Monitor. The account settings (name, password, time zone, email address, notification settings, etc.) are included as well. The PRTG status, on the other hand, contains information regarding the software version, operating system, time, CPU usage, license, etc.

Administrators can use the PRTG status to create a snapshot of the database, in case they require assistance from the Paessler support team, to restart all probes and to write a probe status file. The 'auto-update' function ensures the PRTG Network Monitor is always up to date. This worked flawlessly in the test. Also interesting: the system administrati-

on. Here, the administrator can configure diagrams and colors, define the name of the PRTG website and select a map provider (MapQuest, Nokia Maps, CloudMade or Google). The monitoring tool can even be integrated in the Windows domain so that existing user accounts within the company can be used for PRTG as well. Apart from that, threshold values can be set here to distinguish unusual incidents.

The next entries deal with the settings for sending notifications (via an internal or external mail server), communicating with external probes and working with user accounts. Various user accounts can be set up for different monitoring tasks. Users can be assigned to groups, alarm settings can be made and rights can be assigned ("read/write" or "read only"). Command menus for managing clusters, downloading additional software (Enterprise Console, apps for mobile devices and installation files for remote probes) and entering the license round out the configuration tool's feature set, along with a documentation of the PRTG API. The tool has been set up in a clear manner and – often thanks to the good help function – required only a short familiarization phase.



The Exchange monitoring function comes with a large number of sensors

The Android App

PRTGdroid afforded us secure access to the information from the PRTG Network Monitor, anytime and anywhere. The configuration effort was minimal and the mobile web interface is well suited to viewing data. Large icons make the interface especially 'thumb friendly'. Because it can be used with any browser, the app does not necessarily have to be installed, but it does expand the feature set of the Mobile Web GUI with the very handy opportunity to display notifications on the mobile device.

Exchange Monitoring

The monitoring options Paessler provides for the Exchange Server are extensive. The system places a total of 97 sensors at the user's disposal that are specially designed for Exchange systems and enable monitoring of various areas including memory, the database and the number of active users.

Several sensors are very straightforward and self-explanatory, like the sensor that counts the number of notifications sent per second or the sensor that informs administrators of logon operations per second. Others are not quite as simple, like the "Database Cache % Hit edgetransport". Keeping an eye on individual mail queues is generally important when monitoring Exchange servers, as it makes it easy to determine if email sending starts to pile up. The number of emails sent per second is just as important: this sensor can be used to determine if a computer in the network is being misused to send spam.

Apart from that, the CPU and memory usage should be monitored, as well as the mail services POP3, IMAP4, SMTP and the queues for internal redistribution of emails to email inboxes. If there are no problems here, there is a good chance that the Exchange Server is in good shape.

The "Roundtrip Sensor" shouldn't be forgotten here, either. It sends an email to an external service, which the administrator must configure in advance to instantly and automatically return the email. This enables the administrator to determine how long it takes to send the message to the selected service and back. In our test, monitoring of our Exchange 2010 servers worked flawlessly.

Monitoring vSphere

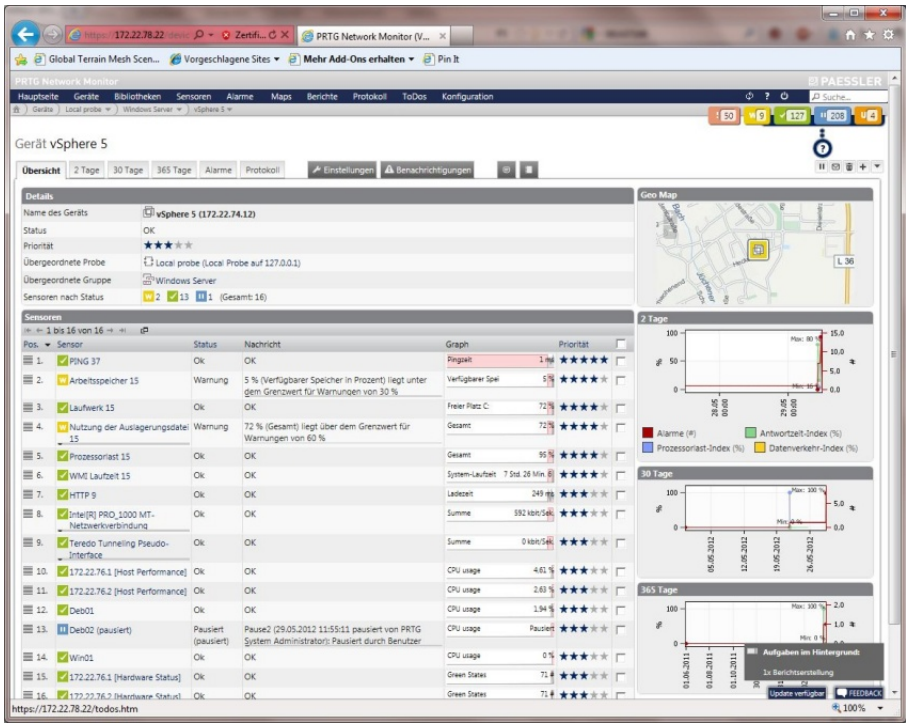
When monitoring virtualization environments based on VMware (we used vSphere 5 and ESXi 5 systems for our test), the following points should be kept in mind: if the credentials for the virtualization hosts are entered correctly, the Network Auto-Discovery will find the system, recognize it as an ESXi host and instantly set up sensors to monitor the VMs running on the system. This entire process is incredibly simple and runs out of the box. When working with vSphere servers that manage multiple ESXi systems and Vmotion, which is used to move VMs from one host to another according to capacity utilization, the procedure described above cannot be used. If Vmotion shifts a VM from one host to another, this process sets off an alarm in PRTG, as the VM suddenly ceases to exist on the corresponding host.

In this case, the ESXi hosts should be monitored over the vSphere server instead of being monitored directly. PRTG thus views the ESXi hosts from the vSphere's perspective and recognizes that the VM is still running, just on a different host. A little bit of handiwork is required in order to realize this. The vSphere server is Windows software that runs on a Windows server. When searching this server with Network Auto-Discovery, the Paessler product sets up standard Windows sensors, but does not set up the VMware sensors; the administrator must do this manually. In this case, the login data for the ESXi server cannot be used as credentials for the VMware environment; instead, one of the Windows user accounts that have access to the vSphere server must be used. This process posed no problems for us during our test.

Conclusion

The PRTG Network Monitor completely convinced us. The system is easy to install and can be set up quickly and seamlessly, thanks to the Configuration Guru. A major feature is that the software operates without agents on the monitored systems. This not only saves the IT department's time, but even prevents having to touch systems in the network, which is very appealing, especially with critical installations.

We also have to emphasize the software's incredible range of functions. Paessler put a lot of effort into providing effective, high-capacity sensors for all servers generally found in modern IT environments. This applies not only for Cloud services like Dropbox and Salesforce, but also for the monitoring of virtual environments and standard applications like Exchange. The administrator can even keep track of network traffic using NetFlow, sFlow, jFlow and packet sniffing. In most cases, the Network Auto-Discovery sets up all necessary sensors on its own. In the event additional sensors must be manually integrated in the environment, this procedure is quick and shouldn't cause any problems for network specialists. Other positive points are the libraries and maps. These provide flexible perspectives that are not only meaningful for technicians, but that are clearly understandable for staff from other departments as well. The required effort for these views is low and it is even possible to publish maps on external sites. The comprehensive, high-performance alarm and report functions complete the positive overall impression we received from the PRTG Network Monitor.



It's important to keep an eye on the vSphere server as well as the individual hosts when monitoring VMware environments