funkschau

LAB TESTED
funkschau

Paessler PRTG
Network
Monitor 12

The sunburst view diagram allows a quick overview of the complete status of the monitored devices. The inner ring represents the entire network. If this ring is red, this indicates that a device in one of the outer rings is showing a failure.

Monitoring in the Fast Lane

Paessler PRTG Network Monitor 12 – Paessler skipped two version numbers at once with the current release of their PRTG Network Monitor. We figure they've added enough new features to justify the jump – and we agree with Paessler, that version numbers are not that relevant anymore these days.

Version 12 of the PRTG Network Monitor, in short PRTG, has just been released. But what about versions 10 and 11? Some PRTG insiders would ask the same question, and even we were surprised to see the jump. Dirk Paessler, CEO of Paessler AG, justifies this by the complete changeover of the rollout strategy to 'continuous rollout,' which just happens to be the first news about PRTG.

Anyone who uses services like Facebook, Google Mail or Salesforce is already familiar with this concept: users of these services don't need to worry about administering software updates; they simply log in and automatically use the newest version. Because PRTG runs in the user's network, Paessler can't replicate this exactly, but with their new concept, the company isn't far off.

Paessler's goal is to distribute new features and fixes more quickly and with higher quality. To achieve this, the company offers three

channels for software updates: Stable, Preview and Canary. PRTG users simply select one of these channels for their installation and by doing so, decide for maximum stability, early access to new features or a combination of both. Paessler then informs the users of new software versions in the respective channel, as they are made available. The Canary channel supplies code directly from the development department, sometimes more than once a day. This is early code, which may not be complete or might not have been thoroughly tested; for that reason, the Canary channel is only recommended for test environments. In the Preview channel, the newest features and fixes are provided on a weekly basis, after they have been tried and tested by the lab. This channel offers the user early access to new features and gives Paessler the opportunity to test new features sooner "in the wild." Lastly, the Stable channel provides users with conservative, extensively tested versions. This

channel is usually updated once or twice per month, or whenever important bug fixes need to be distributed.

So what does this have to do with the version jump? With 'continuous rollout' and auto updates, it doesn't matter anymore which exact version a user is working with; he is always using the most recent version, period. And since the appearance of Version 12, Paessler uses the current year and quarter as the version number, which explains the '12' before the dot. In any case, there are so many new features in PRTG besides the new rollout process that a big (conservative) version jump would be justified.

The Guru shows the way

The installation of PRTG has remained almost unchanged, which is a good thing, because in our opinion there was nothing to improve on there. The product is on the disk in a matter of minutes, including supporting components like, for example, the database engine. We mention the database for a reason: most comparable monitoring applications from other manufacturers use Microsoft SQL Server for data storage, which is not optimal for storing lots of small, constantly changing data records, nor is the initial configuration always as simple as the manufacturers would like us to believe. With data storage integrated in PRTG, on the other hand, there is no hassle and it's quick as lightning.

The first start of the actual management interface (a fast Ajax web interface) reveals one of the most noticeable new features: the Configuration Guru. The Guru takes the administrator step by step through all necessary or useful settings and thus guarantees that nothing is forgotten. For example, this little application points out that it might be a good idea to activate SSL encryption. With such detailed assistance, configuration settings like the credentials for Windows, Linux, Solaris and Mac OS systems, VMware, Xen server, SNMP login data or other server settings for domain controllers, exchange and mail servers that should be monitored can be configured

quickly and accident free. Before the guru goes for a well-deserved rest on his bed of nails, he also recommends searching through a network segment. Which is a good idea, as this is the typical network discovery for network management applications. The administrator enters the name of a group of devices that should be added, specifies a base address for IPv4 as well as start and end addresses, clicks 'Save and Continue' and can begin to familiarize himself with the management interface while the discovery runs in the background.

The Hierarchy

For every device in the network that PRTG Network Monitor should monitor, a corresponding device must be created in the PRTG configuration. The term 'device' should not be taken literally, as these devices can include websites, clouds and Internet connections in addition to servers, workstations, switches or APs. For these devices sensors are assigned, each of which monitors a specific aspect of the network or device. PRTG Network Monitor usually determines the type of device during discovery and installs the appropriate sensors automatically. This creates a solid foundation, which the administrator can build on later. Like the term 'device,' PRTG's use of the word 'sensor' should be interpreted a little differently than someone who is acquainted with other management applications might think: these sensors are not software that run on the monitored devices – instead, these sensors run on a central probe. From there, they call information from the clients via WMI or SNMP, for example.

All objects in a PRTG monitoring configuration are organized in a treelike hierarchy that is displayed in an easy-to-navigate list. Administrators can summarize objects into groups that monitor similar devices, services or a single location. The hierarchy also serves to define standardized settings for larger groups of objects, as settings can be inherited within the hierarchy. The root or main group is located at the top of the hierarchy, which contains all objects for a setup. Settings on this level apply for all objects. Every group other than the main group is part of a probe. A probe is the platform on which monitoring happens. All objects configured under a probe are

monitored via this particular probe. Each PRTG core installation automatically creates a local probe; administrators can create additional remote probes (for monitoring remote devices outside of the network) if necessary. Each probe contains one or more groups, which summarize objects, as explained above. Probes and/or groups contain the devices to be monitored, for example, file or web servers, client computers, routers and switches – in other words, nearly every device in the network that has an IP address. PRTG automatically adds a so-called 'probe device' to the local probe, which uses several sensors to monitors the parameters of the computer that the probe itself is running on. Sensors can be added automatically or manually to every device to monitor the individual aspects of the device. These can include, for example, network services like SMTP, FTP or HTTP, switch port traffic, the CPU usage of a computer, traffic on the network card or a Netflow device. Each sensor has a series of channels over which it receives various data flows.

Relationships can be configured between sensors. For example, it is a good idea to make sensors that monitor a server's network services dependent on the Ping sensor, because if the server already isn't reachable over the network, the network services won't be available, either.

Various predefined views are available for devices, libraries and sensors, including group views, device lists, favorites, top 10 lists and cross-references. In addition to these, the administrator can choose between four quick overviews and a complete sitemap. It's generally a good thing to have so many different views, sorting and filter options available. However, Paessler does need to be careful not to overload the menus. Users that are unfamiliar with the system might feel rather overwhelmed during their first expeditions through PRTG.

Even more GUIs

In addition to the management interface in the browser we mentioned above, the PRTG Enterprise Console, a Windows application, is also available. The Enterprise Console offers nearly the same range of functions as the browser application (approx. 95%) and provides central access to all existing

New Sensors in Version 12

PRTG Network Monitor Version 12 contains the following new sensors:
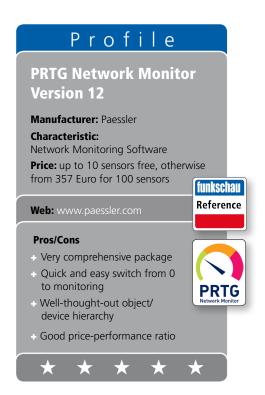
Application Sensors:

❚ VMware Host Server Health Sensor: monitors the hardware status of a VMware host server

❚ Extended Amazon Cloudwatch Sensor: monitors instances of EC2, EBS, RDS DB, ELB, SNS, SQS, Elasticache in the Amazon AWS cloud

❚ WMI SharePoint Process Sensor: monitors SharePoint processes via WMI

❚ WMI IIS Application Sensor: monitors TotalBytesReceived, TotalBytesSent, TotalGetRequests, TotalPostRequests, TotalAnonymousUsers, TotalFilesReceived/Sent and other IIS data using WMI

Hardware Sensors:

❚ SNMP Cisco ASA VPN Connections Sensor: monitors the active VPN connection of a Cisco ASA Firewall via SNMP

❚ SNMP Cisco ASA VPN Traffic Sensor: monitors data flow through permanent VPN IPsec connections via SNMP and alerts whenever the connection is interrupted

❚ SNMP Cisco ADSL Sensor: monitors the connection quality of a Cisco router's ADSL connection

❚ Fritz!Box WAN Interface Sensor: monitors the AVM Internet router for small and medium sized companies

❚ Dell Powervault MDi Sensor: monitors Dell MD3000(i) SANs

❚ WMI HDD Health Sensor: supports local and remote S.M.A.R.T. Monitoring via MWI

Other Sensors:

❚ Google Analytics Sensor: collects traffic data from a website via Google Analytics

❚ WMI Remote Ping Sensor: measures the Ping time to a target from a Windows Remote Computer via WMI

❚ SIP Options Ping Sensor: monitors whether an SIP server is able to receive a call and forward it to the next node

❚ Xen Host Sensor: monitors CPU, storage and network usage as well as other decisive system parameters

❚ Improved Active Directory Integration: PRTG now receives the email addresses from new users directly from the Active Directory, if the AD Integration is used

❚ SSH Script Sensor: enables individual scripts to be run on an OS X/Linux/Solaris system and the returns results as sensor data

❚ SSH Remote Ping Sensor: uses SSH to measure Ping time to a target from a Linux/Unix remote computer

PRTG installations as well. A Mobile Web GUI is also available for mobile administrators, as well as native apps for iOS and Android. These mobile applications are designed to enable access to the monitoring system on the go and, of course, receive alarm and warning messages. Unfortunately, Paessler does not offer anything for the opposite direction (that is, monitoring mobile devices). During Auto-Discovery, PRTG ignored iPads and smartphones, even though these used IP addresses within the address range of the sub network and were online while the discovery was running. These devices could be added manually by entering their IP addresses, but even then, not much more than a Ping test could be done with them. PRTG has room for improvement in this area, as these should really be considered network devices by now.

New Sensors

Each new PRTG version includes new or improved sensors, and Version 12 is no exception. For example, the product now includes monitoring of virtual systems, or rather, the platforms on which these run. This means that there are sensors that monitor the hardware for VMware and Xen host servers. Cisco ASA firewall users can get excited too, as two new sensors monitor the active VPN connections of the ASA firewall as well as the data flow through permanent VPN IPsec connections via SNMP. There is also a new Cisco ADSL sensor

that monitors the connection quality of a Cisco router's ADSL connections. While Cisco routers are often housed in many large networks, the same cannot be said for AVM 'Fritz!Box' routers. Still, Paessler has developed a sensor just for this Internet router, which is popular among private users and small and medium-sized companies. Whether this was actually necessary is open for discussion. In any case, the sensor exists and works very well – as do all PRTG sensors, by the way – and is perfect for quickly checking on the actual performance of the ordered DSL speed. For larger companies, the new Google Analytics sensor is much more practical. PRTG could already measure the availability and loading time of a website; now the product also collects the traffic data provided by Google Analytics. The configuration is simple – just enter the username, password and profile ID for Google Analytics. With this kind of sensor it's especially beneficial that administrators can generate meaningful reports, with data tables and/or diagrams, that can be executed automatically at regular intervals.

The SIP Options Ping Sensor deserves a special mention as well. This sensor monitors whether an SIP server is able to receive a call and forward it to the next node. Good SIP software should execute this kind of monitoring itself, but it is still advantageous to collect information of this kind from various devices in a central console, particularly because the chances of all other applications alarming administrators of failures or errors as dependably and flexibly as PRTG Network Monitor are rather slim.

With that, let's turn to the alarm system from PRTG Network Monitor. The system functions flawlessly. Alarms and warnings are impossible to miss and the program logs these fastidiously – even per Syslog, if desired. Administrators or groups of administrators, which naturally don't all sit in front of the console, receive notifications via email, text message and/or pager. PRTG even sends SNMP Traps, if desired. The program is generally very communicative and is constantly delivering useful information and offering support. Messages can be summarized in order to avoid mass notifications. Programs and/or scripts can be started and HTTP actions can be executed in reaction to errors or failures. The necessary configuration options can be found under 'Account Settings,' 'Notifications,' 'Add New Notification'. This is not intuitive, but it is an important function to be included in the program. Speaking of intuitive, it is obvious

that PRTG Network Monitor has become a highly comprehensive and flexible product. This has unfortunately led to a slight loss of ease in regards to handling and usage, but that is a compromise one must be willing to make for a monitoring product that can be used nearly universally.

Conclusion

PRTG Network Monitor has convinced us once again with Version 12. The product can be installed quickly and, as a rule, problem free. Thanks to the automatic device discovery with automatic sensor installation, the product is ready for operation without much ado. Of course, a basic configuration for the specific company or network must be set up, but administrators that devote two or three hours to working intensively with PRTG should have no problems with the setup. More than 130 sensors guarantee high functionality and flexibility, and new sensors like the Google Analytics or the SIP Options Ping sensors show that the product surpasses the boundaries of regular network monitoring and opens up new areas of application – we hope that mobile devices will be one of these areas in the future. Paessler's expertise in iOS and Android is obvious, thanks to the PRTG management apps for both operating systems. One of the biggest plus points for the product is that it functions without agents. This means that no extra software needs to be installed on the monitored devices. The price-performance ratio is excellent as well.

Dirk Jarzyna,
funkschau editor