

Kommunikationstechnik für Profis

funkschau

Ausgabe 18/2012 28. September 2012

€ 4,90 sfr 8,90

IfKom Ingenieure für
Kommunikation

funkschau.de



**Paessler PRTG
Network
Monitor 12**



Monitoring auf der Überholspur

Paessler PRTG Network Monitor 12 – Mit dem aktuellen Release ihres „PRTG Network Monitors“ hat Paessler gleich zwei Versionsnummern vor dem Punkt übersprungen. Wir finden, dass genug Neues im Produkt steckt, um einen großen Sprung zu rechtfertigen – und Versionsnummern sind heutzutage ohnehin nicht mehr relevant, was Paessler genau so begründet, wie wir selbst es tun würden.

PRTG-Network-Monitor, kurz PRTG, ist soeben in der Version 12 erschienen. Wo sind denn die Versionen 10 und 11 geblieben? Das wird sich mancher PRTG-Insider fragen, und auch wir waren angesichts dieses großen Versionssprungs überrascht. Dirk Paessler, Vorstand der Paessler AG, begründet dies durch die vollzogene Umstellung der Rollout-Strategie auf „Continuous Rollout“, was auch schon die erste Neuigkeit ist. Wer Dienste wie Facebook, Google-Mail oder Salesforce nutzt, kennt das bereits: Nutzer dieser Dienste brauchen sich nicht um die Verwaltung von Software-Aktualisierungen kümmern, sie loggen sich einfach ein und nutzen automatisch die aktuellste Version. Da PRTG im Netzwerk des Nutzers läuft, kann Paessler es zwar nicht genau so machen, aber mit dem neuen Konzept kommt das Unternehmen nah heran.

Paesslers Ziel ist es, neue Features und Fixes schneller und in besserer Qualität zu verteilen. Dafür offeriert das Unternehmen nun drei Kanäle für Software-Aktualisierungen: Stable, Preview und Canary. PRTG-Nutzer selektieren in ihrer PRTG-Installation einfach einen dieser Kanäle und wählen damit entweder maximale Stabilität, frühen Zugriff auf neue Features oder einen Mix aus beidem. Paessler informiert die Nutzer dann über neue Software-Versionen im jeweiligen Kanal. Der Canary-Kanal offeriert beispielsweise Code direkt aus der Entwicklungsabteilung, manchmal gleich mehrmals an einem Tag. Dies ist früher Code, der vielleicht noch nicht vollständig implementiert oder noch nicht intensiv getestet ist, womit der Canary-Kanal nur für Testumgebungen gewählt werden sollte. Im Preview-Kanal erscheinen wöchentlich die letzten Features

Das Sonnendiagramm erlaubt einen schnellen Überblick über den Gesamtzustand der überwachten Geräte. Der innere Ring repräsentiert das gesamte Netzwerk. Ist er rot, dann weist ein Gerät in einem der äußeren Ringe einen Fehler auf.

und Fixes, nachdem sie das eigene Lab erfolgreich durchlaufen haben. Dieser Kanal bietet dem Nutzer frühen Zugriff auf neue Features und gibt Paessler die Gelegenheit, neue Features früher in der „freien Wildbahn“ zu testen. Der Stable-Kanal schließlich offeriert konservative, ausführlich getestete Versionen. Dieser Kanal wird etwa ein oder zwei mal im Monat aktualisiert und immer auch dann, wenn es wichtige Fehlerbehebungen zu verteilen gilt.

Was hat das jetzt mit dem Versionsprung zu tun? Mit „Continuous Rollout“ und Auto-Update spielt es keine Rolle mehr, mit welcher Version genau ein Nutzer arbeitet, er nutzt stets die aktuellste Version, Punkt. Und seit Erscheinen der Version 12 verwendet Paessler das aktuelle Jahr und das jeweilige Quartal als Versionsnummer, womit sich nun die 12 vor dem Punkt erklärt. Aber auch abgesehen vom neuen Rollout-Verfahren steckt so viel Neues in PRTG, dass ein großer (konservativer) Versionsprung in jedem Fall gerechtfertigt gewesen wäre.

Der Guru weist den Weg

Die Installation von PRTG blieb aber nahezu unverändert, und das ist gut so, denn da gab es aus unserer Sicht auch nichts zu verbessern. In wenigen Minuten ist das Produkt auf der Platte, und zwar samt unterstützender Komponenten wie beispielsweise die Datenbank-Engine. Dass wir besonders die Datenbank erwähnen, hat einen Grund: Die meisten vergleichbaren Monitoring-Applikationen anderer Hersteller nutzen Microsoft-SQL-Server als Datenspeicher, aber dieser ist erstens nicht optimal für die Speicherung sich häufig ändernder vieler kleiner Datensätze und zweitens ist die anfängliche Konfiguration nicht immer so einfach, wie die Hersteller uns weismachen wollen. Mit dem in PRTG integrierten Datenspeicher gibt es hingegen keine Schwierigkeiten – und pfeilschnell ist er auch.

Der erste Start der hauptsächlichen Managementschnittstelle (eine schnelle Ajax-Web-Schnittstelle) offenbart mit dem Konfigurations-Guru gleich eine der auffälligsten Neuerungen. Schritt für Schritt führt der Guru den Administrator durch notwendige oder sinnvolle Einstellungen und gewährleistet damit, dass dieser nichts vergisst. Beispielsweise macht diese kleine Applikation darauf aufmerksam, dass es

eine gute Idee sein könnte, SSL-Verschlüsselung zu aktivieren. So an die Hand genommen, sind Konfigurationseinstellungen wie die Anmeldeinformationen für Windows-, Linux-, Solaris- und Mac-OS-Systeme, Vmware-, Xen-Server- sowie SNMP-Anmeldedaten oder weitere Server-Einstellungen für zu beobachtende Domänencontroller, Exchange- und Mail-Server schnell und in der Regel unfallfrei erledigt. Bevor der Guru sich dann zur wohlverdienten Ruhe auf sein Nagelbett zurückzieht, schlägt er noch vor, ein Netzwerksegment zu durchsuchen. Gute Idee, denn dabei handelt es sich um die für Netzwerkmanagementapplikationen typische Netzwerk-Discovery. Der Administrator gibt den Namen einer Gruppe an, der entdeckte Geräte hinzugefügt werden sollen, spezifiziert eine Basisadresse für IPv4 sowie eine Start- und Endadresse, klickt auf „Speichern und Weiter“ und kann dann bereits beginnen, sich mit der Management-schnittstelle vertraut zu machen, während die Discovery im Hintergrund läuft.

Die Hierarchie

Für jedes Gerät im Netzwerk, das PRTG-Network-Monitor beobachten soll, ist ein entsprechendes Gerät in der PRTG-Konfiguration zu erzeugen. Der Begriff Gerät ist dabei nicht wörtlich zu nehmen, denn neben Servern, Arbeitsstationen, Switches oder APs können diese Geräte beispielsweise auch Websites, Clouds und Internetverbindungen sein. Diesen Geräten sind Sensoren zuzuweisen, von denen jeder einen bestimmten Aspekt des Netzwerks beziehungsweise Geräts überwacht. In der Regel findet PRTG-Network-Monitor während der Discovery die Art beziehungsweise den Type eines gefundenen Geräts selbst heraus und installiert entsprechende Sensoren automatisch, womit das Programm eine gute Grundlage schafft, auf die der Administrator später aufbauen kann. Ähnlich wie der Begriff „Gerät“ ist bei PRTG auch der Begriff „Sensor“ etwas anders zu interpretieren, als Kenner manch anderer Managementapplikation es tun würden: Es handelt sich bei diesen Sensoren nicht um Software, die auf den zu überwachenden Geräten läuft, sondern die Sensoren laufen auf einer zentralen Probe. Von dort aus rufen sie Informationen von den Clients zum Beispiel mittels WMI oder SNMP ab.

Sämtliche Objekte einer PRTG-Monitoring-Konfiguration sind in einer baumähnlichen Hierarchie organisiert, die eine einfach navigierbare Liste darstellt. Administratoren können Objekte in Gruppen zusammenfassen, die einander ähnliche Geräte, Services oder dieselben Standorte

beobachten. Die Hierarchie dient ferner zur Definition einheitlicher Einstellungen für größere Gruppen von Objekten, denn innerhalb der Hierarchie lassen sich Einstellungen vererben. Ganz oben in der Hierarchie befindet sich die Root- oder Hauptgruppe, die sämtliche Objekte eines Setups enthält. Einstellungen auf dieser Ebene gelten für alle Objekte. Jede Gruppe außer der Hauptgruppe ist Teil einer Probe. Eine Probe ist die Plattform, auf der das Monitoring stattfindet. Alle unterhalb der Probe konfigurierten Objekte werden über diese spezifische Probe beobachtet. Jede PRTG-Core-Installation erzeugt automatisch eine lokale Probe, Administratoren erzeugen bei Bedarf weitere Probes oder auch Remote-Probes für das Monitoring von Remote-Geräten außerhalb des Netzwerks. Jede Probe enthält eine oder mehrere Gruppen, die Objekte wie oben erwähnt zusammenfassen. Probes und/oder Gruppen enthalten die zu beobachtenden Geräte, beispielsweise Datei- oder Webserver, Client-Computer, Router und Switches oder beinahe jedes Gerät im Netzwerk, das über eine eigene IP-Adresse verfügt. Automatisch fügt PRTG der lokalen Probe ein so genanntes Probe-Gerät hinzu, das mit verschiedenen Sensoren die Parameter des Computers überwacht, auf dem die Probe selbst läuft. Jedem Gerät lassen sich automatisch oder manuell Sensoren hinzufügen, die einzelne Aspekte des Geräts überwachen. Das können beispielsweise Netzwerkdienste wie SMTP, FTP oder HTTP, Switch-Port-Verkehr, die Prozessorlast eines PCs, der Verkehr der Netzwerkkarte oder ein Netflow-Gerät sein. Jeder Sensor verfügt wiederum über eine Reihe Kanäle, über die er die verschiedenen Datenströme empfängt.

Zwischen den Sensoren lassen sich Abhängigkeiten konfigurieren. So ist es beispielsweise eine gute Idee, Sensoren die Netzwerkdienste auf einem Server überwachen, vom Ping-Sensor abhängig zu machen, denn wenn der Server ohnehin nicht über das Netzwerk erreichbar ist, dann stehen die Netzwerkdienste ja gar nicht zur Verfügung.

Für Geräte, Bibliotheken und Sensoren existieren eine Menge verschiedener vordefinierter Ansichten, darunter Gruppenansichten, Gerätelisten, Favoriten, Top-10-Listen und Querverweise. Außerdem kann der Administrator unter vier verschiedenen Schnellübersichten wählen und sich eine vollständige Sitemap anzeigen lassen. Grundsätzlich ist es natürlich gut, so viele verschiedene Ansichten, Sortier- und Filtermöglichkeiten offeriert zu bekommen. Allerdings muss Paessler darauf achten, die Menüs nicht zu überfrachten. Wer

Neue Sensoren in Version 12

PRTG-Network-Monitor Version 12 enthält folgende neue Sensoren:

Anwendungs-Sensoren:

- Vmware-Host-Server-Health-Sensor: überwacht den Zustand der Hardware eines Vmware-Hostservers.
- Erweiterter Amazon-Cloudwatch-Sensor: überwacht Instanzen von EC2, EBS, RDS DB, ELB, SNS, SQS, Elasticsache in der Amazon-AWS-Cloud.
- WMI-Sharepoint-Process-Sensor: überwacht Sharepoint-Prozesse via WMI.
- WMI-IIS-Application-Sensor: überwacht TotalBytesReceived, TotalBytesSent, TotalGetRequests, TotalPostRequests, TotalAnonymousUsers, TotalFilesReceived/Sent und andere Daten des IIS mit WMI.

Hardware-Sensoren:

- SNMP-Cisco-ASA-VPN-Connections-Sensor: überwacht die aktive VPN-Verbindung einer Cisco-ASA-Firewall via SNMP.
- SNMP-Cisco-ASA-VPN-Traffic-Sensor: überwacht den Datenfluss durch permanente VPN-IPsec-Verbindungen via SNMP und alarmiert, wenn die Verbindung nicht besteht.
- SNMP-Cisco-ADSL-Sensor: überwacht die Verbindungsqualität von ADSL-Verbindungen eines Cisco-Routers.
- Fritz!Box-WAN-Interface-Sensor: überwacht den AVM-Internetrouter für KMU.
- Dell-Powervault-MDi-Sensor: überwacht Dell-MD3000(i)-SANs.
- WMI-HDD-Health-Sensor: unterstützt lokales und entferntes S.M.A.R.T.-Monitoring via WMI.

Andere Sensoren:

- Google-Analytics-Sensor: sammelt Trafficdaten einer Website über Google-Analytics.
- WMI-Remote-Ping-Sensor: misst unter Verwendung von WMI die Ping-Zeit zu einem Ziel von einem Windows-Remote-Computer aus.
- SIP-Options-Ping-Sensor: überwacht, ob ein SIP-Server einen Anruf annehmen und zum nächsten Knoten weiterleiten kann.
- Xen-Host-Sensor: überwacht CPU, Speicher und Netzwerkauslastung sowie andere entscheidende Systemparameter.
- Verbesserte Active-Directory-Integration: unter anderem erhält PRTG jetzt die E-Mail-Adressen von neuen Benutzern direkt vom Active-Directory, wenn die AD-Integration verwendet wird.
- SSH-Script-Sensor: ermöglicht es, ein individuelles Script auf einem OSX/Linux/Solaris-System laufen zu lassen und die Ergebnisse als Sensordaten zurück zu bekommen.
- SSH-Remote-Ping-Sensor: misst unter Verwendung von SSH die Ping-Zeit zu einem Ziel von einem Linux/Unix-Remote-Computer aus.

Steckbrief

**PRTG Network Monitor
Version 12****Hersteller:** Paessler**Charakteristik:** Netzwerk-Monitoring-Software**Preis:** bis zu 10 Sensoren kostenlos, sonst ab 357 Euro für 100 Sensoren**Web:** www.de.paessler.com**Plusminus:**

- + Sehr umfangreiches Paket
- + Schnell und einfach von Null auf Monitoring
- + Durchdachte Objekt-/Gerätehierarchie
- + Gutes Preis-Leistungsverhältnis



das System noch nicht kennt, fühlt sich möglicherweise bei einer ersten Entdeckungsreise erschlagen.

Noch mehr GUIs

Neben der erwähnten Management-schnittstelle im Browser gibt es immer noch die PRTG-Enterprise-Console als Windows-Applikation. Die Enterprise-Console erreicht fast den Leistungsumfang (rund 95 Prozent) der Browser-Applikation und bietet zusätzlich einen zentralen Zugriff auf alle vorhandenen PRTG-Installationen. Für mobile Administratoren stehen ferner eine Mobile-Web-GUI sowie native Apps für I-OS und Android zur Verfügung. Diese Mobile-Applikationen eignen sich für Zugriffe auf das Monitoring-System von unterwegs, außerdem empfangen sie natürlich Alarm- und Warnmeldungen. Für den entgegengesetzten Weg, also das Monitoring mobiler Geräte, bietet PRTG leider nichts. Während der Auto-Discovery ignorierte PRTG I-Pads und Smartphones sogar, obwohl sie IP-Adressen aus den Adressbereichen der durchsuchten Subnetze nutzen und zum Zeitpunkt der Discovery online waren. Zwar ließen sich diese Geräte anschließend (durch Eingabe der IP-Adressen) manuell hinzufügen, aber viel mehr als ein Ping-Test ließ sich dann auch nicht machen. Hier ist noch Potenzial für die Weiterentwicklung von PRTG, denn inzwischen müssen diese mobilen Geräte ja schon als Netzwerkgeräte angesehen werden.

Neue Sensoren

Jede neue PRTG-Version kommt immer auch mit neuen oder verbesserten Senso-

ren, Version 12 bildet da keine Ausnahme. Zugelegt hat das Produkt unter anderem beim Monitoring virtueller Systeme beziehungsweise der Plattformen, auf denen sie laufen. So gibt es nun Sensoren, welche die Hardware von Vmware- und Xen-Hostservern überwachen. Die Nutzer von Cisco-ASA-Firewalls können sich ebenfalls freuen, denn gleich zwei neue Sensoren überwachen die aktiven VPN-Verbindungen einer ASA-Firewall sowie den Datenfluss durch permanente VPN-IPsec-Verbindungen via SNMP. Außerdem gibt es nun einen SNMP-Cisco-ADSL-Sensor, der die Verbindungsqualität von ADSL-Verbindungen eines Cisco-Routers überwacht. Während Cisco-Router in vielen großen Netzwerken zu Hause sind, trifft dies auf AVMs „Fritz!Box“ nur bedingt zu. Trotzdem hat Paessler für diesen bei Privatanwendern und KMUs populären Internet-Router einen eigenen Sensor entwickelt. Ob es da wirklich einen Bedarf gab? Jedenfalls gibt es nun diesen Sensor, und er funktioniert sehr gut – wie übrigens alle PRTG-Sensoren. Gut geeignet, um schnell zu checken, wie es mit der bestellten DSL-Geschwindigkeit tatsächlich aussieht. Für größere Unternehmen viel brauchbarer ist da eher wieder der neue Google-Analytics-Sensor. Die Verfügbarkeit und Ladezeit einer Website messen konnte PRTG auch vorher schon, jetzt sammelt das Produkt zusätzlich auch die über Google-Analytics bereitgestellten Verkehrsdaten. Die Konfiguration ist nicht schwer, es reicht, den Benutzernamen, das Passwort und die Profile-ID für Google-Analytics einzugeben. Gerade für einen Sensor dieser Art ist es sehr nützlich, dass sich Administratoren aussagekräftige Berichte generieren lassen können – mit Datentabellen und/oder Diagrammen, automatisch und periodisch ausgeführt.

Unbedingt zu erwähnen ist noch der SIP-Options-Ping-Sensor, der überwacht, ob ein SIP-Server einen Anruf entgegennehmen und zum nächsten Knoten weiterleiten kann. So ein Monitoring führt zwar eine gute SIP-Software selbst durch, aber es ist sicher vorteilhaft, Informationen dieser Art von unterschiedlichen Geräten in einer zentralen Konsole zu sammeln, zumal fraglich ist, ob alle anderen Applikationen bei einem Fehler so zuverlässig und flexibel alarmieren, wie PRTG-Network-Monitor.

Damit zum Alarmsystem von PRTG-Network-Monitor. Das funktioniert einwandfrei. Alarme und Warnungen zeigt das Programm unübersehbar an und protokolliert sie penibel, auf Wunsch auch per Syslog. Administratoren oder Gruppen von Administratoren, die natürlich alle nicht ständig vor der Konsole sitzen, erhalten Benach-

richtungen via E-Mail, SMS und/oder Pager. Außerdem sendet PRTG auf Wunsch SNMP-Traps. Überhaupt ist das Programm sehr mitteilungsfreudig und liefert permanent brauchbare Informationen und Hilfestellungen. Um Massennachrichten zu vermeiden, lassen sich Nachrichten zusammenfassen. Als Reaktion auf einen Fehler können auch beliebige Programme beziehungsweise Scripts gestartet und/oder HTTP-Aktionen ausgeführt werden. Die dazu notwendigen Konfigurationsoptionen verstecken sich hinter „Kontoeinstellungen“, „Benachrichtigungen“, „Eine neue Benachrichtigung hinzufügen“. Das ist nicht intuitiv, aber wichtig ist, dass es solche Funktionalität überhaupt gibt. Apropos intuitiv, es ist offensichtlich, dass PRTG-Network-Monitor ein sehr umfangreiches und flexibel einsetzbares Produkt geworden ist. Damit hat es leider auch ein wenig eingebüßt an der Leichtigkeit, mit der es sich bedienen lässt. Aber das ist wohl ein Kompromiss, den man eingehen muss, möchte man ein wirklich fast universell einsetzbares Monitoring-Produkt nutzen.

Fazit

PRTG-Network-Monitor überzeugte uns einmal mehr auch in der Version 12. Das Produkt ist schnell und in aller Regel problemlos installiert und Dank automatischer Geräteentdeckung mit ebenso automatischer Installation geeigneter Sensoren ohne viel Federlesen einsatzbereit. Sicher ist eine solche Basiskonfiguration für das spezifische Unternehmen beziehungsweise Netzwerk anzupassen, aber Administratoren, die sich vielleicht zwei, drei Stunden intensiv mit PRTG beschäftigen, sollten damit keine Schwierigkeiten haben. Mehr als 130 Sensoren garantieren große Funktionalität und Flexibilität, und neue Sensoren wie der Google-Analytics- oder der SIP-Options-Ping-Sensor zeigen, dass das Produkt die Grenzen des reinen Netzwerk-Monitorings überschreiten und neue Einsatzgebiete erschließen kann – wir hoffen, dass mobile Geräte zukünftig dazu gehören werden. Dass Paessler sich mit I-OS und Android auskennt, zeigen ja die für diese Betriebssysteme bereits vorhandenen PRTG-Management-Apps. Einer der größten Pluspunkte des Produkts dürfte sein, dass es ohne Agenten arbeitet. Das heißt, dass auf den zu überwachenden Geräten keine zusätzliche Software installiert werden muss. Das Preis-Leistungsverhältnis stimmt ebenfalls.

 **Dirk Jarzyna,**
Redaktion funkschau