



Datacenter Security und Hochverfügbarkeit

IT-Abwehrstrategie als Voraussetzung

Physische RZ-Sicherheit gemäß DIN EN 50600

Incident-Response-Management

Mit Marktübersicht USVs



**Citrix Synergy
in Las Vegas**

Windows 10
aus der Cloud

**Sonderschwerpunkt
Monitoring**

Blick auf Performance
und Schwachstellen

Sonderdruck Paessler
Stetig ausgefeiltere
Überwachung

Testserie Monitoring, Teil 1: Paessler PRTG

Stetig ausgefeiltere Überwachung

Ausgefallene Server, leistungsreduzierte Services und vor Wut tobende Anwender am Support-Telefon: Eine solche Vorstellung senkt die Laune der Administratoren auf Anhieb. So etwas passiert, wenn sie ihre IT-Systeme nicht regelmäßig überwachen. Netzwerk- und Performance-Überwachung lohnen sich schon in kleineren Umgebungen, um sich vor Ärger zu schützen. Der Hersteller Paessler liefert hierfür das Tool PRTG Network Monitor.

Viele US-Unternehmen setzen eine Menge daran, in einem Gartner Magic Quadrant „rechts oben“ (also im „Leaders“-Quadranten) aufzutauchen. Für Paessler, ein mittelständisches Unternehmen aus Deutschland, das sich seit Jahren auf Monitoring spezialisiert hat und zudem im Jahreszyklus anbauen muss, um neue Mitarbeiter unterzubringen, ist die Nennung „links unten“ – in der Kategorie „Niche Players“, aber mit der Tendenz in Richtung „Challengers“ – schon ein echter Erfolg.

Nutzungsdatensammler

PRTG Network Monitor läuft auf allen halbwegs aktuellen Windows-Systemen und sammelt verschiedene Nutzungsdaten der Server, Netzwerkgerätschaften, Anwendungen und Workstations, die der Administrator für eine Überwachung auswählt. Verschiedene Hilfsfunktionen, zum Beispiel eine automatisierte Suche oder ein Softwareassistent, der bei der Auswahl der zu überwachenden Parameter behilflich ist, erleichtern dem Administrator den Einstieg. Alle gesammelten Leistungs- und Messungsdaten speichert PRTG für eine spätere Bewertung und für einen Leistungsvergleich in einer mitgelieferten Datenbank ab.

Messdaten, die PRTG über einen längeren Zeitraum ermittelt, helfen den IT-Verantwortlichen somit bei der Fehlersuche, der Sicherstellung vereinbarter Service-Levels oder der Klärung von Veränderungen in der Service-Qualität.



Die Überwachung und Protokollierung von Leistungsdaten, hier bei einem 24-Port-Switch, ist nach wie vor das Brot- und Buttergeschäft für Administratoren.

PRTG, aktuell in der Version 16.2.24.3686, arbeitet in erster Linie Browser-basierend, nutzt eine moderne Ajax-Oberfläche und bietet verschiedene Oberflächensprachen. Neben dem plattformunabhängigen Web-Browser-Zugriff bietet Paessler Apps für IOS und Android. Der Netzwerkmonitor nutzt standardisierte Netzwerkprotokolle zur Bandbreitenüberwachung, darunter zum Beispiel SNMP, WMI, Packet Sniffing, Netflow, Jflow und Sflow.

Mit mehr als 200 Sensoren für die gebräuchlichen Dienste wie Ping, HTTP, SMTP, FTP und POP3, Packet Sniffing sowie SQL-Sensoren für Oracle, MS SQL und Mysql dürften IT-Verantwortliche beinahe alle gängigen Geräte überwachen können. Abhängig von den gesetzten Parametern und Wünschen des Administrators meldet sich die Software per E-Mail, Pager, SMS oder startet automatisch Skript-Jobs oder Zusatzprogramme. PRTG basiert auf den typischen Standardschnittstellen und benötigt keine zusätzliche Client-Software auf den zu überwachenden Systemen. Für einige Aufgabengebiete gibt es sogenannte „Remote Probes“, die eine tiefere Überwachung ermöglichen.

Erfreulich ist, dass die Software in wenigen Minuten von der Homepage des Herstellers heruntergeladen ist und der Anbieter jegliche Aktivitäten von Seiten des Vertriebs erspart. Die Installation dauert auf jedem aktuellen System ebenfalls nur einige Augenblicke: Datenbank und Web-Service inklusive, ganz ohne Klimmzüge. In der Freeware-Variante gibt es gleich 100 Sensoren gratis dazu – damit können Ad-

ministratoren kleine Umgebungen überwachen und ihre Fähigkeiten beim Umgang mit PRTG erproben. Recht schnell können IT-Verantwortliche mit der Software physische und virtuelle Server ebenso wie Applikationsleistungswerte im Auge behalten und SLAs, QoS-Werte oder Event-Logs analysieren. Ein interaktiver „Map-Designer“, mit dem Administratoren die Landkarten ihrer Netzwerke abbilden, bietet rund 300 verschiedene Objekte wie Status-Icons, Daten-Charts oder Top-10-Listen. Zudem

gibt es die Real-Time Dashboards mit Informationen zu Performance und Status in gefühlter Echtzeit, die IT-Verantwortliche mit individuellen Hintergrundbildern wie Netzwerkplänen oder Landkarten versehen können.

Neuerungen

Bereits seit 1997 entwickelt Paessler Network-Monitoring-Tools. Folglich stecken viele tausende Entwicklerstunden in

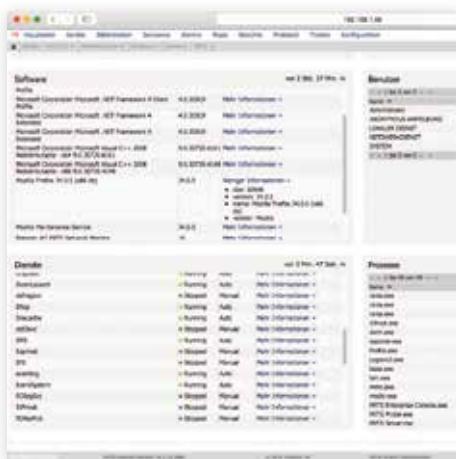
PRTG. Mit einer Basis von 150.000 Benutzern und Zertifizierungen wie „Cisco Compatible“, „Works with Windows Server by Microsoft“ oder „VMware Technology Alliance“-Partner sind die Erwartungen an eine Software bereits sehr hoch. Damit stellt sich die Frage, was die Support-Ingenieure und Entwickler der aktuellen Version mit auf dem Weg gegeben haben.

Der einstige „Guru“, der den Neoadministrator durch die ersten Schritte führte, ist Greg & Co. gewichen: Direkt im Programmfenster tauchen Bilder von Mitgliedern des PRTG-Teams auf und bieten ihre Hilfe an. Sie zeigen dem Benutzer Schritt für Schritt, wo welche Informationen einzugeben sind. Eine symbolisierte Hand fährt beispielsweise von allein auf den jeweiligen Menüpunkt und bittet den Anwender um die Eingabe, zum Beispiel für die SNMP- oder AD-Zugriffsdaten. Insgesamt gelingt so der Start in das Monitoring noch einen Tick schneller.

Im Menü „System Informationen“ liefert PRTG nun Informationen, die Administratoren üblicherweise eher von Inventarisierungsprogrammen erwarten. Wichtige Eckdaten, zum Beispiel Windows-Version, installierte Software, Hardwaredetails wie Prozessor, Drucker, MAC-Adressen, Status der Dienste, aktive Prozesse mit Process ID und verfügbare Benutzerkonten hat PRTG seit der Version 16 zu bieten.

Mit der aktuellen Version umfasst PRTG nun drei neue Sensoren für Dell Equallogic. Grundsätzlich war es zwar auch schon

zuvor möglich, die Storage-Systeme zu überwachen, jedoch liefern die nativen Sensoren SNMP Dell Equallogic Logical Disk, Member Health und Physical Disk feinere Daten. Ein weiterer neuer Sensor heißt ADO SQL v2 und nutzt OLE DB oder ODBC als Nachfolger für den nicht mehr verfügbaren ADO-SQL-Sensor. Die



Neu in der aktuellen Version: Die Systeminformation mit einer Zusammenfassung der wichtigsten Eckdaten zur Hard- und Software.

Leistungswertmessung für die Ein- und Ausgabe von physischen Disks unter Windows haben die Entwickler ebenfalls verjüngt, „Windows Physical Disk I/O“ ersetzt „Windows Physical Disk“, der in den kommenden Versionen nicht mehr verfügbar sein wird. Ähnlich ergeht es dem neuen „WMI Logical Disk I/O“.

Seit dem Februar-Release 16.1.22 erlaubt PRTG für Reports die Ausgabe der zugrunde liegenden Daten in CSV- und XML-Dateien, gemeinsam mit dem eher für Nutzer gedachten neuen PDF-Generator. Die Berichte kann der Administrator weiter auch als HTML anzeigen, die Kombination aus Datendateien und PDF-Bericht erlaubt nun ein Erstellen und Speichern, aber auch einen E-Mail-Versand.

Auch das Hype-Thema „Docker“ fand in diesem Jahr Einzug in die PRTG-Monitoring-Welt. Im vergangenen Jahr verging kaum eine Woche ohne eine neue Meldung zu diesem Tool, und das Interesse an den leichtgewichtigen Linux-Containern und Micro-Services scheint ungebrochen. Dementsprechend bietet PRTG, wenn auch noch als Beta, einige Sensoren für Status, Laufzeit, Exit-Code, CPU-Ausnut-

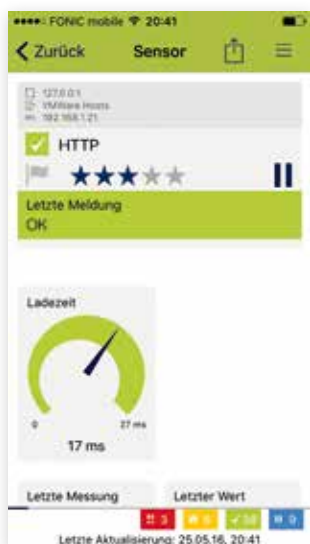
zung und Speicherauslastung für Docker-Container. In den Oberflächen von PRTG entdeckt der Administrator alle notwendigen Elemente, zum Beispiel zur Zertifikatsnutzung oder Eingabe des privaten Schlüssels. Ebenfalls noch im Betastadium ist der neue Amazon-Cloudwatch-Alarm-Sensor, der über die AWS Cloudwatch API die Funktionalität und Zuverlässigkeit der Cloud-Dienste zu überwachen vermag.

Doppeltes Fazit

Unser Fazit fällt gut aus – PRTG war schon vor Jahren gut und wird von Version zu Version einfach immer besser. Während viele Konkurrenzlösungen den Administrator mit Statusmeldungen förmlich überfluten, hält sich die Software von Paessler dezent zurück und beschränkt sich auf die wichtigsten Meldungen. Das Einbinden neuer Geräte gelingt schnell und ist nach einer recht kurzen Gewöhnungsphase durchaus intuitiv. PRTG ist sehr weit entfernt von den Qualen einer Nagios-Überwachung, die jedoch – auch das muss gesagt sein – ebenfalls ihre Vorzüge hat.

Zurück zum magischen Viereck von Gartner: Die Marktforscher sehen die Stärken des Programms in der zügigen Entwicklung und Sensorenbereitstellung im Quartalstakt. Die Clustering-Fähigkeit der Software heben sie ebenfalls hervor. Weiter schätzen die Analysten positiv ein, dass es eine Freeware-Version ohne besondere Verkaufsaktivitäten gibt. Nachteilig, so Gartner, seien die limitierten Fähigkeiten des Paket-Sniffers, die Fokussierung auf den Mittelstand und die gerade erst gestarteten SaaS-Provider-Aktivitäten.

Thomas Bär und Frank-Michael Schlede/jos



Dank Apps können Netzwerkverantwortliche auch per iPhone, Windows Phone oder Android-Device auf ihre Überwachung zugreifen.

Thomas Bär auf LANline.de: **BÄR**

Frank-Michael Schlede auf LANline.de: **Frank-Michael Schlede**

Info: Paessler AG
Tel.: 0911/93775-0
Web: www.de.paessler.com