PAESSLER

WHITEPAPER

11 Aspekte, wie Netzwerk-Monitoring die tägliche Arbeit eines Administrators erleichtern kann

Whitepaper

PRTG NETWORK MONITOR

Autor: Gerald Schoch, Technischer Redakteur, Paessler AG
Erstveröffentlichung: Oktober 2013

Inhalt

Einleitung

Auch der beste IT-Administrator sehnt sich manchmal nach Hilfe. Sein Alltag steckt voller Überraschungen. Störungen im Netzwerk treten meist unangekündigt auf. Der Admin kann beruhigt arbeiten, wenn ihm eine Überwachungs-Software als Freund zur Seite steht. Im Folgenden zeigen elf typische Fälle aus dem Alltag, wie ein Administrator Störfälle durch den Einsatz einer Netzwerk-Monitoring-Software einfacher in den Griff bekommt.

Die IT-Verantwortlichen in Unternehmen haben es in ihrem Arbeitsalltag mit unterschiedlichsten Herausforderungen zu tun. Eine Netzwerk-Monitoring-Software kann sie dabei unterstützen indem das Tool die gesamte IT-Infrastruktur überwacht und die IT-Abteilung alarmiert, sobald Ungewöhnliches passiert. Auch bei der Beantwortung der folgenden, immer wieder gestellten Fragen, kann die Monitoring-Lösung dem Administrator helfen:

- Arbeiten alle Hardware-Komponenten gleichbleibend gut?
- Sind alle Server und Services aktiv?
- Wie überstehe ich geplante Downtimes ohne falsche Alarme?
- Funktioniert die Security-Software im Netzwerk?
- Was passiert, wenn plötzlich Rauch oder Wasser im Serverraum austreten?
- Arbeiten Webseite und Online-Shop einwandfrei?
- Gibt es Störungen bei Voice-over-IP-Verbindungen oder Video-Streams?
- Laufen interne Datenbanken stets auf hohem Niveau?
- Wie finde ich Fehlerquellen in virtualisierten Umgebungen?
- Habe ich alle laufenden Backups im Blick?
- Sind die Drucker jederzeit arbeitsbereit?

Die Bedürfnisse des Netzwerks auf einen Blick

1. POTENZIELLE HARDWARE-PROBLEME FRÜH ERKENNEN

Ein Administrator hat unter anderem die Aufgabe, die Hardware-Komponenten der Infrastruktur täglich zu prüfen. Die Leistung von CPU, Speichergeräten, Servern & Co. sollte gleichbleibend hoch sein. Eine Netzwerk-Monitoring-Lösung hilft ihm, den Status dieser Komponenten zu überwachen. Sie liefert detaillierte Daten und Langzeitberichte zur gesamten Hardware. Durch Analyse dieser Informationen kann der IT-Verantwortliche Trends erkennen und den Optimierungsbedarf bestimmen. Die Software alarmiert ihn sofort, wenn eingerichtete Schwellwerte überschritten werden oder falls Serverausfälle auftreten. Auf diese Weise ist es für den Administrator möglich, vorausschauend zu agieren statt nur zu reagieren.

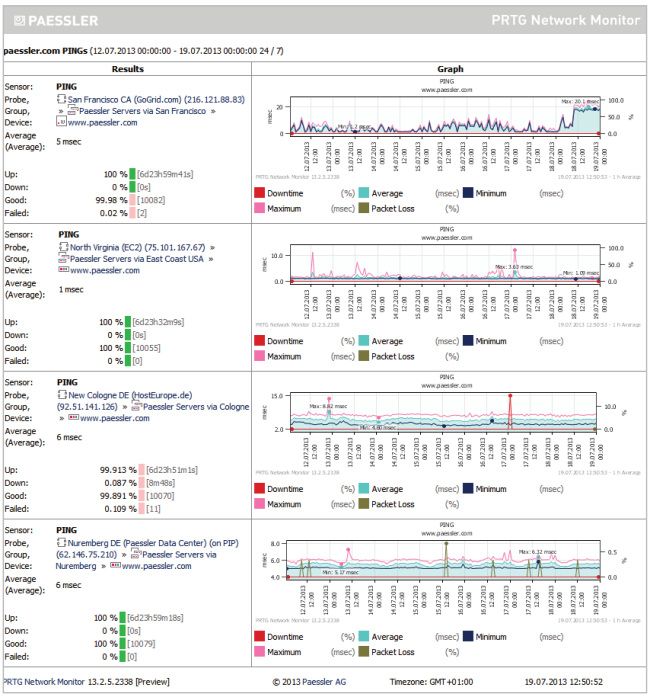


ABBILDUNG:
Bericht über Ping Sensoren

2. FEHLERHAFTE WINDOWS-SERVICES UND SERVER-NEUSTARTS

Innerhalb der IT-Infrastruktur eines Unternehmens sind viele Server und Services aktiv. Wenn es hier zu Fehlern kommt, kann es notwendig werden den Server neu zu starten, um Probleme zu beheben. Wenn Administratoren die Windows-Services via Netzwerk-Monitoring überprüfen lassen, erhalten sie bei Ausfällen eine Benachrichtigung per SMS, E-Mail etc., aber ein Neustart muss manuell ausgeführt werden.

Effizienter wäre es, wenn der Neustart des Servers automatisch ausgelöst wird, ohne Zutun des Admins. Mit dem Benachrichtigungssystem der Monitoring-Software ist dies möglich. Dazu erstellt der Administrator ein Skript, das einzelne Services oder den kompletten Server rebooten kann. Wenn ein Service oder Server für eine gewisse Zeitspanne „down“ ist, führt die Monitoring-Software dieses Skript über eine spezielle Art von Benachrichtigung aus und der Neustart erfolgt automatisch. Ein standardmäßig verfügbarer Sensor kann Windows-Services mit einer entsprechenden Option im Falle eines Ausfalls auch automatisch neu starten.

3. GEPLANTE AUSFALLZEITEN STRESSFREI ÜBERSTEHEN

Ausfälle von Servern geschehen nicht immer ungeplant. Ab und zu ist es erforderlich, Netzwerkgeräte planmäßig außer Betrieb zu setzen – z.B. für Wartungsarbeiten oder einfach um Systeme am Wochenende oder über Nacht herunterzufahren. Damit die Überwachungslösung in diesen Zeiträumen der geplanten Downtimes nicht unnötig falsche Alarme auslöst, kann der Administrator das Monitoring zeitweise pausieren lassen. Die Pausierung kann über zuvor festgelegte Zeitpläne auch für einzelne Netzwerkkomponenten automatisch erfolgen.

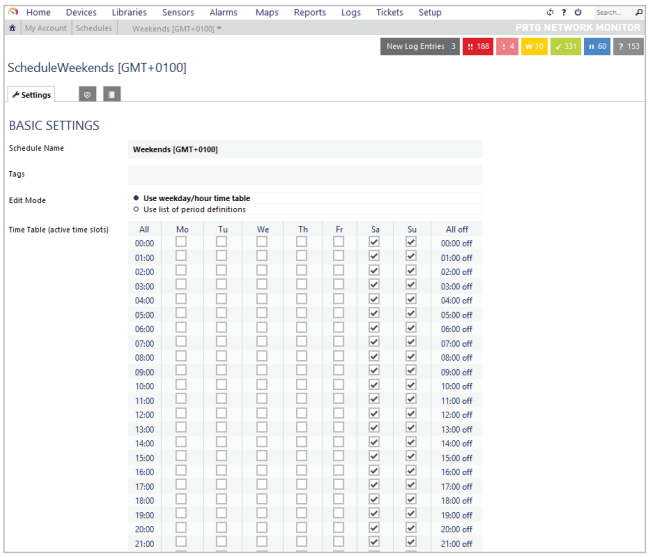


ABBILDUNG :
Variabel festlegbare Zeitpläne

Qualität und Sicherheit im Netzwerk gewährleisten

4. SICHERHEITSPROBLEME IM NETZWERK ERKENNEN

Vor Malware-Gefahren schützen sich die meisten Unternehmen mittels Security-Lösungen wie Antiviren-Scanner, Firewalls etc. Dadurch fühlen sie sich ausreichend abgesichert. Doch auch die Sicherheits-Software ist nicht vor Ausfällen gefeit. Daher überprüfen Administratoren stetig, ob Antiviren-Software und Firewalls auf allen Computern laufen und up-to-date sind. Des Weiteren sollte die aktuelle Windows-Version auf dem neuesten Stand sein und Security-Updates lückenlos durchgeführt werden. Trotz aller Sicherheitsmaßnahmen kann das Unternehmensnetzwerk Cyberattacken zum Opfer fallen. Ungewöhnliche CPU-Last bzw. Traffic-Spitzen können Anzeichen dafür sein.

Eine gute Netzwerk-Management-Software erkennt dies und schaltet die dazugehörigen Sensoren in einen Status, der „ungewöhnliche Werte“ anzeigt. Zusätzlich überwacht die Monitoring-Software den allgemeinen Sicherheitsstatus: z.B. die Antivirus-Software eines Windows-Computers mit WMI Security Center-Sensoren oder Windows Server-Updates mit WSUS Statistics-Sensoren. Eine andere hilfreiche Funktion für das Security-Monitoring ist die „Similar Sensors-Analyse“. Sie kann dabei helfen, verdächtige Abhängigkeiten zwischen Sensoren zu erkennen. Dank dieser vielfältigen Überwachungs- und Analysemöglichkeiten steigert die Monitoring-Lösung die Sicherheit im Netzwerk.

5. PHYSISCHE SICHERHEIT IM DATA CENTER

Neben der Netzwerksicherheit hat auch die physische Sicherheit Priorität: Hohe Temperaturen, Feuchtigkeit, Wasserlecks, Feuer, Rauch etc. könnten die Ausrüstung eines Serverraums oder eines Rechenzentrums beschädigen. Um sicherzustellen, dass alle Geräte außer Gefahr sind, ist es ratsam auch Umgebungsparameter zu monitoren. Mittels Hardware-Sensoren für Temperatur, Feuchtigkeit etc. identifiziert die Software, wenn ungewöhnlich hohe Werte auftreten. Wenn zum Beispiel eine APC-Sensor-Box Temperaturen über 27 Grad misst, wird der IT-Verantwortliche alarmiert. Die Monitoring-Software kann auch die Funktion aller installierten Überwachungskameras prüfen, oder sie checkt, ob alle Türen und Fenster verriegelt sind, wenn die Mitarbeiter am Abend das Gebäude verlassen.

6. WEBSEITEN HOCHVERFÜGBAR HALTEN

Die Webseite ist für Firmen das Aushängeschild schlechthin. Internetauftritt inklusive gegebenenfalls vorhandenem Webshop spiegeln das Unternehmen und seine Leistungen digital wieder. Demnach ist deren Verfügbarkeit von enormer Bedeutung. Ist die Webseite nicht rund um die Uhr erreichbar, kommt es zu langen Ladezeiten oder scheitern beispielsweise die Kauf-Prozesse im Webshop an technischen Fehlern, könnten Anbieter dadurch Kundschaft verlieren.

Um mögliche Verluste zu vermeiden, warnt die Netzwerk-Überwachungslösung sofort, wenn die Webseite ungewöhnliches Verhalten aufweist (sie z.B. sehr langsam ist). Das Monitoring nutzt unter anderem HTTP Full Web Page-Sensoren, um die Ladezeiten der Seite zu überprüfen. Der HTTP Transaction-Sensor misst darüber hinaus den erfolgreichen Abschluss von Transaktionen auf einer interaktiven Webseite (Webshop). Zudem steht dem IT-Personal beispielsweise ein HTTP Apache ModStatus Totals-Sensor zur Verfügung, der Webseiten-Zugriffe und übertragene Daten prüft, um Lastspitzen zu bestimmten Zeiten zu identifizieren. So kann der Administrator auch erkennen, wenn mehr Bandbreite zur Verfügung gestellt werden muss.

7. QUALITY-OF-SERVICE ÜBERPRÜFEN

Für die Business-Kommunikation sind die Tonqualität von Voice-over-IP(VoIP)-Verbindungen sowie das Video-Streaming immens wichtig. Hakt es bei solchen Verbindungen, müssen Administratoren die relevanten Parameter der Netzwerkverbindung (Jitter, Packet Loss oder Packet Delay) untersuchen. Welche Parameter könnten für das Problem verantwortlich sein? Sowohl VoIP als auch Video-Streams verlassen sich auf einen stetigen Strom von Datenpaketen. Die Quality-of-Service leidet z.B. wenn UDP(User Datagram Protocol)-Pakete nicht rechtzeitig empfangen werden oder verloren gehen. Professionelle Monitoring-Lösungen bieten einen vorkonfigurierten Quality of Service(QoS)-Sensor, mit dem Administratoren die Qualität der Netzwerkverbindungen messen können. Durch die detaillierten Informationen können IT-Abteilungen den Optimierungsbedarf präzise bestimmen und entsprechende Probleme beheben.

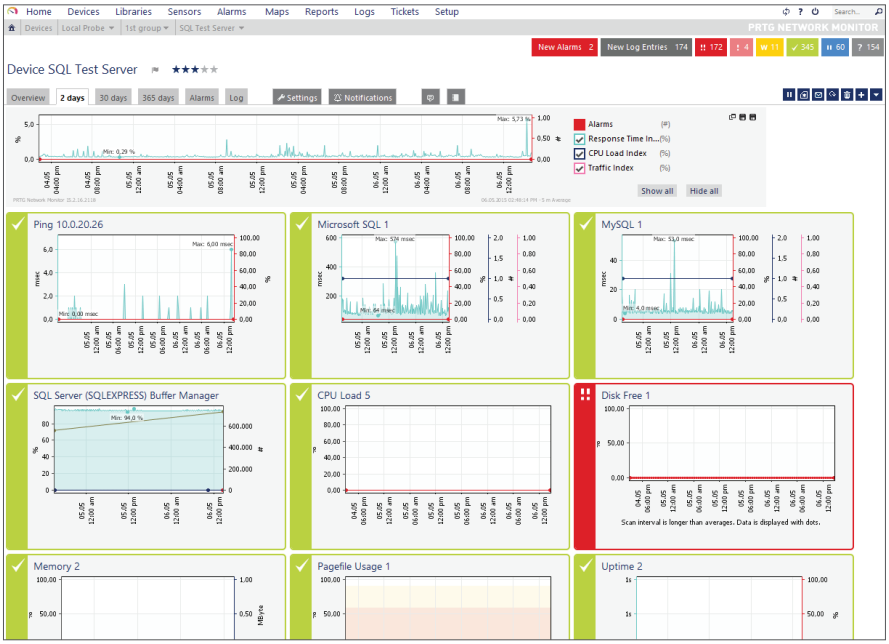
Basissysteme im Blick behalten

8. SCHLECHTE DATENBANK-PERFORMANCE

Im Arbeitsalltag greifen Mitarbeiter auf unzählige Daten aus dem Unternehmensnetzwerk zu. Weisen die internen Datenbanken eine schlechte Leistung auf, lähmt dies die Arbeitsprozesse in der gesamten Firma. Die alltägliche Aufgabe des Administrators besteht also auch darin, die Leistungsindikatoren der Datenbanken zu überprüfen.

Schwankt die Leistung einer Datenbank, müssen IT-Verantwortliche die Gründe dafür finden. Diese Suche kann eine langwierige Aufgabe sein. Eine professionelle Monitoring-Software unterstützt das IT-Personal bei der Leistungssteigerung der Datenbank. Beispielsweise zeigen WMI SQL-Server-Sensoren die Anzahl von Nutzerverbindungen an. Ist die Leistung zu bestimmten Zeiten schlecht, könnten zu viele Nutzer zeitgleich aktiv sein. Ist dies der Fall, wäre es Administratoren z.B möglich, den verfügbaren Speicher auf dem SQL-Server zu erhöhen und das Problem aus der Welt zu schaffen.

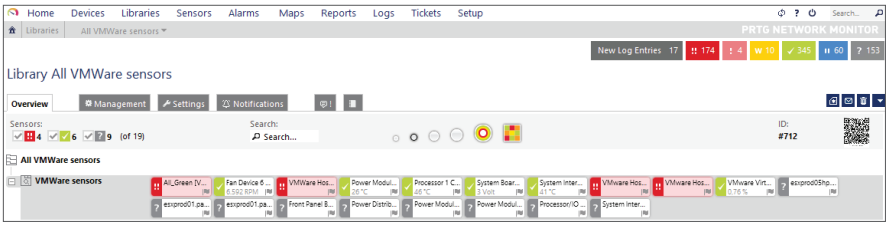
ABBILDUNG:
Monitoring-Daten für einen SQL-Server



9. UNZUVERLÄSSIGES VERHALTEN IN VIRTUELLEN UMGEBUNGEN

In Zeiten hochflexibler IT-Infrastrukturen spielt die Virtualisierung eine große Rolle für den Administrator. Er sollte die virtuellen Systeme immer im Blick haben. Eine Netzwerk-Monitoring-Software bietet verschiedene Sensoren zur Überwachung virtualisierter Umgebungen an. Unter anderem kann das IT-Personal die CPU- und Speicherauslastung, die Netzwerkgeschwindigkeit sowie die Gesamtperformance virtueller Maschinen überwachen. PRTG Network Monitor von Paessler unterstützt dazu z.B. die Plattformen VMware, HyperV, Citrix und Virtuozzo. Auch den Status der Hostserver haben die Administratoren immer im Blick. So können Administratoren unmittelbar erkennen, ob das Problem in der virtuellen Maschine liegt oder von der Hosthardware verursacht wird. Misst einer der Sensoren auffällige Werte, zeigt die Netzwerk-Monitoring-Lösung dies an und sendet eine Nachricht an den zuständigen IT-Verantwortlichen.

ABBILDUNG:
VMware Sensoren



10. BACKUPS ÜBERBLICKEN

In der IT-Infrastruktur werden verschiedene Backups durchgeführt: Im Bereich der Virtualisierung, im Betriebssystem, bezüglich SQL und Exchange sowie online laufen täglich Datensicherungen ab. Hier hilft Administratoren eine Backup-Software. Diese Lösungen senden meist E-Mails, die den Status der nächtlich ablaufenden Datensicherungen bekanntgeben. Aber für den Administrator ist es nicht einfach, den Überblick über all diese Backup-Prozesse zu behalten. Er müsste Unmengen von E-Mails analysieren, bis er endlich ein Backup-Problem identifizieren kann. Allerdings können IT-Verantwortliche ihre Software so konfigurieren, dass sie alle Status-E-Mails an ein Postfach sendet, wo sie mit IMAP-Sensoren des Netzwerk-Monitorings automatisch analysiert werden. Auf diese Weise behält die Überwachungslösung den Überblick über alle Datensicherungen, meldet, wenn Backups nicht ordnungsgemäß durchgelaufen sind und der Administrator ist entlastet.

11. ZEITAUFWÄNDIGE WARTUNG DER DRUCKER

Wegen der vielen wichtigen Aufgaben des Alltags, möchte ein IT-Administrator seine knappe Zeit nicht damit verbringen, jeden Tag den Status aller Drucker manuell zu checken. Es ist nervig, wenn man konzentriert bei der Arbeit ist und wegen mangelndem Papier oder einem Papierstau gerufen wird. Eine Monitoring-Lösung schafft hier unter anderem mit Windows Print Queue-Sensoren Abhilfe. Die Sensoren überwachen alle Aufträge auf einem Drucker-Server. Wenn das Papier zur Neige geht, erhält der Administrator rechtzeitig eine Warnmeldung und kann zu passender Zeit reagieren, bevor Anfragen von Kollegen eintreffen. Zudem ist das IT-Personal in der Lage, die Überwachungs-Software so einzurichten, dass sie einem Lieferanten eine automatische E-Mail schickt, wenn zum Beispiel der Toner fast leer ist. So müssen sich Administratoren weniger Gedanken um diese Standardaufgabe machen.

Fazit

Eine Netzwerk Monitoring-Lösung wie PRTG Network Monitor bietet einem Administrator Hilfestellung bei Herausforderungen seines Arbeitsalltags. Durch die Überwachung aller Netzwerkkomponenten und sogar der Umgebungsparameter des Serverraums gibt die Software der IT-Abteilung ein sicheres Gefühl. Probleme werden schnell erkannt, umgehend gemeldet und können zügig behoben werden, bevor wirklicher Schaden entsteht. Die Netzwerk-Monitoring-Lösung steht dem Administrator als ausfallsicherer und umfassender Helfer rund um die Uhr zur Seite.

ÜBER DIE PAESSLER AG

Die Paessler AG ist seit Jahren führend in der Entwicklung von leistungsfähiger, bezahlbarer und benutzerfreundlicher Netzwerk-Monitoring-Software. Paessler Produkte sorgen für Ruhe und Sicherheit in IT-Abteilungen von Unternehmen aller Größen - von SOHOs über KMUs bis hin zu global tätigen Konzernen – umfassend, unkompliziert und zuverlässig. Vom Firmensitz in Nürnberg aus betreut Paessler über 150.000 Installationen seiner Produkte, die weltweit im Einsatz sind. Das 1997 gegründete Unternehmen ist bis heute privat geführt und sowohl Mitglied des Cisco Solution Partner Program als auch ein VMware Technology Alliance Partner.

Freeware und Testversionen aller Produkte können unter www.paessler.de/prtg/download heruntergeladen werden.

Paessler AG · www.paessler.de · info@paessler.com