Das Ganze Netz im Blick

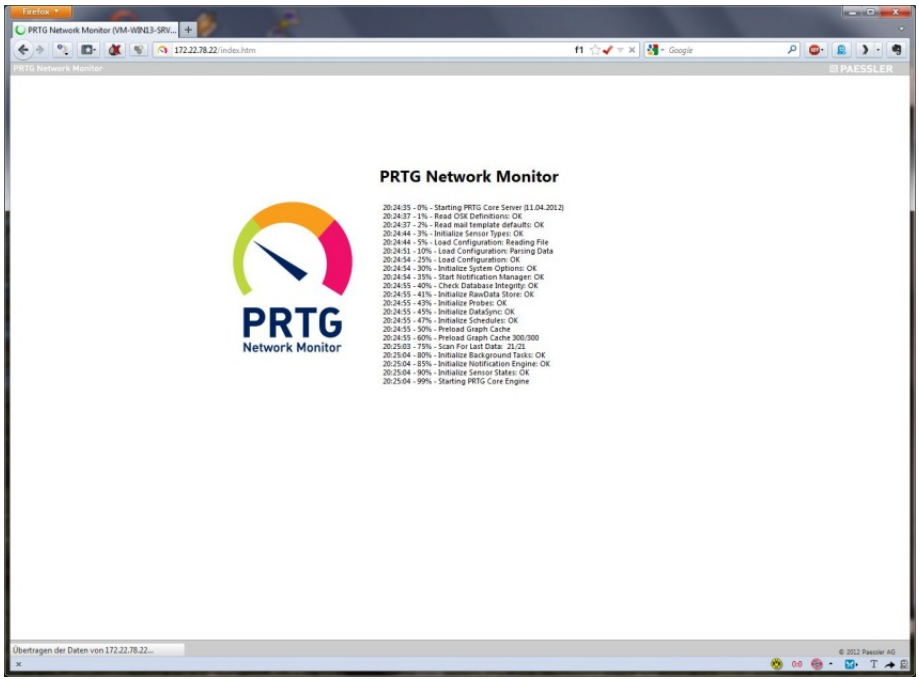
Dr. Götz Güttich

Der PRTG Network Monitor der Paessler AG arbeitet unter Windows und sammelt Nutzungsdaten von Rechnern, Anwendungen und anderen Infrastrukturkomponenten im Netz. Alle Informationen landen in einer zentralen Datenbank und lassen sich später für umfassende Analysen nutzen. Die Administration des Werkzeugs läuft über ein leistungsfähiges Web-Interface oder eine native Windows-Applikation ab. Beim Sammeln der Daten setzt PRTG auf mehrere unterschiedliche Technologien, nämlich WMI, SSH, SNMP, NetFlow, jFlow und sFlow sowie Packet Sniffing. IAIT hat sich angesehen, wie die Arbeit mit der Lösung im laufenden Betrieb von der Hand geht.

Paessler verfolgt mit dem PRTG Network Monitor das Ziel, Administratoren proaktiv auf Schwierigkeiten im Netz aufmerksam zu machen und sie so über Probleme zu informieren, bevor diese auftreten. Zu diesem Zweck bringt die Lösung mehr als 130 Sensortypen mit, die sich dazu eignen, Parameter wie die Prozessorlast einzelner Systeme, den freien Speicherplatz und die Auslastung der Netzwerkschnittstellen zu überwachen. Genauso stehen auch Sensoren für Netzwerkdienste wie HTTP, SMTP, POP3, FTP und ähnliches zur Verfügung. Der Begriff "Sensor" ist in diesem Zusammenhang nicht wörtlich zu verstehen: PRTG arbeitet ohne Agenten, also ohne irgendeine Softwarekomponente auf den zu überwachenden Client-Systemen. Die Sensoren laufen auf einer zentralen "Probe" (bei Bedarf lassen sich auch mehrere Probes im Netz einrichten) und fragen die Clients von dort aus über die genannten Protokolle wie beispielsweise WMI, SNMP oder SSH regelmäßig über ihren Status ab. Die dabei gewonnenen Erkenntnisse landen in der zentralen Datenbank und lassen sich an-

schließend für umfassende Analysen nutzen, die dann ihrerseits zum Einsatz kommen können, um das Netzwerk zu optimieren. Treten irgendwelche Schwierigkeiten auf, so ist PRTG auch dazu in der Lage, Warnmeldungen unter anderem per E-Mail, SMS oder Pager zu verschicken.

Das Lizenzmodell arbeitet mit der Zahl der Sensoren. Bis zu zehn Sensoren sind kostenlos, benötigt ein Unternehmen mehr, so kann es sie je nach Bedarf hinzukaufen. Bei PRTG sind alle Funktionen in jeder Lizenz enthalten, unabhängig von der Lizenzgröße. Es steht eine 30-tägige Testversion mit einer unbegrenzten Anzahl von Sensoren zur Verfügung.



Der PRTG Network Monitor beim Start

Architektur

Was die Architektur angeht, so setzt PRTG auf einen Core Server, der mit einem Ajax-Web-Interface arbeitet. Dieses Interface stellt das Hauptmanagementtool dar und bietet den größten Funktionsumfang. Alternativ steht ein Windows-basiertes Verwaltungswerkzeug namens "Enterprise Console" zur Verfügung, das fast den vollen Leistungsumfang bietet (laut Hersteller 95 Prozent). Dazu kommt noch ein "Mobile Web GUI", das die Daten in einer für mobile Endgeräte optimierten Form bereitstellt. Apps für iOS und Android runden die Zugriffsmöglichkeiten auf das Netzwerküberwachungssystem ab. Die Android-App (PRTGdroid) ermöglicht den Anwendern einen einfachen Zugriff auf das mobile Web-Interface der Paessler-Software und kann die Administratoren darüber hinaus im Fehlerfall direkt informieren. Die iOS-App (iPRTG) ruft die Daten vom Webserver über das API ab und zeigt sie anschließend im nativen iPhone-Stil an. Für die tägliche Arbeit vom Desktop aus empfiehlt Paessler übrigens den Einsatz der Browser Chrome und Firefox, wir setzten im Test auch den Internet Explorer ein und hatten dabei keine Schwierigkeiten.

Neben dem Core Server verwendet PRTG auch noch die zuvor erwähnte Probe, die die Abfragen bei den Clients durchführt. Auf Wunsch lassen sich mehrere verteilte Probes einsetzen, was unter anderem dann Sinn ergibt, wenn es darum geht, neben dem lokalen Netz auch entfernte Installationen zu überwachen und trotzdem alle Informationen an einer zentralen Stelle einzusehen. Mit der Enterprise Console ist es darüber hinaus möglich, mehrere PRTG-Installationen zentral zu verwalten.

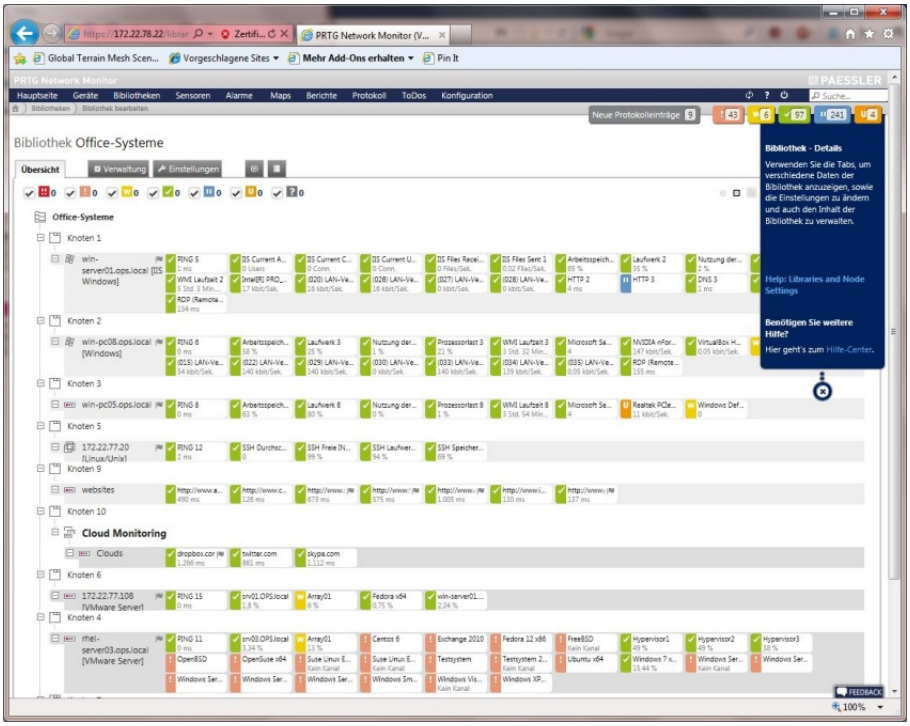
Die Sensoren verfügen wiederum über so genannte Kanäle, mit denen sich einzelne Parameter in Erfahrung bringen lassen. Im Fall des Arbeitsspeicher-Sensors sind das zum Beispiel der Arbeitsspeicher selbst und der verfügbare Speicher in Prozent.

Zwischen den Sensoren lassen sich auch Abhängigkeiten definieren. So ist es beispielsweise möglich, einen Ping- und einen HTTP-Sensor einzusetzen, um einen Webserver zu überwachen. Meldet der Ping-Sensor einen Fehler, so pausiert das System den von ihm abhängigen HTTP-Sensor. Das ergibt Sinn, da der HTTP-Dienst zwangsläufig nicht zur Verfügung steht, wenn sich der betroffene Server über das Netz nicht ansprechen lässt. Der Administrator erhält in diesem Fall nur eine Fehlermeldung, die besagt, dass der Webserver nicht antwortet, nicht zwei. Das verbessert die Übersichtlichkeit deutlich, vor allem wenn es darum geht, Systeme zu überwachen, die mit einer Vielzahl von Sensoren arbeiten.

Generell gilt, dass die Sensoren – je nach Anwendungsgebiet – sehr leistungsfähig sind. Es ist mit ihnen bei Bedarf beispielsweise

IAITested

nicht nur möglich, die Tatsache festzustellen, dass ein Webserver auf Anfragen reagiert, sondern die IT-Verantwortlichen können das System auch so konfigurieren, dass es bestimmte Inhalte abfragt oder sogar einen Kauf in einem Online-Shop simuliert, dagespeichert, auf Wunsch lassen sich auch längere Speicherintervalle einrichten.



In der Geräteübersicht sehen die zuständigen Mitarbeiter den Status der einzelnen Sensoren

mit sichergestellt wird, dass der Dienst wirklich in der gewünschten Form läuft. Wurde zum Beispiel eine Website gehackt, so arbeitet der Webserver danach ja immer noch, die gezeigten Inhalte können aber erheblich von denen abweichen, die das betroffene Unternehmen eigentlich zeigen möchte. So etwas lässt sich nur herausfinden, wenn die Überwachungssoftware nicht nur die Antwort des Dienstes auswertet, sondern auch den Inhalt derselben.

Bei Bedarf ist es zudem möglich, jederzeit eigene Skripts als Sensortypen in PRTG zu integrieren. Alle gefundenen Daten werden standardmäßig bis zu einem Jahr

Der Test

Für unseren Test installierten wir die Version 12.2 des PRTG Network Monitors auf einem Windows-Server-2008-R2-System in unserem Netz und setzten die Lösung anschließend ein, um Rechner unter Windows XP, Windows Server 2008, Windows 7, Windows Server 2008 R2, Redhat- und Fedora-Linux, Ubuntu-Linux, MacOS sowie Solaris zu überwachen. Dazu kamen noch diverse Netzwerkkomponenten wie beispielsweise Switches von Cisco und Router von Netgear und Lancom. Abgesehen davon nahmen wir noch einige Websites, wie etwa die IAIT-Website und die Online-Dienste Dropbox, Twitter und Skype mit in die Überwachung auf. Da PRTG IPv6 unterstützt, überwachten wir diverse Systeme zudem auch mit Hilfe dieses Protokolls.

Nach der Installation und dem Einrichten der von uns benötigten Sensoren legten wir ein besonderes Augenmerk auf das Monitoring unseres Exchange Servers und unserer Virtualisierungsumgebung auf Vmware-Basis. Abgesehen davon nahmen wir den gesamten Leistungsumfang der Monitoring-Software unter die Lupe, einschließlich Gerätebaum, Bibliotheken, Maps, Berichten und Alarmen. Last but not least verwendeten wir die App PRTG-droid, um aus der Ferne auf unsere Installation zuzugreifen.

Installation

Paessler empfiehlt, den PRTG Network Monitor aus Performancegründen nicht in einer virtuellen Maschine zu installieren, sondern ein aktuelles Windows Betriebssystem auf einem dedizierten Host zu verwenden. Für die bestmögliche Leistung sollte ein System mit vier GByte RAM und ein paar hundert GByte Festplattenplatz zum Einsatz kommen. Abgesehen davon muss der zum Überwachen eingesetzte Rechner mit dem Dotnet-Framework 4.0 ausgestattet sein.

Die Installation des Produkts läuft – wie unter Windows üblich – Wizard-gesteuert ab und wird keinen Administratoren vor irgendwelche Probleme stellen. Er muss im Wesentlichen nur die richtige Sprache auswählen, seinen Lizenzschlüssel eingeben und sein Mail-Konto definieren. Ein Failover-Cluster kann auf Wunsch später eingerichtet werden.

Nach dem Abschluss des Setups öffnete sich auf unserem System der Browser mit dem PRTG-Login-Screen und wir konnten uns erstmalig bei dem Monitoring-

Produkt anmelden. Normalerweise kommt zu diesem Zeitpunkt der Konfigurations-Guru hoch, der die Administratoren bei der Erstkonfiguration des Systems unterstützt. Da wir einen Windows Server mit dem Internet Explorer und verstärkter Sicherheitskonfiguration verwendeten, mussten wir die PRTG-Seite aber erst zu den vertrauenswürdigen Seiten des Internet Explorers hinzufügen, um dafür zu sorgen, dass das System alles richtig anzeigte.

Der Konfigurations-Guru

Der Konfigurations-Guru hilft den zuständigen Mitarbeitern bei der grundlegenden PRTG-Konfiguration. Im ersten Schritt macht er die Mitarbeiter darauf aufmerksam, dass es sinnvoll sein könnte, die Zugriffe auf das Web-Interface der Lösung per SSL zu verschlüsseln. Dabei haben die User die Möglichkeit, diese SSL-Verschlüsselung zu aktivieren oder den Schritt zu überspringen. Diese beiden Optionen – also Durchführen der vorgeschlagenen Aufgabe oder Sprung zum nächsten Punkt – stehen bei allen Schritten des Konfigurations-Gurus zur Verfügung.

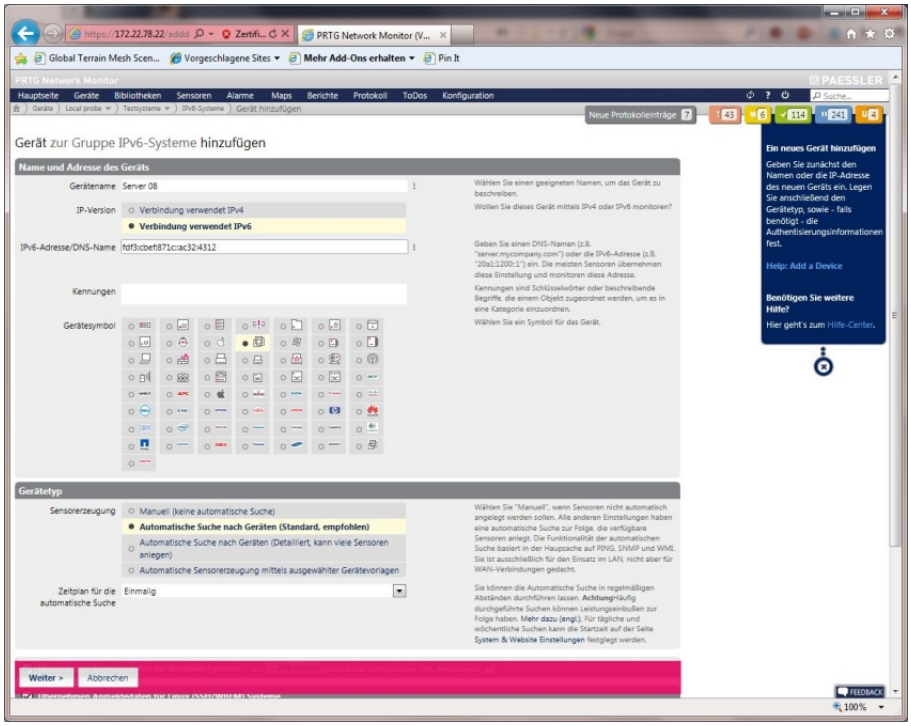
Nachdem wir die SSL-Verschlüsselung eingerichtet hatten, legten wir mit Hilfe des Konfigurations-Gurus zunächst unser Administrations-Passwort fest und trugen die Anmeldedaten für die Windows-Systeme – also die Domäne in unserem Netz – ein. Dieser Schritt ist erforderlich, damit PRTG auf die entsprechenden Rechner zugreifen kann, um Informationen abzufragen. Anschließend fragte der Guru nach SNMP- sowie Vmware- und Xen-Anmeldedaten sowie Credentials für Linux-Systeme und bot an, die Internet-Verbindung mit Gateway und DNS-Servern zu überwachen.

Im nächsten Schritt konnten wir die Server angeben, die PRTG im Netz im Auge behalten sollte. Dazu bot uns der Guru Domänenkontroller, Exchange- oder andere Mail-Server sowie weitere Server nach Name oder IP-Adresse an. Hier trugen wir zunächst nur unseren Domänenkontroller und unseren Exchange Server ein, da wir die weiteren Systeme später über eine allgemeine Netzwerksuche in die PRTG-Umgebung aufnehmen wollten.

führte der Konfigurations-Guru dann eine automatische Netzwerksuche nach Systemen in unserem LAN durch. Dabei wurden alle aktiven Komponenten auf Anhieb gefunden. Bei den Vmware-Systemen erkannte PRTG auch, dass es sich um Hosts virtueller Maschinen (VMs) handelte und führte die darauf installierten VMs gleich als Sensoren mit auf.

Die automatische Netzwerksuche

Die automatische Netzwerksuche lässt sich jederzeit manuell starten oder per Zeitplan regelmäßig automatisch ausführen. Sie stellt



Beim Hinzufügen von Geräten lassen sich unter anderem auch die Icons auswählen, unter denen die Devices in der Übersicht erscheinen

Nach dem Einrichten der Serverüberwachung ging es daran, das Monitoring von Websites und Online-Shops einzurichten und auf Wunsch die Überwachung der Cloud-Dienste Google (Search, Drive und Mail), Office 365, Salesforce, Dropbox, iCloud, Facebook, Twitter und Skype zu aktivieren. Zum Abschluss

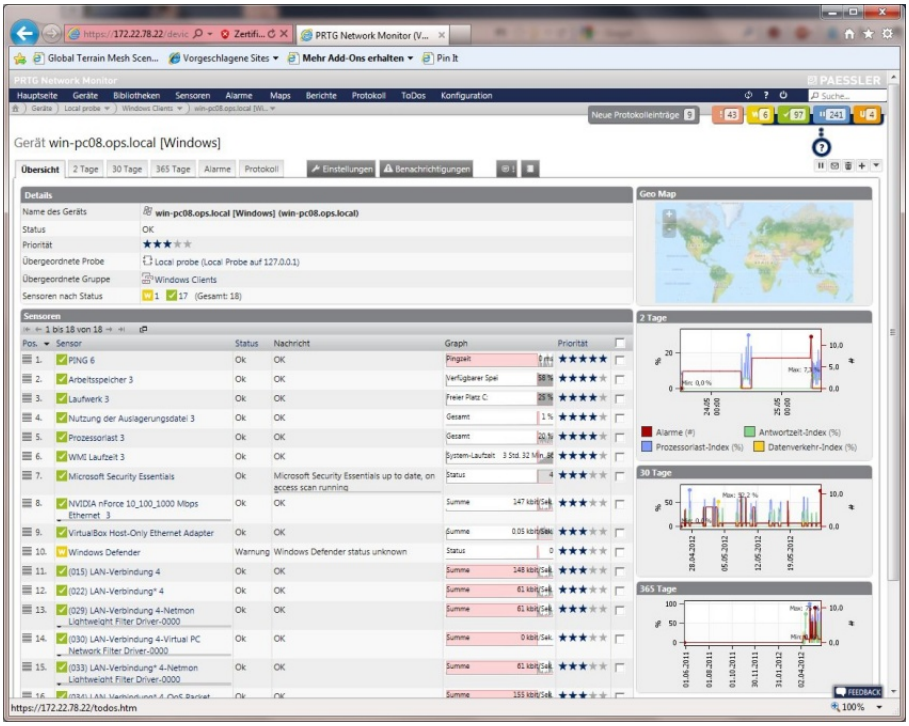
einen guten Weg dar, um die Konfiguration auf dem aktuellen Stand zu halten und neue Systeme mit in die PRTG-Umgebung aufzunehmen. Möchte ein Benutzer beispielsweise eine neue Gruppe mit allen Windows Servern generieren, so reicht es, eine automatische Netzwerksuche anzulegen, die betroffene Probe zu

selektieren, einen Gruppennamen einzutragen und anzugeben, wie die Sensorerzeugung ablaufen soll. Hier gibt es vier Möglichkeiten: manuell, automatisch nach Geräten, automatisch nach Geräten detailliert (diese Methode kann sehr viele Sensoren erzeugen) und Sensorerzeugung mit Hilfe von Gerätevorlagen. Der Einsatz der letztgenannten Methode ergibt vor allem Sinn, wenn sich im Netz mehrere identische Systeme mit bestimmten Komponenten befinden. In den meisten Fällen dürft es sinnvoll sein, eine normale automatische Sensorerzeugung durchlaufen zu lassen und die dabei gefundenen Sensoren bei Bedarf manuell zu ergänzen, etwa um Überwachungsfunktionen für bestimmte Servertypen.

Im nächsten Schritt geht es ans Festlegen des Zeitplans für die automatische Suche und die Angabe des zu durchsuchenden Adressbereichs. Hier stehen verschiedene Möglichkeiten zur Verfügung, nämlich Klasse-C-Basis-IP-Adresse mit Beginn/Ende (IPv4), eine Liste individueller IP-Adressen oder DNS-Namen (IPv4 oder IPv6), eine Netzwerkadresse plus Subnetz (IPv4) sowie IP mit Oktett-Bereich (IPv4). Es sollte also jeder Administrator eine Option finden, die zu seinem Netzwerk passt.

Sobald die für den Adressbereich erforderlichen Angaben vorgenommen wurden, können die zuständigen Mitarbeiter noch eine Namensauflösung mit Hilfe von DNS, WMI oder SNMP aktivieren und die automatische Suche für die Adressen von bereits bekannten Geräten überspringen, um den Vorgang zu beschleunigen.

Zum Schluss geht es an die Angabe der Anmeldedaten für die Windows-, Linux-, Vmware/Xen- und SNMP-Systeme sowie der Einstellungen für den HTTP-Proxy und der Zugriffsrechte. Alle hier erwähnten Angaben lassen sich bei Bedarf aus der bestehenden Konfiguration erben, so dass die automatische Suche beispielsweise die Anmeldedaten verwendet, die zuvor über den Konfigurations-Guru eingegeben wurden. Die Zugriffsrechte legen übrigens fest, welche PRTG-Benutzerkonten Zugriff auf die bei der aktuellen Suche gefundenen Einträge erhalten. Wenn die Suche abgeschlossen ist, erscheinen die neuen Sensoren automatisch in der Geräteübersicht, auf die wir gleich noch genauer eingehen.



Nach dem Drill-Down auf ein einzelnes System finden sich die darauf überwachten Dienste in einer Liste

Das Web-Interface

Nachdem die Installation und Erstkonfiguration abgeschlossen waren, wandten wir uns zunächst dem Leistungsumfang des Monitoring-Werkzeugs zu. Nach dem Login beim Web-Interface im laufenden Betrieb landet der Administrator auf einer Willkommensseite, die es ihm ermöglicht, den Konfigurations-Guru nochmals auszuführen, eine automatische Netzwerksuche zu starten, zur Geräteübersicht zu wechseln, die Enterprise Console herunterzuladen, die Smartphone-Apps zu installieren sowie Hilfe einzusehen und den Support zu kontaktieren.

Am oberen Fensterrand bietet das Konfigurationswerkzeug eine Menüleiste an, die gleich zu den wichtigsten Punkten, wie Geräteübersicht, Bibliothek, Alarmen und so weiter verzweigt. Unterhalb dieser Hauptmenüpunkte finden sich aber noch weitere Einträge, auf die der Anwender wechseln kann, indem er das Menü herunterklappt und dann mit dem Mauspfeil darauf fährt. Im Fall der Hauptseite handelt es sich bei diesen Unterpunkten vor

allem um vier Übersichtsseiten. Diese lassen sich bei Bedarf – wie alle anderen Seiten auch – als Hauptseite festlegen, die direkt nach dem Login angezeigt wird. Sie enthalten Überblicksinformationen über die wichtigsten Sensoren (diese können von den Benutzern als "Favoriten" markiert werden), das Aktivitätsprotokoll, Todos, Alarme, Warnungen, Gruppen, Geräte, Sensoren, ungewöhnliche Vorkommnisse und kürzliche Protokolleinträge. Dazu kommen noch eine Sitemap mit allen Links, die dem aktiven Benutzerkonto zur Verfügung stehen sowie Optionen zum Aufrufen der Mobile Web GUI und der oben erwähnten Willkommensseite. Damit enthält das Menü zur Hauptseite umfangreiche Möglichkeiten, den PRTG Network Monitor so zu konfigurieren, dass er den zuständigen Mitarbeitern sofort nach dem Login umfassende Informationen über ihr Netzwerk liefert. Auf der rechten Fensterseite findet sich zudem eine tiefgehende, kontextbasierte Hilfefunktion, die fast alle angebotenen Konfigurationspunkte erklärt. Diese Hilfe steht auf jeder Seite des Konfigurationstools bereit.

Die Geräteübersicht

Der zweite Menüeintrag verzweigt auf die schon angesprochene Geräteübersicht. Sie stellt das Herzstück des Network Monitors dar und zeigt alle überwachten Systeme mit ihren Sensoren in einer Baumstruktur innerhalb ihrer jeweiligen Gruppen. In dieser Übersicht erkennen die Mitarbeiter auf den ersten Blick, wo Fehler aufgetreten sind, wo Warnungen existieren und so weiter, denn fehlerhafte Sensoren erscheinen rot, Sensoren mit Warnungen gelb und Sensoren ohne Probleme grün. In der Geräteübersicht lassen sich die Daten nicht nur einsehen, sondern es ist auch möglich, bei Bedarf Remote Probes, neue Gruppen sowie neue Geräte und Sensoren hinzuzufügen. Dazu kommen eine Geo-Map, die zeigt, wo sich die jeweils überwachten Systeme auf der Welt befinden sowie grafische Übersichten, die Aufschluss über die Alarme, die Prozessorlast, den Datenverkehr und die Antwortzeiten geben. Diese Übersichten zeigen in der Standardeinstellung jeweils den Status der letzten zwei, der letzten 30 und der letzten 365 Tage.

Der "Sunburst View" gibt auf einen Blick Aufschluss über den Zustand der überwachten Komponenten. Die Übersicht wird von innen nach außen immer feiner und einzelne Systeme vererben ihren Status nach innen. Auf diese Weise stellt Paessler sicher, dass der innere Ring, der das gesamte Netz repräsentiert, nur dann nicht rot ist, wenn keines der äußeren Systeme einen Fehler aufweist.

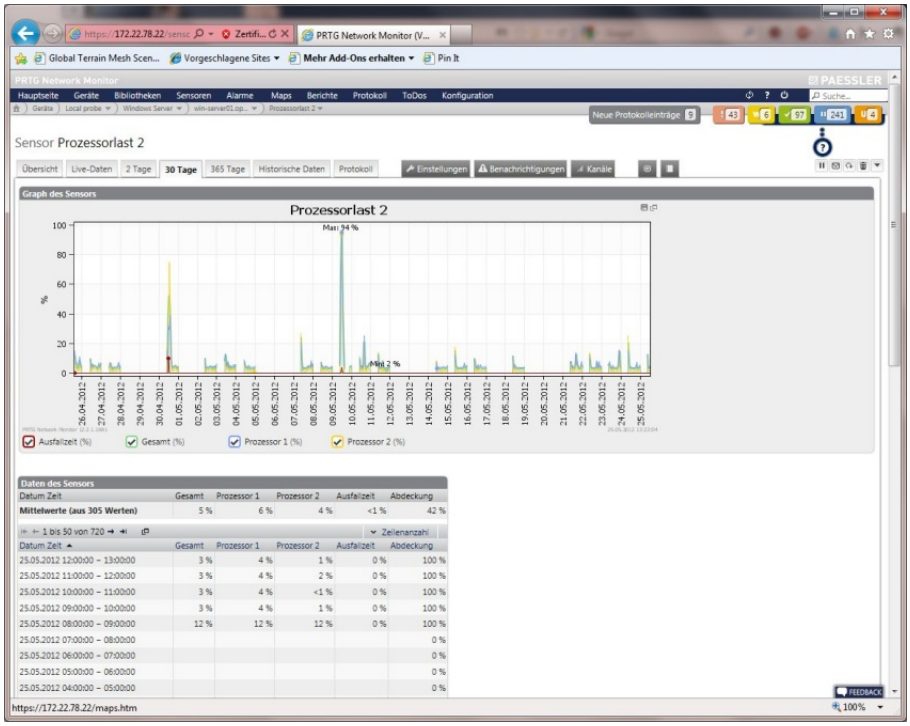
Nach dem Klick auf eine Gruppe, einen Rechner oder eine Probe landen die zuständigen Mitarbeiter immer in einer dazugehörigen Drill-Down-Übersicht. Hat ein Unternehmen also beispielsweise alle Windows Server in einer Gruppe zusammengefasst, so erscheinen nach dem Klick auf diese Gruppe nur noch die dazugehörigen Systeme. Auf diese Weise sind die IT-Mitarbeiter dazu in der Lage, die Anzeige auf einzelne Rechner und sogar einzelne Sensoren zu beschränken. Zeigt das System nur die Daten eines Rechners an, so präsentiert es die darauf befindlichen Sensoren als Liste. Diese Liste umfasst für alle Einträge neben den sensorspezifischen Daten wie Name und Status unter anderem auch kleine grafische Darstellungen, die beispielsweise auf einen Blick Aufschluss über die Auslastung bringen.

Die Übersicht über einzelne Sensoren bringt im Gegensatz dazu detaillierte Informationen, wie Live-Daten, eine 2- und 30-Tage-Übersicht und ähnliches. Darüber hinaus haben die Verantwortli-

IAITested

chen an dieser Stelle die Möglichkeit, Einstellungen zu den Sensoren vorzunehmen und zum Beispiel den Namen, das Abtastintervall, die Priorität (diese bestimmt die Sortierung der Objekte in Listenansichten) und die Zugriffsrechte zu modifizieren. Außerdem ist es möglich, die Sensoren so zu konfigurieren, dass sie bei bestimmten Zuständen oder dem Erreichen bestimmter Schwellenwerte Benachrichtigungen verschicken. Wechselt ein Sensor beispielsweise in den Zustand "Fehler", so kann er nach einer definierten Zeitspanne eine Mail an den zuständigen Administrator senden. Zusätzlich besteht auch noch die Option, einzelnen Kanälen innerhalb der Sensoren Grenzwerte zuzuweisen und sie in die Überblicksgrafiken und Tabellen aufzunehmen. Last but not Least fügen die Administratoren an gleicher Stelle bei Bedarf Kommentare ein und analysieren die zu dem jeweils betroffenen Sensor gehörenden Protokolleinträge.

Zu den soeben genannten Punkten kommen bei den Ansichten für Geräte und Gruppen ebenfalls Reiter, mit denen die IT-Verantwortlichen Live Daten als Grafiken und Tabellen einsehen und das Protokoll aufrufen können.



Die Überwachungssoftware stellt die Messdaten einzelner Sensoren auch grafisch dar. Hier die CPU-Last eines Servers über den Zeitraum von einem Monat hinweg

Zwei-Tages-, Monats- und Jahresübersichten stehen genauso zur Verfügung, das Gleiche gilt für eine Option zum Abfragen "Historischer Daten". Bei letztgenannter geben die Administratoren selbst einen Zeitraum für die anzuzeigenden Informationen vor. Bei den Gruppen und Geräteübersichten gibt es zusätzlich auch noch den Punkt "Verwaltung". Hier besteht die Option, Sensoren mittels Drag-and-Drop je nach den Wünschen des jeweiligen Mitarbeiters anzuordnen.

Über die Einstellungen pausieren die zuständigen Mitarbeiter auf Wunsch alle Sensoren in der Gruppe oder auf dem Gerät und legen den Gruppen- beziehungsweise Gerätetyp mit der Art der Sensorerzeugung (automatisch, manuell und so weiter) fest. An gleicher Stelle ist es auch möglich, Anmeldedaten zu ändern, Zeitpläne zu definieren und weitere Parameter, die bei der ursprünglichen Netzsuche vorgegeben wurden, zu modifizieren. Reiter zum Anlegen von Benachrichtigungen, zum Eingeben von Kommentaren und zum Einsehen des Systemprotokolls runden den Leistungsumfang der Gruppen- und Gerätekonfiguration ab.

Eines ist an dieser Stelle noch zu erwähnen: in den Auflistungen der Sensoren und Computer lassen sich auch stets mehrere Objekte selektieren und über die Multi-Edit-Funktion gleichzeitig bearbeiten. Das bringt großen Nutzen mit sich, zum Beispiel wenn es darum geht, die Konfiguration mehrerer Sensoren auf einmal zu modifizieren oder verschiedene Sensoren gleichzeitig zu pausieren.

Im Test stellten wir fest, dass der Ansatz, das Netz gruppen-, geräte- und sensorenweise zu administrieren, auch in Umgebungen mit sehr vielen Komponenten und Sensoren dabei hilft, den Überblick zu behalten. So ist es beispielsweise einerseits möglich, einen Alarm zu konfigurieren, der beim Auftritt eines Fehlers in einer ganzen Rechnergruppe aktiv wird. Andererseits lassen sich Benachrichtigungen auch so einrichten, dass nur ein einziger Sensor auf einem einzelnen System als Trigger gilt. Die Alert- und Analysemöglichkeiten sind damit ganz genau an die Anforderungen bestimmter Situatio-

nen und bestimmter Mitarbeiter anpassbar, ohne dass die Übersichtlichkeit des Gesamtsystems darunter leidet.

Bibliotheken

Die Bibliotheken ermöglichen es den Anwendern im Gegensatz zur Geräteansicht, individuelle Ansichten, beispielsweise nach funktionalen Kriterien, zu erstellen. So ist es etwa möglich, Umgebungen, die in der Geräteübersicht nach technischen Gesichtspunkten wie Betriebssystemen oder Rollen im Netzwerk aufgeführt werden, in einer entsprechenden Bibliothek so neu anzuordnen, dass sie die Organisationsstruktur des Unternehmens mit Vertrieb, Buchhaltung, IT-Abteilung, Vorstand und so weiter wiederspiegeln. Die Ansichten der einzelnen Bibliotheken lassen sich direkt im Browser per Drag-and-Drop generieren und modifizieren.

Möchte ein Anwender eine Bibliothek hinzufügen, so muss er nur einen Namen und die Zugriffsrechte auf das Objekt vergeben, danach kann er sofort damit arbeiten. Bestehende Bibliotheken lassen sich jederzeit verändern. Im Test ergaben sich bei der Arbeit mit Bibliotheken keine Schwierigkeiten.

Sensoren

Die Sensorübersicht umfasst eine Liste aller Sensoren mit ihrem Status, einer kleinen Grafik, die beispielsweise die Last zeigt und ähnlichem. Möchte der Administrator einen neuen Sensor anlegen, so fragt ihn der PRTG Network Monitor zunächst einmal, ob der Sensor zu einem neuen oder einem bestehenden Gerät gehört, wie das Gerätesymbol aussieht, ob die Verbindung über IPv4 oder IPv6 läuft, wie die Anmeldedaten lauten und ob die Sensorerzeugung manuell oder über eine automatische Suche erfolgen soll.

Entscheidet sich ein Mitarbeiter für das manuelle Anlegen eines Sensors, so kann er aus insgesamt 131 definieren Sensortypen wählen. Um diesen Vorgang zu vereinfachen, bietet Paessler Entscheidungshilfen mit Rubriken an. Dabei beantworten die Anwender Fragen und erhalten dann nur die für sie passenden Sensoren angezeigt. Die Fragen lauten "Was soll gemonitored werden?" (Verfügbarkeit, Bandbreite, Datenverkehr, Geschwindigkeit, Leistung, CPU Nutzung, Datenträgernutzung, Speichernutzung, Hardware-Parameter, Netzwerk-Infrastruktur oder Eigene Sensoren), "Art des Zielsystems?" (Windows, Linux/MacOS, Virtualisierungs-OS, Datei-Server, Mail-Server, SQL-Server) sowie "Eingesetzte Technologie?" (Ping, SNMP, WMI, HTTP, SSH, Packet-Sniffing, NetFlow/sFlow/jFlow). Mit Hilfe dieser Kategorien gelang es uns im Test sehr schnell, die Sensoren einzurichten, die zum Überwachen unseres Exchange-Systems und unserer vSphere-Umgebung erforderlich waren.

Im zu den Sensoren gehörenden Menü stehen den Benutzern verschiedene Optionen zur Verfügung, um einen Überblick über die Sensormesswerte zu erhalten. So gibt es zum Beispiel Top-10-Listen zu Themen wie "beste Verfügbarkeit", "schnellster Ping", "schlechteste Ausfallzeit", "langsamster Ping", "geringste Bandbreitennutzung", "schnellste Website" und ähnlichem. Dazu kommen Übersichten nach Status, Verfügbarkeit, Gruppe, Typ und so weiter. Es ist hier sogar möglich, Sensoren zu vergleichen und historische Daten einzusehen. Dabei ergaben sich bei uns im Test recht interessante Einblicke in die Performance in unserem Netz.

Alarme

Der PRTG Network Monitor bietet umfassende Alarmfunktionen. Die Alarme lassen sich sogar nutzen, um Neustarts zu automatisieren und Powershell-Skripts, Batch-Dateien und DLLs auszuführen. Außerdem findet sich in PRTG auch eine Liste mit aktuellen Alarmen und Warnungen.

Fährt ein Administrator seine Maus im "Hoover"-Modus über diese Liste (das gilt übrigens auch für andere Übersichten wie etwa die über Geräte oder Sensoren), so blendet das Web-Interface immer ein Überblicksfenster mit den wichtigsten Daten und Grafiken zu dem betroffenen Eintrag an. Das ist sehr nützlich, wenn man sich einen schnellen Eindruck über mehrere Einträge machen möchte, ohne diese Einträge alle extra zu öffnen.

Maps

Die Maps bieten eine grafische Netzwerkübersicht, die auf Wunsch auch mit einem Hintergrundbild versehen sein kann. Auf diese Weise ist es unter anderem möglich, einen Lageplan aller Rechner im Haus zu erstellen, auf dem neben dem Ort auch gleich der Status der einzelnen Systeme erscheint. Die zuständigen Mitarbeiter können jederzeit mehrere Maps erstellen und sie auch veröffentlichen, damit Dritte Zugriff auf die darin enthaltenen Daten haben. Maps eignen sich auch sehr gut als Hauptseite, die das

System direkt nach dem Login präsentiert. Sie lassen sich zudem jederzeit problemlos in externe Websites einbinden.

Auch das Erstellen der Maps läuft – genau wie das der Bibliotheken – mit Drag-and-Drop aus dem Gerätebaum heraus. Darüber hinaus stellt Paessler auch noch zusätzliche Symbole für die Maps bereit, die transparente Komponenten wie unmanaged Switches und externe abstrakte Systeme wie das Internet symbolisieren.

Es bringt auch kein Problem mit sich, die Verbindungen zwischen den einzelnen Systemen in die Map mit aufzunehmen. Im Test fanden wir eine Karte unseres LAN als Überblicksmap so nützlich, dass wir sie als Hauptseite einrichteten.

Berichte

Das Monitoring System erlaubt es, bei den Berichten Daten und Grafiken zu kombinieren. Es stehen einmalige und regelmäßig wiederkehrende Berichte zur Verfügung. Der Zeitraum, für den der Bericht gelten soll, lässt sich manuell auswählen und es ist möglich, Berichte als HTML anzuzeigen, als PDF zu erstellen und per Mail zu verschicken. Es sind viele unterschiedliche Berichte vorhanden, wie "Top 100 schnellste HTTP-Sensoren", "Top 100 langsamste Ping-Sensoren" und ähnliches. Dazu kommen noch Berichte zu Bandbreite, CPU-Last, Speichernutzung, Plattenplatz und Verfügbarkeit. Berichte lassen sich jederzeit an die eigenen Bedürfnisse anpassen.

Die zuständigen Mitarbeiter können – falls erforderlich – auch gespeicherte Berichte einsehen. Außerdem lassen sich die Sensoren, die dem Bericht zugrunde liegen, manuell oder nach Kennung auswählen. Eine Auswahl nach Kennung erzeugt dynamische Berichte: weist ein Administrator eine solche Kennung einem Sensor oder einer Gruppe zu, so landet er (beziehungsweise sie) automatisch in dem dazugehörigen Bericht.

Aufgeräumt und übersichtlich: Das Mobile Web GUI in PRTGdroid

Um eine Komponente aus dem Bericht zu löschen, reicht es analog dazu, die entsprechende Kennung zu entfernen. Darüber hinaus besteht die Option, Berichte nach Zeitplänen zu erstellen und zu verschicken. Im Test ergaben sich dabei keine Schwierigkeiten.

Protokoll

PRTG zeigt das Protokoll als Liste. Bei der Protokollübersicht ist es jederzeit möglich, den Zeitraum und die anzuzeigende Zeilenanzahl auszuwählen. Zudem lassen sich entweder alle Einträge einsehen, oder nach Gruppe, nach Systemereignissen und nach Statuswechsel (wie OK, Fehler, Pausiert/Fortgesetzt, Bestätigt oder auch Ungewöhnlich) filtern.

Todos

Die Todos umfassen Informationen, die der Administrator bestätigen muss, wie beispielsweise das Vorhandensein neuer Programmversionen und das Aktivieren neuer Sensoren. Bei den Todos weist das System die zuständigen Mitarbeiter unter anderem auch darauf hin, dass neue Berichte erstellt wurden. Es handelt sich also praktisch um eine Art Benachrichtigungsdienst für die zuständigen Mitarbeiter.

Konfiguration

Das Konfigurationsmenü umfasst alle Punkte zum Verwalten des PRTG Network Monitors selbst. Dazu gehören zunächst die Kontoeinstellungen mit Name, Passwort, Zeitzone, Mail-Adresse, Alarmsettings und so weiter.

Der "Systemzustand" gibt im Gegensatz dazu Aufschluss über die Softwareversion, das Betriebssystem, die Zeit, die CPU-Last, die Lizenz und so weiter. An gleicher Stelle sind die Administratoren auch dazu in der Lage, für den Support-Fall einen Schnappschuss der Datenbank zu erzeugen, alle Probes neu zu starten und eine Probestatusdatei zu schreiben.

Das "Auto-Update" sorgt dafür, den PRTG Network Monitor immer auf dem aktuellen Stand zu halten. Im Test funktionierte das einwandfrei. Ebenfalls interessant: die Systemverwaltung. Hier konfigurieren die zuständigen Mitarbeiter unter anderem Diagramme und Farben, legen

den Namen der PRTG-Website fest und wählen den Map Provider (MapQuest, Nokia Maps, CloudMade oder Google) aus. Darüber hinaus ist es möglich, das Monitoring-Tool in die Windows-Domäne zu integrieren, um die im Unternehmen vorhandenen Benutzerkonten auch für PRTG zu nutzen. Abgesehen davon lassen sich an dieser Stelle auch Schwellenwerte für das Erkennen ungewöhnlicher Vorkommnisse setzen.

Die nächsten Punkte ermöglichen die Konfiguration des Benachrichtigungsversands (über den internen oder einen externen Mail-Server), der Kommunikation mit externen Probes sowie die Arbeit mit Benutzerkonten. Über letzteres lassen sich unterschiedliche User-Accounts für verschiedene Monitoring-Aufgaben einrichten. Es besteht darüber hinaus die Option, die Benutzer zu Gruppen hinzuzufügen, die Alarmeinstellungen vorzunehmen und Rechte zu vergeben ("Lesen/Schreiben" oder "Nur Lesen").

Befehlsmenüs zum Verwalten von Clustern, zum Herunterladen zusätzlicher Software (Enterprise Console, Apps für mobile Geräte sowie Installationsdatei für Remote Probes) und zum Eingeben der Lizenz schließen den Leistungsumfang des Konfigurationswerkzeugs zusammen mit einer Dokumentation des PRTG API ab. Generell gilt, dass das Tool übersichtlich gestaltet wurde und – nicht zuletzt dank der guten Hilfefunktion – wenig Einarbeitungszeit erfordert.

Die Android-App

PRTGdroid ermöglichte uns im Test, jederzeit von überall her verschlüsselt auf die Informationen des PRTG Network Monitors zuzugreifen. Der Konfigurationsaufwand war gering und das mobile Web-Interface eignet sich gut, um alle Daten einzusehen.

Es wurde zudem mit großen Icons "daumenfreundlich" gestaltet. Da es sich mit jedem Browser nutzen lässt, ist die Installation der App nicht unbedingt erforderlich, sie erweitert den Leistungsumfang des Mobile Web GUI aber um die sehr sinnvolle Möglichkeit, Benachrichtigungen auf dem mobilen Gerät auszugeben.

Exchange-Überwachung

Die Überwachungsmöglichkeiten, die Paessler für Exchange-Server bereitstellt, sind sehr umfangreich. Das System stellte uns insgesamt 97 Sensoren zur Verfügung, die speziell für Exchange-Systeme gedacht sind. Damit lassen sich so unterschiedliche Bereiche wie der Speicher, die Datenbank und die Zahl der aktiven Benutzer überwachen.

Einige der Sensoren sind sehr "gerade heraus" und erklären sich praktisch von selbst, wie zum Beispiel der Sensor, der die Zahl der pro Sekunde versandten Nachrichten misst oder der Sensor, der die Administratoren über die Logon-Operationen pro Sekunde informiert. Andere sind nicht so leicht verständlich, wie etwa der "Database Cache % Hit edgetransport".

Generell gilt, dass es beim Überwachen von Exchange-Servern Sinn ergibt, die einzelnen Mail-Queues im Auge zu behalten, da sich hier leicht herausfinden lässt, ob es beim Mail-Versand zu Staus kommt. Ebenfalls wichtig: die Zahl der pro Sekunde verschickten Mails, denn mit diesem Sensor lässt es sich herausfinden, ob irgendwelche Rechner im Netz zum Versenden von Spam missbraucht werden. Abgesehen davon ist es sinnvoll, die CPU- und Speicherlast, die Mail-Dienste POP3, IMAP4, SMTP sowie die Queues zum internen Weiterverteilen der Mails auf die Mailboxen zu überwachen. Wenn es hier zu keinen Problemen kommt, stehen die Chancen gut, dass sich der Exchange-Server in einem guten Zustand befindet. Der "Roundtrip-Sensor" darf in diesem Zusammenhang auch nicht vergessen werden. Er schickt eine Mail an einen externen Dienst, den die Administratoren vorher so konfigurieren müssen, dass er die Mail sofort wieder zurückschickt. Auf diese Art und Weise lässt sich bestimmen, wie lang eine Nachricht zu dem genannten Service und zurück benötigt. Im Test ergaben sich beim Überwachen unseres Exchange-2010-Servers keinerlei Schwierigkeiten.

Das Monitoring von vSphere

Beim Überwachen von Virtualisierungsumgebungen auf Basis von Vmware (wir verwendeten im Text vSphere-5- und ESXi-5-Systeme) sind folgende Punkte zu beachten: Wurden die Credentials für die Virtualisierungshosts korrekt angegeben, so findet die automatische Netzwerksuche die Systeme, erkennt sie als ESXi-Hosts und richtet gleich Sensoren zum Überwachen der darauf laufenden VMs ein.

Die ganze Sache ist folglich sehr einfach und läuft "Out of the Box". Arbeitet ein Unternehmen aber mit vSphere-Servern, die mehrere ESXi-Systeme verwal-

ten und Vmotion, um die VMs ja nach Auslastung von einem Host auf den anderen schieben zu können, dann ergibt der eben beschriebene Ansatz keinen Sinn. Verschiebt Vmotion nämlich eine VM von einem Host auf einen anderen, so löst dieser Vorgang bei PRTG einen Alarm aus, da die VM ja plötzlich auf dem dazugehörigen Host nicht mehr existiert.

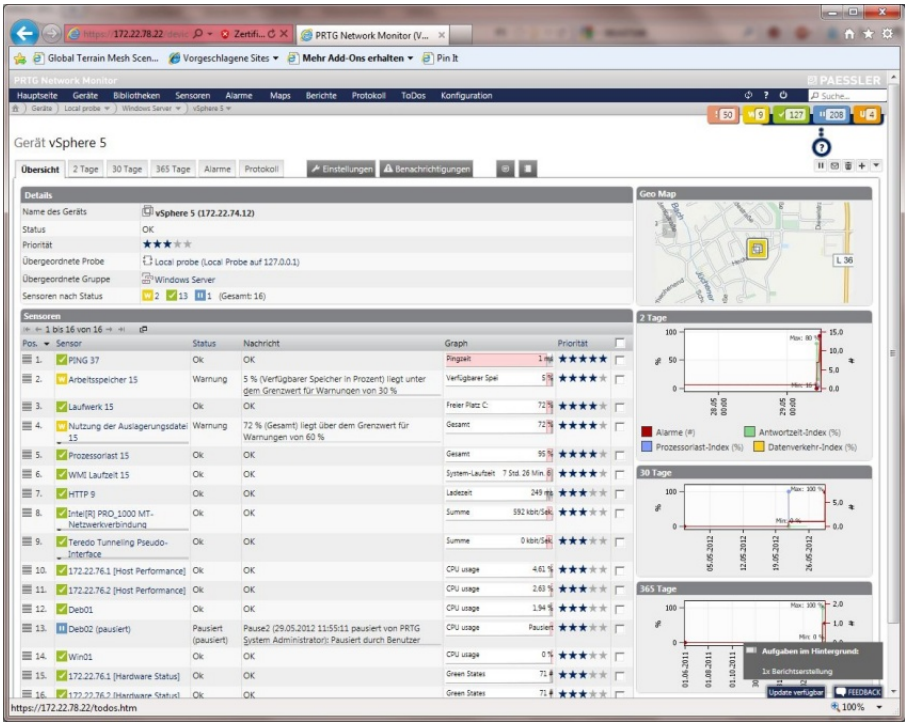
In diesem Fall ist es besser, die ESXi-Hosts nicht direkt, sondern über den vSphere-Server zu überwachen. In diesem Fall hat PRTG die Sichtweise von vSphere und erkennt, dass die VM noch arbeitet, nur eben auf einem anderen Host. Um das genannte Szenario zu realisieren, ist aber Handarbeit angesagt. Beim vSphere-Server handelt es sich nämlich um eine Windows-Software die auf einem Windows-Server läuft. Untersucht das Paessler-Produkt diesen Server mit der automatischen Netzwerksuche, so richtet es zwar die Standard-Windows-Sensoren ein, nicht aber die Vmware-Sensoren. Diese Arbeit müssen die Administratoren manuell nachholen. Dabei dürfen sie als Credentials für die Vmware-Umgebung nicht die Login-Daten für die ESXi-Server verwenden, sondern müssen eines der Windows-Benutzerkonten einsetzen, das Zugriff auf den vSphere-Server hat. Im Test funktionierte das eben genannte Vorgehen bei uns ohne Probleme.

Fazit

Der PRTG Network Monitor konnte uns voll überzeugen. Das System ist schnell installiert und dank des Konfigurations-Gurus auch schnell und ohne Probleme eingerichtet. Positiv fällt vor allem auf, dass die Software ohne Agenten auf den zu überwachenden Systemen auskommt. Auf diese Weise sparen die zuständigen Mitarbeiter nicht nur Arbeit, sondern vermeiden es sogar, die Systeme im Netz überhaupt anzufassen, was gerade bei kritischen Installationen sehr beruhigend sein kann.

Gleichermaßen müssen wir den großen Funktionsumfang der Software hervorheben. Paessler hat sich viel Mühe gegeben, leistungsfähige Sensoren für alle in modernen IT-Umgebungen vorkommenden Dienste bereit zu stellen. Das gilt nicht nur für Cloud-Services wie Dropbox und Salesforce sondern auch für das Monitoring von Standardapplikationen wie Exchange und von virtuellen Umgebungen. Sogar der Netzwerkverkehr lässt sich über NetFlow, sFlow, jFlow und Packet Sniffing im Auge behalten. In den meisten Fällen richtet die automatische Netzwerksuche alle benötigten Sensoren von sich aus ein. Sollte es einmal nötig sein, manuell zusätzliche Sensoren in die Umgebung zu integrieren, so geht diese Arbeit schnell von der Hand und sollte keinen Netzwerkspezialisten vor irgendwelche Schwierigkeiten stellen.

Weitere positive Punkte sind die Bibliotheken und Maps. Sie ermöglichen es, die vorhandenen Infrastrukturen nicht nur aus Sicht eines Technikers darzustellen, sondern flexible Sichtweisen zu schaffen, die auch für Mitarbeiter aus anderen Bereichen verständlich sind. Der Arbeitsaufwand dafür gestaltet sich gering und es ist sogar möglich, die Maps auf externen Seiten zu publizieren. Die umfangreichen und leistungsfähigen Alarm- und Berichtsfunktionen runden den positiven Gesamteindruck des PRTG Network Monitors ab.



Beim Überwachen von Vmware-Umgebungen ergibt es Sinn, nicht nur die einzelnen Hosts im Auge zu behalten, sondern auch den vSphere-Server

Dr. Götz Güttich leitet das IAIT in Korschenbroich. Sein Blog findet sich unter www.sysbus.eu.