Monitoring aus der Cloud

Dr. Götz Güttich

Mit dem PRTG Hosted Monitor bietet Paessler eine Cloud-basierte Lösung an, die es möglich macht, IT-Netzwerke und die darin vorhandenen Komponenten zu überwachen. Das Produkt funktioniert praktisch genauso wie der klassische On-Premises-PRTG, lässt ich aber von überall aus nutzen. Damit eignet sich die Hosted-Variante vor allem für den Einsatz in verteilten Umgebungen und für die Nutzung in Organisationen, denen die Installation, Konfiguration und Verwaltung eines eigenen PRTG-Servers zu aufwendig ist.

Der PRTG Hosted Monitor setzt auf dem On-Premises-PRTG-Server auf und der Funktionsumfang ist fast identisch. Es gibt nur ein paar Unterschiede in den Dialogen und Einstellungen, um das Produkt an die Arbeit in der Cloud anzupassen. Beispielsweise bei Dingen wie der Benutzerverwaltung und der Standardspeicherdauer der Monitoring-Daten.

Die Lösung wird von Paessler im Abonnement-Modell angeboten. Die einzelnen Abonnements unterscheiden sich durch die Zahl der verfügbaren Sensoren. Mit Sensoren meint Paessler Monitoring-Funktionen.

So gibt es beispielsweise Sensoren zum Überwachen bestimmter Dienste, zum Analysieren des Netzwerkverkehrs oder auch zum Monitoring der Festplatten einzelner Rechner im Netz. Die angebotenen Abonnements umfassen 500, 1000, 2500, 5000 und 10.000 Sensoren. Wenn sich die Anforderungen bei den Kunden ändern, haben sie jederzeit Gelegenheit, ihr Abonnement über eine Webseite “on the fly” zu wechseln und so an ihre jeweiligen Bedürfnisse anzupassen.

Die Sicherheit der Daten wird durch unterschiedliche Maßnahmen realisiert

Der PRTG Hosted Monitor läuft in der Amazon Cloud. Bei Cloud-Diensten, vor allem bei solchen, die wie eine Netzwerk-Monitoring-Lösung viele kritische Daten vorhalten, stellt sich immer die Frage nach der Sicherheit. Deswegen wurden sämtliche Datenübertragungen zwischen den Anwendern und den überwachten Maschinen auf der einen, und dem Server auf der anderen Seite, verschlüsselt. Das ist bei der On-Premises-Version von PRTG ebenfalls der Fall.

Innerhalb der AWS-Cloud sind die verwendeten Festplatten für jeden Kunden zusätzlich individuell verschlüsselt. Das System erstellt stündlich verschlüsselte Backups. Diese ermöglichen jederzeit Rollbacks, falls solche erforderlich sein sollten. Die Sicherungen werden gelöscht, sobald sie älter als 24 Stunden sind. Einzige Ausnahme: Eine sonntägliche Sicherung, die jeweils sechs Wochen aufbewahrt wird. Ein Zugriff auf das AWS-Backend ist nur für Paessler-Mitarbeiter aus der Entwicklungs- und der IT-Abteilung möglich und das nur direkt aus der Paessler-Zentrale oder über ein VPN, das über die Paessler-Zentrale läuft.

Im laufenden Betrieb hat der Paessler-Support die Option, sich bei den Maschinen einzuloggen. Jede Maschine hat dabei einen eigenen Administrator-Account mit einem eigenen Passwort, so dass es nicht möglich ist, auf alle Systeme zuzugreifen, wenn man die Zugangsdaten zu einem kennt. Der Zugriff erfolgt zudem nur auf Wunsch des Kunden, um Unterstützung zu leisten. Weitere Informationen zu dieser Thematik finden sich hier: What security features does PRTG include? | Paessler Knowledge Base.

Der PRTG Hosted Monitor stellt folglich eine AWS-basierte Sicherheitslösung dar, die den Vorteil mitbringt, dass der Support über Paessler läuft und nicht über Amazon. Es ist also stets ein direkter Kundenkontakt gewährleistet.

Inbetriebnahme der Lösung

Um den PRTG Hosted Monitor in Betrieb zu nehmen, müssen die zuständigen Mitarbeiter lediglich auf die Webseite https://my-prtg.com gehen und sich für die kostenlose Testversion anmelden. Nach dem Anlegen und Aktivieren des Benutzerkontos können sie sich dann bei dem Dienst einloggen (bei Bedarf lässt sich auch eine Zwei-Faktor-Authentifizierung aktivieren) und eine Subscription erstellen. Dazu geben sie einen Namen für ihre Subdomäne an und legen fest, auf welchem Server der Dienst laufen soll. Dazu stehen neben der Region Europa (in Irland) auch noch "US East" (Nordvirginia), "US West" (Oregon) sowie Singapur und Sidney für den asiatisch-pazifischen Raum zur Verfügung. Zum Schluss kann man dann noch auswählen, ob man den kostenlosen Trial nutzen oder gleich mit einem kostenpflichtigen Plan starten möchte. Im nächsten Schritt fragt das System nach dem Namen, der Rechnungsadresse und der Umsatzsteuer-ID. Damit ist die Einrichtung abgeschlossen und der Hosted-PRTG-Server wird gestartet, was ein paar Minuten dauert. Im Test mussten wir jetzt nur noch die Zeitzone anpassen, danach konnten wir loslegen.

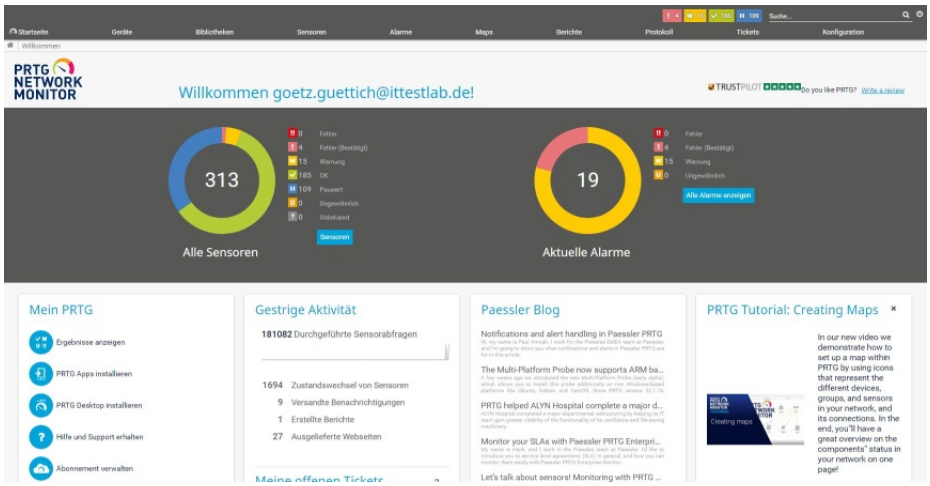
Nach dem Einloggen bei dem Web-basierten Dienst wechselten wir in die Geräteübersicht, um zu sehen, was bereits in unserem gehosteten Dienst aktiv war. Hier finden sich zu diesem Zeitpunkt die Einträge "Hosted Probe" und "PRTG Core Server", also die Geräte, die in der Cloud laufen. Damit wir unser lokales Netz in die Monitoring-Umgebung einbinden konnten, war es nun erforderlich, auf einem Rechner im LAN eine so genannte Remote Probe zu installieren, die die Daten lokal sammelt und an den PRTG-Server weiterleitet.

Darauf machte uns ein Einrichtungsassistent aufmerksam. Es existiert beim Einsatz von Hosted PRTG übrigens keine Beschränkung der Zahl der verwendeten Probes.

Die Installation der Probes läuft einfach ab. Man muss lediglich die Setup-Datei runterladen (wir verwendeten im Test eine Probe für Windows) und starten. Danach nimmt die Remote Probe den Kontakt zum Hosted-PRTG-Server auf. In unserer Umgebung war es allerdings erforderlich, diesen Kontakt dadurch zuzulassen, dass wir Datenübertragungen über den TCP-Port 23560 in beide Richtungen erlaubten, da die Kommunikation über diesen Port stattfindet.

Der erste Netzwerk-Scan

Sobald die Probe mit dem Server in der Cloud kommunizieren kann, besteht die Option, direkt einen automatischen Suchlauf zu starten, der das lokale Netz nach den vorhandenen Komponenten durchsucht. Dieser aktiviert auf den gefundenen Geräten auch gleich eine Auto-Discovery-Funktion, die dort die Sensoren installiert, die nach Ansicht der Verantwortlichen bei Paessler sinnvoll sein könnten. Dabei greifen die Paessler-Mitarbeiter auf Erfahrungswerte zurück, die im Lauf von 20 Jahren gesammelt wurden und optimieren die Konfiguration ständig.



Das Dashboard, das die zuständigen Mitarbeiter nach dem Login standardmäßig zu sehen bekommen

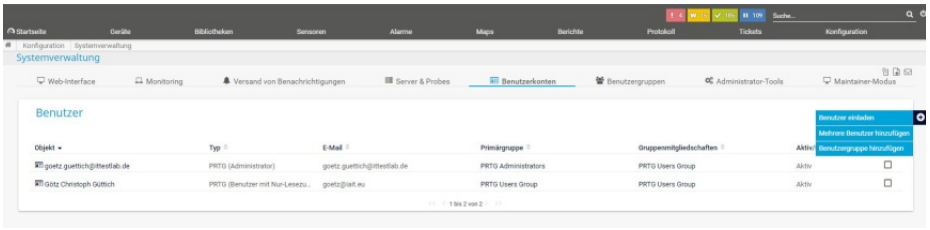
Die Dauer der Discovery hängt von der Größe des Netzes ab. Generell kann man sagen, dass PRTG jede IP-Adresse im Netz anpingt und fünf Sekunden auf Antwort wartet. Die Dauer des Scans liegt also bei der Zahl der IP-Adressen mal fünf. Werden Geräte gefunden, so untersucht PRTG diese genauer, um festzustellen, welche Sensoren darauf zum Einsatz kommen.

Der Zeitbedarf für diesen Schritt ist je nach Gerät unterschiedlich, im Schnitt nimmt der Vorgang

aber etwa zwei Minuten in Anspruch. Die Zahl der Vorhandenen Geräte mal zwei Minuten kommt also noch zu dem zuvor ermittelten Wert hinzu.

Gehen wir nun kurz auf den Aufbau der Monitoring-Lösung ein. Unterhalb der Gesamtstruktur befinden sich im Betrieb einer PRTG-Instanz Gerätegruppen wie “Windows Server”, die alle überwachten Rechner, die zu der jeweiligen Gruppe gehören, umfassen.

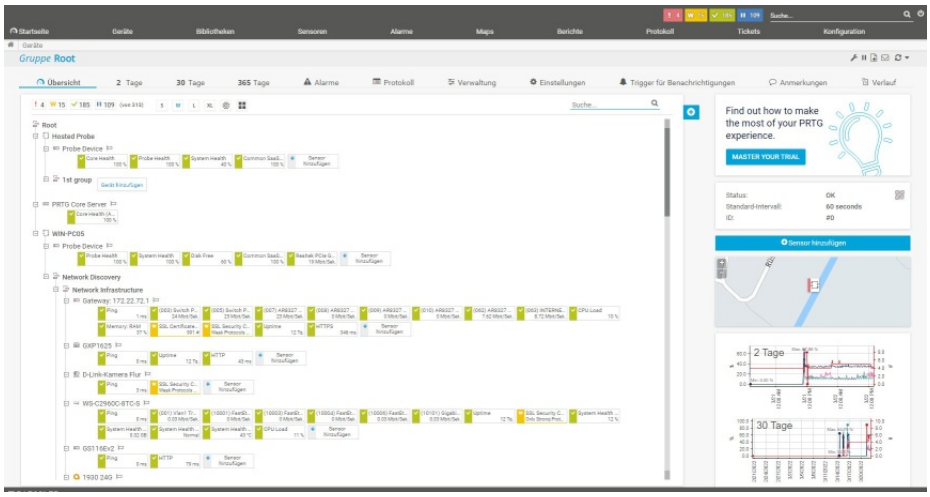
Die einzelnen Geräteeinträge enthalten dann wiederum die Sensoren, die – wie gesagt – bestimmte Komponenten oder Funktionen im Blick behalten. Unterhalb der Sensoren gibt es dann noch die so genannten Kanäle, die bei einem Netzwerkkartensensor beispielsweise Aufschluss über Details wie ein- und ausgehenden Verkehr, die Zahl der Pakete oder die aufgetretenen Fehler gibt. Der automatische Suchlauf erfasst durchaus einen Großteil der Geräte, die im Netz überwacht werden können, ordnet diese dann den genannten Kategorien wie “Windows Clients” oder “Netzwerkinfrastruktur” zu und installiert die wichtigsten Überwachungssensoren darauf. In der Praxis ist es aber erforderlich, die einzelnen Einträge nach dem Suchlauf nochmals durchzusehen, fehlende Geräte manuell zu erfassen, fehlende Sensoren, beispielsweise für das Überwachen bestimmter Anwendungen, anzulegen, die Grenzwerte für Alarme anzupassen und überflüssige Sensoren zu löschen.



Benutzer werden bei der Cloud-basierten Lösung nicht hinzugefügt, sondern eingeladen

Das Erstellen von Geräteeinträgen

Möchte man ein Gerät erfassen, so geht man im Webinterface der Lösung unter “Devices” zu der Rubrik, in die es gehört, wie etwa “Windows Server” und klickt auf den Eintrag “Add Device”. Dann erscheint ein Dialogfeld, in dem man dem Gerät einen Namen geben kann, festlegt, ob die Kommunikation mit dem Device über IPv4 oder IPv6 ablaufen soll und anschließend die IP-Adresse des Geräts einträgt. Zusätzlich gibt es unter anderem auch die Option, dem Device ein Icon zuweisen. Hier stehen Geräte-Icons, etwa für Netzwerkkameras zur Verfügung, das gleiche gilt aber auch für Herstellerlogos, beispielsweise für Produkte von APC, Checkpoint oder auch Huawei.



Die Geräteübersicht mit dem Core-Server in der Cloud und der lokalen Probe sowie den überwachten Komponenten im LAN

Zu guter Letzt gibt es auch noch die Möglichkeit, auf dem Gerät eine Auto-Discovery ablaufen zu lassen. Damit die Discovery-Funktionen möglichst viel erkennen kann, ergibt es Sinn, zuvor die Zugriffsdaten für die entsprechenden Systeme in PRTG zu hinterlegen, damit die Monitoring-Software in die Lage versetzt wird, sich bei den Devices einzuloggen und Informationen abzufragen. Die genannten Credentials werden immer an die Untergruppen weitervererbt. Legt man sie auf Ebene von “Root” fest, gelten sie für die gesamte Umgebung. Legt man sie beispielsweise in der Rubrik “Windows” fest, so gelten sie nur für die dazugehörigen Untergruppen, wie beispielsweise “Windows Clients” oder auch “Windows Server”. In der Praxis müssen die Administratoren sich überlegen, wie sie ihre jeweilige Umgebung abbilden wollen (es wäre auch möglich, die Gruppen nach Abteilungen wie “Buchhaltung” und “Vertrieb” zu gestalten) und auf welcher Ebene sie welche Credentials angeben. Das Definieren der Login-Daten geht auf jeden Fall immer unter den Einstellun-

gen der jeweiligen Probe, der jeweiligen Unterrubrik oder auch des betroffenen Geräts.

Neue Sensoren lassen sich einfach einbinden

Das Hinzufügen von Sensoren gestaltet sich dann relativ einfach. Man wechselt dazu auf den betroffenen Geräteeintrag und selektiert "Add Sensor". Danach bietet PRTG eine übersichtliche

Beim Hinzufügen von Komponenten zur Monitoring-Umgebung können die Administratoren den einzelnen Einträgen unter anderem auch Icons zuordnen

Auswahl an, die drei Fragen stellt. "Was soll gemonitort werden?" (Beispielsweise Prozessornutzung oder Bandbreite), "Art des Zielsystems?" (Windows, Linux, etc.) und "Eingesetzte Technologie?" (wie etwa SNMP, SSH oder WMI). Hat der Administrator diese drei Fragen beantwortet, so zeigt das System die zu der jeweils passenden Kombination gehörenden Sensoren an und der IT-Verantwortliche kann den Gewünschten auswählen. Das System ist übersichtlich und funktioniert schnell, kennt man den Sensornamen bereits, so steht auch eine Suchfunktion bereit, über die man ihn direkt findet. Als alle gewünschten Sensoren vorhanden waren, setzten wir noch die Thresholds einiger Sensoren anders, da diese mit den Standardeinstellungen unerwünschte Alarme produzierten (das geht in den Sensoreinstellungen) und definierten einen Report, der uns täglich per Mail über den Status unseres Netzwerks informierte.

Reports lassen sich unter "Reports / Add Report" einrichten. Hier stehen auch diverse Templates zur Verfügung, die das Einrichten des Reports vereinfachen. Dazu gehören unter anderem "Tabelle mit Daten", "Nur Grafiken", "Liste der Sensoren" und "Top 100 höchste und tiefste". Außerdem kann man auch noch angeben, wann der Report erstellt werden soll, welcher Zeitraum in ihm berücksichtigt wird und Ähnliches. Nach dem Einrichten des Reports war die Konfiguration unserer Umgebung abgeschlossen und wir gingen in den Normalbetrieb über.

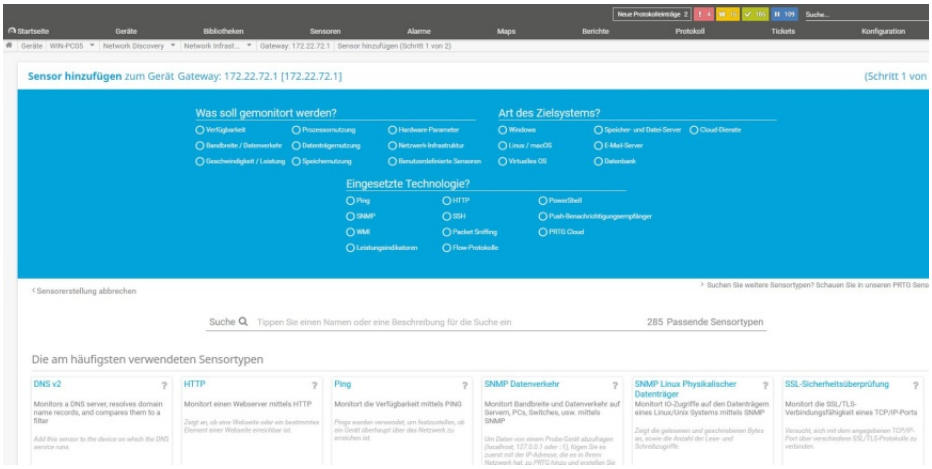
Unterschiede zum On-Premises-PRTG

An dieser Stelle ergibt es Sinn, kurz auf die bereits erwähnten Unterschiede einzugehen, die zwischen dem PRTG on-premises und dem Hosted PRTG bestehen. Der wichtigste Unterschied ergibt sich aus der Benutzerverwaltung. Es existiert keine "Add User"-Funktion, stattdessen findet sich die Möglichkeit, Benutzer per E-Mail einzuladen. Dazu müssen die Administratoren dem betroffenen User einen Namen und eine E-Mail-Adresse geben. Außerdem können sie unter anderem noch den Benutzertyp (Read/Write oder Read-only), die Benutzergruppe und den Status (Aktiv, Pausiert) festlegen.

Die eingeladenen Anwender erhalten dann eine Mail mit ihren Credentials und einem Link zum Einloggen bei Hosted PRTG. Paessler hat auch die Option integriert, mehrere Anwender auf einmal oder sogar ganze Benutzergruppen hinzuzufügen.

Es gibt bei Hosted PRTG abgesehen davon keine SMTP-Einstellungen, da der Mail-Server, über den die Alerts und Tickets verschickt werden, bereits von Paesslerseite aus konfiguriert wurde. Darüber hinaus gibt es aus Sicherheitsgründen keine

Funktion, Programme oder Skripts auf der Hosted Probe auszuführen. Auf der Remote Probe im LAN geht das schon. Weitere Informationen zu dieser Thematik gibt es unter Differences between PRTG Network Monitor and PRTG Hosted Monitor | PRTG Manual (paessler.com).

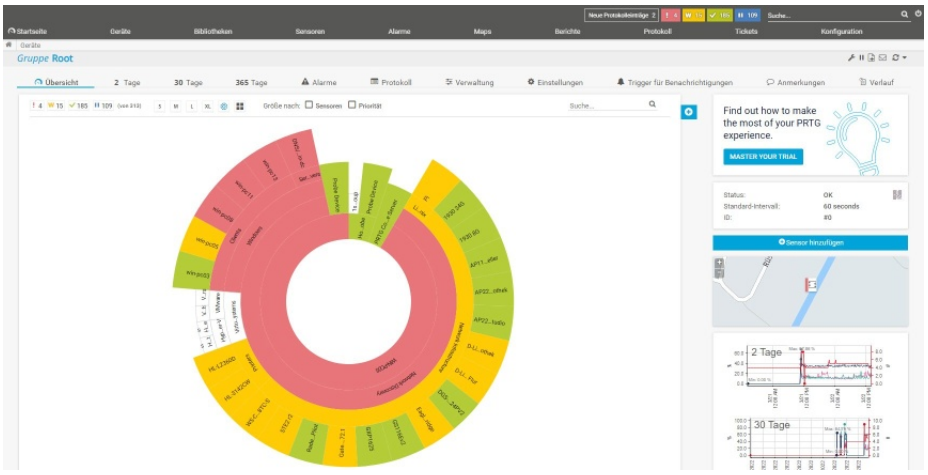


Der Auswahldialog für die Sensorsuche

Die Arbeit mit Hosted PRTG im laufenden Betrieb

Nachdem wir unser Monitoring-System so eingerichtet hatten, dass es alle unsere Komponenten so wie wir das wollten im Auge behielt, nahmen wir im Test kurz den Funktionsumfang der Lösung unter die Lupe. Das Web-Interface wurde in mehrere unterschiedliche Bereiche aufgeteilt. Der erste nennt sich “Home” und umfasst eine grafische Übersicht über die Sensoren mit ihrem Status und die Alarme. Außerdem gibt es Informationen zu den Vortagsaktivitäten mit der Zahl der Sensor-Scans, den Sensor-Statusänderungen, den gesendeten Benachrichtigungen, den erstellten Reports und vielem mehr.

Die Geräteübersicht umfasst im Gegensatz dazu in einer Baumstruktur die erfassten Gerätegruppen mit den darin enthaltenen Devices und Sensoren. Dabei wird der Sensorstatus jeweils farblich hervorgehoben, so dass die zuständigen Mitarbeiter sofort sehen, wo Probleme auftreten. Neben der Baumstruktur gibt es übrigens noch zwei andere Darstellungsformen. Die erste nennt sich "Sunburst-Darstellung" und zeigt von innen nach außen die ganze Infrastruktur. In der Mitte befindet sich die Probe, und dann geht es über die Gerätegruppen und Ähnliches nach außen bis hin zu den einzelnen Devices.



Die Sunburst-Ansicht mit diversen Fehlern

Meldet ein Sensor einen Fehler, so färbt sich nicht nur sein Eintrag rot ein, sondern auch die der dazugehörigen Gruppe und der betroffenen Probe. So können die Verantwortlichen auf einen Blick erkennen, wo der Fehler herkommt. Die Kachelansicht visualisiert die vorhandenen Sensoren im Gegensatz dazu als Rechtecke.

Die “Libraries” kommen zum Einsatz, um einen schnellen Überblick über bestimmte Aspekte des überwachten Netzes zu bekommen. In den genannten Bibliotheken lassen sich Sensoren zusammenfassen, die thematisch zusammenpassen. Das können beispielsweise alle Sensoren sein, die sich mit der CPU-Last auf verschiedenen Geräten befassen, oder auch Sensoren, die den Speicherplatz oder die Bandbreite im Auge behalten.

Die Sensorübersicht umfasst – wie der Name vermuten lässt – eine Liste aller im System vorhandenen Sensoren. Unter “Alarme” findet sich im Gegensatz dazu eine Übersicht über die Sensoren, die sich im Alarmstatus befinden.

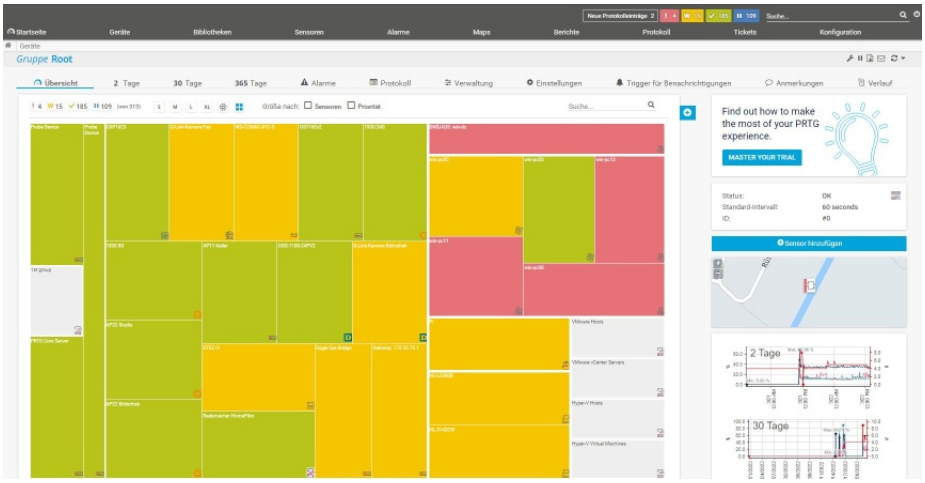
Interessanter ist der Bereich “Maps”, denn hier legen die zuständigen Mitarbeiter bei Bedarf Karten der Topografie ihrer Netze an. Diese Karten können ein be-

liebiges Hintergrundbild (beispielsweise einen Bauplan) verwenden. Die Administratoren sind dann dazu in der Lage, auf diesem Hintergrundbild Icons für die einzelnen überwachten Komponenten zu platzieren. Diese Icons geben auch Aufschluss darüber, welche Sensoren sich auf den betroffenen Geräten in welchem Zustand befinden. Auf die Reports sind wir bereits im Vorfeld eingegangen. Die Log-Übersicht gibt Aufschluss darüber, welche Aktionen in PRTG selbst ausgeführt wurden, beispielsweise das Pausieren eines Sensors oder das Anlegen einer Karte.

Unter "Tickets" findet sich ein Ticketing-System, mit dem die Mitarbeiter ihre Arbeit koordinieren können. "Setup" schließlich umfasst alle Funktionen, die zum Administrieren das PRTG-Systems selbst relevant sind. Dazu gehören die Benutzerverwaltung, Einstellungen zum Management-Interface und vergleichbare Dinge.

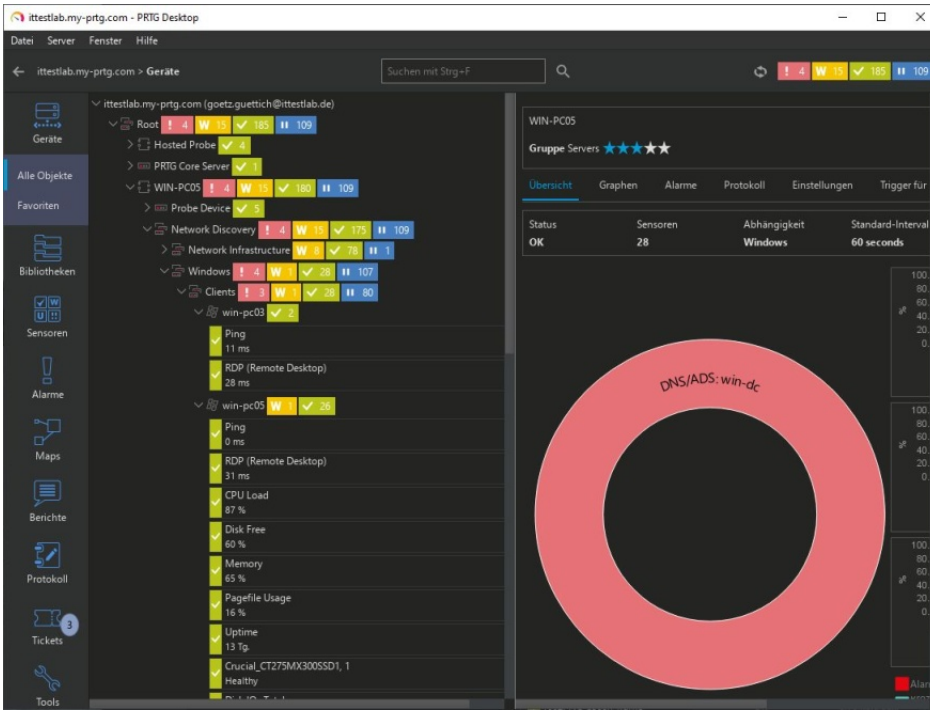
Die Apps

Um PRTG zu nutzen, sind die Anwender nicht auf das Web-Interface beschränkt. Es stehen auch Apps für Android und iOS sowie für Linux, macOS und Windows zur Verfügung.



Die Kachelansicht bietet eine alternative Darstellung

Diese lassen sich sowohl mit dem On-Premises-PRTG als auch mit dem Hosted PRTG nutzen. Sie informieren unter anderem über den Status der Systeme und geben über die mobilen Endgeräte Alarmmeldungen an die Anwender aus.



Die Geräteübersicht mit dem Core-Server in der Cloud und der lokalen Probe sowie den überwachten Komponenten im LAN

Fazit

Der PRTG Hosted Monitor war im Test schnell und problemlos eingerichtet und funktionierte im Betrieb einwandfrei. Gut ist, dass sich das System über die Apps ohne weiteren Konfigurationsaufwand von Überall aus nutzen lässt und dass die Administratoren nicht gezwungen sind, die Verwaltung der PRTG-Instanz selbst, mit dem Einspielen von Updates und so weiter, durchzuführen. Auch die Sicherheitsfunktionen, die Paessler implementiert hat, um die Daten der Kunden zu schützen, lassen keine Fragen offen. IT-Verantwortliche, die auf der Suche nach einen Cloud-basierten Monitoring-Lösung sind, sollten das Angebot auf jeden Fall unter die Lupe nehmen.

PRTG Hosted Monitor

Lösung zum Überwachen von Netzwerkkomponenten über die Cloud.

Vorteile:
- Einfache Inbetriebnahme
- Großer Leistungsumfang

Hersteller:
Paessler AG
www.paessler.com/de