Ausgabe 20/2011 21. Oktober 2011 € 4,90 sfr 8,90 funkschau.de

funkschau

Kommunikationstechnik für Profis

LAB TESTED funkschau

SEI WACHSAM

Netzwerk-Monitoring-Software

Sonderdruck

PAESSLER
the network monitoring company

Bild: funkschau Quelle: fotolia

Sei wachsam

Netzwerk-Monitoring-Software – sie informiert in Echtzeit darüber, wie es um die Gesundheit der Netzwerkhardware, Netzwerkservices und -applikationen bestellt ist. Damit sind Netzwerk-Monitoring-Pakete unverzichtbare Werkzeuge eines jeden Administrators, denn niemand kann es sich heute noch erlauben, sich anbahnende Probleme zu spät zu bemerken.

Die Netzwerkinfrastruktur zählt heute zu den kritischsten Elementen jeder Geschäftsstrategie. Kaum ein Unternehmen, das sich nicht auf die permanente Verfügbarkeit von Geschäftsapplikationen und damit der Technik, die diese Applikationen liefert, verlassen können muss. Dies verlangt von der IT-Abteilung eines jeden Unternehmens, ob KMU oder Großkonzern, eine proaktive Beobachtung aller involvierten Komponenten, denn nur so lassen sich Ausfälle vermeiden oder zumindest schnell und mit minimalen Auswirkungen auf die Produktivität beheben.

Moderne Netzwerk-Monitoring-Produkte sind die Werkzeuge, die das IT-Personal den Puls des Netzwerks und dessen Komponenten spüren lassen. Sie sind heute extrem leistungsfähig, in aller Regel leicht bereitstellbar sowie nutzbar und für Unternehmen jeder Größe erschwinglich. funkschau testete vier typische Vertreter dieser Produktkategorie. Ausgesucht wurden Produkte, die nicht nur von großen Unternehmen mit ausgewachsenen IT-Abteilungen bereitgestellt und angewandt werden können, sondern solche, die auch für KMUs mit vielleicht nur zwei, drei IT-Allroundern problemlos nutzbar sind. Aus diesem Grund blieb beispielsweise Nagios außen vor. Das populäre Produkt hat seine Stärken, aber dazu zählt eine leichte Bereitstellung sicher nicht. Für KMUs besser geeignet ist Nagios, wenn es in Form einer Appliance erworben wird – die Sonarplex-Appliance von Azeti Networks ist beispielsweise ein geniales Produkt, das auf Nagios basiert. Aber in diesem Test sollte es um Softwarelösungen gehen, also blieben Nagios und seine Derivate draußen. Ins Rennen gingen indes folgende Produkte: Ipswitchs „WhatsUp Gold Premium“, ManageEngines „OpManager“, Paesslers „PRTG-Network-Monitor“ und Solarwinds „Orion-Network-Performance-Monitor“.

Paessler PRTG-Network-Monitor Version 9

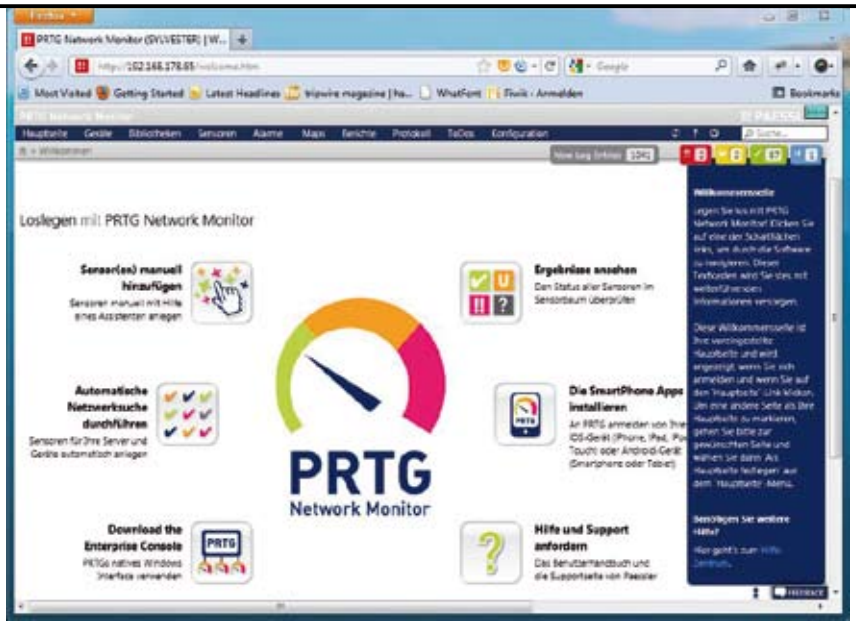
Mit großen Schritten schreitet die Weiterentwicklung bei Paessler voran. Seit unserem letzten Test der ausgezeichneten Netzwerk-Monitoring-Software dieses Herstellers vor gerade mal einem Jahr hat sich die Versionsnummer vor dem Punkt um einen Zähler erhöht: Das in Kürze auf den Markt kommende neue Release des PRTG-Network-Monitors besitzt also die Versionsnummer 9. Wir hatten bereits Gelegenheit, den Release-Candidate 1 zu testen. Und was wir sahen, hat uns gefallen.

Das Setup der Software vollzieht sich wie gewohnt sehr schnell und einfach: nach nicht einmal zwei Minuten war der PRTG-Network-Monitor auf der Platte der Testmaschine. Und das war es dann auch schon. Besondere Voraussetzungen, beispielsweise eine funktionierende Microsoft-SQL-Server- oder MySQL-Installation, sind nicht zu beachten, denn so etwas braucht das Programm im Gegensatz zu einigen anderen Monitoring-Paketen gar nicht. Ein Punkt beim Setup verlangt allerdings Aufmerksamkeit: PRTG-Network-Monitor wird entweder im Einzel- oder im Clustermodus installiert. Der Einzelmodus eignet sich für kleinere Netzwerkumgebungen oder für Einsteiger, die erst einmal Erfahrungen mit dem Produkt sammeln möchten. Im Clustermodus installiert der Administrator das Produkt auf zwei oder mehr Servern. Dadurch erhält er eine Hochverfügbarkeitsinstallation mit automatischem Failover, eine Lastverteilung und die Möglichkeit, das Monitoring von verschiedenen Standorten aus zu betreiben.

Etwas beim Setup-Prozess störte uns trotz seiner Geradlinigkeit: Zum Abschluss startet die Installationsroutine den Rechner neu – und wir sind uns nicht sicher, zuvor eine Warnung gesehen zu haben.

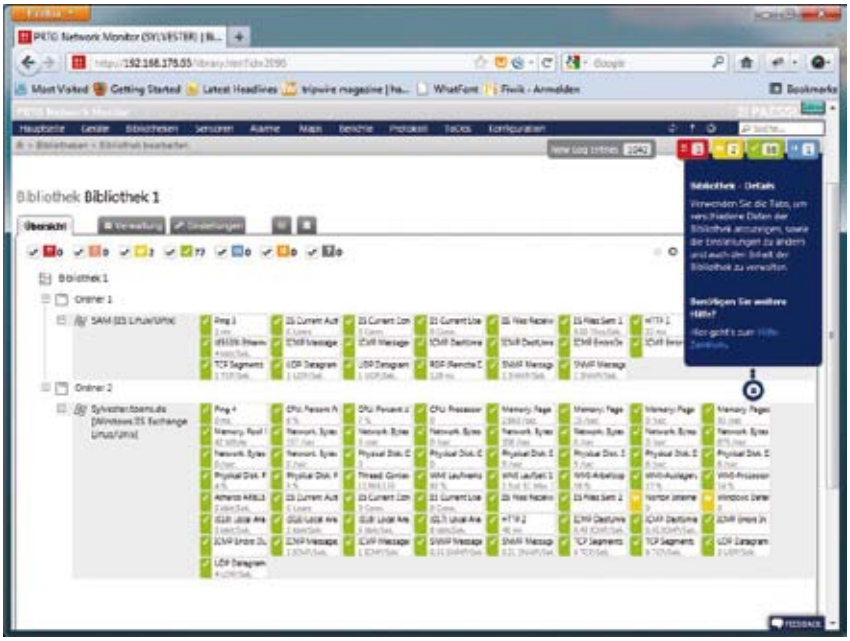
Für jedes physische Gerät im Netzwerk, das PRTG-Network-Monitor beobachten soll, ist vom Administrator ein entsprechendes Gerät in der PRTG-Konfiguration zu erzeugen. Diesen Geräten sind ferner Sensoren zuzuweisen, von denen jeder einen bestimmten Aspekt des Netzwerks beziehungsweise Geräts überwacht. Das klingt nach jeder Menge Arbeit, allerdings kann PRTG-Network-Monitor diese Aufgabe automatisch ausführen – dazu später mehr, zunächst zur Monitoring- beziehungsweise Objekthierarchie: Alle Objekte

Bild: Paessler



Der bunte neue Willkommen-Bildschirm von PRTG macht den Einstieg ins Netzwerk-Monitoring einfach. Überhaupt braucht es wenig Phantasie, sich in der überarbeiteten Web-GUI zurechtzufinden.

Bild: Paessler



PRTGs Bibliotheken machen es Administratoren leicht, sich auf die Geräte und Dienste zu konzentrieren, die ihnen wichtig sind.

einer PRTG-Monitoring-Konfiguration sind in einer baumähnlichen Hierarchie organisiert, die eine einfach navigierbare Liste darstellt. Benutzer 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-Gruppe, die sämtliche Objekte eines Setups enthält. Einstellungen auf dieser Ebene gelten für alle Objekte. Jede Gruppe außer der Root-Gruppe ist Teil einer Probe. Eine Probe ist die Plattform, auf der das Monitoring stattfindet. Alle unterhalb der Probe konfigurierten Objekte werden über diese 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,

Testverfahren Monitoring-Software

Die vier Produkte wurden in einem Netzwerk installiert, in dem mehrere Windows-Server-2003/2008-Maschinen, ein Microsoft-Exchange-Server und ein Microsoft-SQL-Server-2008 ihren Dienst verrichteten. Die Maschinen im Netzwerk waren über Fast-Ethernet-Switches und SMC-WLAN-Router miteinander verbunden, eine Anbindung ans Internet erfolgte über einen ADSL-Router. Die Client-Maschinen arbeiteten mit unterschiedlichen Betriebssystemen, darunter Windows-XP, Windows 7 und Linux (Open-Suse). Zu den im Netzwerk ausgeführten Diensten und Protokollen gehörten neben anderen TCP/IP, DNS, POP3, SMTP, IMAP, SNMP, HTTP, HTTPS und FTP.

Nach einer ersten Installation und – wo nötig – Konfiguration der Monitoring-Programme ließen wir sie das Netzwerk erforschen und eine Weile Informationen über die installierten Geräte, Dienste, Applikationen und Protokolle sammeln. Anschließend wurden Schwellenwerte eingestellt und auszuführende Aktionen definiert. Untersucht wurde, ob die Programme Schwellenwertüberschreitungen, sich ändernde Systemzustände und Performance-Einbrüche erkennen und wie vorgesehen reagieren. Bewertet wurde unter anderem das Preis-Leistungsverhältnis, die Bedienerfreundlichkeit sowie die Art und Weise, in der die Produkte ein Monitoring räumlich verteilter Netzwerke unterstützen.

Steckbrief

PRTG Network Monitor Version 9

funkschau Referenz

Hersteller: Paessler
Charakteristik: Netzwerk-Monitoring-Software
Preis: bis 500 Sensoren 1.071 Euro, bis 1.000 Sensoren 1.636 Euro, unlimitierte Sensoren 4.165 Euro

Web: www.paessler.com/prtg/

Plusminus:

+ Sehr umfangreiches Paket
+ Angenehme und leicht bedienbare Web-GUI
+ Durchdachte Objekt-/Geräte-hierarchie
+ Gutes Preis-Leistungsverhältnis

Lizenzierung

Op-Manager und Whatsup-Gold werden nach der Anzahl zu beobachtender Geräte lizenziert, PRTG-Network-Monitor hingegen nach der Anzahl der Sensoren, die eine Organisation zu nutzen wünscht. Natürlich ist es für eine Organisation einfacher, die Anzahl zu beobachtender Geräte zu bestimmen, als zu entscheiden, wie viele Sensoren sie zur Überwachung einer gewissen Anzahl Geräte benötigt – dafür müsste vor dem Einkauf schon mehr oder weniger klar sein, welche Aspekte des Netzwerks beziehungsweise der Netzwerkgeräte beobachtet werden sollen. Diese unterschiedliche Lizenzierung macht Preisvergleiche schwierig, denn im Fall von PRTG sind für einige Systeme schnell 20 und mehr Sensoren installiert, während für andere Geräte vielleicht schon fünf, sechs Sensoren reichen. Gehen wir für einen Preisvergleich einmal davon aus, dass beim Einsatz von PRTG durchschnittlich zehn Sensoren pro Gerät genutzt werden. In diesem Fall reicht für ein kleines Netzwerk mit 50 zu überwachenden Geräten die 500-Sensoren-Lizenz aus, die vermutlich auch für die Version 9 rund 1.100 Euro kosten wird. Eine Op-Manager-Lizenz für 50 Knoten schlägt zwar nur mit rund 1.000 Dollar zu Buche, dabei ist aber zu berücksichtigen, dass PRTG in der Grundausstattung wesentlich vollständiger ist. Für Whatsup-Gold sind bereits zur Überwachung von nur 25 Geräten 1.700 Euro oder für 100 Geräte 2.100 Euro in die Hand zu nehmen. PRTG erlaubt mit seiner 500-Sensoren-Lizenz bereits Distributed-Monitoring, während Whatsup-Gold und Op-Manager auf das Monitoring in einem einzelnen lokalen Netzwerk eingeschränkt sind. Von diesen Lizenzierungsformen ist die von PRTG am flexibelsten, denn werden weniger Sensoren genutzt lassen sich mehr Geräte überwachen. Irgendwo zwischen diesen beiden Lizenzierungsformen liegt Orion-NPM mit seiner Lizenzierung nach Anzahl der zu beobachtenden Elemente. Aber unabhängig davon, was letztendlich als Element gezählt wird, ist Orion-NPM mit Abstand das teuerste Produkt unter den vier Kandidaten.

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. Dabei handelt es sich um ein internes Systemgerät, das mit verschiedenen Sensoren die Parameter des Computers überwacht, auf dem die Probe selbst läuft. Jedem Gerät lassen sich Sensoren hinzufügen, die jeweils 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. Selbstverständlich kommt die neue Version auch mit einigen neuen Sensoren, darunter besonders erwähnenswert ein Zwei-Wege-QoS-Sensor, ein WMI-Security-Sensor und herstellerspezifische Hardwaresensoren für Dell-, HP- und APS-Systeme.

Lässt sich bereits mit all diesen hierarchisch organisierten Objekten das System sehr übersichtlich, leicht navigierbar und nach funktionellen Gesichtspunkten gegliedert darstellen und nutzen, so erlebt der Benutzer mit den in Version 9 eingeführten Bibliotheken noch eine Steigerung. Mit deren Hilfe können Benutzer ihre eigenen „Bäume" erzeugen. Das verbessert die Übersicht nochmals und führt zu einer höheren Geschwindigkeit bei großen Installationen. Die „Baumdarstellung" innerhalb einer Bibliothek ist sehr interaktiv, beispielsweise verschiebt oder klont der Benutzer Monitoringobjekte in Bäumen oder Bibliotheken einfach per Drag-and-Drop. So stellt er sich sehr schnell und einfach eine Sammlung nur der Objekte zusammen, die er tatsächlich beobachten möchte.

Nach dem Setup des Programms befinden sich zwei neue Verknüpfungen auf dem Desktop beziehungsweise im Windows-Startmenü: „PRTG Network Monitor" und „PRTG Enterprise Console". Die PRTG-Enterprise-Console ist die ehemalige Windows-GUI, die allerdings einige Verbesserungen erfahren hat. Sie unterstützt nun die gleichzeitige Anzeige von Daten mehrerer PRTG-Core-Installationen. Mit anderen Worten: Sämtliche Monitoring-Daten in einem einzelnen Programm, selbst bei den größten Setups. Die Konsole enthält noch viele weitere neue Features und bietet nun fast die gesamte Funktionalität der Web-GUI, dennoch wird die Web-GUI, der PRTG-Network-Monitor, sicher die bevorzugte Arbeitsumgebung der meisten Administratoren bleiben.

Die gesamte Webschnittstelle wurde aufgepeppt, nicht nur optisch, sondern auch technisch. Aber natürlich ist es die neue Optik, die als erstes auffällt. Alles ist viel gefälliger geworden und neue Icons machen die Navigation nochmals intuitiver. Steigernd auf die Produktivität wirken sich einige neue Funktionen aus, beispielsweise Multi-Edit für Sensor-Kanal-Einstellungen, das Bestätigen eines Alarms und das Pausieren eines Sensors für einen bestimmten Zeitraum oder auch der neu geschriebene Willkommen-Assistent, der die Benutzerführung beim anfänglichen Setup verbessert. Beispielsweise macht die Willkommen-Seite nun unübersehbar darauf aufmerksam, dass es eine gute Idee ist, das Standardkennwort des Administrators zu ändern und SSL-Verschlüsselung für die PRTG-Website einzuschalten. Etwas nervig war allerdings, dass wir es nicht schafften, diesen Kennworthinweis verschwinden zu lassen, nachdem wir das Kennwort geändert hatten. Neu geschrieben wurden auch die Seiten zum Editieren der Benachrichtigungs-Trigger, die Sensoren-Auswahl sowie die Konfigurationsseite. All diese Seiten sind viel übersichtlicher und einfacher anwendbar geworden. Aktualisierte Ajax-Funktionalität sorgt für eine Geschwindigkeitsverbesserung und mit Support für Desktop-Benachrichtigungen werden Google-Chrome-Browser jetzt besser unterstützt.

Eine der ersten Aufgaben nach dem PRTG-Setup dürfte das Hinzufügen der zu beobachtenden Geräte sein. Dies geht am einfachsten mit der automatischen Netzwerksuche, die sich direkt von der Willkommen-Seite starten lässt. Die Suche erfolgt über eine Liste individueller IP-Adressen, IP-Adressbereiche mit eingegebener Basisadresse, IP-Adressen plus Subnetzinformationen, IP-Adressen mit Oktett-Bereich und neuerdings auch über Listen individueller IPv6-Adressen. PRTG liefert nicht nur die IP-Adressen und gegebenenfalls DNS-Namen der gefundenen Geräte zurück, sondern versucht anhand der MAC-Adressen der Geräte auch gleich den Hersteller zu ermitteln. Natürlich findet die Suchroutine nicht nur Geräte im Netzwerk, sie installiert auf Wunsch auch gleich geeignete Sensoren darauf. Die Routine dies tun zu lassen, ist sehr empfehlenswert, obwohl die gesamte Discovery dadurch in einem großen Netzwerk recht lange dauert. Wer es schneller haben möchte, kann aber auch nur Geräte entdecken lassen und Sensoren später manuell hinzufügen oder über Gerätevorlagen nur ausgewählte Sensoren automatisch hinzufügen lassen. Die automatische Suche nutzt hauptsächlich Ping, SNMP und WMI; sie funktioniert ausschließlich im LAN. Die Suche lässt sich auch per Zeitplan automatisch und wiederholt starten, zuvor bereits entdeckte Geräte werden dabei auf Wunsch übersprungen.

Das Alarmsystem von PRTG-Network-Monitor funktioniert einwandfrei. Alarme und Warnungen zeigt das Programm deutlich an und protokolliert sie penibel. Admi-

nistratoren, die nicht ständig vor der Konsole sitzen, erhalten Benachrichtigungen via E-Mail und/oder SMS. Überhaupt ist das Programm sehr mitteilungsfreudig und liefert permanent brauchbare Informationen und Hilfestellungen.

Ipswitch WhatsUp-Gold 15

Whatsup-Gold ist ein eigenständiges Monitoring-Produkt, das den Status von Netzwerkgeräten und -diensten beobachtet, bei Abweichungen von der Norm Alerts erzeugt und Aktionen auslöst. So richtig rund wird das Netzwerk-Monitoring aber erst mit weiteren Produkten aus der Whatsup-Gold-Produktfamilie, beispielsweise mit dem Whatsup-Flow-Monitor zur Unterstützung von Netflow, mit Whats-Connected für Layer-2/3-Netzwerk-Discovery und Topologie-Mapping oder Whats-Virtual, das zusätzliche Fähigkeiten zum Monitoring von Vmware-Umgebungen beisteuert. Und Whatsup-Gold selbst, also gewissermaßen das Basisprodukt, ist obendrein noch in vier verschiedenen Editions erhältlich, die sich in ihrem Funktionsumfang voneinander unterscheiden. Diese Vielfalt ist einerseits ganz angenehm, muss doch der Kunde so nicht zwangsläufig für Features zahlen, die er gar nicht braucht und nutzt. Andererseits wird so die Produktauswahl etwas schwieriger und die Gesamtkosten des Pakets sind nicht ganz so einfach kalkulierbar.

funkschau testete Whatsup-Gold in der Premium-Edition, die Geräte und Dienste innerhalb eines einzelnen Netzwerkstandorts überwacht, erweitertes Management für Microsoft-Exchange-, Microsoft-SQL- und SMTP-Mail-Server bietet, Performancedaten in Echtzeit liefert und Applikationsmonitoring via Microsofts WMI unterstützt. Mit dieser Edition ist es jedoch nicht möglich, Remote-Netzwerke von einem zentralen Standort aus zu beobachten, denn dafür offeriert Ipswitch die teurere Distributed-Edition beziehungsweise die für Solution-Provider vorgesehene MSP-Edition.

Das herunterzuladende Whatsup-Gold-Premium-Paket ist mit 300 MByte ein Schwergewicht, allerdings ist hier sofort Whats-Connected mit dabei. Bevor sich der Administrator dann an die Installation begibt, sollte er sein Netzwerk beziehungsweise die Netzwerkgeräte vorbereiten, indem er darauf SNMP und /oder WMI einschaltet. Tut er dies nicht, werden die Ergebnisse der späteren Netzwerk-Discovery nur sehr bescheiden ausfallen. Das Setup für den Test bereitete an und für sich keine Schwierigkeiten, es dauerte nur relativ lange, allerdings nicht so lange, wie bei Orion-NPM. Entscheidet sich der Benutzer für ein typisches Setup, dann installiert die Setup-Routine automatisch den Microsoft-SQL-Server-Express (2005), den das Produkt zur Speicherung der Daten nutzt. Dieser Server mochte im Test-Setup aber nicht starten. Ein wiederholtes Setup von Whatsup-Gold, diesmal benutzerdefiniert, ließ uns einen auf der Testmaschine installierten Microsoft-SQL-Server-2008 auswählen, mit dem schließlich alles funktionierte.

Am Ende der Setup-Routine startet automatisch eine Webschnittstelle, die eine Art Assistent präsentiert, der dem Benutzer einige einfache Fragen stellt, beispielsweise nach dem gewünschten Administrator-Passwort und nach E-Mail-Einstellungen. Dann folgt die Netzwerk-Discovery, die über IP-Adressbereiche funktioniert oder einen SNMP-Smart-Scan durchführt. Und hier sehen wir ein Problem: Natürlich ist jeder Administrator geneigt, diese Netzwerk-Discovery mit einem Klick auch sofort zu starten. Bleibt es bei den Voreinstellungen, findet die Routine sehr zügig alle Geräte und löst die Namen einwandfrei auf, allerdings werden keinerlei Performancemonitore oder aktive und passive Monitore für die entdeckten Geräte installiert beziehungsweise aktiviert. Wer mehr möchte, als die Geräte per Ping pollen zu lassen, muss ihnen nun viele Monitore manuell zuweisen. Trotzdem diese Operation als Bulk-Operation durchführbar ist, bleibt sie unangenehm. Und unnötig ist sie obendrein, denn genau diese Zuweisung funktioniert auch automatisch und relativ einfach. Dafür sind lediglich in der Whatsup-Gold-Konsole Geräterollen anzupassen. Im Verlauf dieser Anpassung spezifiziert der Benutzer einfach die Performancemonitore sowie die aktiven und passiven Monitore, die er je nach Geräterolle automatisch aktiviert haben möchte. Bei der Gelegenheit kann er auch gleich Aktionen konfigurieren, also beispielsweise einstellen, wie er alarmiert werden möchte, wenn Whatsup-Gold einen Fehler auf einem Gerät entdeckt. Diese Einstellungen lassen sich nicht über die Web-Discovery-Konsole durchführen, und deshalb ist es völlig unverständlich, warum Ipswitch genau diese Konsole am Ende des Setups automatisch präsentiert.

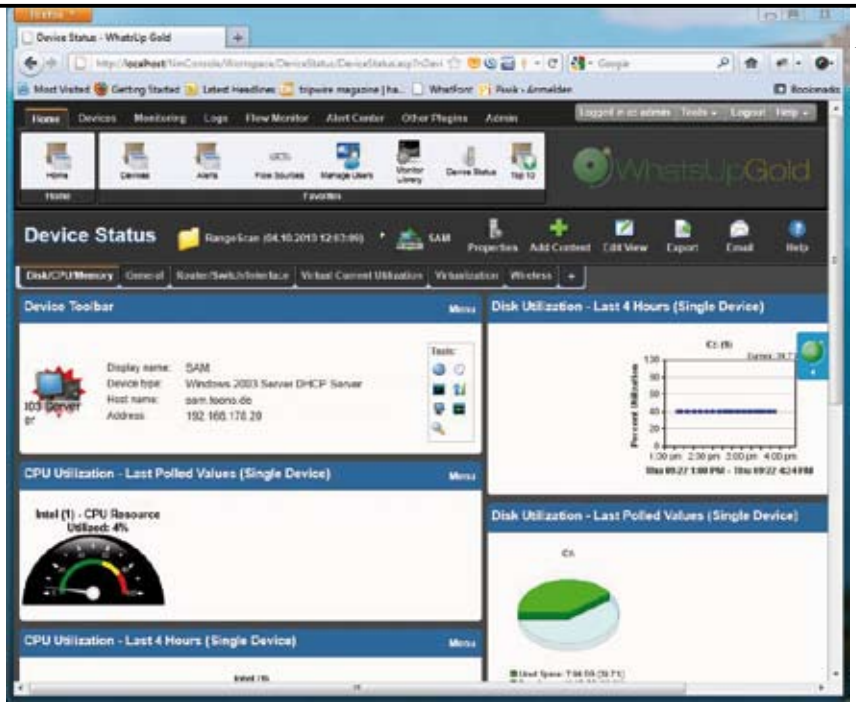


Bild: Ipswitch

Die Webschnittstelle von Whatsup-Gold hat nicht nur optisch zugelegt, sondern zeigt auch neue Leistungszähler. Die Virtualization- und Wireless-Links machen aber nur mit existierenden Vmware-Installationen beziehungsweise Cisco-Airopeek-Produkten Sinn.

Steckbrief

WhatsUp Gold Premium v15

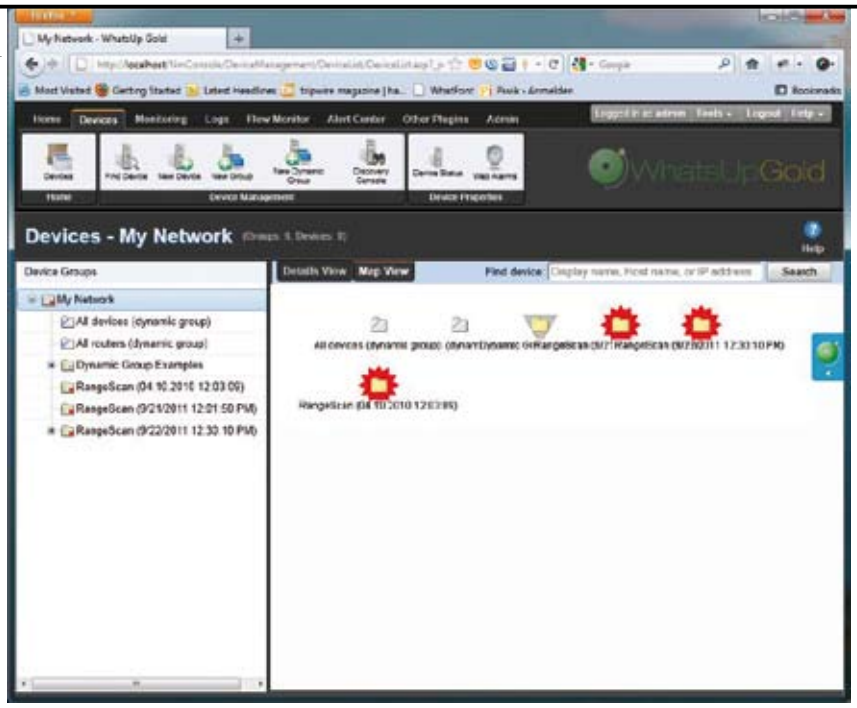
Hersteller: Ipswitch
Charakteristik: Netzwerk-Monitoring-Software
Preis: 25 Geräte 1.712 Euro, 100 Geräte 2.102 Euro, 300 Geräte 3.896 Euro, 500 Geräte 5.846 Euro

Web: www.whatsupgold.com

Plusminus:

+ Extrem umfangreiches Paket (mit Optionen und Plugins)
+ Dashboard-Applikation
– Verlangt mehr Einarbeitung als die anderen Produkte
– Wird sehr teuer, wenn einige der Optionen erforderlich sind

Bild: Ipswitch



Whatsup-Golds Map-View ist sicher verbesserungswürdig. Verschiebt der Benutzer die Icons nicht mit der Maus, dann ist die Beschriftung fast nicht zu entziffern.

Der neue Setup-/Konfigurationsdialog und die neue Web-GUI der Version 15 sehen sehr schick und modern aus. Und die Webschnittstelle lässt sich auch angenehm und zügig bedienen. Nach der Netzwerk-Discovery via Windows- oder Web-Konsole zeigt sich der Home-Workspace mit einigen Summary-Zählern, die beispielsweise die Anzahl der überwachten Geräte, die Anzahl der laufenden und ausgefallenen Geräte und Schnittstellen oder die Geräte im Wartungsmodus anzeigen. Die Navigation zu anderen Ansichten, beispielsweise Device- und Monitoring-Ansichten, Logs, oder das Alert-Center, geht schnell und einfach. Ipswitch bezeichnet die neue Web-GUI als aufgabenorientierte Schnittstelle, was man durchaus so stehen lassen kann.

In der Geräteansicht zeigt Whatsup-Gold am linken Fensterrand eine mit „My Network" überschriebene Baumstruktur. Darin befinden sich einige dynamische Gruppen, beispielsweise „Alle Geräte", „Alle Router", „Cisco-Geräte" oder „Windows-Geräte", ferner Gerätegruppen für jede durchgeführte Netzwerk-Discovery. Die jeweils selektierte Gruppe zeigt das Programm in einer Detail- oder Map-Ansicht. In Verbindung mit Whats-Connected führt Whatsup-Gold Layer-2-Discovery und Mapping durch. In diesem Fall zeigt die Map-Ansicht auch die Beziehungen der Geräte untereinander grafisch an. Die Standard-Map-Ansicht ist allerdings alles andere als übersichtlich, denn Beschriftungen sind teilweise übereinander geschoben und die Beschreibungen der durch Icons dargestellten Geräte und ihre Rollen sind arg winzig geraten und kaum zu entziffern. Hier sollte vielleicht der automatische Abstand der Icons voneinander und die Schriftgröße verbessert werden. Ansonsten sind diese Maps schön interaktiv und Fehler werden, wie es sich gehört, durch rote Farbe kenntlich gemacht.

Whatsup-Gold pollt Geräte im Netzwerk regelmäßig, um Statusänderungen zu erkennen. Dazu nutzt das Programm die oben erwähnten Monitore. Performancemonitore beobachten die Ressourcen eines Geräts, beispielsweise Platten, Schnittstellen und Speicher. Beispiele für aktive Monitore sind Ping-, DNS-, HTTP- und Schnittstellen-Monitore, Typen für passive Monitore sind SNMP-Traps, Syslog und die Windows-Ereignisanzeige. Abhängig von den beim Pollen erhaltenen Antworten führt Whatsup-Gold Aktionen aus, beispielsweise benachrichtigt es den Administrator oder startet einen Dienst neu. Das Alert-Center hatte Ipswitch bereits in Whatsup-Gold Version 14 erneuert; es funktioniert nach wie vor einwandfrei. Das Programm kann auch virtuelle Infrastrukturen (mit Whats-Virtual) überwachen, beschränkt sich dabei jedoch auf Vmware. Ähnlich verhält es sich bei Wireless-Netzwerken, wo sich bei Whatsup-Gold alles um Cisco-Aeronet-Produkte dreht.

Einmalig unter den getesteten Produkten ist die Dashboard-Applikation von Whatsup-Gold. Diese ab der Premium-Edition im Gesamtpaket enthaltene eigenständige Applikation durchläuft wiederholt Reportseiten der Whatsup-Gold-Webschnittstelle und zeigt sie an. Administratoren erhalten damit kontinuierlichen Einblick in Netzwerkzustand und Gesundheit. Allerdings müssen sie dafür zunächst in einer „Playlist" festlegen, welche Seiten sie sehen wollen, was jedoch nicht weiter schwierig ist. Die Einstellungen lassen sich speichern.

Whatsup-Gold kommt mit einer Reihe zusätzlicher Werkzeuge, darunter ein SNMP-MIB-Walker und -File-Explorer, Traceroute, Lookup, ein Web-Performance-Monitor und -Task-Manager sowie ein Diagnose-Tool, das zahlreiche System- und Applikations-Checks durchführt und aus den Resultaten einen Bericht erzeugt. Außerdem ist eine vollständige TFTP-Server-Applikation enthalten, die bis auf die permanente Werbeeinblendung „Try Whatsconfigured" einen guten Eindruck hinterließ.

SolarWinds Orion Network Performance Monitor 10.1

Der „Orion Network Performance Monitor", kurz Orion-NPM, ist Solarwinds Flaggschiff-Produkt und zielt als solches schon nicht mehr auf kleinere Netzwerkumgebungen, sondern eher auf einen Einsatz in größeren Unternehmensnetzwerken. Die Produktbezeichnung lässt bereits vermuten, dass sich Orion-NPM vorrangig auf die Überwachung der Netzwerkperformance konzentriert und dabei beispielsweise Netzwerkapplikationen nicht berücksichtigt. Für ein Produkt, das sich also gewissermaßen auf eine einzige Aufgabe konzentriert, ist erstaunlich, wie dick es daher kommt – keines der getesteten Produkte installiert eine so riesige Menge Dateien, Services und einzelne Applikationen wie Orion-NPM. Schlank ist etwas anderes, und das muss der Benutzer unbedingt auch bei der Auswahl der Maschine für die Orion-NPM-Installation berücksichtigen. Solarwinds empfiehlt als Hardwareausstattung mindestens eine 2-GHz-Dual-Core-CPU, 2 GByte freien Festplattenspeicher – möglichst auf einem RAID-1-Laufwerk – und 3 GByte Arbeitsspeicher. Das klingt zunächst noch bescheiden, aber offensichtlich gelten diese Empfehlungen für ein Serversystem, auf dem nicht noch andere Applikationen oder Services ausgeführt werden. Ausdrücklich empfiehlt Solarwinds beispielsweise zusätzlich, den für den Betrieb von Orion-NPM notwendigen Microsoft-SQL-Server auf einem separaten Server auszuführen. An diesen Server stellt das Produkt dann ganz ähnliche Anforderungen. Anfängliche Versuche, das Produkt auf einem schwächeren System auszuführen, gaben wir rasch auf – es macht keinen Spaß. Die Mitbewerber nennen ähnliche Mindestanforderungen wie Solarwinds,

sind in der Realität aber doch etwas genügsamer. Orion-NPM läuft uneingeschränkt auch in virtuellen Maschinen unter Vmware oder Microsoft-Virtual-Server. Für die virtuellen Maschinen gelten identische Systemvoraussetzungen wie für die physischen Server.

Was die Software betrifft stellt Orion-NPM keine besonderen Anforderungen. Als Betriebssystem für einen Produktiveinsatz sollte Windows-Server-2003 oder -2008 mit Internet-Information-Services, Net-Framework und SNMP-Trap-Service eingesetzt werden. Für den Web-Console-Browser schlägt Solarwinds Internet-Explorer ab Version 6 mit Active-Scripting oder Firefox ab Version 3 vor. Unter Firefox wird allerdings die Toolset-Integration nicht unterstützt. Die Orion-Datenbank verlangt einen Microsoft-SQL-Server-2005-SP1- oder SQL-Server-2008-Express, -Standard oder -Enterprise. Bei typischer Installation beziehungsweise nicht vorhandenem SQL-Server installiert die Setuproutine automatisch die 2005er Express-Version. Und das war gut so, denn ein Testsetup auf einer Windows-7-Maschine (diese Windows-Version unterstützt Solarwinds für eine Evaluierung) wollte nicht wirklich mit dem darauf installierten SQL-Server-2008 Freundschaft schließen.

Zu Anfang erwähnten wir bereits, dass sich Orion-NPM auf das Monitoring der Netzwerkperformance konzentriert. Möchte ein Administrator daneben auch die Performance seiner Netzwerkapplikationen überwachen oder die Netzwerkkonfiguration verwalten, muss er auf separate Produkte beziehungsweise Module zurückgreifen. Optionale Erweiterungen gibt es außerdem für eine Netflow-Traffic-Analyse, ein IP-Adress- und ein IP-SLA-Management sowie für viele weitere Aufgaben. Selbst ohne solche Erweiterungen ist Orion-NPM ein komplexes Produkt, das schon beim Setup Geduld verlangt. Es dauert relativ lange, bis das Basissystem installiert und konfiguriert ist. Der Administrator selbst hat dabei eigentlich nichts zu tun, er muss lediglich warten.

Am Ende des Setups startet automatisch eine Netzwerk-Discovery, die im Test das lokale Subnetz sehr schnell durchsuchte. Sie arbeitete einwandfrei, identifiziert sogar jede einzelne Netzwerkschnittstelle sowie alle darüber laufenden Protokolle und löste Namen sauber auf. Beim ersten Start des System-Managers oder der Webkonsole schaut der Benutzer also nicht ins Leere, sondern die beiden Benutzerschnittstellen sind sofort bevölkert. Und nicht nur das, Orion-NPM hat auch schon mit der Arbeit begonnen und stellt die ersten Performanceinformationen zur Verfügung, darunter durchschnittliche Antwortzeiten und Paketverluste, Verfügbarkeiten, CPU-Lasten und Speichernutzung sowie Netzwerkadapterinformationen (Fehler- und Traffic-Charts). Abrufbar sind ebenfalls schon die ersten, das Netzwerk überspannenden Summary-Charts und Top-10-Summary-Charts. Stichwort Charts: Orion-NPM liebt es (und ist gut darin), die unterschiedlichsten Performancedaten grafisch darzustellen. Natürlich sind auch Detailinformationen abrufbar, beispielsweise in tabellarischer Form.

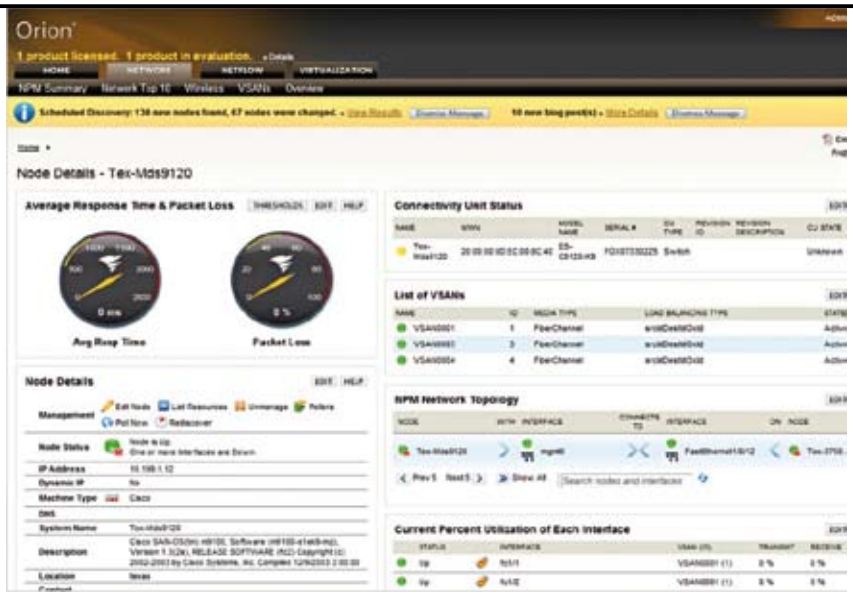


Bild: Solarwinds

Orion-NPMs LUCID-Interface: Logical, Usable, Customizable, Interactive, Drill-down. Eine angenehme Webkonsole, die mehr Fragen beantwortet als stellt.

Dem Administrator stehen also zwei Benutzerschnittstellen zur Verfügung, der System-Manager als Windows-GUI und eine Webkonsole. Die meisten Administratoren werden zur Webkonsole greifen, die der Hersteller nun gern als LUCID-Interface verstanden haben möchte. LUCID steht dabei für Logical, Usable, Customizable, Interactive und Drill-down. Diese Eigenschaften treffen in der Tat auf die Webkonsole zu, allerdings sind es Eigenschaften, die jede Webkonsole einer Managementapplikation besitzen sollte und häufig auch hat. Also so etwas Besonders ist das nun nicht. Aber die Webkonsole von Orion-NPM erlaubt eine einfache Navigation und macht es dem Benutzer leicht, sich zurechtzufinden, sowie Daten in Grafiken, Tabellen, Maps und Top-10-Listen zu betrachten und anzupassen. Lobenswert, dass die Schnittstelle auch mobile Browser unterstützt. Es macht Spaß, mit dieser Schnittstelle zu arbeiten, sie ist reaktionsfreudig, überschaubar, gut anpassbar und stellt den Benutzer nicht vor Rätsel, sondern beantwortet zügig seine Fragen zum Zustand des Netzwerks.

Neben diesen beiden Schnittstellen beziehungsweise Applikationen befinden sich nach der Orion-NPM-Installation im Windows-Startmenü noch einige weitere neue Einträge. Dahinter verbergen sich unter anderem Programme zur Anpassung der Orion-NPM-Konfiguration, zur Pflege der Datenbank, zum manuellen Start der Netzwerk-Discovery und für den Netzwerk-Atlas. Apropos manueller Start der Netzwerk-Discovery: Das ist eigentlich nicht nötig, denn Orion-NPM durchsucht das Netzwerk periodisch nach Änderungen, schlägt dem Benutzer automatisch vor, neue Geräte zu

Steckbrief

Orion Network Performance Monitor 10.1

Hersteller: Solarwinds
Charakteristik: Netzwerk-Monitoring-Software
Preis: 100 Elemente 2015 Euro, 250 Elemente 4460 Euro, 500 Elemente 6905 Euro, unlimitierte Elemente 20350 Euro, Preise ohne Optionen wie Enterprise-Operations-Console oder Scalability-Engines.

Web: www.solarwinds.com

Plusminus:

+ Prima Webkonsole (LUCID-Interface)
+ Flexibles Alertsystem mit zentralem Message-Center
– Langwieriges, nicht immer problemloses Setup
– Für kleinere Umgebungen und unerfahrene Benutzer eine Nummer zu groß

überwachen, und erlaubt ihm, Netzwerk-Maps per Drag-and-Drop zu aktualisieren.

Das Alert-System von Orion-NPM ist flexibel, funktionierte wie die Discovery im Test einwandfrei und ist leicht zu nutzen. Wie die anderen Produkte generiert Orion-NPM Alerts, wenn ein Ereignis eintritt oder ein Schwellenwert überschritten wird. Für die Reaktion auf Alerts bietet das Programm viele Optionen, darunter die üblichen Benachrichtigungsoptionen, eine automatische Script- oder Programmausführung und eine Eskalationssequenz. Netzwerk-Alerts zu konfigurieren ist nicht schwer. Das Produkt erlaubt dem Administrator, Abhängigkeiten zwischen den Geräten beziehungsweise Elementen zu definieren und Alerts für zusammenhängende Ereignisse und/oder für über eine bestimmte Zeit andauernde Zustände zu konfigurieren. Das klingt komplizierter als es eigentlich ist: Der Administrator konfiguriert das System halt so, dass es nicht sofort Alarm schlägt, wenn vielleicht eine CPU-Utilization 90 Prozent überschreitet, sondern nur dann, wenn diese Utilization fünf Minuten lang anhält. Das Message-Center als Schaltzentrale präsentiert nicht nur alle im Netzwerk erzeugten Alerts, sondern auch alle Ereignisse, Syslog-Einträge und Traps.

Virtualisierung ist nach wie vor im Trend. Deshalb lässt sich Orion-NPM nicht nur problemlos selbst auf virtuellen Maschinen ausführen und zum Monitoring virtueller Datacenter nutzen, sondern unterstützt nun auch das Monitoring der virtuellen Infrastruktur. Das Produkt kommuniziert direkt mit der Vmware-Infrastruktur und ermittelt die Performance der Server sowie den Gesundheitszustand individueller virtueller Maschinen. Neu und sehr begrüßenswert sind außerdem die Unterstützung von VSAN und Fibre-Channel fürs Monitoring und Reporting sowie die Integration eines Wireless-Pollers, der das Management von Access-Points und den damit verbundenen Clients erleichtert. Wireless- neben verdrahteten Geräten: so wird das Netzwerk-Monitoring zu einer noch runderen Sache.

Eine Standardinstallation von Orion-NPM auf einer Maschine ist durchaus in der Lage, mehr als 2000 Elemente zu überwachen, sofern die Hardware entsprechend ausgelegt ist. Ein Element kann dabei ein Knoten, eine Schnittstelle oder ein Volume sein. Für die erfolgreiche Überwachung von mehr als 8000 Elementen sind dem Netzwerk jedoch möglicherweise zusätzliche Polling-Engines hinzuzufügen. Ebenso ist es möglich und je nach Netzwerkgröße mitunter erforderlich, zusätzliche Web-Server zu installieren oder beim verteilten Monitoring mehrfache Instanzen von Orion-NPM über die optionale Enterprise-Operations-Console unter einer Schnittstelle zu verwalten.

ManageEngine OpManager 8 (Build 8812)

Op-Manager überraschte uns positiv. Ursprünglich wollten wir diese Monitoring-Software gar nicht mit einbeziehen in diesen Vergleichstest, weil wir bei einem ähnlichen Test im vergangenen Jahr sehr viele Probleme damit hatten und uns kaum vorstellen konnten, dass es diesmal anders aussehen könnte. Manage-Engine hat es jedoch geschafft, ihr Flaggschiff-Produkt in relativ kurzer Zeit enorm zu verbessern. Das Setup, welches uns zuvor nur schwer gelingen wollte, klappte diesmal auf Anhieb, sogar auf einem Windows-7-Computer. Wir wählten zunächst eine Standardinstallation mit der mitgelieferten MySQL-Datenbanksoftware, die glatt über die Bühne ging. Eine spätere Installation auf einer Windows-Server-Maschine mit darauf laufendem Micrsoft-SQL-Server-2008 funktionierte ebenfalls reibungslos.

Die Installation geht schnell und erfordert nur wenig Benutzerinteraktion. Am Ende steht die Anzeige der Readme-Datei, die eine gute Einführung in das System bietet und versucht, dem Benutzer einige optionale Add-ons zu verkaufen. Außerdem starten auf Wunsch gleich die Op-Manager-Services und die Webkonsole. Darin geht es direkt mit der Netzwerk-Discovery, die hier Erkennung heißt, weiter. Dafür muss der Administrator ein paar Eingaben tätigen, darunter Standard-Anmeldeinformationen für SNMP (SNMP-1, -2 und -3) und Windows-Geräte, die zu prüfenden Dienste beziehungsweise Ports sowie die zu durchsuchende IP-Address-Range. Statt einer IP-Range kann die Erkennung auch importierte Daten oder CIDR nutzen. Die Erkennung erledigt das Programm sehr zügig und präsentiert abschließend die gefundenen Geräte in einer Baumstruktur. Die Netzwerk-Discovery funktionierte diesmal nahezu reibungslos. Mit Ausnahme eines Linux-Systems erkannte das Programm alle Gerätetypen und Betriebssysteme einwandfrei, allerdings klassifiziert es Windows-7-Computer noch immer grundsätzlich als Server – andere Programme sind hier genauer. Mit einem Klick importiert der Administrator die Geräte schließlich in die Datenbank, womit sie anschließend sofort in den unterschiedlichsten Ansichten der Webkonsole zur Verfügung stehen. Zunächst präsentiert die Webkonsole aber die Seite „Einleitung", die kurz und bündig per Text und/oder Video durch die ersten Schritte für die Verwaltung des Netzwerks führt. Dabei wird erklärt, wie die (nun ja bereits einmal durchgeführte) Erkennung funktioniert, was es mit Dashboards auf sich hat, wie Geräteabhängigkeiten konfiguriert und Basiswerte für Monitore, Gerätetypen und Schnittstellen etc. eingestellt werden.

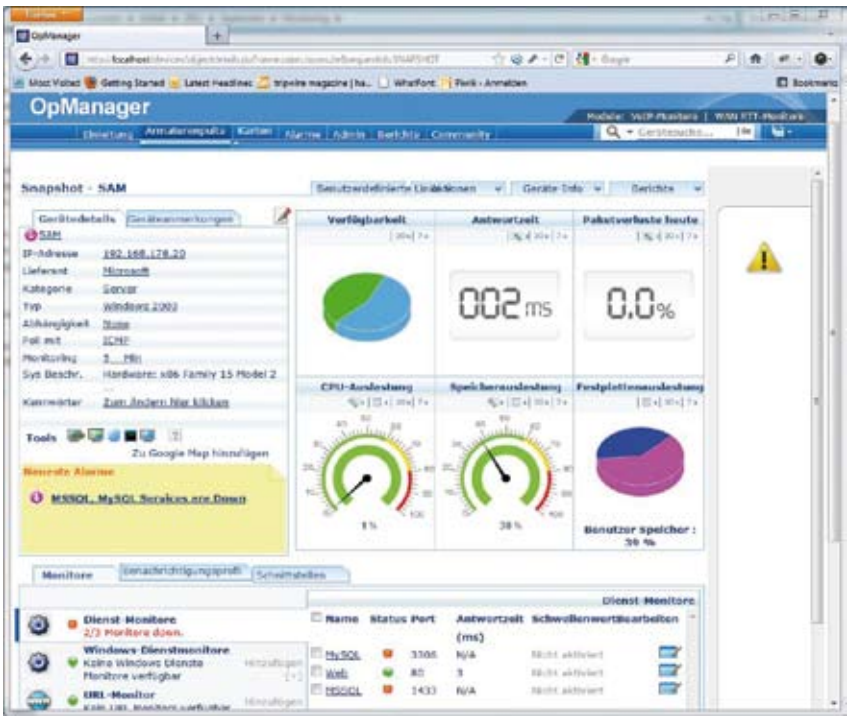


Bild: Manage Engine

Der Geräte-Snapshot in der Op-Manager-Konsole stellt die wichtigsten Performanceinformationen als bunte Grafiken dar. So etwas bevorzugen nicht unbedingt alle Administratoren, aber übersichtlich ist es allemal.

Die Webkonsole von Op-Manager sieht klasse aus, reagiert zügig und es lässt sich darin einfach navigieren. Diesmal gab sie auch untere Windows-7 kaum einen Anlass zur Klage – Kompatibilitätsprobleme gibt es nicht mehr. Gut funktionieren tun nun auch andere Browser als der Internet-Explorer, beispielsweise Firefox und Chrome. Obwohl … in Firefox überlagern sich in der Geräte-Snapshot-Seite teilweise die Beschriftungen der Registerkarten – störend, aber nicht wirklich ein Problem. Prima sind die vielen grafischen Darstellungen und die automatisch erzeugten Layer-2- und Layer-3-Maps. In den Dashboards beziehungsweise Geräteansichten zeigt die Konsole direkt die Verfügbarkeit der Geräte und Dienste, Antwortzeiten, Paketverluste, CPU-, Speicher- und Festplattenauslastungen. Probleme, beispielsweise Schwellenwertüberschreitungen oder ausgefallene oder angehaltene Dienste, stellt das Programm deutlich dar. Natürlich lassen sich auch Benachrichtigungen einstellen, so dass Administratoren bei Abweichungen von der Norm sofort alarmiert werden, beispielsweise via E-Mail, SMS oder gar Twitter. Das Produkt ist insgesamt sehr leistungsfähig und in der Lage, Netzwerke, Netzwerkgeräte und Services zu überwachen, Performance-Engpässe aufzuspüren, Administratoren zu alarmieren und Berichte zu generieren, aber um das Potenzial von Op-Manager voll auszuschöpfen, sind viele Einstellungen manuell vorzunehmen, da es beispielsweise für Schwellenwerte keine Voreinstellungen gibt. Allerdings ist es nicht weiter schwer, die diversen Dienst-, Windows-Dienst-, URL-, Performance-, Prozess-, Datei- und Ordnermonitore entsprechend zu konfigurieren. Eine Sache dabei ist jedoch ziemlich blöd: die Webkonsole als solche, die Feldbezeichnungen darin, sonstige Beschriftungen und so weiter, sind in einwandfreiem Deutsch gehalten, die Hilfe dazu aber in Englisch. Das gibt mitunter Rätsel auf. Was zum Kuckuck ist bei der Schwellenwertkonfiguration der „Nachrüstwert"?

Bild: Manage-Engine

Videos und spezielle Textinformationen erleichtern den Einstieg in Op-Manager.

Manage-Engine bietet Op-Manager nach wie vor in unterschiedlichen Editions an, dazu noch einige Add-ons und Plug-ins. So gibt es beispielsweise einen Vmware-Monitor, Cisco-IPSLA-Monitor, Exchange- und MS-SQL-Monitor, WAN- und Active-Directory-Monitor oder ein Netflow-Analyzer-Plugin und selbst die SMS-Benachrichtigung über Moden nur als spezielle Add-ons oder Plugins. Damit ist es nicht einfach, einen endgültigen Preis für das Produkt zu berechnen. Lobenswert, dass es wie bei PRTG kostenlos los geht. Die kostenlose Version überwacht aber nur maximal zehn Knoten und ist damit wohl nur für kurze Produkttests geeignet. Bereits für 50 zu überwachende Geräte kostet die Professional-Edition, gewissermaßen das Grundpaket, 995 Dollar, für 500 Geräte 5.995 Dollar. Ein optionaler Vmware-Monitor für bis zu zehn virtuelle Hosts schlägt mit 1.495 Dollar zu Buche, ein Exchange-Monitor mit 995 Dollar. Dies waren nur einige wenige Preisbeispiele, die aber gut zeigen, wie teuer eine Komplettlösung werden kann.

Fazit

PRTG-Network-Monitor bleibt Spitzenreiter, diesmal aber nur sehr knapp vor Op-Manager. Trotz identischer A-Note (5 Zähler) gibt es „nur" eine Empfehlung für Op-Manager, weil dieses Produkt, auf das reine Monitoring bezogen, PRTG nicht ganz ebenbürtig ist, dafür aber sehr schnell deutlich teurer werden kann. In diesem Test ging es darum, Monitoring-Produkte auf ihre Einsatzfähigkeit in KMU-Umgebungen zu beurteilen, und zu den KMUs zählen ja auch die kleinen Unternehmen, die kaum über größere IT-Stäbe verfügen. Hier fügt sich Orion-NPM als Produkte der Enterprise-Klasse nicht so geschmeidig ein wie PRTG und Op-Manager. Erfahrenen Administratoren, die sich nicht vor großen, komplexen Produkten scheuen, möchten wir aber durchaus empfehlen, sich Orion-NPM anzuschauen, wenn ihr Budget dies zulässt. PRTG und Orion-NPM kommen mit einer Vielzahl Sensoren, die eine riesige Palette von Systemzuständen, Eigenschaften, Performancewerten und andere Parameter überwachen. Außerdem nutzen sie ausgiebig von SNMP und WMI zur Verfügung gestellte Informationen. Beide Produkte sind leicht bedienbar. Dies gilt auch für Op-Manager, während wir uns bei Whatsup-Gold schon etwas häufiger in der Konsole nach bestimmten Funktionen oder Informationen suchend fanden. Für Orion-NPM und Whatsup-Gold sollten Administratoren grundsätzlich etwas mehr Einarbeitungszeit einplanen, als für die beiden anderen Produkte. Whatsup-Gold-Premium landete hinter PRTG und Op-Manager, weil es teurer ist, sich dabei auch noch auf ein einzelnes Netzwerk beschränkt und insgesamt mehr Einarbeitung verlangt. Hinter Orion-NPM fiel Whatsup-Gold zurück, weil Orion-NPM mit den letzten zwei Versionssprüngen deutlich zugelegt hat und es uns viel leichter viel, uns in den Konsolen von Orion zurechtzufinden. *(RL)*

Dirk Jarzyna
Redaktion funkschau

Steckbrief

OpManager 8 (Build 8812)

Hersteller: Manage-Engine
Charakteristik: Netzwerk-Monitoring-Software
Preis: (Professional-Edition): 995 Dollar (50 Geräte), 3.495 Dollar (250 Geräte), 9.995 Dollar (1000 Geräte). Preise ohne optionale Add-ons und Plug-ins.

Web: www.manageengine.com

Plusminus:

+ Sehr gute Benutzerschnittstelle
+ Schnelles, einfaches Setup
– Wird sehr teuer, wenn einige der Optionen erforderlich sind

funkschau Empfehlung