Noud van Kruysbergen, Tim Smeets

Professionele netwerkmonitoring

Software voor het bewaken van grote netwerken

Als je pc niet meer op internet wil of je NAS niet meer bereikbaar is, kom je daar met de gangbare tools nog wel uit. Maar als het netwerk dat je beheert opeens grote activiteit vertoont – of juist niet – is het niet meteen duidelijk waar dat aan ligt. Dan heb je meer nodig dan de standaard netwerktools.

Als je in je thuisnetwerk tegen een probleem aanloopt, is het vaak een kwestie van logisch nadenken en elementaire deductie om de fout te vinden. Bij een wat groter netwerk kan dat even wat tijd vergen, maar met standaardtools als ping, tracert en netsh moet je een heel eind kunnen komen.

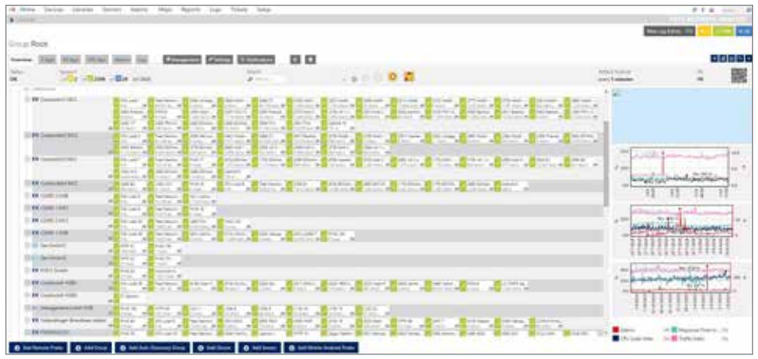
Ook programma's als Portscan, Netscan en Nmap (al dan niet met Zenmap) kunnen daar bij helpen. Dat zijn echter programma's die je alleen gebruikt als er al iets fout loopt in je netwerk. Bij het bewaken van een netwerk wil je echter continu op de hoogte gehouden worden van de status ervan. Dat betekent dat je een monitoringsysteem moet hebben die zelf regelmatig het netwerk scant om te kijken of alles werkt. In een eerder artikel hebben we laten zien hoe je met een Raspberry Pi met Nagios de servers in je netwerk kunt monitoren.

Voor een groter of complexer bedrijfsnetwerk heb je een meer structurele oplossing nodig. Je wilt dan niet alleen de netwerkeigenschappen van de apparaten in het netwerk in de gaten houden, maar ook de verbindingen, koppelingen, actieve gebruikers, het licentiegebruik, de temperatuur in de serverruimte, de belasting van het netwerk en meer van dat soort dingen. Daarbij moet het ook mogelijk zijn om externe verbindingen te kunnen monitoren.

Van de software PRTG Network Monitor van Paessler is een beperkte gratis versie te downloaden die voor een klein netwerk meer dan voldoende zal zijn. Daarmee kun je een goede indruk krijgen van de mogelijkheden van dit pakket. Via de website van Paessler (zie de link onderaan dit artikel) krijg je een license-key. Je kunt ook de onbeperkte versie installeren en die dertig dagen uitproberen.

Sensoren

De bouwstenen van de PRTG Network Monitor zijn sensoren. Iedere sensor heeft één specifieke taak, bijvoorbeeld het monitoren van de SSL-beveiliging van een netwerkapparaat, de vrije schijfruimte op een computer, de snelheid van een netwerkadapter, de bereikbaarheid van een netwerkapparaat, het online zijn van een website, de beschikbaarheid van clouddiensten als Gmail, Dropbox en dergelijke, de SNMP-status en nog veel meer. Omdat een enkel apparaat (computer, switch, router) of dienst (internetverbinding, webserver) meerdere te monitoren eigenschappen kan hebben, moet je in de praktijk rekenen op zo'n tien sensoren per apparaat.



bron: MCC

Met de PRTG Network Monitor heb je in een oogopslag inzicht in alle functies van de netwerkapparaten. Dit complexe netwerk werkt met maar liefst 2400 sensoren.

De resultaten van al die sensoren moeten ergens centraal verzameld worden. Daar zorgt de PRTG Core Server voor. Als je het pakket installeert, wordt die Core Server op je pc geïnstalleerd en is de interface ervan beschikbaar met de browser via https://127.0.0.1 of https://localhost.

Je hoeft niet alle sensoren zelf te definiëren of via de webinterface aan te maken. De Configuration Guru haalt je dat werk uit handen. De Guru vraagt om de administratorgegevens, de Windows-aanmeldgegevens (al dan niet via Active Directory) en allerlei andere mogelijke inloggegevens. Je kunt aangeven welke websites je gemonitord wilt hebben, welke clouddiensten en welk netwerksegment je in de gaten wilt houden. De Guru gaat dan zelf de benodigde sensoren installeren.

Overzicht

Het aantal sensoren kan al vrij snel uit de hand lopen. De freeware-versie kan honderd sensoren aan, dus dat moet genoeg zijn voor een tiental apparaten. Bij een complex netwerk kan dat aantal echter al snel uitgroeien tot enkele duizenden. In het screenshot hieronder is te zien hoe dat eruit kan komen te zien.

Op deze afbeelding zie je een overzicht van de switches die gebruikt worden bij het Melden Coördinatiecentrum Zuid-Limburg. In het MCC zijn de functionaliteiten van de meldkamers politie, brandweer en ambulancezorg, het servicecenter, het Regionaal Beleidsteam en het Regionaal Operationeel Team onder één dak verzameld. Dat zorgt voor een optimale en integrale afstemming van alle processen rondom melding en alarmering, opschaling en afschaling, leiding en coördinatie en informatiemanagement. Het moge duidelijk zijn dat dit tot een nogal complex netwerk heeft geleid, waar op deze manier toch het overzicht over kan worden gehouden.

Naast het globale overzicht is het mogelijk te kijken naar een specifieke sensor. In de afbeelding linksboven op de volgende pagina is bijvoorbeeld tot in detail te zien wat het live netwerkverkeer van een bepaalde netwerkinterface is. Niet alleen de totale snelheid is te monitoren, maar ook waar het momentane verkeer uit bestaat.

Op de IT-afdeling van het MCC werken vijf beheerders, een servicemedewerker en een afdelingshoofd. Met de PRTG Network Monitor kunnen zij alle verbindingen naar bijvoorbeeld de voertuigen op straat in de gaten houden. Door aan sensoren triggers toe te voegen, krijgen zij meteen een melding in de vorm van een e-mail of pushnotificatie, zodat er direct ingegrepen kan worden. Daardoor hoeven zij niet zelf op allerlei schermen in de gaten te houden of alles nog goed gaat.

Groeperen

Al die sensoren bij elkaar kunnen tot een enorme waslijst aan gegevens leiden die niet eenvoudig te analyseren is. Gelukkig kun je de sensoren bij de PRTG Network Monitor

bron: MCC

Ook de resultaten van een enkele sensor zijn te bekijken. Hier het uitgesplitste dataverkeer van een enkele netwerkadapter.

bron: MCC

Door een groep aan te maken kun je gericht kijken naar een bepaald type apparaten. Dit is het overzicht van de aanwezige thin-clients.

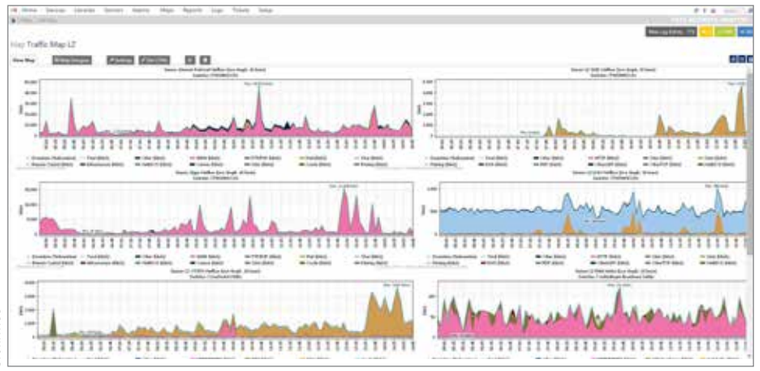
structureren in groepen. De snelste manier om dat te doen is met 'Devices / Add Auto-Discover Group'. Klik op 'Local probe' (waarover later meer), geef de groep een naam en zet 'Server Management' op 'Automatic sensor creation using device template(s)'. Dan verschijnen een aantal templates waaruit je bijvoorbeeld 'FTP Server', 'HTTP Web Server', 'NAS Synology' en/of 'Windows (via WMI)' kunt selecteren – om er maar een paar te noemen. Laat het 'Discover Schedule' op 'Once' staan als er in de nabije toekomst geen apparaten bij gaan komen.

Bij 'IPv4 Base' moet je een netwerksegment opgeven, bijvoorbeeld 192.168.0. Laat de rest even voor wat het is en klik op 'Continue'. Er wordt dan een nieuwe groep aangemaakt met daarin alleen de apparaten of services die je geselecteerd hebt. De afbeelding van de thin-clients van het MCC rechtsboven op deze pagina is op die manier tot stand gekomen.

Toevoegen

Je kunt ook afzonderlijke apparaten aan een groep toevoegen. Behalve het IP-adres moet je dan ook de inloggegevens invoeren. Die gegevens kun je laten overerven van de groep, maar ook apart instellen. Aan een apparaat kun je ook specifieke sensoren koppelen voor bijvoorbeeld de beschikbaarheid, de netwerkbandbreedte en het cpu-gebruik. Op die manier kun je alle gegevens die je in het netwerk in de gaten wilt houden aan de interface toevoegen.

Voor de computer waar de PRTG Core Server op geïnstalleerd staat kan het een aardige klus worden al die sensoren bij te houden. Je kunt het werk van de Core Server dan ook verdelen over meerdere computers door een 'probe' toe te voegen. Paessler adviseert om het aantal sensoren op een probe onder de 120 te houden. Je kunt een andere lokale probe toevoegen, maar ook een remote probe of een cluster probe. Maak verbinding met de AJAX-webinterface van de Core Server en installeer de probe. Op een probe-systeem kun je de PRTG Administration Tool openen voor het beheer van de probe, maar de eindverantwoordelijkheid blijft bij de computer met de Core Server.



bron: MCC

Je kunt de gegevens van meerdere sensoren combineren tot een map waarop je globaal in de gaten kunt houden wat er gebeurt.

Naast een netwerk met een aantal probes met ieder hun eigen groepen en sensoren en een centrale server met zijn webinterface kun je ook meerdere netwerken hebben met ieder hun eigen Core Server en monitoringinstellingen. Om dan niet met een aantal afzonderlijke webinterfaces te hoeven werken is er de PRTG Enterprise Console die in een Windows-applicatie de gegevens van alle Core Servers laat zien. Op die manier kun je het te monitoren netwerk groter en complexer maken zonder dat je daarbij het overzicht verliest.

Conclusie

De PRTG Network Monitor is een uitstekende tool om de activiteiten op je netwerk in de gaten te houden. Dat kan van een lokaal kleinschalig netwerk (waar je aan de freeware-versie waarschijnlijk genoeg hebt) tot aan combinaties van grote en complexe bedrijfsnetwerken. Voor de Unlimited-versie betaal je 10.000 euro (exclusief BTW) – dat lijkt een heel bedrag, maar is altijd nog ruim minder dan een halve systeembeheerder. Als je het achterliggende concept van sensoren, triggers, groepen en probes eenmaal door hebt, kun je zo aan de slag. Zo niet, dan wordt alles in de drieduizend (!) pagina's tellende PDF-handleiding uitgebreid uit de doeken gedaan. (nkr)

www.ct.nl/softlink/1510030

PRTG Network Monitor

Netwerkmonitoringsoftware	
Producent	Paessler, www.paessler.com
Systeemeisen	Windows vanaf 7/Server 2008 R2, dualcore, 3 GB RAM, 250 GB HDD
Prijs (exclusief BTW)	tot 100 sensoren: gratis tot 500: € 1.200 tot 1000: € 2.700 tot 2500: € 4.150 tot 5000: € 7.000 Unlimited: € 10.000