Professionele Bachelor Toegepaste Informatica

End-to-end monitoring

Michiel Bijnens

Promotoren:

De heer Toon Peeters — 3-it bvba
De heer Bram Heyns — Hogeschool PXL Hasselt

Bachelorpaper Academiejaar 2018-2019

Professionele Bachelor Toegepaste Informatica

End-to-end monitoring

Michiel Bijnens

Promotoren:

De heer Toon Peeters — 3-it bvba
De heer Bram Heyns — Hogeschool PXL Hasselt

Bachelorpaper Academiejaar 2018-2019

Dankwoord

In dit dankwoord wil ik graag iedereen bedanken die een bijdrage heeft geleverd aan dit eindwerk.

Eerst en vooral zou ik graag 3-it willen bedanken omdat ze me de kans hebben gegeven om deze leerrijke stage te doen. Verder wil ik ook alle begeleiders binnen 3-it bedanken die me geholpen hebben wanneer ik vragen had of ondersteuning nodig had. Ook wil ik de heer Toon Peeters bedanken: als mijn stagepromotor heeft hij mij goed begeleid en ondersteund. Zijn feedback was ook heel belangrijk.

Naast 3-it zou ik ook graag Van Havermaet willen bedanken voor de stageopdracht: zonder hen was de stageopdracht er niet geweest.

Ook de hogeschool PXL en mijn hogeschoolpromotor, de heer Bram Heyns, hebben een belangrijke rol gespeeld. Ik wil de hogeschool bedanken voor de kennis en voorbereiding die nodig was voor dit eindwerk. De heer Bram Heyns wil ik bedanken voor de wekelijkse feedback en de nuttige tips.

En ten slotte wil ik mijn ouders, familie en vrienden bedanken voor de steun die ze me altijd gegeven hebben.

Abstract

Monitoring-tools spelen een belangrijke rol in de hedendaagse IT-infrastructuur. Harde schijven die onvoldoende ruimte hebben of servers die zonder reden uitvallen: dat zijn incidenten die in de hedendaagse infrastructuur niet meer mogen voorkomen. Het is belangrijk om deze problemen op voorhand te kunnen signaleren. Met een monitoring-tool kan dit probleem gemakkelijk opgelost worden. Door de gegevens te analyseren ontstaat er een beeld van wat er allemaal gebeurt en waar op gelet moet worden. Naast dit alles worden er ook meldingen verzonden wanneer er problemen zijn.

Dit is heel anders in een omgeving zonder monitoring. Hier zal de systeembeheerder zelf moeten zoeken waar het misloopt. Dit kan voor onnodige frustraties zorgen.

Bovenstaand probleem is ook van toepassing bij een klant van 3-it. Momenteel gebruiken zij nog geen tool om hun omgeving te observeren. Vanuit dit probleem is de opdracht gekomen om verschillende monitoring-tools te vergelijken.

Voor dit onderzoek wordt er naar een aantal parameters gekeken om de meest geschikte tool te vinden. Deze parameters zijn: prijs, meldingen, gebruiksvriendelijkheid, en wat er gemonitord zal worden. Verder heeft de klant ook gevraagd om een tool te zoeken die op Windows draait. Om tot deze informatie te komen wordt er een literatuurstudie uitgevoerd.

De tools worden vervolgens in een tabel geplaatst waarin ze vergeleken worden op basis van de eisen van de klant. Aan de hand van deze tabel wordt er besloten welke tool het meest geschikt is voor de klant.

Na dit onderzoek wordt er een proof of concept uitgewerkt met de meest geschikte tools om de haalbaarheid aan te tonen. Hiervoor wordt er een testomgeving voorzien waarin de tools getest kunnen worden.

Inhoudsopgave

Lijst van gebruikte figuren

Lijst van gebruikte tabellen

Lijst van gebruikte afkortingen

AD	Active Directory
API	Application Programming Interface
APM	Application Performance Monitoring
AWS	Amazon Web Services
CPU	Central Processing Unit
CU	Computer Unit
GB	Gigabyte
HTTP	Hypertext Transfer Protocol
I/O	Input/Output
ICMP	Internet Control Message Protocol
IIS	Internet Information Services
IM	Instant Messaging
IP SLA	Internet Protocol Service Level Agreement
ISO	International Organization for Standardization
JMX	Java Management Extensions
JSON	JavaScript Object Notation
LLDP	Link Layer Discovery Protocol
RAM	Random-Access Memory
RDP	Remote Desktop Protocol
REST	Representational State Transfer
SaaS	Software as a Service
SCOM	System Center Operations Manager
sms	Short Message Service
SNMP	Simple Network Management Protocol
SPL	Search Processing Language
SQL	Structured Query Language
SSH	Secure Shell
TCP	Transmission Control Protocol
VoIP	Voice over IP
WMI	Windows Management Instrumentation
XML	Extensible Markup Language

Inleiding

In tijden van steeds complexer wordende infrastructuur, wordt het belang van een monitoring-tool steeds belangrijker. Steeds meer bedrijven verplaatsen hun servers en applicaties naar de Cloud of kiezen ervoor om met containers te werken. Dit zorgt ervoor dat het steeds moeilijker wordt om te zien wat er gebeurt.

Het is belangrijk dat er een overzicht gehouden wordt over de dingen die gebeuren in het netwerk. Hier kan een monitoring-tool bij helpen. Een monitoring-tool kan de gegevens van een infrastructuur of applicatie ophalen en analyseren. Er worden grafieken en tabellen gemaakt zodat de gegevens makkelijk bekeken kunnen worden.

Het is echter belangrijk dat de juiste tool gekozen wordt. Er zijn veel tools beschikbaar op de markt maar niet elke tool is altijd even goed. Hiervoor moet er dus eerst een onderzoek gedaan worden.

Welke monitoring-tool het meest geschikt is voor *end-to-end* monitoring wordt bepaald door een aantal parameters te onderzoeken, de parameters zijn: prijs, meldingen, gebruiksvriendelijkheid, en wat er gemonitord zal worden. Om tot deze informatie te komen wordt er een literatuurstudie uitgevoerd.

I. Stageverslag

1 Plan van aanpak

1.1 Bedrijfsvoorstelling

In dit hoofdstuk volgt een korte omschrijving van het stagebedrijf en de motivering voor dit bedrijf. Er wordt ook een korte beschrijving gegeven van de klant. De opdracht wordt in dit hoofdstuk ook kort besproken.

1.1.1 3-it Bvba

3-it is een ICT-bedrijf dat gespecialiseerd is in infrastructuur. Klanten kunnen bij het bedrijf terecht voor een ruim pakket aan diensten, advies en *managed services* maar ook consultancy en productoplossingen horen tot dit pakket. Het bedrijf richt zich hierdoor ook niet op een specifieke sector. Een gevolg hiervan is dat ze een grote klantenportefeuille hebben.

De focus van 3-it ligt ook op persoonlijke ontwikkeling. Ze bieden zowel interne als externe opleidingen en stages aan. Zo wordt er bijvoorbeeld lesgegeven aan verschillende hogescholen. Daarnaast zoekt 3-it voor zowel medewerkers als klanten de juiste personen voor de verschillende opdrachten.

Het bedrijf is ook gepassioneerd door nieuwe technologieën. Ze houden zich bijvoorbeeld bezig met *Virtual Reality* en *Internet of Things*.

Op 10 april 2007 is het bedrijf opgericht. Vanaf het begin ligt de focus op ICT-infrastructuur. Momenteel telt het bedrijf rond de 60 werknemers en heeft het structurele samenwerkingen met vooraanstaande organisaties in de ICT-branche.

De visie en waarden van het bedrijf zijn partnership, betrouwbaarheid, kwaliteit, duidelijkheid, inlevingsvermogen en passie. Door deze waarden te respecteren proberen zij het verschil te maken.

1.1.2 Van Havermaet

Van Havermaet is een klant van 3-it die zich bezighoudt met alles dat met vermogen te maken heeft. Het is een accountancy bureau dat financieel, juridisch, fiscaal en HR-advies geeft. Dit advies geven ze met een persoonlijke toets.

Ze doen boekhouding, btw-aangiften en zorgen dat de lonen correct betaald worden. Ook kopen en verkopen ze bedrijven en maken ze BI-rapportages.

Doordat ze over een uitgebreid netwerk beschikken hebben ze ook kennis en contacten op internationaal vlak. Hierdoor kunnen ze klanten professioneel advies geven over buitenlandse zaken. Een van hun taken is om ervoor te zorgen dat mensen die in het buitenland gaan werken het juiste loon berekend krijgen, dit geldt ook voor buitenlanders die in België komen werken.

Het bedrijf is opgericht in 1942 en telt rond de 200 werknemers. Het hoofdkantoor is gelegen in Hasselt (Limburg).

1.2 Motivering

Mijn motivering voor 3-it is hun manier van werken. Elke werknemer heeft zijn eigen kwaliteiten en iedereen is belangrijk in het team. Ze richten zich ook niet enkel op een specifieke sector. 3-it is een bedrijf dat kwaliteit wil leveren aan haar klanten door middel van goede communicatie naar de klant toe en een goede werksfeer tussen de medewerkers. Dit zijn dingen die voor mij belangrijk zijn.

De opdracht zelf was ook interessant, aangezien monitoring een belangrijke rol speelt in een IT-omgeving. Voordat ik aan dit project begon had ik nog niet veel met monitoring gewerkt. Door dit project hoop ik hier veel uit te leren en die kennis dan te kunnen toepassen in de toekomst.

1.3 Voorstelling stageopdracht

1.3.1 Aanleiding

Deze stageopdracht is tot stand gekomen omdat een klant van 3-it (Van Havermaet) een beter overzicht wil krijgen over zijn IT-infrastructuur. De klant wil een *end-to-end* monitoringoplossing om de traffic van de server en applicatie volledig te kunnen volgen. Verder wil de klant ook nog door middel van monitoring problemen kunnen opsporen nog voor ze zich voordoen.

1.3.2 Probleemstelling

De klant van 3-it is op zoek naar een volledige *end-to-end* monitoringoplossing. Met deze monitoring-tool willen zij een beter beeld krijgen van wat er allemaal gebeurt in hun infrastructuur. Als er zich problemen voordoen, wil de klant dit zo snel mogelijk kunnen opsporen. Momenteel hebben zij nog geen monitoring-tool, waardoor ze het moeilijk hebben om een overzicht te krijgen van wat er allemaal gebeurt in hun omgeving. Met de tool wil de klant kijken naar de *uptime,* bandbreedte*,* latentie en de beschikbaarheid van zowel de netwerkapparatuur als de applicaties. De klant zou ook graag SQL-servers, telefoons, Azure en Office 365 kunnen monitoren.

1.3.3 Doelstellingen

Het doel van de stage is om een onderzoek uit te voeren naar verschillende monitoring-tools. Hierbij wordt er gedocumenteerd welke parameters gemonitord worden door welke tool en hoe dit is opgesteld. Nadat het onderzoek voltooid is, wordt er een plan van aanpak uitgewerkt om een volledige *end-to-end* monitoring op te zetten wat het mogelijk maakt om het volledige verkeer te monitoren tussen de applicatie en de server.

1.3.4 Randvoorwaarden

- Beperkingen

  Binnen deze opdracht wordt er enkel gekeken naar tools die op een Windows server geïnstalleerd kunnen worden. Hierdoor zijn er een aantal tools die niet onderzocht zijn maar misschien wel evenwaardig zijn.

- Kritische succesfactoren

  Om de slaagkansen van dit project te verhogen zal er een testomgeving voorzien moeten worden. In deze testomgeving is het de bedoeling om een *proof of concept* op te bouwen.

- Afspraken
    - Met het bedrijf

      De werkuren binnen 3-it zijn gewoonlijk van 8u30 tot 17u00, inclusief een half uur pauze. Er kan ook gekozen worden om langer pauze te nemen: dit is dan één uur in plaats van een half uur, maar dan moet er gewerkt worden tot half zes.

      Binnen 3-it wordt er veel aandacht besteed aan de sfeer op de werkvloer. Elke ochtend en avond, wordt er kort iets tegen iedereen binnen het bedrijf gezegd. Verder is het ook vanzelfsprekend dat er op een respectvolle en professionele manier met elkaar omgegaan wordt.

      Op het einde van de dag wordt er verwacht dat alles netjes achtergelaten wordt. Verder is het ook belangrijk dat als er iets leeggemaakt wordt, dit ook bijgevuld wordt. De lege flessen moeten verzameld worden en mogen niet platgedrukt worden. Dit wordt gedaan omdat op de flessen nog statiegeld zit.

      Om ervoor te zorgen dat de stage goed verloopt, wordt er om de drie weken een opvolgpresentatie gegeven. Deze zal plaatsvinden op vrijdagmiddag.

    - Met de hogeschool

      Met de hogeschool is de afspraak gemaakt dat elk document tijdig geüpload wordt op Epos. In voorlopige versies van het bestand wordt er verwacht dat ik de aanpassingen in een andere kleur aanduid zodat dit makkelijk is om te verbeteren.

    - Met mezelf

      Tijdens dit project hoop ik zoveel mogelijk kennis op te doen. Als er problemen zijn, is het belangrijk deze eerst zelf proberen op te lossen. Als het probleem niet opgelost raakt, moet er tijdig hulp gezocht worden.

1.3.5 Tijdsplanning

Voor dit project is er gebruikgemaakt van Microsoft Project om een planning op te stellen voor 12 weken. Er is een Gantt chart opgesteld waarin alle deadlines zitten van de stage. In deze planning wordt er ook tijd voorzien voor de opvolgpresentaties en andere taken.

II. Onderzoekstopic

1 Onderzoeksvraag

Welke monitoring-tool is het meest geschikt voor *end-to-end* monitoring in een Windows-omgeving?

Om de onderzoeksvraag te kunnen beantwoorden is het belangrijk om eerst te kijken welke tools er allemaal beschikbaar zijn op de markt. Hiervoor is er via een literatuurstudie gekeken naar verschillende tools. Bijkomend wordt de mening gevraagd van experten bij 3-it zelf. Deze interviews verschaffen nuttige expert informatie en andere invalshoeken om de verschillende tools met elkaar te vergelijken.

Vanaf dan kan een vergelijking gemaakt worden. Alle resultaten worden in een matrix geplaatst zodat ze makkelijk te vergelijken zijn. De meest geschikte tools worden aan de klant voorgesteld en hieruit wordt er beslist welke tool uitgewerkt wordt in een testomgeving.

Bij het onderzoek naar de tools wordt er naar een aantal aspecten gekeken: wat er gemonitord wordt, de prijs, meldingen en gebruiksvriendelijkheid. Deze aspecten zullen in dit hoofdstuk kort toegelicht worden.

1.1 Wat wordt er gemonitord?

Het is belangrijk dat de juiste componenten gemonitord kunnen worden. Er wordt dus gekeken of de tools aan netwerkmonitoring kunnen doen maar ook aan applicatiemonitoring. Verder wordt er ook gekeken naar de *uptime,* bandbreedte*,* latentie en de beschikbaarheid van zowel de netwerkapparatuur als de applicaties. Hierbij moet er rekening gehouden worden met Azure, *Structured Query Language* (SQL) servers, VoIP en Office 365.

Bijkomend is het ook belangrijk dat er gemonitord kan worden zonder internetverbinding.

1.2 Prijs

De prijs kan een belangrijke rol spelen bij het vergelijken van de verschillende tools. Als een tool evenwaardig is met een andere tool maar de prijs is lager, dan kan de tool met de laagste prijs de voorkeur krijgen.

1.3 Meldingen

Bij het onderzoeken van monitoring-tools is het belangrijk dat er gekeken wordt naar hoe de meldingen bij de gebruiker komen. Kan de gebruiker zelf kiezen welke tool hij gebruikt voor de verschillende meldingen? Verder is het ook belangrijk dat de meldingen snel bij de gebruiker komen. In dit proces is het gewenst dat er zo weinig mogelijk nutteloze meldingen komen.

1.4 Gebruiksvriendelijkheid

Een gebruiksvriendelijke tool is aangenaam voor de eindgebruiker. Hiervoor wordt er een onderzoek gedaan naar een aantal criteria:

- Is er duidelijke documentatie?
- Is er een steile leercurve?
- Is er voldoende support?

1.5 Voor- en nadelen

Het kan ook een meerwaarde zijn om te weten wat andere mensen van deze tool vinden. Hiervoor wordt er gekeken naar reviews van mensen die de verschillende tools gebruikt hebben.

2 Onderzoek

In dit hoofdstuk wordt er kort toegelicht wat monitoring is en waarom dit best gebruikt kan worden. Verder worden de verschillende tools die onderzocht worden kort toegelicht.

2.1 Wat is monitoring?

Monitoring is het proces waarbij een aantal onderdelen nauw worden opgevolgd om de prestaties en de beschikbaarheid weer te geven. Als een service niet meer werkt zoals het zou moeten, zal er een alarm afgaan waardoor er snel gezien kan worden dat de service aandacht nodig heeft.

2.2 Waarom monitoring?

Door gebruik te maken van monitoring kan de gezondheid van een infrastructuur gemakkelijk en efficiënt nagegaan worden. Er worden alerts gestuurd als er iets misloopt, waardoor er niet gezocht moet worden waar de fout zich voordoet. Met monitoring kan er ook op voorhand actie ondernomen worden om systemen die waarschuwingen geven op tijd de nodige aandacht te geven zodat deze niet *down* gaan. Verder is het ook interessant om te weten wat er allemaal gebeurt in de omgeving en een beter overzicht te krijgen van het netwerk.

Dit kan ook kostenbesparend werken. Door de gegevens te analyseren kunnen servers efficiënter gebruikt worden.

2.3 Markt verkennen

Voordat er tools met elkaar vergeleken kunnen worden, moet er eerst geweten zijn welke tools er beschikbaar zijn op de markt. Hiervoor wordt er opzoekingswerk gedaan op het internet. Tabel 1 toont de verschillende tools met hun fabrikant die onderzocht worden in dit document. Deze tools kunnen zowel aan applicatiemonitoring als aan netwerkmonitoring doen. Tijdens het onderzoek zijn er ook andere tools bekeken, maar deze zijn niet verder onderzocht omdat ze ofwel geen applicaties ofwel geen netwerken kunnen monitoren.

Tabel 1: lijst met monitoring-tools

Systeem	Fabrikant
Datadog	Datadog, Inc.
eG Enterprise	eG Innovations
Elastic stack	elastic
Grafana	Grafana Labs
SCOM	Microsoft
netXMS	netXMS
New Relic	New Relic, Inc.
PRTG	Paessler AG
Splunk	Splunk Inc.
WhatsUp Gold	ipswitch

2.4 Beschrijving

2.4.1 Datadog

Figuur 1: Logo Datadog

Datadog is een *software-as-a-service* (SaaS)-pakket dat gebruikmaakt van *agents* die op verschillende platformen geïnstalleerd kunnen worden.

Met Datadog kan de volledige infrastructuur in beeld gebracht worden. Cloud, servers, apps, services, statistieken en meer. Het wordt gemakkelijk weergegeven in grafieken om de data te analyseren en als er zich fouten voordoen, worden er meldingen verzonden.

De load, de connectie, het verkeer en het geheugengebruik zijn een klein deel van wat er allemaal gemonitord kan worden. Datadog biedt ondersteuning voor een groot aantal besturingssystemen en applicaties; als er een specifieke applicatie is die niet ondersteund wordt, kan een nieuwe integratie toegevoegd worden.

Naast de vooraf geconfigureerde instrumentenpanelen kunnen er altijd nieuwe aangepaste panelen gemaakt worden, om precies weer te geven wat er gezien moet worden. Dit wordt het ‘Timeboard’ genoemd.

Als er op een hoger niveau gemonitord moet worden, dan kan er gebruikgemaakt worden van een ‘Screenboard’. Dit wordt gebruikt om de status van een service of een volledige infrastructuur te monitoren. Als er iets zorgwekkend is, kan er overgeschakeld worden naar het ‘Timeboard’ om alles in detail te bekijken.

Van de grafieken kunnen momentopnames genomen worden en vervolgens gedeeld worden met aangepaste tekst. Dit kan geïntegreerd worden met andere communicatie en monitoring-tools.

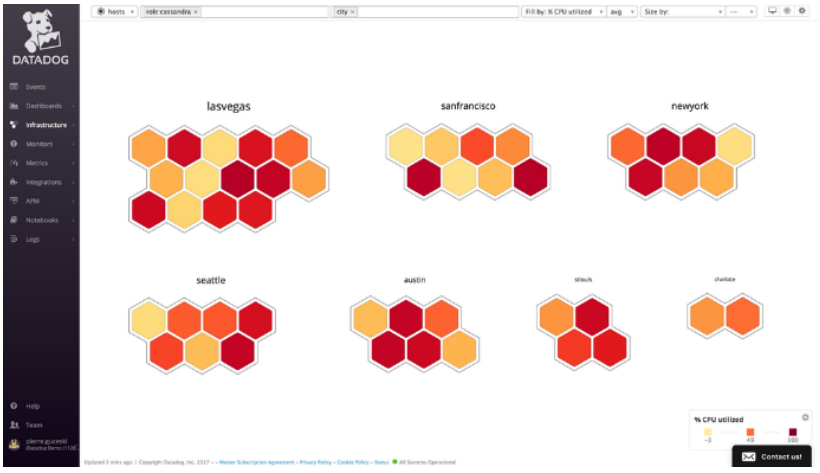
[1]

2.4.1.1 Wat wordt er gemonitord?

In de infrastructuurlijst wordt weergegeven welke toestellen er allemaal gemonitord worden. In deze lijst worden de tags van elke host weergegeven waardoor er gefilterd kan worden. Een host die langer dan 24 uur geen gegevens meer heeft verzonden wordt automatisch verwijderd uit de lijst.

Datadog stopt toestellen automatisch binnen een bepaalde categorie. Hierdoor moet de systeembeheerder minder configureren.

De *hostmap* maakt het mogelijk om meerdere toestellen op één scherm te visualiseren. De toestellen worden hier voorgesteld door middel van figuren. Door gebruik te maken van kleuren wordt de gezondheid van het toestel weergegeven. Deze kaart maakt het mogelijk om alle *hosts* weer te geven ongeacht het aantal. Dit kunnen er 500 zijn, maar het kunnen er ook 50 000 zijn. In Figuur 2 wordt dit geïllustreerd



Figuur 2: Hostmap

Datadog heeft ook een groot aantal integraties. Een aantal van deze integraties zijn: Microsoft *Active Directory* (AD), Azure, Microsoft Azure DB *for* MySQL en Windows Management Instrumentation.

Op het vlak van applicatiemonitoring worden volgende talen ondersteund: Java, Python, Ruby, Go, Node.js, .NET, PHP en C++. Met *Application performance monitoring* (APM) van Datadog kan er gezien worden welke gebruiker wat gedaan heeft of hoe snel de applicatie reageert.

[1]

2.4.1.2 Prijs

Datadog is beschikbaar in verschillende versies: er is een gratis, een Pro- en een Enterprise-versie. De prijs van de Pro- en de Enterprise-versie worden berekend op het aantal *hosts*. De standaardprijs van de Pro-versie is: $15 per *host*, per maand. Deze prijs wordt berekend op jaarlijkse basis ($18 maandelijkse basis). De prijs van de Enterprise-versie is: $23 per *host*, per maand. Ook hier wordt de prijs op jaarlijkse basis berekend ($27 maandelijkse basis).

Bij een hoeveelheid van meer dan 500 *hosts* is er een korting mogelijk.

Bovenstaande prijzen zijn enkel voor het monitoren van de infrastructuur. Het is ook mogelijk om een APM-pakket te kopen. Hier zijn twee mogelijkheden: het 'APM and Distributed Tracing' -pakket en het 'Trace Search & Analytics (*add-on*)'-pakket.

Verder moet er ook betaald worden voor logmanagement. Er zijn drie mogelijkheden: de prijzen zijn $1,27, $1,70 en $2,50. Deze prijzen zijn maandelijks (jaarlijks gefactureerd) en worden berekend per miljoen logboekevents.

En ten slotte kan er ook nog het 'API Tests'-pakket gekocht worden. Dit heeft een prijs van $5 per miljoen testen die uitgevoerd worden, per maand.

[1]

2.4.1.3 Meldingen

Meldingen kunnen onmiddellijk verzonden worden naar Slack of Campfire. Daarnaast kunnen PagerDuty en ServiceNow automatisch problemen triggeren en oplossen. Het is ook mogelijk om met webhooks te werken of via e-mail meldingen verzenden. Hierdoor zijn er veel mogelijkheden. [1]

Op het niveau van een cluster kunnen percentages van servers ingesteld worden zodat niet elke keer een melding gestuurd wordt als er een server down gaat. Het is belangrijk dat de service beschikbaar blijft. Er worden enkel meldingen verzonden als er meer servers *down* gaan dan dat bepaalde percentage. Hierdoor worden er geen onnodige meldingen gestuurd.

Met Datadog kunnen twee soorten waarschuwingen ingesteld worden: waarschuwingen en kritieke waarschuwingen. Een voorbeeld zou zijn dat er bij een webcluster een waarschuwingsdrempel ingesteld wordt op 10% en een kritieke drempel op 20%. Als er 10% van de webservers uitvalt, zal er een waarschuwing gestuurd worden. Als 20% van de webservers uitvalt, wordt er een kritieke melding verzonden.

Aan elke monitor kan een titel gegeven worden. Dit is handig wanneer er iets misloopt: zo kan er snel begrepen worden wat er aan de hand is. Naast de titel kan er ook een korte beschrijving meegegeven worden. Hier kan zowel met *Markdown* gewerkt worden als met *in-line* variabelen en tagvariabelen. [2]

2.4.1.4 Gebruiksvriendelijkheid

Documentatie

Er is een uitgebreide documentatie op de website beschikbaar. Op de startpagina wordt de documentatie onderverdeeld in zes verschillende onderwerpen: *agent*, integratie, grafieken, meldingen, APM (tracering) en ontwikkelaarstools.

De tekst en de code worden van mekaar onderscheiden door de code in een tekstvlak te plaatsen met een donkerdere achtergrond. Verder wordt er ook gewerkt met ondersteunende afbeeldingen. Bij sommige onderwerpen wordt er zelfs gebruikgemaakt van video-ondersteuning.

Door de zoekbalk linksboven aan de pagina kan er snel iets opgezocht worden. Ook door de *TreeView* aan de linkerkant van de pagina kan er snel op een bepaald onderwerp gezocht worden. Aan de rechterkant van de pagina, is er een inhoudstabel beschikbaar van dat bepaalde onderwerp zodat er nog sneller genavigeerd kan worden door de documentatie.

Voor extra duidelijkheid wordt er soms gebruikgemaakt van ondersteunende afbeeldingen die vergroot kunnen worden door erop te klikken.

In de documentatie worden ook verwijzingen (hyperlinks) voorzien om gemakkelijk naar dat bepaalde onderwerp te navigeren. Dit wordt aangegeven door dat stuk tekst te onderlijnen. [1]

Leercurve

Bij het kijken naar beoordelingen van mensen die de tool gebruikt hebben is te zien dat er een zware leercurve is in het begin. Om correct met Datadog te werken moet er tijd vrijgemaakt worden om de verschillende concepten te begrijpen. [3], [4], [5], [6]

Support

Het support hangt af van welk pakket er gekocht wordt. Het Pro-pakket bevat technisch support via chat en e-mail. Het Enterprise-pakket bevat deze twee ook maar heeft daarbovenop ook nog support via telefoon.

Datadog kan gecontacteerd worden via e-mail, live chat en *in-app event stream* berichten. Het e-mailadres is support@datadoghq.com. Voor de live chat kan er gebruikgemaakt worden van de in-app chat of er kan een gesprek gestart worden via Slack. Het team is beschikbaar van 10:00 tot 19:00 tijdens de weekdagen. [7]

2.4.1.5 Voor- en nadelen

Om erachter te komen wat de voor- en nadelen zijn van Datadog, wordt er gekeken naar een aantal beoordelingen van mensen die de tool gebruiken of gebruikt hebben. Datadog krijgt gemiddeld een vier op vijf. [3], [4], [5], [6]

Voordelen

De documentatie en support kunnen helpen bij het gebruik van de tool.

Ook het uitgebreide aantal plug-ins is iets wat vaak terugkomt bij de beoordelingen. Hierdoor zijn er veel mogelijkheden.

Met de *hostmap* kan er snel een overzichtelijk beeld gevormd worden over de gezondheid van de server ongeacht het aantal servers. [3], [4], [5], [6]

Nadelen

Bij het lezen van de beoordelingen wordt er vaak gesproken over een zware leercurve.

De tool is ook enkel beschikbaar als SaaS: dit wil dus zeggen dat er niks gemonitord kan worden als er geen toegang is tot het online-platform. [3], [4] [5], [6]

Om Office 365 te monitoren moet er gebruikgemaakt worden van externe software zoals ‘zapier’ dit kan voor extra kosten zorgen. [8]

2.4.2 eG Enterprise

Figuur 3: Logo eG Enterprise

eG Enterprise is een webgebaseerde monitoringoplossing die zowel beschikbaar is als SaaS als in *on-premises*.

Veel grote bedrijven maken gebruik van de service van eG Enterprise, een aantal van deze bedrijven zijn: Samsung, ebay, BNP Paribas en het Groene Hart Ziekenhuis.

De tool biedt een snel, eenvoudig en volledig overzicht over een IT-Infrastructuur. Naast het overzicht leveren ze diagnoses en rapportages van de belangrijkste IT-diensten.

Er wordt gewerkt met een combinatie van *agent*- en *agentless*-benadering om de gegevens op te halen.

Door gebruik te maken van de *Universal Agent* moet er niet gewerkt worden met verschillende licenties voor het *deployen* van de agent op de verschillende besturingssystemen of applicaties.

Standaard worden meer dan 180 applicaties, 10 virtualisatieplatformen en 10 besturingssystemen ondersteund.

Verder kan er gebruikgemaakt worden van *machine learning.* Zo kunnen fouten sneller opgespoord worden. Door oude data te analyseren kunnen afwijkingen sneller gevonden worden.

[9]

2.4.2.1 Wat wordt er gemonitord?

Wat er gemonitord wordt is voor een deel afhankelijk van het soort abonnement dat er gekozen wordt. Zo is er bijvoorbeeld een beperking op het aantal servers die gemonitord kunnen worden of *high availability*.

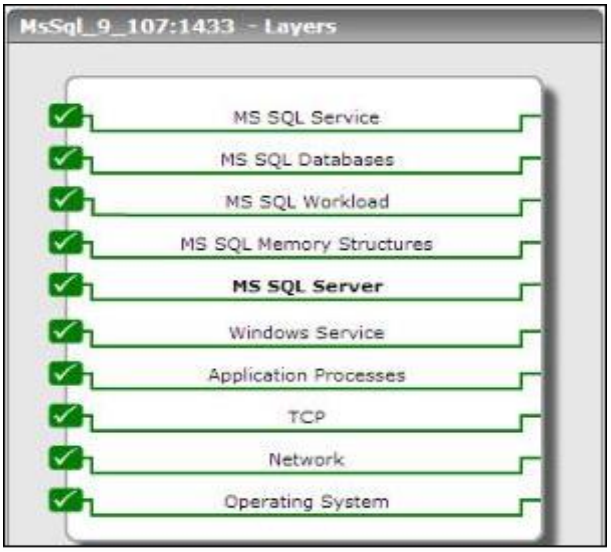
Elke applicatie, server of apparaat kan gemonitord worden doordat eG Enterprise een uitgebreide ondersteuning heeft aan technologieën.

Ze ondersteunen Microsoft Azure en Amazon Web Services (AWS) als Cloudplatform. De ondersteunende virtualisatieplatformen zijn VMware vSphere, Microsoft Hyper-V, Citrix XenServer, Nutanix Acropolis en meer.

In het *uptime* dashboard van een toestel kan er informatie gevonden worden over hoelang het toestel al actief is geweest sinds de laatste keer dat het toestel is opgestart. In dit dashboard wordt er ook een overzicht gegeven over de beschikbaarheid van het systeem in de afgelopen 24 uur. Er wordt getoond hoelang het toestel actief is geweest, het percentage *uptime*, hoelang het toestel niet actief was, het percentage dat het niet actief was en het aantal keer dat het toestel opnieuw opgestart is. Dit wordt verduidelijkt door gebruik te maken van grafieken.

Met eG Enterprise APM kunnen applicaties gemonitord worden. eG Enterprise biedt ondersteuning voor meer dan 180 toepassingen: Java, .NET, Citrix, SAP, PeopleSoft, SharePoint, Microsoft Dynamics, Exchange en Oracle zijn hier voorbeelden van.

De ingebouwde Microsoft SQL-monitor zorgt ervoor dat diepgaande analyses gedaan kunnen worden van Microsoft SQL-servers. Elke laag die in Figuur 4 wordt weergegeven, kan een groot aantal aan meetgegevens tonen. Een uitgebreid overzicht van wat er in de verschillende lagen bekeken wordt is opgenomen in Bijlage A. [10]



Figuur 4: Laagmodel Microsoft SQL-server

2.4.2.2 Prijs

Er zijn verschillende abonnementen om uit te kiezen. De volgende abonnementen zijn beschikbaar: 'Easy Evaluation', 'Perpetual License', 'Subscription', 'SaaS' en 'Audit Service'.

De 'Easy Evaluation' is de goedkoopste versie, deze is namelijk gratis. De andere pakketten zijn afhankelijk van het aantal servers in de infrastructuur. De licenties worden gebaseerd op het aantal besturingssystemen, opslagapparaten of *hypervisors* dat moet worden gecontroleerd. Niet op het aantal *Central Processing Unit's* (CPU's) of kernen.

Het 'Perpetual License' en 'Subscription'-pakket hebben beide een minimumprijs, $10 000 voor de 'Perpetual License' en $300 per maand voor de 'Subscription'. Deze prijzen kunnen nog oplopen naargelang de grootte en de configuratie van de infrastructuur.

Voor Citrix, Microsoft RDS en virtuele desktopinfrastructuren kan eG Enterprise ook worden gelicentieerd voor het aantal gebruikers.

De prijs van de licenties wordt gebaseerd op het aantal servers of het aantal gebruikers en dus niet op het aantal CPU's, *cores* of applicatie componenten.

Deze pakketten bevatten alle types van monitoring, hierdoor moeten er geen extra pakketten gekocht worden. [9]

2.4.2.3 Meldingen

Met eG Enterprise kunnen meldingen ontvangen worden via *short message service* (sms) en e-mail. De gebruiker kan de meldingen zo aanpassen zodat er enkel voor een bepaald onderdeel meldingen verzonden worden. Hierdoor wordt het aantal meldingen beperkt.

Er is ook een Android applicatie beschikbaar waarmee push-meldingen gestuurd kunnen worden. Met de applicatie kan de volledige infrastructuur gemonitord worden via een mobiel toestel. [9], [10]

2.4.2.4 Gebruiksvriendelijkheid

Documentatie

Op de website van eG Enterprise kunnen volgende onderwerpen gevonden worden: Demo's, *White papers*, Webinars, *Case Studies*, video's, *Solution briefs* en *infographics.* Verder is het ook mogelijk om een live demo aan te vragen.

De documentatie is duidelijk, alles wordt stap voor stap uitgelegd en de tekst wordt ondersteund met afbeeldingen. Belangrijke tekst wordt vetgedrukt zodat dit goed opvalt.

Bij de documentatie is er een zoekbalk en een *TreeView* voorzien om snel een bepaald onderwerp te vinden. De zoekbalk is handig maar werkt niet optimaal. Er worden geen suggesties weergegeven als er in de zoekbalk getypt wordt. Verder is het ook zo dat als er een spellingsfout in de zoekbalk getypt wordt, er mogelijk geen resultaten getoond worden. Het kan ook een tijd duren om de zoekopdracht te verwerken.

[10]

Leercurve

Om de leercurve te bepalen is er online gekeken wat mensen van de tool vinden.

Hieruit blijkt dat er vaak gesproken wordt over een makkelijke leercurve. De installatie en configuratie verlopen relatief snel. [11], [12], [13]

Support

Op de website is er de mogelijkheid om te praten met iemand van eG Enterprise door middel van de live chat. Naast de live chat kan eG Enterprise gecontacteerd worden door een mail te sturen naar info@eginnovations.com of te bellen naar een van de telefoonnummers die op de website beschikbaar zijn. [9]

2.4.2.5 Voor- en nadelen

Om de voor een nadelen van eG Enterprise te bepalen is er online gekeken wat gebruikers vinden van deze tool.

Voordelen

eG Enterprise biedt veel mogelijkheden om te monitoren, zeker op het gebied van infrastructuur. Dit komt door de uitgebreide ondersteuning voor virtualisatieplatformen en applicaties.

Prestatieafwijkingen kunnen op voorhand waargenomen worden waardoor de uptime verbeterd kan worden.

Met de topologie map kan er gemakkelijk gekeken worden hoe de verschillende servers afhankelijk zijn van elkaar, met welke database ze verbonden zijn, wat soort applicatie het is en meer. Er kan ook gezien worden welke servers virtueel zijn en op welk platform ze draaien. Verder wordt er ook gebruikgemaakt van kleuren die de gezondheid van de servers of applicaties weergeven.

Ook het support wordt geapprecieerd.

[9], [11], [12], [13], [14]

Nadelen

De meeste gebruikers zijn over het algemeen zeer tevreden over de tool, de nadelen die besproken worden zijn meestal persoonlijke minpunten.

[9], [11], [12], [13], [14]

2.4.3 Elastic stack

Figuur 5: Logo Elastic stack

ELK stack is een afkorting voor drie *open source* projecten: Elasticsearch, Logstash en Kibana. Elasticsearch is een zoekmachine, logstash is een *pipeline* die gegevens verwerkt naar Elasticsearch. Kibana staat in voor het visualiseren van de gegevens, het maakt van de data grafieken en tabellen.

Door beats te installeren op elk toestel kan de informatie verzonden worden naar logstash.

De ELK stack is zowel beschikbaar als *Software as a Service* maar ook lokaal kan alles geïnstalleerd worden.

Verder kan deze tool ook gebruikmaken van *machine learning* om vroegtijdig onregelmatigheden te kunnen opsporen. [15]

2.4.3.1 Wat wordt er gemonitord?

Door gebruik te maken van 'Heartbeat' kan de *uptime* bekeken worden. Het enige dat nodig is, is een netwerktoegang tot het gewenste protocol: Hypertext transfer Protocol (HTTP), *Transmission Control Protocol* (TCP) of *Internet Control Message Protocol* (ICMP) van het eindpunt. Er wordt gekeken of het eindpunt nog beschikbaar is, vervolgens wordt alle data weergegeven in een Kibana dashboard.

Door 'Metricbeat' op alle toestellen te installeren en te verbinden met Elasticsearch kan het CPU-gebruik, het geheugengebruik, het filesysteem, disk input/output (I/O) en netwerk I/O statistieken opgevraagd worden. Dit maakt het mogelijk om bijna elk proces dat draait op het systeem te monitoren.

Met de APM-oplossing kunnen applicaties gemonitord worden. Elastic APM biedt ondersteuning voor Java, Go, Node.js, Python, Ruby en JavaScript.

[15]

2.4.3.2 Prijs

Er zijn drie SaaS-pakketten beschikbaar: 'Elasticsearch service', 'Elastic App Search Service' en 'Elastic Site Search Service'. De prijzen zijn: $16,40 voor 'Elasticsearch Service', $49 voor 'Elastic App Search Service' en $79 voor 'Elastic Site Search Service'. Dit zijn prijzen die maandelijks betaald moeten worden.

De software kan ook *On-premise* geïnstalleerd worden. Dit is volledig gratis.

[15]

2.4.3.3 Meldingen

Meldingen kunnen verzonden worden naar de ingebouwde integraties: e-mail, PagerDuty en Slack. Verder is het ook mogelijk om met webhooks te werken, voor integratie met een bestaande infrastructuur of met systemen van derden.

Via de *user interface* kunnen alerts bekeken, aangemaakt en bewerkt worden. Omdat Elastic gebruikmaakt van *machine learning* kunnen veranderingen die moeilijk zichtbaar zijn toch zichtbaar gemaakt worden.

[15]

2.4.3.4 Gebruiksvriendelijkheid

Documentatie

Er is een duidelijke en gestructureerde documentatie. Er wordt stap voor stap uitgelegd wat er moet gebeuren.

Tussen de tekst staan soms tips en waarschuwingen. Deze worden aangeduid door een tekstvlak met een symbool in van 'TIP', 'NOTE' of 'IMPORTANT'.

De tekst en de code worden gescheiden door een tekstvlak met een donkerdere achtergrond.

Elastic biedt naast tekst ook nog video-ondersteuning. Op de website zijn een aantal video's beschikbaar.

Leercurve

Uit de beoordelingen van gebruikers blijkt dat Elastic Stack in het begin redelijk ingewikkeld kan zijn. Er moet dus tijd gespendeerd worden om uit te zoeken hoe deze tool werkt. [16], [17], [18]

Support

Als er problemen zijn, kan er gebruikgemaakt worden van de online community: hier kunnen vragen gesteld en beantwoord worden. Verder is het ook mogelijk om een e-mail te sturen.

Er worden ook trainingen aangeboden, met de mogelijkheid om certificaten te halen. [15]

2.4.3.5 Voor- en nadelen

Om de voor- en nadelen van Elastic stack te bekijken wordt er gekeken naar beoordelingen op websites zoals 'Capterra', 'Gartner peer insights' en 'logz.io'.

Voordelen

Het is een open source product dat aangepast kan worden naar eigen normen. Elastic geeft de gebruiker de keuze om de tool als SaaS te gebruiken of zelf te hosten. [16], [17], [18]

Nadelen

In het begin kan het redelijk ingewikkeld zijn, het kan even duren om uit te zoeken hoe de tool werkt. [16] [17], [18]

Er is ook geen *out-of-the-box*-oplossing voor Office 365, SharePoint en VoIP (Voice over IP).

2.4.4 Grafana

Figuur 6: Logo Grafana

Grafana laat toe om gegevens op te vragen, te visualiseren en waarschuwingen te sturen wanneer nodig.

Het heeft een uitgebreid aantal visualisatiemogelijkheden. Zo kunnen er *heatmaps*, grafieken en geomappen gemaakt worden. Er is ook de mogelijkheid om verschillende databronnen in één grafiek samen te voegen. Dit werkt ook voor zelfgemaakte databronnen.

Bij elke grafiek is er de mogelijkheid om tags en metadata toe te voegen.

Het is ook mogelijk om *Ad-hoc* filters aan te maken die automatisch worden toegepast op alle query's die gebruikmaken van die gegevensbron.

Grafana analyseert deze gegevens en stuurt meldingen als een bepaalde voorwaarde overschreden is. [19]

2.4.4.1 Wat wordt er gemonitord?

Grafana ondersteunt meer dan 30 opensource en commerciële gegevensbronnen. Dashboards kunnen gemaakt worden door de gegevens van verschillende bronnen samen te nemen.

Met de 'Azure Monitor Data Source For Grafana' kunnen Azure resources gemonitord worden.

[19]

2.4.4.2 Prijs

Grafana komt met 2 oplossingen: De gratis opensource versie die zelf gehost moet worden, ofwel wordt het gehost door Grafana zelf. In dit pakket is 1 gebruiker gratis, met 5 dashboards. De prijs start bij $49/maand. [19]

2.4.4.3 Meldingen

Meldingen kunnen verzonden worden via e-mail, Slack, PagerDuty, VictorOps, OpsGenie of via webhooks. Dit is enkel beschikbaar in Grafana V4.0 en hoger.

Momenteel bevat alleen het 'graph panel' ondersteuning voor *alert rules*. In de toekomst komt er wel ondersteuning voor de 'Singlestat' en 'table panels'.

In het tabblad waar de waarschuwingen van een grafiek getoond worden, kan er ingesteld worden aan welke voorwaarden voldaan moeten worden om een alert te activeren.

Wanneer een alert van status verandert, stuurt het een melding. Elke regel kan meerdere meldingen sturen. Voordat er meldingen verstuurd kunnen worden, moet er eerst een kanaal gekozen worden waarover de meldingen verstuurd moeten worden (Slack, e-mail, VictorOps…). [19]

2.4.4.4 Gebruiksvriendelijkheid

Documentatie

Grafana biedt een overzichtelijke documentatie. Voor elk besturingssysteem is er een specifieke handleiding beschikbaar voor hoe de installatie moet gebeuren.

In de tekst wordt er ook gewerkt met kleuren. Sommige woorden worden blauw gekleurd en omkaderd zodat niet de volledige tekst gelezen moet worden om de verschillende stappen te kunnen begrijpen.

Om linken te leggen tussen verschillende onderwerpen in de tekst wordt er gewerkt met hyperlinks. De tekst wordt dan oranje gekleurd.

Naast de verschillende kleuren zijn er ook aanvullende afbeeldingen met aanduidingen en verwijzingen naar de tekst. Als er met code gewerkt wordt, wordt dit weergegeven in een tekstvlak met een donkerdere achtergrond. Ook het lettertype is verschillend als er code gebruikt wordt. Zo kan er gemakkelijk een onderscheid gemaakt worden tussen code en tekst.

Het is ook mogelijk om video's over verschillende onderwerpen te bekijken. Deze video's zijn wel al een aantal jaar oud.

Grafana heeft er ook voor gezorgd dat er nog documentatie beschikbaar is voor oudere versies. Bovenaan de pagina kan er gekozen worden voor welke versie er documentatie nodig is (oudste versie is v3.1).

De documentatie is zo opgebouwd dat er snel door genavigeerd kan worden. Er zijn verschillende *TreeViews* waaruit gekozen kan worden, of er kan gebruikgemaakt worden van de zoekbalk linksboven op de pagina. [19]

Leercurve

Uit de beoordelingen blijkt dat Grafana ingewikkeld kan zijn voor nieuwe gebruikers. Grafana verzamelt de gegevens niet automatisch waardoor er veel configuratiewerk is. [20], [21], [22]

Support

Als er vragen zijn kan Grafana gecontacteerd worden via het e-mailadres: hello@grafana.com. Een andere manier om ondersteuning te krijgen is door gebruik te maken van de community. Hier kunnen vragen gesteld worden en vragen kunnen beantwoord worden van anderen. [19]

2.4.4.5 Voor- en nadelen

Voor het onderzoek naar Grafana is er ook gekeken naar de beoordelingen. Tijdens dit onderzoek blijkt dat er niet veel beoordelingen online te vinden zijn. Uiteindelijk is er toch een verslag gemaakt van wat deze mensen goed en slecht vinden.

Voordelen

Meestal wordt er gekozen voor Grafana omdat het er goed uitziet. Met de tool kunnen er aanpassingen gemaakt worden naar eigen wensen.

Ook het feit dat er de mogelijkheid is om te kiezen tussen meerdere programma's om data op te halen en het uitgebreide aantal plug-ins is ook een meerwaarde.

Grafana kan gebruikt worden in samenwerking met ander tools om data te visualiseren.

Met de tool kunnen meerdere grafieken in één grafiek gevoegd worden. Hierdoor kan er een beter beeld gevormd worden van wat er gebeurt in de omgeving. [20], [21], [22]

Nadelen

Het kan een tijd duren voordat de configuratie voltooid is. Voor nieuwe gebruikers is het redelijk ingewikkeld om alles te configureren. Een aantal gebruikers klagen ook over de snelheid van de pagina als er grote hoeveelheden data getoond moeten worden.

Grafana is enkel voor het visualiseren van de gegevens, de tool kan zelf geen gegevens verzamelen. Gegevens worden verzameld door gebruik te maken van andere tools. [20], [21], [22]

2.4.5 SCOM

Figuur 7: Logo SCOM

SCOM of System Centre Operations Manager is een monitoring-tool van Microsoft die in het pakket van System Centre zit.

Het is een *cross-platform* dat zowel besturingssystemen als hypervisors kan gaan monitoren. Met SCOM kan de gezondheid en de prestaties van de omgeving geanalyseerd worden. Zowel lokale gegevens als Cloud gegevens kunnen verzameld worden.

Data kan opgehaald worden om de *workload* of de infrastructuur in de gaten te houden.

SCOM maakt gebruik van *agents* om de data te verzamelen van de verschillende systemen. Een *agent* wordt op een computer geïnstalleerd die gemonitord moet worden. Door gebruik te maken van een proxy-*agent* is het mogelijk om de prestaties en beschikbaarheid van een toestel op te volgen zonder dat er een *agent* geïnstalleerd is.

Met SCOM kan de gezondheid, de prestaties en de beschikbaarheid van servers, toestellen, services en applicaties bekeken worden. [23]

2.4.5.1 Wat wordt er gemonitord?

Er is zowel de mogelijkheid om netwerken als applicaties te monitoren.

Applicaties die gebouwd zijn in .NET en Java maar ook webapplicaties kunnen gemonitord worden. Door gebruik te maken van 'Azure Application Insights' kunnen verzoeken van webapplicaties, uitgaande REST- en SQL-calls, en logs gevolgd worden.

Operations Manager maakt gebruik van beheergroepen. In een beheergroep wordt er gebruikgemaakt van managementservers, *operational databases* en *warehouse* databases.

De *operational database* is een SQL-server die standaard zeven dagen alle data bijhoudt. Alle data van deze database wordt ook automatisch opgeslagen in de *warehouse* database. Deze is voor lange-termijndata.

De beheerservers hebben als doel om te communiceren met de *agents* en de databases, maar ook de beheergroepsconfiguratie te beheren.

SCOM maakt gebruik van 'Management Packs' die ervoor zorgen dat de *agent* de juiste informatie doorstuurt naar de beheerservers. Een Management Pack wordt gebruikt om één of meerdere componenten te controleren en te ontdekken. Deze zijn beschikbaar op de website van Microsoft. [23]

2.4.5.2 Prijs

SCOM is een onderdeel van System Center, dit wil dus zeggen dat er een licentie nodig is voor System Center. De prijs wordt bepaald door het aantal *cores* en het aantal servers. Vervolgens moet er ook rekening gehouden worden met een licentie voor virtuele of fysieke servers.

De prijs voor een licentie voor virtuele servers is $3 607 per *core.* Voor fysieke servers bedraagt de prijs $1 323 per *core*. Deze licenties zijn twee jaar geldig.

[24]

2.4.5.3 Meldingen

Wanneer er een alert gegenereerd wordt kan deze verstuurd worden via e-mail, *Instant messaging* (IM) of via sms. Het is ook mogelijk dat er automatisch commando's worden uitgevoerd wanneer er een melding is verstuurd. [23]

2.4.5.4 Gebruiksvriendelijkheid

Documentatie

Aangezien SCOM een product is van Microsoft kan de documentatie ook gevonden worden op de 'docs' pagina van Microsoft.

De documentatie kan volledig opgeslagen worden als pdf-document zodat deze offline beschikbaar is.

In de tekst wordt alles uitgebreid uitgelegd.

Aan de linkerkant van de pagina is er een zoekbalk en een *TreeView* voorzien om snel op een onderwerp te zoeken.

Aan de rechterkant van de pagina is er een inhoudstabel om snel naar de verschillende hoofdstukken te gaan van dat specifieke onderwerp.

Belangrijke informatie wordt in een tekstvlak geplaatst met een andere achtergrond zodat dit zeker goed opvalt.

Sommige woorden worden vetgedrukt. Hierdoor wordt aangegeven welke stappen uitgevoerd moeten worden zonder de tekst volledig te lezen. Dit is echter niet zo duidelijk op de webpagina waardoor de essentie ervan verloren gaat. Zeker wanneer de tekst in 'donkere mode' gelezen wordt is het moeilijk te zien dat deze woorden belangrijker zijn. Dit probleem is wel opgelost als de documentatie gelezen wordt als pdf.

Er wordt ook gebruikgemaakt van waarschuwingen (tekstvlak met rode achtergrond) en tips (tekstvlak met blauwe achtergrond).

Boven elk onderdeel staat ook altijd aangegeven hoelang het duurt om een bepaald gedeelte te lezen.

[23]

Leercurve

De tool configureren kan ingewikkeld zijn omdat er veel mogelijkheden zijn. Het is belangrijk dat er geweten is wat er gemonitord moet worden voor de configuratie van SCOM. Verder is het ook belangrijk dat alles goed geconfigureerd wordt. Zeker op het vlak van meldingen: als dit slecht geconfigureerd is kan het zijn dat er veel overbodige meldingen verzonden worden. [25], [26], [27], [28]

Support

Als er technische vragen zijn kan er gebruikgemaakt worden van het online-platform van System Center. Microsoft biedt ook gratis opleidingen aan via Microsoft Virtual Academy.

2.4.5.5 Voor- en nadelen

Voor de voor- en nadelen is er gekeken naar de reacties op volgende websites: 'Capterra', 'TrustRadius', 'Gartner peer insights' en 'G2 Crowd'.

Voordelen

De instellingen kunnen gedetailleerd aangepast worden waardoor er veel mogelijkheden zijn. Ook de meldingen kunnen aangepast worden naar eigen wensen. [25], [26], [27], [28]

Nadelen

SCOM configureren kan ingewikkeld zijn. Er kunnen veel aanpassingen gedaan worden maar als deze niet goed geconfigureerd worden, kan dit voor frustraties zorgen. Vooral op het vlak van meldingen kan dit irritant zijn. Hierdoor kruipt er veel tijd in het aanpassen van de configuratie.

Voor sommige management packs is er weinig documentatie te vinden. Deze management packs worden meestal aangeboden door externe verkopers en moeten ook aangekocht worden.

Er is geen *out-of-the-box*-ondersteuning voor niet-Microsoft-technologieën zoals VMware, Oracle en Citrix.

Er wordt ook gesproken over een minder goede netwerkmonitoring. [25], [26], [27], [28], [29]

2.4.6 netXMS

Figuur 8: Logo netXMS

netXMS is een *open source* monitoring-tool. De tool kan automatisch laag 2 en laag 3 van het *International Organization for Standardization*-model (OSI-model) ontdekken.

Er kunnen honderden meetgegevens gemeten worden op meer dan duizend toestellen. Door gebruik te maken van de *agents* wordt de data verzameld. Deze data kan bekeken worden door het cross-platform management console, de webinterface of de management console voor Android. [30]

2.4.6.1 Wat wordt er gemonitord?

Met deze tool kunnen er zowel applicaties als servers gemonitord worden. Het is mogelijk om gegevens te visualiseren die betrekking hebben op de CPU, bestandssystemen, I/O, het geheugen en het verkeer.

Er is een *Java Management Extensions* (JMX) bridge voor Java-gebaseerde applicaties. Er is ook ondersteuning voor MySQL, Oracle, PostgreSQL, DB2, MongoDB en nog een aantal. Via de integratie- *application programming interface* (API) kunnen eigen applicaties ook gemonitord worden.

Met netXMS is het mogelijk om met één server duizenden apparaten te monitoren die over heel de wereld actief zijn. [30]

2.4.6.2 Prijs

NetXMS is volledig gratis en open source.

2.4.6.3 Meldingen

Meldingen worden verzonden via e-mail of sms.

Met NetXMS is er de mogelijkheid om met mobile apparaten (Android 2.2 of hoger) de omgeving te bekijken. Met de app kunnen meldingen, dashboards, *nodes*, grafieken en MAC-adressen bekeken worden. [30]

2.4.6.4 Gebruiksvriendelijkheid

Documentatie

Op de website zijn er drie verschillende handleidingen beschikbaar: 'Administrator guide', 'User guide' en 'Database reference'. De 'Database reference' kan echter niet geopend worden.

De andere twee handleidingen kunnen wel geopend worden. In deze handleidingen worden de verschillende stappen uitgelegd.

De tekst wordt aangevuld met ondersteunende afbeeldingen en voorbeelden die volledig uitgeschreven zijn.

Naast de pdf-handleidingen is er ook een NetXMS Wiki. Hier kunnen *tutorials* en voorbeelden gevonden worden. Er is ook de mogelijkheid om video's te bekijken. Bij het openen van de video's is wel te zien dat deze al een aantal jaar oud zijn.

Op NetXMS Wiki is er een link naar de web-versie van de pdf-bestanden die beschikbaar zijn op de startpagina.

[30]

Leercurve

Er wordt niet echt iets gezegd over de leercurve bij de beoordelingen, er wordt wel gesproken over een makkelijke installatie. [31], [32]

Support

NetXMS biedt op haar website drie verschillende trainingen aan: basistraining, gevorderde training en ontwikkelaarstraining. De basistraining is een cursus van drie dagen voor beheerders van kleine en middelgrote netwerken. De gevorderde training is voor grote netwerken en is een cursus van twee dagen. De laatste training die ze aanbieden is een diepgaande cursus voor het ontwikkelen van uitbreidingen voor de software.

Naast de trainingen is het mogelijk om commerciële-ondersteuning of maatschappelijke hulp te vragen.

De commerciële-ondersteuning kan via e-mail, telefoon, Skype of Telegram. Dit zijn meestal de problemen die de hoogste prioriteit hebben. Hier wordt de responstijd gegarandeerd.

De maatschappelijke hulp gebeurt via het NetXMS *form* of in de Telegram-groep. Hier wordt de responsetijd niet gegarandeerd.

Het is echter ook mogelijk om contact op te nemen via sociale media zoals Facebook en Twitter.

[30]

2.4.6.5 Voor- en nadelen

Tijdens het onderzoek naar de beoordelingen van gebruikers, blijkt dat er weinig beoordelingen zijn. De beoordelingen die er zijn, zijn al redelijk oud.

Voordelen

De installatie is simpel. Tijdens het installatieproces moeten er enkel een paar opties aangevinkt worden. NetXMS kan gebruikt worden in samenwerking met de meest voorkomende databases.

Door gebruik te maken van scripts en applicatie specifieke uitbreidingen, kan NetXMS alle versies van *Simple Network Management Protocol* (SNMP) samen met *Secure Shell* (SSH) en ICMP-protocollen gebruiken om gegevens te verzamelen. Voor uitgebreide analyses kan er gebruikgemaakt worden van de *agents*.

Verder is de tool een complete netwerkbeheerapplicatie met een grote hoeveelheid aan functionaliteiten. [31], [32]

Nadelen

Er wordt geen waarschuwing gegeven als er vergeten wordt op te slaan. [31], [32]

Verder is het ook niet mogelijk om Office 365, SharePoint en VoIP te monitoren.

2.4.7 New Relic

Figuur 9: Logo New Relic

Met New Relic moet er niet meer van pagina tot pagina genavigeerd worden. In het overzicht wordt er een rechtstreekse analyse gemaakt van de volledige omgeving in volledige context.

Zowel *On-premise* als in de Cloud kunnen gegevens verzameld en geanalyseerd worden door de *Cloud-ready* integratie

Applicaties kunnen bekeken worden op hun prestaties: bottlenecks kunnen gevonden en opgelost worden.

New Relic is gebouwd voor teams die agile werken, waarbij er regelmatig wijzigingen aangebracht worden. [33]

2.4.7.1 Wat wordt er gemonitord?

Zowel applicaties als netwerken kunnen gemonitord worden met New Relic. De tool biedt ondersteuning voor programma's die geschreven zijn in Go, Java, .NET, Node.js, PHP, Python en Ruby.

Met de New Relic's Microsoft Azure integratie wordt het mogelijk om data uit Azure te analyseren. Azure webapps kunnen gemonitord worden door gebruik te maken van de New Relic .NET *framework-agent*.

Het is echter niet mogelijk om Office 365 te monitoren met New Relic. Applicaties zoals SharePoint worden niet ondersteund.

[33]

2.4.7.2 Prijs

New Relic is opgedeeld in verschillende pakketten: 'APM', 'Infrastructure', 'Browser', 'Mobile', 'Synthetics' en 'Insights'. Er wordt ook een verschil gemaakt tussen de Cloud en *self-hosted*.

De prijs in de Cloud wordt bepaald door de grootte en het aantal instanties, en hoelang ze draaien.

Er kan zowel op maandelijkse als op jaarlijkse basis gefactureerd worden, hierbij is de jaarlijkse facturering goedkoper.

De prijs van de APM is: $149 per maand voor de Pro-versie en $75 voor de Essentials-versie. Deze prijzen zijn berekend op jaarlijkse basis. De prijs bij maandelijkse facturering bedragen: $199 voor de Pro-versie en $119 voor de Essentials-versie.

De Pro-versie is voor organisaties met een complexe-omgeving of als er veel gemonitord moet worden. De Essentials-versie is eerder voor organisaties die enkel de essentiële APM-mogelijkheden nodig hebben. Dit pakket bevat minder functionaliteiten en ondersteuning.

De prijs voor zelf gehoste infrastructuur wordt bepaald door het aantal *computer unit's* (CU's). Er zijn twee pakketten, de '*Infrastructure Pro*' en de '*Infrastructure Essentials*'. Het Pro-pakket heeft een prijs van: $14,40 per maand per host. Het Essentials-pakket heeft een prijs van: $7,20 per maand per host. Bij beide pakketten wordt er uitgegaan dat er maximaal 12 000 CU's zijn. [33]

2.4.7.3 Meldingen

Meldingen kunnen verzonden worden over verschillende kanalen. E-mail, PagerDuty, Campfire en Slack zijn hier een voorbeeld van. Door gebruik te maken van webhooks kan bijna elke applicatie gebruikt worden.

New Relic heeft ook een mobile applicatie voor zowel Android als IOS. Met deze applicatie kunnen dus ook meldingen ontvangen worden. [33]

2.4.7.4 Gebruiksvriendelijkheid

Documentatie

In de documentatie wordt er op een eenvoudige manier stap voor stap uitgelegd wat er gedaan moet worden.

Om code en tekst gescheiden te houden wordt er gewerkt met een ander lettertype. Door met een andere kleur te werken worden variabelen duidelijk gemaakt.

Er wordt ook gewerkt met tips en waarschuwingen. Verder wordt de tekst ook ondersteund met afbeeldingen die de tekst verduidelijken. Dit zorgt ervoor dat de tekst gemakkelijker te begrijpen is.

Als er iets snel opgezocht moet worden kan er altijd gebruikgemaakt worden van de zoekbalk. Deze heeft automatische aanvulling, zodat het gezochte onderwerp snel gevonden kan worden. Ook de *TreeView* aan de linkerkant van de pagina kan hierbij helpen. Wanneer een onderwerp geopend is, dan wordt in deze *TreeView* een inhoudstabel weergegeven. [33]

Leercurve

Bij het bekijken van de beoordelingen wordt er vaak gesproken over een makkelijke leercurve. [34], [35], [36], [37], [38]

Support

Er zijn verschillende manieren om ondersteuning te krijgen. Er kan online hulp aangevraagd worden of de documentatie kan geraadpleegd worden. Voor de online hulp kan er gebruikgemaakt worden van de 'New Relic's *Explorers hub'* (community), hier kunnen vragen gesteld worden en andermans vragen beantwoord worden. Er worden ook training aangeboden waarmee certificaten behaald kunnen worden.

Nadat de gratis proefperiode van het account afgelopen is moet er een betalend abonnement gekocht worden om supporttickets aan te maken. De community kan gebruikt worden voor support als er geen betalend abonnement is.

Het soort support dat aangeboden wordt is afhankelijk van de hoeveelheid geld die jaarlijks betaald wordt. Er wordt een onderscheid gemaakt tussen: 'silver', 'gold', 'platinum' en 'premium'.

De New Relic 'Diagnostics tool' kan helpen om problemen op te lossen. De tool kan veelvoorkomende problemen met *agents* opsporen.

[33]

2.4.7.5 Voor- en nadelen

Om de voor- en nadelen te achterhalen wordt er gekeken naar verschillende websites. De websites die bekeken zijn, zijn: 'PCMag', 'FanancesOnline', 'GetApp' en 'TrustRadius'. Er is ook gekeken naar de discussies op het platform van New Relic.

Voordelen

Met de tool kunnen grote hoeveelheden servers en applicaties gemonitord worden. Het maakt niet uit of deze in de Cloud of *on-premises* gehost worden. Ook het groot aantal plug-ins is een voordeel. [34], [35], [36], [37], [38]

Nadelen

Er is geen integratie met Office 365, om de software te kunnen monitoren zal er gebruikgemaakt moeten worden van extra software.

De interface wordt vaak omschreven als een negatief punt. Ook de prijs kan hoog oplopen als er veel toestellen gemonitord moeten worden.

De tool is een SaaS-pakket: dit wil zeggen dat de tool geen gegevens kan verzamelen als er geen internettoegang is. [34], [35], [36], [37], [38]

2.4.8 PRTG

Figuur 10: Logo PRTG

PRTG is een *agentless* monitoring-tool die ontwikkeld is door Paessler AG. De tool kan netwerkverkeer, applicaties, de beschikbaarheid, de bandbreedte en veel meer monitoren.

PRTG maakt gebruik van standaard protocollen zoals ping, SNMP, SSH, *Windows Management Instrumentation* (WMI) en REST API die *Extensible Markup Language* (XML) of JavaScript Object Notation (JSON) teruggeven.

Alles kan gemonitord worden. Zowel LAN's, WAN'S, serves, websites, applicaties en nog veel meer. Dit kan in de Cloud of in een lokale-omgeving.

De gegevens kunnen in een kaart geplaatst worden om het netwerk in beeld te brengen.

Oude data kan geëxporteerd worden naar pdf, HTML, XML of CSV-bestanden.

PRTG biedt sensoren aan voor bijna elke belangrijke fabrikant van apparaten. Een aantal van deze fabrikanten zijn: Cisco, Dell, Oracle en HP. [39]

2.4.8.1 Wat wordt er gemonitord?

Met PRTG kunnen netwerken en applicaties gemonitord worden. Zowel LAN- als WAN-netwerken, websites en servers. Veel belangrijke technologieën worden ondersteund. Een aantal van deze technologieën zijn: SNMP, WMI, SSH, *Flows* en *Packet Sniffing*, HTTP, REST API's die XML of JSON teruggeven, ping en VoIP.

De tool kan gebruikt worden om de *uptime* weer te geven. Er kan gekeken worden of een apparaat of website beschikbaar is, dit wordt meestal weergegeven in een percentage dat gemeten wordt op één dag tijd.

Er wordt gebruikgemaakt van sensoren, een sensor monitort meestal één meetwaarde in het netwerk.

PRTG heeft ook een SaaS-sensor, hiermee kan de beschikbaarheid van een service procentueel weergegeven worden en de reactietijd van SaaS providers zoals: Bing, Dropbox, facebook, GitHub, Google Apps, Office 365, Salesforce, Twitter en YouTube.

Met de SNMP-disk Free Sensor kan er gemonitord worden naar de vrije ruimte op een schijf. Met deze sensor wordt het percentage vrije ruimte op een schijf, de vrije ruimte in bytes en de totale ruimte op de schijf berekend.

[39]

2.4.8.2 Prijs

Er zijn verschillende pakketten beschikbaar. De pakketten zijn: PRTG 500, PRTG 1000, PRTG 2500, PRTG 5000, PRTG XL1 en PRTG XL5. Alle licenties bevatten alle onderdelen en zijn eeuwigdurend.

Het eerste jaar is het onderhoud automatisch inbegrepen in de prijs van elke nieuwe licentie. Bij elk pakket kan er gekozen worden voor extra onderhoud, hier kan de keuze gemaakt worden tussen 12 (inbegrepen), 24 of 36 maanden onderhoud. Dit onderhoud bevat updates en premium e-mailondersteuning.

PRTG 500 heeft een prijs van €1 200,00 (exclusief btw). Dit pakket bevat 500 sensoren en kan op maximaal 1 server geïnstalleerd worden.

Het PRTG 1000-pakket heeft een prijs van €2 150,00 (exclusief btw) en bevat 1 000 sensoren. Ook met dit pakket kan de tool maar op één server geïnstalleerd worden.

Indien er meer dan 1000 sensoren nodig zijn kan er gekozen worden voor PRTG 2500. Dit pakket bevat 2500 sensoren, en de installatie is maar mogelijk op één server. De prijs start bij €4 500 (exclusief btw).

Als er tot 5000 sensoren nodig zijn, kan er gekozen worden voor het PRTG 5000-pakket. Ook hier wordt de installatie maar op één server geïnstalleerd. De prijs is €8 000,00 (exclusief btw).

Voor een ongelimiteerd aantal sensoren moet er gekozen worden voor PRTG XL1 of PRTG XL5. Beide pakketten bieden een ongelimiteerd aantal sensoren, het verschil zit in het aantal server installaties. PRTG XL1 kan op één server geïnstalleerd worden, en heeft een prijs van €11 500,00. Het PRTG XL5 heeft een prijs van €45 000,00 en kan op vijf servers geïnstalleerd worden.

Er is ook nog een pakket beschikbaar met maximaal 100 sensoren. De prijs van dit pakket is volledig gratis.

Op de website wordt er gezegd dat de meeste klanten ongeveer 10 sensoren per apparaat gebruiken. Met het PRTG 1000 kunnen er dus ongeveer 100 apparaten gemonitord worden. Eén poort op een switch telt wel voor één sensor.

Upgraden naar een ander pakket kan door het prijsverschil tussen de pakketten te betalen.

[39]

2.4.8.3 Meldingen

Er kan gebruikgemaakt worden van e-mail, sms en pushmeldingen naar Android en IOS voor het ontvangen van meldingen. Verder is er ook nog Slack, *Microsoft Teams Message* en *syslog message*. Deze meldingen kunnen zelf aangepast worden. [39]

2.4.8.4 Gebruiksvriendelijkheid

Documentatie

PRTG biedt op haar website drie verschillende mogelijkheden om de documentatie te bekijken: de HTML-documentatie, de pdf-documentatie of de *electronic publication* (EPUB)-documentatie.

Alles wordt stap voor stap uitgelegd van wat er gedaan moet worden. Er wordt ook gewerkt met vetgedrukte tekst en ondersteunende afbeeldingen. Als er op de afbeeldingen geklikt wordt, dan worden deze vergroot zodat deze beter leesbaar zijn.

In de tekst zijn er hyperlinks beschikbaar zodat er snel naar een ander onderwerp genavigeerd kan worden.

Verder wordt er ook gewerkt met tips en waarschuwingen.

Er zijn ook video's beschikbaar op de website die kunnen helpen bij het configureren van de tool.

[39]

Leercurve

Bij het kijken naar wat gebruikers van de tool vinden wordt er vaak gesproken over een eenvoudige en snelle installatie en configuratie. [40], [41], [42], [43], [44]

Support

Op de website wordt er zowel technisch support als customer services aangeboden. Hiervoor moet er eerst een ticket aangemaakt worden. Op de website wordt er wel gezegd dat als er toegang is tot PRTG, dat er dan contact wordt opgenomen via het setup menu.

Vragen kunnen van maandag tot vrijdag beantwoord worden van 07:00 uur tot 22:00 uur (vragen worden gesteld in het Engels). Klanten met een onderhoudscontract krijgen voorrang op klanten zonder onderhoudscontract.

Op de website is er ook een pagina beschikbaar met vaak gestelde vragen. Hierop kan gekeken worden voordat er contact opgenomen wordt met PRTG.

PRTG biedt op haar website *e-learning* modules aan die de belangrijkste functies uitleggen. Daarnaast worden er ook trainingen georganiseerd om de werking van PRTG duidelijk te maken. [39]

2.4.8.5 Voor- en nadelen

Om de voor- en nadelen van PRTG te bekijken wordt er gekeken naar de gebruikservaringen op ‘Truspilot’, ‘GetApp’, ‘Spiceworks’, ‘Capterra’, ‘G2 Crowd’ en ‘Gartner peer insights’. Gemiddeld krijgt deze tool een 4,5 op 5.

Voordelen

De snelheid van de configuratie en de installatie wordt gewaardeerd bij veel gebruikers. Het is gemakkelijk om de standaard onderdelen te monitoren zoals schijfruimte, Random-Access Memory (RAM), de CPU, ping, Remote Desktop Protocol (RDP) en HTTP. Ook de functionaliteit is een voordeel. Het is een krachtige tool met veel mogelijkheden. [40], [41], [42], [43], [44]

Nadelen

Als er veel sensors nodig zijn kan de prijs redelijk hoog zijn. Er zijn vaste pakketten met een bepaalde hoeveelheid aan sensoren. Als er nood is aan een kleine hoeveelheid extra sensoren, dan moet er al een duurder pakket gekocht worden met meer sensoren omdat pakketten niet gecombineerd kunnen worden. Ook het support wordt aanzien als redelijk traag, het duurt meestal een dag voordat ze antwoorden via e-mail. [40], [41], [42], [43], [44]

2.4.9 Splunk

Figuur 11: Logo Splunk

Splunk is een verzameling van verschillende IT-diensten: SIEM, AIOps, applicatiemanagement, eventmanagement, logmanagement.

Het voornaamste doel van Splunk is om de chaos in een infrastructuur op een overzichtelijke manier weer te geven.

Door artificiële intelligentie en *Machine Learning* kunnen er snel onregelmatigheden gedetecteerd worden. [45]

2.4.9.1 Wat wordt er gemonitord?

Met Splunk kan zowel de infrastructuur als de applicaties gemonitord worden. De tool maakt het mogelijk om data te analyseren, doorzoeken en te visualiseren. Gegevens worden verzameld van: websites, applicaties, sensoren, apparaten en meer.

Er kan zowel gewerkt worden met *agents* als *agentless*. Door de WMI-ondersteuning kan het *agentless* toegang krijgen tot Windows prestaties en *event log data* op externe toestellen.

Splunk geeft de gebruiker de mogelijkheid om met een aantal apps of *add-ons* samen te werken. Op Splunkbase kunnen verschillende applicaties of *add-ons* gevonden worden die met een aantal klikken geïntegreerd kunnen worden in Splunk. Dit is inbegrepen in elk abonnement, enkel het Splunk Light abonnement ondersteunt niet alle *add-ons*.

Met de Microsoft Office 365 *add-on* voor Splunk kunnen dashboards gemaakt worden van Office 365 applicaties. Deze *add-on* kan de servicestatus, serviceberichten en logboeken vanuit Office 365 ophalen.

De prestaties van VoIP kunnen gemonitord worden door gebruik te maken van de Corvil VoIP performance-app. Er worden rapportages gemaakt en het kan gebruikt worden om problemen op te lossen bij VoIP.

Verder kan data van elke TCP- of UDP-poort opgehaald en geanalyseerd worden om een beter beeld te krijgen van het netwerk.

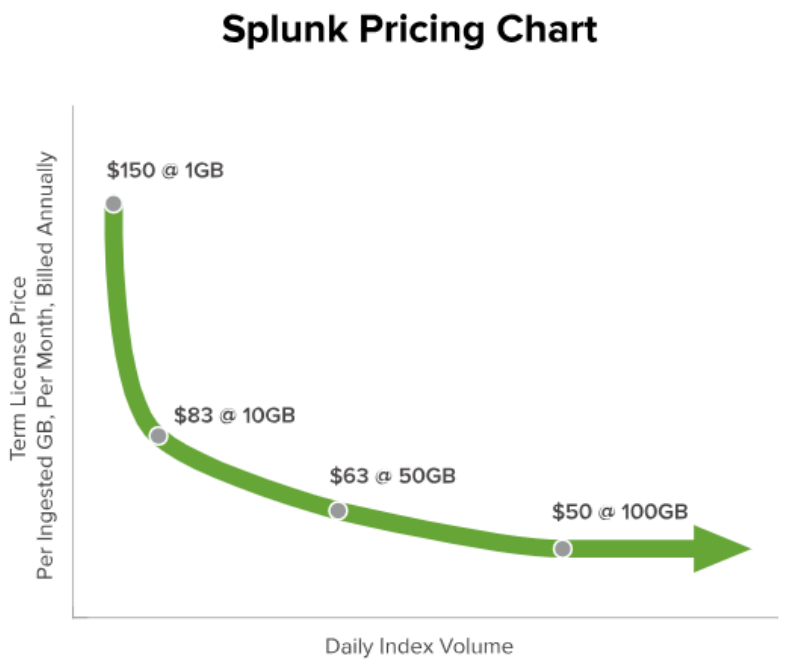
Van elke host kunnen er gegevens verzameld worden zoals het besturingssysteem, de processor, de schijf, de netwerkkaart, services en processen en algemene informatie zoals de naam en het domein waarin die zich bevindt.

Door gebruik te maken van PowerShell kunnen er scripts geschreven worden die ervoor zorgen dat bepaalde dingen gemonitord worden.

[45]

2.4.9.2 Prijs

Er zijn verschillende pakketten beschikbaar. Splunk Enterprise start met een prijs van $173 per opgeslagen gigabyte (GB), per maand. De prijs wordt op jaarlijkse basis gefactureerd. In dit pakket zit: een onbeperkt aantal gebruikers, de mogelijkheid om te schalen naar onbeperkte hoeveelheden gegevens per dag, waarschuwingen en monitoring, standaardondersteuning en een mogelijkheid tot premiumondersteuning. Figuur 12 toont aan dat bij grotere hoeveelheid gegevens die door Splunk geïndexeerd worden, de prijs per GB ook zal dalen.



Figuur 12: Prijzengrafiek.

Splunk *Light* start met een prijs van $87 per opgelopen gigabyte, per maand. De prijzen worden jaarlijks gefactureerd. Met dit pakket kunnen er maximaal vijf gebruikers gebruikmaken van de software. De maximale hoeveelheid aan gegevens per dag is 20 GB. Verder kan alles gemonitord worden en er kunnen meldingen gestuurd worden. Met dit pakket wordt enkel de basisondersteuning geleverd.

Splunk Gratis biedt toegang voor één gebruiker en 500MB gegevens per dag. Met dit pakket kunnen de gegevens van de machines verzameld en geïndexeerd worden. Als er gekozen wordt voor dit pakket is enkel de community-ondersteuning beschikbaar.

Als er gekozen wordt voor een pakket met een eeuwigdurende licentie, dan zal er wel jaarlijks opnieuw ondersteuning gekocht moeten worden. De ondersteuning bevat alle software-updates en klantenondersteuning.

[45]

2.4.9.3 Meldingen

Splunk heeft zowel een mobile applicatie voor Android als voor IOS. Met deze applicatie kunnen *push* notificaties ontvangen worden en er kunnen rapporten, *dashboards* en kritieke servers of applicaties bekeken worden.

Het is ook mogelijk om meldingen te ontvangen via e-mail of sms.

Meldingen kunnen geconfigureerd worden zodat ze niet altijd af moeten gaan als ze gegenereerd worden. Het interval van een melding kan ook geconfigureerd worden. [45]

2.4.9.4 Gebruiksvriendelijkheid

Documentatie

Op de documentatiepagina van Splunk kan de keuze gemaakt worden voor welk product of service documentatie nodig is. Om iets snel op te zoeken is er ook een zoekbalk voorzien. Deze geeft wel geen zoeksuggesties en wanneer er schrijffouten worden ingegeven is het mogelijk dat er geen zoekresultaten zijn.

De documentatie kan gedownload worden als pdf zodat deze offline beschikbaar is. Hierbij is er de keuze om de volledige documentatie te downloaden of enkel dat bepaalde onderdeel.

Als er gebruikgemaakt wordt van een oudere versie van Splunk kan er altijd teruggevallen worden op een oudere versie van de documentatie.

Voor nieuwe gebruikers is er een handleiding gemaakt om snel te kunnen starten. Om de handleiding te kunnen volgen is er gratis software voorzien (gratis evaluatie versie Splunk).

De documentatie is overzichtelijk en er wordt altijd aangegeven wat er in de documentatie staat. Er wordt ook vermeld hoe de handleidingen gebruikt moeten worden.

Verder wordt er gebruikgemaakt van ondersteunende afbeeldingen en vetgedrukte tekst. Bij de instructies wordt er gewerkt met verschillende stappen die aangegeven worden door cijfers. Om snel naar andere pagina's te navigeren wordt de tekst ook aangevuld met hyperlinks. [45]

Leercurve

Om de leercurve te bepalen wordt er gekeken naar beoordelingen. Hiervoor wordt er gekeken naar websites zoal 'Gartner peer insights', 'TrustRadius', 'G2 Crowd' en 'Software Advice'.

Uit de reacties blijkt dat het moeilijk kan zijn als er geen kennis is van Splunk. Het kan een tijd duren voordat er met alle onderdelen gewerkt kan worden.

Dit komt omdat er veel mogelijkheden zijn met de tool. Training is dus zeker nodig voordat de tool gebruikt wordt.

[46], [47], [48], [49], [50]

Support

Support is afhankelijk van het type abonnement. Als er voor Splunk Enterprise, Splunk Enterprise Security, Splunk IT Service Intelligence en andere betaalde apps gekozen is, kan er gebruikgemaakt worden van 'Success Plans'. Dit is een combinatie van ondersteuning, professionele services en succesmanagers van klanten die het juiste serviceniveau aanbieden dat past binnen de bedrijfsbehoeften.

Standaard kan er altijd gebruikgemaakt worden van de community. Dit is inbegrepen in elk pakket dat aangeboden wordt. Als extra service bij het Light/Insights-pakket wordt er toegang gegeven tot de basisondersteuning.

Er worden ook trainingen aangeboden op de website. Dit is in de vorm van *e-Learning* en live lessen. Als een cursus voltooid wordt, worden er ook certificaten behaald. [45]

2.4.9.5 Voor- en nadelen

Bij het bekijken van websites zoals 'Gartner peer insights', 'TrustRadius', 'G2 Crowd' en 'Software Advice' krijgt de tool gemiddeld meer dan vier sterren op vijf.

Voordelen

Ondanks de steile leercurve en de hoge prijs, wordt de tool wel gewaardeerd voor haar functionaliteit. Het is een krachtige tool. Door gebruik te maken van *Search Processing Language* (SPL) kunnen gegevens gezocht, gefilterd, gewijzigd, gemanipuleerd, ingevoegd en verwijderd worden. [46], [47], [48], [49], [50]

Nadelen

Veel van de gebruikers vinden dat het leerproces van Splunk redelijk moeilijk is. Waardoor er veel tijd besteed moet worden aan het leren werken met de tool. Verder kan het verwarrend overkomen bij nieuwe gebruikers.

De prijs komt ook vaak terug in de beoordelingen. Deze kan redelijk hoog oplopen aangezien de licenties worden berekend op het aantal gigabytes aan logbestanden. Er zijn goedkopere alternatieve zoals Elastic Stack.

Om efficiënt met Splunk te kunnen werken wordt er aangeraden om SPL aan te leren.

[46], [47], [48], [49], [50]

2.4.10 WhatsUp Gold

Figuur 13: Logo WhatsUp Gold

Met WhatsUp Gold kan er automatisch een volledige infrastructuur in beeld gebracht worden. Zowel de fysieke apparatuur maar ook een Cloud-omgeving kunnen gemonitord worden.

Alles wordt in een kaart getoond waarin de connecties tussen de verschillende toestellen weergegeven worden. Vanuit deze kaart kan er genavigeerd worden naar de prestaties en de gegevens van de toestellen.

Routers, switches, virtuele machines en applicaties kunnen gemonitord worden.

Meldingen worden onmiddellijk verzonden naar Slack, e-mail of er wordt een sms verstuurd. Het is mogelijk om deze meldingen aan te passen zodat er minder overbodige meldingen zijn.

Het is ook mogelijk om de volledige netwerkinfrastructuur in de gaten te houden op een mobiel apparaat: er is zowel een Android applicatie als een IOS applicatie. [51]

2.4.10.1 Wat wordt er gemonitord?

Met de APM software kunnen Microsoft applicaties gemonitord worden. Dit zijn applicaties zoals Exchange, SharePoint, AD en SQL-server.

Het bandbreedteverbruik over netwerken, servers en applicaties kunnen ook gemonitord worden. De tool kan zelfs verkeer van en naar het ‘dark web’ detecteren.

WhatsUp Gold biedt verder ook de mogelijkheid om elementen in de Cloud te monitoren. Er is ondersteuning voor AWS en Azure Cloud. De software kan automatisch Cloud bronnen ontdekken en geeft deze weer in dashboards.

Door gebruik te maken van het *Address Resolution Protocol* (ARP), SNMP, SSH, *Virtual Infrastructure Management*, IP-adressen, ICMP en het *Link Layer Discovery Protocol* (LLDP) in combinatie met eigen mechanismen kan er automatisch een ontdekking gedaan worden op laag 2 en 3.

De uptime van een apparaat wordt weergegeven door een *progressbar* in te kleuren met rood en groen. Het groene gedeelte is het procentuele gedeelte dat de server actief was of is. Het rode gedeelte is de verhouding dat de server niet bereikbaar was of is. De percentages worden ook weergegeven. [52]

2.4.10.2 Prijs

Er zijn verschillende abonnementen beschikbaar: 'Premium Annual Subscription', 'Premium License' en 'Total Plus License'. Hiernaast zijn er ook een aantal bundels.

De bundels die worden aangeboden zijn: 'Network Admin's Bundle' en 'System Admin's Bundle'. De eerste bundel bevat WhatsUp gold Premium, netwerkverkeer analyse en configuratie management. De tweede bundel bevat ook WhatsUp Gold Premium maar biedt ook applicatiemonitoring en virtualisatiemonitoring.

Bij WhatsUp gold kan er ook gewerkt worden met een *Device-Based* licentie (Premium editie). Dit wil zeggen dat de licentie niet gebaseerd wordt op het aantal poorten dat gebruikt wordt maar op het aantal toestellen. Hierdoor kan er zelf bepaald worden hoeveel interfaces gemonitord worden op een bepaald toestel.

Verder wordt er ook gewerkt met een puntensysteem (Total Plus editie). Zo kan het aantal componenten dat gemonitord moet worden omgezet worden naar punten: er wordt dus een licentie genomen op het aantal punten. Deze punten kunnen op elk moment aangepast worden.

[51]

2.4.10.3 Meldingen

Meldingen kunnen verzonden worden via e-mail en sms.

Het is ook mogelijk om de volledige omgeving te monitoren via een mobiel toestel. Met de IOS of de Android app kan er gekeken worden welke toestellen *down* en *up* zijn, of naar een bepaald toestel gezocht worden en de details ervan te bekijken. [51] [52]

2.4.10.4 Gebruiksvriendelijkheid

Documentatie

Bij het openen van de documentatie is het eerste dat te zien is, de zoekbalk met de verschillende versies van het product. Bij het gebruiken van de zoekbalk valt onmiddellijk op dat er geen suggesties worden weergegeven wanneer erin getypt wordt.

Er zijn verschillende versie van de documentatie beschikbaar.

In de documentatie wordt alles stap voor stap uitgelegd. De verschillende stappen die gevolgd moeten worden, worden vetgedrukt. Hierdoor moet de tekst niet volledige gelezen worden om de verschillende stappen te kunnen volgen.

Verder wordt de tekst ook aangevuld met waarschuwingen en belangrijkheden. Deze worden weergegeven in een tekstvlak dat een donkerdere achtergrond heeft. In het tekstvlak wordt er ook gewerkt met symbolen.

Onderaan elke pagina is er ook een lijst met links die mogelijk ook gelezen kunnen worden na het lezen van het artikel.

Op de website worden ook trainingen aangeboden. Hier wordt er gebruikgemaakt van e-Learning video's.

[52]

Leercurve

Om de leercurve te bepalen wordt er gekeken naar wat andere mensen van de tool vinden. Hiervoor wordt er gekeken naar websites zoals: 'Spiceworks', 'Capterra', 'Gartner peer insights', 'TrustRadius' en 'Trustpilot'.

Uit de reacties blijkt dat het geen steile leercurve heeft. De tool is eenvoudig om te gebruiken. [53], [54], [55], [56], [57]

Support

Voor ondersteuning kan er gebruikgemaakt worden van de community van ipswitch of de online help. Hier worden trainingen aangeboden, kunnen vragen gesteld worden en de gegevens van ipswitch kunnen hier ook gevonden worden. Door gebruik te maken van de community kan er naar een oplossing gezocht worden met anderen gebruikers, maar ook ideeën kunnen hier gedeeld worden.

Met een dienstovereenkomst kan er ongelimiteerd gebruikgemaakt worden van live support. Dit is gewoonlijk tijdens de werkuren maar bij noodgevallen kan er uitgebreide ondersteuning aangevraagd worden. Deze ondersteuning is altijd beschikbaar. [51]

2.4.10.5 Voor- en nadelen

Bij het onderzoeken naar de voor- en nadelen is er gekeken naar de gebruikservaringen van verschillende gebruikers. Er is gekeken op 'Spiceworks',' Capterra', 'Gartner peer insights', 'TrustRadius' en 'Trustpilot'. Hier zijn veel gebruikers positief over de tool, het krijgt gemiddeld een waardering van vier op vijf.

Voordelen

De tool is gemakkelijk om te gebruiken en ziet er goed uit. Veel van de instellingen kunnen in één centrale pagina weergegeven worden. [53], [54], [55], [56], [57]

Nadelen

In de reacties wordt er vaak gesproken over de snelheid van de webinterface: deze is redelijk traag en reageert soms niet. Er zijn ook een aantal gebruikers die klagen over de hoge prijs van de trainingen. [53], [54], [55], [56], [57]

2.5 Vergelijking

Op basis van de eisen van de klant is er een tabel opgesteld waaruit snel kan afgeleid worden welke tools het meest geschikt zijn voor de klant.

Tabel 2: vergelijking tools

		Datadog	eG Enterprise	Elastic stack	Grafana	SCOM	netXMS	New Relic	PRTG	Splunk	WhatsUp Gold
Prijs	Gratis										
	Betalend										
Meldingen	E-mail										
	sms										
Functionaliteit	Uptime										
	Bandbreedte										
	Latentie										
	Beschikbaarheid										
	offline beschikbaar										
	SQL servers										
	Office 365										
	Azure										
	VoIP										
	SharePoint										

Bovenstaande tabel geeft door middel van groene vakken weer wat een tool allemaal kan, de rode vakken geven aan wat de tool niet kan en de oranje vakken geven aan dat er een gratis testversie is. De grijze vakken geven weer dat er een mogelijkheid is maar geen *out-of-the-box*-oplossing.

Een aantal van deze tools voldoen niet aan de eisen van de klant waardoor ze niet verder besproken worden. De tools die aan de klant voorgesteld zijn, zijn: eG Enterprise, SCOM, PRTG, Splunk en WhatsUp Gold.

Het advies voor de klant is om te werken met eG Enterprise of PRTG, dit komt omdat er veel mogelijkheden zijn met deze tools. PRTG werkt zonder *agents* en kan alle onderdelen monitoren die de klant eist. eG Enterprise biedt voor veel applicaties, besturingssystemen en virtualisatiesystemen ondersteuning. Ook de beoordelingen van deze tools zijn goed.

Omdat de tools veel gelijkenissen hebben op vlak van eisen van de klant, heeft de klant besloten om te werken met een combinatie van SCOM en PRTG. Dit besluit komt voornamelijk door de prijs van de producten. Er is gekozen om met twee tools te werken omdat elke tool wel beperkingen heeft. Door met meerdere tools te werken zijn er meer mogelijkheden. Sommige tools zijn ook beter in een bepaald onderdeel dan een ander tool.

Momenteel werkt de klant al met System Center, SCOM kan hier gemakkelijk geïntegreerd worden. Doordat SCOM geen ondersteuning biedt voor VoIP en een matige netwerkmonitoring heeft is ervoor gekozen om PRTG naast SCOM te installeren.

2.5.1 Verdelen onderdelen

Doordat de klant ervoor gekozen heeft om met een combinatie te werken van twee tools, wordt er gekeken welke onderdelen door welke tool gemonitord moet worden.

2.5.1.1 SQL server

SQL server 2012 en nieuwer kan gemonitord worden door gebruik te maken van volgend Management Pack: Microsoft System Center Management Pack voor SQL server. Hiermee kunnen de prestaties, de beschikbaarheid en configuratiemonitoring gebeuren van een SQL server met bepaalde *thresholds*.

Met de PRTG sensor voor Microsoft SQL v2 worden volgende onderdelen gemonitord: uitvoeringstijd van de aanvraag, uitvoeringstijd van de query, het aantal rijen in een query en het kan ook de datatabel verwerken en gedefinieerde waarden in afzonderlijke kanalen weergeven.

2.5.1.2 Office 365

Voor dit onderdeel wordt er gekozen voor SCOM. SCOM biedt veel meer mogelijkheden op het vlak van Office 365-monitoring. De PRTG Common SaaS sensor kan enkel de beschikbare services in percentage weergeven en de reactietijd.

SCOM kan hier veel dieper in gaan: het kan de licentie monitoren, de mail *flow* of de prestaties bekijken.

2.5.1.3 Azure

Ook hier wordt er gekozen voor SCOM. Met het Management Pack voor Microsoft Azure kan de beschikbaarheid en de prestaties gemonitord worden. Het maakt gebruik van REST API's om op afstand prestatie-informatie over de Azure resources te ontdekken en te verzamelen. Hiervoor wordt er gebruikgemaakt van de Azure Active Directory voor de authenticatie van de Azure REST API's.

2.5.1.4 Netwerk

Om de switches, routers en firewalls te monitoren wordt er gebruikgemaakt van PRTG. Dit is voornamelijk omdat netwerkmonitoring niet optimaal is bij SCOM en er moet gewerkt worden met externe management packs, dit kan dan weer leiden tot meer kosten.

2.5.1.5 VoIP

Voor het onderdeel VoIP wordt er gekozen om met PRTG te werken. Dit komt omdat SCOM geen ondersteuning biedt voor VoIP. Met de PRTG VoIP-monitoring kan *Quality of Service*-monitoring (QoS) gedaan worden en *Internet Protocol Service Level Agreement* (IP SLA) monitoring. De kwaliteit en de latentie kunnen gemonitord worden.

2.5.1.6 Conclusie

Voor de meeste onderdelen wordt er voor SCOM gekozen. Dit komt omdat SCOM een Gedetailleerder overzicht geeft van deze onderdelen. Op het vlak van netwerken en VoIP scoort PRTG dan weer beter. Om aan netwerkmonitoring te doen zal er gebruikgemaakt moeten worden van Management Packs van een derde partij.

In Tabel 3 wordt weergegeven wat de verschillende tools best gaan monitoren.

Tabel 3: verdeling onderdelen

	SCOM	PRTG
SQL servers		
Office 365		
Azure		
Netwerk		
VoIP		

3 Installatie en configuratie

In dit onderdeel wordt de installatie en de configuratie besproken van zowel PRTG als SCOM. Deze informatie komt uit eigen ervaring door de tools te installeren in een testomgeving.

3.1 Installatie

Beide tools worden op een Windows server 2016 geïnstalleerd. Deze twee servers worden voorzien van twee schijven van 60 GB. Voor de PRTG server is er 4 GB RAM voorzien, de SCOM server krijgt 8 GB RAM.

3.1.1 PRTG

De installatie van PRTG is eenvoudig. Om PRTG te installeren moet er een bestand afgehaald worden via de website. Als het bestand uitgevoerd wordt, wordt er een wizard geopend. Hier moet enkel de licentieovereenkomst geaccepteerd worden en een e-mailadres ingevoerd worden. Nadat dit gebeurd is wordt het programma geïnstalleerd.

Na de installatie wordt de webinterface geopend. In de documentatie wordt aangeraden om Google Chrome te gebruiken voor de webinterface. In de testomgeving werd er eerst gewerkt met Internet Explorer, deze browser had problemen met inloggen dus is er overgestapt naar Google Chrome.

3.1.2 SCOM

Voordat SCOM geïnstalleerd kan worden, moeten er eerst een aantal vereiste installaties gebeuren. Om te beginnen is het belangrijk dat de server de laatste updates heeft geïnstalleerd.

Verder moet er rekening gehouden worden met de installatie van SQL, *Internet Information Services* (IIS), .NET Framework en PowerShell versie 3.0 moet geïnstalleerd zijn. De server moet ook in een domein zitten met Active Directory en DNS.

Als dit allemaal in orde is kan de installatie van SCOM beginnen. Hiervoor moet het SCOM *International Organization for Standardization* (ISO) -bestand gebruikt worden. Op dit ISO-bestand staat een installatiebestand dat uitgevoerd moet worden. Nadat dit bestand uitgevoerd is kan de setup uitgevoerd worden.

Deze setup geeft duidelijk aan wat er moet gebeuren.

3.1.3 Conclusie installatie

Wanneer de twee tools met elkaar vergeleken worden op vlak van installatie kan er geconcludeerd worden dat PRTG veel sneller en eenvoudiger verloopt. Er moet veel meer geconfigureerd worden bij SCOM en SCOM is afhankelijk van andere programma's en updates.

3.2 Configuratie

In de testomgeving zijn er een aantal servers voorzien die gemonitord kunnen worden zoals: fileservers, SQL servers en webservers. De tools worden geconfigureerd zodat bepaalden onderdelen gemonitord kunnen worden in deze omgeving.

3.2.1 PRTG

Wanneer de webinterface voor de eerste keer gebruikt wordt, is er de keuze om een rondleiding te volgen. Deze rondleiding is handig voor nieuwe gebruikers, waardoor de belangrijkste onderdelen snel worden uitgelegd.

Toestellen toevoegen kan door een IP-adres of een IP-range in te geven. Tijdens het toevoegen kan er ook meegegeven worden of er automatisch sensoren moeten worden toegevoegd.

Er kan ook snel een overzicht gemaakt worden van een bepaalde groep apparaten door bij 'Libararies' een groep aan te maken.

3.2.2 SCOM

Nadat de installatie voltooid is kan de *agent* op de verschillende toestellen geïnstalleerd worden. Dit kan gebeuren door gebruik te maken van de 'Discovery Wizard'. Nadat de *agents* geconfigureerd zijn kunnen Management Packs geïnstalleerd worden. Microsoft heeft voor een handig onderdeel gezorgd binnen SCOM waardoor aanbevolen Management Packs geïnstalleerd kunnen worden zonder deze te moeten zoeken. Dit kan door gebruik te maken van 'Updates and Recommendations'. Hier worden ook de pakketten weergegeven die geüpdatet kunnen worden.

Het is handig om Management Packs één voor één toe te voegen en te configureren. Dit voorkomt dat er een grote lijst met alerts komt.

Sommige Management Packs zijn ook heel gevoelig. Om dit naar eigen wensen te configureren, kan een Management Pack overschreven worden of een nieuw Management Pack aangemaakt worden.

In een eigen Management Pack kan een gepersonaliseerd dashboard, een event view of andere items gemaakt worden om de gegevens te visualiseren.

3.2.3 Conclusie configuratie

PRTG kan snel en eenvoudig gebruikt worden om verschillende onderdelen te monitoren. De rondleiding in het begin laat de belangrijkste onderdelen zien waardoor onmiddellijk de werking van de tool duidelijk wordt. Er kan ook voor gekozen worden om automatisch onderdelen te ontdekken.

Dit is anders bij SCOM, om met SCOM te werken moet er onderzoek gedaan worden hoe de tool gebruikt moet worden. Zelfs om basic Windows services te monitoren is het nodig om te onderzoeken hoe het werkt. In de Operations Manager console wordt er veel weergegeven. Als nieuwe gebruiker is het dan ook belangrijk dat er geweten is wat de tool allemaal kan doen en waar dit geconfigureerd kan worden. Hiervoor is er helaas training nodig.

Eens er geweten is hoe alles geconfigureerd moet worden en waar alles gevonden kan worden is het een handige monitoring-tool.

SCOM kan aangepast worden zodat enkel het nodige getoond wordt. Dit kan door zelf Management Packs te maken met eigen alerts views, event views, state view en meer. Of door instellingen te overschrijven.

3.3 Gebruikservaring

In dit onderdeel wordt de algemene ervaring met de twee tools besproken.

3.3.1 PRTG

PRTG is een aangename tool om mee te werken. Doordat onderdelen automatisch gevonden kunnen worden en omdat er suggesties voor sensoren worden aangeboden, is er niet veel configuratie nodig.

De meldingen van PRTG zijn ook duidelijk, PRTG heeft drie soorten meldingen: *up*, *down* en *warning*. Deze worden weergegeven in de kleuren groen, rood en geel.

Ook de dashboards tonen de nodige gegevens en zorgen voor een beter visueel beeld.

3.3.1.1 Voordelen

PRTG kan snel gebruikt worden en er is bijna geen training voor nodig. Door de rondleiding worden de belangrijkste onderdelen uitgelegd. Verder kan PRTG toestellen automatisch ontdekken waardoor er minder configuratiewerk is. Ook bij het toevoegen van sensoren kan er gebruikgemaakt worden van de aanbevolen sensoren. PRTG kan voor elk toestel een aanbeveling doen van sensoren die bij het toestel passen.

Voor elk toestel kan er ook gekozen worden hoeveel sensoren gebruikt moeten worden. Voor sommige toestellen is het al voldoende om te weten of het toestel beschikbaar is. Hierdoor kunnen extra sensoren gebruikt worden voor toestellen die meer onderdelen gemonitord moeten hebben.

3.3.1.2 Nadelen

Als er met PRTG gewerkt wordt is het belangrijk dat er geweten is wat er gemonitord moet worden op welk systeem. Er wordt een bepaalde hoeveelheid aan sensoren aangekocht, hierdoor moet er gekeken worden om de sensoren zo te verdelen zodat de belangrijkste onderdelen gemonitord worden.

3.3.2 SCOM

SCOM biedt veel mogelijkheden. In het begin is het even zoeken naar hoe de tool gebruikt moet worden. Vanaf het moment dat er geweten is hoe de tool gebruikt moet worden, is het een handige tool.

SCOM zorgt ervoor dat meldingen weergegeven worden in verschillende vormen: kritieke meldingen, waarschuwingen en meldingen voor gezonde toestellen of applicaties.

Als alles goed is wordt dit weergegeven door een groene cirkel met een groen vinkje in. Waarschuwingen worden weergegeven door een gele driehoek met een zwart uitroepteken in en kritieke meldingen worden weergegeven door een rode cirkel met een wit kruis in. Het is ook mogelijk dat deze onderdelen niet gekleurd zijn, dit wil zeggen dat ze niet gemonitord worden.

3.3.2.1 Voordelen

SCOM is een uitgebreide monitoring-tool. De tool kan aangepast worden zodat de nodige gegevens getoond worden. Er zijn ook veel Management Packs beschikbaar die voor verschillende systemen beschikbaar zijn.

Veel kan ook aangepast worden zodat de nodige informatie snel getoond kan worden. Dit kan door eigen Management Packs te maken en instellingen te overschrijven. Verder kunnen er ook aangepaste dashboards gemaakt worden met verschillende widgets.

Er zijn ook tasks voorzien waardoor een Windows toestel snel benaderd kan worden. Zo kan er bijvoorbeeld snel een ping commando verzonden worden of een Remote Desktop geopend worden naar een toestel dat gemonitord wordt.

3.3.2.2 Nadelen

Er is training nodig om met SCOM te kunnen werken. Er zijn veel configuratiemogelijkheden maar het is niet altijd duidelijk waar iets geconfigureerd moet worden.

Sommige Management Packs zijn heel gevoelig, dit zorgt ervoor dat er veel meldingen komen die minder belangrijk zijn. Dit kan wel opgelost worden door het Management Pack te overschrijven.

4 Conclusie

In dit onderzoek is er gezocht naar welke monitoring-tool het meest geschikt is voor *end-to-end* monitoring in een Windows-omgeving.

Er zijn veel monitoring-tools beschikbaar op de markt. Elke tool heeft andere functionaliteiten en een andere werking. Dit zorgt ervoor dat niet elke tool even geschikt is voor elk bedrijf. Veel tools lijken op het eerste zicht op elkaar maar als de tool verder onderzocht wordt, worden de verschillen duidelijk.

De meest geschikte monitoring-tool is dus afhankelijk van de eisen van een bedrijf. De tools die in dit onderzoek bekeken zijn, kunnen voor andere bedrijven een ander resultaten geven. Het is dus belangrijk dat de eisen duidelijk zijn. Met die eisen kunnen dan de verschillende tools gezocht en vergeleken worden.

Sommige tools leggen meer de nadruk op het monitoren van netwerken terwijl andere tools beter zijn in het monitoren van applicaties.

De manier van hoe de tool wordt aangeboden is ook belangrijk. Sommige tools worden enkel aangeboden als SaaS: om de tool te gebruiken is er dus een connectie nodig met het internet.

Wat ook een rol kan spelen bij de keuze voor een tool is de manier waarop de gegevens verzameld moeten worden. Sommige tools werken enkel met *agents* terwijl andere tools enkel *agentless* werken of een combinatie van beide.

Ook de prijs kan een belangrijke rol spelen. Hoeveel is een bedrijf bereid om te betalen voor een tool met bepaalde functionaliteiten en wat met de prijs als er meer toestellen of applicaties bijkomen? Dit zijn allemaal vragen waarmee rekening gehouden moet worden.

Een tool wordt dus niet zomaar gekozen. Het is dus belangrijk dat het bedrijf weet wat nodig is om de juiste tool te kiezen.

Omdat geen enkele tool compleet is, en om zoveel mogelijk te kunnen monitoren is er gekozen om te werken met een combinatie van twee tools.

Doordat er met meerdere tools gewerkt wordt moeten de taken verdeeld worden. Verder is het ook belangrijk dat alles goed geconfigureerd wordt. Als hier niet naar gekeken wordt kan het zijn dat er veel onnodige meldingen gestuurd worden waardoor het niet overzichtelijk is.

Bibliografie

[1] Datadog, „Datadog Docs,” Datadog Inc., [Online]. Available: https://docs.datadoghq.com/. [Geopend 20 februari 2019].

[2] C. Branagan, „Datadoghq,” Datadog Inc., 21 april 2015. [Online]. Available: https://www.datadoghq.com/blog/cluster-level-service-monitoring/. [Geopend 27 februari 2019].

[3] „G2,” G2, [Online]. Available: https://www.g2.com/products/datadog/reviews. [Geopend 1 april 2019].

[4] „GetApp,” GetApp, [Online]. Available: https://www.getapp.nl/reviews/91489/datadog. [Geopend 1 april 2019].

[5] „TrustRadius,” TrustRadius, [Online]. Available: https://www.trustradius.com/products/datadog/reviews. [Geopend 1 april 2019].

[6] „Capterra,” Capterra, [Online]. Available: https://www.capterra.com/p/135453/Datadog-Cloud-Monitoring/. [Geopend 8 april 2019].

[7] Datadog Inc., „DataDog support,” DataDog, [Online]. Available: https://www.datadoghq.com/support/. [Geopend 26 februari 2019].

[8] zapier, „zapier,” zapier, [Online]. Available: https://zapier.com/apps/datadog/integrations/office-365. [Geopend 06 mei 2019].

[9] eG Enterprise, „eG Enterprise,” eG Enterprise, [Online]. Available: https://www.eginnovations.com. [Geopend 15 april 2019].

[10] eG Innovations, „eG Innovations,” eG Innovations, [Online]. Available: https://docs.eginnovations.com/eG_Enterprise_Documentation.htm. [Geopend 15 april 2019].

[11] „Capterra,” Capterra, [Online]. Available: https://www.capterra.com/p/131785/eG-Enterprise/. [Geopend 27 maart 2019].

[12] „IT Central Station,” IT Central Station, [Online]. Available: https://www.itcentralstation.com/products/eg-enterprise-reviews. [Geopend 27 maart 2019].

[13] „Gartner peer insights,” Gartner , [Online]. Available: https://www.gartner.com/reviews/market/apm/vendor/eg-innovations/product/eg-enterprise. [Geopend 27 maart 2019].

[14] R. Monaghan, „RORYMON,” 3 september 2018. [Online]. Available: https://www.rorymon.com/blog/review-eg-enterprise/. [Geopend 27 maart 2019].

[15] elastic, „elastic,” elastic, [Online]. Available: https://www.elastic.co/elk-stack. [Geopend 19 april 2019].

[16] „Gartner peerins ights,” Gartner peerins ights, [Online]. Available: https://www.gartner.com/reviews/market/security-information-event-management/vendor/elasticsearch. [Geopend 28 maart 2019].

[17] D. Berman, 20 december 2018. [Online]. Available: https://logz.io/learn/complete-guide-elk-stack/. [Geopend 28 maart 2019].

[18] „capterra,” capterra, [Online]. Available: https://www.capterra.com/p/149304/Elasticsearch/. [Geopend 23 april 2019].

[19] Grafana Labs, „Grafana Labs,” Grafana Labs, [Online]. Available: https://grafana.com/. [Geopend 2 april 2019].

[20] „OverOps Blog,” OverOps Blog, [Online]. Available: https://blog.overops.com/production-tools-guide/visualization-and-metrics/. [Geopend 28 maart 2019].

[21] „featured customers,” featured customers, [Online]. Available: https://www.featuredcustomers.com/vendor/grafana. [Geopend 28 maart 2019].

[22] „G2,” G2, [Online]. Available: https://www.g2.com/products/grafana/reviews. [Geopend 28 maart 2019].

[23] Microsoft, „docs Microsoft,” Microsoft, [Online]. Available: https://docs.microsoft.com/en-us/system-center/scom/?view=sc-om-2019. [Geopend 19 april 2019].

[24] Microsoft, „how to buy System Center,” Microsoft, [Online]. Available: https://www.microsoft.com/en-us/cloud-platform/system-center-pricing. [Geopend 12 maart 2019].

[25] „Capterra,” Capterra, [Online]. Available: https://www.capterra.com/p/70929/System-Center/. [Geopend 29 maart 2019].

[26] „TrustRadius,” TrustRadius, [Online]. Available: https://www.trustradius.com/products/system-center-operations-manager/reviews?lu=3. [Geopend 29 maart 2019].

[27] „Gartner peerinsights,” Gartner peerinsights, [Online]. Available: https://www.gartner.com/reviews/market/apm/vendor/microsoft. [Geopend 29 maart 2019].

[28] „G2,” G2, [Online]. Available: https://www.g2.com/products/microsoft-system-center/reviews. [Geopend 29 maart 2019].

[29] M. Wilson, „PC & Network Downloads,” 12 december 2018. [Online]. Available: https://www.pcwdld.com/prtg-vs-scom-comparison. [Geopend 30 april 2019].

[30] NetXMS, „NetXMS,” NetXMS, [Online]. Available: https://www.netxms.org/. [Geopend 15 april 2019].

[31] S. Perschke, „Computerworld,” Computerworld, 22 januari 2019. [Online]. Available: https://www.computerworld.com.au/article/656564/review-4-open-source-network-management-tools-improve-usability-performance/. [Geopend 2 april 2019].

[32] A. W., „Skyose,” Skyose, 25 november 2018. [Online]. Available: https://skyose.com/full-netxms-open-source-monitoring-system-review-all-you-need-to-know-about-netxms-open-source-monitoring-system/. [Geopend 2 april 2019].

[33] New Relic, „New Relic,” New Relic, [Online]. Available: https://newrelic.com/. [Geopend 20 maart 2019].

[34] „New Relic discuss,” New Relic, [Online]. Available: https://discuss.newrelic.com/. [Geopend 3 april 2019].

[35] „TrustRadius,” TrustRadius, [Online]. Available: https://www.trustradius.com/products/new-relic/reviews. [Geopend 3 april 2019].

[36] „GetApp,” GetApp, [Online]. Available: https://www.getapp.com/it-management-software/a/new-relic/reviews/. [Geopend 2 april 2019].

[37] „FinancesOnline,” FinancesOnline, [Online]. Available: https://reviews.financesonline.com/p/new-relic/#user-review. [Geopend 2 april 2019].

[38] W. Rash, „PCMag,” PCMag, 16 april 2018. [Online]. Available: https://www.pcmag.com/review/360178/new-relic-infrastructure. [Geopend 2 april 2019].

[39] PAESSLER, „PAESSLER,” PAESSLER, [Online]. Available: https://www.paessler.com/prtg?utm_source=google&utm_medium=cpc&utm_campaign=BEL_EN_Search-Brand_broad_1&utm_adgroup=prtg&utm_adnum=90697957582&utm_keyword=%2Bprtg&utm_device=c&utm_position=1t1&utm_campaignid=277659142&utm_adgroupid=17746830982&utm_targeti. [Geopend 8 april 2019].

[40] „Spiceworks,” Spiceworks, [Online]. Available: https://community.spiceworks.com/products/15779-paessler-prtg-network-monitor. [Geopend 3 april 2019].

[41] „Trustpilot,” Trustpilot, [Online]. Available: https://www.trustpilot.com/review/paessler.com. [Geopend 3 april 2019].

[42] „Capterra,” Capterra, [Online]. Available: https://www.capterra.com/p/21581/PRTG-Network-Monitor/. [Geopend 3 april 2019].

[43] „G2,” G2, [Online]. Available: https://www.g2.com/products/prtg/reviews. [Geopend 3 april 2019].

[44] „Gartner peerinsights,” Gartner peerinsights, [Online]. Available: https://www.gartner.com/reviews/market/it-infrastructure-monitoring-tools/vendor/paessler. [Geopend 3 april 2019].

[45] Splunk, „Splunk,” Splunk, [Online]. Available: https://www.splunk.com/. [Geopend 25 maart 2018].

[46] „TrustRadius,” TrustRadius, [Online]. Available: https://www.trustradius.com/products/splunk-enterprise/reviews/pros-and-cons?f=25. [Geopend 4 april 2019].

[47] „Gartner peer insights,” Gartner peer insights, [Online]. Available: https://www.gartner.com/reviews/market/security-information-event-management/vendor/splunk?months=12. [Geopend 4 april 2019].

[48] „G2,” G2, [Online]. Available: https://www.g2.com/products/splunk-enterprise/reviews. [Geopend 4 april 2019].

[49] „Software Advice,” Software Advice, [Online]. Available: https://www.softwareadvice.com/bi/splunk-enterprise-profile/. [Geopend 4 april 2019].

[50] „Spiceworks,” Spiceworks, [Online]. Available: https://community.spiceworks.com/products/31136-splunk-enterprise. [Geopend 4 april 2019].

[51] ipswitch, „ipswitch,” ipswitch, [Online]. Available: https://www.whatsupgold.com/. [Geopend 9 april 2019].

[52] ipswitch, „ipswitch documentation,” ipswitch, [Online]. Available: https://docs.ipswitch.com/. [Geopend 20 maart 2019].

[53] „Spiceworks,” Spiceworks, [Online]. Available: https://community.spiceworks.com/products/22602-whatsup-gold. [Geopend 27 maart 2019].

[54] „Capterra,” Capterra, [Online]. Available: https://www.capterra.com/p/96050/WhatsUp-Gold/. [Geopend 27 maart 2019].

[55] „G2,” G2, [Online]. Available: https://www.g2.com/products/ipswitch-whatsup-gold/reviews. [Geopend 27 maart 2019].

[56] „Gartner peer insights,” Gartner, [Online]. Available: https://www.gartner.com/reviews/market/npm/vendor/ipswitch?pid=10745. [Geopend 27 maart 2019].

[57] „TrustRadius,” TrustRadius, [Online]. Available: https://www.trustradius.com/products/whatsup-gold/reviews. [Geopend 27 maart 2019].

Bijlage

A. Overzicht lagen Microsoft SQL-server in eG Enterprise

A. Overzicht lagen Microsoft SQL-server in eG Enterprise

Database Service Monitoring	Is the database server available for servicing requests?
	What is the response time for a typical query?
	How many logins/logouts are happening on the SQL server?
	Which applications/users are accessing the SQL server and what is their respective resource usage?
	What queries are each of the applications currently executing?
Database Server Engine Monitoring	What is the CPU utilization of the database server engine?
	How much time is the SQL server spending on processing vs. I/O?
	What is the typical workload on the database server?
	Which databases are imposing most load on the database server engine?
	How many processes are running, and what queries are they executing?
	Which user(s) are executing these queries?
Lock Activity Monitoring	What is the typical locking activity on the database?
	Which processes are being blocked and by whom?
	Which are the root-blocker processes, and what queries are they executing?
	Are any deadlocks happening?
Database Activity and Space Monitoring	What databases are hosted on the SQL server?
	Is any of the databases reaching capacity?
	Which of the databases is seeing more transaction activity?
	How many active transactions are currently happening to each of the database server?
SQL Memory Monitoring	Is there sufficient memory available for the SQL server?

	How much memory is the server consuming and how much is it willing to consume?
	How much memory is used for connections, how much for locks, and how much for query optimizations?
	What is the server's cache hit ratio?
	How many pages are available in the server's buffer pool?
	How many of these are free pages?
Operating System Monitoring	Is there sufficient disk capacity?
	Is there excessive contention for CPU or memory resources?
	Are the disks unusually busy?
	Which processes are taking up most resources (CPU, memory, disk, etc.)?