Whitepaper Nagios

Inleiding.

Het bedrijfsleven stelt steeds hogere eisen aan de ICT-infrastructuur, vanwege de veranderende werkomstandigheden: 24-uurs economie, het nieuwe werken. Kortom de ICT-infrastructuur moet meer dan vroeger altijd beschikbaar zijn en uitstekend presteren. Tevens worden deze omgevingen steeds complexer: combinatie bedraad/draadloos, naast on premise applicaties ook cloud oplossingen. En daarnaast worden de middelen om de omgeving te beheren steeds kleiner: lagere budgetten, minder FTE.

Dit alles leidt ertoe dat we moeten gaan zorgen dat het beheer efficiënter uitgevoerd wordt en de beschikbaarheid zo hoog mogelijk houden. Met behulp van trendanalyse en gerichte monitoring van de ICT-infrastructuur kan deze doelstelling worden behaald.

Monitoring met Nagios.

Door de proactieve monitoring met de producten van Nagios kan er voldaan worden aan de hoge eisen die gesteld worden aan de beschikbaarheid van de ICT-infrastructuur. Door middel van Nagios XI of Nagios Core kunnen er maatregelen genomen worden voordat er problemen ontstaan. Door middel van trendanalyse en op voorhand geschatte verwachtingen kunnen metingen worden uitgevoerd. De kracht van Nagios XI en Nagios Core zit hem in het feit dat er op vastgestelde tijden een controle wordt uitgevoerd. Deze controle kan variëren van het meten van de gebruikte diskcapaciteit tot de controle of een proces nog functioneert. Op deze manier is eigenlijk alles wat door een geautomatiseerd proces is uit te lezen ook te monitoren. Daarnaast kan Nagios hierover rapporteren. Dat kan door middel van een mail, sms of door een script te laten uitvoeren waardoor er een ticket wordt aangemaakt.

Door de juiste manier van monitoring kunnen er een aantal business doelstellingen verbeterd worden. Zo kan een eventuele uitval van de ICT-infrastructuur tot een minimum beperkt worden door op de juiste componenten te monitoren en hierdoor het daadwerkelijke probleem sneller vast te kunnen stellen. Daarmee wordt de productiviteit en efficiëntie verhoogt.

Voor ICT binnen de organisatie biedt het monitoren ook grote voordelen. Door performance data vast te leggen is er in verloop van tijd een verbeterde capaciteitsplanning mogelijk. Door inzichtelijk te hebben wat de gemiddelde groei is van datastromen of de groei van data op de storage omgeving, is er beter een inschatting te maken hoe lang de huidige omgeving nog volstaat. Hiermee is het ook mogelijk iets te kunnen zeggen over de performance van de huidige omgeving.

Nagios kan alle systemen waaronder Microsoft, Linux en Unix servers monitoren. Applicatie en keten monitoring kunnen eenvoudig worden toepast binnen Nagios waarmee Nagios een totaal proactieve monitoring oplossing is voor het monitoren op alle vlakken binnen uw organisatie.

Hoe kunnen we monitoren.

Er zijn verschillende manieren waarop een systeem kan worden gemonitord. Er kunnen actieve of passieve checks zijn binnen Nagios waarmee de status van een systeem wordt weergegeven. Bij een actieve check wordt er door Nagios op een vooraf ingestelde tijd een script gestart welke de status van een systeem controleert. Bij een passieve check wordt er vanuit het systeem een bericht gestuurd wat de huidige status van het systeem is. Ook kunnen passieve checks gebruikt worden om snmptraps van een systeem weer te geven. Dit houdt in dat als een systeem een snmptrap verstuurd, deze afgevangen wordt door het Nagios systeem en omgezet wordt in een leesbare statusupdate.

Actief of Passief?

Voorbeelden voor passieve checks kunnen zijn dat er aan het einde van een systeem backup een melding wordt gestuurd naar de Nagios server of de backup succesvol verlopen is. Aangezien het tijdstip dat de backup afgelopen is niet vooraf bekend is, is het handiger om deze melding vanuit het systeem te versturen dan een controleslag uit te voeren vanuit de Nagios server.

Standaard wordt er meer gebruik gemaakt van actieve checks waarbij gecontroleerd wordt of een database server nog naar behoren functioneert. Er is echter nog wel een verschil of de database wel draait, maar niet meer reageert, of dat de database helemaal niet meer draait en daarom niet reageert. Ook zou het nog kunnen zijn dat de database server niet meer bereikbaar is. Onder de streep hetzelfde probleem, maar de oplossing ligt misschien bij een ander persoon of zelfs beheer team.

Afhankelijkheden.

Door voor meerdere, totaal verschillende, problemen dezelfde notificatie te kunnen krijgen wordt het duidelijk dat afhankelijkheden erg belangrijk zijn. Als een switch is uitgevallen is het logisch dat de systemen achter deze switch ook niet meer bereikbaar zijn. Een alert dat de switch niet meer bereikbaar is volstaat dan. Ook op een server is dit toepasbaar. Als een database server niet meer draait (het proces draait niet meer) hoeft er geen controle te worden gedaan of er vanaf een ander systeem nog verbonden kan worden met deze database server.

Is er nog meer?

Naast het monitoren van systemen en componenten, kan het belang van loganalyse en security traps een onderdeel uitmaken van het in kaart brengen van de ICT-infrastructuur. Met behulp van log analyse kan worden gezien dat systemen bezig zijn om valse inlog pogingen of oneigenlijke aanvragen naar een server. Door gebruik te maken van de Nagios Logserver kunnen dit soort problemen opgemerkt worden en kan hier ook een alert voor worden gegenereerd. Ook kan door het afvangen van snmptraps security issues worden gezien. Veel (netwerk)devices hebben de mogelijkheid een snmptrap te sturen op het moment dat deze niet juiste inlogpogingen of oneigenlijk gedrag detecteren.

Wat is er aan de hand?

Naast een waarschuwing te krijgen van problemen in de ICT-infrastructuur, is het ook van belang te weten wat er gaande is. Hoe fijn is het om te weten waarom je een extra investering zou moeten doen voor extra bandbreedte voor de internetverbinding. Of een onderbouwde reden kunnen geven waarom de netwerk upgrade wel of misschien nog helemaal niet noodzakelijk is. Of eindelijk aan kunnen geven waarom de VoIP oplossing niet helemaal naar wens functioneert. Door een Nagios Network Analyser in te zetten worden veel van deze problemen heel snel te verklaren.

Tot slot.

Door monitoring op de juiste manier te implementeren kunnen de volgende zaken worden bereikt:

- Meer efficiëntie door behulp van trendanalyse niet met brandjes blussen bezig te zijn, maar op voorhand problemen voorkomen.
- Grotere beschikbaarheid door tijdige detectie van problemen.
- Weer een stap dichterbij een veilige ICT-infrastructuur
- Gedegen onderzoek voor nieuwe investeringen