hupra

Managed Services

Proactief beheer bij Hupra

M.M.J. de Weijer
28 mei 2012
Versie: 1.0

Hogeschool Utrecht
Systeembeheer

Managed Services

Proactief beheer bij Hupra

Auteur:
M.M.J. de Weijer
Studentnummer: 1546128
Hogeschool Utrecht
Faculteit Natuur & Techniek
Systeembeheer

Bedrijf:
Hupra Automatisering
Hoofdstraat 105
3901 AK Veenendaal

Begeleiders:
Hupra: Dhr. P.A. Willemsen
Hogeschool Utrecht: Dhr. H. van Nimwegen

Afstudeerperiode:
februari 2012 - juni 2012

Versie: 1.0
Datum: 28 mei 2012

Versie beheer:

Versie	Datum	Wijzigingen
0.0	27-03-2012	Initiële versie document, geen inhoud
0.1	01-05-2012	Wijzigingen in opmaak hoofdstukken, inhoudelijke invulling hoofdstukken 2 t/m 8
0.2	20-05-2012	Conclusie toevoegen, feedback van dhr. van Nimwegen verwerkt, opmaak, management samenvatting
0.3	24-05-2012	Aanpassen opmaak, verwerken feedback op hoofdstuk 5
0.4	26-05-2012	Verwerken laatste feedback, evaluatie procesgang, controleren verwijzingen
1.0	28-05-2012	Controle taalfouten, laatste wijzigingen opmaak

Voorwoord

Veenendaal, 28 mei 2012

Geachte lezer,

Voor u ligt mijn scriptie ‘Managed Services’. In deze scriptie wil ik u een beeld geven van de aanpak, uitgevoerde werkzaamheden en resultaten van het onderzoek naar Managed Services (Proactief beheer) bij Hupra.

Het onderzoek beschrijft en adviseert Hupra in de mogelijkheden en inzet van Managed Services ter verbetering van de dienstverlening en werkwijze. Dit onderzoek is gevolgd door een daadwerkelijke implementatie van de bevindingen. Bij afronding van dit project is er dus niet alleen een advies uitgebracht, maar is ook een omgeving gecreëerd waarmee Hupra direct kan werken en op verder kan bouwen.

Tijdens dit project ben ik geholpen en gesteund door een aantal mensen, welke mij adviezen en feedback hebben gegeven, een andere blik op het project hebben geworpen, of hebben ondersteund in de taalkundige verbetering van de documenten. Hiervoor wil ik de volgende personen bedanken:

Dhr. P.A. Willemsen – Voor het aanbieden van een afstudeerplek en de ondersteuning en het vertrouwen bij de uitvoering hiervan.

Dhr. H. van Nimwegen – Voor de uitgebreide feedback en de ondersteuning vanuit de Hogeschool Utrecht.

Dhr. C. van Westen – Voor de vele commerciële adviezen en gesprekken, welke een andere dimensie aan het project hebben gegeven.

Mevr. J.B.E. de Weijer – Voor het controleren van de documenten op spel- en grammaticafouten.

Ik hoop dat u deze scriptie met veel interesse zult lezen.

Mike de Weijer

Samenvatting

Door het groeiende aantal klanten en de drang om iets extra's te bieden wil Hupra af van het chaotische reactieve beheer bij haar klanten. Door sneller problemen in de ICT van de klant te ontdekken en deze eerder op te lossen dan voorheen het geval was, kan Hupra een sterkere concurrerende positie innemen. Bovendien wil Hupra met de inzet van Managed Services (proactief beheer) meer rust binnen de organisatie creëren, zodat er meer tijd overblijft voor innovatie en een algehele verbetering van de dienstverlening.

De opdracht bestaat uit een onderzoek, ontwerp en een implementatie van proactief beheer en procedures m.b.t. nieuwe werkwijzen. De stap naar Managed Services moet uiteindelijk bijdragen aan de volgende doelstellingen (aangeduid over 1 jaar):

- onderscheidend vermogen Hupra;
- kosten terugdringen (aantal facturabele uren verhogen met 20%);
- klantwerving (25+ klanten in het proactieve model);
- verlaging werkdruk (terugdringen break-fix werkzaamheden van 99% naar 50%);
- betrouwbaarheid dienstverlening/ ICT van de klant (van ±90% naar 99% beschikbaarheid);
- automatisering terugkomend onderhoud (van 0% naar 10-20%).

Managed Service Providers (MSP's) kunnen ingedeeld worden in een volwassenheidsmodel. Dit model kent 5 niveaus. Op dit moment bevinden de meeste activiteiten van Hupra zich in de fases 'break-fix' (niveau 1) en 'responsive' (niveau 2). Het uiteindelijke doel van Hupra is deze werkzaamheden te verschuiven naar de fases 'proactive' (niveau 3) en 'managed' (niveau 4).

Om dit te bereiken kunnen vier mogelijke scenario's worden gevolgd: vasthouden aan huidig model, inzetten van monitoring, implementatie proactief model en een totale aanpak van zowel het inzetten van het model als het implementeren van een software pakket. Dit laatste zal de enige mogelijkheid zijn om door te groeien in het volwassenheidsmodel.

Hoewel de markt voor monitoring pakketten groot is en veel verschillende soorten en maten oplossing worden geboden, is in vergelijking de markt voor echte MSP tools erg klein. Na een snelle inventarisatie te hebben uitgevoerd, bleek al snel dat er maar 3 producten zijn welke de moeite waard zijn om verder te onderzoeken. Dat waren N-central, Kaseya en GFI Max.

In open interviews en vergaderingen met werknemers is getracht zoveel mogelijk informatie over de verwachtingen van het proactieve model en de software boven water te krijgen. Deze vergaderingen en interviews zijn gehouden onder medewerkers van verschillende disciplines. Resultaten en conclusies zijn samengevat en gebruikt bij de productkeuze.

Onderzoek naar de genoemde pakketten heeft vooral plaats gevonden in de vorm van een document onderzoek. Informatie is verkregen van internetbronnen en de leveranciers. Op basis van deze informatie zijn de producten vergeleken. Al snel bleek GFI Max af te vallen. De verschillen tussen Kaseya en N-central zijn minimaal. De invulling van de functies wil nog wel eens verschillen. Hiervoor zijn de producten met elkaar vergeleken en zijn cijfers en weging toegekend aan de verschillende functies.

Tabel 1: Product vergelijking

	N-Central	Kaseya	GFI MAX Remote Management
Totaal	104 / 70,4	104 / 65,5	53 / 34,0
Gemiddelde	**4,3 / 2,9**	**4,2 / 2,6**	**4,1 / 2,6**

Deze weging is verkregen na overleg met de opdrachtgever en de overige betrokkenen. De toekenning van de cijfers is gebaseerd op de uitwerking van een functie en de tests met de trial versies. Daarnaast is er een financiële vergelijking uitgevoerd, naar inschatting van de benodigde licenties. Na bovenstaande productvergelijkingen en rekening houdende met in hoofdstuk 5 vastgestelde eisen en wensen van Hupra, is te adviseren gebruik te gaan maken van N-central.

Tabel 2: Verwachte kosten N-central

Eenmalig (eerste jaar)	Terugkomend vanaf jaar 2 (per jaar)	Totaal (na 24 maanden)
€ 18.438,-	€ 3.880,-	€ 22.318,-

Na de productkeuze zijn er adviezen uitgebracht over de productconfiguratie, de procedures en het beheerproces. Deze zijn gebaseerd op een aantal tests. Er zijn adviezen opgesteld voor de omgeving en infrastructuur, maar ook voor configuratie van productfuncties.

Naast de productconfiguratie zijn adviezen opgenomen over de op te stellen procedures ter ondersteuning van de nieuwe MSP software en het stroomlijnen van de werkzaamheden. Deze processen zijn ingedeeld naar een ITIL model. Volledige implementatie van ITIL is afgeraden. Gezien de grote van Hupra is dit niet relevant en zal negatief werken voor de flexibiliteit van de organisatie.

Deze adviezen zijn vervolgens getest in een speciaal ontworpen testomgeving en vervolgens in de productie omgeving geïmplementeerd. De testomgeving is zo natuurgetrouw mogelijk en bestaat uit een aantal servers met daarop een typische MKB omgeving. Voor tests welke verder ontwikkeld zijn is het lokale netwerk van Hupra gebruikt. Veilige tests, zonder enige risico voor de omgeving, zijn door gezet naar een netwerk van een klant voor verdere tests, alvorens deze daar te implementeren. De testomgeving zal naast de productie omgeving blijven bestaan voor mogelijke tests in de toekomst bij nieuwe functies of wijzigingen in de configuratie.

Na anderhalve maand regelmatig te werken met de productie omgeving, worden langzaamaan wat verschillen merkbaar. Er zijn na implementatie 10 van de 50 klanten in het systeem geregistreerd. Hierdoor wordt er meer werk uit het systeem gehaald. Het aantal facturabele uren loopt op van gemiddeld 20 naar 22 uren per beheerder. Op dit moment bestaat 10% van de werkzaamheden uit taken afkomstig van het nieuwe proactieve model en is te zien dat bijna 40% van het onderhoud geautomatiseerd verloopt via N-central. Als Hupra deze lijn blijft vasthouden zullen op de gestelde termijn van één jaar de overige doelstellingen makkelijk te halen zijn.

Het MSP model blijft een model onderhevig aan wijzigingen. Vervolgstappen voor verdere ontwikkeling zijn: het bekijken van de extra uitbreiding ‘Report Manager’ en de koppeling van N-central met een ticket systeem als AutoTask of een integratie met het bestaande pakket OFB. Verder zullen er nieuwe pakketfuncties uitkomen, welke getest zullen moeten worden en zal het nodig zijn de configuratie te blijven ontwikkelen.

De basis is er nu en met het vasthouden hieraan en het nemen van de vervolgstappen kan Hupra doorgroeien in het volwassenheidsmodel en doorontwikkelen naar het beoogde niveau 3 en in de toekomst zelfs 4 of 5. De basis voor een goed MSP pakket is geconfigureerd en geïmplementeerd. Het is nu aan Hupra om hiermee verder te gaan en dit verder te ontwikkelen.

Een doorgroei naar de hogere niveaus van het volwassenheidsmodel zal voor zowel Hupra als de klant meer zekerheid en duidelijkheid geven en zal de algehele ICT dienstverlening op een hoger niveau brengen. Met deze kwaliteit en eenvoud zal Hupra zich zeker kunnen onderscheiden op de markt.

Inhoudsopgave

1. Inleiding

Managed Services (proactief beheer) is een methode/model voor het onderhouden van de infrastructuur bij een klant. De focus bij deze werkwijze ligt op de controle van de infrastructuur, structurering van de werkzaamheden en het uiteindelijk voorkomen van storingen. Hupra (opdrachtgever) wil deze werkwijze gaan benutten ter verbetering van de huidige dienstverlening.

Hupra heeft een automatiseringsafdeling welke werkt volgens een break-fix model. In het verleden heeft dit nooit voor problemen gezorgd. Met de groei van het aantal klanten begint Hupra tegen problemen aan te lopen. Deze toename van klanten leidt vooral tot een chaotische werkwijze, een toenemende werkdruk en minder controle over de werkzaamheden. Hupra wil de controle weer terug nemen en de werkdruk verlagen, zodat meer tijd overblijft voor bijvoorbeeld innovatie. Dit moet voor Hupra een algehele verbetering van de dienstverlening gaan opbrengen.

Managed Services maakt gebruik van een software pakket voor controle van het netwerk. Alle werkzaamheden zullen worden gestart vanuit meldingen van dit pakket. Naast het monitoren van het netwerk zal het pakket ook geautomatiseerd onderhoudstaken gaan uitvoeren. De insteek van het model is het beheer te automatiseren en stroomlijnen. Dit wordt gedeeltelijk gerealiseerd met de implementatie van het software pakket en de configuratie daarvan, daarnaast zijn procedures en een andere werkwijze van belang.

Dit rapport beschrijft het onderzoek, de adviezen, en de implementatie van Managed Services binnen Hupra. Hoofdstuk 2 zal een beeld schetsen van Hupra als organisatie en geeft een algemene indruk van de omgeving waarin het project is uitgevoerd. Dit wordt gevolgd door de projectdefinitie in hoofdstuk 3. Hier worden de kaders en de doelstellingen van het project vastgelegd. Hoofdstuk 4 zal in meer detail uitleg geven over wat Managed Services inhoudt. Na een algemeen beeld te hebben gevormd van Managed Services zullen in de hoofdstukken 5 en 6 de eisen en wensen van Hupra en het productonderzoek naar aanleiding hiervan worden beschreven. In hoofdstuk 7 worden de aanbevelingen voor productkeuze en configuratie toegelicht. Daarnaast staan de aanbevelingen voor de procedures ter ondersteuning van het pakket, centraal. Er wordt afgesloten met een conclusie in hoofdstuk 9.

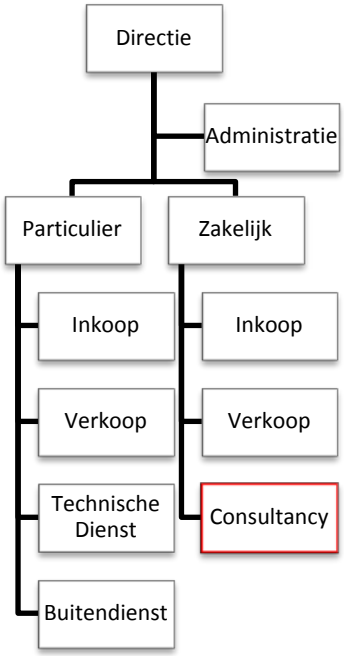
Aan dit document zijn een aantal bijlagen toegevoegd. Dit zijn onder anderen: het plan van aanpak, productonderzoek opgesteld tijdens de uitvoering van het project ter informatie van Hupra, adviesrapport met productkeuze en adviezen voor configuratie en implementatie, en een testrapport met de resultaten van de uitgevoerde tests. Informatie uit deze documenten zal ook gebruikt worden in de scriptie, voor meer details zal verwezen worden naar deze bijlagen.

Allereerst zal er gestart worden met de beschrijving van de organisatie.

2. Organisatie

Hupra is opgericht in het jaar 1980. Toen in 1981 de eerste PC op de markt werd gebracht, richtte de organisatie zich steeds meer op de ICT-dienstverlening. Hupra betrof vanuit origine een elektronicawinkel, gericht op de particuliere markt. De afgelopen jaren is de vraag naar elektronica-componenten echter sterk afgenomen en heeft Hupra besloten deze tak af te stoten en zich volledig te richten op computers, laptops, randapparatuur en reparaties. Naast deze winkel, welke volledig gericht is op de particuliere klant, is Hupra vanaf 2001 ook gestart met de dienstverlening aan de zakelijke markt en heeft men zich gefocust op de bedrijfsautomatisering. Hupra richt zich hierbij voornamelijk op de MKB bedrijven, gezien het feit dat deze bedrijven veelal geen 'eigen' systeem- en netwerkbeheerder binnen de organisatie hebben. Met deskundig advies, hoogwaardige en snelle service en daarnaast het verzorgen van de implementatie van nieuwe apparatuur ondersteunt Hupra bedrijven met netwerkbeheer. Hupra ontzorgt de klant met bijvoorbeeld het beheren van het netwerk, de implementatie van een nieuw bedrijfsnetwerk, de installatie van nieuwe werkstations en alles op het gebied van online services en onderhoud van servers en werkstations. Hupra gaat erg servicegericht te werk. Dankzij de hoogwaardige kennis, innovatieve technieken en uitstekende service zorgt Hupra ervoor dat ICT een positieve bijdrage levert aan de werkzaamheden van haar klanten. Veel bedrijven zien Hupra dan ook als een betrouwbare partner op het gebied van ICT, voor zowel particuliere als zakelijke klanten.

Hupra is opgesplitst in een afdeling zakelijk en een afdeling particulier. De afdeling particulier richt zich op de verkoop van voornamelijk desktop systemen en randapparatuur aan particulieren. De afdeling zakelijk richt zich op implementatie en onderhoud van ICT in het MKB. De particuliere en de zakelijke tak zijn volledig los van elkaar te beschouwen, hoewel er soms nog wel wat overloop plaats vindt. De zakelijke afdeling maakt bijvoorbeeld voor reparaties bij zakelijke klanten wel eens gebruik van de technische dienst van de afdeling particulier.



Figuur 1: Organigram

Typische klanten zijn MKB bedrijven met 2 tot 50 werkstations. Deze bedrijven worden steeds meer afhankelijk van hun ICT, echter is het voor deze bedrijven niet reëel een eigen ICT afdeling in te richten. Daarom hebben zij dus belang bij een goede ICT partner. Deze klanten bevinden zich in allerlei branches.

Als afstuderend student ben ik werkzaam geweest op de afdeling consultancy, ICT zakelijk. Op deze afdeling is ook het onderzoek uitgevoerd en heeft de uiteindelijke implementatie plaats gevonden. Voor het onderzoek en de implementatie is veel overleg geweest met de beheerders en de directeur (opdrachtgever) dhr. Willemsen. Omdat het project van toepassing is op deze afdeling is het gemakkelijk input en feedback te krijgen van collega's, welke uiteindelijk ook met het product moeten gaan werken.

3. Projectdefinitie

Na een eerste indruk te hebben gekregen van de projectomgeving en de organisatie wordt in dit hoofdstuk meer informatie gegeven over het project, de opdracht, en de aanpak hiervan. Deze informatie is afkomstig uit het plan van aanpak. Het plan van aanpak is als bijlage D aan dit document toegevoegd.

3.1. Probleemstelling

Door het groeiende aantal klanten en de drang om iets extra's te bieden, wil Hupra af van het klassieke, reactieve beheer bij klanten. Het zogenaamde "brandjes blussen", de klant belt zelf als er een probleem is. Men wil zo veel mogelijk van deze werkwijze af en over gaan naar een model voor proactief beheer. Door over te gaan naar proactief beheer wil Hupra de concurrentie het hoofd bieden en voorkomen dat men achter komt te liggen op de ontwikkelingen. Door sneller problemen in de ICT van de klant te ontdekken en deze eerder en gemakkelijker op te lossen dan voorheen het geval was, kan Hupra een sterkere concurrerende positie innemen. Bovendien wil Hupra met de inzet van proactief beheer meer rust binnen de organisatie creëren, zodat er meer tijd overblijft voor bijvoorbeeld innovatie. Men kan dus stellen dat Hupra op dit moment niet in staat is de door haar gewenste kwaliteit te bieden, omdat de focus nog teveel ligt op het reactieve beheer, waardoor weinig tijd overblijft voor innovatie en ontwikkeling.

3.2. Opdracht

De opdracht bestaat uit een onderzoek naar proactief beheer, een ontwerp van hoe dit beheer ingezet kan worden en een implementatie van proactief beheer (software en procedures m.b.t. nieuwe werkwijzen). De procedures moeten ervoor zorgen dat de software optimaal benut kan worden.

Het onderzoek moet uitwijzen wat de mogelijkheden van proactief beheer voor Hupra zijn. Wat voor methodes hiervoor toegepast kunnen worden, welke procedures moeten worden opgesteld en welke tools er ingezet moeten worden. Hupra is in het verleden door partners meerdere malen aangeraden hiervoor een Managed Service Provider (MSP) tool te gebruiken. In het onderzoek wordt deze mogelijkheid meegenomen en zal worden onderzocht wat de mogelijkheden hiervan zijn, of dit überhaupt wel de juiste oplossing is en of er eventueel nog alternatieven zijn.

Verder bestaat de opdracht uit een implementatie van de plannen voor proactief beheer binnen Hupra. Hieronder vallen zowel de implementatie van procedures m.b.t. werkwijzen als de implementatie en configuratie van ondersteunende software. Eerste indrukken van de software doen vermoeden dat de software dermate complex is dat verder onderzoek naar configuratie, best practices en fine tuning van de software nodig is om optimaal aan te kunnen sluiten bij Hupra.

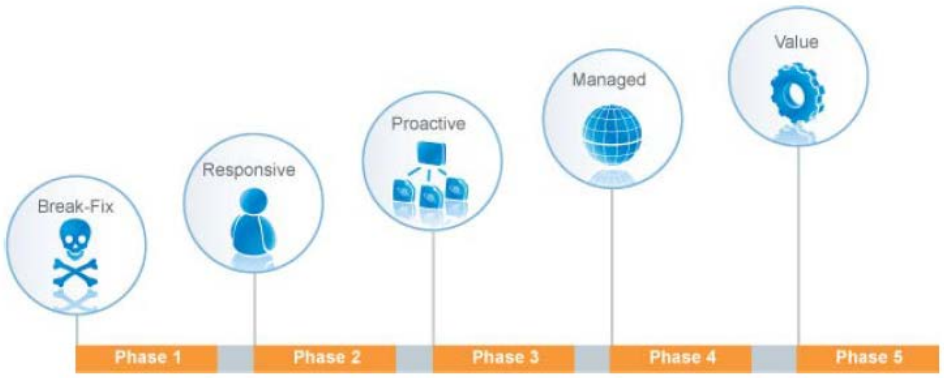
De uiteindelijke doelstelling van het project is een beheermodel waarmee Hupra proactief te werk kan gaan, de problemen tijdig kan ontdekken en de impact van de problemen kan beperken. Dit naar alle waarschijnlijkheid met behulp van een MSP pakket en ondersteunende werkprocedures. Deze doelstellingen kunnen tot het volgende worden samengevat:

- proactief beheermodel;
- advies procedures/ verantwoordelijkheden;
- implementatie/ configuratie ondersteunende software;
- inrichting beheer met ondersteunende software.

Bovenstaande moet er uiteindelijk voor zorgen dat eerder genoemde problemen worden weggenomen en wordt bijgedragen aan de uiteindelijke doelen van Hupra (aangeduid over 1 jaar):

- onderscheidend vermogen Hupra;
- kosten terugdringen (aantal facturabele uren verhogen met 20%);
- klantwerving (25+ klanten in het proactieve model);
- verlaging werkdruk (terugdringen break-fix werkzaamheden van 99% naar 50%);
- betrouwbaarheid dienstverlening/ ICT van de klant (van ±90% naar 99% beschikbaarheid);
- automatisering terugkomend onderhoud (van 0% naar 10-20%).

De werkwijze van Hupra (en ieder ander MSP) kan getoetst worden aan een MSP Maturity Model zoals weergegeven in onderstaande figuur (N-able Technologies, 2006). Op dit moment bevinden de meeste activiteiten van Hupra zich in de fases 'break-fix' en 'responsive'. Het uiteindelijke doel van Hupra is deze werkzaamheden te verschuiven naar de fases 'proactive' en 'managed'.



Figuur 2: MSP Maturity Model (N-able Technologies)

3.3. Scope

Bij de start van het project is de volgende scope gedefinieerd om te voorkomen dat teveel wordt afgeweken van de 'kern' en het behalen van de doelstellingen onmogelijk wordt. De scope bevat zowel een onderzoek naar een oplossing voor proactief beheer, als een implementatie hiervan. Hieronder zijn de onderdelen van de scope opgesomd:

- in kaart brengen wensen Hupra aan het proactieve model;
- onderzoek proactief beheer;
- onderzoek naar ondersteunende software voor proactieve werkwijze (MSP software);
- product vergelijking/advies ondersteunende software;
- advies configuratie/implementatie ondersteunende software voor proactief beheer;
- implementatie ondersteunend software pakket en procedures;
- fine tuning van de software (optimale aansluiting bij Hupra).

Daarnaast zijn er ook een aantal zaken welke niet onder de scope van het project vallen. Dit zijn bijvoorbeeld het onderzoeken van de mogelijke besparingen bij implementatie van het proactieve model, de gevolgen voor het personeelsbestand of het onderzoek naar de uiteindelijke verbetering van de marktpositie (zie doelstellingen, onderscheidend vermogen).

3.4. Aanpak

Om tot een gestructureerde aanpak te komen, is het project onderverdeeld in een aantal fases. Deze fases zorgen voor een duidelijke afbakening binnen het project en zijn bedoeld om meer grip te krijgen op het project. Het project is opgedeeld in de volgende fases:

- Fase 1: Project start
- Fase 2: Onderzoek
- Fase 3: Ontwerp
- Fase 4: Test
- Fase 5: Implementatie
- Fase 6: Project afronding

3.4.1. Fase 1: Project start

In deze fase zal al het voorbereidende werk voor het project worden verricht en zullen de planningen en project documenten worden opgesteld.

3.4.2. Fase 2: Onderzoek

In deze fase vindt het hoofdonderzoek plaats. Dit is een onderzoek naar de verschillende mogelijkheden voor proactief beheer en de verschillende beschikbare software producten. Dit onderzoek zal o.a. een productvergelijking bevatten. Verder zal onderzocht worden op welke manier dit proactief beheer het beste binnen Hupra vorm gegeven kan worden.

De onderzoeksfase betreft voornamelijk een documentonderzoek waarbij informatie wordt verzameld van artikelen op het internet, uit de literatuur en documentatie afkomstig van verschillende fabrikanten en onderzoeksbureaus. Naast inzicht in de bestaande documentatie heeft Hupra mij ook de mogelijkheid gegeven presentaties en demo's van fabrikanten bij te wonen.

Aansluitend aan deze fase zullen overleggen en vergaderingen worden gehouden met de opdrachtgever en twee werknemers van verschillende disciplines om de eisen en verwachtingen aan het project in kaart te brengen.

3.4.3. Fase 3: Ontwerp

In deze fase van het project zullen de onderzoeksresultaten worden verwerkt tot een ontwerp voor proactief beheer. Dit ontwerp is een advies over hoe om te gaan met de eindeloze hoeveelheid mogelijkheden die door een MSP pakket worden geboden en op welke manieren dit binnen Hupra kan worden gebruikt ter ondersteuning van het beheer.

De ontwerpen en adviezen voor procedures worden gedeeltelijk gebaseerd op de ITIL standaarden. Er is voor gekozen delen van de standaard te gebruiken omdat een gehele implementatie van ITIL in combinatie met proactief beheer te uitgebreid is en bovendien niet optimaal zal zijn in een kleinere organisatie als Hupra, omdat dit de flexibiliteit van de organisatie niet ten goede zal komen.

3.4.4. Fase 4-5: Test/ Implementatie

De vierde fase van het project is een testfase waarin het gekozen product (uit het productadvies) zal worden getest op een speciaal hiervoor ingerichte testomgeving. Details van deze testomgeving zijn in de ontwerpfase uitgewerkt. Vast staat dat deze omgeving een gedeeltelijke replica van de uiteindelijke productie omgeving is, welke de kritische eigenschappen van de productie omgeving moet verantwoorden.

In de testfase zal de software worden getest op mogelijke configuraties uit het 'advies proactief beheer' en zal verder detailonderzoek worden gedaan naar de functionaliteiten van het pakket. Configuraties kunnen tijdens de testfase aangepast worden indien nodig. Verder zal het product ook worden getest op stabiliteit en zal er worden gekeken naar acceptatie binnen de afdeling zakelijk. De testomgeving zal na afloop blijven bestaan om eventuele riskante wijzigingen in de productie omgeving te testen.

De vijfde fase van het project is de implementatiefase. In deze laatste fase zal de ondersteunende software worden geïmplementeerd en een werkbare omgeving worden opgeleverd. Verder zal in deze fase de implementatie van het proactieve beheer worden afgerond. De resultaten van de voorgaande fases zullen in deze laatste fase in praktijk worden gebracht. De positieve testresultaten uit fase 4 zullen in deze productie omgeving worden geïmplementeerd. De implementatiefase zal veel overlap met de testfase hebben, omdat het beter is resultaten meteen te implementeren.

3.4.5. Fase 6: Project afronding

Onder deze laatste fase van het project vallen vooral zaken als de afronding van de documentatie, kennisoverdracht aan Hupra, afronding van de scriptie en voorbereiding van de presentatie e.d.

3.5. Kwaliteitsbewaking

Het is van groot belang dat de uiteindelijke producten zullen voldoen aan de verwachtingen en de eerder gestelde doelstellingen waargemaakt kunnen worden. Daarom zijn er bij de start van het project een aantal afspraken gemaakt omtrent controle en kwaliteitsbewaking. Gedurende het project zal het volgende ondernomen worden.

Allereerst zal er iedere week een contactmoment zijn met de opdrachtgever en de begeleider. Op deze wekelijkse contactmomenten zal niet alleen de voortgang van het project aan de orde komen, maar ook hoe het staat met de producten en de kwaliteit hiervan. Op deze momenten wordt gekeken of het (concept)product op dat moment aan de verwachtingen voldoet of kan gaan voldoen; zo niet dan kon dit nog tijdig worden bijgestuurd. Deze momenten bieden ook ruimte voor feedback van de beheerders, die uiteindelijk met het product moeten werken.

4. Managed Services

In de projectdefinitie is al meerdere malen gesproken over proactief beheer of Managed Services. Twee begrippen welke door elkaar heen worden gebruikt. Voordat er verder wordt gesproken over de huidige situatie van Hupra en haar doelstellingen voor proactief beheer, wordt er eerst een hoofdstuk gewijd aan wat het proactieve beheer nu eigenlijk precies inhoud en wat de verschillen nu zijn ten opzichte van het traditionele break-fix model.

Door de enorme groei die de IT de laatste jaren heeft meegemaakt zijn veel systemen in hoeveelheid en complexiteit gegroeid. Het traditionele 'break-fix' model is in veel gevallen niet meer toereikend. Door de 'zero tolerance' mentaliteit bij bedrijven stijgt de werkdruk bij automatiseerders terwijl op rustige momenten de helft van de beheerders met de armen over elkaar zit. Door dit 'break-fix' model loopt een serviceprovider altijd achter de feiten aan. Er is geen grip en inzicht in wat de systemen doen en er is geen inschatting of planning te maken in de toekomstige werkzaamheden. Dit levert voor de service providers veel onzekerheden op. Het is bijvoorbeeld moeilijk inschattingen te maken van de verwachte inkomsten. Bovendien is de concurrentie op deze markt erg sterk en hebben serviceproviders in dit 'break-fix' model nauwelijks tot geen mogelijkheid om zich te onderscheiden van de concurrenten (N-able Technologies, 2007; The Seven Major Obstacles on the Road to Managed Services, 2007).

Om deze problemen te verminderen, zoeken veel automatiseerders de oplossingen in de techniek en schaffen een monitor pakket aan voor het monitoren van een aantal basisvereisten aan de kritieke systemen. Vaak is dit een overhaaste aanschaf en geeft het niet alle mogelijkheden om uit het 'break-fix' model te komen. Er worden zelfs combinaties van verschillende pakketten gemaakt, wat niet bijdraagt aan de eenvoud in beheer. Zelfs als deze eenvoud bereikt wordt, is het aanschaffen van software alleen niet genoeg. Om uit dit 'break-fix' model te komen zullen service providers veranderingen in hun werkwijze, marketing, sales en management moeten doorvoeren. (The Fundamentals of a Successful Managed Services Practice, 2007)

4.1. Wat is MSP/proactief beheer?

Een Managed Server Provider (MSP) verschilt van de "normale serviceprovider" of automatiseerder in die zin dat een Managed Service Provider het beheer onder controle heeft en proactief te werk kan gaan. Een MSP is in staat de mogelijke problemen bij een klant aan te zien komen en dit probleem nog voor het optreed te verhelpen of de impact hiervan te beperken zonder dat de klant hier hinder van ondervindt. Bovendien is de MSP in staat verschillende standaard beheerstaken geautomatiseerd en gecontroleerd uit te voeren. Hierbij valt bijvoorbeeld te denken aan back-up, patches, antivirus updates en standaard onderhoud. De MSP moet als het ware alle ICT zorgen bij de klant wegnemen en deze klant op een actieve wijze ondersteunen in zijn ICT. Het liefst allemaal voor een vast bedrag per maand.

Een volgende stap in dit systeem is 'ICT as a utility' aanbieden. De MSP biedt ICT aan, in welke vorm dan ook, en de klant betaalt alleen voor wat er wordt gebruikt. De klant wordt gefactureerd voor de waarde van een geleverde service en de hoeveelheid service die geleverd is, niet meer voor de besteedde tijd zoals bij het klassieke 'break-fix' model het geval was. De MSP draagt dan de

verantwoordelijkheid voor de werking van de ICT, de klant mag hier verder geen hinder van hebben. Dit wordt meestal vastgelegd in een Service Level Agreement.

Voor een automatiseerder zal een proactief model voor meer overzicht zorgen en moet een toekomstig MSP in staat stellen werkzaamheden gestructureerd in te plannen. Bovendien zal een proactief model gepaard gaan met bijbehorend service level agreement wat de MSP een zekerheid geeft van haar inkomsten. De voordelen voor de MSP zullen vooral te vinden zijn in werkdruk verlaging en zekerheid. Daarnaast zullen ook een aantal praktische besparingen worden bereikt. Zo zal het minder vaak voorkomen dat een beheerder naar een klant op locatie moet. Dit spaart reistijd en reiskosten uit. Bovendien zal er meer “rust” en ruimte ontstaan om de relaties met de klanten te verbeteren.

Voordelen voor klanten zijn onder andere het zorgeloos gebruik maken van de ICT omgeving en voor een vast bedrag per maand verzekerd zijn van goed en zorgvuldig onderhoud op de ICT omgeving. De klant heeft een SLA afgesloten met de MSP en kan er op vertrouwen dat zijn ICT in goede handen is bij de MSP. De klant zal minder in aanraking komen met problemen omdat deze door de MSP tijdig worden opgemerkt en worden verholpen. Mocht de klant in aanraking komen met een probleem dan zal dit zijn omdat de MSP de klant hiervan op de hoogte stelt, niet andersom.

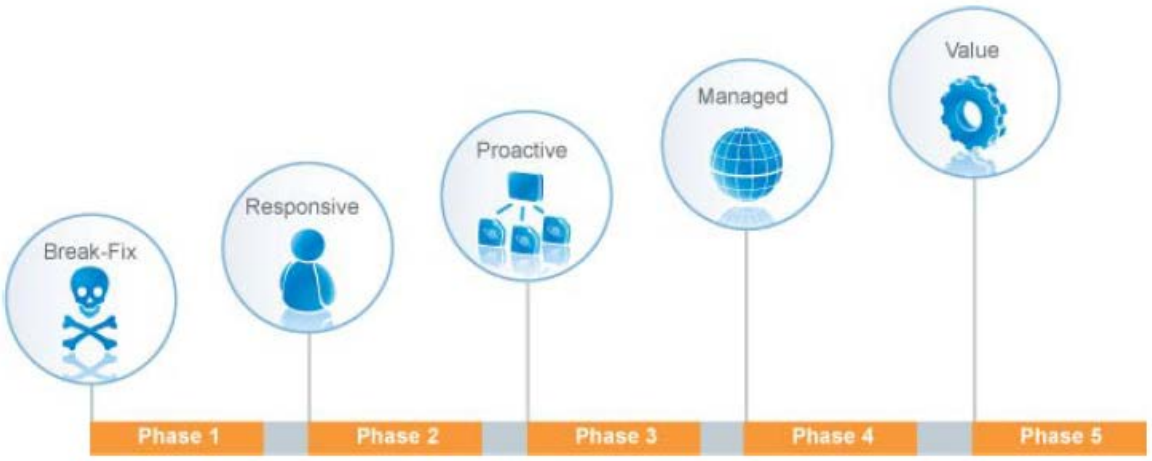
Door deze gestructureerde manier van werken wordt het voor een MSP weer mogelijk tijd te steken in innovatie en verbetering van de dienstverlening. Dit wordt mogelijk gemaakt door de waardevolle informatie welke de MSP kan verzamelen uit het gedrag van de systemen bij de klanten. Zo kan de MSP focussen op innovatie gericht op knelpunten bij de klanten en dit vervolgens voor alle klanten toepassen om problemen in de toekomst bij alle klanten weg te nemen. Een proactief model zal dus ook gaan bijdragen aan een algehele verbetering van de dienstverlening.

4.2. Vormen van proactief beheer/MSP Maturity Model

Om MSP’s inzicht te geven in hun proces naar proactief beheer is een speciaal MSP Maturity Model ontwikkeld (N-ables MSP Maturity Model, 2006). Dit model is gebaseerd op best practices uit de MSP wereld en is mede ontwikkeld door N-able Technologies, een van de leveranciers van MSP software. N-able heeft een hele tak van het bedrijf gewijd aan het ondersteunen van MSP’s in het traject naar proactief beheer. N-able is hier de afgelopen jaren erg vooruitstrevend in geweest. Men ziet nu dat andere MSP software leveranciers dit voorbeeld volgen en soortgelijke diensten aanbieden bij de aankoop van een MSP product.

Dergelijke modellen geven een MSP een duidelijk beeld van waar hij op dit moment staat en hoe volwassen de dienstverlening van de MSP op dit moment is. Bovendien geef het model in groter detail weer welke vormen van proactief beheer er zijn.

Onderstaande figuur geeft het MSP Maturity model weer. Zowel de service providers als haar klanten zullen de genoemde fases moeten doorlopen op de weg naar proactief beheer. In veel gevallen is proactief een eerste streven, omdat in de proactieve fase de eerste problemen weg worden genomen. Verdere doorgroei in het model is wenselijk.



Figuur 3: MSP Maturity Model (N-able Technologies, 2006)

4.2.1. Fase 1: Break-Fix

Klanten in deze categorie hebben de minst ontwikkelde ICT omgevingen. Alle werkzaamheden betreffende de ICT zijn ad-hoc en niet gedocumenteerd. Deze klanten vertrouwen op een automatiseerder om hun problemen op te lossen, maar hebben hiervoor geen SLA's of andere contracten. De automatiseerder moet dus maar net tijd vrij hebben. Deze klanten worden gefactureerd voor het aantal uren arbeid.

De problemen worden door de klant zelf waargenomen, daardoor is het moeilijk deze klanten goede service te verlenen. De klant belt immers zelf als het probleem al schade heeft aangericht. Een automatiseerder met een grote hoeveelheid klanten zal aan deze fase een behoorlijk chaotische werkwijze overhouden en is voor zijn inkomsten geheel afhankelijk van het aantal problemen dat bij de klant optreed.

4.2.2. Fase 2: Responsive

Deze fase heeft veel overeenkomsten met de break-fix fase. Verschillen zijn te vinden in het feit dat de automatiseerder de systemen voor de klant heeft gedocumenteerd en in uitzonderlijke gevallen een beperkte monitoring beschikbaar is. Dit zal in de meeste gevallen beperkt zijn tot simpele controles of servers niet uitstaan en wel beschikbaar zijn. De MSP kan het probleem misschien wel zien aankomen of op het moment zelf zien gebeuren, maar zal niet ingrijpen omdat hiervoor geen contract is opgesteld. De automatiseerder is op de hoogte en zal misschien de klant inlichten, maar zal wachten met de reparatie totdat er toestemming is van de klant.

4.2.3. Fase 3: Proactive

Het grote verschil met de twee bovengenoemde fases is dat preventief onderhoud een belangrijke en serieuze activiteit is van de automatiseerder welke vanaf deze fase MSP genoemd mag worden. Omdat de focus hier meer ligt op het preventief onderhoud en het voortijdig aan zien komen van problemen, kunnen service providers de gevolgen van fouten zo veel mogelijk inperken. Bovendien hebben service providers via de remote monitoring & management (RMM) software de mogelijkheid gegevens betreffende capaciteit en beschikbaarheid te verzamelen welke het mogelijk maken een Service Level Agreement (SLA) af te sluiten met de klant. Standaard onderhoudstaken zullen worden geautomatiseerd en kleine problemen kunnen door het systeem of door een simpele ingreep van een beheerder worden opgelost. In dit model zal nog maar 50-70% van de tijd worden besteed aan

het ad-hoc oplossen van problemen. (IT Service Delivery: From Basic Automation through to Managed Services, 2008)

4.2.4. Fase 4: Managed

Dit is het eerste niveau in het model waar de klant bewust is van het belang dat zijn bedrijf heeft bij een goede ICT omgeving. In deze fase wordt er niet meer gemanaged op systeemcomponenten. Klanten zijn meer geïnteresseerd in performance, capaciteit en continuïteit, dan in routers en switches. In deze fase ligt het belang dus bij de **waarde** van de systemen en de waarde van de geleverde service. Klanten betalen een vaste prijs per maand en verwachten hiervoor dat de ICT systemen werken, goed onderhouden worden en problemen automatisch worden opgepakt door de MSP. De klant heeft het onderhoud van de ICT omgeving uitbesteed aan de MSP, hiervoor zijn contracten en SLA's opgesteld waarin de service verlening staat beschreven.

4.2.5. Fase 5: Value

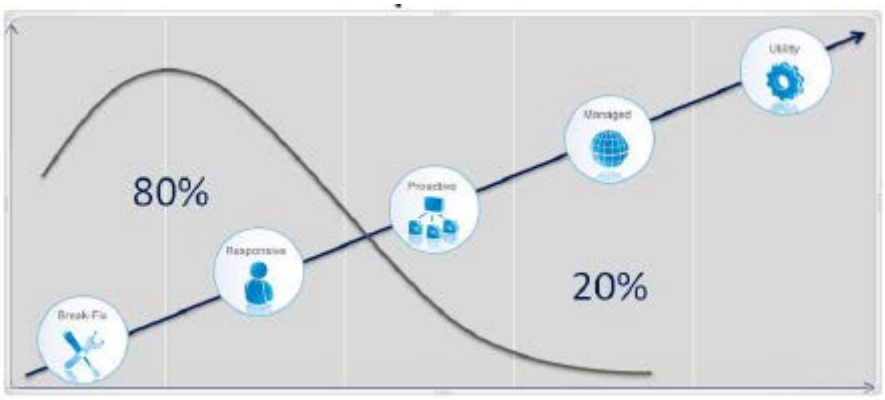
Deze laatste fase gaat nog een stap verder dan de Managed fase, in die zin dat de ICT geleverd door de MSP uitgebreid wordt meegenomen in bedrijfsbesluiten van de klant en dat de MSP 'self-supporting' wordt voor de klant. Dat wil zeggen flexibel en zorgeloos ICT afgeeft aan de klant op het moment dat dit nodig is en dit ook doorberekent aan de klant. Dit zijn als het ware 'all you can eat' oplossingen en deze moeten kunnen meegroeien met de vraag van de klant. Dit idee is te vergelijken met het afnemen van energie. "De ICT moet uit de muur komen" en er wordt betaald voor wat wordt gebruikt. In de praktijk zullen vrijwel alle MSP's niet in staat zijn een dergelijke dienst aan te bieden omdat de technieken hiervoor nog niet ver genoeg ontwikkeld zijn. Deze plannen worden echter wel als serieuze opties voor de toekomst gezien. (IT Service Delivery: From Basic Automation through to Managed Services, 2008)

4.3. Moeilijkheden

Op papier klinken deze plannen veelbelovend, maar onderzoeken (The Seven Major Obstacles on the Road to Managed Services, 2007) wijzen uit dat veranderen van een 'break-fix' model naar een Managed model niet gemakkelijk is en een behoorlijke inspanning van de automatiseerder vereist. Deze stap naar MSP is meer dan alleen de implementatie van een tool. De service provider zal ook moeten veranderen van werk- en denkwijze. Bovendien zullen marketing en sales ook anders moeten omgaan met de verandering, het in de markt zetten en het verkopen van een MSP service vraagt een totaal andere aanpak dan deze afdelingen gewend zijn met de traditionele producten en diensten.

De reden dat er achteraf nog wel eens moeilijkheden zijn, komt omdat MSP's hun bedrijf moeten veranderen; iets wat ze meestal liever niet willen. Om succesvol de overstap naar MSP te maken, moet er genoeg 'commitment' vanuit het bedrijf zijn.

Een ander punt wat deze overgang extra moeilijk maakt, is dat niet alleen de MSP de fases van het volwassenheidsmodel moet doorlopen, maar ook haar klanten. Een MSP kan geen managed of proactieve services verkopen aan een break-fix klant. De belangen botsen dan teveel. Klanten moeten goed ingelicht worden over de voordelen en de belangen van een goede gemanagede omgeving welke zal bijdragen aan de bedrijfscontinuïteit. Dit proces blijkt in de praktijk moeilijk. MSP's moeten hier voldoende aandacht aan besteden om succesvol te zijn in het verkopen van deze 'fixed-price' services.



Figuur 4: MSP Klanten (N-able Technologies)

Bovenstaande figuur geeft weer waar het grootste deel van de MSP klanten zich bevinden. 80% van deze klanten bevindt zich nog in het 'break-fix' en responsive gebied (Going beyond RMM, 2011). Het heeft voor de MSP's daarom geen nut om zich volledig te focussen op proactieve en managed klanten. MSP's moeten zich bewust zijn van deze verdeling en moeten deze "achterblijvende" klanten ook oplossingen kunnen aanbieden en motiveren om verder te groeien naar proactief, wat veel voordelen heeft voor zowel de klant als de MSP.

Wat vaak mis gaat is dat MSP's te veel focussen op proactieve klanten, hiervoor één product samen stellen en dat vervolgens willen verkopen aan alle klanten. Het is beter om een aantal managed producten samen te stellen met bijvoorbeeld een instapmodel, of voor ieder niveau van het model een apart product verkopen. Dit kan ook opgebouwd worden met bijvoorbeeld een 'blox' model. Dit soort constructies geven een reactieve klant als het ware "een kijkje in de keuken" van de MSP. Als klanten de voordelen en belangen gaan inzien, kan dit mogelijkheden creëren voor het laten door groeien van een klant naar proactief.

Het gevaar van een goed werkende gemanagede omgeving is dat klanten niet meer door hebben waarvoor wordt betaald. De klant heeft immers geen weet van de problemen omdat deze automatisch door de MSP worden opgepakt en de klant niet meer hoeft te bellen. Het is belangrijk dat MSP's uitgebreid rapporteren naar de klant en inzichtelijk maken wat er de afgelopen periode allemaal voor de klant gedaan is. Veel MSP producten hebben hier een rapportage functie voor. Men kan erover nadenken deze rapportages toe te voegen aan de factuur.

Overige problemen kunnen zijn (The Seven Major Obstacles on the Road to Managed Services, 2007):

- niet volledig benutten van de MSP software;
- waarde van de service niet duidelijk krijgen naar de klant;
  Als de waarde van de service niet duidelijk wordt gemaakt naar de klant, kan de klant zichzelf gaan afvragen waarvoor hij iedere maand betaald en de band met de MSP kwijtraken en op zoek gaan naar een andere automatiseerder welke goedkoper is, maar waarschijnlijk minder service levert.
- te veel gericht op techniek i.p.v. de 'pijnpunten' van de klant aanpakken;
- flexibiliteit verliezen;
  Het is belangrijk passende service te verkopen aan de verschillende klanten en niet naar één model te gaan. (Walsh, 2011).

5. Doelen/ Eisen aan Managed Services

Voordat een gefundeerd advies kan worden uitgebracht is het belangrijk de eisen en wensen van Hupra in kaart te brengen. Een aantal van deze eisen zijn verkregen bij de start van het project en opgegeven door de opdrachtgever of verkregen in gesprekken over de project initiatie. Andere zijn verkregen in vergaderingen en overleggen met beheerders en de opdrachtgever.

Voor deze doelen en eisen verwijs ik naar Hoofdstuk 3.2 van dit document. Deze zijn nog een keer kort samen te vatten als:

- onderscheidend vermogen Hupra;
- kosten terugdringen (aantal facturabele uren verhogen met 20%);
- klantwerving (25+ klanten in het proactieve model);
- verlaging werkdruk (terugdringen break-fix werkzaamheden van 99% naar 50%);
- betrouwbaarheid dienstverlening/ ICT van de klant (van ±90% naar 99% beschikbaarheid);
- automatisering terugkomend onderhoud (van 0% naar 10-20%).

Met als uiteindelijke doelstelling een beheermodel waarmee Hupra proactief te werk kan gaan, problemen tijdig kan ontdekken en de impact van deze problemen kan beperken. En een uiteindelijk niveau 3 op het volwassenheidsmodel van hoofdstuk 4.2.

5.1. Vorm vergaderingen

In open interviews en vergaderingen met werknemers van de afdeling zakelijk is getracht zoveel mogelijk informatie over de verwachtingen aan het proactieve model en de software boven water te krijgen. Deze vergaderingen en interviews zijn gehouden onder medewerkers van verschillende disciplines. In het bijzonder, marketing, sales, consultancy en beheer.

Deze vergaderingen en vragenrondes zijn gevoerd aan de hand van een probleem dat zich heeft voorgedaan of een pijnpunt dat op tafel is gelegd. In de beginfase van dit project waren dit vooral gesprekken over de verwachtingen van het model en het pakket, waarna deze later in het project meer over inhoudelijke eisen aan het pakket gingen. Deze gesprekken zijn later omgezet en samengevat tot concrete eisen aan het pakket en de configuratie.

Bij deze vergaderingen en vragenrondes waren altijd aanwezig: de opdrachtgever, hoofd sales/marketing en hoofd beheer. Afhankelijk van het te bespreken onderwerp zijn er ook een aantal gesprekken geweest waarbij uitvoerend beheerders aanwezig waren. De gesprekken zijn altijd heel open en informeel geweest. Alle aanwezigen hebben hun mening kunnen geven over het onderwerp, waarna er vervolgens werd gebrainstormd totdat aan het einde van die bespreking meteen een mening kon worden gevormd of een knoop kon worden doorgehakt. Deze resultaten zijn samengevat in de rest van dit hoofdstuk.

Typische punten welke aan de orde zijn gekomen zijn:

- Wat moet het model opleveren voor Hupra als organisatie?
- Hoe wordt het werken met het product gezien?
- Hoeveel informatie wordt verwacht van het systeem?
- Welk onderhoud wordt nu handmatig uitgevoerd?
- Wat wordt verwacht van de leverancier?
- Hoeveel 'false positives' mogen uit het pakket komen?
- Enz.

Wat duidelijk naar voren kwam waren de verschillende belangen van een aantal aanwezigen. Over het algemeen zaten alle aanwezigen op dezelfde lijn, de Hupra lijn, maar in de vergaderingen waren de verschillende disciplines goed terug te vinden. Waar beheerders meer waarde hechten aan hoe men met het product werkt, welke functies aanwezig zijn en hoe technisch diepgaand een functie moet zijn, waren de managers en marketing mensen juist meer geïnteresseerd in wat het voor Hupra moet gaan opleveren aan klantwinning, financiële- en imagoverbetering.

Hieronder wordt een overzicht gegeven van de belangrijkste gesprekken en vergaderingen m.b.t. het vaststellen van de eisen.

Tabel 3: Vergaderingen en gesprekken t.b.v. vaststellen eisen

Datum	Aanwezigen	Onderwerp	Belangrijkste uitkomsten
20-02-2012	Cornel van Westen (sales/marketing) Pieter Willemsen (opdrachtgever/technisch beheer) Mike de Weijer (projectleider)	Doelen Hupra	Onderscheidend vermogen Kosten terug dringen Betrouwbaarheid dienstverlening
27-02-2012	Cornel van Westen Pieter Willemsen Mike de Weijer	Proactief model Procedures	Verantwoordelijkheden beheerders Notificaties per mail, indeling aan prioriteit. Verhogen efficiëntie (facturabele uren) Unique selling points
05-03-2012	Cornel van Westen Pieter Willemsen Chiel de Groot (technisch beheerder) Mike de Weijer	Producteisen	Dashboards voor beheerders op kantoor. Automatisering onderhoudstaken Maatwerk d.m.v. scripts
08-03-2012	Cornel van Westen Mike de Weijer	Procedures Doelen Hupra	Imago verandering, professioneler Werkdruk verlaging
12-03-2012	Cornel van Westen Pieter Willemsen Chiel de Groot Mike de Weijer	Productkeuze	N-central Weinig feeling bij Kaseya, vooral licentie model slecht ontvangen GFI weinig functies, sluit niet aan bij het streven van Hupra

Hieronder zijn de resultaten uit deze gesprekken samengevat. De eisen zijn te verdelen in eisen aan het proactieve model en eisen aan het software pakket. De eisen aan het pakket zijn vooral afkomstig van de technische beheerders. De eisen aan het model zijn vooral afkomstig van de opdrachtgever en de managers.

5.2. Eisen proactief model

Resultaten van deze interviews en vergaderingen zijn samen te vatten tot het volgende.

Procedures

In het proactieve model moeten procedures worden opgenomen voor het beheer. Deze procedures moeten structuur in de werkzaamheden brengen en ervoor zorgen dat het beheer op een goed gestructureerde manier verloopt. Het beheer moet vooral professionaliteit naar de klant uitstralen, want dit is het niveau dat Hupra wil bereiken. Daarnaast moeten deze procedures ook duidelijkheid voor Hupra bieden, aan bijvoorbeeld nieuwe gebruikers van het model.

Vastleggen verantwoordelijkheden

Bovengenoemde procedures werken alleen als alle verantwoordelijkheden vastgelegd zijn en deze beheerders deze verantwoordelijkheden ook nemen. Hupra wil niet alleen duidelijkheid en structuur in de manier van werken, maar wil daarnaast ook dat de verantwoordelijkheden goed geregeld zijn. Zo moet bij de aanvang van een incident meteen duidelijk zijn welke beheerder verder verantwoordelijk wordt voor het oplossen van het probleem, zodat het werk niet langs elkaar heen loopt. Bovendien wordt voorkomen dat meerdere beheerders langs elkaar heen aan het zelfde probleem werken. Dit zal niet de beoogde professionaliteit uitstralen.

Priotarisering notificaties

Priotarisering van de notificaties is een eis aan zowel het proactieve model als een eis aan het softwarepakket. Hupra wil dat er een duidelijke scheiding van notificaties op prioriteit wordt gemaakt en dat deze meldingen meteen aan de juiste verantwoordelijke worden gekoppeld. Bovendien is een systeem of indeling nodig waarmee werknemers niet meteen overspoeld worden met meldingen voor kleine problemen. Deze eis zal ook van belang zijn bij een toekomstige koppeling aan een ticket systeem, ter voorkoming van onjuiste tickets.

Aantal facturabele uren verhogen

Het nieuwe model moet bijdragen aan het verminderen van verloren uren. In de huidige break-fix situatie is het vaak zo dat een consultant bij een klant langs moet voor een reparatie. De reistijd wordt weliswaar opgenomen in de factuur, toch gaan er uren verloren welke niet gefactureerd kunnen worden. Als de consultant bijvoorbeeld een half uur tussendoor op kantoor aanwezig is. Meestal is dit niet de moeite om een nieuwe taak te starten. Met het nieuwe model moet het mogelijk worden een duidelijk overzicht van de werkzaamheden de krijgen zodat er makkelijker van ticket naar ticket kan worden gegaan. Bovendien zullen veel taken in het nieuwe model remote opgelost kunnen worden waardoor consultants minder vaak naar de klant hoeven en de eerder genoemde problemen minder vaak optreden.

Klantwerving
Hupra wil een goed uitgewerkt model voor proactief beheer inzetten als “unique selling point”. Een professionele en volwassen vorm van proactief beheer is een eigenschap die goed gebruikt kan worden bij het werven van nieuwe klanten. Hupra wil de klant vooral een goed gevoel meegeven, zodat de klant er van uit kan gaan dat zijn zaken goed geregeld zijn. Bovendien zal het de professionaliteit uitstralen waar Hupra naar op zoek is.

Verlaging werkdruk
Een invoering van een dergelijk model voor proactief beheer moet de werkdruk bij de werknemers van Hupra verlagen. Het systeem moet overzicht en duidelijkheid bieden. Een goed werkend proactief model moet in de ogen van Hupra de stress en de druk bij de werknemers wegnemen.

Verbetering van de betrouwbaarheid van de dienstverlening
Een goed proactief model moet voor Hupra bijdragen aan een verbetering van de dienstverlening. Door een goede duidelijke structuur en het hebben van een duidelijk overzicht moeten fouten in het beheer minder vaak voorkomen en waar mogelijk een versnelling van de doorlooptijd opleveren. Met het model moet de beheerafdeling proactief te werk kunnen gaan en op rustige momenten proactief onderhoud kunnen uitvoeren om problemen in de toekomst voor te zijn.

5.3. Eisen software pakket

Naast de eisen aan het proactieve beheermodel hebben de interviews met werknemers en de opdrachtgever ook een aantal eisen aan het software pakket opgeleverd.

Automatisering terugkomend onderhoud
Hupra vindt het belangrijk dat een ondersteunend software pakket voldoende mogelijkheden biedt voor automatisering van terugkomend onderhoud om op deze manier beheerders ‘vervelend’ werk uit handen te nemen. Minimaal de volgende taken moeten geautomatiseerd verlopen:

- Schijfopruiming
- Defragmentatie
- Schijfcontrole
- Virus scan
- Patch management

Interface
Hupra verwacht van het product een duidelijke ‘nette’ interface welke een compleet overzicht moet geven van de huidige problemen. Het moet bijvoorbeeld mogelijk zijn deze interface op een groot scherm aan de muur weer te geven. Beheerders moeten een duidelijk overzicht hebben van alle problemen. Vanuit dit overzicht moeten zij direct kunnen werken. Dit moet in de vorm van aanpasbare en duidelijke dashboards gepresenteerd worden.

Support
Hupra hecht veel waarde aan goede support vanuit de fabrikant. Het is belangrijk dat er goede ondersteuning bij problemen aanwezig is. Het software pakket word immers een onmisbaar product binnen de beheerafdelingen van Hupra. Er moet een mogelijkheid zijn voor een servicecontract met de fabrikant en ondersteuning op zowel technisch als niet technisch gebied.

Technisch diepgaand
Hupra wil een technisch diepgaand product. Dat wil zeggen een product dat vooruitstrevend is en veel mogelijkheden biedt. Het is ook belangrijk dat eventuele benodigde uitbreidingen makkelijk zelf kunnen worden toegevoegd en er met scripts bijvoorbeeld specifieke controles worden uitgevoerd op maatwerksystemen welke Hupra in beheer heeft bij de klant.

Moet te vertrouwen zijn
Een belangrijke eis is dat het product betrouwbaar is, dat er geen false positives/negatives worden gegeven. Dit levert onnodig werk op voor beheerders. Of het product betrouwbaar is, heeft meer te maken met een bepaald gevoel wat een product geeft. Technisch gezien hangt het voor het merendeel af van de configuratie of een product betrouwbaar is of niet. Doelstelling moet zijn dat 1 op de 100 meldingen een false positive mag zijn.

Aansluiting met andere pakketten binnen het bedrijf
Hupra vindt het belangrijk dat het pakket ondersteuning biedt voor integratie met andere bestaande pakketten. Denk bijvoorbeeld aan een financieel pakket. Daarnaast is het van belang dat ook in de toekomst, bij migratie naar een groter ticket systeem, deze mogelijkheid tot integratie nog steeds bestaat.

6. Probleem aanpak

Nu duidelijk is wat de wensen van Hupra zijn, moet worden gekeken hoe deze wensen waar gemaakt kunnen worden. Hupra wil duidelijk een stap maken richting Managed Services en heeft hier al een vrij uitgesproken beeld over. Daarom is het dus al snel duidelijk dat de werkwijze van Hupra moet veranderen wil men op het beoogde niveau 3 van het volwassenheidsmodel komen (zie hoofdstuk 4.2). Na een eerste inventarisatie en overleg met de opdrachtgever blijkt dat er vier mogelijke scenario's uiteengezet kunnen worden. Een implementatie van een proactief model met ondersteunende software is een vereiste om op niveau 3 te kunnen komen (IT Service Delivery: From Basic Automation through to Managed Services, 2008). Dit stond al snel als een paal boven water. Voor de compleetheid en vervolgonderzoek in de toekomst, zijn de andere scenario's ook besproken.

Vasthouden aan huidige model
Vasthouden aan het huidige model betekent kort door de bocht: "niets doen". Het is wel mogelijk een aantal verbeteringen in het huidige model door te voeren, echter zal dit alleen maar leiden tot opschuiven van het probleem.

Inzetten monitoring
Een voor de hand liggende oplossing is het inzetten van monitoring, echter zal dit niet alle problemen wegnemen. Het inzetten van monitoring geeft het bedrijf de mogelijkheid een duidelijk beeld te vormen van de systemen en de fouten die daarin optreden. Echter is er geen mogelijkheid om iets proactief te ondernemen als hiervoor geen andere werkwijze wordt aangenomen. Met deze oplossing zal men nooit verder komen dan niveau 2 (reactief) van het volwassenheidsmodel.

Implementatie proactief model
Een implementatie van een proactief model, zonder hierbij ondersteunende software te gebruiken, is vrijwel onmogelijk. Het overzicht en de functionaliteit dat de software biedt, is een vereiste bij het hanteren van een dergelijk model. Het is niet mogelijk een probleem aan te zien komen als hier geen software voor aanwezig is. Daarnaast is het onmogelijk de Service Level Agreements in dit proactieve model te garanderen als er geen middelen zijn om aan te tonen af deze daadwerkelijk gehaald worden.

Tabel 4: Keuze oplossing

	Vasthouden aan huidige model	Monitoring	Procedures aanpassen	Procedures + software tool
Kosten terugdringen			X	x
Verlaging werkdruk			X	x
Betrouwbaarheid dienstverlening		x		x
Automatisering onderhoud				x
Max. niveau MSP Maturity Model	1	2	-	5

Implementatie proactief model met ondersteunende software

Een combinatie van de implementatie van het proactieve model, met ondersteunende software, is hier de meest complete oplossing. Deze ondersteunende software moet een capabele tool zijn om alle aspecten van het proactieve model te ondersteunen. De bedrijfsprocessen dienen aan te sluiten op de mogelijkheden van de tool om deze zo goed mogelijk te benutten.

Al vrij snel is, in overleg met Hupra, de keuze gevallen op het inzetten van een proactief model met ondersteunend software pakket. Hupra is vanaf het begin nauw betrokken geweest bij het onderzoek, daardoor is er vanuit Hupra al vrij snel de voorkeur ontstaan voor het pakket N-central. Verder heeft Hupra ook veel positieve signalen gehad van partners over N-central. Om deze redenen is N-central sowieso opgenomen in het onderzoek. Daarnaast is even een stapje terug gedaan en zijn ook andere pakketten betrokken in het onderzoek om een totaal beeld van de mogelijkheden te vormen.

Hoewel de markt voor monitoring pakketten groot is en veel verschillende soorten en maten oplossingen biedt, is in vergelijking de markt voor echte MSP tools erg klein. Na een snelle inventarisatie te hebben uitgevoerd bleek al snel dat er maar 3 producten zijn welke de moeite waard zijn om verder te onderzoeken. Dat waren N-central, Kaseya en GFI Max.

Deze producten zijn producten ontwikkeld met als doel MSP. Deze producten gaan verder in het ondersteunen van het model. Naast monitoring functies zijn deze pakketten ook uitgerust met mogelijkheden voor het managen van back-up, patch management, onderhoud, anti virus, enz. Voor een uitgebreid overzicht van alle functionaliteiten verwijs ik graag naar het productonderzoek, opgenomen in bijlage F. Hierin worden de mogelijkheden en de verschillen van de pakketten besproken.

Onderzoek naar de genoemde pakketten heeft vooral plaats gevonden in de vorm van een document onderzoek. Er is veel onderzoek gedaan naar de mogelijkheden van de pakketten door middel van informatie op internet en informatie verkregen van de software leveranciers. Verder is aanvullende informatie verkregen uit test resultaten van trail versies. Informatie is later aangevuld naar mate meer test informatie beschikbaar was.

Alle informatie over de werking en de functies van de onderzochte producten is vervolgens uitgewerkt in hoofdstuk 3 van het productonderzoek. De onderzochte pakketten hebben veel overeenkomsten op het gebied van functionaliteit. De invulling hiervan wil nog wel eens verschillen. Deze invulling en werking is kort toegelicht met de informatie beschikbaar op het moment van schrijven. Gedurende het onderzoek is meer informatie beschikbaar gekomen over de invulling van sommige onderdelen. Deze informatie is verder verwerkt in de testrapporten.

Een aantal functies die men terug vindt in bijna alle MSP producten zijn functies als:

- Dashboards
- Remote Control
- Self Healing
- Mobiele toegang
- Patch Management
- Notificaties/PSA (Professional Services Automation) Integratie
- Managed Anti Virus
- Backup
- Reporting

De werking van de functies wordt in paragrafen 1 t/m 3 hoofdstuk 3 van het productonderzoek verder toegelicht. Daarnaast worden in het onderzoeksrapport ook de aanvullende mogelijkheden per product toegelicht. Deze functies, de uitwerking hiervan en de extra mogelijkheden zullen in hoofdstuk 7.1 worden gebruikt om tot een vergelijking van de pakketten te komen. Deze zullen uiteindelijk gebruikt worden in de product advies/keuze.

7. Aanbevelingen

Na eerst het concept van Managed Services onderzocht te hebben en de mogelijkheden van de producten en de doelen en wensen van Hupra in kaart te hebben gebracht, was voldoende basis aanwezig om een advies uit te brengen over de situatie. De eerste stap hierin was een advies over het aan te schaffen product. Gedurende het project had Hupra al een lichte voorkeur ontwikkeld voor een bepaald pakket. Aan mij de taak de andere pakketten toe te lichten en mijn mening uit te spreken betreffende de productkeuze en te onderzoeken of deze voorkeur terecht was.

De tweede stap bestond uit het adviseren betreffende de product configuratie. Door vooral te zoeken naar best practices en door veel test uit te voeren, is een advies gevormd over hoe het product het beste geconfigureerd kan worden om zo goed mogelijk aan te sluiten bij Hupra.

Als laatste aanbeveling een advies over hoe te werken met het product. Op welke manier kan er zoveel mogelijk voordeel worden behaald met het gebruik van het pakket. Waar moet allemaal rekening mee worden gehouden als men aan het werk gaat met het pakket en hoe moet het bedrijf hierop aansluiten. Deze zaken zullen allemaal worden toegelicht in onderstaande hoofdstukken. Daarnaast verwijs ik voor gedetailleerde informatie naar het adviesrapport opgenomen in bijlage G.

7.1. Product aanbevelingen

Er zijn in de onderzoeksfase drie pakketten onderzocht en vergeleken. Uitgebreide informatie over deze pakketten is te vinden in het eerder besproken productonderzoek. In dit productonderzoek is al een korte vergelijking van de pakketten gemaakt. Deze tabellen geven alleen de verschillen tussen de pakketten weer op het gebied van functies en invulling hiervan. Daarnaast worden de kosten van de verschillende pakketten vergeleken. De uiteindelijke productkeuze wordt verder uitgewerkt in hoofdstuk 4.1 van het adviesrapport.

In het onderzoeksrapport komt al naar voren dat een aantal verschillen tussen de pakketten minimaal zijn. De invulling van de functies wil nog wel eens verschillen. Met het wel of niet hebben van functies is nog niet alles gezegd. In hoofdstuk 3 van het productonderzoek is al verder ingezoomd op de invulling van de functies en de diepgang hiervan.

Onderstaande tabel (5) geeft een overzicht van de verschillende functies van de pakketten. De volledige versie van deze tabel is opgenomen in bijlage B, tabel (12). Op basis van deze functies, de kosten van de pakketten (weergegeven in tabel 6 pag. 37) en de in hoofdstuk 5 vastgestelde eisen is een productkeuze geformuleerd.

Cijfers zijn toegekend aan de invulling en compleetheid van de functies. Deze worden ingedeeld op een schaal van 1 tot 5 en zijn verkregen door ervaringen met trial versies en op basis van product informatie en documentatie. Deze worden vervolgens vermenigvuldigd met het gewicht. Weging is verkregen na overleg met de opdrachtgever en de overige betrokkenen bij het vaststellen van de eisen.

Tabel 5: Inhoudelijke product vergelijking (McCabe, 2007)

	Relatief gewicht (0-1)	N-Central	Kaseya	GFI MAX Remote Management
On-premise	0,8	5 / 4,0	5 / 4,0	- / -
Cloud	0,2	2 / 0,4	2 / 0,4	5 / 1,0
Web based dashboard	0,5	4 / 2,0	4 / 2,0	4 / 2,0
Integratie PSA	0,7	4 / 2,8	4 / 2,8	2 / 1,4
Remote control	0,1	4 / 0,4	4 / 0,4	4 / 0,4
Totaal		104 / 70,4	104 / 65,5	53 / 34,0
Gemiddelde		**4,3 / 2,9**	**4,2 / 2,6**	**4,1 / 2,6**

Na bovenstaande productvergelijkingen en rekening houdende met in hoofdstuk 5 vastgestelde eisen en wensen van Hupra, is het advies aan Hupra gebruik te gaan maken van N-central. Voor meer details wordt verwezen naar hoofdstuk 4.1 van het adviesrapport. De functies van N-central zijn in de toekomst mogelijk uit te breiden met uitbreidingen als: Report Manager (N-compas), Backup Manager en Remote Support Manager. Voor nu is gekozen voor een basis installatie van N-central.

GFI MAX RemoteManagement is op de eerste plaats afgevallen omdat dit pakket simpelweg maar een beperkt aantal functies heeft, in vergelijking met Kaseya en N-central behoorlijk achterblijft en minder technisch diepgaand is. Het gebrek aan technische diepgang valt gemakkelijk te verklaren. GFI heeft ervoor gekozen het pakket alleen als Cloud oplossing aan te bieden. Daardoor zal het product erg gestandaardiseerd zijn en is de flexibiliteit verloren gegaan. Maatwerk is niet mogelijk.

GFI heeft daarentegen wel een aantrekkelijk licentie model, maar zal uiteindelijk niet veel goedkoper zijn dan de concurrenten. Verder heeft de oplossing van GFI wel voordelen op het gebied van beschikbaarheid. Rekening houdend met de eisen van Hupra wegen deze voordelen uiteindelijk niet op tegen het gebrek aan functies. En zeker ook in de toekomst zal het met een pakket als GFI lastig worden verder te ontwikkelen en uit te breiden.

De keuze tussen N-central en Kaseya is lastig geweest. De verschillen tussen N-central en Kaseya zijn immers minimaal en de producten vertonen erg veel overeenkomsten met elkaar. Kaseya heeft ten opzichte van N-central een aantal extra functies in huis, echter heeft N-central meer mogelijkheden tot uitbreiding. Lettend op de invulling van de standaard aanwezige functies ben ik ervan overtuigd dat N-central verder ontwikkeld, verder gaat met de functies, daarom ook meer mogelijkheden biedt en technisch diepgaander is. Daarnaast zijn er nog een aantal andere eigenschappen welke ervoor hebben gezorgd dat de uiteindelijke keuze op N-central is gevallen.

Automatisering onderhoud
De functies voor automatisch onderhoud in N-central zijn behoorlijk uitgebreid en sluiten aan bij de wens naar geautomatiseerd beheer (Hoofdstuk 6.2). Het is mogelijk de in de eis vastgestelde taken geautomatiseerd uit te laten voeren.

Self-healing
Het systeem kan eerst zelf actie ondernemen voordat er een beheerder wordt ingelicht.

Interface
N-central heeft een overzichtelijke interface welke de gewenste meldingen overzichtelijk weer kan geven in een volledig aanpasbaar dashboard.

Technisch diepgaand
De functies van N-central zijn ver ontwikkeld en zijn bovendien naar eigen wens nog verder te configureren en uit te breiden.

Product ondersteuning
N-able heeft na de aanschaf van N-central uitgebreide trajecten ter ondersteuning van de MSP, niet alleen op het gebied van implementatie, maar biedt ook complete ondersteuning in het traject naar Managed Services.

Reporting met de uitbreiding Report Manager
De Report Manager uitbreiding maakt het mogelijk uitgebreide rapportages te maken van systemen voor de klant. Dit kan Hupra helpen met het onderbouwen en verantwoorden van de SLA's. De rapporten van Report Manager zien er strak en professioneel uit, deze zouden zonder aanpassingen direct naar de klant gestuurd kunnen worden.

Schaalbaarheid
Het door N-able gehanteerde licentie model maakt het mogelijk het systeem onbeperkt te laten groeien. Met de indeling van agent licenties voor de verschillende doeleinden gaat er minder geld 'verloren'. Bij het licentie model van Kaseya bijvoorbeeld, waar voor iedere agent hetzelfde bedrag wordt betaald, kan men zich afvragen of het nodig is de volledige prijs te betalen terwijl er alleen maar een werkstation wordt gemonitord.

Naast de bovenstaande punten wordt er een interessant licentie model gehanteerd. De kosten hiervoor zijn weergegeven in tabel 7 op pag. 38. Door de verschillende prijzen voor servers, werkstations, netwerk modules en Essentials licenties, kan bij de aankoop van de licenties precies afgestemd worden wat nodig is. Voor N-central als product hoeven geen terugkomende kosten te worden betaald. Voor ieder te monitoren apparaat dient een licentie te worden aangeschaft, afhankelijk van het type apparaat. Deze licentie wordt eenmalig gekocht. Na het eerste jaar worden kosten voor onderhoud en support op de licentie gevraagd. Deze zijn beduidend minder dan het aankoopbedrag.

Als we dit vergelijken met een simpel model zoals Kaseya hanteert, worden de verschillen al snel zichtbaar. Kaseya hanteert een model waarbij eenmalig een bedrag voor het pakket wordt betaald. Daarnaast moet er per 24 maanden een bedrag voor de agent licenties worden betaald. Op het eerste gezicht lijkt Kaseya goedkoper, maar omdat de terugkomende investering veel hoger is, wordt Kaseya al snel duurder dan N-central.

Tabel 6: Vergelijking kosten (500 licenties, voor details zie onderzoeks-/adviesrapport)

	Eenmalige investering	Terugkomende investering (per maand)	Investering na 12 maanden	Investering na 24 maanden
N-central	€ 40.580,-	€ 677,- (vanaf jaar 2)	€ 40.580,-	€ 48.700,-
Kaseya	€ 4.500,-	€ 2.333,-	€ 32.500,-	€ 60.500,-
GFI MAX	€ 1.660,-	€ 1.707,-	€ 22.144,-	€ 42.628,-

Mijn advies aan Hupra is N-central aan te schaffen. De eenmalige investering is wat groter waardoor de drempel wat hoger zal liggen, echter zal dit zich snel terugbetalen vanwege het flexibele licentie model van N-central. Op de lange termijn zal N-central vele malen goedkoper zijn dan een product als Kaseya.

Als laatste heb ik Hupra geadviseerd na te denken over de mogelijke uitbreidingen van N-central. In het bijzonder Report Manager en de Backup Manager. Report Manager is een handige uitbreiding voor het maken van rapportages ter ondersteuning van de SLA's en kan een enorm voordeel hebben bij verkoop en binding van de huidige klanten. Het is zelfs van zo groot belang de klanten middels rapportages inzicht te geven in de omgeving en de verrichte werkzaamheden, dat ik Report Manager zou adviseren als een vereiste.

De Backup Manager is daarnaast een goede stap in de richting van een compleet gemanagede omgeving. De back-up is een cruciaal onderdeel van een betrouwbare omgeving en dienstverlening. Inzet van dit systeem is een grote stap in de richting van een niveau 4 en hoger van het volwassenheidsmodel in hoofdstuk 4.2.

7.1.1. Product aanschaf

De mogelijkheden van de pakketten, de kosten, mijn visie en advies betreffende N-central, en de uitbreidingen hiervoor zijn vervolgens voorgelegd aan Hupra. Hiervoor zijn vergaderingen gepland. Gedurende de onderzoeksfase is Hupra al nauw betrokken geweest bij de resultaten, dus men was hiervan al op de hoogte. Daarnaast zijn de rapporten voorafgaand aan de vergadering verspreid. In deze vergaderingen zijn de opties en de mogelijkheden van de producten besproken. Uiteindelijk is de keuze gevallen op het door mij geadviseerde pakket N-central. Juist vanwege de aansluiting van N-central op de eisen van Hupra, de mogelijkheden voor de toekomst, en de technische diepgang.

In eerste instantie is gekozen voor de aanschaf van het basispakket met bijbehorende licenties. Er is voor gekozen een minder aantal licenties aan te schaffen dan in de vergelijking gebruikt. Dit is in tabel 3 weergegeven. De uiteindelijke aanschaf is redelijk snel gerealiseerd. Dit vanwege de lopende contacten betreffende de Trial versies van het pakket. De upgrade naar de volledige versie is een kwestie van een activering aan de kant van N-able. Verdere regelingen met licenties en betalingen waren in dit geval aan Hupra. Daarna konden de tests en implementatiefases verder worden ingezet en kon een start worden gemaakt met het toevoegen van eigen systemen en een selectie klanten.

Tabel 7: Uiteindelijke aanschafkosten

	Eenmalig (eerste jaar)	Terugkomend vanaf jaar 2 (per jaar)	Totaal (na 24 maanden)
Server	€ 220,80 x 50 = € 11.040,-	€ 44,16 x 50 = € 2.208,-	€ 11.040,- + € 2.208,- = € 13.248,-
Desktop	€ 46,- x 75 = € 3.450,-	€ 9,20 x 75 = € 690,-	€ 3.450,- + € 690,- = € 4.140,-
Network Essentials	€ 110,40 x 20 = € 2.208,-	€ 22,08 x 20 = € 442,-	€ 2.208,- + € 442,- = € 2.650,-
	€ 15,- x 100 = € 1.500,-	€ 3,- x 100 = € 300,-	€ 1.500,- + € 300,- = € 1.800,-
Endpoint Security	€0,80x300 = € 240,-	€ 0,80 x 300 = € 240,-	€ 240,- + € 240,- = € 480,-
	€ 18.438,-	€ 3.880,-	€ 22.318,-

De aanschaf van de uitbreidingen Backup Manager en Report Manager is nog even voor de toekomst behouden. De opties worden wel serieus overwogen. Ook mijn visie hierop is eerst energie in de basis steken en de uitbreidingen bewaren voor de toekomst. Pas als de basis correct functioneert, kan voordeel worden behaald uit de aanvullende functies.

Gedurende de uitvoering van het project is ook bij Hupra het belang van deze uitbreidingen duidelijk geworden. Tegen het einde van het project is daarom toch besloten een ontwerp en eerste tests te starten met de Backup Manager. Dit proces is ook versterkt door sterke ontevredenheid met het huidige back-up pakket.

7.2. Product configuratie

Als volgende stap in het adviesproces is een beeld gevormd over de configuratie van het systeem (in grote lijnen). Denk bijvoorbeeld aan hoe het product moet worden ingezet en in welke omgeving? Hoe moet de beschikbaarheid geregeld worden? Wat moet geregeld worden om een basis neer te zetten en aan de eisen en wensen te voldoen? En wat moet hiervoor geconfigureerd worden? (N-able Technologies, 2009)

7.2.1. Omgeving/infrastructuur

Een dergelijk pakket en server zal altijd beschikbaar moeten zijn om te voorkomen dat er onbetrouwbare meldingen naar de beheerders worden gestuurd en onbetrouwbare tickets worden aangemaakt. Het is aan te raden de locatie van de N-central server te voorzien van meerdere internetverbindingen en een redundant netwerk. Daarnaast zal de server moeten worden uitgerust met technieken als UPS en High Availability.

Deze problemen kunnen worden opgevangen door gebruik te maken van de reeds aanwezige virtuele omgevingen van Hupra. Daarnaast zijn op locatie twee verbindingen aanwezig. Bij uitval van de primaire lijn is er een terugvalmogelijkheid voor de tweede lijn. Deze is weliswaar langzamer, maar zal wel een goede beschikbaarheid van de server garanderen.

Een tweede mogelijkheid is het verplaatsen van de server naar een data center. Hiermee worden de meeste onzekerheden betreffende beschikbaarheid weggenomen. Bovendien zal een dergelijke oplossing voor meer stabiliteit zorgen. Daarnaast kan het voor het gebruik van bepaalde product features wenselijk zijn over een data center locatie te beschikken. Het verplaatsen naar een data center zal voor Hupra pas in de toekomst interessanter worden, als er meer klanten aan het pakket worden gekoppeld en het direct belang van de N-central server groter zal zijn.

7.2.2. Service templates

Verder zullen er duidelijke plannen moeten komen waarin wordt vastgelegd welke services moeten worden gemonitord. Dit zal afhankelijk zijn van het type machine dat wordt gemonitord. Hiervoor zullen templates worden opgesteld. Zo zullen bijvoorbeeld voor alle Windows servers een aantal vaste punten worden gecontroleerd als:

- Processor
- Geheugen
- Harde schijf status
- Patch status
- Beschikbaarheid
- Event Logging

Daarnaast zullen een aantal templates moeten worden opgesteld voor bijvoorbeeld het monitoren van de backups. Op dit moment worden daarvoor Symantec Backup Exec, Acronis Backup & Recovery en Solcon Online Backup gebruikt. Verder zullen er templates nodig zijn voor het monitoren van de geplaatste firewalls en templates voor het controleren van de onderhoudsprocessen.

Naast een overzicht van welke services precies gecontroleerd dienen te worden, moet er ook duidelijk worden vastgesteld wat de bijbehorende thresholds zijn bij de te monitoren services en wat de prioriteit van een service is. De invulling van deze templates wordt verder uitgewerkt in hoofdstuk 8.1.1.

7.2.3. Notificaties

Een tweede kritiek punt bij de werking van de server zal de inrichting van notificaties zijn. Een van de belangrijkste functies van het pakket is immers het informeren van de beheerders. Het is belangrijk dat alle meldingen bij de juiste beheerders terecht komen, maar het is ook prettig als dit alleen belangrijke meldingen zijn. Om te voorkomen dat de beheerders overspoeld worden met “nutteloze” informatie, moeten er duidelijke plannen komen voor de implementatie en configuratie van notificaties. Deze configuratie is uiteindelijk samengesteld op basis van tests gedurende lange periodes. Deze tests zijn uitgevoerd door “er gewoon mee te werken”. Aan deze configuratie wordt meer aandacht besteed in hoofdstuk 8.3.

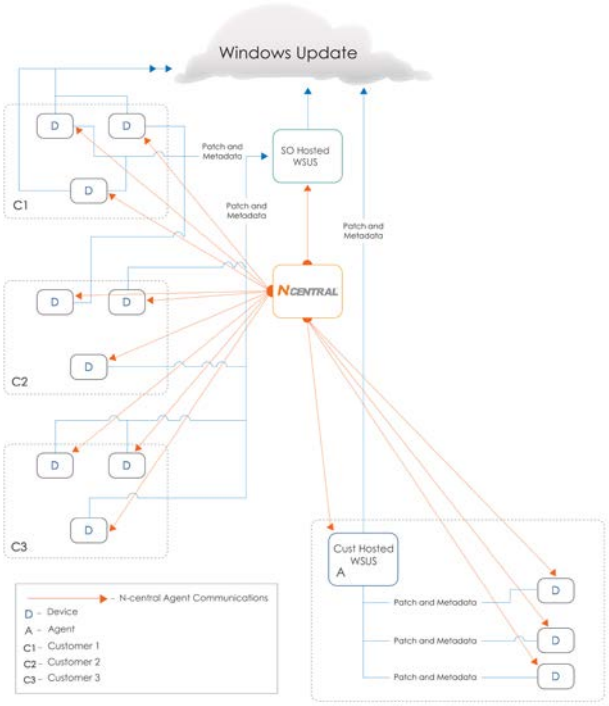
Een van de grote lijnen die men hierin van te voren kan trekken is bijvoorbeeld het indelen van meldingen op prioriteit. Zo zal server uptime een belangrijk punt worden. Daarnaast is het bijvoorbeeld minder belangrijk als de processor van de server zwaar belast wordt. Dit is geen prettig probleem, maar zolang de server nog beschikbaar is, heeft het niet direct prioriteit. Deze indeling is gemaakt op de impact dat een bepaald probleem kan hebben op de bedrijfscontinuïteit. Deze configuraties zijn toegelicht in hoofdstuk 6 van het testrapport (bijlage H).

Daarnaast zullen er keuzes moeten worden gemaakt over de manier van notificatie. Het is mogelijk de beheerders een mail te sturen, wat de meest gebruikte manier van informeren zal zijn. Daarnaast is het ook mogelijk om de beheerders een sms te sturen of zelfs te bellen. De standaard optie zal zijn de notificaties weer te geven op een dashboard. Deze dashboards kunnen vervolgens weer worden afgestemd op het type beheerder en de toegewezen verantwoordelijkheden.

Door wat wijzigingen van configuratie en visie betreffende de notificaties gedurende de tests is het belang van dashboards extra groot geworden. Daarom zal er in hoofdstuk 8.3.1 extra aandacht worden besteed aan de inzet en configuratie van deze dashboards.

7.2.4. Patch management

Om enige vorm van patch management te kunnen implementeren, is er nagedacht over 3 verschillende vormen van patch management welke in N-central kunnen worden geconfigureerd. Er is een mogelijkheid tot downloaden van de Microsoft Update Server, een WSUS server gehost door de MSP en een WSUS server op locatie van de klant. In onderstaande figuur 5 wordt een overzicht gegeven van de 3 oplossingen. Deze figuur is op volledige grote opgenomen in bijlage A, als figuur 18.



Figuur 5: Overzicht patch management architectuur

In onderstaande tabel wordt een advies gegeven welke oplossing wanneer in te zetten. De oplossing WSUS gehost bij de MSP wordt niet gebruikt. Het voegt voor Hupra niets toe om een doorgeefluik van patches te worden. Dit kost alleen maar bandbreedte.

Tabel 8: Afbakening architectuur keuze patch management

	0 – 10 Devices	10 > Devices
Patch architectuur	Gebruik maken van Microsoft Update Servers	WSUS server op locatie van de klant

Daarnaast is een keuze gemaakt voor het daadwerkelijke moment van het doorvoeren van de patches. Voor servers is dit moment zondag op maandag nacht gekozen, omdat hier mogelijk een herstart bij betrokken is. Mocht er dan iets fout gaan in het proces dan kan er maandagochtend meteen een beheerder klaarstaan. Op deze manier zal de downtime bij problemen beperkt blijven tot een minimum.

Voor werkstations is gekozen de patches iedere werkdag om 11:00 uur door te voeren. Op dat moment is de grootste kans dat alle machines aanwezig zijn en zijn ingeschakeld. Het kan zo nu en dan voorkomen dat een werkstation of laptop uitstaat of op dat moment niet aanwezig is in het netwerk. Daarom wordt het patch moment iedere dag herhaald. Zodat het geen ramp is als deze een keer wordt gemist.

Tabel 9: Advies patch momenten

	Server	Werkstation
Tijdstip doorvoeren patches	Wekelijks op maandag 01:00 uur.	Iedere werkdag om 11:00 uur.

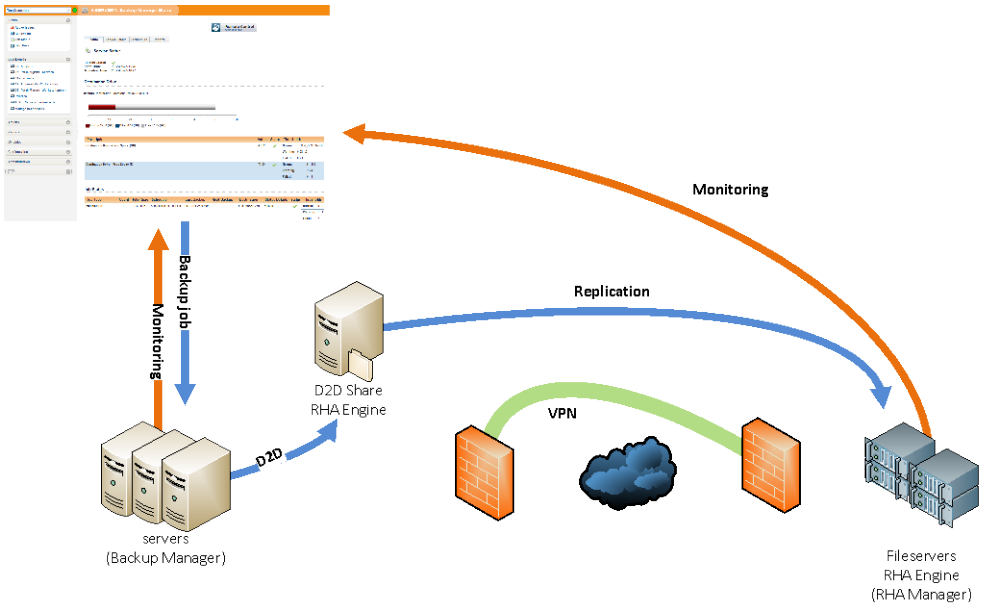
Het goedkeuren van de patches wordt opgenomen in de proces beschrijvingen. Deze zullen verder worden toegelicht in hoofdstuk 7.3.

7.2.5. Managed back-up

Voor de controle van een aantal backup oplossingen zijn templates ontwikkeld. Deze templates worden verder toegelicht in hoofdstuk 8.1.1. Daarnaast bestaat er nog een backup oplossing van N-central. Dit is een samenwerking tussen CA en N-able en is volledig geïntegreerd in N-central. Om deze oplossing werkend te krijgen, moet een duidelijk beeld van de architectuur worden gevormd.

De backup oplossing van N-central maakt gebruik van een op locatie geplaatste NAS of File server om de ARCserve D2D backups op te slaan. Daarna kan het geheel worden uitgebreid met een replicatie van de gemaakte backup naar een offsite locatie. Dit proces wordt weergegeven in figuur 6 op de volgende pagina.

Voor deze offsite locatie moet een speciale server van Hupra worden ingericht. Het is aan te bevelen deze server in een data center onder te brengen. Het onderbrengen in een data center brengt in deze situatie een aantal voordelen met zich mee. Denk hierbij bijvoorbeeld aan de beschikbaarheid van de server, de aanwezige bandbreedte, maar ook de gedeeltelijke afdekking van verantwoordelijkheden en beveiliging. Het gaat hier immers wel over data van klanten.



Figuur 6: Architectuur Backup Manager

7.2.6. Managed Onderhoud

Voor het uitvoeren van onderhoud zijn een aantal taken vastgelegd. Deze worden met de tijdsplanning in tabel 10 weergegeven. Ook hier is gekozen om de taken in het weekend uit te voeren, met voldoende tijd tussen de taken, zodat er zo min mogelijk overlap plaatsvindt.

Basis onderhoud zal bestaan uit een aantal basis taken, welke wekelijks dan wel maandelijks worden uitgevoerd. Deze taken zijn inzetbaar op servers en werkstations. De taken kunnen later uitgebreid worden met specifieke taken voor bijvoorbeeld Microsoft SQL servers. Onderstaande tabel geeft een overzicht van de basis taken.

Tabel 10: Voorstel planning onderhoud

Taak	Frequentie	Tijdstip
Schijfopruiming (CCleaner)	1x per week	ZO 13:00 uur
Verwijderen Temp Files	1x per week	ZO 13:15 uur
Defragmentatie (alle partities)	1x per week	ZO 13:30 uur
Volledige virus scan (Endpoint Security)	1x per week	ZO 18:00 uur
Schijfcontrole (CHKDSK)/ Geplande herstart	1x per maand	Eerste ZA 23:00 uur

Er is voor gekozen de meeste taken wekelijks uit te voeren, zodat de systemen goed “bij blijven”. Door deze taken wekelijks uit te voeren zullen deze uiteindelijk sneller verlopen, denk bijvoorbeeld aan de defragmentatie. De taak schijfcontrole wordt maar één keer per maand uitgevoerd vanwege de tijd die deze controle in beslag neemt en de server dus onbereikbaar zal zijn.

7.3. Procedures/Beheerproces

Hieronder worden een aantal adviezen betreffende de implementatie van procedures en processen bij gebruik van MSP software binnen Hupra aangedragen. Deze processen zijn over het algemeen voor de implementatie vastgelegd. Een aantal product specifieke processen zijn gedurende de test en implementatie van het project toegevoegd. De ondergenoemde procedures zijn lichtelijk ingedeeld naar ITIL standaarden. Er is bewust voor gekozen alleen bepaalde onderdelen uit deze standaard te gebruiken en alleen de meest belangrijke uit te werken. Voor een volledige implementatie heeft het bedrijf te weinig medewerkers. Bovendien zullen te strikte procedures alleen maar remmend werken op de flexibiliteit van Hupra.

7.3.1. Incident Management

Verantwoordelijkheden

Bij het optreden van een incident is het verstandig een aantal zaken van te voren duidelijk te hebben betreffende de verantwoordelijkheden. In eerste instantie zullen in het geval van Hupra alle beheerders een melding ontvangen. Mocht Hupra in de toekomst beschikbaarheid krijgen over meer beheerders dan kan de overweging worden gemaakt groepen te maken op het gebied van specialiteiten. Zo zullen in het geval van een netwerkstoring alleen de netwerkbeheerders worden ingelicht. Een beheerder blijf verantwoordelijk voor een ticket totdat dit ticket gesloten is of wordt geëscaleerd/overgedragen aan een andere beheerder. In het ticket systeem kan gecontroleerd worden wat de status van een ticket is en welke nog openstaan per beheerder.

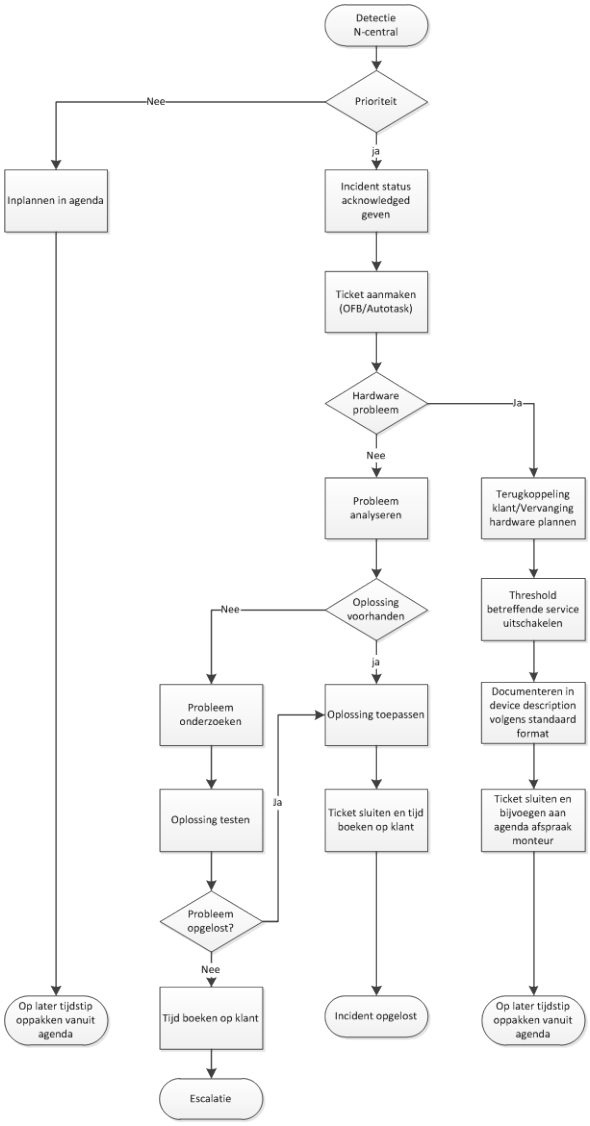
Oppakken incident

In het geval van Hupra zullen alle beheerders een melding ontvangen. De eerst beschikbare beheerder zal het probleem oppakken en deze in het software pakket de status ‘Acknowledged’ geven. Dan zullen er verder geen berichten over dat specifieke probleem worden gestuurd totdat het probleem wordt afgesloten. Op deze manier wordt het voor de andere beheerders ook duidelijk of het probleem reeds opgepakt is.

Meldingen van kritieke problemen zullen direct naar de beheerders gemaild worden of worden verstuurd via een SMS. Problemen die niet kritiek zijn, zullen alleen verschijnen in het zo geheten Dashboard. Beheerders op kantoor zullen vanuit dit dashboard werken en “tussendoor” de minder kritische problemen oppakken.

Meldingen die worden opgepakt zullen voor nu handmatig moeten worden aangemaakt in het ticket systeem. Deze slag moet in de toekomst geautomatiseerd worden. Dit is alleen mogelijk als er een koppeling met OFB gerealiseerd kan worden of als er duidelijkheid komt omtrent de aanschaf van een systeem als AutoTask. Er mag niet gewerkt worden aan een opgemerkt probleem zonder dat hiervan een ticket aanwezig is in het ticket systeem.

Het oppakken van incidenten is een van de belangrijkste processen. Het juiste ingrijpen hier kan voorkomen dat een incident gaat escaleren tot een probleem. Om dit proces extra helder te hebben is in figuur 7 (pag. 44) een visuele weergave van het proces gegeven. Deze is ook op volledige grote opgenomen in bijlage A, figuur 21.



Figuur 7: Visuele weergave proces incident oppakken

7.3.2. Problem Management

Terugkomende problemen

Voor terugkomende problemen met bijvoorbeeld hardware kan worden besloten de meldingen op deze service stop te zetten. Een voorbeeld hiervan is een processor welke aan de top van zijn belasting zit. De klant weet hiervan af en er is in overleg besloten dat de server over een aantal maanden vervangen zal worden voor een server met meer capaciteit. Om te voorkomen dat deze melding terug blijft komen wordt het threshold van de service verwijderd. De service wordt nog wel gecontroleerd, maar er zullen geen meldingen meer worden verstuurd en er zullen geen tickets worden aangemaakt.

Het is van belang deze aanpassing duidelijk te noteren in het ticket systeem. In bovengenoemde situatie moet bij vervanging van de server deze instelling weer ongedaan worden gemaakt. Bij het uitschakelen van een dergelijk threshold moet het gesloten ticket worden toegevoegd aan de afspraak in de agenda. Daarnaast moet een description worden toegevoegd in N-central. Deze description moet aan het volgende format voldoen:

“Threshold off: <service> - <rede van uitschakeling> - <datum ingang> - <verwachte einddatum>”

Deze descriptions worden met een filter in N-central gefilterd op de tekst “threshold off”. Vervolgens worden deze machines weergegeven in een lijst. Deze lijst kan bijvoorbeeld één keer in de twee maanden worden gecontroleerd of de uitschakeling van de thresholds nog terecht is, of dat deze inmiddels weer ingeschakeld had moeten worden.

Oppakken escalaties
Voor terugkerende incidenten of incidenten welke geëscaleerd zijn, moet een monteur worden gepland voor de klant. Er wordt nu niet vanuit het dashboard gewerkt maar de monteur krijgt in zijn agenda geplande tijd om het probleem (op klant locatie) te onderzoeken. Indien nodig kan dit worden herhaald totdat er een oplossing voor het probleem is. Resultaten en uren worden allemaal gedocumenteerd in het bijbehorende ticket.

7.3.3. Configuration Management

Asset informatie
De asset informatie uit het MSP systeem kan worden gebruikt om de CMDB aan te vullen met accurate informatie over systemen. In sommige gevallen kan de asset informatie op zich al een vervanging voor een CMDB zijn, echter dit is niet aan te raden vanwege het gebrek aan de mogelijkheid om zelf informatie toe te voegen en tot toevoeging van configuratie.

Bewaking correctheid informatie
De Asset informatie van systemen in de MSP software dient gecontroleerd te worden op correctheid om te voorkomen dat er misverstanden optreden bij het beheer van de machine. Denk bijvoorbeeld aan het aanschaffen van extra geheugen voor een server. Als men dit vanuit de MSP software wil doen, moet men er zeker van kunnen zijn dat de informatie correct is.

Dit proces zal ook raakvlakken hebben met change management. Bij iedere wijziging aan het systeem moet worden gecontroleerd of de asset informatie nog correct is. Desnoods moet een handmatige asset scan uitgevoerd worden.

Naamgeving systemen
Systemen worden onder een standaard naamgeving toegevoegd. Dit om duidelijkheid te verschaffen in N-central. Aan de naam van een systeem kan direct worden uitgelezen wat de primaire functies van dat systeem zijn. Deze naamgeving is vastgesteld op het volgende: functie-klant-nummer. Hupra gebruikt dit model al langer. Functies kunnen zijn:

- FS – File/Print/AD/DNS Server (Algemeen)
- TS – Terminal Server
- DB – Database Server
- NC – N-central
- RM/BM – Report Manager/ Backup Manager
- PC – PC
- NB/LP – Notebook/Laptop

Een voorbeeld van naamgeving kan zijn: FS-HUPRA-01.

Software/ Licence Appliance
De functies Software Applicance en Licence Applicance zijn bijzonder handig voor het beheren van de software bij een klant. Met Software Applicance kan worden afgedwongen welke software op het system aanwezig moet en/of mag zijn. Met de Licence Appliance functie kunnen controles op de licenties van de in het netwerk geïnstalleerde software worden uitgevoerd. Deze kunnen vervolgens vergeleken worden met de ingestelde licentie configuratie voor de betreffende klant. Hiermee kan de correctheid van de licenties binnen het netwerk worden gecontroleerd en worden onderhouden.

Het is belangrijk dat de in het pakket geconfigureerde licenties overeenkomen met de hoeveelheid werkelijk aangeschafte licenties van bijvoorbeeld Windows. Klopt dit niet, dan bestaat er een verhoogde kans op foutieve meldingen. Bij het toevoegen van een klant en het achteraf wijzigen van de licenties, dienen deze instellingen gecontroleerd te worden.

7.3.4. Change Management

Inplannen down time
Onderhoud aan een of meerdere servers dient vooraf te worden ingepland als server down time. Dit om te voorkomen dat tijdens werkzaamheden beheerders overspoeld worden met ‘nutteloze’ mail. Hiermee wordt ook voorkomen dat beheerders tijd gaan besteden aan een probleem dat eigenlijk niet bestaat. Als de uiteindelijke koppeling met het ticket systeem tot stand is gekomen, wordt dit proces extra belangrijk. Onnodige notificaties zullen onnodige tickets aanmaken. Het uitzoeken van deze tickets en het sluiten van de valse meldingen zal extra tijd kosten.

Patch approval
Patch approval dient als belangrijk onderdeel van Change Management te worden opgenomen. Het doorvoeren van patches kan gevolgen hebben voor de betreffende systemen. In het patch approval proces moet daar rekening mee worden gehouden. De architectuur van de patch omgeving en de afspraken betreffende de patch momenten zijn uitgewerkt in hoofdstuk 7.2.4. Het patch approval proces zal na iedere grote patch release moeten worden uitgevoerd. Vanuit Microsoft is dit meestal de derde dinsdag van de maand.

Controle correctheid service templates
Bij wijzigingen aan servers moet worden gecontroleerd of de ingestelde services en service templates nog wel overeenkomen met de functies die de server in de nieuwe situatie vervuld. De informatie kan meteen worden aangepast in het MSP pakket door de juiste service templates toe te wijzen of onnodige service templates te verwijderen.

7.3.5. Release Management

Software Deployment
Software Deployment kan worden uitgevoerd via het MSP pakket of via een Group Policy. Het is belangrijk om ook na een deployment te controleren of de service templates nog aansluiten bij de servers/werkstations. Indien nodig kunnen deze aangepast worden. Een software deployment moet altijd eerst op een testomgeving worden uitgevoerd.

Toevoegen nieuwe systemen/klanten
Voor het toevoegen van nieuwe klanten of systemen bij bestaande klanten is een checklist ontwikkeld van de te nemen acties en de standaard instellingen voor de nieuwe systemen. Deze checklist is opgenomen als bijlage E. Daarna zal moeten worden gecontroleerd of de juiste service templates zijn toegepast en indien nodig aangepast moeten worden. In dit proces moet ook het juiste aantal licenties voor de klant geconfigureerd worden. In de checklist is dit verder omschreven.

Patch management
De release fase van het patch management zal een geautomatiseerde fase zijn. Het goedkeuren van de patches valt onder change management. De releases zullen dan wel geautomatiseerd verlopen, echter het is wel belangrijk om hiervan goed op de hoogte te zijn en vooraf te onderzoeken wat voor gevolgen het doorvoeren van de patches kan hebben voor de bestaande software. Ook het moment waarop de patches worden uitgevoerd (hoofdstuk 7.2.4) dient bekend te zijn.

Updates N-central server
Er moet regelmatig (1x per maand) worden gecontroleerd of er nieuwe releases, service packs of hotfixes beschikbaar zijn voor de N-central server. Deze updates kunnen vervolgens worden geëvalueerd en worden toegepast. Voor deze evaluatie kan men gebruik maken van de testomgeving. Daarnaast zal natuurlijk een backup van de N-central configuratie moeten worden gemaakt. De procedure voor een N-central server update is beschikbaar in het N-able Resource Center.

7.3.6. Reporting
Reporting is voor een MSP een belangrijk onderdeel. Omdat de MSP de problemen voor de klant op de achtergrond probeert te houden, heeft de klant veel minder inzicht in wat er daadwerkelijk gedaan wordt. Het is daarom belangrijk de klant dat overzicht terug te geven in de vorm van een rapportage.

Rapportage kan met de meeste MSP producten volledig geautomatiseerd en aangepast worden. Deze rapportages moeten als onderdeel van de factuur worden meegestuurd om de klant extra inzicht te geven in haar omgeving. (From Promises to Proof: How To Demonstrate Value to Your Customers, 2006). Rapportage is tenminste nodig op de volgende onderwerpen:

Service Level Management/ Availability Management
Geeft een overzicht van de behaalde beschikbaarheid van de systemen waarover een Service Level Agreement is afgesloten. Tevens zal dit overzicht inzicht geven in het behalen van de afgesproken SLA en waar het eventueel fout is gelopen.

Service Continuity Management
Dit rapport geeft een overzicht van de incidenten die de afgelopen periode zijn opgetreden en zijn waargenomen door het pakket. Daarnaast zal dit rapport een goede aanvulling zijn op de werkzaamheden opgenomen in de factuur.

Backup Report
Voor klanten die een Managed Backup oplossing afnemen moet iedere maand een Backup rapport worden aangeleverd. Dit rapport zal de klant een overzicht geven van de conditie van de backup. Dit rapport bevat een overzicht van alle backup taken en de bijbehorende status. Daarnaast geeft het overzichten van de grootte van de backup, tot hoever men kan herstellen en de beschikbare ruimte op de doel locatie en of hier in de toekomst uitbreiding nodig is.

Capacity Planning Report (Report Manager)
Als extra aanvulling op deze basisrapporten kan er ook worden besloten een rapport voor Capaciteitsbeheer toe te voegen. Dit rapport is alleen beschikbaar in de Report Manager uitbreiding. Dit rapport zal de klant inzicht geven in de gebruikte capaciteit (Processor, Harde schijf, Geheugen en Netwerkverkeer) en eventuele toekomstige problemen met machines welke aan hun maximum zitten.

Endpoint Security/ Firewall incident (Report Manager)
Ook dit rapport zal alleen beschikbaar zijn in Report Manager. Er kan worden overwogen dit rapport als extra toe te voegen. In dit rapport wordt een overzicht gegeven van alle meldingen uit de SonicWall firewalls en alle Endpoint Security systemen en zal een totaaloverzicht geven van de beveiliging van het netwerk.

7.3.7. Planning
Nu er een kort overzicht is gegeven van de procedures die komen kijken bij het proactieve beheer, wordt er nog even ingegaan op de initiatie van deze procedures. Een aantal procedures geïnitieerd uit een bepaalde gebeurtenis, zoals een incident of een aanpassing.

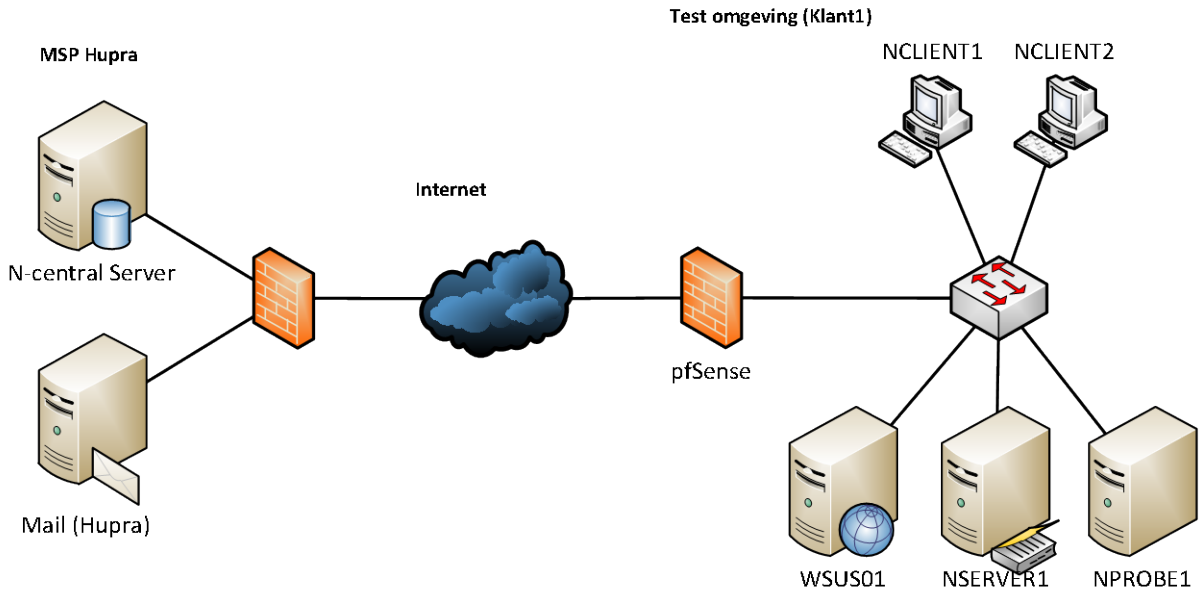
Andere procedures worden automatisch uitgevoerd, bijvoorbeeld de maandelijkse rapportage. Voor deze procedures is minimale aandacht van de beheerder nodig.

Een derde vorm zijn procedures die “uit het niets” moeten worden geïnitieerd. Hiervoor is discipline nodig. Procedures als het onderhoud aan de N-central server en patch approval zullen één maal in een bepaalde periode moeten worden uitgevoerd. Het is aan te raden deze taken te plannen als interne opdrachten in de agenda’s van beheerders. Het is goed om deze zaken gestructureerd in te plannen, anders wordt het vergeten.

8. Test, Implementatie

Als laatste stap in het proces zijn alle plannen en wensen uitgewerkt, getest in een speciaal daarvoor opgestelde testomgeving, en geïmplementeerd in de productie omgeving. In dit hoofdstuk worden de tests en implementatie van de verschillende onderdelen verder toegelicht. De fases test en implementatie zijn samengevoegd omdat deze tijdens de uitvoering van het project veel overlap hebben gehad, zoals eerder toegelicht in hoofdstuk 3.4.4. De belangrijke resultaten en grote lijnen van de tests worden in dit hoofdstuk toegelicht. Gedetailleerde informatie over te tests is terug te vinden in het testrapport, bijgevoegd als bijlage H.

Allereerst is er een basis testomgeving ontwikkeld met een N-central server installatie bij Hupra. Daarnaast zijn een aantal servers, werkstations en een probe geplaatst op een offsite locatie. Er is gekozen voor deze offsite locatie om op deze manier een gelijkwaardige omgeving te creëren gelijk aan een productie omgeving van een klant. Onderstaande afbeelding geeft een overzicht van de gebruikte testomgeving.



Figuur 8: Basis testomgeving (TestCustomer)

Deze basis testomgeving zal naast de productie omgeving blijven bestaan en zal gebruikt kunnen worden voor risicovolle tests. Overige tests kunnen worden uitgevoerd op de productie server, zolang deze tests geen directe gevolgen hebben voor de geïmporteerde klanten.

De standaardprocedure voor het uitvoeren van deze tests is als eerste uitvoeren op de virtuele ‘schone’ testomgeving. Daarna kan de test door gezet worden naar de interne omgeving van Hupra (Figuur 2). Als derde stap kan gekozen worden deze test uit te voeren op een select aantal klanten, alvorens de aanpassingen over het gehele systeem te implementeren.

8.1. Installatie/Deployment N-central server

De N-central server is te downloaden van het N-able Resource Network en wordt aangeleverd als een ISO bestand voor installatie. Installatie van de N-central server is vrij rechttoe rechtaan. Het installatie bestand (iso) bevat een door N-able aangepaste versie van Red Hat Enterprise Linux, welke voorgeconfigureerd is en uitgerust met alle benodigde software, aanvullende pakketten en standaard configuraties.

Tijdens de installatie worden een aantal standaard vragen gesteld voor bijvoorbeeld netwerk configuratie, server naam, landinstellingen, enz. Na de installatie kan meteen via de web interface worden ingelogd met het administrator account. Na het aanpassen en toevoegen van gebruikers kan men meteen aan het werk met een basis configuratie van de server.

De server is voor nu geplaatst in het netwerk van Hupra, op een van de Hyper-V servers. HV-HUPRA-01 om precies te zijn. N-central is in eerste instantie geplaatst in een virtuele machine met 4GB geheugen. Gedurende de tests zijn wat problemen aan het licht gekomen met een crashende N-central server. Uiteindelijk bleek dit een probleem te zijn met tekort aan geheugen. Dit wordt echter nergens duidelijk door het pakket aangegeven. Uiteindelijk is in samenwerking met N-able support de oorzaak gevonden. Een upgrade naar 12GB heeft het probleem voor de eerste jaren opgelost.

De configuratie van de server dient nog wel verder afgestemd te worden op de wensen van de organisatie. Verder zullen een aantal uitgebreide functies niet werken zonder aangepaste configuratie en zullen maatwerk oplossingen nog niet beschikbaar zijn, omdat deze nog moeten worden geschreven. Deze onderdelen zullen in de rest van dit document verder worden uitgewerkt.

Daarnaast is het te overwegen de N-central server in de toekomst in een data center onder te brengen, ter verbetering van de beschikbaarheid. Deze beschikbaarheid heeft al in de testfase voor problemen gezorgd met o.a. de notificaties. Bij een herstart van de N-central server worden meldingen verstuurd van down time op klant systemen, terwijl hier eigenlijk niets aan de hand is.

8.1.1. Services/ Service templates

Gedurende de tests en implementatie van de verschillende onderdelen is meerdere malen naar voren gekomen dat de standaard service templates opgenomen in N-central niet geheel voldoen aan de verwachtingen. De templates kunnen meestal wel worden gezien als basis, echter ontbreken er een aantal services om het template compleet te maken en de verwachte kwaliteit te bieden. Gedurende de tests zijn de volgende aangepaste service templates ontwikkeld:

- Windows server (uitgebreid met een aantal Event Logs voor o.a. schijffouten)
- HP Servers (Hardware monitoring)
- Hyper-V Clients (Hyper-V integratie monitoring)
- Acronis Backup & Recovery (monitoring van de backup)
- Solcon Online Backup (monitoring van de Solcon backup)
- CA Replication & High Availability (monitoring van de replicatie slag voor Managed Backup)
- SonicWall (uitgebreid met interface status, traffic monitoring, en IPS monitoring)
- Managed Maintenace (monitoring van de onderhoudstaken, Managed Maintenance)

8.2. Installatie klant omgeving

Na het installeren van de N-central server is de eerstvolgende logische stap het toevoegen van een aantal klanten en servers. Deze stap moet dienen als testfase voor het toevoegen van nieuwe klanten aan het systeem, maar ook voor het toevoegen van bestaande klanten. Daarom is deze test in twee versies uitgevoerd. Als eerste een test op een schone nieuwe omgeving en daarnaast op een “vuile” omgeving. Hieronder worden de twee scenario’s beschreven.

8.2.1. Basis Installatie

Voor de test met een schone omgeving is een testomgeving van virtuele machines opgesteld volgens figuur 8 op pagina 49. Deze omgeving zal vervolgens worden toegevoegd als klant ‘TestCustomer’. De machines van deze test klant zullen verschillende virtuele machines zijn, met verschillende operating systems (Windows) om zo veel mogelijk de verschillende aspecten van deze systemen na te bootsen.

Het basis netwerk van ‘TestCustomer’ is vergelijkbaar met een klein basis netwerk bij een zakelijke klant. Het netwerk zal bestaan uit een server met daarop Active Directory, DNS, DHCP en een aantal shares. Daarnaast zal er een server aanwezig zijn waarop de Windows Probe kan worden geplaatst. Aan de rand van het netwerk is een firewall geplaatst welke ook zal worden uitgelezen met N-central. Als laatste zijn er vanzelfsprekend een aantal werkstations aanwezig waarop de agent software kan worden getest.

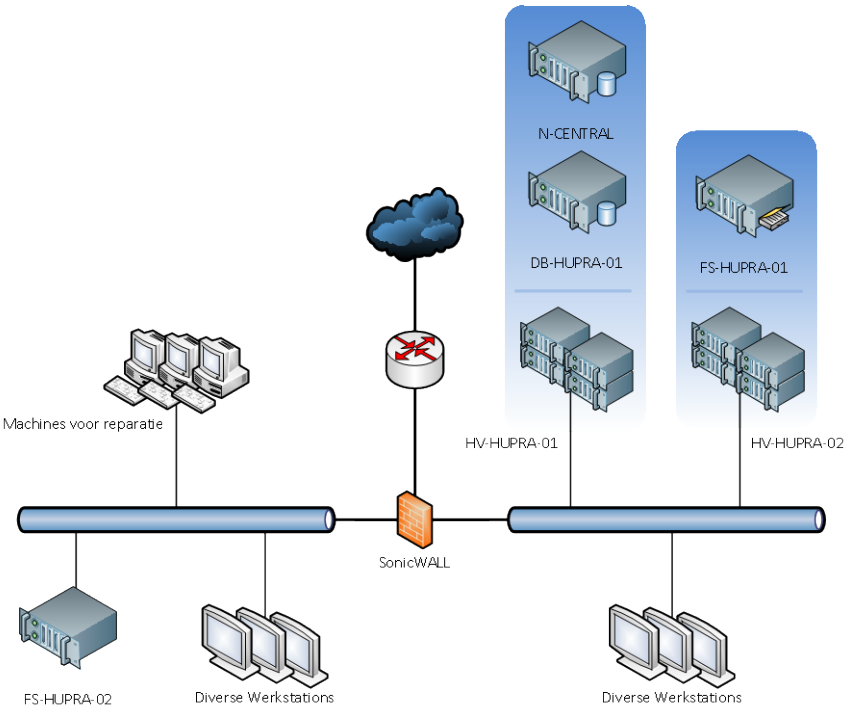
Uitvoering van deze test verliep vrijwel vlekkeloos en resultaten zijn gebruikt voor het opstellen van richtlijnen voor procedures en de installatie checklist. Omdat deze test zo vlekkeloos verliep, is er voor gekozen een volgende basis test uit te voeren op een “vuile omgeving”, een omgeving welke al een aantal jaar intensief gebruikt wordt.

Een aantal bijzonderheden uit de basis test:

- Installatie op Windows server 2008 core niet mogelijk
- Geen ondersteuning voor Windows 8 Server
- Problemen bij automatische verspreiding in werkgroepen (Authenticatie)

8.2.2. Basis installatie “Vuile omgeving”

Als toevoeging op de eerste test (schone omgeving) is besloten een extra test uit te voeren op een ‘vuile omgeving’. Hiervoor is het kantoor netwerk van Hupra gekozen (Figuur 9 pag. 52). Deze omgeving wordt ‘vuil’ genoemd omdat deze al enkele jaren wordt gebruikt. Daarnaast zijn er veel verschillende configuraties aanwezig. Zoals bijvoorbeeld het gebruik van verschillende virus scanners en verschillende instellingen voor Windows Updates, gescheiden netwerken voor kantoor en technische dienst en veel verschillende besturingssystemen uiteenlopend van Small Business Server 2003 tot Windows Server 2008 R2 Enterprise. Alle werkstations zijn nagenoeg wel uitgerust met Windows 7 Professional.



Figuur 9: Omgeving Hupra

Bij de uitvoering van deze test is de checklist, opgesteld in de eerdere test, aangehouden.

Bij het importeren van de machines uit de probe discovery zijn in de Hupra omgeving een aantal problemen aan het licht gekomen. Zo bleek dat een aantal machines niet correct in het domein waren opgenomen, waardoor het voor de probe onmogelijk werd om de agent software geautomatiseerd te verspreiden. Problemen hiermee zijn snel en makkelijk op te lossen door deze machines als nog goed in het domein op te nemen of ervoor te kiezen deze machines handmatig toe te voegen aan N-central. Voor dit handmatig toevoegen is fysieke toegang tot de machine nodig. Het handmatig toevoegen is niet meer dan het handmatig installeren van de agent. De registratie met de N-central server wordt automatisch opgepakt.

Endpoint Security

Een tweede probleem bij implementatie op de “vuile” omgeving was het gebruik van veel verschillende virus scanners. Voor een succesvolle uitrol van N-able’s Endpoint Security is een ‘schone’ machine zonder geïnstalleerde virus scanner vereist. Een aantal van de reeds geïnstalleerde virus scanners kan automatisch worden verwijderd. Echter ging dit voor Norman niet op. Hupra heeft voorheen altijd Norman verkocht aan zakelijke klanten, daarom zullen veel bestaande klanten een Norman product geïnstalleerd hebben welke bij overgang naar Managed Services vervangen moeten worden voor N-central Endpoint Security.

Er zijn meerdere mogelijkheden om de reeds geïnstalleerde virus scanner te verwijderen. Zo is het mogelijk op afstand in te loggen of fysiek achter de machine plaats te nemen. In beide gevallen zal de gebruiker moeten worden gestoord.

Alvorens over te gaan tot een van de hierboven genoemde oplossingen is een test uitgevoerd met de scripting functie van N-central in combinatie met wat programmatuur van Norman. Norman biedt op de site software aan voor geautomatiseerde verwijdering van de virus scanner. Dit programma delnvc5.exe kan worden uitgevoerd met een /quiet functie. Door deze taak geautomatiseerd te laten uitvoeren vanuit N-central, zijn zonder hinder van de gebruikers de laatste Norman installaties op de achtergrond verwijderd, waarna de Endpoint Security software van N-able geïnstalleerd werd.

SonicWall

Zowel in de kantoor omgeving van Hupra, als in de omgevingen van haar klanten, wordt bijna altijd gebruik gemaakt van een SonicWall Firewall oplossing. N-central biedt een standaard template voor het monitoren van een SonicWall. Echter betrof dit alleen basis gegevens als connectivity en de beschikbaarheid van de management console. Deze services zijn d.m.v. een SNMP connectie uitgebreid om een veel completere lijst te krijgen met o.a. traffic informatie en inzicht in het aantal security incidents opgemerkt door de IPS van de SonicWall. Deze uitgebreide lijst is ondergebracht in een nieuw template, welke ook zal worden toegepast op de SonicWall systemen bij klanten.

Services

Add | Delete | Create Service Template | -- More Actions --

Service	Status	Transition	Probe/Agent	Last Scan Time
Connectivity	✓	2012-Apr-17 12:12	fs-ace-01 - Windows	2012-May-09 14:51
FW-SonicWALL	✓	2012-Apr-09 02:43	fs-ace-01 - Windows	2012-May-09 14:49
HTTP	✓	2012-Apr-17 11:21	fs-ace-01 - Windows	2012-May-09 14:49
HTTPS	✓	2012-Apr-17 11:21	fs-ace-01 - Windows	2012-May-09 14:51
Interface Health - X0 (LAN)	✓	2012-May-09 14:17	fs-ace-01 - Windows	2012-May-09 14:51
Interface Health - X1 (WAN)	✓	2012-May-09 13:17	fs-ace-01 - Windows	2012-May-09 14:51
SonicWALL Connections	✓	2012-May-09 14:47	fs-ace-01 - Windows	2012-May-09 14:51
SonicWALL CPU - 0	✓	2012-May-09 11:58	fs-ace-01 - Windows	2012-May-09 14:53
SonicWALL Memory	✓	2012-May-09 14:47	fs-ace-01 - Windows	2012-May-09 14:51
SSH	✓	2012-Apr-17 11:21	fs-ace-01 - Windows	2012-May-09 14:52
Traffic - X0 (LAN)	✓	2012-May-09 14:47	fs-ace-01 - Windows	2012-May-09 14:46
Traffic - X1 (WAN)	✓	2012-May-09 12:31	fs-ace-01 - Windows	2012-May-09 14:51

Figuur 10: SonicWall Monitoring

Daarnaast zijn er nog een aantal kleine problemen aan het licht gekomen met wat instellingen van de Windows Update Service (zie patch management hoofdstuk 8.4) en de connectivity monitoring. De standaard firewall instellingen op nieuwere Windows versies staan een binnenkomende ping aanvraag niet toe. De connectivity test van N-central is afhankelijk van deze ping aanvraag. Een aanpassing in de Windows Firewall voor het toestaan van icmp-echo aanvragen lost het probleem op.

Een ander nieuw onderdeel in deze testomgeving was het monitoren van fysieke servers. N-central is in staat gegevens over de hardware, zoals fan, raid-controller, PSU, e.d. te monitoren. In de basis testomgeving (TestCustomer) zijn alleen tests uitgevoerd op virtuele machines. De configuratie van deze hardware monitoring heeft een paar kleine haken en ogen betreffende instellingen voor de monitor software van de fabrikant en de SNMP instellingen. Omdat bij Hupra en haar klanten alleen HP hardware wordt gebruikt, is alleen gefocust op de mogelijkheid HP hardware te monitoren.

Hiervoor is installatie van de HP Insight Manager Agent nodig. Vervolgens dienen de instellingen van SNMP op de machine aangepast te worden. Zodat SNMP ook te benaderen is vanaf de N-central server. Voor de exacte configuratie wordt verwezen naar de installatie checklist (bijlage E).

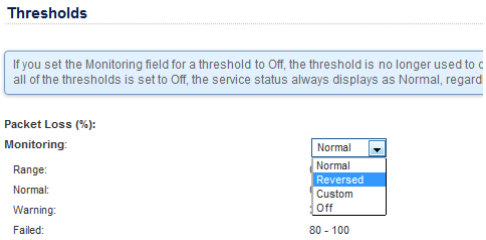
8.3. Notificaties

Een van de belangrijkste configuraties aan een nieuwe N-central omgeving zijn de Notification profiles. In deze profielen wordt geconfigureerd welke incidenten gemeld moeten worden via een email of sms. Deze configuratie is erg belangrijk voor een goede werking van N-central. Er is bewust gewacht met deze test en implementatie totdat er een aantal test machines waren opgenomen in het systeem.

Een notificatie profiel kan meerdere services bevatten. Per profiel worden één of meerdere ontvangers geconfigureerd met, indien gewenst, een vertraging op het verzenden van de mail. Daarnaast is het mogelijk een herhaling in te stellen mocht het probleem nog steeds actief zijn. De configuratie voor deze profielen is opgenomen in hoofdstuk 7.2.3 en hoofdstuk 6, bijlage H.

Na het invoeren van de notificatie profielen zijn deze getest door op een aantal test servers de thresholds van een bepaalde service op reversed te zetten, waarmee deze worden omgedraaid. Op deze manier kan een melding worden afgedwongen. Vervolgens kan simpel worden gecontroleerd of de meldingen op de juiste plekken aankomen.

Een eerste opzet voor de Notification profiles is vastgelegd in hoofdstuk 6 van het adviesrapport. Zaken als notificaties zullen altijd aan wijzigingen onderhevig zijn en zullen constant moeten worden aangepast om in te spelen op de behoeftes van de beheerders en de klanten.



Figuur 11: Threshold wijzigen

Na deze notificatie profielen enige weken getest te hebben, is duidelijk geworden dat deze teveel informatie opleveren. De mailboxen worden overspoeld met mail. De hoeveelheid mail neemt al snel het belang van de meldingen weg. Er wordt hoogstens even snel doorheen gekeken, met het gevolg dat belangrijke berichten over het hoofd worden gezien.

In een tweede notificatie ontwerp is meer gelet op het belang van de meldingen en is het aantal mails drastisch teruggebracht tot alleen kritische meldingen. De opzet is hetzelfde gebleven aan de opzet van de eerder vastgestelde notificatie profielen, echter is de insteek veranderd. Alleen kritische meldingen worden per mail verstuurd. Deze worden niet herhaald en worden niet automatisch geëscaleerd. Het is aan beheerders de verantwoordelijkheid te nemen en deze melding serieus op te nemen. Bovendien is met deze opzet rekening gehouden met een mail koppeling voor een ticket systeem. Men wil immers geen dubbele tickets aanmaken.

8.3.1. Dashbords

In dit tweede notificatie ontwerp is ook het belang van dashboard groter geworden. De meest kritische storingen worden dan wel via de mail naar de beheerders verstuurd, de minder kritische niet. Ook deze minder belangrijke meldingen kunnen van belang zijn bij het voorkomen van grote storingen. Deze meldingen moeten op een duidelijke wijze kenbaar worden gemaakt aan de beheerders zonder dat hiervoor meteen een melding moet worden verstuurd.

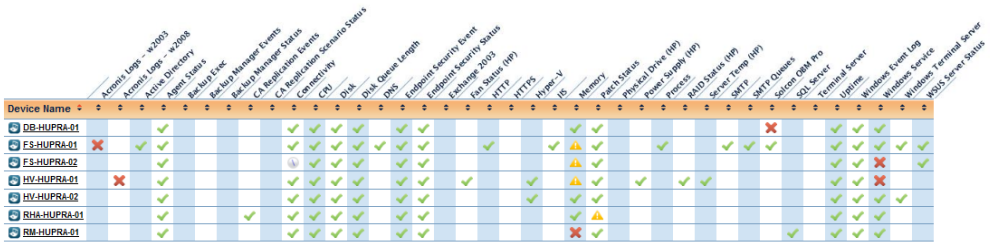
Om dit gat in het nieuwe notificatie profiel te dichten, is na een aantal brainstormsessies met een aantal beheerders een beeld gevormd over welke meldingen belangrijk zijn om te zien, maar niet belangrijk genoeg om een mail van te ontvangen. Deze meldingen zijn vervolgens verder uitgewerkt naar een tweetal dashboards.

De meldingen zijn onderverdeeld in servers Prio I en servers Prio II. Het Prio I dashboard zal meldingen bevatten voor services waarvan de klant direct hinder kan ondervinden. Dit zijn naast de kritieke services als uptime en connectiviteit bijvoorbeeld cpu, dns, disk, active directory, backup status, enz. Van een aantal services uit dit dashboard zullen ook email meldingen worden verstuurd. Het streven zal zijn dit dashboard altijd op groen te houden.

Het Prio II dashboard heeft als basis het Prio I dashboard. Dat wil zeggen, alle services van Prio I plus een aantal extra services. Het Prio II dashboard moet een totaaloverzicht geven van de belangrijke en minder belangrijke services. Hierin zijn ook services opgenomen die niet direct hinder voor de klant zullen betekenen, maar wel belangrijk zijn bij het voorkomen van storingen. Dit kunnen bijvoorbeeld services zijn als patch management, WSUS status, Event logging, Windows services, enz.

Hieronder worden de dashboards weergegeven. Deze zijn ook op volledige grote opgenomen als afbeelding 19 en 20, bijlage A.

Figuur 12: Prio I Dashboard



Figuur 13: Prio II Dashboard

8.4. Patch management

Het testen van Patch management is een tijdrovende taak. Op een selecte groep servers/werkstations zijn een aantal test profielen geactiveerd. Deze profielen zijn beschreven in het voorstel patch management. Dit voorstel is als bijlage I toegevoegd. Voor de tests en implementatie is de configuratie zoals beschreven in hoofdstuk 7.2.4 aangehouden.

De patch management tests zijn op een beperkt aantal servers toegepast en bevatten meer patch momenten dan de productie servers. Voor deze tests zijn daarom een aantal nieuwe test profielen aangemaakt. Dit om het proces enigszins te versnellen en te voorkomen dat men weken moest wachten voordat het resultaat onderzocht kon worden. De testprofielen zijn handmatig verschoven voor installatie op servers rond 22:00 uur en voor werkstations iedere dag rond 11:00 uur om er zeker van te zijn dat deze ingeschakeld waren.

Controle van het patch proces vond iedere volgende dag plaats. De status van dit proces kan worden uitgelezen via N-central, maar ook handmatig op de servers/werkstations zelf en de WSUS server op de betreffende locatie. Vervolgens konden er direct aanpassingen worden gemaakt die werden meegenomen in de eerstvolgende patchronde (de volgende avond) totdat het proces naar wens verliep.

De eerste doelen van het patch management waren een complete inrichting en automatisering van de patchrondes, waarin alle machines werden meegenomen. Dat een machine niet helemaal up-to-date was, had geen gevolgen voor deze test. Het is belangrijker dat de machine meeloopt in het patch proces. Daarna is het een kwestie van tijd voordat de machine helemaal up-to-date zal zijn.

Verder zijn de volgende punten getest:

- Deelname aan het patch proces (handmatige controle).
- Duur patch proces (gegevens uit N-central).
- Controle over herstart servers (gegevens uit N-central).
- Interruptie gebruikers (test op eigen werkstation).

De eerste test met Patch management zijn uitgevoerd in de eerder opgestelde testomgeving ‘TestCustomer’. Ongeveer een week later is dezelfde test ingezet op de interne systemen van Hupra. Wat opviel is dat de test in de schone ‘TestCustomer’ omgeving meteen zonder problemen verliep. De test in het kantoor netwerk van Hupra verliep niet meteen vlekkeloos. Deze problemen vielen vrijwel allemaal te wijten aan de oude WSUS installatie en de bijbehorende Group Policies. Het verwijderen van deze policies (deze zijn immers niet meer nodig) en een herinstallatie van de WSUS hebben deze problemen opgelost. Er is voor gekozen meteen over te gaan tot herinstallatie van de WSUS omdat deze toch geen vitale informatie bevat, en men meteen verzekerd kan zijn van een ‘frisse’ WSUS omgeving.

Na dit proces een aantal weken nauwlettend in de gaten te hebben gehouden, is besloten deze test door te zetten naar drie klanten van Hupra. Dit zijn klanten van verschillende omvang, waarop verschillende profielen van toepassing zullen zijn. Zo kunnen tests uitgevoerd worden met WSUS op locatie van de klant voor zowel servers als werkstations, WSUS op locatie met alleen servers en een profiel welke gebruik maakt van de Microsoft Update servers.

In de onderstaande tabel worden de belangrijkste instellingen voor het patch management weergegeven zoals deze zijn ingezet in de test omgevingen. Deze zijn in de productie omgeving aangepast naar de instellingen beschreven in het advies van hoofdstuk 7.2.4.

Tabel 11: Profiel instellingen

	MSU		WSUS	
	Server	Werkstation	Server	Werkstation
Schedule Install Day	-	Iedere dag	-	Iedere dag
Schedule Install Time	22:00	11:00	22:00	11:00
Patch Server	Microsoft Update	Microsoft Update	WSUS klant locatie	WSUS klant locatie

8.4.1. WSUS configuratie

Een probleem dat regelmatig naar voren kwam tijdens de tests is een bestaande WSUS oplossing in een gebruikte omgeving. Voordat men iets kan doen met deze omgeving zullen alle Group Policies betreffende WSUS uitgeschakeld of verwijderd moeten worden. Daarnaast kan het ook handig zijn een verse installatie van WSUS uit te voeren. In sommige gevallen zal dit niet mogelijk zijn en moet geprobeerd worden de instellingen zoveel mogelijk standaard te configureren. Er is gebleken dat er op deze manier de minste kans op problemen zal zijn. Uit ervaringen met de testomgevingen is gebleken dat er beter een schone installatie van WSUS uitgevoerd kan worden. Dit kost meestal minder tijd dan het oplossen van de problemen achteraf.

8.4.2. Windows Update Service

Naast problemen met de WSUS server is uit de test gebleken dat er ook wel eens wat problemen met de clients kunnen optreden. Het meest voorkomende probleem hierin was dat een client weigerde te koppelen met een WSUS server. Vaak was dit een probleem in de configuratie van de client en kon det opgelost worden door een aantal simpele stappen te volgen zoals de Windows Update Service resetten. Hiervoor is later ook een script gevonden op de N-able community forums die de bovengenoemde opschoning automatisch zal uitvoeren. Details hierover zijn te vinden in hoofdstuk 5 van het testrapport, bijlage H.

8.5. Maintenance

Geplande taken kunnen gemakkelijk gecontroleerd uitgevoerd worden op servers en werkstations in N-central. Dit brengt de mogelijkheid met zich mee om gecontroleerde onderhoudstaken uit te voeren op een groep servers of werkstations. Deze onderhoudstaken zijn vastgelegd in een onderhoudsplan en zullen volledig geautomatiseerd worden uitgevoerd m.b.v. N-central. Deze taken kunnen zowel op servers als op werkstations met een professional licentie worden uitgevoerd.

De standaard scripts zijn getest op de 'TestCustomer' omgeving. Al snel werd duidelijk dat deze scripts niet geheel voldeden aan de verwachtingen. De scripts schieten meestal tekort in functie. Bijvoorbeeld het script voor defragmentatie had geen mogelijkheid meerdere partities te defragmenteren. Voor iedere partitie moest een aparte taak worden aangemaakt. Het moge duidelijk zijn dat hierbij veel werk komt kijken en het onmogelijk is een universeel inzetbare taak te maken.

Om deze tekortkomingen weg te nemen zijn een aantal scripts ontwikkeld. Daarnaast is het nodig geweest bepaalde basis programma's te installeren. Bijvoorbeeld CCleaner met bijbehorende configuratie, om gebruik te kunnen maken van de schijfopruiming taak. Deze basisprogramma's zullen worden gebruikt in de opruimingsscripts.

Er zijn vervolgens twee scripts ontwikkeld en getest. Een script voor het defragmenteren van de harde schijven en een script voor het uitvoeren van een schijfcontrole en een geplande herstart. Deze scripts zijn opgenomen als bijlage C.

8.5.1. Defragmentatie

Het defragmentatie script is ontwikkeld om alle partities op een systeem te defragmenteren. Bij toevoegen van deze onderhoudstaak moet gecontroleerd worden of er gebruik wordt gemaakt van een SSD. Is dit het geval, dan mag de defragmentatie taak voor dat systeem niet worden geactiveerd. Er is helaas nog geen mogelijkheid dit automatisch te laten controleren. Op een systeem voorzien van traditionele harde schijven gaat het script als volgt te werk. Eerst worden alle mogelijke stations letters gecontroleerd op aanwezigheid van een harddisk. DVD drives en netwerk mappen worden er uit gefilterd. Vervolgens zal voor deze partities een defragmentatie op de achtergrond starten, waarna het script stopt. De Event logging van het betreffende systeem wordt vervolgens gecontroleerd op fouten uit het defragmentatie process.

8.5.2. Schijfcontrole

Het schijfcontrole script werkt volgens een soortgelijk principe. De eerste stap is de controle van de aanwezigheid van een harde schijf op een stations letter. Vervolgens zal een dirty bit worden geactiveerd die ervoor zorgt dat bij de eerstvolgende herstart een schijfcontrole op het systeem wordt uitgevoerd. Ook hier is terugkoppeling via de logging in de Windows Event Log. Na het aanpassen van de flag zal het script de server laten herstarten en de geplande controle uitvoeren. Dit script zorgt er daarnaast ook voor dat de server iedere maand een preventieve herstart krijgt.

De genoemde taken zijn geïmplementeerd en getest volgens het schema van hoofdstuk 7.2.6.

8.5.3. CCleaner uitrol

Voor de uitrol van CCleaner is een portable versie van CCleaner gebruikt. Er is gekozen voor de portable versie omdat hieraan makkelijk een CCleaner configuratie bestand (INI) kan worden toegevoegd. Deze configuratie is zo algemeen mogelijk gehouden zodat deze over verschillende systemen ingezet kan worden, op zowel servers als werkstations. Vanwege de inzet op werkstations is rekening gehouden met het gebruikersgemak. Zo zullen bijvoorbeeld de opgeslagen wachtwoorden en cookies in internet browsers niet worden opgeruimd om de gebruiker zo min mogelijk tot last te zijn.

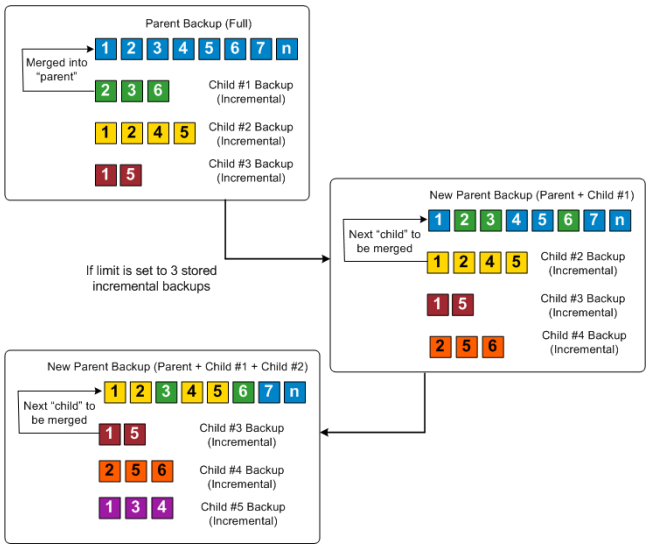
Het gehele pakket is vervolgens in een installatiebestand ingepakt zodat het met de “Push Third Party Software” functie van N-central verspreid kan worden over de doel machines. Het installatie-bestand is eenmalig geconfigureerd en toegevoegd aan de N-central Software Repository. De uitrol kan gemakkelijk via een geplande N-central taak worden uitgevoerd. De INI configuratie voor CCleaner is inbegrepen, dus er is geen verdere configuratie nodig. De inhoud van deze configuratie is te vinden in de bijlage C en in hoofdstuk 8.1 van het testrapport.

De aansturing van CCleaner verloopt via een Visual Basic Script wat is aangeleverd door N-able en standaard is opgenomen in de N-central server. Het CCleaner proces kan op dit moment nog niet worden gecontroleerd binnen N-central; dit vanwege het gebrek aan logging vanuit CCleaner.

8.6. Managed Back-up

De back-up manager maakt het mogelijk gecontroleerde backups uit te voeren vanuit N-central. Onderliggende techniek is afkomstig van CA en is een geïntegreerde versie van ARCserve D2D.

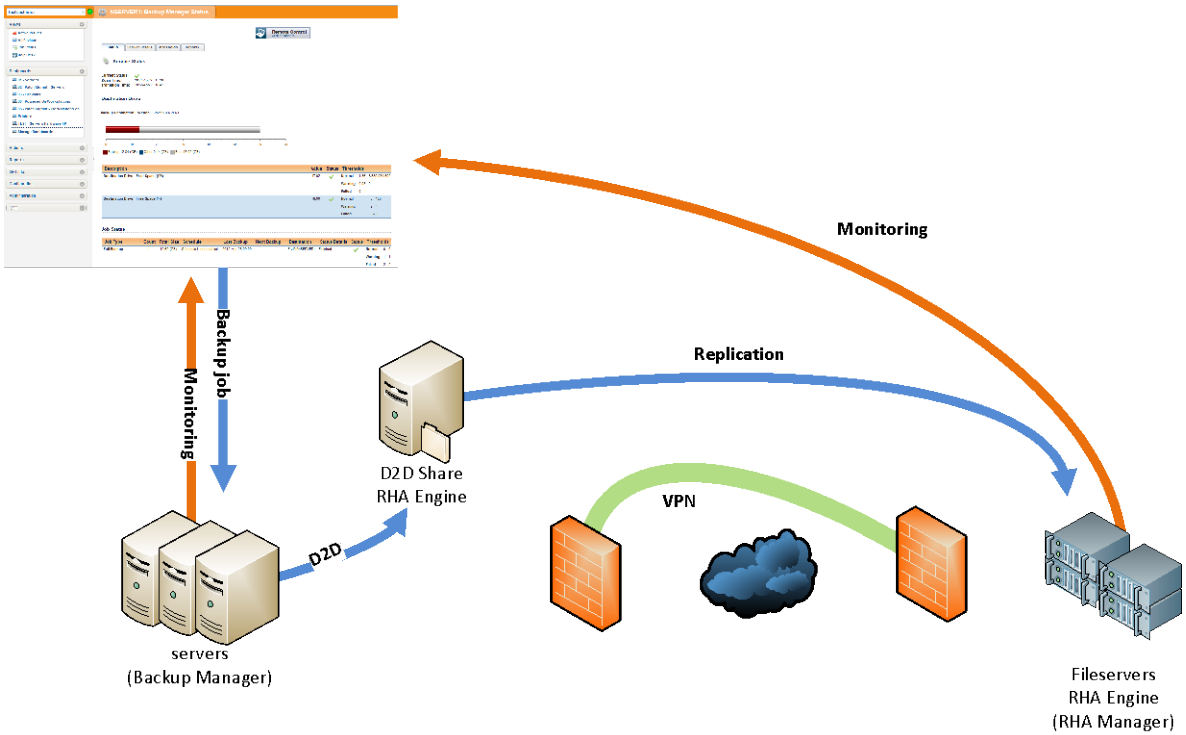
D2D (Disk 2 Disk) maakt blocklevel backups van systemen. Dit zijn als het ware volledige images van servers/werkstations, geschikt voor bare metal recovery. Maar de echte kracht van D2D zit in de “infinite incremental” functie. Deze functie maakt het mogelijk de initiële full back-up image, oneindig aan te blijven vullen met incremental backups, waarna de oude incremental sets samen worden gevoegd met de full back-up. Deze techniek wordt verder toegelicht in hoofdstuk 7 van het testrapport. In onderstaande figuur 14 wordt een overzicht gegeven van de techniek.



Figuur 14: D2D Infinite Incremental

Deze D2D backups worden lokaal op het netwerk bewaard. Daarnaast is het mogelijk de backups via een VPN verbinding te repliceren naar een tweede locatie. Dit kan een locatie van de klant zijn of een opslagruimte in het netwerk van Hupra.

De architectuur voor de back-up oplossing is weergegeven in figuur 15. Deze opstelling zal ook als testcase worden ingezet. Het backup proces start bij de N-central server welke een aantal geplande taken voor back-up zal hebben. De N-central server zal het startcommando versturen naar de agent geïnstalleerd op de doel server, waarna de back-up manager software het zal overnemen en de voortgang van het proces zal rapporteren aan de N-central server.



Figuur 15: Architectuur Backup Manager

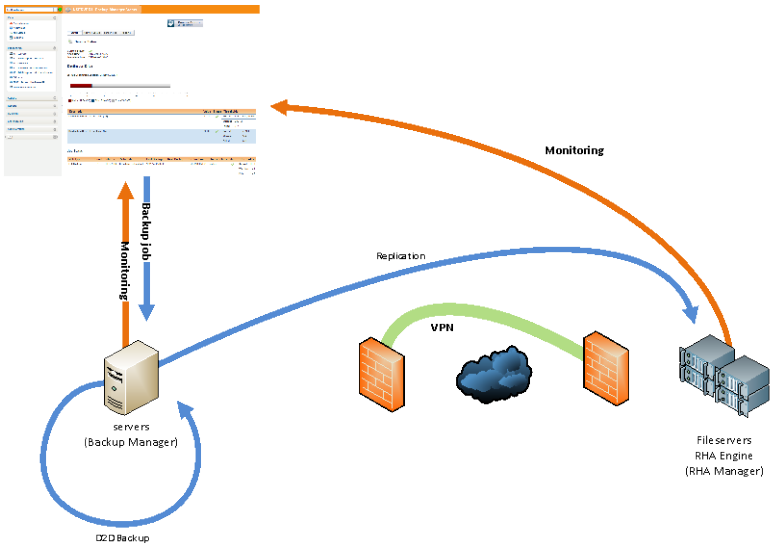
De Back-up Manager maakt in eerste instantie een full D2D back-up van de server. Deze full backup zal gevolgd worden door incremental backups zoals hierboven beschreven. Deze backups worden op een file server in het lokale netwerk geplaatst, waarna de Replication Manager (RHA Manager) de “D2D store” naar een offsite locatie repliceert. De replicatie zal net als de D2D backup via een block-level methode verlopen, zodat alleen de wijzigingen over het internet worden verstuurd.

Voor de eerste replicatie is het aan te raden de data op een externe schijf mee te nemen naar de offsite locatie en naar de juiste store te kopiëren, waarna de replicatie kan worden ingezet. Op deze manier wordt voorkomen dat in een keer alle data over het internet moet worden gekopieerd, wat vooral in de tests nog wel eens voor wat oponthoud heeft gezorgd.

De tests met backup manager zijn als eerst uitgevoerd op de TestCustomer omgeving en zijn gebaseerd op de architectuur van figuur 15. Zoals bij bijna alle tests op deze schone omgeving het geval was, verliep deze vlekkeloos. Daarom is deze test meteen doorgezet naar een omgeving van een klant, waar op dat moment nog geen backup aanwezig was. In de tests is duidelijk geworden dat

bovengenoemde architectuur alleen zinvol is in een groter bedrijfsnetwerk. In kleinere netwerken is het al snel overdreven om een extra server voor backup neer te zetten. Er kan dan worden gekozen voor een andere architectuur of het achterwege laten van de replicatie. Hiermee vervalt de eis voor een fileshare met agent software en kan er gebruik worden gemaakt van een NAS.

Voor de tweede test (bij de klant) is een aangepaste versie ontworpen. Met de nieuwe opstelling is het wel mogelijk een backup te maken en deze vervolgens te repliceren, bij gebruik van maar één Windows server. Deze server is uitgerust met een schijf/partitie uitsluitend bedoeld voor de D2D back-up. De server maakt een back-up naar deze schijf of partitie (een back-up naar zichzelf). Daarna zal de back-up worden gerepliceerd naar de offsite locatie (Hupra netwerk). Dit aangepaste proces staat nog een keer in figuur 16 weergegeven.



Figuur 16: Architectuur Backup manager II

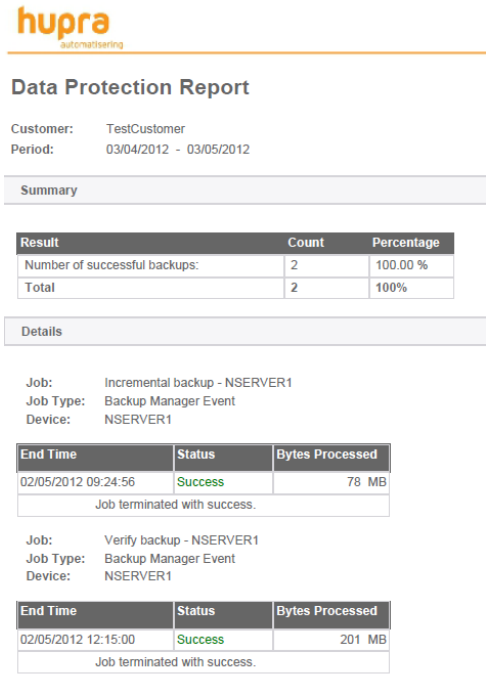
8.6.1. Installatie/ Configuratie

De eerste stap in het installatieproces was het installeren van de benodigde software. Dit wordt automatisch door de N-central agent geregeld op het moment dat de back-up optie voor de betreffende server/pc wordt geactiveerd. Het is ook mogelijk de software handmatig te installeren alvorens deze optie aan te vinken. Hiermee wordt voorkomen dat 350 MB aan software moet worden gedownload van de N-central server. De software voor de replicatie kan alleen handmatig worden geïnstalleerd.

De tweede stap is het opstellen van een Back-up profiel. Het is wenselijk een standaard te creëren voor de back-up strategie, zodat er een aantal standaard profielen aangemaakt kunnen worden welke inzetbaar zijn bij verschillende klanten. In deze speciale, niet veel voorkomende situatie, was het nodig een aangepast profiel te maken.

De back-up profielen worden aangemaakt in N-central. Hierin worden instellingen als de back-up bron/doel, planning, type back-up, encryptie, enz. ingesteld. Bij het gebruik van de replicatie dient de RHA software handmatig te worden ingesteld. Deze instellingen (scenario's) worden geconfigureerd in de RHA Manager (locatie Hupra). Voor iedere locatie (lees klant) zal een apart scenario worden gemaakt. Hierin worden zaken als IP adressen, bron/doel bestand, replicatie methode, e.d. geconfigureerd.

De installatie en configuratie van de RHA Manager en Engines verloopt handmatig buiten N-central om. N-central heeft wel de mogelijkheid de RHA manager te monitoren en zelfs individuele scenario's te controleren. De resultaten van de back-up kunnen vervolgens in rapportages worden weergegeven. Hieronder zijn een Data Protection Report en een Backup Manager Status Report weergegeven.



hupra automatisering

Data Protection Report

Customer: TestCustomer
Period: 03/04/2012 - 03/05/2012

Summary

Result	Count	Percentage
Number of successful backups:	2	100.00 %
Total	2	100%

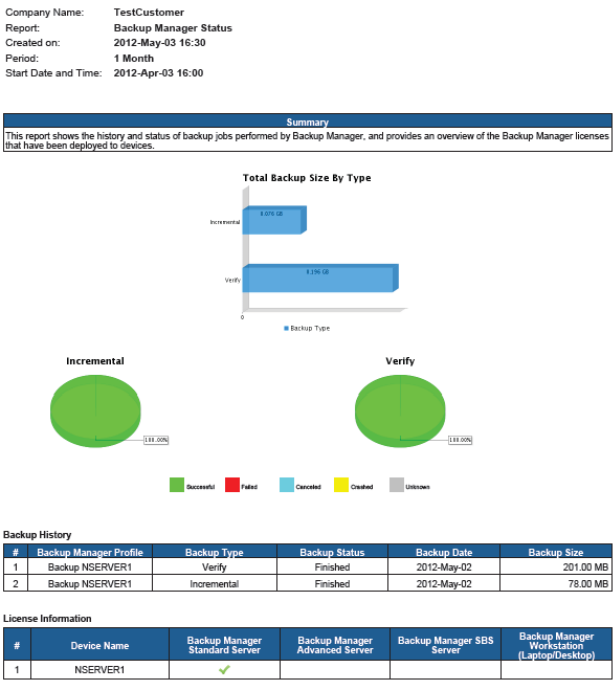
Details

Job: Incremental backup - NSERVER1
Job Type: Backup Manager Event
Device: NSERVER1

End Time	Status	Bytes Processed
02/05/2012 09:24:56	Success	78 MB
Job terminated with success.		

Job: Verify backup - NSERVER1
Job Type: Backup Manager Event
Device: NSERVER1

End Time	Status	Bytes Processed
02/05/2012 12:15:00	Success	201 MB
Job terminated with success.		



Company Name: TestCustomer
Report: Backup Manager Status
Created on: 2012-May-03 16:30
Period: 1 Month
Start Date and Time: 2012-Apr-03 16:00

Summary

This report shows the history and status of backup jobs performed by Backup Manager, and provides an overview of the Backup Manager licenses that have been deployed to devices.

Total Backup Size By Type

Incremental
Verify
Backup Type

Incremental **Verify**

Successful Failed Canceled Crashed Unknown

Backup History

#	Backup Manager Profile	Backup Type	Backup Status	Backup Date	Backup Size
1	Backup NSERVER1	Verify	Finished	2012-May-02	201.00 MB
2	Backup NSERVER1	Incremental	Finished	2012-May-02	78.00 MB

License Information

#	Device Name	Backup Manager Standard Server	Backup Manager Advanced Server	Backup Manager SBS Server	Backup Manager Workstation (Laptop/Desktop)
1	NSERVER1	✓			

8.6.2. Problemen

Gedurende de tests zijn een aantal kleine problemen aan het licht gekomen. Zo is het bijvoorbeeld bij het instellen van de replicatie van groot belang dat men consistent is met het ingeven van de IP adressen voor de master en slave server. Dit houdt in dat als er gebruik wordt gemaakt van publieke adressen, deze zowel voor de master als de slave worden ingesteld. Het is niet mogelijk een intern adres te gebruiken voor de master en een publiek adres voor de slave en vice versa. Gebeurt dit wel dan zal er geen duidelijke foutmelding worden gegeven.

Voor het gebruik van de replicatie oplossing in netwerken waar gebruik wordt gemaakt van NAT dient poort 25000 TCP open gezet te worden. Het forwarden van deze poort zal in de toekomst komen te vervallen als de NAT helper wordt toegevoegd in de volgende release van de replicatie software.

Een tweede probleem wat zich heeft voorgedaan in de tests was een probleem met een corrupte VSS (Volume Snapshot Service) op een Windows XP machine. De D2D backup gebruikt de VSS service voor het veilig stellen van een snapshot van de disk. Dit probleem deed zich voor in een test op een 'vuile' omgeving. Met het resetten van de VSS DLL's en bijbehorende registerwaardes was het probleem tijdelijk opgelost, totdat het probleem weer terug kwam na een nieuwe backup. Meer details hierover zijn te vinden in hoofstuk 7.1 van het testrapport.

9. Conclusie

In hoofdstuk 3.1 is een beeld geschetst van de werkwijze welke voorheen door Hupra gehanteerd werd. Het chaotische reactieve beheer, ook wel brandjes blussen genoemd. In deze omschrijving staat daarnaast het verlangen van Hupra om over te stappen naar een nieuwe proactieve werkwijze centraal. Hupra wil de geleverde ICT dienstverlening naar een hoger niveau brengen en meer professionaliteit naar de klant uitstralen.

Niet alleen de klant moet baat hebben bij deze wijzigingen, vooral de interne werkwijze van Hupra moet verbeterd worden. Om deze verbetering te kunnen meten en sturen, zijn een aantal doelstellingen vastgelegd in hoofdstuk 3.2. De doelstellingen zijn opgesteld voor een tijdsperiode van één jaar en zijn als volgt:

- onderscheidend vermogen Hupra;
- kosten terugdringen (aantal facturabele uren verhogen met 20%);
- klantwerving (25+ klanten in het proactieve model);
- verlaging werkdruk (terugdringen break-fix werkzaamheden van 99% naar 50%);
- betrouwbaarheid dienstverlening/ ICT van de klant (van ±90% naar 99% beschikbaarheid);
- automatisering terugkomend onderhoud (van 0% naar 10-20%).

Daarnaast wil Hupra doorgroeien van een break-fix automatiseerder naar een proactieve automatiseerder, oftewel Managed Service Provider (niveau 3 van het volwassenheidsmodel). Met het juiste software pakket, de juiste inrichting hiervan en de juiste ondersteuning en commitment vanuit de organisatie, zijn alle bovengenoemde doelstellingen waar te maken.

Zijn nu, na de keuze voor N-central, de configuratie onderzoeken, de tests, de implementatie en het opstellen van de procedures voor omgang met N-central, deze doelstellingen bereikt? Na anderhalve maand regelmatig te werken met N-central worden langzaamaan wat verschillen merkbaar. Er zijn op het moment van schrijven 10 van de 50 klanten in het systeem geregistreerd. Hierdoor wordt er meer werk uit het systeem gehaald, wat anders over het hoofd zou worden gezien. Het aantal facturabele uren loopt op van gemiddeld 20 naar 22 uren per beheerder. Op dit moment bestaat 10% van de werkzaamheden uit taken afkomstig van het nieuwe proactieve model en zien we dat al bijna 40% van het onderhoud geautomatiseerd verloopt via maintenance scripts in N-central.

Als Hupra deze lijn blijft vasthouden zullen op de gestelde termijn van één jaar de overige doelstellingen makkelijk te halen zijn. Hupra heeft met dit project een solide basis om op verder te bouwen. De basis voor een goed MSP pakket is geconfigureerd en geïmplementeerd en belangrijkste procedures zijn vastgelegd. Het is nu aan Hupra hierin verder te ontwikkelen en haar sales en marketing strategieën hier op aan te passen.

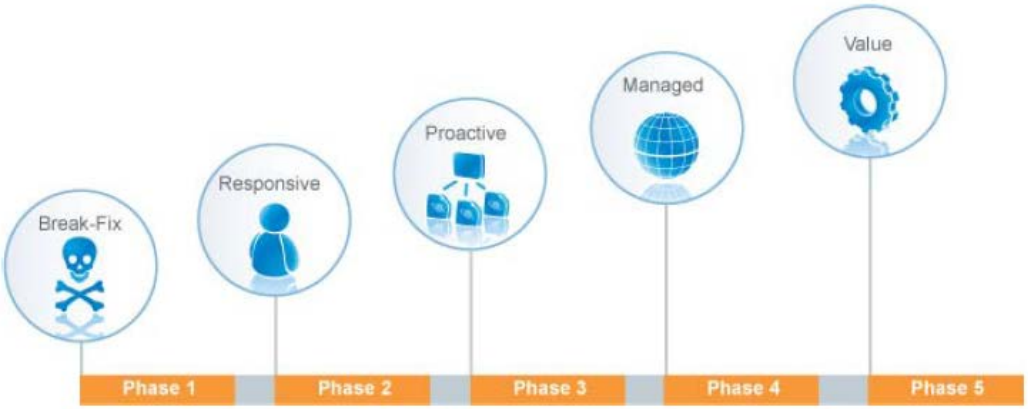
Het MSP model blijft een model onderhevig aan wijzigingen. Hupra zal daarom ook vooruit moeten blijven kijken en moeten vernieuwen. Razend snel komen nieuwe versies, functies of ideeën uit betreffende MSP. Functies of ideeën waarmee Hupra misschien haar voordeel kan doen. Zo zal ook de configuratie van het pakket constant moeten veranderen om aan te blijven sluiten bij deze vernieuwingen. Een simpel voorbeeld hiervan zijn de notificatie profielen.

Een aantal andere zaken om in de toekomst in de gaten te houden of te overwegen zijn bijvoorbeeld een uitbreiding als Report Manager. Een uitbreiding als Report Manager zal Hupra in de toekomst kunnen ondersteunen in de rapportages naar klanten. Dit zal ook een bepaalde vorm van professionaliteit uitstralen. Een eigenschap die Hupra al wat langer beoogd. Daarnaast zal dit van belang zijn als Hupra door wil groeien in het MSP volwassenheidsmodel.

Een tweede stap, benodigd voor deze doorgroei, is het inrichten van een goede koppeling met een ticket systeem. Hupra maakt gebruik van het systeem OFB, echter is hiervoor geen goede koppeling met N-central beschikbaar. Als Hupra verder wil groeien in het MSP model moet misschien overwogen worden te kijken naar een pakket als AutoTask. AutoTask werkt nauw samen met N-central en heeft een tweezijdige koppeling. AutoTask zal nooit als vervanging van OFB ingezet kunnen worden, maar er kan wel onderzocht worden of deze pakketten ook naast elkaar ingezet kunnen worden en misschien weer onderling gekoppeld kunnen worden.

Kortom, Hupra is een aardig eind op weg en heeft met dit project een solide basis om verder te groeien in het MSP model. De vooruitgang is al op veel vlakken merkbaar. Er is echter geen tijd om er rustig bij te gaan zitten en van het resultaat te genieten. Er moet nog flink door ontwikkeld en doorgegroeid worden voordat het door veel MSP's befaamde niveau 5 behaald kan worden.

Een doorgroei naar de hogere niveaus van het volwassenheidsmodel zal voor zowel Hupra als de klant meer zekerheid en duidelijkheid geven en zal de algehele ICT dienstverlening op een hoger niveau brengen. Met deze kwaliteit en eenvoud zal Hupra zich zeker kunnen onderscheiden op de markt.



Figuur 17: MSP Maturity Model (N-able Technologies, 2006)

10. Evaluatie van de procesgang

Voor de start van het project is een plan van aanpak opgesteld. In deze evaluatie wordt dit plan van aanpak vergeleken met de daadwerkelijke uitvoering van het project. Allereerst wordt een samenvatting van de gebeurtenissen gegeven, daarna wordt afgesloten met een conclusie betreffende de procesgang.

10.1. Samenvatting van gebeurtenissen

De eerste maand van het afstuderen stond in het teken van het plan van aanpak. Gedurende deze periode zijn veel gesprekken gevoerd over de afbakening van het project en de verwachtingen hiervan. Deze zijn vervolgens vastgelegd in het plan van aanpak. In overleg met de heer Willemsen en de heer Van Nimwegen is het plan afgestemd op de wensen van Hupra en de Hogeschool Utrecht.

Gedurende deze eerste fase van het project, is fase 2 (onderzoeksfase) gestart. Deze fase is eerder gestart dan gepland, om tussen de werkzaamheden van fase 1 door, alvast een begin te kunnen maken met een oriënterend onderzoek betreffende Managed Services. De resultaten van dit onderzoek zijn vastgelegd in het onderzoeksrapport, later productonderzoek genoemd. In deze fase zijn ook de verschillende functies van de producten vergeleken en zijn prijsopgaven van de verschillende producten opgevraagd. Een financiële vergelijking is behouden voor het adviesrapport.

Zoals te lezen viel in de originele omschrijving van deze fase zouden bij afronding van deze fase twee documenten worden opgeleverd. Een document welke Managed Services (Proactief beheer) in het algemeen beschrijft en een document met een onderzoek naar software oplossingen. Deze documenten zijn uiteindelijk samengevoegd tot het onderzoeksrapport, of productonderzoek.

In de tweede week van maart is begonnen met de ontwerpfase. Deze fase heeft eerst veel overlap gehad met de onderzoeksfase. Bij de overlap van deze fases is het begin van het adviesrapport ontstaan. Gebaseerd op de resultaten uit de onderzoeksfase is een productadvies uitgebracht. Dit advies is in verschillende vergaderingen toegelicht totdat uiteindelijk over is gegaan tot aankoop van N-central. Daarna is verder gegaan met het ontwerpen van mogelijke configuraties en procedures. Deze zijn ook vastgelegd in het adviesrapport. Het adviesrapport is niet geheel afgesloten in deze fase. Gedurende de testfase zijn een aantal configuraties en procedures aangescherpt op basis van nieuwe informatie. Tegen het einde van de ontwerpfase zijn tests ontwikkeld welke in de testfase gebruikt konden worden voor het testen van de adviezen en configuraties.

Al vrij snel (na 1 à 2 weken ontwerpfase) is overgegaan naar de testfase waarin de eerste configuraties zijn getest en vastgelegd in het testrapport. Na de basistests is meteen de implementatie fase gestart. Hier is bewust afgeweken van de planning. In plaats van alles eerst te testen en dan te implementeren, is er voor gekozen om een functie van het pakket te testen en deze daarna meteen te implementeren. Dit had een aantal voordelen ten opzichte van de originele planning. De functies konden makkelijker geïmplementeerd worden omdat men nog goed in de materie zat en eventuele problemen met een tekort aan tijd in de implementatiefase is voorkomen.

Gedurende de test- en implementatiefase zijn een aantal nieuwe functies van N-central uitgebracht. Deze functies zijn alsnog onderzocht en opgenomen in het test- en adviesrapport. Een van deze nieuwe functies was bijvoorbeeld de Backup Manager. Uiteindelijk zijn alle beoogde basisfuncties geïmplementeerd en is midden/eind mei gestart met de afrondende fase.

10.2. Conclusie

Terugkijkend op het onderzoek kan gesteld worden dat er een vrij hoge mate van effectiviteit is gehaald. Dit mede door de werkwijze binnen Hupra, in het bijzonder de korte lijnen en de informele gesprekken. Zoals in het plan van aanpak vastgesteld, is iedere week geprobeerd een voortgangsgesprek te houden, waarin de resultaten van de afgelopen periode aan bod kwamen en de planning van de te ondernemen acties voor de komende weken. In deze en extra geplande gesprekken zijn ook de eisen aan het proactieve model en de software vastgesteld. Ook deze gesprekken waren vanwege de korte lijnen en de informele sfeer zeer doeltreffend.

Door de test- en implementatiefase samen te voegen en het geheel op te delen aan de hand van de functies zijn ‘mini projectjes’ ontstaan, waarop makkelijk gestuurd kon worden. In de wekelijkse gesprekken is Hupra nauw betrokken geweest bij de status en voortgang van deze tests. Gedurende de tests is zoveel mogelijk feedback verzameld. Hierdoor is een goede aansluiting met Hupra gerealiseerd en is veel vooruitgang geboekt met de tests en implementatie.

Hupra had graag extra focus op de producttests en implementatie. Het is voor een bedrijf als Hupra belangrijk dat er daadwerkelijk een resultaat opgeleverd wordt. Niet alleen in de vorm van een adviesrapport. Daarom is vanaf het begin het belang van een implementatie benadrukt. Hupra moest een oplossing hebben waarmee meteen gewerkt kon worden. Tijdens het onderzoek zijn de belangen van het productonderzoek, -vergelijking en het opstellen van de procedures niet uit het oog verloren. Door de hierboven beschreven aanpak en de flexibiliteit van Hupra heeft men snel kunnen beslissen over deze zaken, waarna zo snel mogelijk aandacht is besteed aan de tests en implementatie.

11. Bibliografie

McCabe, J. D. (2007). *Network Analysis, Architecture, and Design.* Amsterdam: Morgan Kaufman Publishers.

N-able Technologies. (2006). From Promises to Proof: How To Demonstrate Value to Your Customers.

N-able Technologies. (2006). N-ables MSP Maturity Model.

N-able Technologies. (2007). The Fundamentals of a Successful Managed Services Practice.

N-able Technologies. (2007). The Seven Major Obstacles on the Road to Managed Services.

N-able Technologies. (2008). IT Service Delivery: From Basic Automation through to Managed Services.

N-able Technologies. (2009). Doing More with Less: Automating IT Services in Your Midsize Business.

N-able Technologies. (2011). Going beyond RMM.

Walsh, L. M. (2011). Countering artificial commoditization and poor pricing practices in managed services.

Bijlage A: Afbeeldingen

Proactief beheer bij Hupra

Auteur:
M.M.J. de Weijer
Studentnummer: 1546128
Hogeschool Utrecht
Faculteit Natuur & Techniek
Systeembeheer

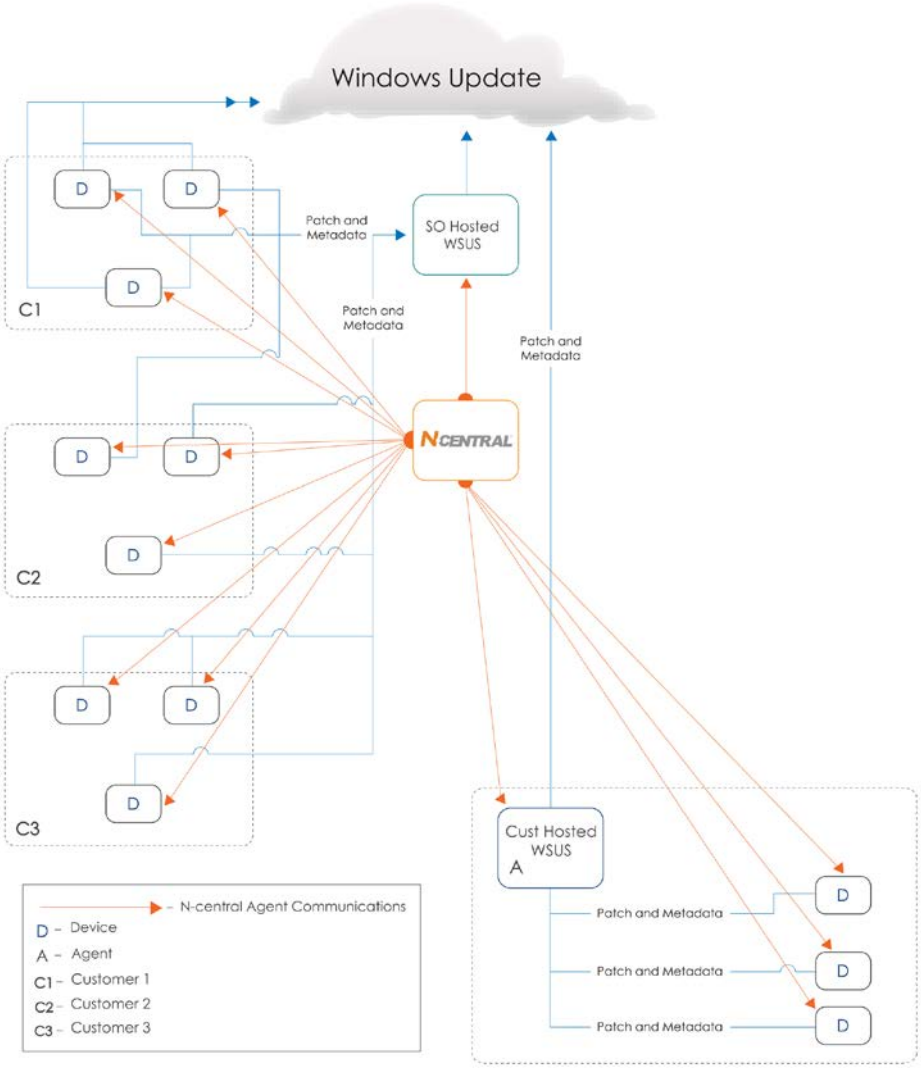
Bedrijf:
Hupra Automatisering
Hoofdstraat 105
3901 AK Veenendaal

Begeleiders:
Hupra: Dhr. P.A. Willemsen
Hogeschool Utrecht: Dhr. H. van Nimwegen

Afstudeerperiode:
februari 2012 - juni 2012

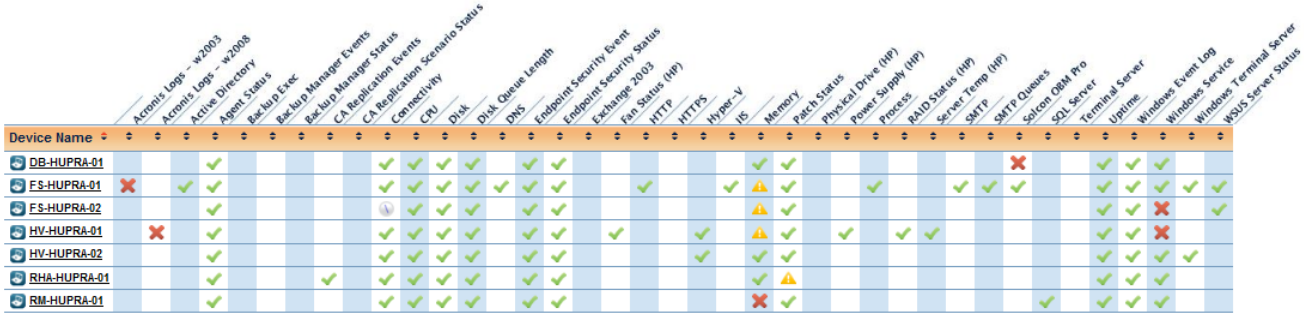
Versie: 1.0
Datum: 24 mei 2012

Bijlage A: Afbeeldingen

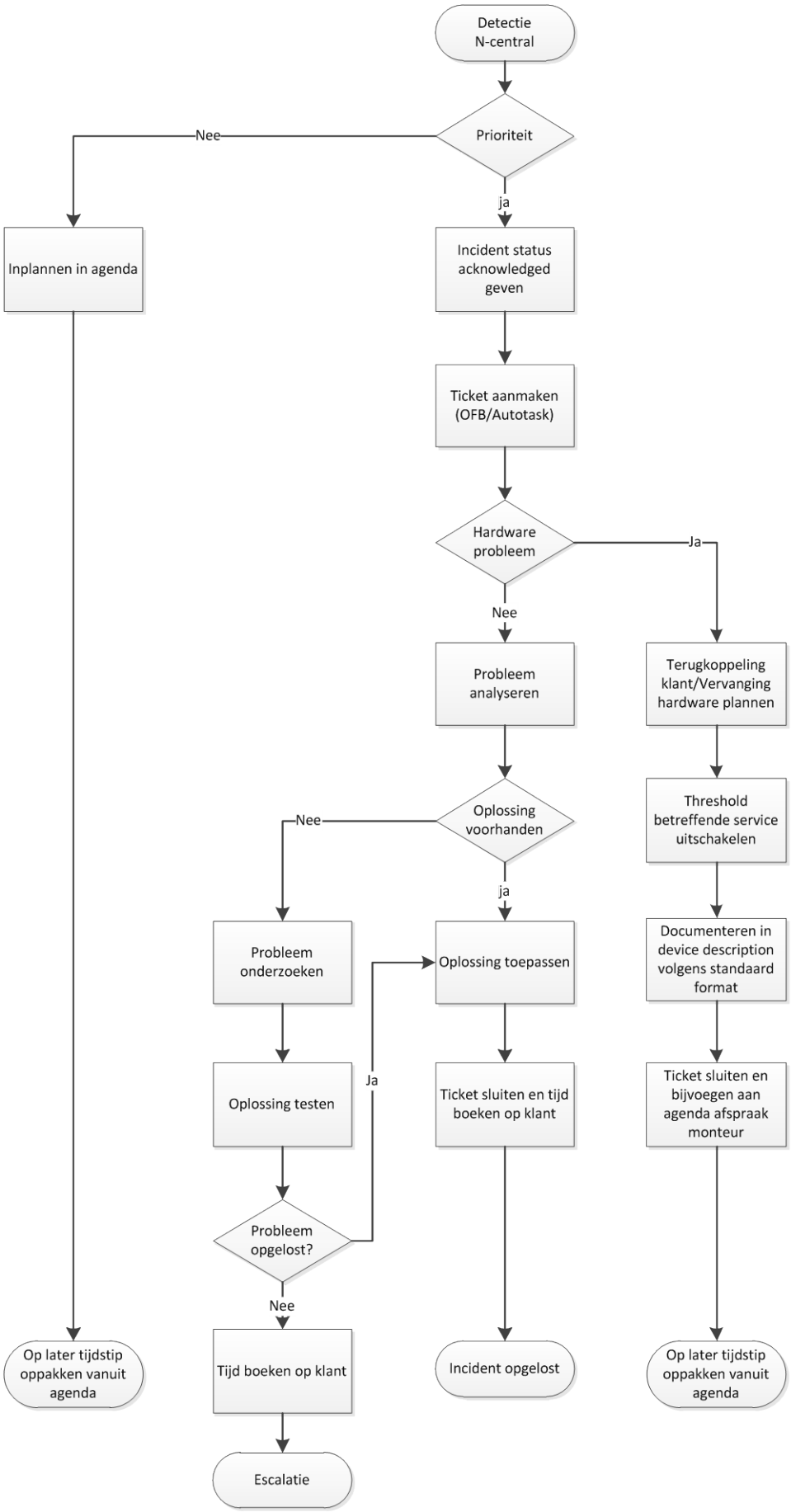


Figuur 18: Drie vormen van patch management

Figuur 19: Prio I Dashboard



Figuur 20: Prio II Dashboard



Figuur 21: Visuele weergave proces incident oppakken

Bijlage B: Tabellen

Proactief beheer bij Hupra

Auteur:
M.M.J. de Weijer
Studentnummer: 1546128
Hogeschool Utrecht
Faculteit Natuur & Techniek
Systeembeheer

Bedrijf:
Hupra Automatisering
Hoofdstraat 105
3901 AK Veenendaal

Begeleiders:
Hupra: Dhr. P.A. Willemsen
Hogeschool Utrecht: Dhr. H. van Nimwegen

Afstudeerperiode:
februari 2012 - juni 2012

Versie: 1.0
Datum: 24 mei 2012

Bijlage B: Tabellen

Tabel 12: Inhoudelijke vergelijking producten

	Relatief gewicht (0-1)	N-Central	Kaseya	GFI MAX Remote Management
On-premise	0,8	5 / 4,0	5 / 4,0	- / -
Cloud	0,2	2 / 0,4	2 / 0,4	5 / 1,0
Web based dashboard	0,5	4 / 2,0	4 / 2,0	4 / 2,0
Integratie PSA	0,7	4 / 2,8	4 / 2,8	2 / 1,4
Remote control	0,1	4 / 0,4	4 / 0,4	4 / 0,4
Asset control	0,8	5 / 4,0	4 / 3,2	4 / 3,2
Automatiseren beheerstaken	1,0	5 / 5,0	4 / 4,0	4 / 4,0
Mobiele toegang	0,3	5 / 1,5	3 / 0,9	4 / 1,2
Patch management	0,7	5 / 3,5	5 / 3,5	4 / 2,8
Antivirus/malware	0,9	5 / 4,5	5 / 4,5	5 / 4,5
Reporting	1,0	4 / 4,0	3 / 3,0	3 / 3,0
Software deployment	0,4	4 / 1,6	5 / 2,0	- / -
Audit network vulnerability	0,3	3 / 0,9	4 / 1,2	- / -
Unattended remote control	0,2	3 / 0,6	3 / 0,6	- / -
Self-healing	0,8	5 / 4,0	4 / 3,2	- / -
Netflow monitoring	0,5	4 / 2,0	4 / 2,0	- / -
Backup automatisering	0,9	5 / 4,5	5 / 4,5	- / -
Policy manager	0,7	3 / 2,1	5 / 3,5	- / -
Branding	0,5	5 / 2,5	4 / 2,0	5 / 2,5
Desktop migratie	0,2	- / -	5 / 1,0	- / -
Active directory services	0,5	- / -	5 / 2,5	- / -
Imaging (Ghosting/D2D)	0,6	5 / 3,0	5 / 3,0	- / -
WSUS integratie	0,8	5 / 4,0	- / -	- / -
Website monitoring	0,8	- / -	- / -	5 / 4,0
Software trainingen/handleidingen	1,0	5 / 5,0	5 / 5,0	4 / 4,0
Ondersteuning implementatie MSP model	0,9	4 / 3,6	2 / 1,8	- / -
Ondersteuning bij software implementatie	0,9	5 / 4,5	5 / 4,5	- / -
Totaal		104 / 70,4	104 / 65,5	53 / 34,0
Gemiddelde		**4,3 / 2,9**	**4,2 / 2,6**	**4,1 / 2,6**

Profile	Trigger (state)	Service
Critical – Connectivity Primary Delay: 1 min Repeat: 60 min First Escalation Delay: 30 min	**Availability (failed)** Servers – Windows Servers – Generic SBS Servers Network Devices	Connectivity
	Uptime (stale) Servers – Windows SBS Servers Domain Controllers	Uptime
Critical – Backup Primary Delay: 5 min Repeat: - First Escalation Delay: 1 day	**Backup (failed)**	Acronis Logs - w2003
		Acronis Logs - w2008
		Backup Exec
		Backup Manager Events
		Backup Manager Status
		CA Replication Events
		CA Replication Scenario Status
Critical – Hardware Primary Delay: 1 min Repeat: 60 min First Escalation Delay: 15 min	**Hardware – Failed (failed)** Servers – Windows Hupra - Fysieke servers	Fan Status (Dell/HP/IBM/Intel/VMware)
		Physical Drive (Adaptec/Dell/HP/Intel/VMware)
		Power Supply (Dell/HP/Intel/VMware)
		RAID Status (Adaptec/Dell/HP/VMware)
		Server Temp (Dell/HP/IBM/Intel)
		Temperature Status (VMware)
Critical – Services Primary Delay: 2 min Repeat: 60 min First Escalation Delay: 30 min	**AD (failed)** Domain Controllers Servers - Windows	Active Directory
	DNS (failed) Domain Controllers Servers - Windows	DNS
	Exchange – failed (failed) Exchange 2003	Exchange 2003
		Exchange 2007

	Exchange 2007 Exchange 2007 - CAS Role Exchange 2007 - Hub and Mailbox Exchange 2010 Exchange 2010 - CAS Role Exchange 2010 - Hub and Mailbox SBS Servers Servers - Windows	IMAP
		POP
		SMTP
	Hyper-V (failed) Servers - Windows	Hyper-V
	Website (failed) SBS Servers Servers - Windows	HTTP
		HTTPS
		IIS
Performance Primary Delay: 5 min Repeat: 60 min First Escalation Delay: 30 min	**CPU (failed)** Network Devices Servers - Windows	CPU
	Disk (failed) Network Devices Servers - Windows	Disk
		Disk Queue Length
	Memory (failed) Network Devices Servers - Windows	Memory
Warning - Firewall Security Primary Delay: 2 min Repeat: -	**SonicWALL (failed)** Network Devices	FW-SonicWALL

Tabel 13: Notification Profiles

Bijlage C: Scripts/ Configuratie

Proactief beheer bij Hupra

Auteur:
M.M.J. de Weijer
Studentnummer: 1546128
Hogeschool Utrecht
Faculteit Natuur & Techniek
Systeembeheer

Bedrijf:
Hupra Automatisering
Hoofdstraat 105
3901 AK Veenendaal

Begeleiders:
Hupra: Dhr. P.A. Willemsen
Hogeschool Utrecht: Dhr. H. van Nimwegen

Afstudeerperiode:
februari 2012 - juni 2012

Versie: 1.0
Datum: 24 mei 2012

Bijlage C: Scripts/ Configuratie

Defragmentatie

```
@echo off
setlocal enabledelayedexpansion

set partitions=
for %%a in (a b c d e f g h i j k l m n o p q r s t u v w x y z) do (
      vol %%a: > nul 2>nul
      if not errorlevel 1 (
            set partitions=!partitions! %%a:
      )
)

defrag.exe %partitions% /H /M
```

Checkdisk

```
@echo off & setLocal enableDELAYedexpansion
for %%a in (a b c d e f g h i j k l m n o p q r s t u v w x y z) do (
      vol %%a: > nul 2>nul
      if not errorlevel 1 (
            fsutil dirty set %%a:
      )
)

shutdown -r -t 20
```

Ccleaner configuratie

```
[Options]
Language=1033
UpdateKey=05/02/2012 09:05:58 AM
(App)History=False
(App)Cookies=False
(App)Recently Typed URLs=False
(App)Windows Error Reporting=False
(App)DNS Cache=True
(App)Font Cache=True
(App)Old Prefetch data=True
(App)Menu Order Cache=False
(App)Tray Notifications Cache=False
(App)Window Size/Location Cache=False
(App)Environment Path=True
(App)User Assist History=False
(App)IIS Log Files=False
(App)Mozilla - Internet History=False
(App)Mozilla - Cookies=False
(App)Mozilla - Site Preferences=True
(App)Mozilla - Compact Databases=True
(App)Google Chrome - Internet History=False
(App)Google Chrome - Cookies=False
(App)Google Chrome - Compact Databases=True
WINDOW_MAX=1
WINDOW_LEFT=0
WINDOW_TOP=0
WINDOW_WIDTH=0
WINDOW_HEIGHT=0
```

Bijlage D: Plan van Aanpak

Proactief beheer bij Hupra

Auteur:
M.M.J. de Weijer
Studentnummer: 1546128
Hogeschool Utrecht
Faculteit Natuur & Techniek
Systeembeheer

Bedrijf:
Hupra Automatisering
Hoofdstraat 105
3901 AK Veenendaal

Begeleiders:
Hupra: Dhr. P.A. Willemsen
Hogeschool Utrecht: Dhr. H. van Nimwegen

Afstudeerperiode:
februari 2012 - juni 2012

Versie: 1.1
Datum: 23 mei 2012

Versie beheer:

Versie	Datum	Wijzigingen
0.0	06-02-2012	Initiële versie document, geen inhoud
0.1	08-02-2012	Basis invulling onderdelen plan van aanpak
0.2	17-02-2012	Verwerking feedback
0.3	29-02-2012	Verwerking feedback n.a.v. bedrijfsbezoek
0.4	05-03-2012	Verwerking feedback risico's (kans indeling)
0.5	08-03-2012	Verwerking laatste feedback, herschrijven onderdelen
1.0	12-03-2012	Definitieve versie
1.1	23-05-2012	Opmaak document voor bijlage scriptie

Inhoud

1. Inleiding

Dit document is een plan van aanpak voor een onderzoek, ontwerp en implementatie betreffende het gebruik van proactief beheer en mogelijke methodes en tools ter ondersteuning van dit proactieve beheer. Aanleiding van dit afstudeerproject is de sterke groei van het aantal klanten dat Hupra op dit moment doormaakt en het verlangen van het bedrijf om meer onderscheidend te worden ten opzichte van de concurrentie. Men wil dit bereiken door over te gaan op een proactieve manier van beheer, dit met alle waarschijnlijkheid met bijbehorende ondersteuning van een aantal ICT producten. Dit alles heeft aanleiding gegeven tot de start van dit project.

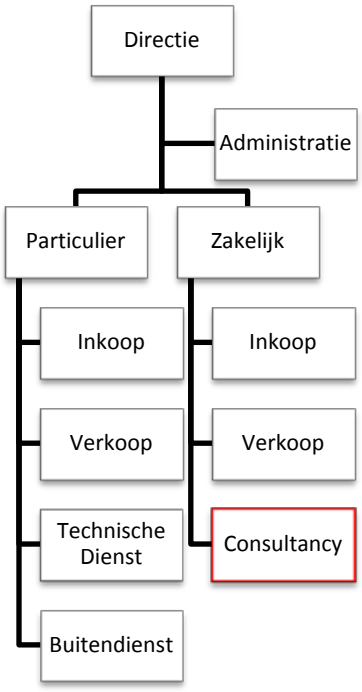
De bedoeling van dit document hierin is duidelijkheid te scheppen betreffende: De omgeving waarin het project wordt uitgevoerd, de probleembeschrijving, de opdrachtformulering, projectinrichting, op te leveren producten en de eisen hieraan, de aanpak van het project, aansluiting met mijn opleiding en benodigde kennis, planning van de projectactiviteiten en een kwaliteitsborging.

Dit document zal het uitgangspunt zijn voor het project. Samen met het bijgevoegde formulier aan het einde van dit document zal dit document dienen als het afstudeercontract en dient ondertekend te worden door de student, de docentbegeleider en de bedrijfsbegeleider.

2. Bedrijfscontext

Hupra is opgericht in het jaar 1980. Toen in 1981 de eerste PC op de markt werd gebracht, richtte de organisatie zich steeds meer op de ICT-dienstverlening. Hupra betrof vanuit origine een elektronicawinkel, gericht op de particuliere markt. De afgelopen jaren is de vraag naar elektronica-componenten echter sterk afgenomen en heeft Hupra besloten deze tak af te stoten en zich volledig te richten op computers, laptops, randapparatuur en reparaties. Naast deze winkel, welke volledig gericht is op de particuliere klant, is Hupra vanaf 2001 ook gestart met de dienstverlening aan de zakelijke markt en heeft men zich gefocust op de bedrijfsautomatisering. Hupra richt zich hierbij voornamelijk op de MKB bedrijven, gezien het feit dat deze bedrijven veelal geen 'eigen' systeem- en netwerkbeheerder binnen de organisatie hebben. Met deskundig advies, hoogwaardige en snelle service en daarnaast het verzorgen van de implementatie van nieuwe apparatuur ondersteunt Hupra bedrijven met netwerkbeheer. Hupra ontzorgt de klant met bijvoorbeeld het beheren van het netwerk, de implementatie van een nieuw bedrijfsnetwerk, de installatie van nieuwe werkstations en alles op het gebied van online services en onderhoud van servers en werkstations. Hupra gaat erg servicegericht te werk. Dankzij de hoogwaardige kennis, innovatieve technieken en uitstekende service zorgt Hupra ervoor dat ICT een positieve bijdrage levert aan de werkzaamheden van haar klanten. Veel bedrijven zien Hupra dan ook als een betrouwbare partner op het gebied van ICT, voor zowel particuliere als zakelijke klanten.

Hupra is opgesplitst in een afdeling zakelijk en een afdeling particulier, welke volledig los van elkaar beschouwd kunnen worden. De afdeling particulier richt zich op de verkoop van voornamelijk desktop systemen en randapparatuur aan particulieren. De afdeling zakelijk richt zich op implementatie en onderhoud van ICT in het MKB. De particuliere en de zakelijke tak zijn volledig los van elkaar te beschouwen, hoewel er soms nog wel wat overloop plaats vind. De zakelijke afdelingen maken bijvoorbeeld voor reparaties bij zakelijke klanten wel eens gebruik van de technische dienst.



Figuur 1: Organigram

Typische klanten zijn MKB bedrijven met 2 tot 50 werkstations. Deze bedrijven worden steeds meer afhankelijk van hun ICT, echter is het voor deze bedrijven niet reëel een eigen IT afdeling in te richten. Daarom hebben zij dus belang bij een goede ICT partner. Deze klanten bevinden zich in allerlei branches.

Als afstuderend student zal ik werkzaam zijn op de afdeling consultancy, ICT zakelijk waar ik als hoofdtaak de uitvoering van het afstudeerproject zal hebben. Daarnaast kan ik in tijd van nood op de afdeling consultancy bijspringen. Het afstudeerproject heeft ten alle tijden prioriteit. Mijn collega's zullen met name de medewerkers van de afdeling consultancy zijn (zie Figuur1: Organigram). Mijn opdrachtgever zal Dhr. P.A. Willemsen zijn, welke tevens de technische begeleiding voor het project zal verzorgen.

Voor meer informatie verwijs ik naar de website van Hupra: www.hupra.nl

3. Probleemstelling

Door het groeiende aantal klanten en de drang om iets extra's te bieden, wil Hupra af van het klassieke, reactieve beheer bij klanten. Het zogenaamde "brandjes blussen", de klant belt zelf als er een probleem is. Men wil zo veel mogelijk van deze werkwijze af en over gaan naar een model voor proactief beheer. Door over te gaan naar proactief beheer wil Hupra de concurrentie het hoofd bieden en voorkomen dat men achter komt te liggen op de ontwikkelingen. Door sneller problemen in de ICT van de klant te zien en deze eerder en gemakkelijker op te lossen dan voorheen het geval was, kan Hupra een sterkere concurrerende positie innemen. Bovendien wil Hupra met de inzet van proactief beheer meer rust binnen de organisatie creëren, zodat er meer tijd overblijft voor innovatie. Men kan dus stellen dat Hupra op dit moment niet in staat is de door haar gewenste kwaliteit te bieden omdat de focus nog teveel ligt op het reactieve beheer waardoor weinig tijd voor innovatie overblijft.

4. Projectopdracht

De opdracht zal bestaan uit een onderzoek naar proactief beheer, een ontwerp van hoe dit beheer ingezet kan worden om de eerder genoemde problemen van Hupra weg te nemen, een implementatie van proactief beheer (implementatie ondersteunende software) en procedures m.b.t. nieuwe werkwijzen. Deze procedures moeten ervoor zorgen dat de software optimaal benut kan worden.

In het onderzoek zal worden bekeken wat de mogelijkheden van proactief beheer voor Hupra zijn. Wat voor methodes hiervoor toegepast kunnen worden, welke procedures moeten worden opgesteld en welke tools er ingezet moeten worden. Hupra is meerdere malen aangeraden hiervoor een Managed Service Provider (MSP) tool te gebruiken. In mijn onderzoek zal ik dit meenemen en zal ik onderzoeken wat de mogelijkheden hiervan zijn, of dit wel de juiste oplossing is en of er eventueel nog alternatieven zijn.

Verder zal de opdracht bestaan uit de implementatie van de plannen voor proactief beheer binnen Hupra. Hieronder vallen zowel de implementatie van procedures m.b.t. werkwijzen als de implementatie en configuratie van ondersteunende software. Eerste indrukken van de software doen vermoeden dat het hier om geavanceerde pakketten gaat welke volledig moeten worden gefinetuned in configuratie, om optimaal aan te kunnen sluiten bij het bedrijf. Deze fine tuning zal daarom ook een belangrijk deel van het project zijn.

4.1. Doelstelling project

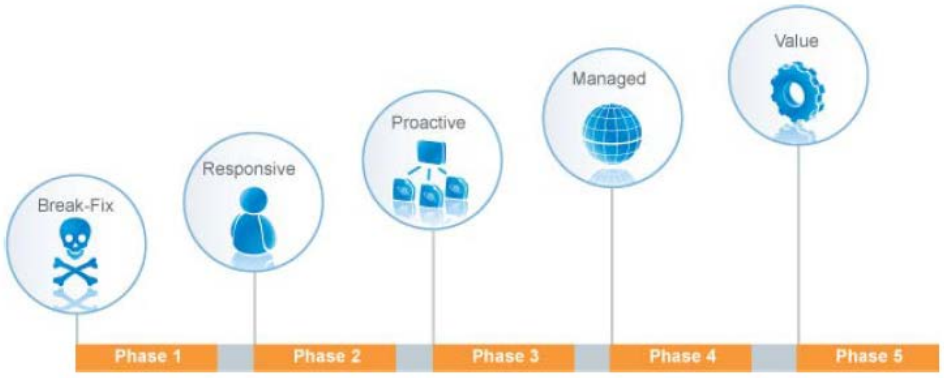
Uiteindelijke doelstelling van het project is een beheermodel waarmee Hupra proactief te werk kan gaan, de problemen tijdig kan ontdekken en de impact van de problemen kan beperken. In alle waarschijnlijkheid zal dit gebeuren met ondersteunende software welke actieve controles kan uitvoeren op systemen van klanten. Ondersteunt door aansluitende procedures betreffende de proactieve werkwijze. Doelstelling is ook deze ondersteunende software en procedures op een dusdanige manier in te richten dat druk in de organisatie wordt weggenomen door terugkomend onderhoud automatisch te laten uitvoeren en ervoor te zorgen dat werk bij de juiste beheerders terecht komt om een snelle afhandeling te garanderen. Dit kan tot het volgende worden samengevat:

- Proactief beheermodel;
- advies procedures/ verantwoordelijkheden;
- implementatie/ configuratie ondersteunende software;
- inrichting beheer met ondersteunende software.

Bovenstaande moet er uiteindelijk voor zorgen dat eerder genoemde problemen worden weggenomen en wordt bijgedragen aan de uiteindelijke doelen van Hupra (aangeduid over 1 jaar):

- Onderscheidend vermogen Hupra;
- kosten terugdringen (aantal facturabele uren verhogen met 20%);
- klantwerving (25+ klanten in het proactieve model);
- verlaging werkdruk (terugdringen break-fix werkzaamheden van 99% naar 50%);
- betrouwbaarheid dienstverlening/ ICT van de klant (van ±90% naar 99% beschikbaarheid);
- automatisering terugkomend onderhoud (van 0% naar 10-20%).

De werkwijze van Hupra (en ieder ander MSP) kan getoetst worden aan een MSP Maturity Model zoals weergegeven in onderstaande figuur. Op dit moment bevinden de meeste activiteiten van Hupra zich in de fases ‘break-fix’ en ‘responsive’. Het uiteindelijke doel van Hupra is deze werkzaamheden te verschuiven naar de fases ‘proactive’ en ‘managed’. Met deze werkwijze krijgt Hupra meer grip en zekerheid vanwege de mogelijkheid een ‘fixed price’ model te hanteren. Het project zal ondersteunend zijn aan deze hogere doelstelling.



Figuur 2: MSP Maturity Model (N-able Technologies)

4.2. Producten

Onderstaande tabel geeft een overzicht van de op te leveren producten en wat deze producten inhouden. Gegevens met betrekking tot afronding en oplevering van producten zijn te vinden in hoofdstuk 6 ‘planning’.

Product	Beschrijving
Plan van aanpak	Dit document
Onderzoeksrapport Proactief beheer	Het onderzoeksrapport ‘Proactief beheer’ zal een overzicht geven van het onderzoek naar de mogelijkheden van proactief beheer. In alle waarschijnlijkheid zal dit in combinatie met ondersteunende software pakketten gaan. Als toevoeging op het bovengenoemde zal er daarom een productvergelijking van dergelijke producten zijn bijgevoegd.
Ontwerp voor proactief beheer	Het ontwerp voor proactief beheer zal inzicht geven in de manier waarop ondersteunende software ingezet en geconfigureerd moet worden, en wat de bijbehorende procedures zijn. **De focus zal komen te liggen op adviezen van mogelijke configuratie van de software en de inrichting van ondersteunende procedures aan het proactieve beheermodel.** Verder zal dit document een advies voor product aanschaf bevatten.
Testomgeving ondersteunende software	Voordat de geadviseerde ondersteunende software in de productieomgeving ingezet kan worden dient deze eerst getest te worden. Deze tests zullen worden uitgevoerd in een hiervoor speciaal gebouwde omgeving. Deze omgeving en de test resultaten zullen worden vastgelegd in een testrapport.
Implementatie proactief beheer	Hupra verwacht een uiteindelijke **implementatie van de ondersteunende software en procedures voor proactief beheer**. De belangrijkste en meest stabiele en geteste oplossingen kunnen in de productie omgeving worden geïmplementeerd. Verwachtingen hiervan zijn hoog en Hupra hoopt hier in de toekomst verder op te kunnen bouwen.
Scriptie met bijlagen	De scriptie met alle bovengenoemde documenten toegevoegd als bijlagen. In de scriptie wordt het verloop van het project, de gemaakte keuzes en de uitwerking hiervan verantwoord.

4.3. Projectomgeving

Zoals ook te lezen is in hoofdstuk 2 'Bedrijfscontext' is Hupra op te splitsen in een afdeling zakelijk en een afdeling particulier, welke volledig los van elkaar beschouwd kunnen worden. De afdeling particulier richt zich op de verkoop van voornamelijk desktop systemen en randapparatuur aan particulieren. De afdeling zakelijk richt zich op implementatie en onderhoud van ICT in het MKB.

Dit project wordt uitgevoerd voor de afdeling zakelijk en zal van toepassing zijn op systemen die door deze afdeling worden gebruikt en zal betrekking hebben op de gehanteerde werkwijze binnen deze afdeling. Mogelijke implementatie van ondersteunende software pakketten t.b.v. deze proactieve werkwijze zullen worden getest in een speciaal hiervoor ontwikkelde testomgeving, welke is afgesloten en veiliggesteld van de huidige productieomgeving. Details van deze omgeving zullen worden vastgelegd in het testrapport.

Eventuele implementatie zal plaatsvinden in de productieomgeving welke ook betrekking zal hebben op omgevingen van klanten van Hupra. Typische klanten zijn MKB bedrijven met 2 tot 50 werkstations. Een gemeenschappelijk belang van deze partijen is een goede en foutloze werking van hun omgevingen zonder teveel problemen. Het is daarom bijzonder belangrijk rekening te houden met deze partijen en de continuïteit van deze systemen te waarborgen.

4.4. Scope

Voor de uitvoering van het project wordt een scope gedefinieerd om te voorkomen dat teveel wordt afgeweken van de 'kern' en het behalen van de doelstellingen onmogelijk wordt. Hieronder volgt een opsomming welke de uiteindelijke scope zal vormen:

- In kaart brengen wensen Hupra Automatisering aan het proactieve model;
- onderzoek proactief beheer;
- onderzoek naar ondersteunende software voor proactieve werkwijze (MSP software);
- product vergelijking/advies ondersteunende software;
- advies configuratie/implementatie ondersteunende software voor proactief beheer;
- implementatie ondersteunend software pakket en procedures;
- fine tuning van de software (optimale aansluiting bij Hupra).

Hieronder een aantal zaken welke niet onder de scope van het project zullen vallen. Als aanvulling hierop verwijs ik naar de beperkingen in hoofdstuk 4.6:

- kostenaspecten m.b.t. onderzoeken van besparingen;
- gevolgen voor het personeelsbestand;
- onderzoek naar de uiteindelijke verbetering van de marktpositie (zie doelstellingen, onderscheidend vermogen), dit is aan Hupra.

4.5. Randvoorwaarden

Om een goed verloop van het project te garanderen worden hier een aantal randvoorwaarden aan het project gesteld.

- Toegang tot een werkplek;
- Toegang tot systemen ;
  - Netwerk
  - Virtuele omgeving (hypervisor)
- Toegang tot een testomgeving voor ondersteunende tools;
- Op basis van het productadvies een aanschaf van de MSP software, voor de uiteindelijke implementatie;
- Iedere week zal er met de opdrachtgever en de begeleider een bespreking plaats vinden waarin de voortgang van het project kan worden besproken;
- Mogelijkheid tot het interviewen van werknemers en opdrachtgever. In het kader van het vaststellen van de eisen.

4.6. Beperkingen

Hieronder worden de beperkingen bij het project besproken.

- Beperking in tijd (840 uur)
  Voor dit project is een beperkt tijdsbestek beschikbaar van 840 uur. Dit is de vastgestelde tijd voor afstudeer opdrachten van het HBO. Hierbij is inbegrepen de benodigde tijd voor het opstellen van documentatie voor de opleiding en het schrijven van de scriptie.
- Financiële beperkingen
  Voor de implementatie van een proactief beheermodel met ondersteunend software pakket heeft Hupra 40.000 euro begroot. Hiernaast zijn er 800 uren begroot voor de uitvoering van het onderzoek en de implementatie.
- Beperking in beschikbare kennis (MSP software)
  Er is beperkte kennis aanwezig betreffende de ondersteunende software. Deze beperkingen hoop ik in de start en onderzoeksfases van het project weg te nemen. Hupra heeft voldoende tijd en mogelijkheden/materiaal beschikbaar gesteld om zoveel mogelijk kennis te vergaren.
- Beperkingen testomgeving
  De test omgeving is een beperkte omgeving in beschikbare apparatuur. Alleen het noodzakelijke zal aanwezig zijn. Bovendien zullen veel pakketten een proefversie van 30 dagen hanteren.

4.7. Projectrisico's en Maatregelen

Hieronder worden een aantal reële projectrisico's besproken. Tijdens het project is het mogelijk dat een of meer van deze risico's optreden. Ook wordt besproken hoe deze risico's voorkomen kunnen worden, wat de geschatte kans van optreden is, en hoe de impact van deze risico's zoveel mogelijk beperkt kan worden mochten deze optreden. Genoemde percentages zijn gebaseerd op ervaringscijfers en worden over het algemeen vergeleken met andere vergelijkbare afstudeerprojecten, dan wel technische projecten vergelijkbaar met deze. Daarnaast kan de kans beïnvloed worden door informatie voorhanden betreffende dit specifieke project.

Voor ieder risico is er bijvoorbeeld een geschatte kans van optreden. Deze cijfers komen voort uit onderzoeken en ervaringen van eerdere projecten. Na aanleiding van deze projecten weet men dat eens in de zoveel tijd het genoemde risico optreed. Daarvan uitgaand kan worden geschat dat deze zelfde kans ook voor dit project geld.

Men ziet bijvoorbeeld dat in 1 van de 20 vergelijkbare projecten een bepaald risico optreed. Met deze gegevens kan geschat worden dat de kans 1 op 20 (5%) is dat het risico ook in dit project optreed. Tenzij er van te voren al beperkende maatregelen zijn genomen waarvan gezegd kan worden dat deze het risico dusdanig beperken dat er een lagere kans kan worden opgegeven.

Overschrijden budget/ Uitlopen op de begroting

Het overschrijden van de geplande begroting zal niet direct consequenties met zich meebrengen, aangezien het een eenmalige aanschaf van software betreft is het nog voor de aanschaf duidelijk of de begroting overschreden wordt. Op het moment dat een overschrijding dreigt zal met Hupra overlegd worden wat de vervolg acties zijn, echter weegt dit niet zwaar en zal het geen directe consequenties voor de uitvoering van het project met zich meebrengen.

Geschatte kans van optreden: 10%. Bij algemene projecten zal deze kans veel groter zijn, echter betreft het hier alleen een eenmalige uitgave. De kans is nog wel minimaal aanwezig in het geval van bijvoorbeeld verkeerd ingeschatte product prijzen. De impact op het project is zoals gezegd minimaal.

Vertraging kennisvergaring

Het is mogelijk dat de kennisvergaring vertraging op loopt door bijvoorbeeld onvoorziene complexiteit van de materie.

Momenten inplannen in de start en onderzoek fase van het project, speciaal gereserveerd voor kennisvergaring betreffende het onderzoek.

Geschatte kans van optreden: 35%. De impact op het project wordt niet groot geschat, omdat het gedurende de uitvoering van het project nog mogelijk is verder detail onderzoek te verrichten.

Gebrekkige kwaliteitscontrole
Een gebrekkige kwaliteitscontrole kan als gevolg hebben dat bij oplevering de gewenste kwaliteit niet wordt behaald en het product dus niet voldoet.

Om dit te voorkomen is er iedere week een overleg met de opdrachtgever gepland waar o.a. zaken als projectvoortgang en kwaliteit aan de orde komen. Er kan wekelijks worden bijgestuurd op de verwachtingen omtrent de kwaliteit en voortgang.

Geschatte kans van optreden: 10%. Er worden voldoende maatregelen genomen, echter is de impact op het project nog steeds groot.

Extreme kwaliteitseisen
De kwaliteitseisen worden vastgelegd in dit plan van aanpak en bij ondertekening wordt hiermee akkoord gegaan. Deze eisen staan dus vast en kunnen niet zomaar wijzigen. Echter is het wel mogelijk dat de opdrachtgever gedurende het project met nieuwe eisen komt.

De wekelijkse momenten voor overleg met opdrachtgever en de duidelijk beschrijvingen van de producten dienen hierin duidelijkheid te verschaffen. Nieuwe eisen kunnen worden meegenomen indien deze goed overlegd worden, realistisch zijn en onder de scope van het project vallen.

Geschatte kans van optreden: 5%. In vergelijkbare afstudeerprojecten komt het wel eens voor dat de opdrachtgever gedurende het project met nieuwe kwaliteitseisen komt of extreme verwachtingen heeft bij de vastgestelde eisen in het plan van aanpak. Vaak valt dit te wijten aan onduidelijke afspraken in het plan van aanpak. De impact hiervan op het project schat ik klein omdat de afspraken in het plan van aanpak worden aangehouden, bijkomende eisen kunnen individueel beoordeeld worden, waarna besloten kan worden of hiermee wat wordt gedaan.

Tegenvallende testresultaten
De mogelijkheid bestaat dat de testresultaten uit de testomgeving tegenvallen en oplossingen extra tijd in beslag nemen, wat tot vertraging van de implementatie fase kan leiden.

Dit risico kan moeilijk voorkomen worden, mocht het risico tijdens het project optreden en is het dusdanig ernstig, moet er in een overleg met de opdrachtgever worden besloten of er extra tijd wordt besteed aan een oplossing. Of misschien moet het onderdeel worden weggelaten in de productie omgeving. In het vooronderzoek kunnen een aantal verwachtingen al worden ingevuld, zodat de verwachten testresultaten al tijden gestuurd kunnen worden.

De geschatte kans van optreden: 40%. Het gaat hier natuurlijk om testresultaten, deze test worden uitgevoerd met een reden, onzekerheden wegnemen. Een dergelijke test kan op verschillende manieren uitpakken. Hierover kan van te voren weinig worden gezegd. Er wordt geschat dat in 4 uit de 10 gevallen onderdelen uit de tests dusdanig tegenvallen dat deze op een andere manier dan in eerste instantie gewenst, geïmplementeerd moeten worden. De impact hiervan op het project is matig. Vaak is het mogelijk het beoogde resultaat ook op een andere manier te behalen.

Scopewijzigingen
Wijzigingen in de scope zijn net als wijzigingen van kwaliteitseisen niet mogelijk. De scope is vastgelegd in dit document. Er bestaat wel een mogelijkheid dat deze wijzigingen wel worden meegenomen, echter vormen deze dan een nieuw project buiten dit project om.

Gedurende de uitvoering van het project moet de scope (opgesteld in dit document) nauwlettend in de gaten worden gehouden zodat er niet wordt afgeweken.

De kans van een wijziging in de scope is statistisch gezien 0%, omdat dit niet mogelijk is. De kans dat er onderdelen worden toegevoegd aan de scope in de vorm van een aanvullend mini-project, wordt geschat op 30%.

Onvoorziene taken
Onvoorziene taken kunnen ertoe leiden dat het project vertraging oploopt, in ernstige gevallen een tekort aan tijd wordt veroorzaakt.

In de planning zijn zoveel mogelijk voorziene taken opgenomen. In de huidige planning is ruimte beschikbaar om deze mogelijke onvoorziene taken op te vangen. Mocht dit niet voldoende zijn, dan moet in overleg worden bepaald of de planning mogelijk aangepast wordt.

De geschatte kans van optreden: 30%.

Onvoorziene technische problemen
Onvoorziene technische problemen kunnen net als onvoorziene taken tot gevolg hebben dat het project uitloopt.

Zorgvuldig onderzoek naar de producten en systemen moet zoveel mogelijk onvoorziene problemen voorkomen. In de praktijk is dit alleen niet te realiseren. Bij onvoorziene problemen moet zo snel mogelijk een oplossing worden verzonnen. In extreme gevallen kan worden besloten dat onderdeel te laten ‘vallen’ of in beperkte vorm op te leveren, om de rest van het project niet in gevaar te brengen.

De kans van optreden wordt geschat op 60%. De kans dat deze problemen ernstige vertraging van het project tot gevolg hebben wordt lager ingeschat op ongeveer 10%.

Uitlopen werkzaamheden
Door bijvoorbeeld technische problemen is het mogelijk dat werkzaamheden uitlopen, met mogelijke uitloop van het project als gevolg. Verder zijn er ook veel andere factoren welke uitloop van het project tot gevolg kunnen hebben. Denk bijvoorbeeld aan ziekte van de uitvoerend student.

Een duidelijke planning moet hier uitkomst bieden. De planning moet wel mogelijkheid voor uitloop bieden zodat men niet direct in de problemen komt bij uitloop van een activiteit. Mocht het toch voorkomen dat een activiteit uitloopt dan moet worden gezocht naar een mogelijkheid deze tijd ergens anders in de planning vrij te maken.

De geschatte kans van optreden is hier: 5%. Het kan voorkomen dat het project dusdanig uitloopt (door bijvoorbeeld ziekte of optreden van bovengenoemde risico’s) dat de planning en de uiteindelijke oplevering in gevaar komt.

5. Aanpak

In dit hoofdstuk zal de aanpak van het project worden toegelicht. Hierbij wordt o.a. de fasering van het project toegelicht, welke in het volgende hoofdstuk verder uitgewerkt zal worden tot een planning. Verder worden een aantal zaken als benodigde en beschikbare kennis besproken een zal er kort aandacht worden besteed aan de te gebruiken standaarden, methodes en kwaliteitsbewaking.

5.1. Fasering

Om tot een duidelijke planning van het project te komen wordt het project opgedeeld in een aantal fases. Deze fases zijn bedoeld om meer grip op het project en op de voortgang te krijgen. Het project zal worden opgedeeld in de onderstaande fases:

- Fase 1: Project start
- Fase 2: Onderzoek
- Fase 3: Ontwerp
- Fase 4: Test
- Fase 5: Implementatie
- Fase 6: Project afronding

Het is mogelijk dat bovengenoemde fases van het project met elkaar overlappen. De fase test kan bijvoorbeeld overlappen met een aantal andere fases zoals ontwerp en implementatie. Dit komt voor omdat activiteiten uit verschillende fases veel op elkaar lijken, hetzelfde, of sterk van elkaar afhankelijk zijn.

5.1.1. Fase 1: Project start

In deze fase zal al het voorbereidende werk voor het project worden gedaan. Hier worden de planningen gemaakt en de project documenten opgesteld zoals bijvoorbeeld het plan van aanpak.

Het opstellen van het plan van aanpak en het maken van de planningen zal verlopen volgens projectstandaarden (licht gebaseerd op PRINCE2) en formats aangereikt in de afstudeerleidraad.

5.1.2. Fase 2: Onderzoek

In deze fase zal het onderzoek plaatsvinden. Dit is een onderzoek naar proactief beheer en welke ondersteunende software hiervoor beschikbaar is. Er zal worden onderzocht op welke manier dit proactief beheer het beste vorm kan worden gegeven binnen Hupra. Bovendien zal deze fase ook aanleiding zijn voor een product analyse/vergelijking van MSP software oplossingen. Resultaten van de onderzoeksfase zullen worden vastgelegd in het onderzoeksrapport ‘Proactief beheer’.

Dit onderzoek is voornamelijk een documentonderzoek waarbij informatie zal worden verzameld van artikelen op het internet, uit de literatuur, en documentatie afkomstig van verschillende fabrikanten en onderzoeksbureaus. Naast inzicht in de bestaande documentatie heeft Hupra mij ook de mogelijkheid gegeven presentaties en demo’s van fabrikanten bij te wonen. Aansluitend zullen open interviews worden gehouden met de opdrachtgever en twee werknemers van verschillende disciplines om de eisen en verwachtingen duidelijk te stellen. Na aanleiding van de uitkomsten van deze interviews zal gedurende de uitvoering van het project bekeken worden of het nodig is ook de klanten te benaderen.

5.1.3. Fase 3: Ontwerp

In deze fase van het project worden de onderzoeksresultaten verwerkt tot een ontwerp voor proactief beheer binnen Hupra. Dit ontwerp is een advies over hoe om te gaan eindeloze hoeveelheid mogelijkheden die door een dergelijk MSP pakket worden geboden en op welke manieren dit binnen Hupra kan worden gebruikt ter ondersteuning van het beheer. De ontwerp fase zal ook een product advies opleveren welke Hupra ondersteunt in het maken van een product keuze.

Ontwerpen en advies voor procedures zullen gedeeltelijk gebaseerd zijn op de ITIL standaarden. De ITIL standaard kan volledig worden benut, echter kan er ook voor worden gekozen alleen bepaalde onderdelen uit ITIL te 'lenen'. Dit laatste is waarschijnlijker aangezien Hupra geen grote organisatie is en een volledige implementatie van ITIL weinig resultaat zal hebben. Dit zal alleen de flexibiliteit van het bedrijf wegnemen. Een definitieve keuze hierover zal gedurende de loop van het project gemaakt worden.

5.1.4. Fase 4: Test

De vierde fase van het project is een testfase waarin het gekozen product (uit het productadvies) zal worden getest op een speciaal hiervoor ingerichte testomgeving. Details van deze testomgeving zijn in de ontwerp fase uitgewerkt. Vast staat dat deze omgeving een gedeeltelijke replica van de uiteindelijke productieomgeving is. Welke de kritische eigenschappen van de productie omgeving moet verantwoorden.

In de test fase zal de software worden getest op mogelijke configuraties uit het 'advies proactief beheer' en zal verder detail onderzoek worden gedaan naar de functionaliteiten van het pakket. Er is voor gekozen alleen de definitieve keuze grondig te testen, dit vanwege de mogelijke kosten en tijd aan deze geavanceerde pakketten. Deze fase zal daarom ook enige overlap hebben met fase 3 'ontwerp'. Verder zal het product ook worden getest op stabiliteit en zal er worden gekeken naar acceptatie binnen de afdeling zakelijk. Resultaten van deze fase zullen worden vastgelegd in een testrapport. Deze fase zal bovendien ook dienen als een acceptatie fase voor de software.

5.1.5. Fase 5: Implementatie

De vijfde fase van het project is de implementatie fase. In deze laatste fase zal de ondersteunende software worden geïmplementeerd en een werkbare omgeving worden opgeleverd. Verder zal in deze fase de implementatie van het proactieve beheer worden afgerond. De resultaten van de voorgaande fases zullen in deze laatste fase in de praktijk worden gebracht. De positieve testresultaten uit fase 4 zullen in productie worden genomen. Plannen voor deze implementatie zullen worden opgesteld aan het einde van de implementatie fase en zullen worden gebaseerd op de testresultaten.

5.1.6. Fase 6: Project afronding

Dit is de laatste fase van het project. Onder deze fase vallen zaken als de afronding van de documentatie, kennis overdracht aan het bedrijf, afronding van de scriptie en voorbereiding van de presentatie e.d. Verder worden in deze fase mogelijke 'losse eindjes' aan elkaar geknoopt.

5.2. Kennis

De vereiste kennis voor deze opdracht betreffende de ondersteunende software en mogelijke problemen hiermee zal vooral afkomstig zijn van de support van de fabrikanten. Voor een aantal van de mogelijke tools is Nederlandse support beschikbaar, voor een aantal anderen is support alleen beschikbaar in het Engels. Kennis betreffende monitor systemen en server beheer is vooral afkomstig zijn van een aantal vakken uit de hoofdfase zoals:

- Exploitatie en Beheer (inrichting beheer, beheers methodieken);
- Windows (Windows beheer, OS);
- Netwerkbeheer & Infrastructuren (algemene kennis infrastructuren);
- CISCO (netwerk kennis, configuratie);
- Monitoring (SNMP structuren);
- ICT Architectuur (systeem architecturen, service architectuur);
- Scripting (server scripting, beheer automatiseren);
- ervaringen uit de semester 5 stage (server- en netwerkbeheer, Hosting).

Overige kennis en ervaringen over de gebruikte systemen bij klanten en binnen het bedrijf, zal ik uit het bedrijf zelf moeten halen.

Kennis op het gebied van proactief beheer zal ik kunnen halen uit vakken als Exploitatie en Beheer en ICT architecturen. Verder is over dit onderwerp voldoende literatuur beschikbaar om te raadplegen. Denk hierbij bijvoorbeeld aan verschillende standaarden als ITIL, met bijbehorende literatuur.

Een aantal fabrikanten van de ondersteunende tools bieden verschillende mogelijkheden voor opleidingen en uitgebreide ondersteuning bij gebruik en implementatie trajecten van hun software. Dit varieert van online trainingen tot officiële trainingen in klaslokalen. Hupra heeft mij in de mogelijkheid gesteld een aantal van deze training te volgen om mijn kennis betreffende de verschillende producten te vergroten en op basis van deze informatie een evenwichtige keuzes tussen de producten te kunnen maken. Deze kennis en de literatuur op het gebied van deze software kan ik op deze manier makkelijk uitbreiden. Ik ben ervan overtuigd dat ik met deze informatie de eerder genoemde beperking ‘tekort aan kennis betreffende MSP’ hiermee weg kan nemen.

5.3. Standaarden

Op dit project zullen vanzelfsprekend een aantal standaarden en methoden/Technieken van toepassing zijn. Hieronder wordt een korte opsomming gegeven van een aantal standaarden/methoden waarmee men in aanraking kan komen:

- MSP Maturity Model, N-able Technologies (onderzoek, ontwerp)
- ISO27001 (ontwerp, test, implementatie)
- Netwerkmonitoring SNMP (test en implementatie)
- Windows/UNIX/Netwerk beheer (van toepassing gedurende het gehele project)
- Standaarden projectmanagement (PRINCE2) (van toepassing gedurende het gehele project)
- ITIL (onderzoek, ontwerp)
- VBscript/Batch scripting (ontwerp, test, implementatie)

5.4. Kwaliteitsbewaking

Het is van groot belang dat de uiteindelijke producten zullen voldoen aan de verwachtingen, en de eerder gestelde doelstellingen waargemaakt kunnen worden. Daarom moeten er een aantal afspraken worden gemaakt omtrent controle en kwaliteitsbewaking.

Allereerst zal er iedere week een contactmoment zijn met de opdrachtgever en de begeleider. Op deze wekelijkse contactmomenten zal niet alleen de voortgang van het project aan de orde komen, maar ook hoe het staat met de producten en de kwaliteit hiervan. Op deze momenten zal worden gekeken of het (concept) product op dat moment aan de verwachtingen voldoet of kan gaan voldoen, zo niet dan kan dit nog tijdig worden bijgestuurd.

Naast de contactmomenten met de opdrachtgever en de begeleider zullen er ook verschillende contactmomenten met de docentbegeleider plaatsvinden. Op deze momenten kan ook vanuit school een oordeel worden gegeven over de eerdergenoemde onderwerpen. Ook vanuit school is de mogelijkheid aanwezig voor aanpassing en/of bijsturing.

6. Planning

Voor de planning van het project zijn 840 uren beschikbaar gesteld. Hieronder zal worden uitgewerkt hoe deze uren over de verschillende projectactiviteiten worden verdeeld. De planning moet voor houvast binnen het project zorgen. Er kan mogelijk worden afgeweken van onderstaande planning, dit ten alle tijden in overleg met de opdrachtgever, begeleider en docentbegeleider.

Fase	Start	Eind	Producten
1. Project start	1 feb	15 feb	Concept plan van aanpak
	15 feb	16 mrt	Plan van aanpak en contract afstudeeropdracht
2. Onderzoek	6 feb	24 feb	Onderzoeksrapport Proactief beheer
	6 feb	24 feb	Onderzoek ondersteunende software
3. Ontwerp	27 feb	9 mrt	Ontwerp Proactief beheer
	12 mrt	14 mrt	Ontwerpen testomgeving
	12 mrt	14 mrt	Opstellen test criteria
4. Test	15 mrt	21 mrt	Opzetten testomgeving
	22 mrt	11 apr	Testen ondersteunende software
	22 mrt	11 apr	Vastleggen testresultaten
5. Implementatie	14 apr	25 mei	Implementatie Proactief beheer en ondersteunende tools
6. Project afronding	14 mei	1 jun	Documentatie omgeving
	1 jun	11 jun	Voorbereiden presentatie
	27 feb	16 mei	Scriptie met bijlagen

Als bijlage aan dit document zal van de bovenstaande planning ook een visuele weergave worden toegevoegd. Deze weergave is te vinden in bijlage 1 ‘Project planning’.

Als toevoeging op deze project planning zal er iedere week een contactmoment met opdrachtgever en bedrijfsbegeleider worden gepland. Hiervoor wordt iedere week een uur uitgetrokken. Op verzoek kan hier van af worden geweken mochten er problemen zijn waardoor meer tijd benodigd is.

7. Projectinrichting

Het betreft hier een zelfstandig project wat uniek is binnen Hupra, er zijn eerder geen vergelijkbare projecten uitgevoerd. Onderhoud wordt op dit moment handmatig uitgevoerd, wat een tijdrovende klus is. Opdrachtgever van dit project is Dhr. P.A. Willemsen, directeur Hupra Automatisering. Welke tevens ook mijn aanspreekpunt is voor technische ondersteuning van het project. Voor dagelijkse begeleiding bij het project kan ik mezelf wenden tot Dhr. C. van Westen.

Er zal iedere week een uur worden uitgetrokken voor overleg met Dhr. P.A. Willemsen en Dhr. C. van Westen om de voortgang van het project door te spreken. Verder zullen zij vrijwel altijd beschikbaar zijn voor vragen of directe dringende problemen.

7.1. Contactgegevens

Bedrijf
Hupra Computers & Automatisering
Hoofdstraat 105
3901 AK Veenendaal

Opdrachtgever/ (Bedrijfsbegeleider)
Dhr. P.A. Willemsen
p.a.willemsen@hupra.nl
06-25037562

Bedrijfsbegeleider
Dhr. C. van Westen
cvwesten@hupra.nl
+31 (0)318 528 528

Student
M.M.J de Weijer
Spilbergen 4
4032 NW Ommeren
06-30720031
mike.deweijer@student.hu.nl

8. Bronnen

Afstudeerleidraad Instituut voor ICT 2011-2012
http://www.voorbedrijven.hu.nl/los/ICT/Praktijkbureau%20ICT/~/media/HU-BEDRIJVEN/docs/Praktijkbureau%20cluster%20ICT/Afstudeerleidraad%20Instituut%20voor%20ICT%20vt%20dt%20du%20cursus%202011-2012.ashx

MSP Maturaty Model – N-Able

Opdrachtgever
Dhr. P.A. Willemsen

Bedrijfsbegeleider
Dhr. C. van Westen

Internet bronnen
http://zbc.nu/ict/project-management/standaard-plan-van-aanpak/
http://www.hbo-kennisbank.nl/nl/page/home/

Bijlage E: Installatie Checklist

Proactief beheer bij Hupra

Auteur:
M.M.J. de Weijer
Studentnummer: 1546128
Hogeschool Utrecht
Faculteit Natuur & Techniek
Systeembeheer

Bedrijf:
Hupra Automatisering
Hoofdstraat 105
3901 AK Veenendaal

Begeleiders:
Hupra: Dhr. P.A. Willemsen
Hogeschool Utrecht: Dhr. H. van Nimwegen

Afstudeerperiode:
februari 2012 - juni 2012

Versie: 1.2
Datum: 24 mei 2012

Versie beheer:

Versie	Datum	Wijzigingen
0.0	20-04-2012	Initiële versie document, geen inhoud
1.0	27-04-2012	Invulling document
1.1	17-05-2012	Aanpassingen aan SonicWall Configuratie
1.2	24-05-2012	Afronden document, opmaak

Over de checklist

Dit document is een checklist welke gebruikt kan worden bij installatie of toevoegen van een nieuwe klant aan het Managed Services systeem: N-central. Deze lijst heeft als doel een houvast en een geheugensteun te zijn voor beheerders. Deze lijst is niet bedoeld als een strikte handleiding welke opgevolgd MOET worden. In deze lijst worden een aantal punten als herinnering genoemd. Daarnaast staat beschreven hoe deze punten geconfigureerd kunnen worden.

Deze lijst zal constant aan veranderingen onderhevig zijn. Naarmate er meer functies in het managed services model worden opgenomen, zal deze lijst ook groeien. Daarnaast is het mogelijk dat in de toekomst de lijst moet worden aangepast omdat er op dat moment misschien betere methodes voorhanden zijn.

Aanmaken nieuwe klant

1. Klant aanmaken via **Actions -> Add Customer/Site**

   Default Credentials
   In het domein van de klant een account aanmaken genaamd n-able en deze administrator rechten geven. Deze zijn benodigd voor het installeren van agents en het uitvoeren van scripts en geplande taken.

   Licenties configureren
   Bij het toevoegen moet het aantal verkochte licenties worden ingesteld op de klant in N-central.

   Administration - > Customers/Sites -> <Customer> -> Limits

2. Installeer vervolgens een Windows Probe op een centrale server in het netwerk van de klant. Zijn er meerdere gescheiden netwerken dan is het aan te raden in ieder netwerk een probe te installeren.

   Bij de installatie van de Windows Probe zal nogmaals om het gemaakte n-able account worden gevraagd.

   Er wordt automatisch een Discovery Job aangemaakt voor het opgegeven netwerk.

3. Wacht totdat de Discovery voltooid is.

Windows Werkstations/Servers

1. Devices zullen worden weergegeven onder **Actions -> Add/Import Devices**. Desgewenst kunnen devices ook handmatig worden toegevoegd door de agent te installeren.

2. Controleren en toevoegen service templates.

   Werkstations zijn standaard voorzien van de juiste templates. Servers worden voorzien van alleen de basis templates. Aanvullende templates voor bijvoorbeeld Active Directory dienen te worden toegevoegd.

   Voor fysieke servers zijn extra service templates beschikbaar voor het monitoren van de Hardware. Voor meer informatie, zie bijlage: ‘Hardware Monitoring HP’.

3. Niet aanwezige services verwijderen.

   Het kan voorkomen dat er een aantal services worden toegevoegd via een service template, welke niet van toepassing zijn op de geselecteerde server. Deze services kunnen verwijderd worden, om foutieve meldingen te voorkomen.

4. Voor een goede werking van de Connectivity service kan het nodig zijn dat een extra regel in de Windows Firewall voor het toestaan van icmp-echo aanvragen wordt aangemaakt.

5. (Bij het gebruik van Endpoint Security) Oude virus scanner verwijderen. Norman verwijderen met het script aanwezig in N-central, of handmatig met Del

6. Optie selecteren voor Endpoint security op het N-central Device Properties tabblad

7. Controleren en instellen garantie monitoring met bijbehorende data op het Device Properties tabblad.

SonicWall

1. Toevoegen van een SonicWall kan vanuit een discovery job, zoals hierboven beschreven, of geheel handmatig.
2. Na het toevoegen SNMP instellingen controleren.

   Controleer de SNMP instellingen op de Device properties pagina van de SonicWall. De checkbox 'Use SNMP' dient aangevinkt te zijn en de community string dient overeen te komen met de SNMP instellingen van de SonicWall. Een asset scan kan benodigd zijn.

3. Instellingen Connectivity monitoring.

   Standaard zal de Connectivity van de SonicWall worden gemeten vanaf de Windows Probe in het netwerk. Als men de Connectivity van de internet verbinding wil meten, dient dit veranderd te worden naar een meting vanaf de N-central server.

   1. Ga naar de Status tab.
   2. Klik op de service Connectivity
   3. Tabblad Service Details

      Monitored By: Central server – ms.hupra.nl

   4. Save

   Het is ook mogelijk een extra service toe te voegen zodat zowel de interne connectiviteit als de connectiviteit van de internet verbinding kan worden gemeten.

   1. Ga naar de Status tab.
   2. Add

      Monitoring Probe: Central server – ms.hupra.nl

   3. Connectivity: 1
   4. OK

4. Traffic instellingen op WAN interface

Device -> Status tab -> Traffic – X1 (WAN) -> Tab Service Details

Thresholds Tab
Alle thresholds op 'off' behalve: Outgoing Bandwidth Utilization (%) en incoming Bandwidth Utilization (%).

Configuratie op de SonicWall zelf kan benodigd zijn mocht hier nog geen SNMP op geconfigureerd zijn. Dit kan worden gedaan door:

1. Inloggen op de management interface van de SonicWall

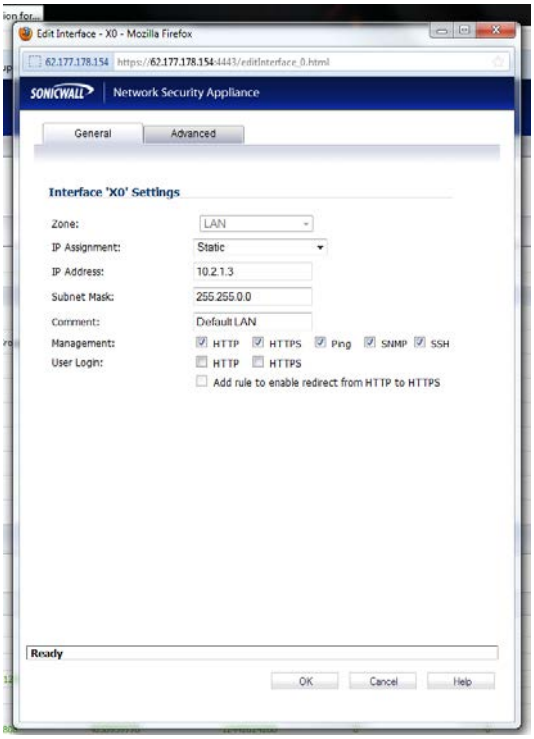
2. **System -> Advanced ->** Optie voor SNMP aanvinken
   Configuratie van de instellingen is mogelijk. Let op bij het wijzigen van de community string, deze zal ook in N-central moeten worden aangepast naar dezelfde waarde

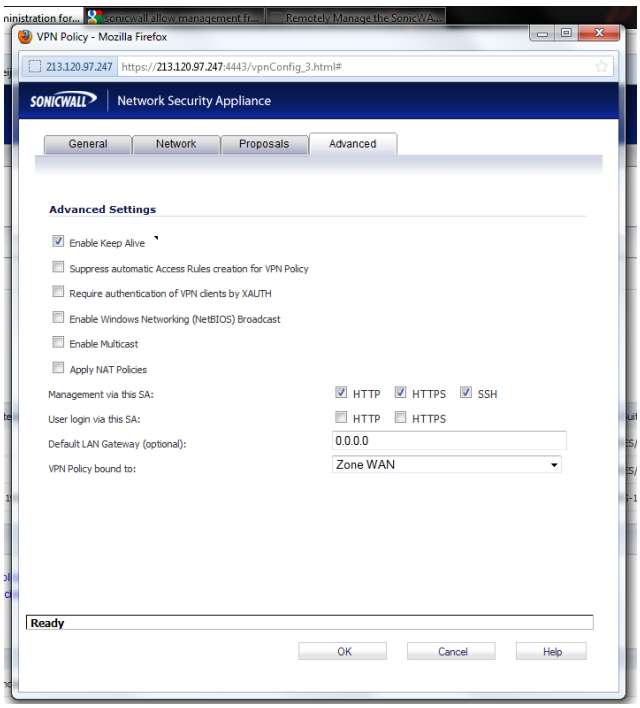
3. **Network -> Interfaces**
   Op Edit klikken achter de interface X0 – LAN
   Bij de optie management SNMP aanvinken.

4. Met sonicwall systemen welke gekoppeld zijn via VPN tunnels kan het nodig zijn SNMP management over VPN in te schakelen.

   VPN -> Settings -> VPN policy -> Configure

   Op het tabblad advanced: Management via this SA HTTP, HTTPS en SSH aanvinken





Patch management

Het activeren van patch management bij een klant bestaat uit de volgende stappen:

1. Patch methode bepalen aan de hand van de adviezen vastgelegd in het document 'Voorstel Patch management'. Als er wordt gekozen voor het profiel 'Microsoft Update Servers' dan kan meteen verder worden gegaan met stap 5.

	0 – 10 Devices	10 > Devices
Patch architectuur	Gebruik maken van Microsoft Update Servers	WSUS server op locatie van de klant

2. Server selecteren welke de WSUS server taak zal gaan uitvoeren. Deze server dient voldoende schijfruimte beschikbaar te hebben, 30-60GB voor WSUS content.
3. WSUS server installeren met standaard instellingen. Basisselectie in producten kan worden gemaakt, maar kan ook vanuit N-central worden doorgevoerd. De WSUS functie van de server wordt automatisch herkend bij een Asset Scan.
4. In sommige gevallen is het nodig de WSUS server in N-central in te schakelen en te configureren onder: **Configuration -> Patch Management -> WSUS servers**
5. De laatste stap is het inschakelen van het patch management op de 'Properties' pagina van de betreffende machines. Hier wordt ook de keuze gemaakt voor het toe te passen patch profiel.

Profiel	Server	Tijdstip
MSU – Workstation	Microsoft Update	Iedere werkdag om 11:00 uur.
MSU – Server	Microsoft Update	Wekelijks op maandag 01:00 uur.
WSUS – Workstation	WSUS klantlocatie	Iedere werkdag om 11:00 uur.
WSUS – Server	WSUS klantlocatie	Wekelijks op maandag 01:00 uur.

Backup

Backup manager (N-central)

Alvorens het juiste profiel in te schakelen, eenmalig de backup share voor de klant instellen:
Configuration -> Backup Manager -> Backup Share

Op het device properties tabblad kan vervolgens de backup functie worden aangevinkt en het juiste profiel worden gekozen.

Is er een afwijkend profiel nodig dan kan deze worden aangemaakt door op de **Add** knop te klikken en hier een nieuw profiel aan te maken.

Acronis

Wordt er gebruik gemaakt van een Acronis backup dan kan deze controle simpel worden toegevoegd door het Acronis service template toe te voegen. Dit template zal alle mogelijke controles toevoegen. Sommige controles dienen weer verwijderd te worden als deze functies niet zijn geïnstalleerd.

Na het toevoegen kan het zijn dat de Acronis log controle de status Misconfigured geeft met een foutmelding “logfile not found”. In dit geval dient de log file locatie te worden aangepast door naar het tabblad **Service Details** te gaan. Op Windows 2003 servers is dit over het algemeen:

C:\Documents and Settings\All Users\Application Data\Acronis\ServiceProcess.log - B&R 11*
C:\Documents and Settings\All Users\Application Data\Acronis\TrueImage\Logs.log – B&R 10*

Op Windows 2008 zijn deze veranderd naar:

C:\ProgramData\Acronis\ServiceProcess.log - B&R 11*
C:\ProgramData\Acronis\TrueImage\Logs.log – B&R 10*

Backup Exec

Toevoegen van Backup Exec kan op de properties pagina van de machine in kwestie. Onder monitor backups kan de Backup Exec optie worden aangevinkt. Vervolgens dient er een username en password te worden ingevoerd voor het uitlezen van de Backup taken.

Naast het inschakelen van de Backup Exec optie kan het ook nodig zijn het juiste service template te activeren (Backup Exec).

Naast het toepassen van het template kan het af en toe voorkomen dat de backup exec service handmatig moet worden toegevoegd omdat deze niet goed mee zou komen van uit het service template.

Dit kan gedaan worden door op het tabblad **Status** en vervolgens op de knop **Add** te klikken. Voer in het veld ‘Backup Exec’ het aantal services in dat moet worden toegevoegd (één voor elke job). Door vervolgens op de service status te klikken kan een job worden toegekend.

Solcon Online Backup

Toevoegen van monitoring op Solcon Online Backup verloopt hetzelfde als het toevoegen van een Acronis check. Solcon Online Backup kan toegevoegd worden met het bijbehorende service template. Ook hier kan het wel eens voorkomen dat er een misconfigured status wordt gegeven omdat de logfile niet gevonden kan worden. Deze kan worden aangepast via het tabblad **Service Details.**

Windows Server 2003:

C:\Documents and Settings\All Users\Application Data\Solcon OBM Pro\CDP\log\info.log

Windows Server 2008:

C:\ProgramData\Solcon OBM Pro\CDP\log\info.log

Controle Service templates

Als laatste stap een soort optimalisatie stap ter controle of alle mogelijke functies van het pakket worden benut.

Wat voor servers zijn aanwezig en opgenomen? Klopt dit?

Welke functies vervult de server? Zijn hiervoor de juiste Service Templates toegepast?

Zijn er misschien maatwerk services/pakketten aanwezig op de server welke gemonitord kunnen worden?

Betreft het een fysieke of virtuele server? Zijn de Hyper-V service templates toegevoegd? Is de HP monitoring geïnstalleerd op de fysieke server? Zijn de templates hiervoor toegevoegd?

Geven alle services een betrouwbare meting? Geen misconfigured status?

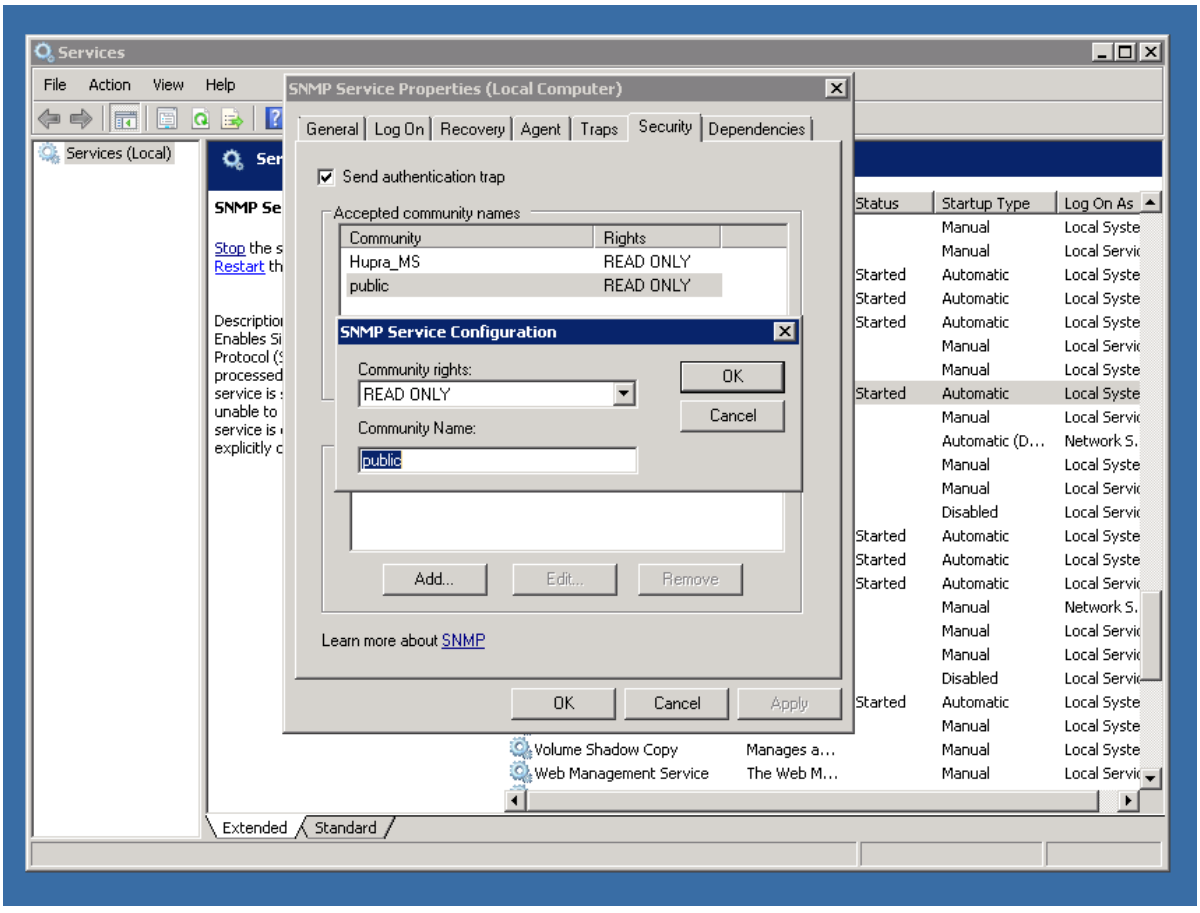
Hardware monitoring HP

Op de fysieke server:

- HP insight manager agents installeren
- SNMP community public als read-only toevoegen
- Windows Firewall SNMP controleren

In N-central:

- SNMP inschakelen device properties
- HP Servers template toevoegen



Bijlage F: Productonderzoek

Proactief beheer bij Hupra

Auteur:
M.M.J. de Weijer
Studentnummer: 1546128
Hogeschool Utrecht
Faculteit Natuur & Techniek
Systeembeheer

Bedrijf:
Hupra Automatisering
Hoofdstraat 105
3901 AK Veenendaal

Begeleiders:
Hupra: Dhr. P.A. Willemsen
Hogeschool Utrecht: Dhr. H. van Nimwegen

Afstudeerperiode:
februari 2012 - juni 2012

Versie: 1.0
Datum: 24 mei 2012

Versie beheer:

Versie	Datum	Wijzigingen
0.0	08-02-2012	Initiële versie document, geen inhoud
0.1	13-02-2012	Invulling Producten
0.2	17-02-2012	Uitwerking MSP
0.3	20-02-2012	Configuratie Service Templates
1.0	24-05-2012	Verwerking feedback, Afronden document, opmaak voor bijlage scriptie

Inhoud

1. Inleiding

Dit document is het resultaat van een onderzoek naar proactief beheer. In dit document zijn de bevindingen van het onderzoek naar proactief beheer beschreven. De aanleiding voor dit onderzoek is de vraag naar proactief beheer bij Hupra. Het doel van dit document is duidelijkheid verschaffen betreffende proactief beheer in het algemeen. Dit onderzoek zal als basis dienen voor een ontwerp/adviesrapport voor proactief beheer binnen Hupra. Gedurende het onderzoek is er aandacht besteed aan wat proactief beheer is en wat voor gevolgen het voor een bedrijf kan hebben, zowel positief als negatief. Bovendien zal er veel aandacht worden besteed aan software welke ondersteunend moet zijn aan het proactieve model, wat de mogelijkheden hiervan zijn en hoe een MSP deze kan benutten om een zo efficiënt mogelijke dienstverlening te bieden aan de klant.

Allereerst zal een algemene indruk van proactief beheer worden gegeven. Hierbij komen een aantal zaken zoals een algemene uitleg, voor- en nadelen en valkuilen aan bod. Daarna zal een groot deel van dit document worden besteed aan beschikbare software ter ondersteuning van dit proactieve model. Ten slotte zal er worden afgesloten met een conclusie betreffende de mogelijkheden van het proactieve model.

2. Proactief beheer

Door de enorme groei die de IT de laatste jaren heeft doorgemaakt, zijn veel systemen in hoeveelheid en complexiteit gegroeid. Het traditionele 'break-fix' model is in veel gevallen niet meer toereikend. Door de 'zero tolerance' mentaliteit bij bedrijven stijgt de werkdruk bij service providers, terwijl op rustige momenten de helft van de beheerders met de armen over elkaar zit. Door dit 'break-fix' model loopt een service provider altijd achter de feiten aan. Er is geen grip en inzicht in wat de systemen doen en er is geen inschatting of planning te maken in de toekomstige werkzaamheden. Dit levert voor de service providers veel onzekerheden op, het is bijvoorbeeld moeilijk inschattingen te maken van de verwachte inkomsten. Bovendien is de concurrentie op deze markt erg sterk en hebben service providers in dit 'break-fix' model nauwelijks tot geen mogelijkheid om zich te onderscheiden van de concurrenten.

Om deze problemen te verminderen, zoeken veel service providers de oplossingen in de techniek en schaffen een monitorpakket aan voor het monitoren van een aantal basisvereisten aan de kritieke systemen. Vaak is dit een overhaaste aanschaf en geeft het niet alle mogelijkheden om uit het 'break-fix' model te komen. Er worden zelfs combinaties van verschillende pakketten gemaakt, wat niet bijdraagt aan de eenvoud in beheer. Zelfs als deze eenvoud bereikt wordt, is het aanschaffen van software alleen niet genoeg. Om uit dit 'break-fix' model te komen, zullen service providers veranderingen in hun werkwijze, marketing, sales en management moeten doorvoeren.

2.1. Wat is MSP/proactief beheer?

Een Managed Server Provider (MSP) verschilt van de "normale service provider" of automatiseerder in die zin dat een Managed Service Provider het beheer onder controle heeft en proactief te werk kan gaan. Een MSP is in staat de mogelijke problemen bij een klant vroegtijdig te ontdekken en dit probleem nog voor het optreedt te verhelpen. Hierdoor zal de impact van het probleem minimaal blijven. Bovendien is de MSP in staat verschillende standaard beheerstaken geautomatiseerd uit te voeren. Hierbij valt bijvoorbeeld te denken aan back-up, patches, antivirus updates. De MSP moet als het ware alle ICT zorgen bij de klant wegnemen en deze klant op een actieve wijze ondersteunen in zijn ICT. Het liefst allemaal voor een vast bedrag per maand. Een volgende stap in dit systeem is 'ICT as a utility' aanbieden. De MSP biedt ICT aan, in welke vorm dan ook, en de klant betaald alleen voor wat er wordt gebruikt. De klant wordt gefactureerd voor de waarde van een geleverde service en de hoeveelheid service die geleverd is. Niet meer voor de besteedde tijd zoals bij het klassieke 'break-fix' model het geval was. De MSP draagt dan de verantwoordelijkheid voor de werking van de ICT, de klant mag hier verder geen hinder van ondervinden. Deze afspraken worden meestal vastgelegd in een Service Level Agreement.

Een proactief beheermodel moet een aantal voordelen bij zowel de automatiseerder als de klant opleveren. Voor een automatiseerder zal een proactief model bijvoorbeeld voor meer overzicht zorgen en moet een automatiseerder in staat stellen werkzaamheden gestructureerd in te plannen. Bovendien zal een proactief model gepaard gaan met bijbehorende service level agreements wat de automatiseerder een zekerheid geeft van zijn inkomsten. De voordelen voor de MSP zullen vooral te vinden zijn in werkdrukverlaging en zekerheid. Daarnaast zullen ook een aantal praktische besparingen worden bereikt. Zo zal het bijvoorbeeld minder vaak voorkomen dat een beheerder naar een klant op locatie moet. Dit spaart reiskosten en -tijd uit. Bovendien zal deze "rust" meer ruimte

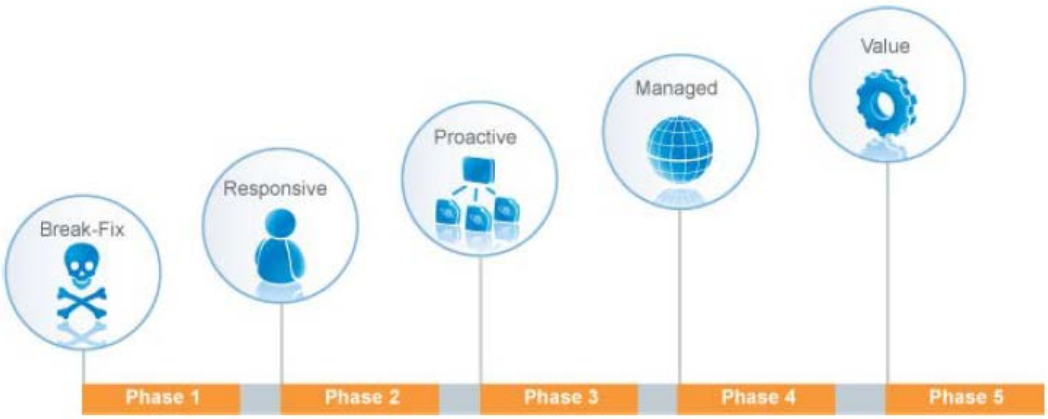
bieden om de relaties met de klanten te verbeteren. De klant hoeft niet meer te bellen in stressvolle situaties. De MSP heeft de ICT onder controle en de klant weet waar hij aan toe is en weet dat hij kan rekenen op de MSP als het fout gaat.

Voordelen voor klanten zijn onder andere het zorgeloos gebruik maken van de ICT omgeving en voor een vast bedrag per maand verzekerd zijn van goed en zorgvuldig onderhoud op de ICT omgeving. Bij het gebruik van een dergelijk 'fixed price' model is niet alleen de MSP verzekerd van vaste inkomsten, ook de klant weet waar hij/zij aan toe is en komt niet voor verrassingen te staan. Bovendien zal de klant zich geen zorgen meer hoeven maken over de ICT. De klant heeft een SLA afgesloten met de MSP en kan er op vertrouwen dat zijn ICT in goede handen is bij de MSP op het moment er iets fout dreigt te gaan. De klant zal minder in aanraking komen met problemen omdat deze door de MSP tijdig worden opgemerkt en worden verholpen. Mocht de klant in aanraking komen met een probleem dan zal dit zijn omdat de MSP de klant hiervan op de hoogte stelt, niet andersom.

Door deze gestructureerde manier van werken wordt het voor een MSP weer mogelijk tijd te steken in innovatie. Dit wordt bovendien mogelijk gemaakt door de waardevolle informatie welke de MSP kan verzamelen uit het gedrag van de systemen bij de klanten. Zo kan de MSP focussen op innovatie gericht op knelpunten en dit vervolgens voor alle klanten toepassen om problemen in de toekomst bij alle klanten weg te nemen. Een proactief model zal dus ook gaan bijdragen aan een algehele verbetering van de dienstverlening.

2.2. Vormen van proactief beheer/MSP Maturity Model

Om MSP's inzicht te geven in hun voortgang naar proactief beheer is een speciaal MSP Maturity Model ontwikkeld (N-ables MSP Maturity Model, 2006). Dit model is gebaseerd op best practices uit de MSP wereld en is mede ontwikkeld door N-able Technologies, fabrikant van MSP software. N-able heeft een hele tak van het bedrijf gewijd aan het ondersteunen van MSP's in het traject naar proactief beheer. Niet alleen bij het implementeren van de software, maar ook alle ondersteunende processen zoals het opstellen van geschikte werkprocedures en de verkoop van de nieuwe services aan klanten. N-able is hier de afgelopen jaren erg vooruitstrevend in geweest. Men ziet nu dat andere fabrikanten dit voorbeeld volgen en soortgelijke diensten aanbieden bij de aankoop van een MSP product. Dit model geeft een MSP een duidelijk beeld van waar hij op dit moment staat en hoe volwassen de dienstverlening van de MSP op dit moment is. Bovendien geef het model in groter detail weer wat voor vormen proactief beheer er zijn.



Figuur 1: MSP Maturity Model (N-able Technologies)

Bovenstaande figuur geeft het MSP volwassenheidsmodel weer. Zowel de service providers als haar klanten zullen de genoemde fases moeten doorlopen op de weg naar proactief beheer. (IT Service Delivery: From Basic Automation through to Managed Services, 2008). Zoals te zien is, gaat het model nog een aantal stappen verder dan alleen proactief. Maar in veel gevallen is voor service providers proactief een eerste streven, omdat in de proactieve fase de eerste problemen, als in de inleiding van hoofdstuk 2 besproken, weg worden genomen.

2.2.1. Fase 1: Break-Fix

Klanten in deze categorie hebben de minst ontwikkelde ICT omgevingen. Alle werkzaamheden betreffende de ICT zijn Ad-hoc en niet gedocumenteerd. Deze klanten vertrouwen op een automatiseerder om hun problemen op te lossen, maar hebben hiervoor geen SLA's of andere contracten. De automatiseerder moet dus maar net tijd vrij hebben. Deze klanten worden gefactureerd voor het aantal uren arbeid dat de automatiseerder heeft besteedt. De klant kan moeilijk inschattingen maken over hoeveel de ICT hem nou werkelijk kost.

De problemen worden door de klant zelf waargenomen en doorgegeven aan de automatiseerder. Het is moeilijk deze klanten goede service te verlenen. De klant belt immers zelf als het probleem al schade heeft aangericht. De automatiseerder kan het probleem dan wel hebben opgelost, maar in de ogen van de klant had het probleem helemaal niet mogen voorkomen. De automatiseerder kan hier echter niet veel aan doen. Een automatiseerder met een grote hoeveelheid klanten zal aan deze fase een behoorlijk chaotische werkwijze overhouden en is voor zijn inkomsten geheel afhankelijk van het aantal problemen dat bij de klant optreed.

2.2.2. Fase 2: Responsive

Deze fase heeft veel overeenkomsten met de break-fix fase. Verschillen zijn te vinden in het feit dat de automatiseerder de IT systemen voor de klant heeft gedocumenteerd en in uitzonderlijke gevallen een beperkte monitoring beschikbaar heeft. Dit zal in de meeste gevallen beperkt zijn tot simpele controles of servers niet uitstaan en wel bereikbaar zijn. De automatiseerder kan het probleem misschien wel zien aankomen of op het moment zelf zien gebeuren, maar zal niet ingrijpen omdat hiervoor geen contract is opgesteld. De automatiseerder is op de hoogte en zal misschien de klant inlichten, maar zal wachten met de reparatie totdat er toestemming is van de klant. 100% van de tijd wordt dus nog steeds besteed aan het ad-hoc oplossen van problemen.

2.2.3. Fase 3: Proactive

Het grote verschil met de twee bovengenoemde fases is dat preventief onderhoud een belangrijke en serieuze activiteit is van de automatiseerder, welke vanaf nu Managed Service Provider (MSP) mag worden genoemd. Omdat de focus hier meer ligt op het preventief onderhoud en het voortijdig ontdekken van problemen, kunnen MSP's de gevolgen van fouten zoveel mogelijk inperken. Bovendien hebben MSP's via de remote monitoring & management (RMM) software de mogelijkheid gegevens betreffende capaciteit en beschikbaarheid te verzamelen, welke het mogelijk maken een Service Level Agreement (SLA) af te sluiten met de klant. Standaard onderhoudstaken zullen worden geautomatiseerd en kleine problemen kunnen door het systeem of door een simpele ingreep van een beheerder worden opgelost. In dit model zal nog maar 50-70% van de tijd worden besteed aan het ad-hoc oplossen van problemen.

2.2.4. Fase 4: Managed

Dit is het eerste niveau in het model waar de klant bewust is van het belang dat zijn bedrijf heeft bij een goede ICT omgeving. In deze fase wordt er niet meer gemanaged op systeemcomponenten. Klanten zijn meer geïnteresseerd in performance, capaciteit en continuïteit, dan in routers en switches. In deze fase ligt het belang dus bij de **waarde** van de systemen en de waarde van de geleverde service. Klanten betalen een vaste prijs per maand en verwachten hiervoor dat de ICT-systemen werken, goed onderhouden worden en problemen automatisch worden opgepakt door de MSP. De klant heeft het onderhoud van de ICT omgeving uitbesteed aan de MSP, hiervoor zijn contracten opgesteld waarin de serviceverlening staat beschreven. De klant wil geen zorgen meer over de omgeving en wil weten waar hij aan toe is.

2.2.5. Fase 5: Value

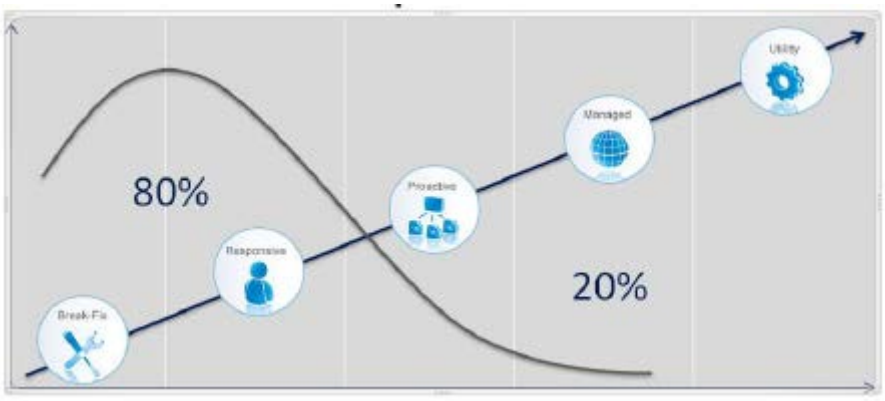
Deze laatste fase gaat nog een stap verder dan de Managed fase, in die zin dat de ICT geleverd door de MSP uitgebreid wordt meegenomen in bedrijfsbesluiten van de klant en dat de MSP 'self-supporting' wordt voor de klant. Dat wil zeggen flexibel en zorgeloos ICT afgeeft aan de klant op het moment dat dit nodig is en de klant daarvoor ook in rekening brengt. Dit zijn als het ware 'all you can eat' oplossingen en moeten kunnen meegroeien met de vraag van de klant. Dit idee is te vergelijken met het afnemen van energie. "De ICT moet uit de muur komen" en er wordt betaald voor wat wordt gebruikt. In de praktijk zullen vrijwel alle MSP's niet in staat zijn een dergelijke dienst aan te bieden, echter zijn dit wel serieuze plannen voor de toekomst.

2.3. Moeilijkheden

Onderzoeken wijzen uit dat veranderen van een 'break-fix' model naar een Managed model niet gemakkelijk is en een behoorlijke inspanning van de automatiseerder vereist (The Seven Major Obstacles on the Road to Managed Services, 2007). Deze stap naar MSP is meer dan alleen de implementatie van een tool. Daarnaast moet een automatiseerder veranderen van werk- en denkwijze. Bovendien zullen marketing en sales ook anders moeten omgaan met de verandering. Het in de markt zetten en het verkopen van een MSP service vraagt een totaal andere aanpak dan deze afdelingen gewend waren met de traditionele producten en diensten.

De reden dat er achteraf nog wel eens moeilijkheden zijn, komt omdat MSP's hun bedrijf moeten veranderen. Om succesvol de overstap naar MSP te maken, moet er genoeg 'commitment' vanuit het bedrijf zijn. (The Fundamentals of a Successful Managed Services Practice, 2007; Kaseya®Managed Services Edition, 2009)

Een ander punt wat deze overgang extra moeilijk maakt, is dat niet alleen de MSP de fases van het Maturity Model moet doorlopen, maar ook de klanten. Een MSP kan geen managed of proactieve services verkopen aan een break-fix klant. De belangen botsen dan teveel. Een klant vindt het niet prettig als hij ineens moet betalen voor dure SLA's waarvan hem het nut niet direct duidelijk is. Het werkt nu toch ook? Het is voor veel MSP's moeilijk deze klanten met dezelfde snelheid mee te laten ontwikkelen in dit model. Klanten moeten goed ingelicht worden over de voordelen en de belangen van een goed gemanagede IT omgeving voor hun bedrijfscontinuïteit. Dit proces is extreem moeilijk en MSP's moeten hier voldoende aandacht aan besteden om succesvol te zijn in het verkopen van deze 'fixed-price' services.



Figuur 2: Verspreiding van MSP Klanten over het model (N-able Technologies, 2007)

Bovenstaande figuur geeft weer waar het grootste deel van de klanten van MSP's zich bevinden. 80% van deze klanten bevinden zich nog in het 'break-fix' en responsive gebied (Going beyond RMM, 2011). Het heeft voor de MSP daarom geen nut om zich volledig te focussen op proactieve en managed klanten. MSP's moeten zich bewust zijn van deze verdeling en moeten deze "achterblijvende" klanten ook oplossingen kunnen aanbieden en motiveren om verder te groeien naar proactief, wat veel voordelen heeft voor zowel de klant als de MSP.

Wat vaak mis gaat is dat MSP's teveel focussen op proactieve klanten en hiervoor één product samenstellen en verkopen. (The Fundamentals of a Successful Managed Services Practice, 2007) Het is beter om een aantal managed producten samen te stellen met bijvoorbeeld een instapmodel of voor ieder niveau van het model een apart product verkopen. Dit soort constructies geven een reactieve klant de mogelijkheid gebruik te maken van de voordelen van MSP, wat vervolgens het laten doorgroeien van een klant naar proactief makkelijker kan maken zodat klanten het belang en de voordelen zelf gaan inzien.

Het gevaar van een goed werkende omgeving is dat klanten niet meer doorhebben waarvoor wordt betaald. De klant heeft immers geen weet van de problemen, omdat deze automatisch door de MSP worden opgepakt en de klant niet meer hoeft te bellen, zoals eerder het geval was. Er komt maandelijks een factuur binnen, maar er wordt niet of nauwelijks inzichtelijk gemaakt wat er allemaal voor de klant gedaan is. Het is belangrijk dat MSP's uitgebreid rapporteren naar de klant en inzichtelijk maken wat er de afgelopen periode allemaal voor de klant gedaan is. (From Promises to Proof: How To Demonstrate Value to Your Customers, 2006)

Overige problemen kunnen zijn:

- Niet volledig benutten van de MSP software.
  Door het niet volledig benutten van de software maakt de MSP het zichzelf onnodig nuttig en zal niet de maximale efficiëntie behalen.
- Waarde van de service niet duidelijk krijgen naar de klant.
  Als de waarde van de service niet duidelijk wordt gemaakt naar de klant, kan de klant zichzelf gaan afvragen waarvoor hij iedere maand betaald en de band met de MSP kwijtraken en op zoek gaan naar een andere MSP die het goedkoper aanbiedt, maar waarschijnlijk minder service levert.
- Teveel gericht op techniek i.p.v. de ‘pijnpunten’ van de klant aanpakken.
  Klanten hebben niets aan de techniek. Klanten hebben baat bij een service die hun problemen zonder al te veel zorgen kan verminderen of wegnemen
- Flexibiliteit verliezen.
  Het is belangrijk passende service te verkopen aan de verschillende klanten. Uit onderzoek blijkt dat één model voor alle klanten geen oplossing is en voor veel stroefheid binnen de organisatie zorgt (Walsh, 2011).

3. Productonderzoek

Het bovengenoemde MSP model is niet te realiseren zonder ondersteunende software pakketten. De MSP zal tools beschikbaar moeten hebben om de systemen van de klant te kunnen monitoren, anders wordt het voor een MSP onmogelijk deze proactieve werkwijze te bereiken. Daarom is als onderdeel van dit onderzoek ook aandacht besteed aan ondersteunende MSP software en de mogelijkheden die deze software voor een MSP kan bieden. Dit hoofdstuk zal niet alleen een overzicht geven van de functionaliteiten van de verschillende software, maar zal ook een aanvulling geven op de voorgaande hoofdstukken betreffende de mogelijkheden van proactief beheer met dergelijke software pakketten. Zoals gebleken uit het eerdere hoofdstuk is proactief beheer veel meer dan alleen een goede tool inzetten. Daarom is het belangrijk dat beide kanten van het verhaal worden bekeken.

Na een snelle inventarisatie zijn er 3 vooraanstaande producten naast elkaar gezet welke in de volgende paragrafen worden beschreven. Deze producten zijn N-central, Kaseya en GFI MAX RemoteManagement. Hieronder wordt in respectievelijk de paragrafen 3.1 tot en met 3.3 een indruk van de pakketten gegeven en wordt beschreven wat de mogelijkheden voor een MSP zijn.

3.1. N-Central

Het eerste onderzochte pakket is N-central van N-able. N-central is een geavanceerd vooruitstrevend product uit Canada, speciaal ontwikkeld om ondersteuning te bieden aan MSP's die een proactieve werkwijze willen hanteren. (N-able Technologies; Going beyond RMM, 2011; Doing More with Less: Automating IT Services in Your Midsize Business, 2009)

3.1.1. Omgeving

N-able biedt twee oplossingen voor MSP's voor het gebruik van het product. Het product kan worden afgenomen als een Cloud oplossing of een on-premise oplossing. De Cloud oplossing brengt zowel de voor- en nadelen van Cloud applicaties met zich mee. Zo is de beschikbaarheid van de Cloud versie erg hoog en zullen beheer aan het pakket en updates door N-able worden verzorgd. Nadelen van deze oplossing zijn bijvoorbeeld: geen mogelijkheid tot maatwerk en een moeilijke integratie met andere software. Bovendien geeft N-able aan dat er in de Cloud oplossing een aantal functies ontbreken en er maar een beperkte vorm van beheer mogelijk is. De on-premise oplossing is een traditionele server op locatie van de MSP, met daarop een versie van N-central. Dit kan zowel een fysieke als virtuele server zijn. Aangeraden wordt N-central niet als Hyper-V guest in te zetten vanwege de beperkte I/O van Linux systemen onder Microsofts Hyper-V. De on-premise oplossing biedt ook weer voor- en nadelen. Zo moet er bijvoorbeeld overwogen worden hoe de beschikbaarheid moet worden gerealiseerd. Aan de andere kant is er wel een mogelijkheid tot maatwerk, wat onderscheidend kan werken.

3.1.2. Functies

'Single Pane of Glass'

N-central biedt een nette duidelijke interface met een Dashboard waarin problemen of waarschuwingen bij klanten overzichtelijk worden weergegeven. Dit is een volledige web-based management console. Er zijn dus geen extra client installaties nodig, alleen een browser. Daarnaast slaat de term 'single pane of glass' ook op het feit dat alle werkzaamheden uitgevoerd worden vanuit hetzelfde pakket. N-central heeft integratiemogelijkheden voor een groot aantal andere pakketten. Dit kunnen modules van N-able zijn als bijvoorbeeld de back-up module en de audit manager, maar ook complete PSA systemen als Autotask.

Remote control

N-central maakt het mogelijk vanuit het dashboard direct remote support te bieden. Hiervoor is geen extra configuratie vereist. Remote support kan worden opgezet middels 3 technieken. UDP Hole punching, een SSH tunnel (waarover een RDP of VNC gaat) (voor het geval de UDP connectie niet mogelijk is) en als laatste mogelijkheid een HTTPS verbinding, ook i.c.m. RDP of VNC. De combinaties van technieken maakt het mogelijk remote support te bieden zonder dat hier extra netwerk of firewall configuratie voor nodig is. Hierdoor is een monteur altijd in staat remote support te bieden, vanaf welke locatie dan ook. De 'unattended remote control' oplossing maakt het mogelijk alle acties op de achtergrond uit te voeren zonder dat de eindgebruikers van hun werk gehouden worden.

Garantie controle

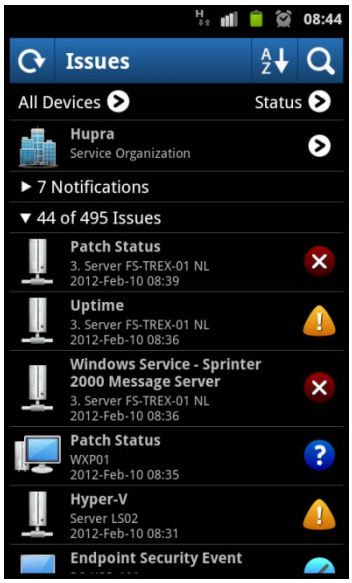
Door middel van de 'asset control' functie in N-central is het mogelijk alle informatie betreffende hardware, software, licenties, enz. binnen een netwerk te verzamelen. Deze informatie kan erg waardevol zijn bij het oplossen van problemen en kan zelfs als dit nodig is, worden meegestuurd met het ticket naar de monteur. N-central kan op basis van deze informatie ook waarschuwingen weergeven op het Dashboard als bijvoorbeeld licenties of garantieperiodes van hardware binnen korte tijd dreigen te verlopen. Hiervan kunnen vervolgens rapporten en overzichten worden gemaakt die aan de klant kunnen worden voorgelegd.

Self-healing

N-central's self-healing functionaliteit maakt het mogelijk veel voorkomende beheerstaken en foutmeldingen automatisch via een script op te lossen. Deze scripts kunnen bijvoorbeeld ingezet worden om een schijfopruiming te starten op het moment dat een schijf te vol is, of bijvoorbeeld een service te starten/herstarten op een server als deze problemen vertoond. Een aantal van deze scripts worden met N-central meegeleverd, maar men kan ook besluiten deze scripts zelf te 'schrijven' via de Automation Manager of m.b.v. traditionele batch of Visual Basic scripting. De Automation Manager geeft de scripts visueel weer en maakt het script inzichtelijk voor de beheerder. Het maken en aanpassen van scripts wordt hierdoor makkelijker gemaakt.

Mobiele toegang

N-central wordt geleverd met een aantal mobiele applicaties voor zowel Android als iOS. Deze applicaties verschaffen toegang tot een mobiele interface voor N-central. Dit maakt het mogelijk voor beheerders/monteurs om meldingen en informatie uit N-central te ontvangen, ook als deze niet op kantoor zijn.



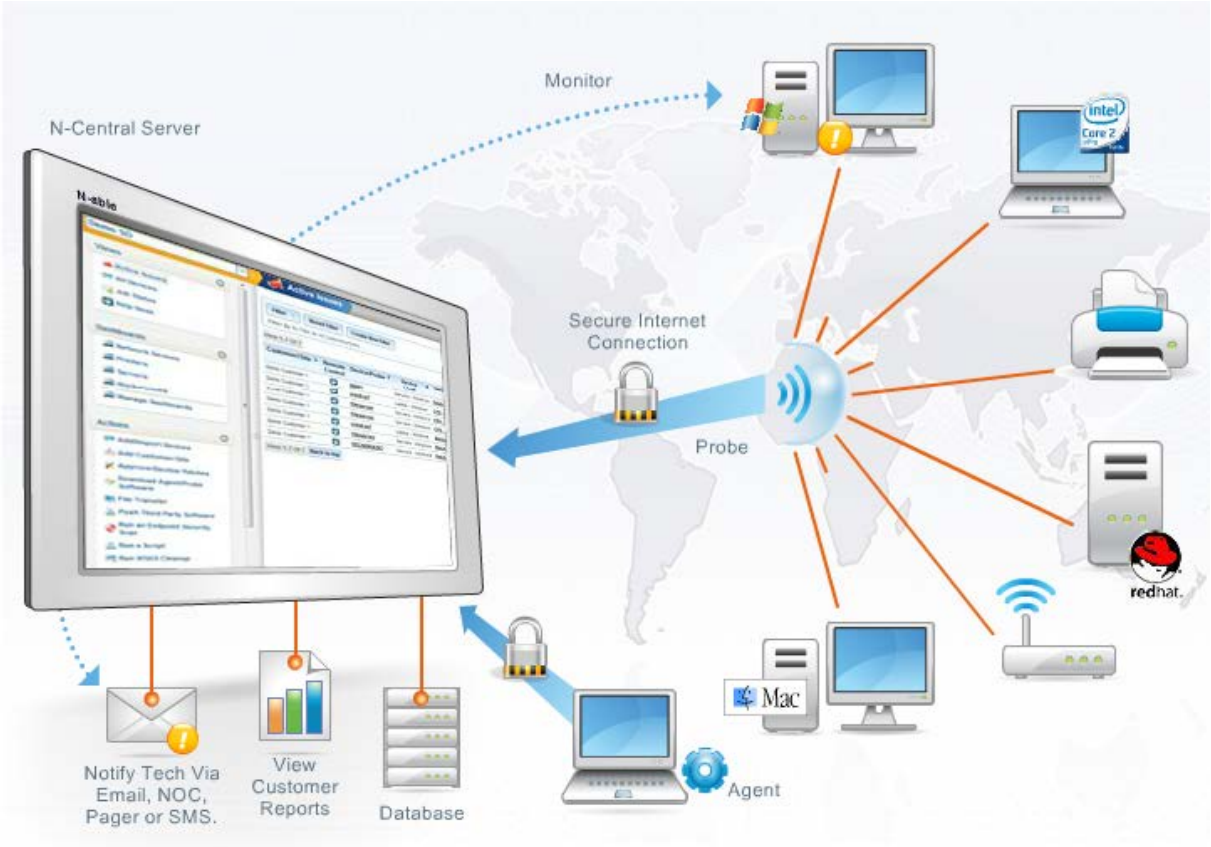
Figuur 3: N-central mobile interface

"VMware Ready" certificatie

N-central is een van de weinige software pakketten om een “VMware Ready” certificatie te behalen. In samenwerking met VMware zijn een groot aantal diepgaande tests uitgevoerd om met zekerheid te kunnen garanderen dat de twee producten ‘compatible’ met elkaar zijn. Dit geeft N-central de mogelijkheid verschillende, kritische hardware aspecten van VMware ESX en ESXi te monitoren, bijvoorbeeld: power supply, fans, RAID-hardware en hardware prestaties. Dit geeft beheerders de mogelijkheid om ook de hardware problemen in een virtuele omgeving aan te zien komen en hier vooraf op te kunnen anticiperen.

Eenvoudig monitoren van alle werkstations, servers en netwerk apparaten

De architectuur van N-central is dusdanig opgebouwd dat het met een paar acties mogelijk is een complete netwerk te monitoren. Er worden een of meerdere probes binnen het netwerk geplaatst die het netwerk zullen scannen op apparatuur. Vervolgens wordt deze apparatuur direct toegevoegd aan de N-central server. Daarna kunnen op de apparaten, die dit ondersteunen, agents worden uitgerold. Dit kan via policies, via de N-central probe, of handmatig. Al het verkeer vanaf de probes en agents zal uitgaand zijn, daarom is verdere netwerk/firewall configuratie met publieke adressen niet nodig. Beheerders kunnen ten alle tijden via een beveiligde verbinding contact maken met de apparatuur.



Figuur 4: N-central Architecture Overview

Patch Management

N-central heeft de mogelijkheid Windows werkstations en Servers met een agent te monitoren op geïnstalleerde patches en mogelijk nieuwe beschikbare patches. Er kan dan voor worden gekozen om in extreme gevallen deze informatie op het Dashboard te laten zien of een beheerder/monteur in te lichten. In combinatie met de self-healing functie kan ook eerst worden geprobeerd automatisch de goedgekeurde patches door te voeren. Patch management van N-central is volledig te integreren met en WSUS server van Microsoft. Dit kan een WSUS server van de MSP of op locatie bij de klant zijn. Patch Management maakt het mogelijk vanuit de N-central interface patches goed te keuren of te verwijderen. Hierdoor is management van de WSUS server niet meer nodig, dit wordt volledig geïntrigeerd in N-central.

PSA integratie

N-central is gemakkelijk te koppelen met verschillende PSA systemen. Bijvoorbeeld: ConnectWise, TigerPaw en Autotask. Deze koppeling maakt het mogelijk voor N-central een issue te escaleren, mocht deze niet opgemerkt worden en direct een ticket aan te maken in het ticketsysteem. De integratie van de twee systemen maakt het ook mogelijk het ticket te voorzien van uitgebreide informatie betreffende het falende systeem. Zo heeft een beheerder direct de benodigde informatie beschikbaar. Na het oppakken van het ticket zal N-central de status van het probleem updaten naar “acknowledged” en bij het sluiten van het ticket zal ook de bijbehorende melding worden gesloten.

Software Deployment
N-central maakt het mogelijk third-party software gemakkelijk en geautomatiseerd uit te rollen. Dit kan zowel ad-hoc als gepland. N-central biedt hierbij uitgebreide functies voor het controleren of de uitrol daadwerkelijk succesvol was en op welke systemen er problemen zijn opgetreden. Deze gegevens kunnen worden weergegeven op het Dashboard of kunnen direct worden gemeld aan de verantwoordelijke, afhankelijk van de opgegeven instelling bij de uitrol.

Managed Anti-virus
N-central heeft een geïntegreerde anti-virus/malware oplossing genaamd Endpoint Security. Dit is een samenwerking van N-able en Panda Security. De Endpoint security beschermd het gehele systeem en kan ingezet worden op zowel servers als werkstations. De updates van de virus definities worden aangestuurd en gecontroleerd vanuit N-central. Bij problemen kan er meteen een melding worden weergegeven. Door de integratie met N-central wordt het ook mogelijk de virus scans geautomatiseerd uit te voeren.

3.1.3. Mogelijke Uitbreidingen
N-able biedt een aantal uitbreidingen voor het standaard pakket N-central. Deze uitbreidingen voegen extra functies aan het standaard pakket toe. Deze modules integreren naadloos met N-central en worden volledig aangestuurd vanuit de interface van N-central.

Audit Manager
De audit manager module maakt het mogelijk op afstand audits en vulnerability scans uit te voeren op het netwerk en hier vervolgens rapporten van te maken voor presentatie aan de klant. Deze functie kan handig worden ingezet bij een maandelijkse controle van de netwerken, maar ook bij de inventarisatie van het netwerk van een nieuwe klant.

Security Manager
De security manager module biedt een gemanagede beveiligingsapplicatie voor werkstations en servers voorzien van het Microsoft Windows besturingssysteem. De security manager wordt naadloos geïntegreerd in N-central en problemen worden direct gemeld via het Dashboard of doorgestuurd naar de beheerders. De machines worden op deze manier voorzien van antivirus beveiliging, anti-spam en anti-malware.

NetFlow Manager
NetFlow manager maakt het verkeer binnen een netwerk inzichtelijk. Dit geeft de beheerders de mogelijkheid capaciteitsmanagement toe te passen en enige vorm van capaciteitsplanning te voeren. Zo kunnen problemen met netwerk/hardware resources tijdig worden opgemerkt en kunnen mogelijk upgrades van netwerk/hardware eenvoudig worden gepland en verantwoord.

Back-up Manager

De back-up manager maakt een integratie van N-central met een vooraanstaand back-up pakket van CA mogelijk. N-central kan gebruik maken van de back-up oplossingen van CA zoals bijvoorbeeld ARCserve Backup/ARCserve D2D en een aantal oplossingen voor back-up in de Cloud. Deze integratie met back-up software maakt het niet alleen mogelijk om te controleren of een back-up succesvol is uitgevoerd, maar heeft ook de mogelijkheid te controleren of deze back-up ook daadwerkelijk gerestored kan worden. Het gebruik van deze module neemt de verantwoordelijkheid van de gebruiker weg. De gebruiker hoeft zich niet meer druk te maken over het controleren van back-ups en het wisselen van de tape.

N-compass (Report Manager)

N-compass stelt de MSP in staat uitgebreide rapporten te maken van werkzaamheden, performance, up-time, enz. De MSP kan deze rapporten vervolgens gebruiken om de factuur aan de klant te onderbouwen. Het verschil met de standaard reporting van N-central is dat N-compass de mogelijkheid heeft gegevens veel langer vast te houden en zo uitgebreidere rapporten kan produceren. Daarnaast kunnen de rapportages geheel naar eigen wens en stijl worden aangepast.

Policy Manager

De policiy manager maakt het mogelijk om Group policy beheer in N-central te integreren. Op deze manier kan het uitvoeren en de naleving van policies worden beheerd en gecontroleerd met de benodigde meldingen in N-central als er problemen optreden. In combinatie met de self-healing functie kunnen problemen in een van de modules middels een script weer automatisch worden opgelost.

N-SupportPro

N-SupportPro maakt het mogelijk een uitgebreide vorm van remote support, op afstand, aan de klanten te bieden, zonder dat hiervoor extra configuratie bij de klant nodig is.

3.1.4. Bijzonderheden

Hieronder volgen een aantal bijzonderheden aan N-central.

Trainingen

Bij aanschaf van het product N-central krijgt de MSP o.a. toegang tot het N-able resource center. Dit is een bron van informatie waar White papers te vinden zijn over uiteenlopende N-able onderwerpen, zowel technisch, sales, als bedrijfskundig. Verder zijn hier online trainingen te vinden en uitgebreide producthandleidingen. Men krijgt bovendien toegang tot community forums en uitgebreide support van N-able.

Licenties

N-able hanteert een opmerkelijke licentie structuur voor haar producten. Zo is er voor N-central geen minimale afname voor licenties en wordt de MSP de mogelijkheid geboden hun klanten te voorzien van een goedkope/gratis Essentials licentie (met beperkte mogelijkheden) of een Professional licentie. Het doel van deze Essentials licentie is de MSP klanten kennis te laten maken met het systeem tegen lage kosten of zelfs gratis. Vanuit die positie kan de MSP de klant van het nut overtuigen en in de toekomst een Professional licentie aan de klant verkopen.

Integratie modules/externe programma's

De naadloze integratie van de modules en de externe programma's maken N-central tot een geavanceerd pakket wat gemakkelijk te beheren valt door het 'single pane of glass' principe.

Blueprint Program

N-able biedt een speciaal programma voor MSP's genaamd 'the blueprint for succes'. Dit is uniek op deze markt. N-able probeert hiermee MSP's te begeleiden bij het in productie nemen van hun product en de MSP te ondersteunen in het verkopen van deze services aan de klant. N-able biedt de MSP als het ware een strategie voor het in de markt brengen van het product en de services op een manier waarmee zo veel mogelijk winst kan worden behaald.

Branding

N-able stelt de MSP in staat software, waaronder N-central, volledig aan de passen aan de huisstijl van de MSP. Dit kan een handige functionaliteit zijn als bijvoorbeeld wordt besloten de klanten van de MSP beperkte toegang te geven tot het systeem.

3.1.5. Requirements

Hardware Configuration

N-able geeft de volgende hardware specificaties voor N-central vrij. Deze specificaties zijn ingedeeld op het totaal aantal te monitoren devices. Dit zijn advies specificaties waarmee N-able een minimale prestatie van N-central kan garanderen.

Up to 3,500 Devices	Up to 7,000 Devices	Up to 10,500 Devices
one Xeon processor	one Xeon processor	two Xeon processors
8 GB RAM	16 GB RAM	24 GB RAM
146 GB HDD**	300+ GB HDD**	500+ GB HDD**

Tabel 1: N-able Hardware Requirements

Virtuele hardware

N-central is ook virtueel in te zetten, wel moet er dan rekening mee worden gehouden dat er wordt voldaan aan de vastgestelde minimum guest requirements. N-able biedt support voor zowel VMware als Hyper-V omgevingen, hoewel deze Hyper-V support in de requirements van versie 8.0 en 8.1 weer ingetrokken lijkt te zijn. N-able vermeld namelijk het volgende bij de nieuwe versie:

> *"Due to the limited Disk I/O performance of Linux-based Guests in Hyper-V, N-able Technologies does not recommend or support running N-central as a Hyper-V Guest. While N-central can be successfully installed as a Hyper-V Guest, this should only be carried out for non-production N-central servers and only if no other virtualization environments or physical resources are available."*

In de laatste versie van N-central, 8.1.1 (SP1) lijkt de Hyper-V support weer terug te zijn, daar wordt Windows Server 2008 R2 Hyper-V weer vermeld bij de supported environments.

N-central Guest Configuration (minimum)

Guest Type	Typical
Guest Operating System	Linux
Version	RedHat Enterprise Linux 5 (64 bit)
Number of Virtual Processors	2 minimum
Memory	6,144MB (6 GB) minimum
Network	1 network interface card required
Virtual Disk Capacity	140 GB minimum

3.1.6. Licenties

N-able hanteert twee licentie modellen voor uitrol op de agents en probes bij MSP klanten. Dit zijn een Essential Licentie en een Professional licentie. De Essential licentie is voor MSP's gratis en MSP's kunnen deze licentie daarom gratis of tegen een lage vergoeding aan de klant aanbieden. Een nadeel van deze Essential licenties is de beperkte 'feature set' welke in de onderstaande tabel is weergegeven. Een van de voordelen van deze Essential licentie is dat een MSP een klant gratis kan laten kennis maken met het systeem. Als de klant hier eenmaal de voordelen van inziet kan deze Essential licentie zonder problemen naar een uitgebreidere Professional licentie worden overgezet.

Deze professional licentie is eigenlijk gewenst omdat deze niet beperkt is in functionaliteit, echter kost deze licentie de MSP een vast bedrag per maand. De MSP zal voor deze licentie daarom ook meer kosten in rekening moeten brengen.

Tabel 2: N-central licenties

	Essential Mode	Professional Mode
Remote Control		
Terminal Services, Web, VNC	✔	✔
Remote Support Manager, SSH		✔
Asset Discovery	✔	✔
Monitoring	Basic	Advanced
Scanning Interval	Less Frequent	More Frequent
Agent Status, Connectivity	✔	✔
CPU, Disk, Memory	✔	✔
TCP Services Monitoring	Generic, DNS & SMTP only	Full
Windows Security Center	✔	✔
Event Log		✔
Patch Management		✔
SNMP (Network Equip., Servers, Other O/S)		✔
Windows Services		✔
Advanced Asset Management		✔
Printers	✔	✔
Self Healing		✔
Alerts & Notifications	✔	✔
Reporting	Limited	Full
Management Tasks (Scripting, Software Distribution)		✔
Windows 7 support	✔	✔

De kosten van N-central, zonder uitbreidingen, zijn in de onderstaande tabel weergegeven. Deze kosten bestaan uit een eenmalige investering voor zowel de aanschaf van de software, als de aanschaf van de licenties. Terugkomende kosten zijn kosten op onderhoud en support per licentie. N-able maakt onderscheid tussen verschillende doeleinden van een licentie. Zo zijn er bijvoorbeeld verschillende prijzen voor een licentie op een server, een netwerk probe, en een werkstation. Een voorbeeld is gegeven in de onderstaande tabel. Er is uitgegaan van 100 servers, 250 desktops, 50 network probes en 100 Essentials licenties.

Tabel 3: Kosten N-central

	Eenmalig (eerste jaar)	Terugkomend na eerste jaar (per jaar)	Totaal (na 24 maanden)
Server	€ 220,80 x 100 = € 22.080,-	€ 44,16 x 100 = € 4.416,-	€ 22.080,- + € 4.416,- = € 26.496,-
Desktop	€ 46,- x 250 = € 11.500,-	€ 9,20 x 250 = € 2.300,-	€ 11.500,- + € 2.300,- = € 13.800,-
Network	€ 110,40 x 50 = € 5.500,-	€ 22,08 x 50 = € 1.104,-	€ 5.500,- + € 1.104,- = € 6.604,-
Essentials	€ 15,- x 100 = € 1.500,-*	€ 3,00 x 100 = € 300,-	€ 1.500,- + € 300,- = € 1.800,-
	€ 40.580,-	€ 8.120,-	€ 48.700,-

*De reguliere prijs voor Essentials licenties. N-able heeft vaak acties en aanbiedingen waarin deze Licenties gratis zijn

Door de hantering van de verschillende type licenties is het moeilijk een daadwerkelijke inschatting te maken van de kosten. Dit is pas mogelijk als duidelijk in kaart is gebracht welke licenties precies nodig zijn.

3.2. Kaseya

N-able en Kaseya zijn op dit moment de twee grootste spelers op de MSP software markt en zijn behoorlijk aan elkaar gewaagd. Zo vertoont Kaseya erg veel overeenkomsten met N-central en vice versa. Beide pakketten bieden ongeveer dezelfde functies aan, soms zelfs onder dezelfde naam. Het echte verschil tussen deze twee pakketten moet worden gezocht in de invulling van deze functies en de extra's die bij het pakket worden geboden.

3.2.1. Omgeving

Net als bij N-central wordt de mogelijkheid geboden gebruik te maken van een on-premise of een Cloud oplossing. De Cloud oplossing van Kaseya draagt de naam Kaseya IT Center. Ook hier is een duidelijk verschil tussen deze oplossingen merkbaar. De Could oplossing van Kaseya heeft aanzienlijk minder functies dan de on-premise oplossing. Zelfs een aantal van de basis functies, welke wel beschikbaar zijn in de on-premise oplossing, ontbreken in de Cloud. (Automating IT Systems Management, 2010; Kaseya; Kaseya® Professional Services, 2009)

3.2.2. Functies

Interface

Kaseya hanteert net als N-central een 'single pane of glass' principe. Alle werkzaamheden zijn uit te voeren uit één overzichtelijke interface waaronder alle componenten en uitbreidingen te vinden zijn. Het is niet nodig management software te installeren, net als N-central maakt Kaseya gebruik van een web interface, het enige benodigde is een werkende browser.

Info Center

Het info Center voorziet de beheerders van de mogelijkheid geavanceerde rapporten te maken van de huidige omgevingen. Deze rapporten kunnen vervolgens aan de klanten worden getoond om een overzicht van hun omgeving weer te geven. Daarnaast is het Info Center uitgerust met een Dashboard waarop actieve issues en server statussen worden weergegeven.

Live Connect

Live Connect is een module voor beheer op afstand. Net als bij de N-central versie is het mogelijk zowel servers als werkstations op afstand te beheren, zonder dat gebruikers hierbij van hun werk worden gehouden. Configuratie van firewalls en netwerk is niet nodig vanwege de actieve verbindingen met de Kaseya agent.

Audit & Inventory

Maakt het mogelijk snel en eenvoudig een inventarisatie van software en hardware te maken en hier audits op uit te voeren. Bijvoorbeeld het controleren van een netwerk op mogelijke kwetsbaarheden.

Patch Management

Net als N-central heeft Kaseya de mogelijkheid om via de geïnstalleerde agent informatie van een server of werkstation te verzamelen en te controleren welke patches zijn doorgevoerd en of er mogelijk nog nieuwe patches beschikbaar zijn. Vervolgens wordt de mogelijkheid geboden deze patches via Kaseya te installeren.

Desktop Policy Management

Kaseya's Desktop Policy Management maakt het mogelijk group policies te beheren vanuit de Kaseya interface. Bovendien kan gemonitord worden af deze policies ook daadwerkelijk worden nageleefd op de systemen.

Desktop Migratie

Desktop Migratie maakt het mogelijk een back-up te maken en gebruikersinstellingen te verzamelen. Deze kunnen vervolgens gekopieerd worden naar een andere computer. Dit maakt het mogelijk bij ernstige problemen een gebruiker makkelijk te verhuizen naar een ander werkstation en de instellingen te behouden, ook als er geen Active Directory met roaming profiles aanwezig is.

Network Discovery

Kaseya maakt het mogelijk, door middel van agents, individuele servers en werkstations te monitoren. Het verkeer van deze agents naar de Kaseya server zal verlopen via beveiligde verbindingen op basis van het HTTPS protocol en er is geen verdere configuratie van firewalls of netwerk benodigd. Deze agents dienen op de server of het werkstation te worden geïnstalleerd. Naast deze mogelijkheid biedt Kaseya ook nog een network monitor. Deze "probe" maakt het mogelijk op basis van SNMP uiteenlopende netwerk apparatuur te ontdekken en te monitoren.

Agent Procedures
De functie agent procedures maakt het mogelijk scripts uit te voeren via de Kaseya interface. Deze functie is vergelijkbaar met de Automation Manager van N-central. Veel standaard beheerstaken kunnen op deze manier geautomatiseerd worden. Resultaten van deze scripts kunnen vervolgens worden weergegeven op het Dashboard.

3.2.3. Mogelijke uitbreidingen

Naast de standaard functies is het mogelijk het standaardpakket van Kaseya te voorzien van verschillende uitbreidingen. Hieronder worden deze extra uitbreidingen beschreven.

Antivirus/Endpoint Security/Antimalware
De uitbreiding van Kaseya met de Antivirus, Antimalware en/of Endpoint Security module zorgt ervoor dat Windows systemen ten alle tijden voorzien zijn van goede beveiliging. Door de integratie met het Kaseya pakket worden problemen met de beveiliging van de servers/werkstations direct opgemerkt en mogelijk automatisch opgelost.

Back-up
Kaseya Back-up is gebaseerd op de back-up technologieën van Acronis en biedt in realtime een geautomatiseerde back-up van schijven, schijfimages, back-up op bestandsniveau en bare-metal herstel, voor Windows-servers en werkstations. Deze oplossing geeft beheerders de mogelijkheid om gedistribueerde systemen vanaf één interface te implementeren, te configureren, te bewaken, te beveiligen en er een back-up van te maken en te herstellen.

Directory Services
De integratie van Directory Services maakt het mogelijk een Active Directory omgeving te monitoren en te beheren via de Kaseya interface. Deze integratie maakt het voor MSP's bijzonder makkelijk standaard Active Directory beheerszaken uit te voeren, te monitoren en te automatiseren. MSP's kunnen bijvoorbeeld gemakkelijk nieuwe accounts voor hun klanten aanmaken zonder hiervoor eerst extern in te loggen.

Imaging & Deployment
Imaging & Deployment is een functie die het mogelijk maakt complete images te maken van een systeem en dit vervolgens als "baseline" op het netwerk op te slaan. Vervolgens is het mogelijk op gezette tijden reeksen van werkstations te "ghosten", allemaal gecontroleerd vanuit de Kaseya interface. Deze functie kan ook worden ingezet voor een simpele restore van een werkstation of uitrol van een nieuw station.

Network Monitor
De network monitor plug-in maakt het mogelijk niet alleen het server gebruik te monitoren, maar ook het gehele netwerk. De plug-in kan het hele netwerk in kaart brengen en vervolgens overzichten en rapporten van bandbreedte en CPU gebruik weergeven, zodat mogelijke problemen in het netwerk tijdig kunnen worden opgemerkt.

PSA integratie
Ook Kaseya bied de mogelijkheid een PSA systeem als ConnectWise, TigerPaw en Autotask te koppelen aan het pakket. Dit maakt het mogelijk problemen opgemerkt door Kaseya te escaleren en een bijbehorend ticket aan te maken. Ook zullen de meldingen in Kaseya en de tickets in het ticket-systeem met elkaar worden gesynchroniseerd. Net als bij N-central is het mogelijk een automatisch aangemaakt ticket te voorzien van uitgebreide systeem info en diagnostics.

Mobile Device Management
Het is mogelijk de smartphones van de beheerders/monteurs te voorzien van een Kaseya Mobile App voor de iPhone. Met deze app is het mogelijk overal in te loggen, berichten te ontvangen en toegang te hebben tot het systeem. Er is op het moment van schrijven nog geen app voor Android beschikbaar.

Software Deployment & Update
Ook bij Kaseya is het mogelijk third-party software gemakkelijk en geautomatiseerd uit te rollen. Dit kan zowel ad-hoc als gepland.

3.2.4. Bijzonderheden

Na aanschaf van het pakket van Kaseya krijgt de MSP's toegang tot een "Customer Portal". Hierin zijn net als bij N-able verschillende trainingen te vinden en wordt de MSP ondersteund in het implementeren van het product en begeleid bij het verkopen van de services. Een aantal diensten die Kaseya aanbied aan MSP's na aanschaf van het product:

- Kaseya Education Services - een individuele diepgaande reeks online informatieve sessies
- Online, CBT - toegang tot computer gebaseerde productopleiding
- Kaseya Workshops - toegang tot uitgebreide technische opleiding
- Kaseya Consultancy

3.2.5. Requirements

Agent Requirements

CPU	333 MHz Pentium-class CPU or greater
RAM	128 MB
Disk Space	30 MB
OS	Microsoft Windows 98, Me, NT 4.0, 2000,XP, Vista, Server 2003, Macintosh OSX v10.3.9 and above, Intel and PowerPC editions
Network	TCP/IP Outbound Port 5721, No Inbound Ports

Kaseya Server Requirements

CPU	Single processor (Intel Xeon 3 Ghz Dual Core, 1066 Mhz front side bus, 4MB cache)
RAM	8 GB
Disk Space	3x73Gig 10k SAS (hardware RAID 5)
OS	Microsoft Windows Server 2003 or 2008 Standard Edition 64 Bit Microsoft SQL Server 2005 or 2008 32 Bit (with AWE enabled) or 64 Bit
Network	100 Mbps Network Interface Card (NIC) DSL or Cable modem internet connection TCP/IP open ports: 80 inbound and outbound, 5721 inbound

3.2.6. Licentie

Kaseya rekent voor de aankoop van het systeem een vast opstartbedrag. Verder worden er kosten in rekening gebracht voor het aantal agents dat aan het systeem gekoppeld zal worden. Voor deze agents moeten licenties worden aangeschaft. Deze licenties zijn los bij te bestellen naarmate het systeem groeit en er meer klanten in komen.

Er wordt eenmalig € 4.500,- betaald voor de aanschaf van het product en de implementatie door de Kaseya consultants. Daarnaast zal per agent (zowel server als workstation) een bedrag van € 112,- voor 24 maanden in rekening worden gebracht. Genoemde bedragen bevatten alleen het basis programma, uitbereidingen zijn niet meegerekend.

Een nadeel van dit vaste licentiemodel is het gebrek aan flexibiliteit. Het model is interessant als er veel servers worden gemonitord, dan is het model goedkoper dan dat van de concurrenten. Echter is het monitoren van werkstations bijna zonde; er wordt immers hetzelfde betaald als voor een server. Deze investering kan dus beter worden besteed aan het monitoren van een belangrijke server dan aan het monitoren van een ‘onbelangrijk’ werkstation.

Als we een model met 500 agents aanhouden komen we op de volgende rekensom uit:

Tabel 4: Kosten Kaseya

Eenmalig	Terugkomend (per maand)	Totaal (na 24 maanden)
	500 x € 112,- = € 56.000,- / 24	500 x € 112,- = € 56.000,- + € 4.500,-
€ 4.500,-	€ 2.333,33	€ 60.500,-

3.3. GFI MAX RemoteManagement

3.3.1. Omgeving

GFI MAX RemoteManagement is een verzameling van een aantal GFI tools in de Cloud speciaal samengesteld voor MSP's. De tools zijn voor bedrijven ook los te bestellen als een on-premise oplossing. Er is zelfs een combinatie mogelijk tussen de twee oplossingen, als het ware een hybride oplossing tussen on-premise en Cloud. Voor een MSP is dit echter geen oplossing. GFI biedt het RemoteManagement pakket voor MSP's alleen in de Cloud aan. (GFI)

3.3.2. Functies

Server monitoring

De server monitoring functie gebruikt een agent om de gegevens te verzamelen. Deze agent is geïnstalleerd op de betreffende server. De gegevens die zoal verzameld worden, zijn gegevens als de schijfstatus en prestatie, processor, werkgeheugen, enz. Resultaten en storingen worden vervolgens weergegeven in het Dashboard.

Netwerk monitoring

De netwerk monitoring functie maakt het mogelijk overige apparaten binnen het netwerk te monitoren op basis van SNMP. Op deze manier kunnen ook Network Devices als routers, switches, printers en overige, niet door de agent ondersteunde, servers worden gemonitord. Hiervoor zal wel een server met een soort van probe in het netwerk nodig zijn.

Website monitoring

Website monitoring van GFI maakt het mogelijk specifiek een website en bijbehorende prestatie kenmerken te monitoren. Naast standaard checks op beschikbaarheid, is de website monitor ook in staat te meten hoelang het duurt voordat een pagina in de browser geladen is. Deze informatie kan gemonitord worden. Mochten deze waardes niet meer acceptabel zijn dan kunnen hier meldingen over worden verstuurd. Deze functie kan ook gemakkelijk extern gehoste websites monitoren, zonder dat hiervoor extra software nodig is.

Werkstation monitoring

Net als bij de server monitoring kunnen ook de werkstations worden uitgerust met een agent die gegevens over het systeem gaat verzamelen. Deze werkstations zullen echter op andere punten worden gecontroleerd. Vervolgens kunnen ook op de werkstations automatische taken worden gepland als een dagelijkse 'health check' om gebruikers iedere ochtend weer een optimaal werkende machine te garanderen.

Patch management
De patch management functie maakt het mogelijk zowel servers als werkstations te controleren op ontbrekende patches en deze automatisch te installeren. Er is geen verdere integratie met WSUS aanwezig.

Reporting
De reporting tool maakt het mogelijk rapporten te genereren van issues, uitgevoerde werkzaamheden, prestatiegegevens, up time, enz. Deze rapporten kunnen vervolgens worden gebruikt om de klant een overzicht te geven van de uitgevoerde werkzaamheden en het nut hiervan.

Managed antivirus
De antivirus oplossing van GFI kan gemakkelijk worden uitgerold op zowel de werkstations als de servers en zorgt voor een up-to-date bescherming van deze systemen. Problemen met de antivirus worden direct op het Dashboard van GFI gemeld. Scans kunnen gemakkelijk worden gepland in de GFI interface en worden automatisch uitgevoerd op de geselecteerde systemen. De Managed antivirus oplossing is gebaseerd op de antivirus van VIPRE Enterprise Software.

Systems branding
Het is mogelijk alle branding van GFI te vervangen voor de huisstijl van de MSP. Naar de klant toe staat dit professioneler en is het net alsof het pakket van de MSP zelf is.

PSA Integration
Ook GFI biedt een integratiemogelijkheid voor PSA software. Pakketten die out-of-the-box ondersteund worden zijn Autotask en ConnectWise. Er is ook ondersteuning voor andere pakketten echter zijn hier geen kant en klare oplossingen voor en dienen deze geprogrammeerd te worden tegen de GFI API.

Remote access
GFI MAX RemoteManagement heeft een ingebouwde remote access functie. Via één simpele handeling kan een machine direct vanuit het Dashboard worden overgenomen. Afstand op beheer kan actief worden uitgevoerd, door het overnemen van een scherm, maar ook passief door het sturen van commando's naar de agent. Op deze manier zal een actieve gebruiker niet of nauwelijks gestoord worden in zijn/haar werk.

Alerting & viewing
GFI is uitgerust met een makkelijk configureerbaar alerting en viewing systeem. Notificaties zijn gemakkelijk in te stellen en kunnen bestaan uit email of SMS notificaties. GFI bevat een zogenaamde WallChart view, dit is een overzicht van het Dashboard welke als het ware op een groot scherm op de muur kan worden getoond op de automatisering afdeling. Bovendien hebben beheerders de mogelijkheid gebruik te maken van een MiniDash, dit is een applicatie voor op de smartphone welke een compact overzicht geeft van het Dashboard. Zo hebben beheerders overal toegang tot het systeem.

Asset tracking
De asset tracking functie maakt het mogelijk lijsten met details van de te monitoren machines te maken. Dit kunnen hardware gegevens zijn als serienummers, componentenlijsten en garantie periodes, maar ook software details en licenties.

3.3.3. Bijzonderheden

Licenties

Het licentie model van GFI is zo ingericht dat men alleen hoeft te betalen voor wat wordt gebruikt. Er is geen minimale afname per jaar. Als een bepaalde functie niet wordt gebruikt dan hoeft hiervoor ook niet betaald te worden. Voor de functies die wel worden gebruikt, wordt betaald voor de hoeveelheid gebruik, men zit dus niet vast aan vaste prijzen. Bovendien zijn de contracten direct opzegbaar.

Building Blocks

Het Building Blocks programma van GFI is samengesteld om MSP's te trainen in de nieuwe manier van werken en te ondersteunen in het verkopen van de nieuwe services aan klanten.

3.3.4. Licentie

GFI hanteert twee verschillende licentiemodellen voor het gebruik van GFI MAX RemoteManagement. Een model gebaseerd op een vast bedrag per maand het 'MAXimum Customer Care Pack' en een model waarbij alleen betaald wordt voor wat wordt gebruikt het 'Per Module Monitoring & Reporting'. Dit laatste model blijft erg abstract en het is moeilijk een inschatting te maken waar men uiteindelijk aan toe is. Daarom wordt in de vergelijking het vaste bedrag per maand gebruikt. In dit model wordt onderscheid gemaakt tussen een licentie voor een server en een licentie voor een werkstation. Voor de serverlicentie dient, naast het vaste bedrag per maand, ook een eenmalige activatie betaald te worden.

Verder worden er geen kosten voor onderhoud en ondersteuning gevraagd, dit zit in de prijs inbegrepen. De gehanteerde prijzen in het licentiemodel worden lager naarmate er meer licenties tegelijk worden afgenomen. Verder hanteert GFI geen opzegtermijn voor de overeenkomst en kan deze op ieder gewenst moment worden beëindigd.

In de onderstaande rekensom wordt uitgegaan van het 'MAXimum Customer Care Pack', het vaste bedrag per maand. Er wordt, net als bij de voorgaande rekensommen, uitgegaan van een totaal van 500 licenties. Hiervan zijn er 150 vrij gemaakt voor servers en 350 blijven over voor het monitoren van werkstations.

	Eenmalig	Terugkomend (per maand)	Totaal (na 24 maanden)
Server	€ 7,40 x 150 = € 1.110,-	€ 9,63 x 150 = € 1.444,50	24 x € 1.444,50 = € 34.668,- + € 1.110,- = € 35.778,-
Werkstation		€ 0,75 x 350 = € 262,50	24 x € 262,50 = € 6.300,-
Dashboard branding	€ 368,-		€ 368,-
Agent branding	€ 182,-		€ 182,-
Totaal	€ 1.660,-	€ 1.707,-	€ 42.628,-

Tabel 5: Kosten GFI MAX RemoteManagement

3.4. Vergelijking

Een snelle vergelijking van de functies van bovengenoemde pakketten levert de volgende tabel op. GFI MAX RemoteManagement heeft maar een beperkt aantal functies en blijft duidelijk achter bij de andere pakketten. N-central en Kaseya daarentegen vertonen erg veel overeenkomsten. Het zou oneerlijk zijn puur af te gaan of een functie wel of niet beschikbaar is als men een goede afweging tussen deze twee pakketten wil maken. Het verschil tussen deze pakketten moet gezocht worden in het gegeven hoe goed en hoe uitgebreid en bepaalde functie is.

	Relatief gewicht (0-1)	N-Central	Kaseya	GFI MAX Remote Management
On-premise	0,8	5 / 4,0	5 / 4,0	- / -
Cloud	0,2	2 / 0,4	2 / 0,4	5 / 1,0
Web based dashboard	0,5	4 / 2,0	4 / 2,0	4 / 2,0
Integratie PSA	0,7	4 / 2,8	4 / 2,8	2 / 1,4
Remote control	0,1	4 / 0,4	4 / 0,4	4 / 0,4
Asset control	0,8	5 / 4,0	4 / 3,2	4 / 3,2
Automatiseren beheerstaken	1,0	5 / 5,0	4 / 4,0	4 / 4,0
Mobiele toegang	0,3	5 / 1,5	3 / 0,9	4 / 1,2
Patch management	0,7	5 / 3,5	5 / 3,5	4 / 2,8
Antivirus/malware	0,9	5 / 4,5	5 / 4,5	5 / 4,5
Reporting	1,0	4 / 4,0	3 / 3,0	3 / 3,0
Software deployment	0,4	4 / 1,6	5 / 2,0	- / -
Audit network vulnerability	0,3	3 / 0,9	4 / 1,2	- / -
Unattended remote control	0,2	3 / 0,6	3 / 0,6	- / -
Self-healing	0,8	5 / 4,0	4 / 3,2	- / -
Netflow monitoring	0,5	4 / 2,0	4 / 2,0	- / -
Backup automatisering	0,9	5 / 4,5	5 / 4,5	- / -
Policy manager	0,7	3 / 2,1	5 / 3,5	- / -
Branding	0,5	5 / 2,5	4 / 2,0	5 / 2,5
Desktop migratie	0,2	- / -	5 / 1,0	- / -
Active directory services	0,5	- / -	5 / 2,5	- / -
Imaging (Ghosting/D2D)	0,6	5 / 3,0	5 / 3,0	- / -
WSUS integratie	0,8	5 / 4,0	- / -	- / -
Website monitoring	0,8	- / -	- / -	5 / 4,0
Software trainingen/handleidingen	1,0	5 / 5,0	5 / 5,0	4 / 4,0
Ondersteuning implementatie MSP model	0,9	4 / 3,6	2 / 1,8	- / -
Ondersteuning bij software implementatie	0,9	5 / 4,5	5 / 4,5	- / -
Totaal		104 / 70,4	104 / 65,5	53 / 34,0
Gemiddelde		**4,3 / 2,9**	**4,2 / 2,6**	**4,1 / 2,6**

Tabel 6: Productvergelijking (McCabe, 2007)

Cijfers zijn toegekend aan de invulling en compleetheid van de functies. Deze worden ingedeeld op een schaal van 1 tot 5 en zijn verkregen door ervaringen met trial versies en op basis van product informatie en documentatie. Deze worden vervolgens vermenigvuldigd met het gewicht. Weging is verkregen na overleg met de opdrachtgever en de overige betrokkenen bij het vaststellen van de eisen. Deze wegingen zijn in vergaderingen en interviews vastgesteld.

4. Conclusie

Een Managed Server Provider (MSP) verschilt van de “normale service provider” of automatiseerder in die zin dat een Managed Service Provider het beheer onder controle heeft en proactief te werk kan gaan. Een MSP is in staat de mogelijke problemen bij een klant vroegtijdig te ontdekken en dit probleem nog voor het optreedt te verhelpen. Daarnaast is de MSP in staat verschillende standaard beheerstaken geautomatiseerd uit te voeren. Hierbij valt bijvoorbeeld te denken aan back-up, patches, antivirus updates. De MSP moet als het ware alle ICT zorgen bij de klant wegnemen en deze klant op een actieve wijze ondersteunen in zijn ICT.

De volwassenheid van een MSP kan gemeten worden aan een MSP volwassenheidsmodel. Dit volwassenheidsmodel kent een indeling van vijf niveaus, deze verschillen van break-fix en reactief tot managed en value. Deze niveaus hebben allen hun eigen eigenschappen. Niet alleen de MSP moet deze niveaus doorlopen, ook de klanten moeten zich ontwikkelen in dit model. Dit is een van de punten waar de groei in het MSP model vaak mis gaat. Een MSP kan geen managed services verkopen aan een break-fix klant. Andere moeilijkheden zijn:

- het niet volledig benutten van de software;
- teveel richten op techniek;
- de waarde niet duidelijk krijgen aan de klant;
- en de flexibiliteit verliezen.

Zolang de MSP zich bewust blijft van deze punten en de oplossingen hiervoor, zal deze er weinig hinder van ondervinden. Daarom zijn de volgende zaken belangrijk:

- verplaatsen in de klant, wat wil de klant echt?
- duidelijk en veel communiceren met de klant;
- oplossingen in bouwstenen aanbieden, de klant kan zijn ‘eigen’ oplossing samenstellen;
- en blijven rapporteren!

Om deze vormen van dienstverlening aan de klant te bieden, heeft de MSP wel een krachtig pakket nodig dat hem hierbij kan ondersteunen. Hiervoor zijn drie pakketten onderzocht: N-central, Kaseya en GFI MAX RemoteManagement. Al deze pakketten beschikken over een uitgebreide set functies, met ieder hun eigen specialiteiten en toepassingsmogelijkheden.

Wat alle pakketten met elkaar gemeen hebben zijn functies als: antivirus, backup, onderhoud, patch management, notificaties, dashboards en rapportage. Het ene pakket zal hier beter in zijn dan het andere. Daarom is er voor iedere functie een weging samengesteld en zijn de pakketten beoordeeld op compleetheid en invulling van de functies. Uit deze vergelijking komt uiteindelijk N-central als beste oplossing voor Hupra naar voren.

	N-Central	Kaseya	GFI MAX Remote Management
Totaal	104 / 70,4	104 / 65,5	53 / 34,0
Gemiddelde	**4,3 / 2,9**	**4,2 / 2,6**	**4,1 / 2,6**

Bibliografie

GFI. (sd). Opgehaald van GFI MAX RemoteManagement: http://www.gfi.com/it-managed-services-software

Kaseya. (sd). Opgehaald van Kaseya: http://www.kaseya.nl/solutions.aspx

Kaseya. (2009). Kaseya® Professional Services.

Kaseya. (2009). Kaseya®Managed Services Edition.

Kaseya. (2010). Automating IT Systems Management.

McCabe, J. D. (2007). *Network Analysis, Architecture, and Design.* Amsterdam: Morgan Kaufman Publishers.

N-able Technologies. (sd). Opgehaald van N-able: http://www.n-able.com/

N-able Technologies. (2006). From Promises to Proof: How To Demonstrate Value to Your Customers.

N-able Technologies. (2006). N-ables MSP Maturity Model.

N-able Technologies. (2007). The Fundamentals of a Successful Managed Services Practice.

N-able Technologies. (2007). The Seven Major Obstacles on the Road to Managed Services.

N-able Technologies. (2008). IT Service Delivery: From Basic Automation through to Managed Services.

N-able Technologies. (2009). Doing More with Less: Automating IT Services in Your Midsize Business.

N-able Technologies. (2011). Going beyond RMM.

Walsh, L. M. (2011). Countering artificial commoditization and poor pricing practices in managed services.

Bijlage G: Adviesrapport

Proactief beheer bij Hupra

Auteur:
M.M.J. de Weijer
Studentnummer: 1546128
Hogeschool Utrecht
Faculteit Natuur & Techniek
Systeembeheer

Bedrijf:
Hupra Automatisering
Hoofdstraat 105
3901 AK Veenendaal

Begeleiders:
Hupra: Dhr. P.A. Willemsen
Hogeschool Utrecht: Dhr. H. van Nimwegen

Afstudeerperiode:
februari 2012 - juni 2012

Versie: 1.0
Datum: 24 mei 2012

Versie beheer:

Versie	Datum	Wijzigingen
0.0	10-02-2012	Initiële versie document, geen inhoud
0.1	02-03-2012	Invulling eisen en wensen Hupra
0.2	10-03-2012	Aanvullen mogelijke oplossingen
0.3	19-03-2012	Invullen adviezen, processen
1.0	24-05-2012	Verwerking feedback, Afronden document, opmaak

Inhoud

1. Inleiding

Dit document is een adviesrapport aan Hupra over de inzet van proactief beheer en wat dit voor het bedrijf kan opleveren. Aanleiding van dit advies is de sterke groei van het aantal klanten die Hupra op dit moment doormaakt en het verlangen van het bedrijf om meer onderscheidend te worden ten opzichte van de concurrentie. Men wil dit bereiken door over te gaan op een proactieve manier van werken en beheer, dit met bijbehorende ondersteuning van een Managed Service Provider (MSP) software pakket.

In dit document wordt een advies uitgebracht voor productkeuze en de uiteindelijke configuratie van het gekozen product. Dit pakket kan vervolgens op de geadviseerde manier worden ingezet. Daarnaast zal Hupra ook geadviseerd worden over inrichting van het beheer omtrent deze nieuwe manier van proactief werken. Om een goed advies uit te kunnen brengen, zijn eerst de eisen en wensen van Hupra in kaart gebracht. Deze eisen en wensen zijn in dit document uitgewerkt en zullen in de adviezen worden meegenomen.

Voorafgaand aan dit advies is een onderzoek uitgevoerd naar de mogelijkheden van proactief beheer in het algemeen, welke vormen er zijn, wat de voor- en nadelen van deze methode zijn en waar mogelijke valkuilen zitten. Bovendien is er uitgebreid onderzoek gedaan naar de mogelijkheden van de ondersteunende software pakketten. Dit rapport zal verder bouwen op de resultaten van het productonderzoek en toelichten hoe Hupra deze bevindingen kan inzetten voor een sterk proactief beheermodel.

2. Eisen en wensen van Hupra

Voordat een gefundeerd advies kan worden uitgebracht, is het belangrijk de eisen en wensen van Hupra in kaart te brengen. Een aantal van deze eisen zijn verkregen bij de start van het project en opgegeven door de opdrachtgever. Deze eisen zijn hieronder opgenomen. Om de eisen verder in kaart te brengen zijn er een aantal aanvullende interviews gehouden met de opdrachtgever en werknemers van Hupra. Er is voor gekozen ook de werknemers van Hupra te benaderen om een compleet beeld van de situatie te vormen. Deze werknemers moeten immers met het nieuwe model en de nieuwe software gaan werken. De eisen en wensen van de werknemers zijn verkregen via open interviews met werknemers van verschillende disciplines. Deze verzamelde eisen en wensen zullen van groot belang zijn voor de rest van het advies.

Door het groeiende aantal klanten en de drang om iets extra's te bieden, wil Hupra af van het klassieke, reactieve beheer bij klanten. Het zogenaamde "brandjes blussen", de klant belt zelf als er een probleem is. Men wil zo veel mogelijk van deze werkwijze af en over gaan naar een model voor proactief beheer. Door over te gaan naar proactief beheer wil Hupra de concurrentie het hoofd bieden en voorkomen dat men achter komt te liggen. Door sneller problemen in de ICT van de klant te ontdekken en deze eerder en gemakkelijker op te lossen dan voorheen het geval was, kan Hupra een sterkere concurrerende positie innemen. Bovendien wil Hupra met de inzet van proactief beheer meer rust binnen de organisatie creëren, zodat er meer tijd overblijft voor innovatie. Men kan dus stellen dat Hupra op dit moment niet in staat is de door haar gewenste kwaliteit te bieden, omdat de focus nog teveel ligt op het reactieve beheer waardoor weinig tijd voor innovatie overblijft.

De uiteindelijke doelstelling van het gehele project is een beheermodel waarmee Hupra proactief te werk kan gaan, de problemen tijdig kan ontdekken en de impact van de problemen beperken, ondersteund door procedures en ondersteunende software. Doelstelling is ook deze ondersteunende software en procedures op een dusdanige manier in te richten dat druk in de organisatie wordt weggenomen door terugkomend onderhoud automatisch te laten uitvoeren en ervoor te zorgen dat werk bij de juiste beheerders terecht komt om een snelle afhandeling te garanderen. Bovenstaande kan kort samengevat worden tot de volgende globale punten:

- onderscheidend vermogen Hupra;
- kosten terugdringen (aantal facturabele uren verhogen met 20%);
- klantwerving (25+ klanten in het proactieve model);
- verlaging werkdruk (terugdringen break-fix werkzaamheden van 99% naar 50%);
- betrouwbaarheid dienstverlening/ ICT van de klant (van ±90% naar 99% beschikbaarheid);
- automatisering terugkomend onderhoud (van 0% naar 10-20%).

Bovengenoemde eisen zijn tot stand gekomen door verschillende gesprekken met de opdrachtgever en een aantal medewerkers van Hupra in de vorm van open interviews. Deze zijn afgenomen onder werknemers van verschillende disciplines, zoals consultants, beheerders, maar ook sales & marketing.

De eisen kunnen verder worden opgesplitst in eisen aan het model voor proactief beheer en eisen aan het software pakket.

2.1. Eisen proactief model

Hupra stelt een aantal eisen aan het model voor proactief beheer. Deze eisen en/of verwachtingen zijn vastgesteld in overleg met de opdrachtgever en interviews met een aantal werknemers van Hupra.

Procedures

In het proactieve model moeten procedures worden opgenomen voor het beheer. Deze procedures moeten structuur in de werkzaamheden brengen en ervoor zorgen dat het beheer op een goed gestructureerde manier verloopt. Het beheer moet vooral professionaliteit naar de klant uitstralen, want dit is het niveau dat Hupra wil bereiken. Daarnaast moeten deze procedures ook duidelijkheid voor Hupra bieden aan bijvoorbeeld nieuwe gebruikers van het model.

Vastleggen verantwoordelijkheden

Bovengenoemde procedures werken alleen als alle verantwoordelijkheden vastgelegd zijn en deze beheerders deze verantwoordelijkheden ook nemen. Hupra wil niet alleen duidelijkheid en structuur in de manier van werken, maar wil daarnaast ook dat de verantwoordelijkheden goed geregeld zijn. Zo moet bij de aanvang van een incident meteen duidelijk zijn welke beheerder verder verantwoordelijk wordt voor het oplossen van het probleem, zodat het werk niet langs elkaar heen loopt. Bovendien wordt voorkomen dat meerdere beheerders langs elkaar heen aan het zelfde probleem werken. Dit zal niet de beoogde professionaliteit uitstralen.

Priotarisering notificaties

Priotarisering van de notificaties is een eis aan zowel het proactieve model als aan het softwarepakket. Hupra wil dat er een duidelijke scheiding van notificaties op prioriteit wordt gemaakt en dat deze meldingen meteen aan de juiste verantwoordelijke worden gekoppeld. Bovendien is een systeem of indeling nodig waarmee werknemers niet meteen overspoeld worden met meldingen voor kleine problemen. Deze eis zal ook van belang zijn bij een toekomstige koppeling aan een ticket systeem, ter voorkoming van onjuiste tickets.

Aantal facturabele uren verhogen

Het nieuwe model moet bijdragen aan het verminderen van verloren uren. In de huidige break-fix situatie is het vaak zo dat een consultant bij een klant langs moet voor een reparatie. De reistijd wordt weliswaar opgenomen in de factuur, toch gaan er uren verloren welke niet gefactureerd kunnen worden, bijvoorbeeld als de consultant een half uur tussendoor op kantoor aanwezig is. Meestal is dit niet de moeite om een nieuwe taak te starten. Met het nieuwe model moet het mogelijk worden een duidelijk overzicht van de werkzaamheden de krijgen, zodat er makkelijker van ticket naar ticket kan worden gegaan. Bovendien zullen veel taken in het nieuwe model remote opgelost kunnen worden waardoor consultants minder vaak naar de klant hoeven en de eerder genoemde problemen minder vaak optreden.

Klantwerving
Hupra wil een goed uitgewerkt model voor proactief beheer inzetten als “unique selling point”. Een professionele en volwassen vorm van proactief beheer is een eigenschap die goed gebruikt kan worden bij het werven van nieuwe klanten. Hupra wil de klant vooral een goed gevoel meegeven, zodat de klant er van uit kan gaan dat zijn zaken goed geregeld zijn. Bovendien zal het de professionaliteit uitstralen waar Hupra naar op zoek is.

Verlaging werkdruk
Een invoering van een dergelijk model voor proactief beheer moet de werkdruk bij de werknemers van Hupra verlagen. Het systeem moet overzicht en duidelijkheid bieden. Een goed werkend proactief model moet in de ogen van Hupra de stress en de druk bij de werknemers wegnemen.

Verbetering van de betrouwbaarheid van de dienstverlening
Een goed proactief model moet voor Hupra bijdragen aan een verbetering van de dienstverlening. Door een goede duidelijke structuur en het hebben van een duidelijk overzicht moeten fouten in het beheer minder vaak voorkomen en, waar mogelijk, een versnelling van de doorlooptijd opleveren. Met het model moet de beheerafdeling proactief te werk kunnen gaan en op rustige momenten proactief onderhoud kunnen uitvoeren om problemen in de toekomst voor te zijn.

2.2. Eisen software pakket

Naast de eisen aan het proactieve beheermodel hebben de interviews met werknemers en de opdrachtgever ook een aantal eisen aan het software pakket opgeleverd.

Automatisering terugkomend onderhoud
Hupra vindt het belangrijk dat een ondersteunend software pakket voldoende mogelijkheden biedt voor automatisering van terugkomend onderhoud om op deze manier beheerders ‘vervelend’ werk uit handen te nemen. Minimaal de volgende taken moeten geautomatiseerd verlopen:

- Schijfopruiming
- Defragmentatie
- Schijfcontrole
- Virus scan
- Patch management

Interface
Hupra verwacht van het product een duidelijke ‘nette’ interface welke een compleet overzicht moet geven van de huidige problemen. Het moet bijvoorbeeld mogelijk zijn deze interface op een groot scherm aan de muur weer te geven. Beheerders moeten een duidelijk overzicht hebben van alle problemen. Vanuit dit overzicht moeten zij direct kunnen werken. Dit moet in de vorm van aanpasbare en duidelijke dashboards gepresenteerd worden.

Support
Hupra hecht veel waarde aan goede support vanuit de fabrikant. Het is belangrijk dat er goede ondersteuning bij problemen aanwezig is. Het softwarepakket wordt immers een onmisbaar product binnen de beheerafdelingen van Hupra. Er moet een mogelijkheid zijn voor een servicecontract met de fabrikant en ondersteuning op zowel technisch als niet technisch gebied.

Technisch diepgaand
Hupra wil een technisch diepgaand product. Dat wil zeggen een product dat vooruitstrevend is en veel mogelijkheden biedt. Het is ook belangrijk dat eventuele benodigde uitbreidingen makkelijk zelf kunnen worden toegevoegd en er met scripts bijvoorbeeld specifieke controles worden uitgevoerd op maatwerksystemen welke Hupra in beheer heeft bij de klant.

Betrouwbaarheid
Een belangrijke eis is dat het product betrouwbaar is, dat er geen false positives/negatives worden gegeven. Dit levert onnodig werk op voor beheerders. Of het product betrouwbaar is, heeft meer te maken met een bepaald gevoel wat een product geeft. Technisch gezien hangt het voor het merendeel af van de configuratie of een product betrouwbaar is of niet. Doelstelling moet zijn dat 1 op de 100 meldingen een false positive mag zijn.

Aansluiting met andere pakketten binnen het bedrijf
Hupra vindt het belangrijk dat het pakket ondersteuning biedt voor integratie met andere bestaande pakketten. Denk bijvoorbeeld aan een financieel pakket. Daarnaast is het van belang dat ook in de toekomst, bij migratie naar een groter ticket systeem, deze mogelijkheid tot integratie nog steeds bestaat.

3. Mogelijke oplossingen

In dit hoofdstuk zullen een aantal oplossingen worden aangedragen aan de hand van de eisen die in het vorige hoofdstuk zijn beschreven. Na een eerste inventarisatie en overleg met de opdrachtgever blijkt dat er vier mogelijke scenario's uiteengezet kunnen worden. Deze zullen in dit hoofdstuk besproken en vergeleken worden.

3.1. Vasthouden aan huidige model

Vasthouden aan het huidige model betekent kort door de bocht: "niets doen". Het zal niet totaal onverwacht zijn dat dit niet de oplossing is die Hupra zoekt. Het is mogelijk een aantal verbeteringen in het huidige model door te voeren, echter zal dit alleen maar leiden tot opschuiven van het probleem. De eisen omtrent het efficiënt werken zullen hiermee niet worden opgelost. Het verlagen van de werkdruk is in het huidige model wel mogelijk, maar zal slechts een uitstel zijn en bij een snelle groei van het aantal klanten zal men zichzelf weer snel in de oude situatie bevinden.

3.2. Inzetten monitoring

Een voor de hand liggende oplossing is het inzetten van monitoring, echter zal dit niet alle problemen wegnemen. Het inzetten van monitoring geeft het bedrijf de mogelijkheid een duidelijk beeld te vormen van de systemen en de fouten die daarin optreden. Echter zijn de meeste monitoring pakketten niet in staat de gewenste geavanceerde controle te bieden welke door Hupra beoogd is. Bovendien zal het inzetten van monitoring alleen niet voldoende zijn. Bij het inzetten van monitoring en vasthouden aan het huidige model, wat in feite gebeurd, wordt maar de helft van het probleem bekeken. Er wordt wel een overzicht geboden, maar is geen mogelijkheid om iets proactief te ondernemen als hiervoor geen andere werkwijze wordt aangenomen.

3.3. Implementatie proactief model

Een implementatie van een proactief model, zonder hierbij ondersteunende software te gebruiken, is vrijwel onmogelijk. Het overzicht en de functionaliteit dat de software biedt, is een vereiste bij het hanteren van een dergelijk model. Het is bijvoorbeeld niet mogelijk een probleem aan te zien komen als hier geen software voor aanwezig is. Sterker nog, er is totaal geen overzicht van de huidige systemen. Over het handmatig controleren van de systemen wordt niet eens meer gesproken. Bovendien is het ook onmogelijk de Service Level Agreements in dit proactieve model te garanderen als er geen middelen zijn om aan te tonen af deze daadwerkelijk gehaald worden.

3.4. Implementatie proactief model met ondersteunende software

Een combinatie van de implementatie van het proactieve model met ondersteunende software is hier de meest complete oplossing. Deze ondersteunende software moet een capabele tool zijn om alle aspecten van het proactieve model te ondersteunen. De bedrijfsprocessen dienen aan te sluiten op de mogelijkheden van de tool om deze zo goed mogelijk te benutten. Met een complete aanpak van dit probleem is het weer mogelijk de ICT onder controle te krijgen.

	Vasthouden aan huidige model	Monitoring	Procedures aanpassen	Procedures + software tool
Kosten terugdringen			x	x
Verlaging werkdruk			x	x
Betrouwbaarheid dienstverlening		X		x
Automatisering onderhoud				x
Max. niveau MSP Maturity Model	1	2	-	5

Tabel 1: Keuze oplossingen

De tabel hierboven geeft een overzicht van de bovengenoemde oplossingen en het effect hiervan op de eerder vastgestelde eisen. Zoals al meerdere malen aangekaart in het productonderzoek, is de inzet van een proactief model met procedures en ondersteunend softwarepakket de meest volledige oplossing. Deze aanpak biedt ook meer mogelijkheden voor de toekomst. Alleen met deze aanpak kan een MSP doorgroeien in het volwassenheidsmodel.

4. Advies

Aan de hand van de bovenstaande oplossingen zijn een aantal adviezen tot stand gekomen voor de keuze van het product, de configuratie en inzet hiervan en procedures welke opgezet dienen te worden.

4.1. Productkeuze

Om te beginnen zal een advies worden geven over het aan te schaffen softwarepakket. Er zijn in de onderzoeksfase drie pakketten onderzocht en vergeleken. Uitgebreide informatie over deze pakketten is te vinden in het productonderzoek. In het productonderzoek is al een korte vergelijking van de pakketten gemaakt. Deze tabellen geven alleen de verschillen tussen de pakketten weer op het gebied van functies. Hieronder worden deze tabellen nog een keer weergegeven om een samenvatting van de pakketten te geven. Voor meer informatie over deze pakketten verwijs ik naar het productonderzoek, hoofdstuk 3 ‘Product onderzoek’.

	Relatief gewicht (0-1)	N-Central	Kaseya	GFI MAX Remote Management
On-premise	0,8	5 / 4,0	5 / 4,0	- / -
Cloud	0,2	2 / 0,4	2 / 0,4	5 / 1,0
Web based dashboard	0,5	4 / 2,0	4 / 2,0	4 / 2,0
Integratie PSA	0,7	4 / 2,8	4 / 2,8	2 / 1,4
Remote control	0,1	4 / 0,4	4 / 0,4	4 / 0,4
Asset control	0,8	5 / 4,0	4 / 3,2	4 / 3,2
Automatiseren beheerstaken	1,0	5 / 5,0	4 / 4,0	4 / 4,0
Mobiele toegang	0,3	5 / 1,5	3 / 0,9	4 / 1,2
Patch management	0,7	5 / 3,5	5 / 3,5	4 / 2,8
Antivirus/malware	0,9	5 / 4,5	5 / 4,5	5 / 4,5
Reporting	1,0	4 / 4,0	3 / 3,0	3 / 3,0
Software deployment	0,4	4 / 1,6	5 / 2,0	- / -
Audit network vulnerability	0,3	3 / 0,9	4 / 1,2	- / -
Unattended remote control	0,2	3 / 0,6	3 / 0,6	- / -
Self-healing	0,8	5 / 4,0	4 / 3,2	- / -
Netflow monitoring	0,5	4 / 2,0	4 / 2,0	- / -
Backup automatisering	0,9	5 / 4,5	5 / 4,5	- / -
Policy manager	0,7	3 / 2,1	5 / 3,5	- / -
Branding	0,5	5 / 2,5	4 / 2,0	5 / 2,5
Desktop migratie	0,2	- / -	5 / 1,0	- / -
Active directory services	0,5	- / -	5 / 2,5	- / -
Imaging (Ghosting/D2D)	0,6	5 / 3,0	5 / 3,0	- / -
WSUS integratie	0,8	5 / 4,0	- / -	- / -
Website monitoring	0,8	- / -	- / -	5 / 4,0
Software trainingen/handleidingen	1,0	5 / 5,0	5 / 5,0	4 / 4,0
Ondersteuning implementatie MSP model	0,9	4 / 3,6	2 / 1,8	- / -

Ondersteuning bij software implementatie	0,9	5 / 4,5	5 / 4,5	- / -
Totaal		104 / 70,4	104 / 65,5	53 / 34,0
Gemiddelde		**4,3 / 2,9**	**4,2 / 2,6**	**4,1 / 2,6**

Tabel 2: Product vergelijking

	Eenmalig (eerste jaar)	Terugkomend vanaf jaar 2 (per jaar)	Totaal (na 24 maanden)
Server Desktop Network Essentials	€ 220,80 x 100 = € 22.080,- € 46,- x 250 = € 11.500,- € 110,40 x 50 = € 5.500,- € 15,- x 100 = € 1.500,-*	€ 44,16 x 100 = € 4.416,- € 9,20 x 250 = € 2.300,- € 22,08 x 50 = € 1.104,- € 3,- x 100 = € 300,-	€ 22.080 + € 4.416,- = € 26.496,- € 11.500 + € 2.300,- = € 13.800,- € 5.500 + € 1.104,- = € 6.604,- € 1.500 + € 300,- = € 1.800,-
	€ 40.580,-	€ 8.120,-	€ 48.700,-

Tabel 3: Kosten N-central

Eenmalig	Terugkomend (per maand)	Totaal (na 24 maanden)
€ 4.500,-	500 x € 112,- = € 56.000,- / 24 € 2.333,33	500 x € 112,- = € 56.000,- + € 4.500,- € 60.500,-

Tabel 4: Kosten Kaseya

	Eenmalig	Terugkomend (per maand)	Totaal (na 24 maanden)
Server	€ 7,40 x 150 = € 1.110,-	€ 9,63 x 150 = € 1.444,50	24 x € 1.444,50 = € 34.668,50 + € 1.110,- = € 35.778,-
Werkstation		€ 0,75 x 350 = € 262,50	24 x € 262,50 = € 6.300,-
Dashboard branding	€ 368,-		€ 368,-
Agent branding	€ 182,-		€ 182,-
Totaal	+ € 1.660,-	+ € 1.707,-	+ € 42.628,-

Tabel 5: Kosten GFI MAX RemoteManagement

Na bovenstaande productvergelijkingen en rekening houdende met in hoofdstuk 2 vastgestelde eisen en wensen van Hupra, is het advies aan Hupra gebruik te gaan maken van N-central van N-able, mogelijk in combinatie met een aantal uitbreidingen aangeboden door N-able.

GFI MAX RemoteManagement is op de eerste plaats afgevallen omdat dit pakket simpelweg maar een beperkt aantal functies heeft en in vergelijking met Kaseya en N-central behoorlijk achterblijft en minder technisch diepgaand is. GFI heeft daarentegen wel een aantrekkelijk licentie model, maar na wat rekenwerk valt al snel op dat dit niet heel veel goedkoper is voor wat men er daadwerkelijk voor

krijgt. Verder heeft GFI wel een bijna perfecte beschikbaarheid, omdat gebruik wordt gemaakt van een Cloud oplossing. Rekening houdend met de eisen van Hupra wegen deze voordelen uiteindelijk niet op tegen het gebrek aan functies.

De keuze tussen N-central en Kaseya is moeilijk en heeft uiteindelijk ook meer te maken met een gevoel bij het product. De verschillen tussen N-central en Kaseya zijn minimaal. De producten vertonen erg veel overeenkomsten met elkaar. Kaseya heeft ten opzichte van N-central een aantal extra functies in huis, echter heeft N-central meer mogelijkheden tot uitbreidingen van componenten als bijvoorbeeld: N-compass, audit manager, netflow manager, ed.

Lettend op de invulling van de standaard aanwezige functies ben ik ervan overtuigd dat N-central verder ontwikkeld is in de verschillende functies en daarom ook meer mogelijkheden biedt en technisch diepgaander is.

Wat verder de doorslag heeft gegeven voor de keuze voor N-central zijn onder anderen:

Automatisering onderhoud
N-central biedt uitgebreide mogelijkheden voor het automatiseren van terugkomend onderhoud zoals het uitrollen van patches, schijf opruimingen en defragmentatie. Bovendien valt dit verder uit te breiden door eigen scripts op te nemen. De functies voor automatisch onderhoud in N-central zijn behoorlijk uitgebreid en sluiten aan bij de wens naar geautomatiseerd beheer

Self-healing
De self-healing functie is een unieke functie die het mogelijk maakt standaard oplossingen voor problemen aan te geven in het systeem. Het systeem kan vervolgens eerst zelf actie ondernemen voordat er een beheerder wordt ingelicht.

Nette interface
N-central heeft een overzichtelijke interface welke de gewenste meldingen overzichtelijk weer kan geven. De interface ziet er ‘fris’ en nieuw uit en is eenvoudig om mee te werken.

Technisch diepgaand
Een van de eisen aan het pakket was dat het systeem technisch diepgaand moest zijn. De functies van N-central zijn ver ontwikkeld en zijn bovendien naar eigen wens nog verder te configureren en uit te breiden. Met de informatie die ik voorhanden heb gekregen, kan ik stellen dat ook hier N-central verder gaat dan Kaseya.

Productondersteuning
N-able heeft na de aanschaf van N-central uitgebreide trajecten ter ondersteuning van de MSP, niet alleen op het gebied van implementatie, maar biedt ook complete ondersteuning in het traject naar Managed Services.

Duidelijke reporting met N-compass (Report manager)
De N-compass uitbreiding maakt het mogelijk uitgebreide rapportages te maken van systemen voor de klant. Dit kan Hupra helpen met het onderbouwen en verantwoorden van de SLA’s. De rapporten van N-compas zien er strak en professioneel uit, deze zouden zonder aanpassingen direct naar de klant gestuurd kunnen worden. Het belang van deze rapportages is groot. De klant moet gevoel houden bij wat Hupra precies voor hem doet. Dit is de enige manier om dat inzichtelijk te maken.

Schaalbaarheid

Het door N-able gehanteerde licentie model maakt het mogelijk het systeem onbeperkt te laten groeien. Met de indeling van agent licenties voor de verschillende doeleinden gaat er minder geld 'verloren'. Bij het licentie model van Kaseya bijvoorbeeld, waar voor iedere agent hetzelfde bedrag wordt betaald, kan men zich afvragen of het nodig is de volledige prijs te betalen terwijl er alleen maar een werkstation wordt gemonitord.

N-central is in mijn ogen niet alleen verder ontwikkeld, het product sluit ook beter aan bij Hupra als bedrijf. Daarnaast wordt er een interessant licentiemodel gehanteerd. Door de verschillende prijzen voor servers, werkstations, netwerk modules en Essentials licenties, kan bij de aankoop van de licenties precies afgestemd worden op wat benodigd is, zo wordt nooit teveel of te weinig betaald. Voor N-central als product hoeven geen kosten betaald te worden. Voor ieder te monitoren apparaat dient een licentie te worden aangeschaft, afhankelijk van het type apparaat. Deze licentie wordt eenmalig gekocht. Na het eerste jaar worden kosten voor onderhoud en support op de licentie gevraagd, dit is beduidend minder dan het aankoopbedrag.

Als we dit vergelijken met een simpel model zoals Kaseya hanteert, worden de verschillen al snel zichtbaar. Kaseya hanteert een model waarbij eenmalig een bedrag voor het pakket wordt betaald. Daarnaast moet er per 24 maanden een bedrag voor de agent licenties worden betaald. Op het eerste gezicht lijkt Kaseya goedkoper maar omdat de terugkomende investering veel hoger is wordt Kaseya al snel duurder dan N-central.

	Eenmalige investering	Terugkomende investering (per maand)	Investering na 12 maanden	Investering na 24 maanden
N-central	€ 40.580,-	€ 677,- (vanaf jaar 2)	€ 40.580,-	€ 48.700,-
Kaseya	€ 4.500,-	€ 2.333,-	€ 32.500,-	€ 60.500,-
GFI MAX RemoteManagement	€ 1.660,-	€ 1.707,-	€ 22.144,-	€ 42.628,-

Tabel 6: Vergelijking kosten (500 licenties, voor details zie bovenstaande tabellen)

Ik adviseer Hupra N-able aan te schaffen. De eenmalige investering is wat groter waardoor de drempel wat hoger zal liggen, echter zal dit zich snel terugbetalen vanwege het flexibele licentie model van N-central. Uiteindelijk zal N-central vele malen goedkoper zijn dan een product als Kaseya.

Als laatste adviseer ik Hupra na te denken over de mogelijke uitbreidingen van N-central. In het bijzonder N-compass en de Backup Manager. N-compass is een erg handige uitbreiding voor het maken van rapportages ter ondersteuning van de SLA's en kan een enorm voordeel hebben bij verkoop en binding van de huidige klanten.

4.2. Inzet ondersteunende software

Om zeker te kunnen zijn van een betrouwbare werking van het pakket zal men goed moeten nadenken over een aantal belangrijke aspecten welke komen kijken bij de inzet van een dergelijk pakket. De basisinrichting van het pakket zal niet heel spannend worden, deze basis configuraties gaan in bijna alle omgevingen direct werken. Echter is het wel belangrijk om na te denken over zaken als beschikbaarheid van het management pakket.

4.2.1. Beschikbaarheid

Een dergelijk pakket en server zal altijd beschikbaar moeten zijn om te voorkomen dat er onbetrouwbare meldingen naar de beheerders worden gestuurd. Het is aan te raden de locatie van de centrale server te voorzien van meerdere internetverbindingen. Daarnaast zal de server moeten worden uitgerust met technieken als UPS en High Availability.

Deze problemen kunnen worden opgevangen door gebruik te maken van de reeds aanwezige virtuele omgevingen van Hupra. Daarnaast zijn op locatie twee verbindingen aanwezig. Bij uitval van de primaire lijn is er een terugvalmogelijkheid voor de tweede lijn, deze is weliswaar langzamer, maar zal wel een goede beschikbaarheid van de server kunnen garanderen.

Een tweede mogelijkheid is het verplaatsen van de server naar een data center. Hiermee worden de meeste onzekerheden betreffende beschikbaarheid weggenomen. Bovendien zal een dergelijke oplossing voor meer stabiliteit zorgen. Daarnaast kan het voor het gebruik van bepaalde product features wenselijk zijn over een data center locatie te beschikken. Het verplaatsen naar een data center zal voor Hupra pas in de toekomst interessanter worden als er meer klanten aan het pakket worden gekoppeld.

4.2.2. Notificaties

Een tweede kritiek punt bij de werking van de server zal de inrichting van notificaties zijn. Een van de belangrijkste functies van het pakket zal immers het informeren van de beheerders zijn. Het is belangrijk dat alle meldingen bij de juiste beheerders terecht komen, maar het is ook prettig als dit alleen belangrijke meldingen zijn. Om te voorkomen dat de beheerders overspoeld worden met “nutteloze” informatie, moeten er duidelijk plannen komen voor de implementatie en configuratie van notificaties.

Een aantal grote lijnen die men hierin kan trekken zijn bijvoorbeeld het indelen van meldingen op prioriteit. Zo zal server uptime een belangrijk punt worden, daarnaast is het bijvoorbeeld minder belangrijk als de processor van de server zwaar belast wordt. Dit is geen prettig probleem, maar zolang de server nog beschikbaar is, heeft het niet direct prioriteit. Deze indeling zal moeten worden gemaakt op de impact dat een bepaald probleem heeft op de bedrijfscontinuïteit.

Daarnaast zullen er keuzes moeten worden gemaakt over de manier van notificatie. Het is mogelijk de beheerders een mail te sturen, wat de meest gebruikte manier van informeren zal zijn. Daarnaast is het ook nog mogelijk om de beheerders een sms te sturen, of zelfs te bellen. Dit zal in extreme situaties of bij uitval van servers een gewenste methode kunnen zijn. De laatste optie is notificaties weergeven op een Dashboard. Deze dashboards kunnen vervolgens weer worden afgestemd op het type beheerder en de toegewezen verantwoordelijkheden.

Omdat in deze fase nog geen definitieve uitspraken kunnen worden gedaan over de configuratie van notificaties zal deze configuratie later beschikbaar komen in een apart document. Als de definitieve keuze van het pakket bekend is, zal ook meer kunnen worden ingezoomd op de specifieke configuratie.

4.2.3. Service templates

Verder zullen er duidelijke plannen moeten komen waarin wordt vastgelegd welke services moeten worden gemonitord. Dit zal afhankelijk zijn van het type machine dat wordt gemonitord. Hiervoor zullen templates worden opgesteld. Zo zullen bijvoorbeeld voor alle Windows servers een aantal vaste punten worden gecontroleerd als:

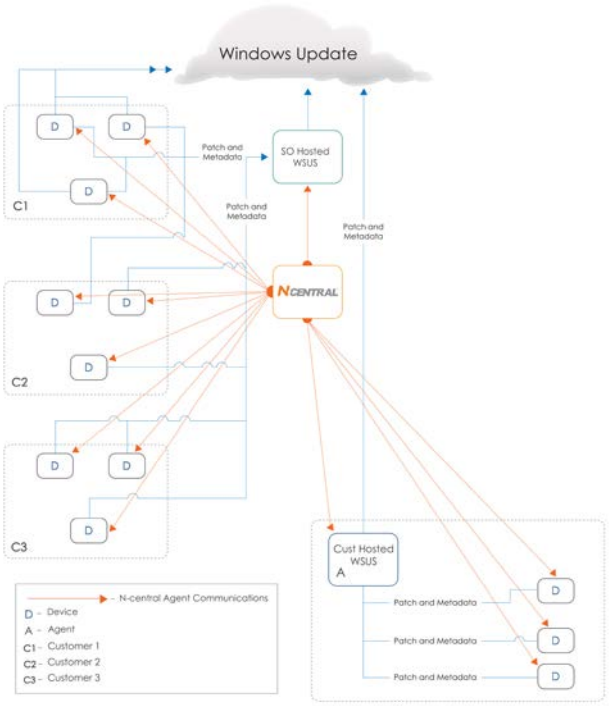
- Processor
- Geheugen
- Harde schijf status
- Patch status
- Beschikbaarheid
- Event Logging

Daarnaast zullen een aantal templates moeten worden opgesteld voor bijvoorbeeld het monitoren van de backups. Op dit moment worden daarvoor Symantec Backup Exec, Acronis Backup & Recovery en Solcon Online Backup gebruikt. Verder zullen er templates nodig zijn voor het monitoren van de geplaatste firewalls en templates voor het controleren van de onderhoudsprocessen.

Naast een overzicht van welke services precies gecontroleerd dienen te worden, moet er ook duidelijk worden vastgesteld wat de bijbehorende thresholds zijn bij de te monitoren services en wat de prioriteit van een service is.

4.2.4. Patch management

Om enige vorm van patch management te kunnen implementeren, is er nagedacht over 3 verschillende vormen van patch management welke in N-central kunnen worden geconfigureerd. Er is een mogelijkheid tot downloaden van de Microsoft Update Server, een WSUS server gehost door de MSP en een WSUS server op locatie van de klant. In onderstaande figuur 1 wordt een overzicht gegeven van de 3 oplossingen.



Figuur 1: Overzicht patch management architectuur

In onderstaande tabel wordt een advies gegeven over welke oplossing wanneer in te zetten. De oplossing WSUS gehost bij de MSP wordt niet gebruikt. Het voegt voor Hupra niets toe om een doorgeefluik van patches te worden. Dit kost alleen maar bandbreedte.

Tabel 7: Afbakening architectuur keuze patch management

	0 – 10 Devices	10 > Devices
Patch architectuur	Gebruik maken van Microsoft Update Servers	WSUS server op locatie van de klant

Daarnaast is een keuze gemaakt voor het daadwerkelijke moment van het doorvoeren van de patches. Voor servers is dit moment zondag op maandag nacht gekozen, omdat hier mogelijk een herstart bij betrokken is. Mocht er dan iets fout gaan in het proces dan kan er maandagochtend meteen een beheerder klaarstaan. Op deze manier zal de downtime bij problemen beperkt blijven tot een minimum.

Voor werkstations is gekozen de patches iedere werkdag om 11:00 uur door te voeren. Op dat moment is de grootste kans dat alle machines aanwezig zijn en zijn ingeschakeld. Het kan zo nu en dan voorkomen dat een werkstation of laptop uitstaat of op dat moment niet aanwezig is in het netwerk. Daarom wordt het patch moment iedere dag herhaald, zodat het geen ramp is als deze een keer wordt gemist.

Tabel 8: Advies patch momenten

	Server	Werkstation
Tijdstip doorvoeren patches	Wekelijks op maandag 01:00 uur.	Iedere werkdag om 11:00 uur.

Het goedkeuren van de patches wordt opgenomen in de proces beschrijvingen. Deze zullen verder worden toegelicht in hoofdstuk 4.2.

4.2.5. Maintenance

Voor het uitvoeren van onderhoud moeten een aantal taken worden vastgelegd. Deze worden met de tijdsplanning in tabel 8 weergegeven. Er is bewust voor gekozen om de taken in het weekend uit te voeren, met voldoende tijd tussen de taken, zodat er zo min mogelijk overlap plaatsvindt.

Basis onderhoud zal bestaan uit een aantal basis taken, welke wekelijks dan wel maandelijks worden uitgevoerd. Deze taken zijn inzetbaar op servers en werkstations. De taken kunnen later uitgebreid worden met specifieke taken voor bijvoorbeeld Microsoft SQL servers. Onderstaande tabel geeft een overzicht van de planning van deze basistaken.

Tabel 9: Voorstel planning onderhoud

Taak	Frequentie	Tijdstip
Schijfopruiming (CCleaner)	1x per week	ZO 13:00 uur
Verwijderen Temp Files	1x per week	ZO 13:15 uur
Defragmentatie (alle partities)	1x per week	ZO 13:30 uur
Volledige virus scan (Endpoint Security)	1x per week	ZO 18:00 uur
Schijfcontrole (CHKDSK)/ Geplande herstart	1x per maand	Eerste ZA 23:00 uur

De keuze voor deze wekelijkse herhaling van de taken zal ook als voordeel hebben dat de systemen goed “bij blijven”. Door deze taken wekelijks uit te voeren, zullen deze uiteindelijk sneller verlopen, denk bijvoorbeeld aan de defragmentatie. De taak schijfcontrole hoeft maar één keer per maand uitgevoerd te worden, vanwege de tijd die deze controle in beslag neemt en de server onbereikbaar zal zijn.

4.3. Procedures/Processen

Hieronder wordt een advies betreffende de implementatie van procedures en processen bij gebruik van MSP software binnen Hupra aangedragen. Een aantal van deze zaken zullen later in het project, bij de test en implementatie mogelijk worden aangevuld en uitgewerkt. De ondergenoemde procedures zijn lichtelijk ingedeeld naar ITIL standaarden. Er is voor gekozen alleen bepaalde onderdelen uit deze standaard te gebruiken. Voor een volledige implementatie heeft het bedrijf te weinig medewerkers. De processen zijn ingedeeld aan de hand van de verschillende ITIL onderdelen: Incident management, problem management, configuration management, change management en release management. Om dit hoofdstuk af te sluiten wordt kort aandacht besteed aan rapportage en de planning van een aantal procedures/processen.

4.3.1. Incident Management

Verantwoordelijkheden

Bij het optreden van een incident is het verstandig een aantal zaken van te voren duidelijk te hebben betreffende de verantwoordelijkheden. In eerste instantie zullen in het geval van Hupra alle beheerders een melding ontvangen. Mocht Hupra in de toekomst de beschikbaarheid krijgen over meer beheerders dan kan de overweging worden gemaakt groepen te maken op gebied van specialiteiten. Zo kunnen bijvoorbeeld in het geval van een netwerkstoring alleen de netwerk beheerders worden ingelicht.

Oppakken incident

In het geval van Hupra zullen alle beheerders een melding ontvangen. Het is aan te raden dat de eerst beschikbare beheerder het probleem oppakt en deze in het software pakket de status ‘Acknowledged’ geeft. Dan zullen er verder geen berichten over dat specifieke probleem worden gestuurd totdat het probleem wordt afgesloten. Op deze manier wordt het voor de andere beheerders ook duidelijk of het probleem reeds opgepakt is.

Meldingen van kritieke problemen zullen direct naar de beheerders gemaild worden of worden ingelicht via SMS. Problemen welke niet kritiek zijn, zullen alleen verschijnen in het zo geheten Dashboard. Beheerders op kantoor zullen vanuit dit dashboard werken en “tussendoor” de minder kritische problemen oplossen.

Van de meest kritische meldingen zal meteen een ticket worden aangemaakt in het ticket systeem OFB, als deze koppeling gerealiseerd is. Meldingen die worden opgepakt vanuit het dashboard moeten handmatig worden aangemaakt in het ticket systeem. Alle incidenten en problemen welke binnenkomen via N-central moeten worden aangemaakt als een ticket voordat het incident opgepakt mag worden. Er mag dus niet gewerkt worden aan een opgemerkt probleem zonder dat hiervan een ticket aanwezig is in het systeem.

Vanwege de beperkingen van OFB zal het incident eerst in N-central Acknowledged moeten worden, daarna kan er verder worden gewerkt in het ticket van OFB. Er is geen terugkoppeling naar N-central. Deze beperking kan worden weg genomen door over te stappen naar een systeem als AutoTask, welke deze integratie wel biedt.

4.3.2. Problem Management

Terugkomende problemen

Voor terugkomende problemen met bijvoorbeeld hardware kan worden besloten de meldingen op deze service stop te zetten. Een voorbeeld hiervan is bijvoorbeeld een processor welke aan de top van zijn belasting zit. De klant weet hiervan af en er is in overleg besloten dat de server over een aantal maanden vervangen gaat worden voor een server met meer capaciteit. Om te voorkomen dat deze melding terug blijft komen, wordt het treshhold van de service verwijderd. De service wordt nog wel gecontroleerd, maar er zullen geen meldingen meer worden verstuurd en er zullen geen tickets worden aangemaakt.

Het is van belang deze aanpassing duidelijk te noteren in het ticket systeem en in het geval van een migratie het ticket toe voegen aan de migratie afspraak in de agenda. In bovengenoemde situatie moet bij vervanging van de server deze instelling weer ongedaan worden gemaakt.

Daarnaast moet bij het uitschakelen van de threshold een description worden toegevoegd in N-central. Deze description moet aan het volgende format voldoen:

“Threshold off: <service> - <rede van uitschakeling> - <datum ingang> - <verwachte einddatum>”

Deze descriptions worden met een N-central filter gefilterd op de tekst “threshold off”. Vervolgens worden deze machines weergegeven in een lijst. Deze lijst kan bijvoorbeeld één keer in de twee maanden worden gecontroleerd of de uitschakeling van de thresholds nog gegrond is, of dat deze weer ingeschakeld moeten worden.

Oppakken escalaties

Voor terugkerende incidenten of incidenten welke geëscaleerd zijn, moet een monteur worden gepland voor de klant. Er wordt nu niet vanuit het dashboard gewerkt maar de monteur krijgt in zijn agenda geplande tijd om het probleem (op klant locatie) te onderzoeken. Indien nodig kan dit worden herhaald totdat er een oplossing voor het probleem is. Resultaten en uren worden allemaal gedocumenteerd in het bijbehorende ticket.

4.3.3. Configuration Management

Asset informatie

De asset informatie uit het MSP systeem kan worden gebruikt om de CMDB aan te vullen met accurate informatie over systemen. In sommige gevallen kan de asset informatie op zich al een vervanging voor een CMDB zijn, echter is dit niet aan te raden vanwege het gebrek om zelf informatie toe te voegen aan de asset informatie en het gebrek aan toevoeging van configuratie.

Bewaking correctheid informatie

De Asset informatie van systemen in de MSP software dient gecontroleerd te worden op correctheid om te voorkomen dat er misverstanden optreden bij het beheer van de machine. Denk bijvoorbeeld aan het aanschaffen van extra geheugen modules voor een server. Als men dit vanuit de MSP software wil doen, moet men er zeker van kunnen zijn dat de informatie correct is.

Dit process zal ook raakvlakken hebben met change management. Bij iedere wijziging aan het systeem moet worden gecontroleerd of de asset informatie nog correct is en desnoods handmatig worden ingevoerd.

Naamgeving systemen
Systemen worden onder een standaard naamgeving toegevoegd. Dit is om duidelijkheid te verschaffen in N-central. Aan de naam van een systeem kan direct worden uitgelezen wat de primaire functies van dat systeem zijn. Deze naamgeving is vastgesteld op het volgende: functie-klant-nummer.

Functies kunnen zijn:

- FS – File/Print/AD/DNS Server (Algemeen)
- TS – Terminal Server
- DB – Database Server
- NC – N-central
- RM/BM – Report Manager/ Backup Manager
- PC – PC
- NB/LP – Notebook/Laptop

Een voorbeeld van naamgeving kan zijn: FS-HUPRA-01.

Software/ Licence Appliance
De functies Software applicance en Licence applicance zijn bijzonder handig voor het beheren van de software bij een klant. Met software applicance kan worden afgedwongen welke software op het system aanwezig moet/mag zijn. Vervolgens zullen meldingen worden weergegeven. Dit is eigenlijk een geautomatiseerd proces. Bij een normale werking is er geen tussenkomst van een beheerder nodig.

Met de Licence appliance functie kunnen controles op de licenties van de in het netwerk geïnstalleerde software worden uitgevoerd. Deze kunnen vervolgens vergeleken worden met de ingestelde licentie configuratie voor de betreffende klant. Hiermee kan de correctheid van de licenties binnen het netwerk worden gecontroleerd en worden onderhouden.

4.3.4. Change Management

Inplannen down time
Onderhoud aan een of meerdere servers dient vooraf te worden ingepland als server down time. Dit om te voorkomen dat tijdens werkzaamheden beheerders overspoeld worden met nutteloze mail. Hiermee wordt ook voorkomen dat beheerders tijd gaan besteden aan een probleem dat eigenlijk niet bestaat. Als de uiteindelijke koppeling met het ticket systeem tot stand is gekomen, wordt dit proces extra belangrijk. Onnodige notificaties betekend onnodige tickets. Het uitzoeken van deze tickets en het sluiten van de valse meldingen zal extra tijd kosten.

Patch approval
Patch approval dient als belangrijk onderdeel van Change Management te worden opgenomen. Het doorvoeren van patches kan gevolgen hebben voor de betreffende systemen, daar moet in het patch approval proces rekening mee worden gehouden. De architectuur van de patch omgeving en de afspraken betreffende de patch momenten zullen later worden gespecificeerd. Het patch approval proces zal na iedere grote patch release moeten worden uitgevoerd. Vanuit Microsoft is dit meestal de derde dinsdag van de maand.

Controle correctheid service templates
Bij wijzigingen aan servers moet worden gecontroleerd of de ingestelde services en service templates nog wel overeenkomen met de functies die de server vervuld. De informatie kan meteen worden aangepast in het MSP pakket door de juiste service templates toe te wijzen, of onnodige service templates te verwijderen.

4.3.5. Release Management

Software Deployment
Software Deployment kan worden uitgevoerd via de MSP pakketten of via een Group Policy. Het is belangrijk om ook na een deployment te controleren of de service templates nog aansluiten bij de servers/werkstations. Indien nodig kunnen deze aangepast worden. Een software deployment moet altijd eerst op een testomgeving worden uitgevoerd.

Toevoegen nieuwe systemen/klanten
Voor het toevoegen van nieuwe klanten of systemen bij bestaande klanten is een checklist ontwikkeld van de te nemen acties en de standaard instellingen voor de nieuwe systemen. Daarna zal moeten worden gecontroleerd of de juiste service templates zijn toegepast en indien nodig aangepast moeten worden. In dit proces moet ook het juiste aantal licenties voor de klant geconfigureerd worden. In de checklist is dit verder omschreven.

Patch management
De release fase van het patch management zal een geautomatiseerde fase zijn. Het goedkeuren van de patches valt onder change management. De releases zullen dan wel geautomatiseerd verlopen, echter is het wel belangrijk om hiervan goed op de hoogte te zijn en vooraf te onderzoeken wat voor gevolgen het doorvoeren van de patches kan hebben voor de bestaande software.

Updates N-central server
Er moet regelmatig (1x per maand) worden gecontroleerd of er nieuwe releases, service packs of hotfixes beschikbaar zijn voor de N-central server. Deze updates kunnen vervolgens worden geëvalueerd en worden toegepast. Voor deze evaluatie kan men gebruik maken van de testomgeving. Daarnaast zal natuurlijk een backup van de N-central configuratie moeten worden gemaakt. De procedure voor een N-central server update is beschikbaar in het N-able Resource Center.

4.3.6. Reporting

Reporting is voor een MSP een belangrijk onderdeel. Omdat de MSP de problemen voor de klant op de achtergrond probeert te houden, heeft de klant veel minder inzicht in wat er daadwerkelijk gedaan wordt. Het is daarom belangrijk de klant dat inzicht terug te geven in de vorm van een rapportage.

Rapportage kan met de meeste MSP producten volledig geautomatiseerd en aangepast worden. Deze rapportages moeten als onderdeel van de factuur worden meegestuurd om de klant extra inzicht te geven in haar omgeving. Rapportage is ten minste nodig op de volgende onderwerpen.

Service Level Management/ Availability Management
Geeft een overzicht van de behaalde beschikbaarheid van de systemen waarover een Service Level Agreement is afgesloten. Tevens zal dit overzicht inzicht geven in of de afgesproken SLA is gehaald en waar het eventueel fout is gelopen.

Service Continuity Management
Dit rapport geeft een overzicht van de incidenten die de afgelopen periode zijn opgetreden en zijn waargenomen door het MSP pakket. Daarnaast zal dit pakket een goede aanvulling zijn op de werkzaamheden opgenomen in de factuur.

Backup Report (Backup Manager)
Voor klanten die een Managed Backup oplossing afnemen, moet iedere maand een Backup rapport worden aangeleverd. Dit rapport zal de klant een overzicht geven van de conditie van de backup. Dit rapport bevat een overzicht van alle backup taken en de bijbehorende status. Daarnaast geeft het overzichten van de grootte van de backup, tot hoever men kan herstellen en de beschikbare ruimte op de doel locatie en of hier in de toekomst uitbreiding nodig is.

Capacity Planning Report (Report Manager)
Als extra aanvulling op deze drie basis rapporten kan er ook worden besloten een rapport voor Capaciteitsbeheer toe te voegen. Dit rapport is alleen beschikbaar in de Report Manager uitbreiding. Dit rapport zal de klant inzicht geven in de gebruikte capaciteit (Processor, Harde schijf, Geheugen en Netwerkverkeer) en eventuele toekomstige problemen met machines die hun maximum bijna bereikt hebben.

Endpoint Security/ Firewall incident (Report Manager)
Ook dit rapport zal alleen beschikbaar zijn in Report Manager. Er kan worden overwogen dit rapport als extra toe te voegen. In dit rapport wordt een overzicht gegeven van alle meldingen uit de SonicWall firewalls en alle Endpoint Security systemen en zal een totaal overzicht geven van de beveiliging van het netwerk.

4.3.7. Planning

Nu er een kort overzicht is gegeven van wat voor procedures er komen kijken bij het proactieve beheer, wordt er nog even ingegaan op de initiatie van deze procedures. Een aantal procedures geïnitieerd uit een bepaalde gebeurtenis, zoals een incident of een aanpassing.

Andere procedures worden automatisch uitgevoerd, bijvoorbeeld de maandelijkse rapportage. Voor deze procedures is minimale aandacht van de beheerder nodig.

Een derde vorm zijn procedures die “uit het niets” moeten worden geïnitieerd. Hiervoor is discipline nodig. Procedures als het onderhoud aan de N-central server en patch approval zullen één maal in een bepaalde periode moeten worden uitgevoerd. In figuur 2 hieronder is een voorbeeld gegeven van een dergelijke planning. Het is aan te raden deze taken te plannen als interne opdrachten in de agenda’s van beheerders. Het is goed om deze zaken gestructureerd in te plannen, anders wordt het vergeten.

In het voorbeeld is een planning gemaakt voor het onderhoud van de N-central server en het patch approval proces. In het voorbeeld wordt de eerste vrijdag van de maand aangehouden voor onderhoud van de server en controle voor N-central updates. Het patch approval proces wordt iedere vrijdag na Patch Tuesday gestart.

maandag	dinsdag	woensdag	donderdag	vrijdag	zaterdag	zondag
april 30	mei 1	2	3	4	5	6
				Onderhoud N-central		
7	8	9	10	11	12	13
	Patch Tuesday			Patch approval		
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31	juni 1	2	3

Figuur 2: Voorbeeld planning procedures

5. Conclusie

Dit adviesrapport bouwt verder op het eerder uitgevoerde productonderzoek en de resultaten daarvan. Om Hupra tot een succesvol MSP te maken, zijn een aantal veranderingen nodig. Voor deze veranderingen kunnen grofweg vier aanpakken worden gekozen: vasthouden aan het huidige model, inzetten van monitoring, implementatie van een proactief model en implementatie van een proactief model met ondersteunend MSP pakket. Deze laatste optie is het meest compleet en biedt ook de beste basis voor eventuele verdere ontwikkelingen.

Hupra stelt wel een aantal eisen aan dit proactieve model en het MSP pakket. Deze eisen en/of verwachtingen zijn vastgesteld in overleg met de opdrachtgever en interviews met een aantal werknemers van Hupra. Deze zijn afgenomen onder werknemers van verschillende disciplines, zoals consultants, beheerders, maar ook sales & marketing.

Na het vaststellen van deze eisen is onderzocht welk pakket hierbij het beste aansluit en het beste bij Hupra past. Hiervoor zijn in het document 'Productonderzoek' de pakketten N-central, Kaseya en GFI Max Remote Management vergeleken. De vergelijking op functionaliteit is in dit rapport uitgebreid met een financiële vergelijking en een advies over het aan te schaffen product.

	Eenmalige investering	Terugkomende investering (per maand)	Investering na 12 maanden	Investering na 24 maanden
N-central	€ 40.580,-	€ 677,- (vanaf jaar 2)	€ 40.580,-	€ 48.700,-
Kaseya	€ 4.500,-	€ 2.333,-	€ 32.500,-	€ 60.500,-
GFI MAX RemoteManagement	€ 1.660,-	€ 1.707,-	€ 22.144,-	€ 42.628,-

Tabel 10: Financiële vergelijking

Uit deze financiële vergelijking komt het pakket GFI Max Remote Management als goedkoopste oplossing. Als deze uitkomsten vergeleken worden met de uitkomsten van de functionele vergelijking uit het productonderzoek, kan worden gesteld dat N-central de beste prijs/functionaliteit verhouding heeft.

	N-Central	Kaseya	GFI MAX Remote Management
Totaal	104 / 70,4	104 / 65,5	53 / 34,0
Gemiddelde	**4,3 / 2,9**	**4,2 / 2,6**	**4,1 / 2,6**

Tabel 11: Functionele vergelijking

GFI MAX RemoteManagement is al snel afgevallen omdat dit pakket simpelweg maar een beperkt aantal functies heeft in vergelijking met Kaseya en N-central behoorlijk achterblijft en minder technisch diepgaand is. De verschillen tussen N-central en Kaseya zijn minimaal. Lettend op de invulling van de standaard aanwezige functies valt te concluderen dat N-central verder ontwikkeld is. Het advies aan Hupra is daarom gebruik te gaan maken van N-central, met uitbreidingen voor de toekomst behouden.

Naast de keuze van het pakket is Hupra ook geadviseerd over de inzet hiervan. Zo zal een overweging voor de toekomst zijn de N-central server in een data center te plaatsen, ter verbetering van de beschikbaarheid. Naast adviezen over beschikbaarheid zijn service templates en een aantal pakket functies besproken.

Als laatste is Hupra geadviseerd over de in te zetten procedures. Deze procedures zijn opgesteld om het werk en het beheer van en met N-central duidelijk en consistent te krijgen. Belangrijk hierbij zijn bijvoorbeeld de processen voor het oppakken van een incident en het afhandelen van hardware problemen. Daarnaast zijn standaard taken beschreven, als het inplannen van down time bij het uitvoeren van onderhoud. Daarnaast is er een advies gegeven over de planning van onderhoudsprocessen. Deze processen verschillen van de standaardprocessen in die zin dat deze op geplande tijdstippen gestart moeten worden, waar de standaard processen gestart worden door een andere activiteit. Het is voor Hupra belangrijk hier aandacht aan te besteden om te voorkomen dat deze geplande processen vergeten worden.

De adviezen over inzet en de geadviseerde configuraties zullen in de testfase worden onderworpen aan een aantal tests op werking en mogelijke verbetering. Configuraties zullen in de testrapporten verder worden uitgewerkt waar nodig.

Bijlage H: Testrapport

Proactief beheer bij Hupra

Auteur:
M.M.J. de Weijer
Studentnummer: 1546128
Hogeschool Utrecht
Faculteit Natuur & Techniek
Systeembeheer

Bedrijf:
Hupra Automatisering
Hoofdstraat 105
3901 AK Veenendaal

Begeleiders:
Hupra: Dhr. P.A. Willemsen
Hogeschool Utrecht: Dhr. H. van Nimwegen

Afstudeerperiode:
februari 2012 - juni 2012

Versie: 1.1
Datum: 23 mei 2012

Versie beheer:

Versie	Datum	Wijzigingen
0.0	27-03-2012	Initiële versie document, geen inhoud
0.1	06-04-2012	Aanvullen informatie Testomgevingen
0.2	10-04-2012	Tests met basis installaties
0.3	15-04-2012	Configuratie Service Templates
0.4	25-04-2012	Notificaties, Patch management uitgewerkt
0.5	10-05-2012	Backup Manager en Maintenance uitgewerkt
1.0	20-05-2012	Verwerking feedback
1.1	23-05-2012	Afronden document, opmaak

Inhoud

1. Inleiding

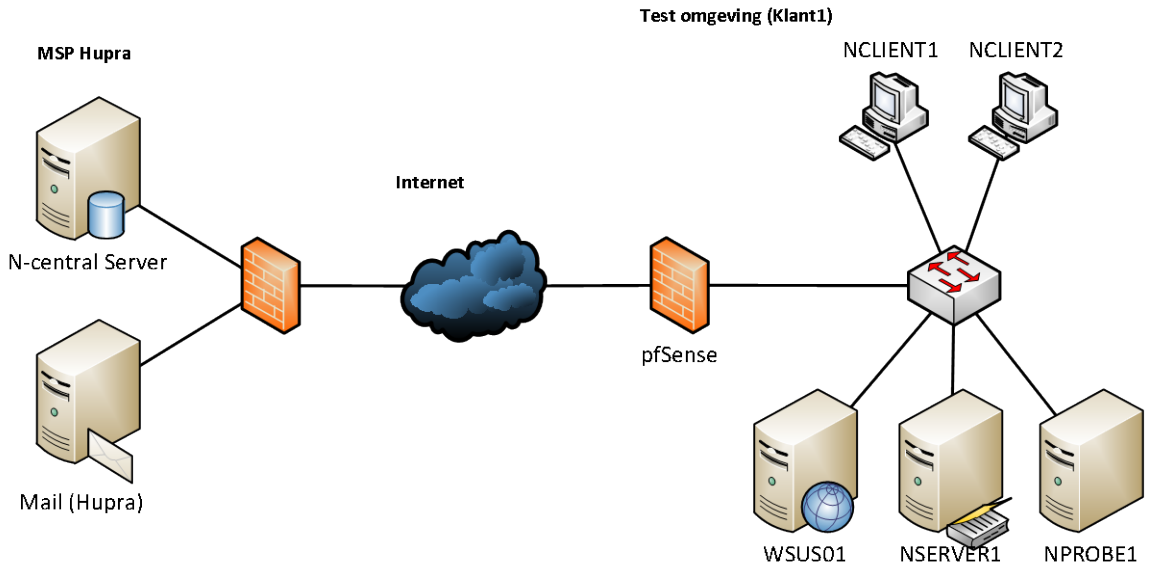
In dit document worden alle uitgevoerde tests beschreven en worden de resultaten en keuzes, gemaakt tijdens de uitvoering van deze tests, toegelicht. Deze tests hebben in het onderzoek centraal gestaan. Door middel van de tests is een basisconfiguratie samengesteld en is onderzocht en vastgelegd wat de beperkingen en pijnpunten van bepaalde onderdelen zijn. De resultaten van de tests zijn van groot belang geweest voor de uiteindelijke implementatie van N-central en bijbehorende onderdelen. Daarnaast hebben de tests gezorgd voor ervaring met de verschillende onderdelen. Deze ervaring is weer benut bij het opstellen van standaard procedures voor werking met N-central.

Alle tests met het product zijn uitgevoerd op een speciaal ontworpen testomgeving. Voor deze testomgeving is een tweede N-central server geplaatst. Voor het testnetwerk zijn zowel een schone virtuele omgeving en het “vuile” interne netwerk van Hupra gebruikt. Dit afhankelijk van de risico’s welke aan de tests kleven. Tests in een ver gevorderd stadium zijn later, in overleg met de klant, uitgevoerd op klant omgevingen. Dit alleen als alle risico’s zo goed als weggenomen waren.

De testomgevingen zullen in het eerste hoofdstuk ‘Testomgeving’ verder worden uitgewerkt en toegelicht. Er zal eerst een beschrijving worden gegeven van de testomgeving gevolgd door de beschrijvingen van de tests. Hoofdstuk 3 en 4 beschrijven de tests voor installatie op een schone en een vuile omgeving. In hoofdstuk 4 zullen ook zaken als configuratie en tests van service templates voor bijvoorbeeld de sonicwall worden uitgewerkt. Verder worden de tests voor Patch management, notificaties, backup, en onderhoud uitgewerkt. Eerst zullen de testomgevingen worden toegelicht.

2. Testomgeving

Allereerst is er een basis testomgeving ontwikkeld met een N-central server installatie bij Hupra (de MSP) en een aantal servers, werkstations en een probe. Deze omgeving is offsite geplaatst en zal benaderd moeten worden over een internet verbinding. Hiervoor is bewust gekozen om zo natuurgetrouw mogelijk een klantomgeving na te bootsen.



Figuur 1: Basis testomgeving (TestCustomer)

Deze basis testomgeving zal naast de productie omgeving blijven bestaan en zal gebruikt kunnen worden voor risicovolle tests. Overige tests kunnen worden uitgevoerd op de productie server, zolang deze tests geen directe gevolgen hebben voor de geïmporteerde klanten.

Overige tests worden als eerst uitgevoerd op de interne omgeving van Hupra (Figuur 2), waarna gekozen kan worden deze tests ook uit te voeren op een select aantal klanten, alvorens de aanpassingen over het gehele systeem te implementeren.

De N-central server is te downloaden van het N-able Resource Network en wordt aangeleverd als een ISO bestand voor installatie. Installatie van de N-central server is vrij rechttoe rechtaan. De installatie ISO bevat een door N-able aangepaste versie van Red Hat Enterprise Linux, welke voor geconfigureerd is en is uitgerust met alle benodigde software, aanvullende pakketten en configuraties.

Tijdens de installatie worden een aantal standaard vragen gesteld voor bijvoorbeeld netwerk configuratie, server naam, landinstellingen, enz. Na de installatie kan er meteen worden ingelogd met het administrator account, via de web interface. Na het aanpassen en toevoegen van gebruikers kan men meteen aan het werk met een basisconfiguratie van de server.

De configuratie van de server dient nog wel verder afgestemd te worden op de wensen van de organisatie. Verder zullen een aantal uitgebreide functies niet werken zonder aangepaste configuratie en zullen maatwerk oplossingen nog niet beschikbaar zijn, omdat deze nog moeten worden geschreven. Deze onderdelen zullen in de rest van dit document verder worden uitgewerkt.

3. Basis installatie

De test voor basis installatie houdt niet meer in dan het installeren van N-central, het toevoegen van een nieuwe klant (TestCustomer, Figuur 1) en het toevoegen van machines van deze klant. De machines van de klant zullen verschillende virtuele machines zijn, met verschillende operating systems, om zo veel mogelijk de verschillende aspecten van deze systemen te simuleren.

Het basis netwerk van TestCustomer is vergelijkbaar met een klein basis netwerk bij een zakelijke klant. Het netwerk zal bestaan uit een server met daarop Active Directory, DNS, DHCP en FileShares. Daarnaast zal er een server aanwezig zijn waarop de Windows Probe kan worden geplaatst. Aan de rand van het netwerk is een firewall geplaatst welke ook zal worden uitgelezen met N-central. Als laatste zijn er vanzelfsprekend een aantal werkstations aanwezig waarop de agent software kan worden getest.

Uitvoering van deze test verliep vrijwel vlekkeloos en resultaten zijn gebruikt voor het opstellen van richtlijnen voor procedures en de installatie checklist. Omdat deze test zo vlekkeloos verliep is er voor gekozen een volgende basis test uit te voeren op een “vuile omgeving”, een omgeving welke al een aantal jaar intensief gebruikt wordt.

Een aantal bijzonderheden uit de basis test:

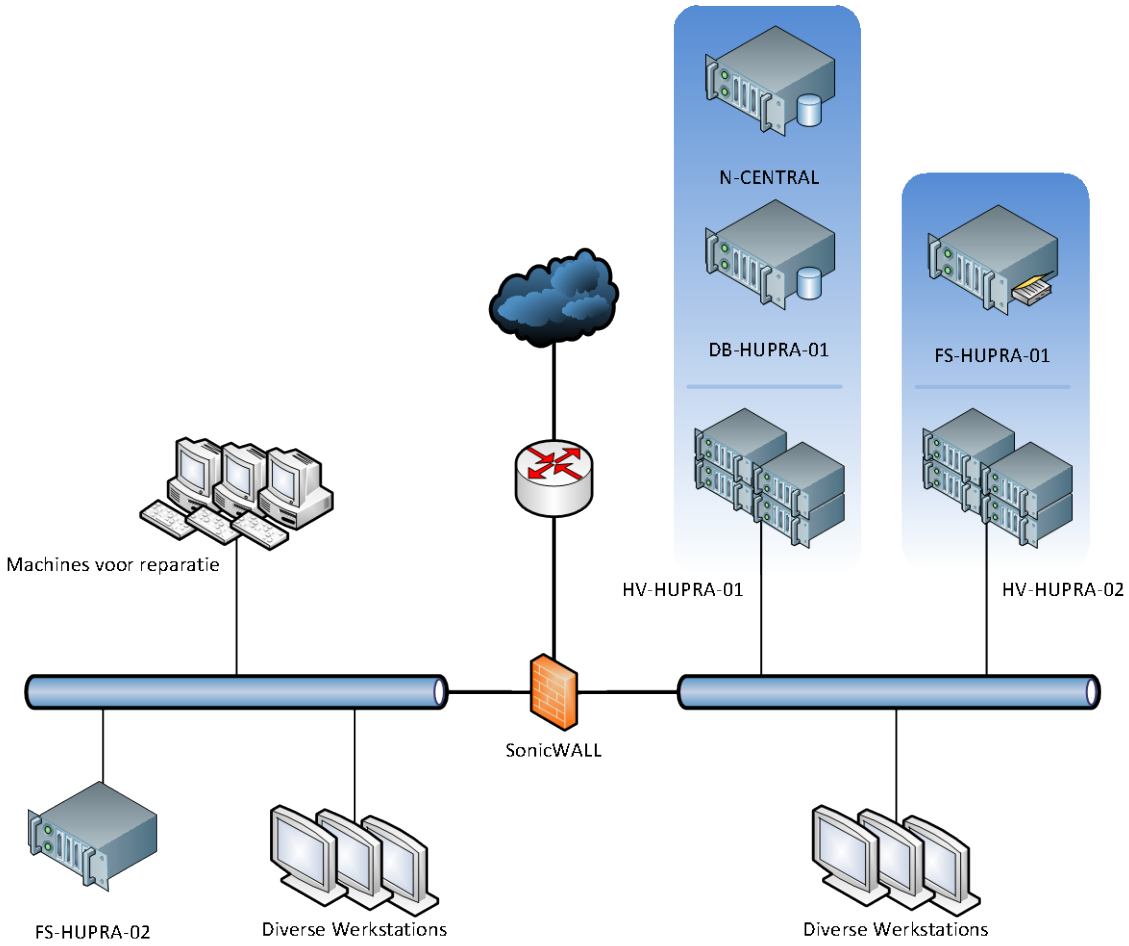
- Installatie op Windows server 2008 core niet mogelijk.
- Geen ondersteuning voor Windows 8 Server.
- Problemen bij automatische installatie in werkgroepen.

Hiervoor zijn geen directe oplossingen voorhanden. Het probleem met de Windows Server 2008 Core installatie is niet verder onderzocht en opgepakt, dit omdat binnen Hupra geen gebruik wordt gemaakt van dit type installatie. De ondersteuning voor Windows 8 Server wordt verwacht bij de release.

Voor de problemen met rechten in werkgroepen is een workaround. In dergelijke situaties kan het best de installatie van de agent software handmatig worden uitgevoerd. Er moet wel rekening worden gehouden met eventuele problemen met rechten die kunnen optreden bij het uitvoeren van geplande taken via N-central.

4. Basis installatie “Vuile omgeving”

De eerste test met N-central, het toevoegen van een klant met schone omgeving, heeft niet veel moeilijkheden opgeleverd. Als toevoeging hierop is besloten een extra test uit te voeren op een “vuile omgeving”. Hiervoor is het kantoor netwerk van Hupra gekozen (Figuur 2). Deze omgeving wordt “vuil” genoemd omdat deze al enkele jaren wordt gebruikt. Daarnaast zijn er veel verschillende configuraties aanwezig, zoals bijvoorbeeld het gebruik van verschillende virus scanners en verschillende instellingen voor Windows Updates.



Figuur 2: Omgeving Hupra

De installatie is uitgevoerd op basis van eerdere ervaringen en checklists gemaakt bij de basis installatie in de schone (TestCustomer) omgeving.

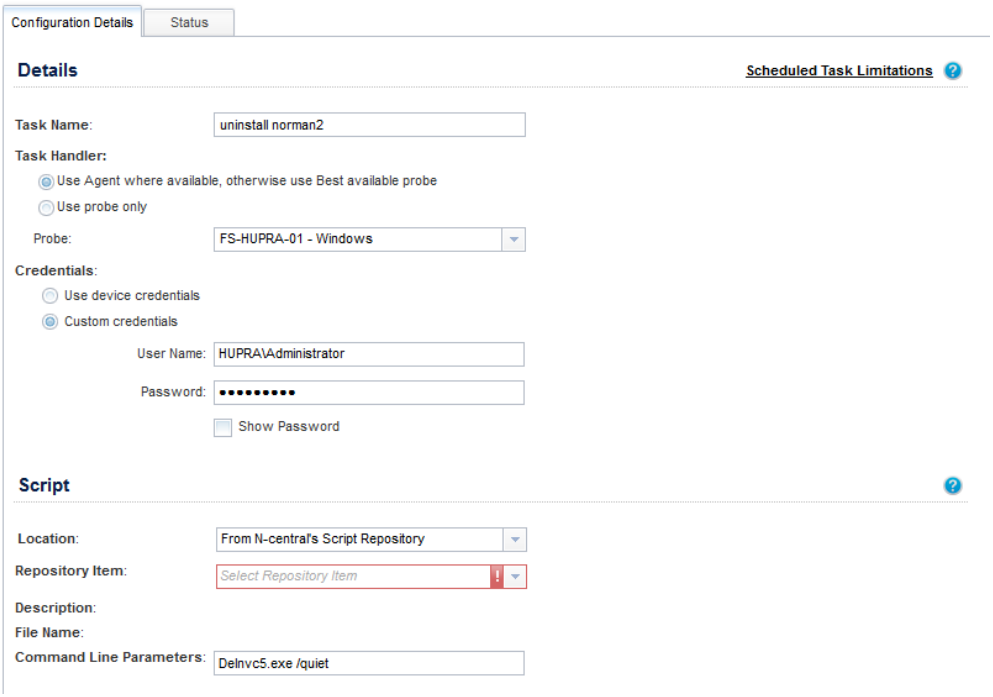
Bij het importeren van de machines uit de probe discovery zijn in de Hupra omgeving een aantal problemen aan het licht gekomen. Zo bleek dat een aantal machines niet correct in het domein waren opgenomen, waardoor het voor de probe onmogelijk werd om de agent software geautomatiseerd te verspreiden. Problemen hiermee waren snel en makkelijk op te lossen door deze machines als nog goed in het domein te configureren.

4.1. Endpoint Security

Een tweede probleem bij implementatie op de “vuile” omgeving was het gebruik van veel verschillende virus scanners. Voor een succesvolle uitrol van N-able’s Endpoint Security is een ‘schone’ machine zonder geïnstalleerde virus scanner vereist. Een aantal van de reeds geïnstalleerde virus scanners kon automatisch worden verwijderd. Echter voor Norman ging dit niet op. Hupra heeft voorheen altijd Norman verkocht aan zakelijke klanten, daarom zullen veel bestaande klanten een Norman product geïnstalleerd hebben welke bij overgang naar Managed Services vervangen moeten worden voor N-central Endpoint Security.

Er zijn meerdere mogelijkheden om de reeds geïnstalleerde virus scanner te verwijderen. Zo is het mogelijk op afstand in te loggen of fysiek achter de machine plaats te nemen. In beide gevallen zal de gebruiker moeten worden gestoord.

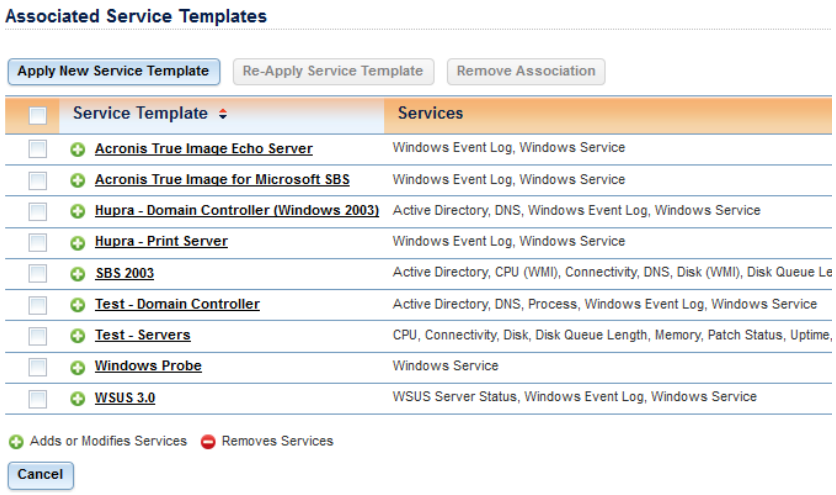
Alvorens over te gaan tot een van de hierboven genoemde oplossingen is een test uitgevoerd met de scripting functie van N-central in combinatie met wat programmatuur van Norman. Norman biedt op de site een klein stuk software aan voor geautomatiseerde verwijdering van de virus scanner. Dit programma delnvc5.exe kan worden uitgevoerd met een /quiet functie. Door deze taak geautomatiseerd te laten uitvoeren vanuit N-central, zijn zonder hinder van de gebruikers de laatste Norman installaties op de achtergrond verwijderd, waarna de Endpoint Security software van N-able geïnstalleerd werd.



Figuur 3: Verwijderen Norman

4.2. Service templates

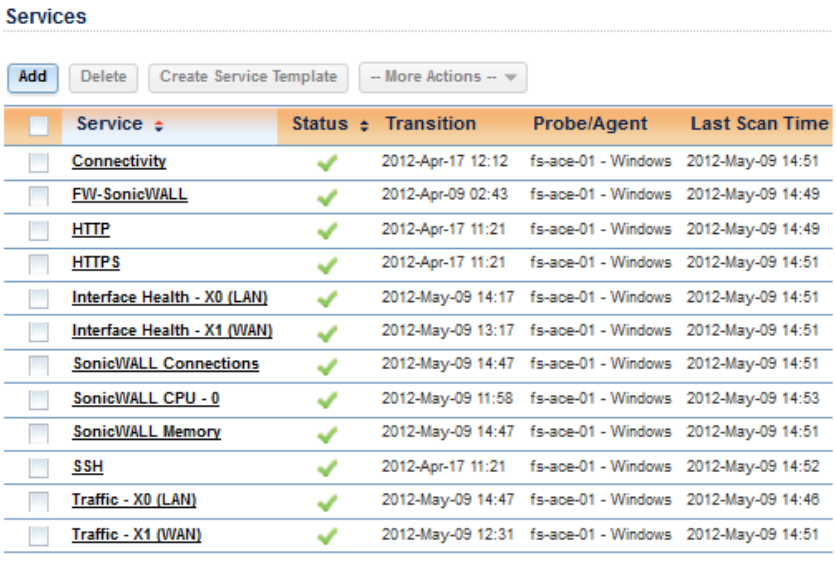
De standaard service templates aanwezig in N-central bieden voldoende mogelijkheden voor de basis monitoring van de systemen. Deze templates worden bij het ontdekken van een machine door de probe automatisch toegewezen aan de hand van zogeheten rules. Daarnaast zijn een aantal extra services als eventlogging en een aantal Windows services checks toegevoegd en ondergebracht in aanvullende templates.



Figuur 4: Service templates Windows Server

4.3. SonicWall

Zowel in de kantoor omgeving van Hupra, als in de omgevingen van haar klanten, wordt bijna altijd gebruik gemaakt van een SonicWall Firewall oplossing. N-central biedt een standaard template voor het monitoren van een SonicWall. Echter betrof dit alleen basis gegevens als connectivity en de beschikbaarheid van de management console. Deze services zijn d.m.v. een SMPT connectie uitgebreid om een veel completere lijst te krijgen met o.a. traffic informatie en inzicht in het aantal security incidents opgemerkt door de IPS van de SonicWall. Deze uitgebreide lijst is ondergebracht in een nieuw template, welke ook zal worden toegepast op de SonicWall systemen bij klanten.

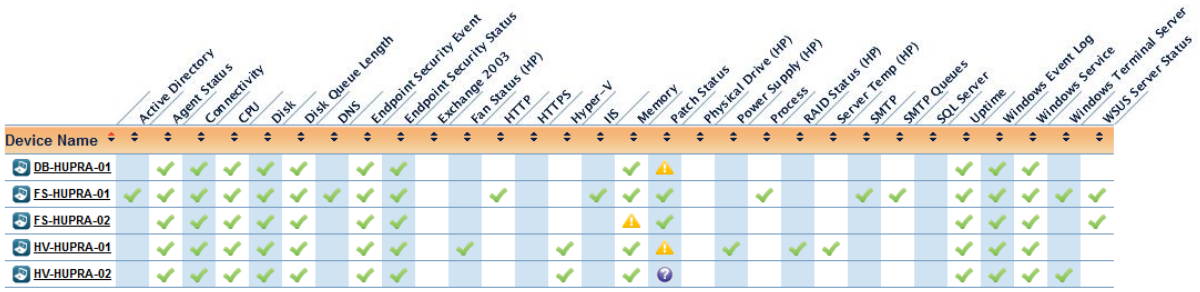


Figuur 5: SonicWall Monitoring

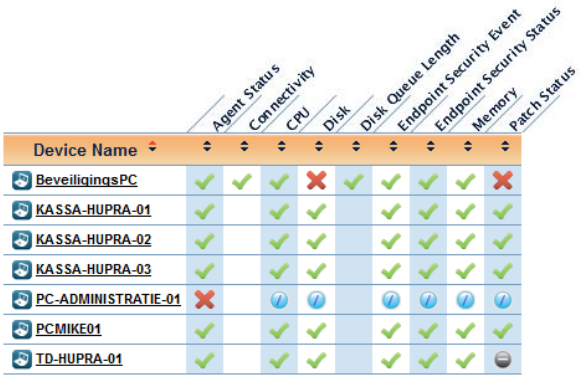
Daarnaast zijn er nog een aantal problemen aan het licht gekomen met wat instellingen van de Windows Update Service, deze zullen verder worden uitgewerkt in het hoofdstuk patch management.

Standaard instellingen van de Windows Firewall op nieuwere Windows versies staan een ping aanvraag standaard niet toe. De connectivity test van N-central is afhankelijk van deze ping test. Een aanpassing in de Windows Firewall voor het toestaan van icmp-echo aanvragen lost het probleem op.

Wat nieuw was in deze testomgeving is het monitoren van fysieke servers. N-central is in staat gegevens over de hardware, zoals fan, raid-controller, PSU, e.d. te monitoren. In de basis testomgeving (TestCustomer) zijn alleen tests uitgevoerd op virtuele machines. De configuratie van deze hardware monitoring heeft een paar kleine haken en ogen betreffende instellingen voor de monitor software van de fabrikant en de SNMP instellingen. Voor de configuratie op HP servers is een kort document opgesteld. Verder zullen deze instellingen ook te vinden zijn in de checklist 'toevoegen nieuwe klant'.



Figuur 6: Dashboard Hupra servers



Figuur 7: Dashboard Hurpa werkstations

5. Patch management

Het testen van Patch management is een tijdrovende taak. Op een selecte groep test servers/werkstations zullen een aantal test patch profielen worden geactiveerd. Deze profielen zullen verschillend zijn, zoals beschreven in het voorstel patch management.

Er zijn twee test profielen aangemaakt. Een profiel voor servers, welke een aangepaste instelling voor het patchmoment bevatten en daarnaast een aantal instellingen voor herstart en gebruikers notificatie en een profiel voor werkstations welke hun eigen aangepaste instellingen hebben voor het bovengenoemde. Daarnaast zijn er vergelijkbare profielen opgesteld voor gebruik van de Microsoft Update servers i.p.v. de WSUS servers op locatie.

Deze testprofielen zullen op een beperkt aantal servers worden toegepast en zullen meer patch momenten bevatten dan de productieprofielen. Dit om het proces enigszins te versnellen en te voorkomen dat men weken moet wachten voordat het resultaat onderzocht kan worden. De test profielen zullen handmatig worden verschoven voor installatie op servers rond 22:00 uur en voor werkstations iedere dag rond 11:00 uur om er zeker van te zijn dat deze ingeschakeld zijn.

Controle van het patch proces zal de volgende dag plaatsvinden. De status van dit proces kan worden uitgelezen via N-central, maar ook handmatig op de servers/werkstations zelf en de WSUS server op de betreffende locatie. Vervolgens kunnen er direct aanpassingen worden gemaakt die zullen worden meegenomen in de volgende patchronde (de volgende avond) totdat het proces na wens verloopt.

Status Details

Patch Summary	Value	State	Thresholds
Missing Patches	0	Threshold Off	--
Patches installed with errors	0	✔	Normal 0 - 0
			Warning 1 - 1
			Failed 2 - 255
Missing Patches by Category	**Value**	**State**	**Thresholds**
Security Updates	0	✔	Normal 0 - 0
			Warning 1 - 4
			Failed 4 - 4,294,967,296
Critical Updates	0	✔	Normal 0 - 0
			Warning 1 - 4
			Failed 4 - 4,294,967,296
Service Packs	0	✔	Normal 0 - 0
			Warning 1 - 4
			Failed 4 - 4,294,967,296
Update Rollups	0	✔	Normal 0 - 0
			Warning 1 - 4
			Failed 4 - 4,294,967,296
Feature Packs	0	Threshold Off	--
Updates	0	Threshold Off	--
Software Driver Updates	0	Threshold Off	--
Definition File Updates	0	Threshold Off	--
Tools Updates	0	Threshold Off	--
Unknown Updates	0	Threshold Off	--
Missing Patches That Were Approved Over 60 Days Ago	**Value**	**State**	**Thresholds**
Missing Patches Older Than 60 Days	0	Threshold Off	--
Additional Details	**Value**	**State**	**Thresholds**
Synchronizing From	http://10.0.1.1:80	--	--
Reboot Required	False	✔	Normal If Not Found
			Warning If Found

Figuur 8: Patch Status

De eerste doelen van het patch management zijn een complete inrichting en automatisering van de patchrondes, waarin alle machines worden meegenomen. Dat een machine niet helemaal up-to-date is, is geen probleem voor deze test. Het is belangrijker dat de machine meeloopt in het patch proces. Daarna is het een kwestie van tijd voordat de machine helemaal up-to-date zal zijn.

Verder zijn de volgende punten getest:

- Deelname aan het patch proces (handmatige controle).
- Duur patch proces (gegevens uit N-central).
- Controle over herstart servers (gegevens uit N-central).
- Interruptie gebruikers (test op eigen werkstation).

De eerste test met Patch management zijn uitgevoerd op de interne systemen van Hupra. Na dit proces een aantal weken nauwlettend in de gaten te hebben gehouden, is besloten deze test door te zetten naar drie klanten van Hupra. Dit zijn klanten van verschillende omvang, waarop verschillende profielen van toepassing zullen zijn. Zo kunnen tests uitgevoerd worden met WSUS op locatie van de klant voor zowel servers als werkstations, WSUS op locatie met alleen servers en een profiel welke gebruik maakt van de Microsoft Update servers.

Hiervoor zijn 4 profielen aangemaakt:

- MSU – Server
- MSU – Werkstation
- WSUS – Server
- WSUS – Werkstation

In de onderstaande tabel worden de belangrijkste instellingen voor het patch management weergegeven. Deze zullen in de productie omgeving worden aangepast, zie voorstel patch management.

	MSU		**WSUS**	
	Server	Werkstation	**Server**	**Werkstation**
Schedule Install Day	-	Iedere dag	-	Iedere dag
Schedule Install Time	22:00	11:00	22:00	11:00
Patch Server	Microsoft Update	Microsoft Update	WSUS klant locatie	WSUS klant locatie

Tabel 1: Profiel instellingen

Disable Automatic Updates:	No
Configure Automatic Updating:	Automatic download and scheduled installation
Schedule Install Day:	Monday
Schedule Install Time:	01:00
Enable Automatic Updates Detection:	Yes
Automatic Updates Detection Frequency (Hours):	3
Allow Non-Administrators to receive update notifications:	No
Turn on Software Notifications:	Yes
Allow Automatic Updates Immediate Installation:	No
No Auto Restart with Logged On User for Scheduled Automatic Updates:	No
Delay Restart for Scheduled Installations:	No
Wait (minutes) before proceeding with scheduled restart:	15
Re-Prompt Restart with Scheduled Installations:	No
Wait (minutes) before proceeding with scheduled restart:	15
Reschedule Automatic Updates Scheduled Installation:	Yes
Wait (minutes) after system startup:	1
Enable Windows Update Power Management to Automatically Wake up the System:	Yes
Specify Patch Server to use (WSUS or Windows Update):	Best Available
Allow Signed Updates from an Intranet Microsoft update service location:	No
Do not display "Install Updates and Shut Down" option in Shut Down Menu:	Yes
Do not adjust default option to "Install Updates and Shut Down" in Shut Down Menu:	Yes

Figuur 9: Totaal overzicht instellingen patch profiel

5.1. WSUS configuratie

Een probleem dat regelmatig na voren kwam tijdens de tests is een bestaande WSUS oplossing in een gebruikte omgeving. Alvorens men iets kan doen met deze omgeving zullen alle Group Policies betreffende WSUS uitgeschakeld of verwijderd moeten worden. Daarnaast kan het ook handig zijn een verse installatie van WSUS uit te voeren. In sommige gevallen zal dit niet mogelijk zijn en moet geprobeerd worden de instellingen zoveel mogelijk standaard te configureren. Er is gebleken dat deze manier de minste kans op problemen zal geven. Hiervoor is een script samengesteld. Onderstaande script kan vervolgens worden uitgevoerd via een taak in N-central.

```
1  net stop wuauserv
2  reg delete HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate /v AccountDomainSid /f
3  reg delete HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate /v PingID /f
4  reg delete HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate /v SusClientId /f
5  del %SystemRoot%\SoftwareDistribution\*.* /S /Q
6  reg delete HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate /f
7  net start wuauserv
```

Figuur 10: WSUS reset

5.2. Windows Update Service

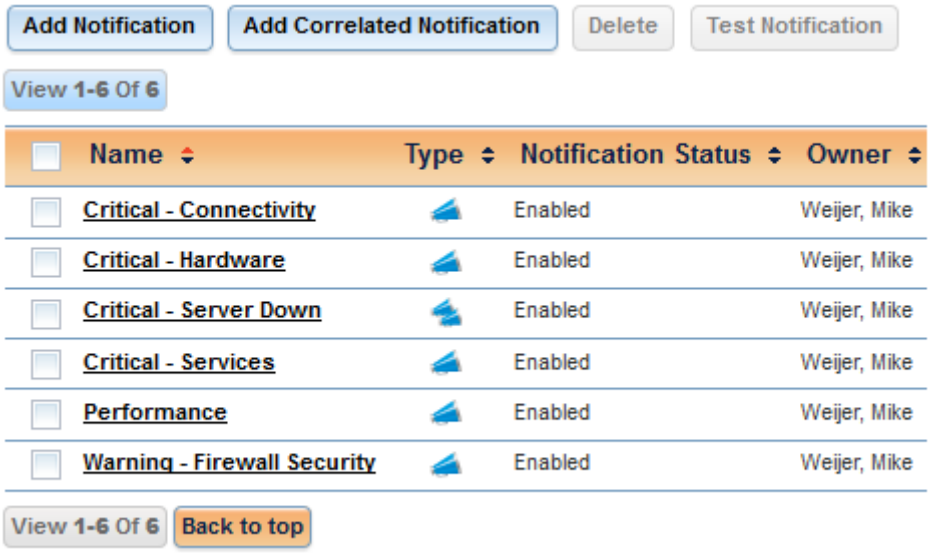
Naast problemen met de WSUS server is uit de test gebleken dat er ook wel eens wat problemen met de clients kunnen optreden. Het meest voorkomende probleem hierin was dat een client weigerde te associeren met een WSUS server. Vaak was dit een probleem in de configuratie van de client en dit kon opgelost worden door een aantal simpele stappen te volgen om als het ware de Windows Update Service 'op te schonen'. Hiervoor is later ook een programma gevonden op de N-able community forums welke het onderstaande proces automatisch zal uitvoeren. Deze procedure is ook handmatig uit te voeren door het volgende te doen. Onderstaande uit te voeren handelingen komen uit de Microsoft Knowledge Base:

Troubleshooting Error 0x80240FFF
For the SyncUpdates failure, the following can resolve the issue:

Click Control Panel > Admin Tools > Services.
Stop the Automatic Updates service.
Click Control Panel > Admin Tools > Services again.
Stop the Windows Agent Service service
Delete the contents of the C:\windows\windowsupdate.log file.
Save the revised log file.
Delete everything in the C:\Windows\SoftwareDistribution\DataStore folder.
Delete everything in the C:\Windows\SoftwareDistribution\Download folder.
Click Control Panel > Admin Tools > Services.
Start the Automatic Updates service.
Click Control Panel > Admin Tools > Services.
Start the Windows Agent Service service.

6. Notificaties

Na het invoeren van de notificatie profielen kunnen deze getest worden door op een aantal test servers de thresholds van een bepaalde service op reversed te zetten. Op deze manier kan een melding worden getriggerd, vervolgens kan simpel worden gecontroleerd of de meldingen op de juiste plekken aankomen.



Figuur 11: Notification Profiles

Een eerste opzet voor de Notification Profiles is vastgelegd in het adviesrapport. Zaken als notificaties zullen altijd aan wijzigingen onderhevig zijn en zullen constant moeten worden aangepast om in te spelen op de behoeftes van de beheerders en de klanten. Voor de tests is uitgegaan van de volgende set Notification profiles. Deze zijn vervolgens allen getest op een goede werking.

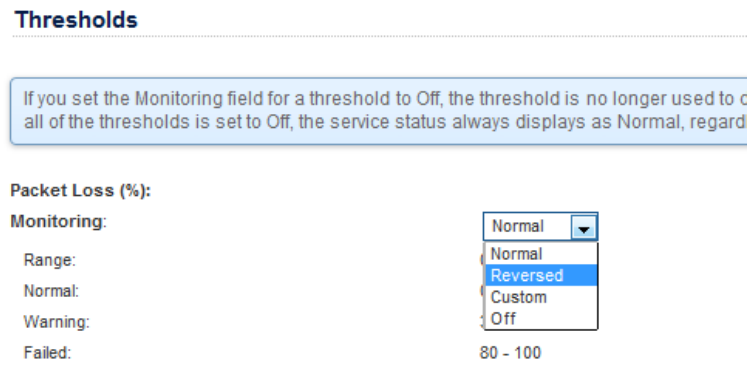
Profile	Trigger (state)	Service
Critical – Connectivity Primary Delay: 1 min Repeat: 60 min First Escalation Delay: 30 min	**Availability (failed)** Servers – Windows Servers – Generic SBS Servers Network Devices	Connectivity
	Uptime (stale) Servers – Windows SBS Servers Domain Controllers	Uptime

Critical – Hardware Primary Delay: 1 min Repeat: 60 min First Escalation Delay: 15 min	**Hardware – Failed (failed)** Servers – Windows Hupra - Fysieke servers	Fan Status (Dell/HP/IBM/Intel/VMware)
		Physical Drive (Adaptec/Dell/HP/Intel/VMware)
		Power Supply (Dell/HP/Intel/VMware)
		RAID Status (Adaptec/Dell/HP/VMware)
		Server Temp (Dell/HP/IBM/Intel)
		Temperature Status (VMware)
Critical – Services Primary Delay: 2 min Repeat: 60 min First Escalation Delay: 30 min	**AD (failed)** Domain Controllers Servers - Windows	Active Directory
	DNS (failed) Domain Controllers Servers - Windows	DNS
	Exchange – failed (failed) Exchange 2003 Exchange 2007 Exchange 2007 - CAS Role Exchange 2007 - Hub and Mailbox Exchange 2010 Exchange 2010 - CAS Role Exchange 2010 - Hub and Mailbox SBS Servers Servers - Windows	Exchange 2003
		Exchange 2007
		IMAP
		POP
		SMTP
	Hyper-V (failed) Servers - Windows	Hyper-V
	Website (failed) SBS Servers Servers - Windows	HTTP
		HTTPS
		IIS

Performance Primary Delay: 5 min Repeat: 60 min First Escalation Delay: 30 min	**CPU (failed)** Network Devices Servers - Windows	CPU
	Disk (failed) Network Devices Servers - Windows	Disk
		Disk Queue Length
	Memory (failed) Network Devices Servers - Windows	Memory
Warning - Firewall Security Primary Delay: 2 min Repeat: -	**SonicWALL (failed)** Network Devices	FW-SonicWALL

Tabel 2: Notification Profiles

Door voor iedere service de threshold op een test server op reversed te zetten, wordt een notificatie gegenereerd. Daarna kan gecontroleerd worden of de melding op de juiste plek aankomt, binnen de gestelde tijden, volgens tabel 2.



Figuur 12: Threshold wijzigen

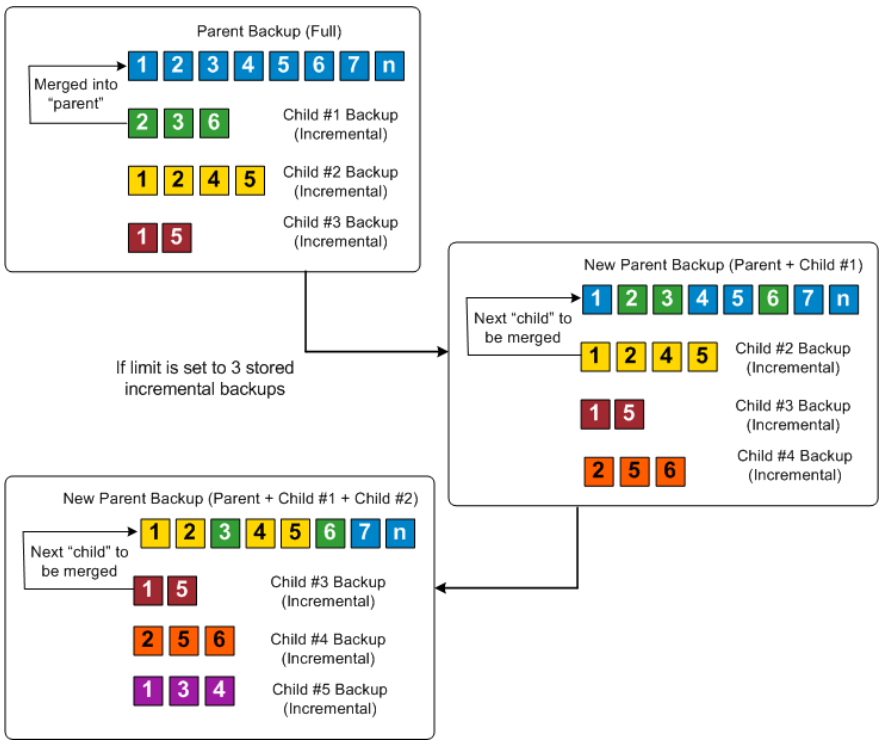
Na deze notificatieset enige weken getest te hebben, is duidelijk geworden dat deze te veel informatie oplevert. De mailboxen worden overspoeld met mail. De hoeveelheid mail neemt al snel het belang van de meldingen weg en er wordt hoogstens even snel doorheen gekeken met het gevolg dat belangrijke berichten over het hoofd worden gezien.

In een tweede notificatie ontwerp is meer gelet op het belang van de meldingen en is het aantal mails drastisch terug gebracht tot alleen kritische meldingen. De opzet is hetzelfde gebleven als de opzet van tabel 2, echter is de insteek veranderd. Alleen kritische meldingen worden per mail verstuurd en worden niet herhaald. Het is aan beheerders de verantwoordelijkheid te nemen en deze melding serieus op te nemen. Bovendien is met deze opzet rekening gehouden met een mail koppeling voor een ticket systeem. Men wil immers geen dubbele tickets aanmaken.

7. Back-up Manager

De back-up manager, toegevoegd in versie 8.2 van N-central, maakt het mogelijk gecontroleerde backups uit te voeren vanuit N-central. Onderliggende techniek is afkomstig van CA en is een geïntegreerde versie van ARCserve D2D.

De kracht van dit product zit in het maken van blocklevel “Disk 2 Disk” backups, dit is als het ware een volledige image van de server, geschikt voor bare metal recovery. De echte kracht van D2D zit in de “infinite incremental” functie. Deze functie maakt het mogelijk de initiële full back-up image, oneindig aan te blijven vullen met incremental backups, waarna de oude incremental sets samen worden gevoegd met de full back-up.



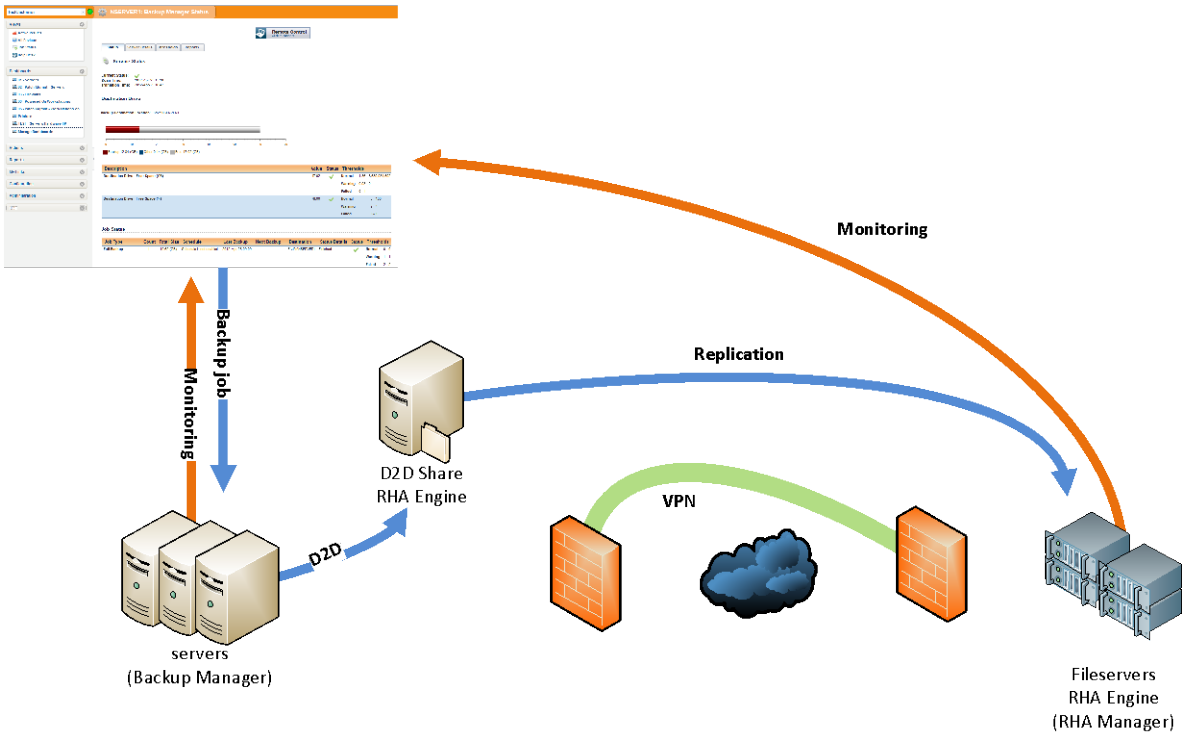
Figuur 13: D2D Infinite Incremental

Deze backups worden lokaal op het netwerk bewaard. Daarnaast is het mogelijk deze backups via een VPN verbinding te repliceren naar een tweede locatie. Dit kan een locatie van de klant zijn of een opslagruimte in het netwerk van Hupra. In een toekomstige release is het gebruik van een VPN niet meer nodig, door de toevoeging van een NAT-helper-agent, wat het product ideaal maakt voor plaatsing bij kleine klanten.

De architectuur voor de back-up oplossing is weergegeven in onderstaande figuur 14. Het proces start bij de N-central server die een aantal geplande taken voor back-up zal hebben. De N-central server zal het startcommando versturen naar de agent geïnstalleerd op de doel server, waarna de back-up manager software het zal overnemen en de voortgang van het proces zal rapporteren aan de N-central server.

De Back-up Manager maakt in eerste instantie een full D2D back-up van de server. Deze full back-up zal gevolgd worden door incremental backups zoals hierboven beschreven. Deze backups worden op een file server in het lokale netwerk geplaatst, waarna de Replication Manager (RHA Manager) de "D2D store" naar een offsite locatie repliceert. De replicatie zal ook via een block-level methode verlopen, zodat alleen de wijzigingen over het internet worden verstuurd.

Voor de eerste replicatie is het aan te raden de data op een externe schijf mee te nemen naar de offsite locatie en naar de juiste store te kopiëren, waarna de replicatie kan worden ingezet. Op deze manier wordt voorkomen dat in een keer alle data over het internet moet worden gekopieerd.



Figuur 14: Architectuur Backup Manager

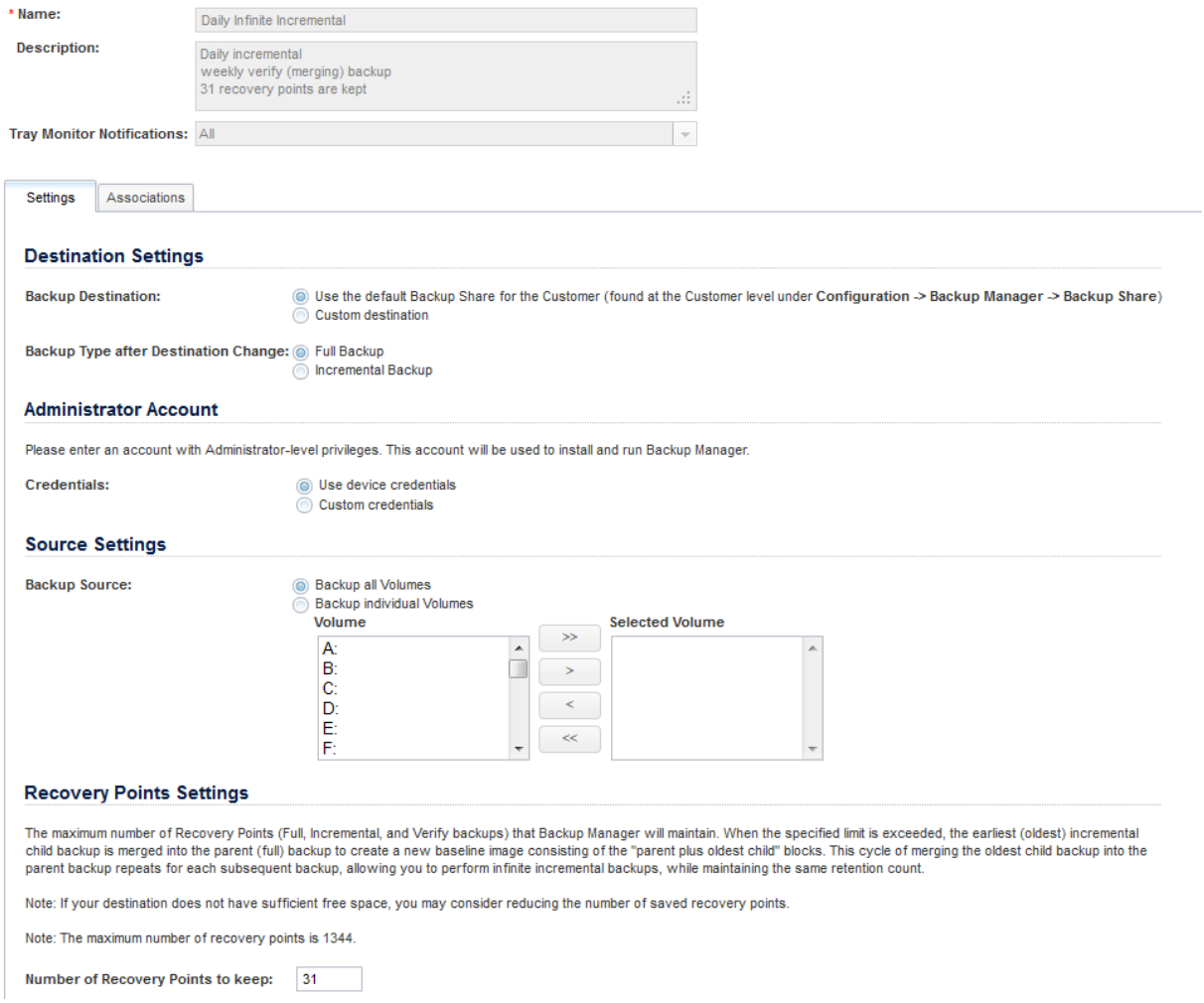
De tests van dit onderdeel zijn gebaseerd op bovenstaande architectuur. Er is voor gekozen deze test in te zetten bij een kleine nieuwe klant, waar op dat moment nog geen back-up aanwezig was. In de tests is snel duidelijk geworden dat bovengenoemde architectuur alleen zinvol is in een groter bedrijfsnetwerk.

Voor de testcase is deze architectuur aangepast om deze ook geschikt te maken voor kleine netwerken met maar één server. Deze server is uitgerust met een schijf/partitie uitsluitend bedoeld voor de D2D back-up. De server maakt een back-up naar deze schijf of partitie (een back-up naar zichzelf), daarna zal de back-up worden gerepliceerd naar de offsite locatie (Hupra netwerk).

Stap 1 is het installeren van de benodigde software. Deze wordt automatisch door de N-central agent geïnstalleerd op het moment dat de back-up optie voor de betreffende server/pc wordt geactiveerd. De software voor de replicatie dient wel handmatig geïnstalleerd te worden. Op de back-up locatie bij de klant wordt een RHA Engine geïnstalleerd. Op de offsite locatie (Hupra) wordt een server ingericht voor het opslaan van de offsite back-up data. Deze server wordt uitgerust met zowel een RHA Engine als een RHA Manager. De inrichting van de offsite locatie hoeft vanzelfsprekend maar éénmaal uitgevoerd te worden. Nieuwe omgevingen kunnen hieraan toegevoegd worden.

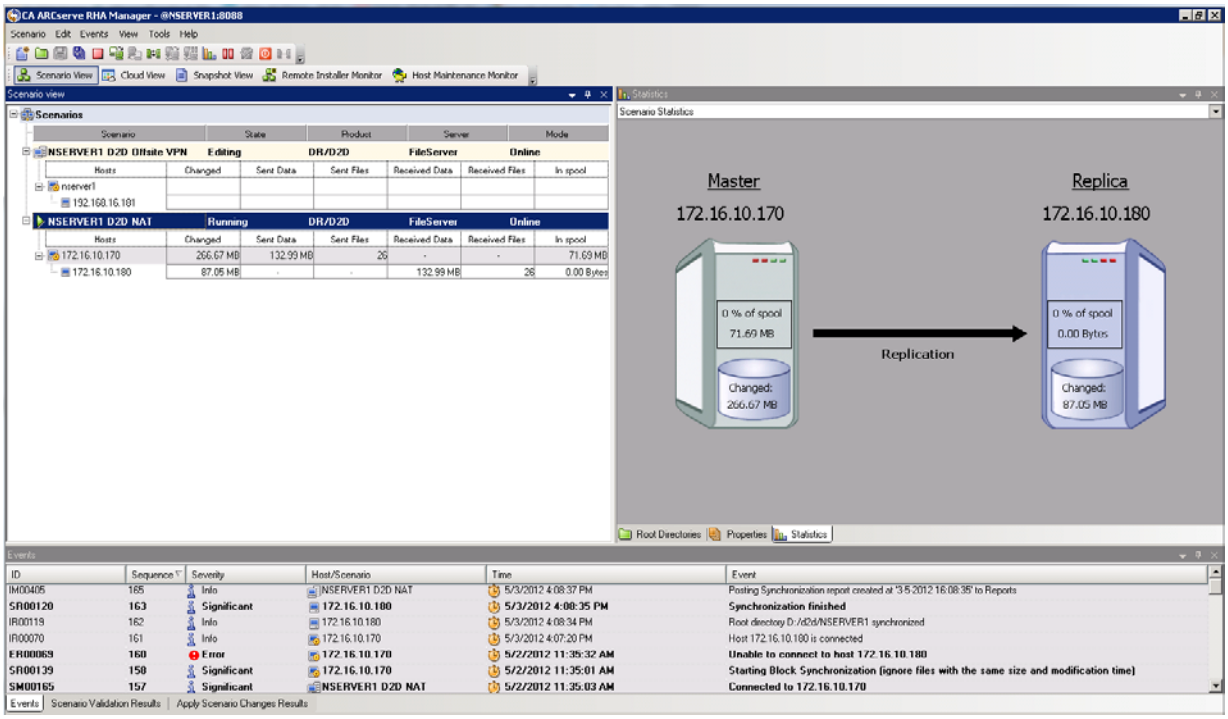
De tweede stap is het opstellen van een back-up profiel. Het is wenselijk een standaard te creëren voor de back-up strategie, zodat er een aantal standaard profielen aangemaakt kunnen worden die bij verschillende klanten ingezet kunnen worden. In deze speciale, niet veel voorkomende situatie, was het nodig een aangepast profiel te maken.

Deze back-up profielen worden aangemaakt in N-central. Hierin worden instellingen als de back-up bron/doel, planning, type back-up, encryptie, enz. ingesteld.



Figuur 15: Instellingen backup profiel (selectie)

Bij het gebruik van de replicatie dient de RHA software handmatig te worden ingesteld. Deze instellingen (scenario's) worden geconfigureerd in de RHA Manager (locatie Hupra). Voor iedere locatie (lees klant) zal een apart scenario worden gemaakt. Hierin worden zaken als IP adressen, bron/doel bestand, replicatie methode, e.d. geconfigureerd.



Figuur 16: RHA Manager

De installatie en configuratie van de RHA Manager en Engines verloopt handmatig buiten N-central om. N-central heeft wel de mogelijkheid de RHA manager te monitoren en zelfs individuele scenario's te controleren. De resultaten van de back-up kunnen vervolgens in rapportages worden weergegeven.

hupra
automatisering

Data Protection Report

Customer: TestCustomer
Period: 03/04/2012 - 03/05/2012

Summary

Result	Count	Percentage
Number of successful backups:	2	100.00 %
Total	2	100%

Details

Job: Incremental backup - NSERVER1
Job Type: Backup Manager Event
Device: NSERVER1

End Time	Status	Bytes Processed
02/05/2012 09:24:56	Success	78 MB
Job terminated with success.		

Job: Verify backup - NSERVER1
Job Type: Backup Manager Event
Device: NSERVER1

End Time	Status	Bytes Processed
02/05/2012 12:15:00	Success	201 MB
Job terminated with success.		

Company Name: TestCustomer
Report: Backup Manager Status
Created on: 2012-May-03 16:30
Period: 1 Month
Start Date and Time: 2012-Apr-03 16:00

Summary

This report shows the history and status of backup jobs performed by Backup Manager, and provides an overview of the Backup Manager licenses that have been deployed to devices.

Total Backup Size By Type

Incremental
Verify
Backup Type

Incremental **Verify**

Successful Failed Canceled Crashed Unknown

Backup History

#	Backup Manager Profile	Backup Type	Backup Status	Backup Date	Backup Size
1	Backup NSERVER1	Verify	Finished	2012-May-02	201.00 MB
2	Backup NSERVER1	Incremental	Finished	2012-May-02	78.00 MB

License Information

#	Device Name	Backup Manager Standard Server	Backup Manager Advanced Server	Backup Manager SBS Server	Backup Manager Workstation (Laptop/Desktop)
1	NSERVER1	✓			

7.1. Problemen

Gedurende de tests zijn een aantal kleine problemen aan het licht gekomen. Zo is het bijvoorbeeld bij het instellen van de replicatie van groot belang dat men consistent is met het ingeven van de IP adressen voor de master en slave server. Dit houdt in dat als er gebruik wordt gemaakt van publieke adressen, deze zowel voor de master als de slave worden ingesteld. Het is niet mogelijk een intern adres te gebruiken voor de master en een publiek adres voor de slave en vice versa. Gebeurt dit wel, dan zal er geen duidelijke foutmelding worden gegeven.

Voor het gebruik van de replicatie oplossing in netwerken waar gebruik wordt gemaakt van NAT dient poort 25000 TCP open gezet te worden. Het forwarden van deze poort zal in de toekomst komen te vervallen als de NAT helper wordt toegevoegd in de volgende release.

Een tweede probleem wat zich heeft voorgedaan in de tests was een probleem met een corrupte VSS (Volume Snapshot Service) op een Windows XP machine. De D2D backup gebruikt de VSS service voor het veilig stellen van een snapshot van de disk. Dit probleem deed zich voor in een test op een “vuile” omgeving. Deze problemen komen hoogstwaarschijnlijk voort uit een met nLite bewerkte installatie van Windows XP. Er is geen directe oplossing voorhanden. Aangeleverd door Microsoft support is een script voor het resetten en opniew registreren van de VSS DLL’s en register sleutels. Dit script wordt hieronder weergegeven.

```
cd /d %windir%\system32
net stop vss
net stop swprv
regsvr32 ole32.dll
regsvr32 oleaut32.dll
regsvr32 /i eventcls.dll
regsvr32 vss_ps.dll
vssvc /register
regsvr32 /i swprv.dll
regsvr32 es.dll
regsvr32 stdprov.dll
regsvr32 vssui.dll
regsvr32 msxml.dll
regsvr32 msxml3.dll
regsvr32 msxml4.dll
```

Script 1: VSS reset script

Het uitvoeren van dit script en het herstarten van de machine in kwestie bleek het probleem tijdelijk op te lossen. Echter na een succesvolle full back-up was het probleem weer terug. De opeenvolgende incremental backups konden daarna niet uitgevoerd worden. Uiteindelijk is besloten in deze situatie een tijdelijke simpele back-up oplossing in te zetten totdat de betreffende machine vervangen was. Dit simpelweg vanwege de tijd en de kosten die anders gemaakt moeten worden op een systeem dat toch op de lijst voor vervanging staat. Backups op de schone omgevingen verliepen zonder problemen.

8. Maintenance

Geplande taken kunnen gemakkelijk gecontroleerd uitgevoerd worden op servers en werkstations in N-central. Dit brengt de mogelijkheid met zich mee om gecontroleerde onderhoudstaken uit te voeren op een groep servers of werkstations. Deze onderhoudstaken zijn vastgelegd in een onderhoudsplan, maar zullen volledig geautomatiseerd worden uitgevoerd m.b.v. N-central. Deze taken kunnen zowel op servers als op werkstations met een professional licentie worden uitgevoerd.

Basisonderhoud zal bestaan uit een aantal basistaken, welke wekelijks dan wel maandelijks worden uitgevoerd. Deze taken zijn inzetbaar op servers en werkstations. De taken kunnen later uitgebreid worden met specifieke taken voor bijvoorbeeld Microsoft SQL servers. Onderstaande tabel geeft een overzicht van de basis taken.

Tabel 3: Basis Onderhoudstaken

Taak	Frequentie	Tijdstip
Schijfopruiming (CCleaner)	1x per week	ZO 13:00 uur
Verwijderen Temp Files	1x per week	ZO 13:15 uur
Defragmentatie (alle partities)	1x per week	ZO 13:30 uur
Volledige virus scan (Endpoint Security)	1x per week	ZO 18:00 uur
Schijfcontrole (CHKDSK)/ Geplande herstart	1x per maand	Eerste ZA 23:00 uur

De standaard scripts zijn getest op de TestCustomer testomgeving. Als snel werd duidelijk dat deze scripts niet geheel voldoen aan de verwachtingen. De scripts schieten meestal tekort in functie. Hiervoor zijn een aantal scripts geschreven, die deze tekortkomingen moeten wegnemen. Daarnaast is het nodig CCleaner met bijbehorende configuratie uit te rollen om gebruik te kunnen maken van de schijfopruiming taak.

```
1  @echo off
2  setlocal enabledelayedexpansion
3
4  set partitions=
5  for %%a in (a b c d e f g h i j k l m n o p q r s t u v w x y z) do (
6      vol %%a: > nul 2>nul
7      if not errorlevel 1 (
8          set partitions=!partitions! %%a:
9      )
10 )
11
12 defrag.exe %partitions% /H /M
```

Script 2: Defragmentatie

Bovenstaand script wordt ingezet voor defragmentatie van alle gevonden harde schijven op het systeem. Dit script zal ingezet worden met onderhoudstaken als schijfopruiming en schijfcontrole, waarbij de defragmentatie als laatste zal worden uitgevoerd. De resultaten en foutmeldingen zullen

worden terug gekoppeld via de Windows Event Logging, welke weer kan worden gecontroleerd met N-central.

```
@echo off & setLocal enableDELAYedexpansion
for %%a in (a b c d e f g h i j k l m n o p q r s t u v w x y z) do (
    vol %%a: > nul 2>nul
    if not errorlevel 1 (
        fsutil dirty set %%a:
    )
)

shutdown -r -t 20
```

Script 3: Schijfcontrole

Script 3 wordt 1 maal per maand uitgevoerd en zal alle schijven in het systeem als “dirty” markeren. Deze flag zal ervoor zorgen dat de schijven bij de eerstvolgende herstart door CHKDSK gecontroleerd worden. Na het aanpassen van de flag zal het script de server laten herstarten en de geplande controle uitvoeren. Dit script zorgt er daarnaast ook voor dat de server iedere maand een preventieve herstart krijgt.

8.1. CCleaner uitrol

Voor de uitrol van CCleaner is een portable versie van CCleaner gebruikt. Er is gekozen voor de portable versie omdat hieraan makkelijk een CCleaner configuratie bestand (INI) kan worden toegevoegd. Deze configuratie is zo algemeen mogelijk gehouden zodat deze over verschillende systemen ingezet kan worden, voor zowel servers als werkstations. Vanwege de inzet op werkstations is rekening gehouden met het gebruikersgemak. Zo zullen bijvoorbeeld de opgeslagen wachtwoorden en cookies in internet browsers niet worden opgeruimd.

Het gehele pakket is vervolgens in een installatiebestand ingepakt zodat het met de “Push Third Party Software” functie van N-central verspreid kan worden over de doelmachines. Het installatie bestand is eenmalig geconfigureerd en toegevoegd aan de N-central software repository. De uitrol kan gemakkelijk via een geplande N-central taak worden uitgevoerd. Er is geen verdere configuratie benodigd, de INI configuratie voor CCleaner is immers inbegrepen.

De aansturing van CCleaner verloopt via een Visual Basic Script wat is aangeleverd door N-able en standaard is opgenomen in de N-central server. Het CCleaner proces kan op dit moment nog niet worden gecontroleerd binnen N-central, dit vanwege het gebrek aan logging vanuit CCleaner.

```
[Options]
Language=1033
UpdateKey=05/02/2012 09:05:58 AM
(App)History=False
(App)Cookies=False
(App)Recently Typed URLs=False
(App)Windows Error Reporting=False
(App)DNS Cache=True
(App)Font Cache=True
(App)Old Prefetch data=True
(App)Menu Order Cache=False
(App)Tray Notifications Cache=False
(App)Window Size/Location Cache=False
(App)Environment Path=True
(App)User Assist History=False
(App)IIS Log Files=False
(App)Mozilla - Internet History=False
(App)Mozilla - Cookies=False
(App)Mozilla - Site Preferences=True
(App)Mozilla - Compact Databases=True
(App)Google Chrome - Internet History=False
(App)Google Chrome - Cookies=False
(App)Google Chrome - Compact Databases=True
WINDOW_MAX=1
WINDOW_LEFT=0
WINDOW_TOP=0
WINDOW_WIDTH=0
WINDOW_HEIGHT=0
```

Figuur 17: Configuratie CCleaner

9. Conclusie

Samenvattend kan gezegd worden dat alle tests redelijk naar verwachting zijn verlopen. De standaard testomgeving bleek al snel weinig problemen aan het licht te brengen. Deze virtuele omgeving bestond uit allemaal schone installaties. Alle tests verliepen zonder problemen op deze omgeving. Daarom is er snel besloten de test procedure uit te breiden met een tweetal aanvullende omgevingen, het Hupra netwerk en netwerken van een select aantal klanten. Deze 'vuile' omgevingen brachten wat meer problemen met zich mee.

Naast verdere informatie over het pakket en de configuratie hiervan te verschaffen, hebben deze tests ook een aantal andere aandachtspunten aan het licht gebracht. Dit waren onder andere:

- problemen met rechten bij automatische agent verspreiding via de probe;
- problemen met rechten in werkgroepen;
- verwijdering van oude antivirus installaties, in het bijzonder Norman;
- incomplete Service Templates;
- vervuilde WSUS installaties;
- en tekortkomingen in de standaard onderhoudsscripts.

Voor al deze punten is uiteindelijk een oplossing of een workaround gevonden. Deze oplossingen zijn vastgelegd in dit document en in een installatie checklist, welke beheerders kunnen gebruiken bij de migratie van een klant naar het Managed Services systeem. Daarnaast hebben de tests waardevolle informatie opgeleverd voor de in te zetten configuraties.

De problemen met het installeren van de agent op een Windows Server 2008 Core en een Windows Server 8 installatie zijn voor nu naar de achtergrond geschoven. De Windows Server 2008 Core installatie is niet verder onderzocht omdat deze nergens in de omgevingen van Hupra wordt gebruikt. Wat betreft de installatie van de agent op Windows Server 8 wordt verwacht dat deze ondersteuning wordt toegevoegd na de release.

De testomgevingen, zoals gebruikt in de testfase, zijn bewust behouden zodat in de toekomst, bij onduidelijkheden over nieuwe configuraties, teruggevallen kan worden op deze testomgevingen. Ook bij het invoeren van nieuwe functies of het testen van patches voor de N-central server kunnen deze omgevingen goed van pas komen.

Bijlage I:
Voorstel Patch Management
Proactief beheer bij Hupra

Auteur:
M.M.J. de Weijer
Studentnummer: 1546128
Hogeschool Utrecht
Faculteit Natuur & Techniek
Systeembeheer

Bedrijf:
Hupra Automatisering
Hoofdstraat 105
3901 AK Veenendaal

Begeleiders:
Hupra: Dhr. P.A. Willemsen
Hogeschool Utrecht: Dhr. H. van Nimwegen

Afstudeerperiode:
februari 2012 - juni 2012

Versie: 1.1
Datum: 24 mei 2012

Versie beheer:

Versie	Datum	Wijzigingen
0.0	27-02-2012	Initiële versie document, geen inhoud
0.1	02-03-2012	Invulling Architectuur
0.2	09-03-2012	Invulling Profielen en configuratie na overleg betreffende tijdsplanning
0.3	13-03-2012	Invulling patch approval
1.0	16-03-2012	Definitief document
1.1	24-05-2012	Opmaak aanpassen voor bijlage aan scriptie

Managementsamenvatting

Hieronder een korte samenvatting van de adviezen en keuzes vastgelegd in dit document.

	0 – 10 Devices	10 > Devices
Patch architectuur	Gebruik maken van Microsoft Update Servers	WSUS server op locatie van de klant

Tabel 1: Patch Architectuur

Profielen dienen te worden opgedeeld op basis van server/werkstation en test/productie. Het is daarnaast ook mogelijk opdeling in klanten te maken. Op deze manier kan worden voorkomen dat alle patches tegelijk worden doorgevoerd.

Als installatiemethode wordt aanbevolen gebruik te maken van de instelling: “updates downloaden en installeren volgens schema”. De gebruiker wordt geweigerd aanpassingen te maken. Zo wordt een goede werking gegarandeerd.

	Server	Werkstation
Tijdstip doorvoeren patches	Wekelijks op maandag 01:00 uur.	Iedere werkdag om 11:00 uur.

Tabel 2: Patch Planning

Eenmaal per week controleren op nieuwe patches welke goedgekeurd moeten worden. Patches in de categorie Critical en Security worden automatisch goedgekeurd. Een keer per maand grondig controleren op goed te keuren patches.

Configuratie van de WSUS server:

- Installeren WSUS, standaard instellingen, geen configuratie nodig.
    - Bij overzetten van bestaande WSUS omgeving naar een N-central beheerde omgeving moet er rekening mee gehouden worden dat alle Group Policies actief op het gebied van patch management, uitgeschakeld dienen te worden. Daarnaast is het aan te bevelen WSUS instellingen op standaard te zetten of een schone installatie van WSUS uit te voeren.
- WSUS wordt na Asset Discovery en installatie van de Windows agent automatisch herkend en toegevoegd. Desgewenst kan de agent handmatig worden geïnstalleerd.
- Devices opnemen in patch management door een patch profiel toe te wijzen (handmatig of via rule)

Inhoud

1. Inleiding

Dit document is een voorstel voor configuratie om het patch management te implementeren in N-central. Hier zullen de keuzes en configuraties betreffende het patch management verder worden toegelicht. Dit document is opgesteld op verzoek van de opdrachtgever om een compleet overzicht van de patch management configuratie te geven.

In dit document zullen de verschillende soorten architectuur van patch management aan de orde komen, gevolgd door een advies welke architectuur het beste waar ingezet kan worden. In hoofdstuk 4 zal een advies worden gegeven over de indeling van de patch profielen. De hoofstukken 5 en 6 zullen een advies geven over de mogelijke configuratie en een procedure voor patch approval.

2. Architectuur

Er zijn verschillende mogelijkheden binnen N-central voor implementatie van patch management. Patch management kan geconfigureerd worden voor updates van een WSUS-server gehost op de SO (Service Organisation) locatie, een WSUS-server op locatie van de klant of direct vanaf Microsoft update. Elke configuratie heeft zijn voor- en nadelen welke hieronder zullen worden besproken. De configuraties worden op de volgende pagina in figuur 1 weergegeven.

2.1. Direct vanaf Microsoft Update

In deze opstelling zullen de updates direct vanaf de Microsoft servers worden gedownload. Dit model kan vergeleken worden met het standaard update model van Windows. Een verschil met het standaard model is dat het d.m.v. N-central wel mogelijk wordt controle te houden over welke updates geïnstalleerd mogen worden. Updates moeten in N-central worden goedgekeurd. Dit is vergelijkbaar met de goedkeuring van procedures in bestaande WSUS opstellingen. Daarnaast kan vanuit N-central ook worden afgedwongen dat gebruikers niet zelf aan hun update instellingen kunnen zitten.

Dit model biedt dus de meeste voordelen van een WSUS opstelling, maar dan direct vanaf de download servers van Microsoft. Een nadeel hiervan is de benodigde bandbreedte. Ieder device zal zijn updates moeten downloaden via het internet wat dus zal leiden tot dubbele downloads.

2.2. WSUS op SO level

Een tweede mogelijkheid is een opstelling met een WSUS server op SO level, d.w.z. een WSUS server gehost door de MSP (Managed service provider). In dit model zal het goedkeuren van patches ook verlopen via de N-central server. Het verschil met het bovengenoemde model is dat in deze situatie de MSP de updates zal aanbieden en als het ware de rol van de Microsoft Update servers zal vervullen. De MSP zal dienen als een doorgeefluik van updates. Ook in dit model zal er voldoende bandbreedte aanwezig moeten zijn, niet alleen aan de kant van de devices die de updates downloaden, maar ook aan de kant van de MSP welke de updates moet uploaden. Een voordeel van dit model is dat de MSP meer controle kan krijgen over het update proces.

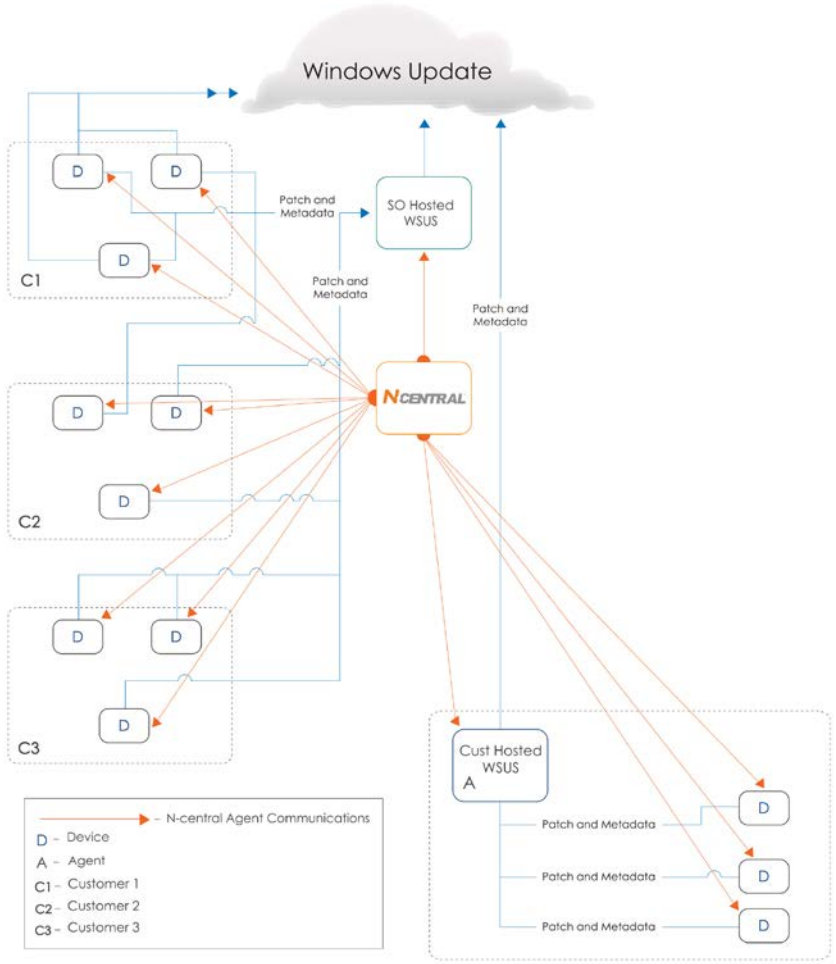
2.3. WSUS bij de klant

Het derde en laatste model gaat uit van een WSUS server op de locatie van de klant. Deze opstelling biedt een aantal voordelen, zeker als er een groot aantal devices op locatie van de klant aanwezig is. In deze opstelling zal de WSUS server de updates synchroniseren met de Microsoft Update servers en vervolgens zelf verspreiden naar de andere aanwezige devices op dat netwerk. De werking hiervan is hetzelfde als in een normale WSUS opstelling. Ook hier wordt het verschil gemaakt bij het goedkeuren van de patches. Ook hier zal dit verlopen via de N-central server. Daarnaast zal alle verdere configuratie van de WSUS server uit de interface van N-central mogelijk zijn.

In alle bovengenoemde oplossingen zullen de goedkeuring en de naleving van de update instellingen geregeld worden vanuit N-central. Het configureren van Group Policies welke in normale situaties deze instellingen naleven, is niet benodigd. Daarnaast zal de configuratie van de WSUS server, in de bijbehorende opstellingen, ook vanuit WSUS verlopen.

3. Advies inzet patch management

In onderstaande figuur wordt een beeld gegeven van de verschillende mogelijkheden voor inzet van patch management. Het is ook mogelijk een combinatie van bovenstaande modellen te maken. Kleine klanten kunnen bijvoorbeeld in een model worden ondergebracht voor Microsoft Update servers en grotere klanten, welke beschikken over een eigen WSUS server, kunnen van deze server gebruik maken voor hun patch management.



Figuur 1: De 3 vormen van Patch management

Als richtlijn voor de te configureren opstelling kan het volgende worden aangehouden. Mijn advies is geen gebruik te maken van de door de MSP gehoste WSUS server. Dit model biedt niet direct voordelen ten opzichte van de andere modellen. Bovendien zal de MSP alleen maar gaan functioneren als een doorgeefluik voor updates. Dit zal ten koste gaan van de resources van de MSP, welke elders beter benut kunnen worden.

De richtlijnen voor gebruik van de twee overige modellen (Microsoft Update Servers en WSUS op locatie bij de klant) zijn als volgt. Ik adviseer klanten met 1 tot 10 devices gebruik te maken van de Microsoft Update Servers. Het gebruik van bandbreedte blijft redelijk beperkt en de servers hoeven niet extra belast te worden met WSUS.

Voor klanten met meer dan 10 devices is het aan te bevelen een WSUS op klant locatie te plaatsen. Deze server zal eenmalig de updates synchroniseren en deze vervolgens verspreiden over de machines binnen het netwerk van de klant. Het gebruik van Microsoft Update Servers met meer dan 10 devices is af te raden. Er zal simpelweg teveel bandbreedte worden ‘verspild’.

4. Advies Profielen

De instellingen voor patch management worden vastgelegd in profielen. Er kunnen meerdere profielen worden aangemaakt, compleet afgestemd op de behoeftes van een bepaalde groep machines. In figuur 2 wordt een overzicht gegeven van de configuratiemogelijkheden.

Het is aan te bevelen om verschillende profielen te gebruiken voor servers en werkstations aangezien deze machines verschillende instellingen vereisen. Zo is het bijvoorbeeld niet gewenst dat een server overdag patches gaat installeren welke een reboot vereisen. Voor werkstations is dit geen probleem. Indien gewenst kan er ook nog onderscheid worden gemaakt tussen werkstations en pc’s.

4.1. Installatie methode

Belangrijke configuratiepunten zijn de manier en het tijdstip van updaten. Net als bij configuratie van een Windows device kan worden gekozen uit de volgende mogelijkheden:

- alleen een melding geven;
- updates downloaden en een melding geven voor installatie;
- updates downloaden en installeren volgens schema;
- configuratie wordt overgelaten aan de gebruiker.

Voor algehele automatisering van het patch management is het aan te bevelen alle devices gebruik te laten maken van de optie: “downloaden en installeren volgens schema”. De gebruiker mag geen mogelijkheid worden gelaten hier zelf instellingen te veranderen. Dit is de enige manier waarop een goede werking van het patch management kan worden gegarandeerd.

Disable Automatic Updates:	No
Configure Automatic Updating:	Automatic download and scheduled installation
Schedule Install Day:	Tuesday
Schedule Install Time:	22:00
Enable Automatic Updates Detection:	Yes
Automatic Updates Detection Frequency (Hours):	3
Allow Non-Administrators to receive update notifications:	No
Turn on Software Notifications:	Yes
Allow Automatic Updates Immediate Installation:	No
No Auto Restart with Logged On User for Scheduled Automatic Updates:	No
Delay Restart for Scheduled Installations:	Yes
Wait (minutes) before proceeding with scheduled restart:	15
Re-Prompt Restart with Scheduled Installations:	Yes
Wait (minutes) before proceeding with scheduled restart:	15
Reschedule Automatic Updates Scheduled Installation:	Yes
Wait (minutes) after system startup:	1
Enable Windows Update Power Management to Automatically Wake up the System:	Yes
Specify Patch Server to use (WSUS or Windows Update):	Best Available
Allow Signed Updates from an Intranet Microsoft update service location:	No
Do not display "Install Updates and Shut Down" option in Shut Down Menu:	Yes
Do not adjust default option to "Install Updates and Shut Down" in Shut Down Menu:	Yes

Figuur 2: Configuratie Patch profielen

4.2. Tijdstip installatie en herstart

Aansluitend op het bovenstaande advies betreffende de installatie methode (updates downloaden en installeren volgens schema) dient er een moment voor installeren van de patches gekozen te worden. Voor een server verdient het kiezen van dit moment extra aandacht, omdat het de huidige geplande taken niet in de weg mag zitten. Denk bijvoorbeeld aan taken als onderhoud en back-up. Voor een werkstation is dit van minder belang. De patches voor werkstations kunnen gerust overdag worden geïnstalleerd.

Voor een server is het advies de patches te installeren in de nacht van zondag op maandag. Er zijn op dat moment geen andere taken bekend. Bij installatieproblemen van de patches kan maandag direct actie worden ondernomen. Indien gewenst kunnen de servers uit voorzorg via een script een herstart krijgen.

Voor werkstations is het tijdstip van installeren niet van groot belang. Een goed uitgangspunt voor het installeren van werkstation patches is iedere dag om 11:00 uur. Er is gekozen voor deze aanpak omdat deze patches alleen geïnstalleerd kunnen worden als de machine aan staat. Er is gekozen voor 11 uur omdat er van uit wordt gegaan dat op dat moment de meeste werknemers op kantoor zijn. Dit proces wordt iedere werkdag herhaald, dit om te garanderen dat machines welke een patch moment hebben gemist, zo snel mogelijk weer bijgewerkt worden.

4.3. Download server

Wat verder belangrijk is bij het configureren van een patch profiel is welke server er wordt gebruikt voor het verkrijgen van de updates. De standaard instelling is hier: “Best Available”. Deze instelling zal bekijken of er een WSUS server op locatie beschikbaar is. Is dit niet het geval dan zal er worden terug gevallen op een WSUS server van de MSP of op de Microsoft Update Server. Het is ook mogelijk direct een keuze te maken, mocht de server van keuze niet beschikbaar zijn, dan zal het patch proces mislukken. Het direct toewijzen van een service kan bijvoorbeeld handig zijn bij het maken van profielen voor grote en kleine klanten, welke van een andere server gebruik zullen maken, zoals hierboven besproken.

4.4. Testen patches

Om er zeker van de zijn dat de patches geen problemen gaan opleveren, is het te adviseren om een aantal servers/werkstations aan te wijzen welke de patches een paar dagen eerder zullen krijgen. Deze machines dienen vervolgens gekoppeld te worden aan speciale profielen. Op deze manier kan worden gecontroleerd of de patches geen problemen gaan geven. Mocht dit wel voorkomen dan kunnen de patches in kwestie van de approval lijst worden gehaald totdat er een oplossing beschikbaar is. Op deze manier kan men voorkomen dat ineens alle klanten problemen krijgen na het doorvoeren van een patch.

4.5. Profielen

De bovengenoemde combinaties van patch tijdstippen en patch methodes kan worden gecombineerd in de onderstaande patch profielen.

Tabel 3: Profielen

Profiel	Server	Tijdstip
MSU – Workstation	Microsoft Update	Iedere werkdag om 11:00 uur.
MSU – Server	Microsoft Update	Wekelijks op maandag 01:00 uur.
WSUS – Workstation	WSUS klantlocatie	Iedere werkdag om 11:00 uur.
WSUS – Server	WSUS klantlocatie	Wekelijks op maandag 01:00 uur.

5. Configuratie

Patch management configuratie bestaat uit de volgende stappen:

- Installeren WSUS server, geen configuratie nodig
- Toevoegen WSUS server aan N-central
- Configureren patch profiles
- Devices configureren voor patch management/ Rules toevoegen

Het installeren van een WSUS server voor gebruik met N-central is een kleine moeite. De installatie van WSUS kan op de normale manier worden gevolgd. Na installatie dient er een update synchronisatie plaats te vinden. Configuratie van de server is niet nodig, dit wordt vanuit N-central geregeld.

Als men een bestaande WSUS omgeving van een klant wil overzetten naar een N-central beheerd model, moet er rekening worden gehouden dat alle Group Policies (welke betrekking hebben op updates en/of WSUS) uitgeschakeld dienen te worden. Deze instellingen zullen vanuit N-central worden beheerd. Hiervoor wordt gebruik gemaakt van de agents geïnstalleerd op de machines. Daarnaast moeten de instellingen van de WSUS server zoveel mogelijk naar default worden teruggebracht. Een mogelijke snelle oplossing hiervoor is de oude WSUS in zijn geheel te verwijderen en opnieuw te installeren, dit om problemen in de toekomst te voorkomen.

Het toevoegen van de WSUS server in N-central verloopt geheel automatisch. In de Discovery jobs van de netwerk probe zal de WSUS server worden opgemerkt en automatisch als WSUS server worden toegevoegd. Mocht dit proces niet goed verlopen dan bestaat er ook nog de mogelijkheid de server handmatig toe te voegen.

De patch profiles dienen eenmalig geconfigureerd te worden. Bij patch management implementatie bij nieuwe klanten zal deze stap overbodig zijn. In deze profiles worden de instellingen voor patch management vastgelegd, welke vervolgens zullen worden toegepast op de machines. Het is mogelijk verschillende profielen te gebruiken voor de verschillende groepen machines. Hier later meer over.

De laatste stap is het inschakelen van patch management op de machine. Dit zal verlopen vanuit N-central en zal niet meer zijn dan een “vinkje zetten”. Deze stap kan ook geautomatiseerd worden door een rule aan te maken waarin deze instelling voor die groep machines wordt ingeschakeld.

6. Patch Approval

Na configuratie van de WSUS omgevingen, patch profiles en device instellingen rest nog één taak en dat is het goedkeuren van de patches. Dit is een terugkomende taak welke uitgevoerd dient te worden door een beheerder. Binnen N-central is het mogelijk ook deze stap te automatiseren, maar het is aan te raden hier voorzichtig mee te zijn. Kritische patches voor ernstige security lekken kunnen direct worden goedgekeurd, terwijl men voor niet dringende patches toch graag de goedkeuring van een beheerder wil hebben.

Het is aan te raden iedere week een moment te plannen waarop een beheerder snel de nieuwe patches doorneemt, deze beoordeeld en wel of niet goedkeurt voor uitrol. Eens per maand dient hieraan extra aandacht te worden besteed. Om precies te zijn na de tweede dinsdag van de maand, als Microsoft veel nieuwe patches zal uitbrengen.

Het bepalen of de nieuwe patches doorgevoerd zullen worden, zal vooral afhankelijk zijn van de kennis hierover van de beheerder en de resultaten uit de testomgeving. Voor informatie betreffende de werking van patches of eventuele problemen welke zich voor kunnen doen na installatie van een patch, kan men zich wenden tot de Master Knowledge Base van Microsoft. Hierin wordt alle informatie betreffende producten en patches bijgehouden. Problemen met patches zullen hierin ook vermeld worden.

In de praktijk zal het echter niet voorkomen dat iedere update wordt gecontroleerd. Het is aan te raden patches te testen op de test servers en vanuit die positie de Master Knowledge Base te raadplegen mochten er problemen optreden.

Daarnaast zijn er ook nog derde partijen welke de patches van Microsoft testen op hun werking en hiervan een lijst bijhouden. Deze lijsten geven een snel overzicht, maar bieden geen garanties voor een goede werking van de patches, immers iedere omgeving is anders.

Bijlage J:
Persoonlijke Evaluatie

Auteur:
M.M.J. de Weijer
Studentnummer: 1546128
Hogeschool Utrecht
Faculteit Natuur & Techniek
Systeembeheer

Bedrijf:
Hupra Automatisering
Hoofdstraat 105
3901 AK Veenendaal

Begeleiders:
Hupra: Dhr. P.A. Willemsen
Hogeschool Utrecht: Dhr. H. van Nimwegen

Afstudeerperiode:
februari 2012 - juni 2012

Versie: 1.0
Datum: 27 mei 2012

1. Algemene indruk

Over het algemeen ben ik erg tevreden met het resultaat. Vooral de technische stukken van het project hebben veel voldoening gegeven. Pas hier zie je het product echt in werking en komt het besef pas van wat het nu echt allemaal kan en doet.

Kritisch terugkijkend op het project waren er natuurlijk wel hier en daar een aantal zaken die niet helemaal naar tevredenheid gingen. De technische inrichting ging over het algemeen wel vrij probleemloos en hier ben ik ook zeer tevreden over, echter waren er wel een aantal moeilijkheden met bijvoorbeeld het geheugenprobleem van de N-central server. Dit probleem startte als een onbereikbare server. Op dat moment wees niets op de geheugenproblemen en was de oorzaak moeilijk te vinden. De eerste reactie is dan het zelf door blijven zoeken naar een oplossing en de eigenwijsheid N-able support niet in te willen schakelen. Uiteindelijk was het voor de support een kleine moeite en was het probleem snel opgelost. Hetzelfde gold voor het onderzoek naar de configuratie van de backup manager/replicatie, welke in de testfase niet van de grond wou komen.

Wat naar mijn mening erg goed is verlopen, was bijvoorbeeld het duidelijk stellen van de eisen betreffende het product, configuratie en processen. Dit vanwege de korte lijnen binnen het bedrijf en de makkelijke informele manier van vergaderen. Daarnaast was er bij keuzes of problemen altijd snel tot een besluit te komen.

Wat ik jammer vond was dat door de omvang van het project, zowel de technische implementatie als het onderzoek en de procedures, men niet erg diep op de onderwerpen in kon gaan. Ik had graag dieper in gegaan op bijvoorbeeld de techniek of de uitwerking van de procedures. Daar tegenover staat dat er nu een completer beeld is ontstaan waarbij alle aspecten zijn bekeken, wat het tot een completer geheel maakt.

2. Leermomenten

Eén van de belangrijkste dingen die ik heb geleerd is het efficiënter werken. Ook iets wat voort is gekomen uit de bovengenoemde problemen. Tijd is geld. Natuurlijk geeft het meer voldoening als je het probleem zelf kunt oplossen. Daarnaast leer je er ook meer van, maar sommige problemen zijn bijna niet zelf op te lossen. Dus waarom niet de support inschakelen als je deze toch ter beschikking hebt? Een afweging van kosten baten.

Dit was voor mij in het begin moeilijk. Ik los graag mijn eigen problemen op, maar naarmate het project verder vorderde, is deze ‘eigenwijsheid’ afgenomen.

Een ander leermoment is het kijken naar de belangen van de klant geweest. Hupra heeft vooral midden- en kleinbedrijven als klant. Klanten zijn totaal niet geïnteresseerd in techniek en hebben hier ook totaal geen verstand van. Het is daarom belangrijk om zelf in te kunnen leven in de klant, om ook deze klant de beste oplossing te bieden. Het belangrijkste bij deze klanten is het abstract maken en richten op de pijnpunten.

3. Aansluiting met de opleiding

Veel verschillende aspecten van systeembeheer zijn in dit project samengekomen in één opdracht. Het gaat hier niet over een oplossing voor een specifiek probleem, het moet uiteindelijk een oplossing zijn voor het geheel aan ICT en de manier waarop met deze oplossing gewerkt moet worden. Zo zijn onderwerpen als backup, beschikbaarheid, virtualisatie, monitoring, onderhoud, netwerken en beveiliging aan bod gekomen. Ook minder technische onderwerpen zoals stroomlijning processen, aansluiting op de organisatie en rapportages naar de klant, zijn aan de orde gekomen.

In mijn ogen zijn er weinig andere opdrachten te bedenken waarin zoveel verschillende aspecten van het systeembeheer aan bod komen. Er moet een totaaloplossing aan de klant worden geboden, dus er moet naar alle aspecten van beheer worden gekeken.

4. Competenties

Gedurende het project zijn veel competenties aan de orde gekomen. Hieronder worden de belangrijkste opgesomd:

- *Communiceren*
  Deze competentie en twee onderstaande zijn bijzonder belangrijk geweest bij het verkrijgen van de eisen uit vergaderingen en informele gesprekken.
- *Concreet maken van verwachtingen*
  Ook deze competentie is vooral aan de orde gekomen bij het vaststellen van de eisen, maar ook gedurende de rest van het project bij eventuele wijzigingen of het krijgen van feedback.
- *Organiseren van vergaderingen*
  Als projectleider ben ik verantwoordelijk geweest voor de vormgeving van de voortgangsvergaderingen.
- *Kwaliteit en voortgang bewaken*
- *Resultaatgericht en planmatig werken*
- *Besluiten durven nemen en onderbouwen*
  Dit is vooral van belang geweest bij de productkeuze. Ook in combinatie met het zelfstandig werken, was het belangrijk zelf besluiten te durven nemen en ook hier de verantwoording voor te nemen.
- *Zelfstandig werken*
  Het zelfstandig werken is in dit project belangrijk geweest. Het is vaak druk op kantoor en om zo efficiënt mogelijk te blijven, moeten taken zo veel mogelijk zelfstandig opgepakt worden.
- *Documenteren*

5. Toekomst

Ik vind de omgeving erg prettige om in te werken. De Informele sfeer van het MKB ligt mij goed. Ook gedurende het afstudeerproject ben ik in aanraking gekomen met veel verschillende aspecten van het systeembeheer. Ik ben veel verschillende problemen tegengekomen en met ieder probleem de bijbehorende uitdagingen. Juist vanwege deze diversiteit zie ik nog veel mogelijkheden om ervaring op te doen. Ik vind het belangrijk zo veel mogelijk ervaring op te doen en zo veel mogelijk gezien te hebben voordat ik mij later verder wil specialiseren.

Voor in de toekomst denk ik uiteindelijk meer uitdagingen te vinden in de netwerktechniek, netwerkbeveiliging of een combinatie van beiden. Het liefst zou ik me in de toekomst hier ook in willen specialiseren.

6. Conclusie

Ik ben erg tevreden met het resultaat. In het bijzonder de technische aspecten van het project, omdat hier ook meer mijn persoonlijke interesse ligt. Een aantal dingen kunnen in de toekomst beter, zoals het niet te lang blijven hangen in een probleem en direct de beschikbare hulpmiddelen gebruiken. Dit vanuit het principe effectief werken, wat een grote rol speelt in het MKB. Een ander belangrijk leermoment was de verplaatsing in de klant. Het product uitleggen en promoten, zonder technisch te worden, geeft toch een andere kijk op het geheel.

Er is veel aansluiting met de opleiding geweest. Er zullen weinig andere projecten zijn waarin zoveel aspecten van systeembeheer samenkomen.

Ik heb de omgeving waarin het project is uitgevoerd als erg prettig en interessant ervaren. Men wordt geconfronteerd met veel verschillende aspecten van het systeembeheer en komt veel verschillende problemen tegen. Ik zou hier nog veel ervaring kunnen opdoen, maar in de toekomst zou ik me graag meer willen specialiseren in onderwerpen als netwerktechniek en beveiliging.