Scriptie

Self Service Portal GTS Online

Student: Johan de Haan
Studentnummer: 1523226
Eerste examinator: Peter van Rooijen

Documentbeheer

Datum	Auteur	Omschrijving	Versie
26-01-2012	Johan de Haan	Initieel document	0.1
01-03-2012	Johan de Haan	Begin installatiebeschrijving SC 2012	0.2
16-03-2012	Johan de Haan	Aanpassen n.a.v. overleg P. van Rooijen d.d. 13-03-2012	0.2.5
05-04-2012	Johan de Haan	Bijlage 5 grotendeels afgerond	0.3
13-04-2012	Johan de Haan	Bijlage 5: multi-tenancy toegevoegd	0.3.1
20-04-2012	Johan de Haan	“Services in de Self Service Portal” & “Multi-tenancy” toegevoegd	0.3.2
25-04-2012	Johan de Haan	Aanpassen n.a.v. overleg P. van Rooijen d.d. 20-04-2012	0.3.5
26-04-2012	Johan de Haan	Hoofdstuk “Product configuratie”	0.4
27-04-2012	Johan de Haan	Hoofdstuk Rollen bijgewerkt, Hoofdstuk Processen gemaakt	0.4.1
09-05-2012	Johan de Haan	Opmaakstijlen bijgewerkt	0.4.2
10-05-2012	Johan de Haan	Hoofdstukvolgorde bijgewerkt, opmerkingen verwerkt n.a.v. overleg P. van Rooijen (8-5)	0.4.3
17-05-2012	Johan de Haan	Laatste onderdeel FO afgerond & toegevoegd	0.5.0
20-05-2012	Johan de Haan	Hoofdstuk modellen toegevoegd	0.5.1
21-05-2012	Johan de Haan	Hoofdstuk PoC toegevoegd	0.5.2
21-05-2012	Johan de Haan	Hoofdstuk Evaluatie toegevoegd	0.6.0
21-5-2012	Johan de Haan	Laatste hand gelegd aan Voorwoord & Management samenvatting; Uitgebreide spellingcontrole	0.9.0
23-05-2012	Johan de Haan	Verbetering structuur & Management Samenvatting n.a.v. gesprek P. van Rooijen (22-5)	0.9.1
24-05-2012	Johan de Haan	Aanpassingen n.a.v. overleg H. Bloemendal	1.0

1. Voorwoord

Dit verslag is tot stand gekomen naar aanleiding van de afstudeeropdracht die ik bij GTS-GRAL heb mogen uitvoeren. Dit verslag beschrijft niet alleen de aanpak en de stappen die ik heb doorlopen, maar is ook zeker bedoeld als naslagwerk voor mijn collega's over hoe de gebruikte producten werken en hoe het eindproduct tot stand is gekomen.

Ik wil in de eerste plaats GTS-GRAL, maar dan vooral Henk Bloemendal als mijn leidinggevende en bedrijfsbegeleider, bedanken voor de mogelijkheid die hij mij heeft gegeven voor het uitvoeren van deze opdracht. Ook mijn collega's hebben mij flink ontzien tijdens de afgelopen periode, zodat ik genoeg tijd vrij kon maken voor het afronden van deze opdracht.

Verder heeft Peter van Rooijen, in de functie als docentbegeleider, mij op een zeer constructieve manier geholpen in het verbeteren van mijn scriptie en mij op een fijne manier de goede richting op gestuurd.

En 'last, but not least' wil ik Tamara, mijn vrouw, bedanken voor de ruimte die ze me heeft gegeven de laatste jaren, maar zeker ook de afgelopen maanden tijdens het afronden van mijn studie.

Johan de Haan
Mei, 2012

2. Managementsamenvatting

Voor de afronding van mijn opleiding Informatica aan het HBO aan de Hogeschool Utrecht heb ik een Proof of Concept van een Self Service Portal opgezet in opdracht van mijn werkgever GTS-GRAL. In de periode van november 2011 tot mei 2012 heb ik mij bezig gehouden met onderzoek naar welke functionaliteit er beschikbaar moest komen via deze Self Service Portal, hoe deze gebruikt zou moeten gaan worden en hoe dit op technisch vlak zou moeten gaan werken door gebruik te maken van System Center Service Manager en Orchestrator van Microsoft.

Naast een Proof of Concept heb ik allereerst diverse documenten opgeleverd. Een Functioneel ontwerp waarin ik uitgebreid in ga over hoe ik de aangeboden functionaliteit wil verdelen over verschillende rollen en waarin ik modellen heb gemaakt die beschrijven hoe deze functionaliteit vorm moet krijgen. Deze modellen heb ik vervolgens vertaald naar Service Requests in Service Manager en zogeheten Runbooks in Orchestrator. Ook heb ik een beschrijving gemaakt over hoe de Proof of Concept omgeving is geïnstalleerd, over hoe de verschillende onderdelen van Service Manager en Orchestrator met elkaar samenwerken en welke keuzes ik heb moeten maken om de gegevens van de verschillende klanten van elkaar te scheiden.

Dit alles heeft geleid tot een Self Service Portal waarin een aantal basisfunctionaliteiten in worden aangeboden, welke op basis van de rol die de ingelogde gebruiker bekleed beschikbaar zijn of niet. Deze functionaliteit ziet er voor de gebruiker uit als een aantal in te vullen formulieren, waarbij de ingevoerde gegevens worden gebruikt om de wijziging door te voeren. Helaas bleek het niet mogelijk met de gekozen software in de wens te voorzien van een betere informatievoorziening. De rapportage mogelijkheden in Service Manager bieden niet de functionaliteit die we wensen en ook hierin bleek het lastig om de gegevens van klanten te scheiden.

Al met al levert dit project een goede basis om een productieomgeving op te zetten, waarbij een groot gedeelte van de functionaliteit één op één kan worden overgenomen uit deze Proof of Concept. Verder is de documentatie die ik heb gegenereerd door het schrijven van deze scriptie en de diverse bijlagen een goed naslagwerk voor zowel mijzelf als voor GTS-GRAL.

Inhoudsopgave

3. Organisatie

3.1. GTS-GRAL

GTS-GRAL heeft zijn oorsprong in Duitsland waar zij sinds 1988 als Server Based Computing specialist een vooraanstaande positie heeft weten te verwerven in deze markt. In Nederland wordt in 1998 een dochter onderneming gestart: GTS-GRAL Nederland B.V.

GTS-GRAL Nederland is sinds 1998 volledig zelfstandig en heeft zijn kantoor in Veenendaal. Vanuit Veenendaal, maar vaak ook bij de klant, implementeren, configureren en beheren onze medewerkers veelal grote (terminal) server omgevingen of delen hiervan. Het borgen van informatie en het gestructureerd uitvoeren van wijzigingen zit diep in de organisatie ingeworteld en hoge kwaliteit afleveren staat voorop.

Mede door deze instelling is in de loop van de jaren het product IMProve ontstaan, waarmee op eenvoudige wijze volledige herinstallaties van servers uitgevoerd kunnen worden, waarbij men iedere keer met hetzelfde eindresultaat komt. Op deze manier kunnen wijzigingen (patches en nieuwe installaties) gemakkelijk getest worden en kan er altijd op een oudere configuratie teruggevallen worden.

Naast het leveren van diensten "on premise", intern bij de klant, levert GTS-GRAL steeds meer diensten direct vanuit de eigen omgeving. Een combinatie van beide is ook denkbaar, waarbij de servers van de klant in het datacenter draaien onder het beheer van GTS-GRAL. Of dat de servers bij de klant intern draaien, maar door GTS-GRAL beheerd en gemonitord worden.

3.1.1. Visie

De visie van GTS-GRAL luidt als volgt:

“De wereld wordt mobieler en mensen gaan steeds flexibeler om met hun werkplek. Ze willen overal toegang tot hun gegevens en probleemloos bereikbaar zijn. De eisen aan kwaliteit en productiviteit stijgen: minder mensen moeten meer doen.

Technologie maakt een snelle uitwisseling van informatie en diensten mogelijk en laat mensen niet alleen communiceren, maar overal werken waar zij willen. GTS-GRAL gelooft dat betrouwbare, snelle en veilige beschikbaarheid van data de basis is voor een gezond en efficiënt bedrijfsleven. Daartoe ontwikkelen wij oplossingen en concepten met de nieuwste technologieën.

GTS-GRAL is specialist in het opzetten, onderhouden en beheren van ICT-infrastructuren. Onze focus ligt op de inrichting van serveromgevingen, opslag, virtualisatie en applicatie-beschikbaarheid. Technologie moet mogelijk maken, niet beperken. Wij zijn een kennispartner voor onze klanten, met professionele en gemotiveerde medewerkers en werken samen aan oplossingen die naadloos aansluiten bij de groeiende mobiliteitseisen van deze wereld.”

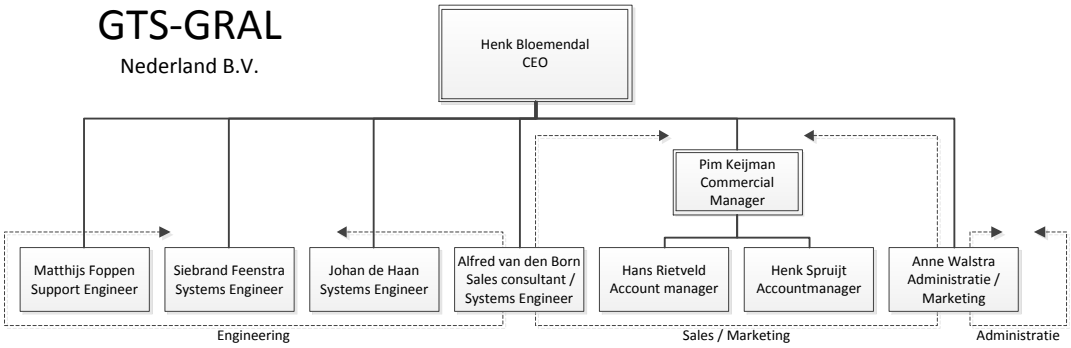
3.1.2. Missie

De visie van GTS-GRAL zorgt voor de volgende speerpunten als missie:

- Wij willen onze klanten ontzorgen op ICT-gebied, zodat zij zich bezig kunnen houden met dat wat zij het beste doen.
- Als ICT-partner willen wij behoren tot de besten in ons vakgebied.
- Wij geloven in een pragmatische aanpak en zijn open in het delen van onze kennis.

3.1.3. Organigram

De organisatie van GTS-GRAL ziet er ongeveer zo uit als weergegeven in Figuur 1. Een grotere versie van deze afbeelding is opgenomen in Bijlage 4. Zoals ook duidelijk uit onderstaande afbeelding blijkt is GTS-GRAL een platte organisatie waarbij sommige personen meerdere functies bekleden. Zo is één van de Systems Engineers regelmatig betrokken bij Pre-sales activiteiten en houdt een andere medewerker zich deels bezig met de administratie en boekhouding en deels met marketing.



Figuur 1

Door deze platte structuur is er sprake van korte en directe lijnen. Van de medewerkers van GTS-GRAL wordt dan ook een grote mate van zelfstandigheid en betrokkenheid gevraagd.

3.1.4. GTS-Online

GTS-Online is het nieuwste vlaggenschip van GTS-GRAL. GTS-Online is een cloud-dienst waar gebruikers te allen tijde toegang hebben tot hun gegevens, kantoor- en bedrijfsapplicaties, waarbij de focus ligt op bedrijven tot 250 werkplekken. Alle applicaties draaien in het data center, waardoor de klant overal vandaan verbinding kan maken met deze online desktop: het nieuwe werken.

Een klant betaalt per maand een vast bedrag per gebruiker om gebruik te kunnen maken van deze dienst. Daarnaast is het mogelijk een werkplek te huren, zoals een notebook, monitor, thin client en/of PC voor een vast bedrag per maand.

In de standaard GTS-Online desktop zit veel inbegrepen: niet alleen kantoorapplicaties, zoals Office Professional 2010, Adobe Reader en Internet Explorer, en voldoende ruimte voor persoonlijke en gedeelde bestanden, maar ook een professionele helpdesk staat tijdens kantooruren voor de klant

klaar om te assisteren bij het oplossen van mogelijke IT-problemen. Van alle bestanden van de klant wordt dagelijks een back-up gemaakt, e-mail is overal (telefoon, pda, tablet en desktop) beschikbaar door gebruik te maken Microsoft Exchange 2010 en de gehele omgeving wordt nauwlettend in de gaten gehouden met high-end monitoring software. Een compleet pakket, waar we trots op zijn.

3.2. Positie en werkervaring

Kort nadat ik begon met mijn opleiding HBO Informatica aan de Hogeschool Utrecht, ben ik ook gaan werken in de IT. Via OGD ben ik bij Gemeente Baarn als helpdesk medewerker begonnen en heb ik de eerste kneepjes van het systeembeheer vak mogen leren.

Op het moment dat ik de studie in deeltijd vervolgde ben ik bij DBNetwerken gaan werken. Via DBNetwerken heb ik bij veel verschillende klanten gedetacheerd automatiseringswerkzaamheden verricht, maar ben ik ook actief geweest in de interne organisatie met de verkoop van diverse soft- en hardware oplossingen. Voordat ik bij GTS-GRAL ben komen werken heb ik ook nog een aantal maanden via JC Groep in de detachering gewerkt, voornamelijk als systeembeheerder.

Na een aantal jaren voornamelijk in de detachering werkzaam te zijn geweest ben ik sinds november 2011 ben ik werkzaam bij GTS-GRAL als Systems Engineer. Naast mijn afstuderen, waar ik op dat moment bijna meteen mee begonnen ben, ondersteun ik mijn collega's in het onderhoud aan de GTS-Online omgeving en ben ik ook regelmatig bij klanten 'on site' aanwezig om hen te ondersteunen met hun ICT-omgeving.

Al heb ik een relatief korte loopbaan in de ICT, het werken in de detachering heeft me wel geholpen zo effectief mogelijk te werken: tijd is geld en dat maakt de klant je vaak maar al te goed duidelijk. Bij GTS-GRAL komt dit principe ook naar boven: hoe beter en slimmer je oplossing is voor een bepaald probleem is, hoe minder tijd je vaak later nog aan een zelfde probleem hoeft te besteden. Het werken op een hoog niveau straalt GTS-GRAL ook uit naar zijn klanten, waardoor we niet een willekeurige automatiseerder voor hun zijn, maar een kennispartner met ambitie.

Dat laatste heeft er ook toe geleid dat ik direct mocht beginnen met mijn afstuderen. Niet alleen kan ik daardoor mijn opleiding afronden en kan ik me vervolgens gaan richten op andere manieren om mijn kennis te vergroten, maar ook om het product GTS-Online nog professioneler en beter schaalbaar te maken.

4. Projectopdracht

4.1. Situatie

Zoals in vorig hoofdstuk besproken, is GTS-Online een belangrijk product voor GTS-GRAL, wat naast het leveren van de wat traditionelere ICT diensten bij klanten intern een steeds groter aandeel krijgt in de omzet van ons bedrijf. Het aantal klanten stijgt en daarmee ook het aantal gewenste aanpassingen, gebruikersvragen en nieuwe wensen. Dat is logisch bij de manier waarop we dit product aanbieden: geen klant is hetzelfde en dus proberen we voor iedere klant een geschikte oplossing voor zijn probleem te maken. Daarbij proberen we uiteraard zo'n oplossing zo generiek mogelijk op te zetten om de herbruikbaarheid ervan te maximaliseren.

4.1.1. Helpdesk

Zoals al aangegeven: het aantal gebruikersvragen stijgt hard, soms nog harder dan het aantal gebruikers op het systeem. Om dit soort vragen enigszins gestructureerd aan te pakken gebruiken we een helpdesksysteem, die we al enkele jaren in gebruik hebben, ook voor niet-GTS-Online klanten.

Het helpdesksysteem werkt overigens prima en dit of een soortgelijk helpdeskpakket moet ook altijd aanwezig blijven, zodat er een centrale locatie is waar incidenten en bijbehorende problemen geregistreerd worden, maar waar ook een kennisbank ontstaat van al eerder geboden oplossingen.

Waar de helpdesk echter ook steeds voor gebruikt wordt, is het doorgeven van administratieve wijzigingen: het wijzigen van gegevens van een gebruiker, de toegang tot een bepaalde beveiligde map of het aanmaken van een nieuwe e-mailadres. Voorheen had de klant zelf de mogelijkheid om dit soort zaken te regelen in hun eigen omgeving, maar in onze omgeving hebben ze slechts beperkt rechten om zaken te wijzigen. Het doen van wijzigingen rust dus op onze eigen schouders en naarmate het aantal gebruikers groter wordt, groeit het aantal wijzigingen stug mee.

Hierdoor is de wens ontstaan om de klant te faciliteren in het kunnen doen van wijzigingen, maar wel dat dit gecontroleerd uitgevoerd wordt. En aangezien er meerdere klanten gebruik maken van dezelfde systemen en ze logischerwijs geen inzage mogen hebben in elkaars gegevens, moet dit in een afgeschermde omgeving zijn.

4.1.2. Borging van informatie

Een ander belangrijk punt is het borgen van kennis over de manier waarop deze wijzigingen in de omgeving gedaan worden. Bij het opzetten van GTS-Online zijn er al een aantal scripts ontwikkeld, zodat bijvoorbeeld op een eenduidige manier een nieuwe klant toegevoegd kan worden en gebruikers aangemaakt kunnen worden.

Maar hoe meer klanten er bij komen, hoe groter de diversiteit die hierin toch blijkt te ontstaan en langzamerhand groeit het aantal scripts waarmee wijzigingen gedaan wordt de spreekwoordelijke pan uit. Daarnaast verdwijnt het overzicht naarmate de scripts langer worden, bijvoorbeeld het alsmaar toevoegen van functionaliteit. Verder dienen er, juist om de klant meer mogelijkheden te geven om componenten te wijzigen in onze omgeving, nog

meer scripts beschikbaar te komen zodat de wijzigingen altijd op dezelfde manier uitgevoerd worden.

Documentatie over al deze scripts en een (ver)beter(d) versiebeheer wordt hierdoor noodzakelijk.

4.1.3. Informatievoorziening

Als laatste groeit de vraag naar inzichtelijkheid voor zowel de klant als voor ons over wat er door de klant in gebruik is. Onze klanten betalen per maand een bedrag voor ieder gebruikersaccount of software licentie die ze in gebruik hebben, maar ook voor iedere PC, laptop of beeldscherm die ze per maand huren. Nu wordt iedere maand weer een overzicht gemaakt van alles wat er die maand gebruikt is om een correcte factuur te kunnen sturen.

Maar ook de klant wil graag inzicht krijgen van de in gebruik zijnde accounts, computers en software licenties. Zo kan de klant makkelijker de kosten drukken: hoe minder er in gebruik is, hoe minder de klant hoeft te betalen.

4.2. Afstudeeropdracht

De combinatie van de wens voor het automatiseren van een aantal veelvoorkomende taken, het voor een deel beschikbaar maken van deze taken aan eindklanten en het inzichtelijk maken van de diensten en producten waar de klant gebruik van maakt, vormt de kern van mijn afstudeeropdracht.

De informatie over de (opnieuw) te automatiseren taken zal geborgd worden door de workflow ervan te documenteren en de functionele (welke informatie is er nodig) en niet-functionele eisen (waarom worden taken op een bepaalde manier opgelost en niet op een andere) er van vast te leggen. Deze documentatie zal eerst door de engineers van GTS-GRAL gecontroleerd worden op juistheid alvorens deze te implementeren.

Niet alle taken dienen voor iedere klant en medewerker van een klant beschikbaar te komen. De verschillende taken zullen aan rollen gekoppeld moeten worden, zodat vervolgens een gebruiker één of meerdere rollen toebedeeld kan krijgen en hierdoor meer of minder mogelijkheden tot zijn of haar beschikking krijgt. Deze rollen zullen in het project veelvuldig gebruikt worden om een workflow mee te kunnen maken.

De software waarmee de opdracht uitgevoerd zal worden zijn twee pakketten uit de System Center 2012 reeks van Microsoft: Service Manager en Orchestrator. Service Manager is gericht op het centraal registreren van incidenten, wijzigingen en de achterliggende workflow hierbij, terwijl met Orchestrator systeembeheertaken overzichtelijk uitgevoerd kunnen worden. Deze twee pakketten kunnen goed in combinatie met elkaar gebruikt worden en in de toekomst kunnen ook andere pakketten van Microsoft System Center die al in gebruik zijn gekoppeld worden.

Aangezien met de te gebruiken software ook de mogelijkheid bestaat om andere helpdeskvragen te registeren en af te handelen, zal dit ook meteen worden meegenomen in de scope van het project.

5. Projectaanpak

5.1. Fasering

Het project is in grote lijnen op te delen in de volgende fasen, welke ik heb overgenomen uit DSDM en goed van toepassing zijn op hoe het project is opgedeeld.

5.1.1. Feasibility Study

In deze fase wordt er onderzoek gedaan naar de mogelijkheden van de te gebruiken tools en zal het afstudeervoorstel worden ingediend. Uit de afstudeeropdracht bleek al dat de software die gebruikt moest worden om de gewenste oplossingen op te leveren System Center 2012 Service Manager (Service Manager) en System Center 2012 Orchestrator (Orchestrator) van Microsoft moesten zijn.

Onze omgeving is, voor zover mogelijk, opgezet met software van Microsoft. Dat uit zich niet alleen in het feit dat al onze werkplekken en servers voorzien zijn van een besturingssysteem van Microsoft, maar ook dat de software die we gebruiken om alles te beheren, indien mogelijk, van Microsoft afkomstig zijn. We hebben al diverse beheerpakketten van Microsoft System Center in gebruik en kunnen daardoor deze twee nieuwe pakketten hiermee goed integreren. Ik zal hier in het hoofdstuk Realisatie verder op in gaan.

5.1.2. Business Study

In deze fase zullen de mogelijkheden van de software en de mogelijkheden hiermee voor het implementeren van de gewenste producten verder onderzocht. Ten behoeve van het plan van aanpak wordt er een overzicht van de eisen opgesteld en de (deel)producten bepaald. Het plan van aanpak wordt ingediend aan het eind van deze fase, waaruit duidelijk blijkt wat de wensen en eisen zijn die gesteld zijn aan het eindproduct.

5.1.3. Functional model iteration

Voor iedere taak zal er vastgelegd worden wat de functionele en niet-functionele eisen zijn en wat voor workflow er nodig is om de taak uit te voeren. Door middel van prototyping worden deze specificaties getoetst, nadat de specificaties zijn gecontroleerd door de engineers van GTS-GRAL. Dit zal zowel voor de beheertaken, informatievoorziening als de gebruikerstaken gedaan worden.

5.1.4. Design and build iteration

In deze fase zullen de prototypes van de verschillende deelproducten verder uitgewerkt en al deels opgeleverd en steeds meer geïntegreerd worden tot een samenhangend geheel.

5.1.5. Implementation

In deze fase zullen de verschillende opgeleverde producten getest worden door geselecteerde gebruikers in de eigen organisatie en bij diverse klanten. Op dit moment kan er nog voor worden gekozen om (bepaalde onderdelen) opnieuw of anders op te zetten.

5.2. Planning

Het project zal uitgevoerd worden gedurende een periode van ongeveer 26 weken, waarbij er per week ongeveer 20 uur aan het project gewerkt kan worden op kantoor. Daarnaast zal ik nog 8 uur per week in mijn eigen tijd besteden aan het project, waarin ik voornamelijk verslagen en documentatie zal uitwerken.

Ik verwacht de hierop volgende planning aan te kunnen houden. Tussen haakjes staat in welke fase deze werkzaamheden vallen.

Periode	*Werkzaamheden*
November t/m half januari	• Afstudeervoorstel indienen (wk 47) • Onderzoek naar mogelijkheden van de te gebruiken software (wk 45, 46) • Plan van Aanpak opstellen (wk 48 - 4) • Plan van Aanpak indienen (wk 4)
Januari t/m half april	• Basis implementatie van de te gebruiken software (wk 4 - 7) • Uitwerken van de benodigde processen en uitzoeken hoe deze zo effectief mogelijk geïmplementeerd kunnen te worden in de te gebruiken software. (wk 8 - 15) • Implementeren van deze processen (wk 8 - 15) • Inrichten van de portals (wk 7)
April	• Portals beschikbaar maken voor testen (wk 14) • Mogelijke problemen oplossen t.b.v. werkend eindproduct (wk 14 - 18)
Mei	• Uitloop (wk 19 - 21) • Afronding scriptie (wk 19 - 21) • Inleveren scriptie op 29-05-2012 (wk 22)

Deze planning is ook in Bijlage 3 te vinden, in de vorm van een Gantt diagram.

5.3. Kwaliteitsbewaking

Het grootste risico aan het project is dat het opgeleverde eindproduct niet naar wens is van GTS-GRAL doordat deze niet goed bruikbaar en de kwaliteit onvoldoende is. Om dit te voorkomen zal er gedurende het gehele project regelmatig overleg worden gevoerd over de voortgang van het project.

De voortgang van het project zal dan ook niet alleen tijdens het tweewekelijks werkoverleg plaats vinden met de rest van mijn collega's, maar ook op een aantal nader te bepalen momenten met alleen mijn leidinggevende (tevens bedrijfsbegeleider). Ik wil dit overleg maandelijks inplannen om te voorkomen dat de verwachtingen van beide partijen teveel uiteen gaan lopen tijdens het project.

Ook zal het van te voren documenteren en modelleren van de taken die het systeem aan het project moet kunnen uitvoeren zorgen voor een stuk kwaliteitsbewaking. Deze modellen en bijbehorende documentatie kan

voordat deze worden geïmplementeerd worden bekeken door mijn collega's en kunnen.

5.4. Projectorganisatie

Dit project zal ik volledig zelfstandig uitvoeren. Uiteraard zal er echter wel overleg zijn met mijn directe collega's en leidinggevende om beslissingen te nemen over hoe bepaalde technische zaken geïmplementeerd dienen te gaan worden. De op te leveren producten dienen namelijk wel zo opgeleverd te worden dat deze in de toekomst, met het oog op nieuwe klanten met mogelijk andere wensen en eisen, ook gebruikt kunnen gaan worden.

5.4.1. Bedrijfsgegevens

GTS-GRAL Nederland BV

Adres:	Turbinestraat 3b
	3903 LV Veenendaal
Telefoonnummer:	0318-550884
Bedrijfsbegeleider:	Henk Bloemendal
E-mailadres begeleider:	h.bloemendal@gtsgral.nl

5.4.2. Persoonsgegevens

Mijn eigen gegevens zijn als volgt:

Naam:	Johan de Haan
Telefoonnummer:	0318-550884
Mobiel nummer	0628532362
Emailadres	j.dehaan@gtsgral.nl

5.4.3. Docentbegeleider

De gegevens van de docentbegeleider, tevens eerste examinator:

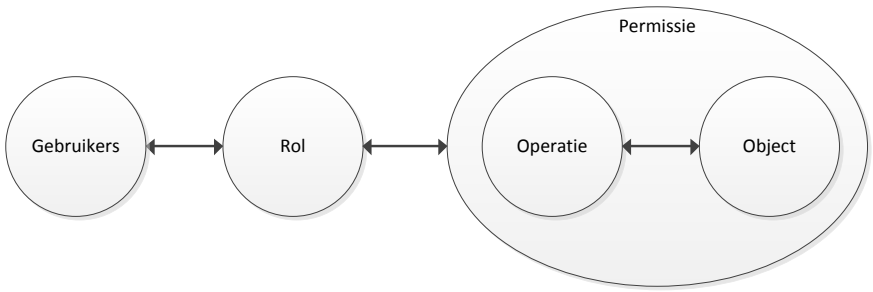
Naam:	Peter van Rooijen
Emailadres	peter.vanrooijen@hu.nl

6. Rollen

Niet iedere medewerker van onze klanten krijgt zomaar toegang tot alle functionaliteit die we willen gaan aanbieden via de Self Service Portal. In dit hoofdstuk wil ik dieper in gaan over hoe het verlenen van toegang tot objecten in theorie verloopt, hoe dit in de huidige situatie is geregeld en op welke manier ik de rollen beter wil gaan gebruiken en scheiden.

6.1. Role Based Access Control

In het Functioneel ontwerp (Bijlage 2) wordt uitgebreid ingegaan op het de theorie, maar ik ga ook hier eerst kort in op de theorie achter Role Based Access Control, vaak afgekort tot RBAC. RBAC is de algemene term voor het verlenen van toegang tot objecten op basis van een rol. Met onderstaande afbeelding wordt dit goed duidelijk gemaakt:



Figuur 2 Role Based Access Control

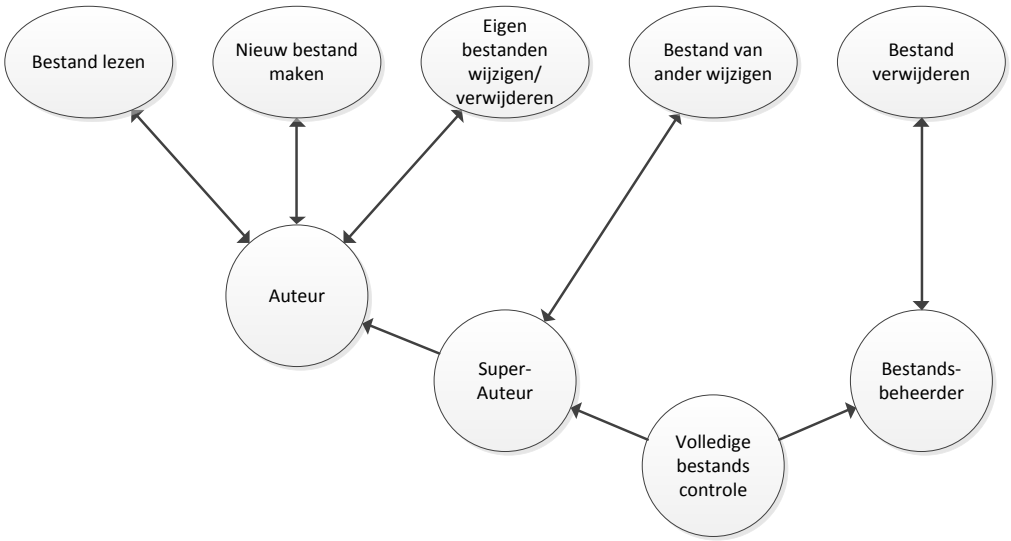
Een gebruiker krijgt bij het gebruik van RBAC niet direct rechten op bijvoorbeeld een bestand of een map binnen het systeem, maar krijgt een rol toebedeeld. Aan deze rol is een bepaalde permissie gekoppeld. Een permissie bestaat altijd uit het toestaan van een bepaalde operatie op een object, zoals bijvoorbeeld het lezen (operatie) van een bepaald document (object).

6.1.1. Voordelen

Het beheren van rechten wordt hiermee een stuk overzichtelijker. Het definiëren van rechten op een object (en eventueel de objecten die daaronder liggen, zoals een map met documenten) hoeft slechts één keer. Het toekennen of ontnemen van rechten aan gebruikers wordt daardoor ook makkelijker en er is gemakkelijker een overzicht te maken welke rechten een gebruiker heeft in een IT omgeving.

6.1.2. Overerving

Door de algemene opzet van RBAC kan deze techniek op veel manieren worden toegepast en desgewenst ook uitgebreid. Ook is er vaak de mogelijkheid tot overerving van rollen, waardoor en boomstructuur gemaakt kan worden van rollen en de onderliggende permissies. Een voorbeeld uit het Functioneel ontwerp is te zien in de volgende afbeelding.



Figuur 3 Voorbeeld van overerving van permissies

In bovenstaande afbeelding zijn de permissies (rechten op één of meerdere objecten) aangegeven met ellipsen, de rollen zijn cirkels. Goed is te zien dat het bijvoorbeeld mogelijk is om meerder permissies aan een rol toe te kennen (rol Auteur): een rol hoeft niet alleen gekoppeld te zijn aan een Permissie, maar kan ook met een andere rol kan worden gekoppeld (rol Super-Auteur). Ook een rol die alleen andere sub rollen bevat is niet ondenkbaar (rol Volledige bestands controle).

6.2. Huidige rollen

Met de theorie over RBAC in het achterhoofd ben ik gaan uitzoeken of er in grote lijnen (op organisatie niveau) verschillende rollen te beschrijven zijn. Dat bleek het geval, al zijn die niet zo specifiek vastgelegd.

6.2.1. Rollen binnen GTS-GRAL

Op basis van het organigram van GTS-GRAL bijvoorbeeld (zie Bijlage 4) kan al verschil worden gemaakt tussen de Administratie, Support- en System Engineers en de “gewone gebruikers”.

Aangezien wij als GTS-GRAL zelf ook klant zijn van onze eigen dienst is iedereen in de eerste plaats gebruiker. Daarnaast hebben uiteraard de personen die zich bezig houden met de techniek een andere rol, maar ook de persoon die zorgt voor de administratie heeft meer inzicht nodig in het systeem om bijvoorbeeld tot een juiste facturatie te komen.

Maar ook binnen de medewerkers in de techniek is er verschil: de Support Engineer heeft niet evenveel rechten in de GTS-Online omgeving als de System Engineers. Mocht de Support Engineer rechten tekort komen om een bepaalde aanpassing te doen, die wel wenselijk is voor zijn werkzaamheden, dan proberen we altijd hier een passende oplossing voor te verzinnen, maar dit is dan weer maatwerk.

6.2.2. Rollen bij de klant

Bij de meeste van onze huidige klanten zijn zo’n drie rollen die de boventoon voeren: de “beslissersrol”, de “lokale beheerdersrol” en de “gebruikersrol”.

Voordat de klant gebruik ging maken van onze GTS-Online dienst was er meestal al een medewerker die zich wat meer met de ICT zaken bezig hield dan de rest van de medewerkers, een lokale beheerder. Deze persoon was (en is dat vaak nog steeds) het eerste aanspreekpunt voor problemen op IT gebied. Aangezien wij over het algemeen alleen ondersteuning op afstand zullen geven, is het erg handig dat er bij de klant zelf nog iemand is die verstand heeft van IT en kleine dingen zelf op kan lossen.

Is er een wijziging nodig die organisatorische of financiële gevolgen heeft, dan worden die meestal bevestigd door personen met de “beslissersrol”. De gewone gebruiker heeft niet veel rechten, zowel op het systeem als op organisatorisch vlak: bij belangrijke wijzigingen zal altijd de persoon met de beslissersrol worden geraadpleegd.

6.3. Gewenste rollen

We willen de klant via de Self Service Portal veel meer mogelijkheden geven binnen GTS-Online om zelf aanpassingen te doen. We willen graag af van de situatie dat gewone gebruikers helemaal niets kunnen, en aanpassingen door één of enkele personen in de organisatie gedaan moeten worden. Als bijvoorbeeld een gebruiker in dienst komt, dan zullen de medewerkers van HRM dit als eerste weten en ook alle gegevens beschikbaar hebben: zou toch veel efficiënter zijn als zij zelf een gebruiker kunnen aanmaken, rechten kunnen aangeven en wanneer deze gebruiker in dienst komt in plaats van dat deze gegevens via via bij ons terecht komen.

In het Plan van Aanpask zijn al diverse taken genoemd die we graag op korte termijn beschikbaar zouden willen hebben. Op basis van die taken heb ik in het functioneel ontwerp (Bijlage 2) een aantal rollen opgesteld, waarbij een aantal overervingen plaats vinden. Een aantal voorbeelden van de belangrijkste rollen:

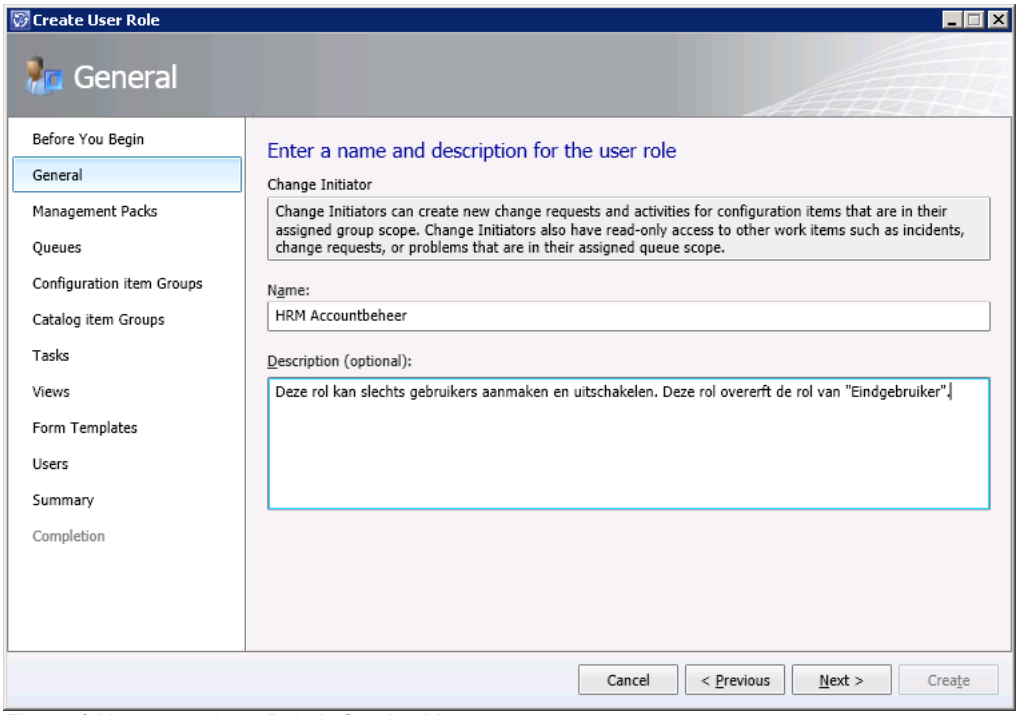
- Gewone gebruiker
  - Aanmaken, wijzigen en verwijderen ticket
- Accountbeheer HRM
  - Aanmaken en uitschakelen gebruikersaccount
- Accountbeheer uitgebreid
  - Overerft de functies van “Accountbeheer HRM”
  - Verwijderen en wijzigen gebruikersaccount
  - Wachtwoord resetten
- Account- en groepsbeheer
  - Overerft de functies van “Accountbeheer uitgebreid”
  - Toevoegen en verwijderen van accounts uit beveiligings- en distributiegroepen
- Werkplekbeheer
  - Computeraccounts verwijderen en toevoegen
- E-mailbeheer
  - Distributiegroepen toevoegen, verwijderen en lidmaatschap wijzigen;
  - Resource mailboxen aanmaken, verwijderen, rechten wijzigen en e-mailadressen toevoegen

Zoals eerder aangegeven zijn deze rollen en nog een aantal nog uitgebreidere rollen opgenomen in een overzichtelijke tabel in het functioneel ontwerp.

6.4. Rollen binnen Service Manager

Binnen Service Manager kunnen deze rollen vrij gemakkelijk gedefinieerd worden. Standaard zijn er zelfs al 13 rollen die binnen een ITIL omgeving van belang zijn, zoals “Problem analysts”, “Change Managers” en “End Users”. Deze rollen zijn echter niet niet van toepassing op ons omgeving, vanwege het feit dat we te maken hebben met meerder klanten in dezelfde omgeving. Dit heeft gevolgen voor de installatie (zie ook 8.4 Multi-tenancy), maar ook voor de manier waarop rollen moeten worden verdeeld: een persoon in de Change Manager rol mag niet zomaar de changes of incidenten van een andere klant zien.

Ik zal dus nieuwe rollen maken, onder andere op basis van de tabel uit het Functioneel Ontwerp. Bij het aanmaken van een rol wordt een selectie gemaakt van welke objecten deze rol mag gebruiken, wat voor wijzigingen deze rol mag doen op deze objecten en welke Service Requests of aanvragen deze rol mag gebruiken om deze wijzigingen door te voeren. Deze rol kan vervolgens worden gekoppeld aan Active Directory gebruikersaccounts of aan Active Directory groepen.



Figuur 4 Maken van User Role in Service Manager

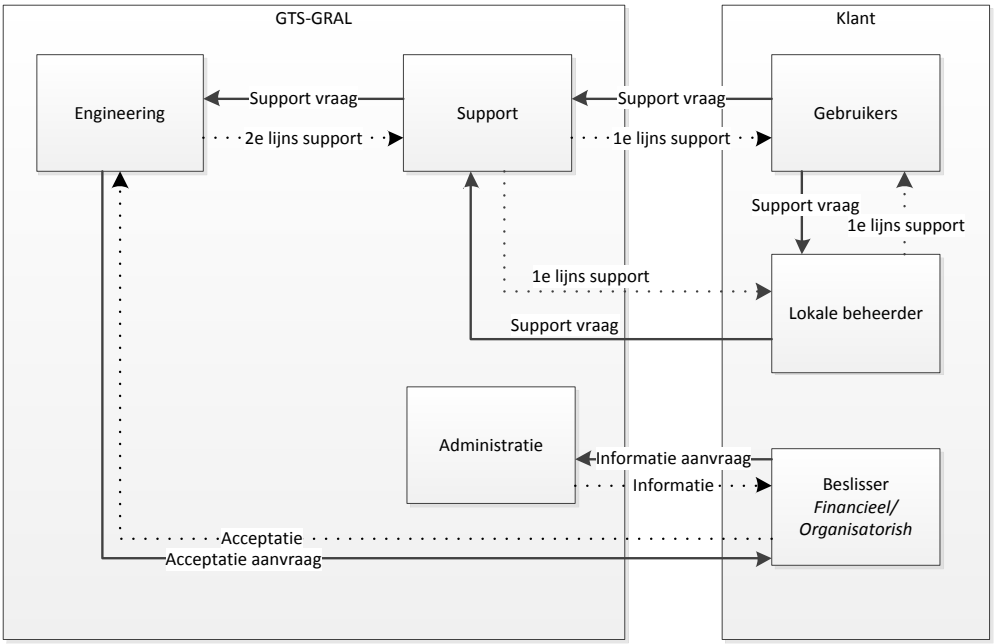
7. Proces verbetering

Zoals al uit het vorige hoofdstuk duidelijk werd, zijn de rollen die medewerkers bij onze klanten vervullen niet of nauwelijks vastgelegd en ook met de beheerprocessen is dat het geval. Medewerkers van klanten zijn vaak nog gewend om eerst de (voormalig) IT beheerder aan de mouw te trekken voor vragen of problemen, terwijl wij veel liever hebben dat zij veel van dit soort vragen bij ons neerleggen. Niet omdat wij zo graag de controle hebben over alles wat er op IT gebied gebeurt, maar voornamelijk omdat er vaak ruis ontstaat over wat precies het probleem is waar de gebruiker tegen aan loopt.

Ik heb een overzicht gemaakt van hoe de processen nu lopen en hoe deze zouden kunnen gaan verlopen door gebruik te gaan maken van de Self Service Portal. De zaken die hier op volgen zijn overigens nog een stuk uitgebreider besproken in het functioneel ontwerp (zie bijlage 2).

7.1. Huidige situatie

Voor het omschrijven van de huidige situatie heb ik gebruik gemaakt van de rollen die ik eerder gedefinieerd heb. Voor de klant zijn dat de gebruikers, de lokale beheerder en de beslisser; voor GTS-GRAL is dat de Support Engineering, System Engineering en de Administratie. In volgende figuur zijn in hoofdlijnen de processen weergegeven die voor dit project van belang zijn.



Figuur 5 Processen huidige situatie

Een korte uitleg bij bovenstaande figuur: gebruikers kunnen nu hun problemen zowel bij de lokale beheerder als bij ons neerleggen. Bespreken ze hun probleem of vraag met de lokale beheerder dan zal deze persoon de vraag vaak alsnog bij onze Support Engineer neerleggen.

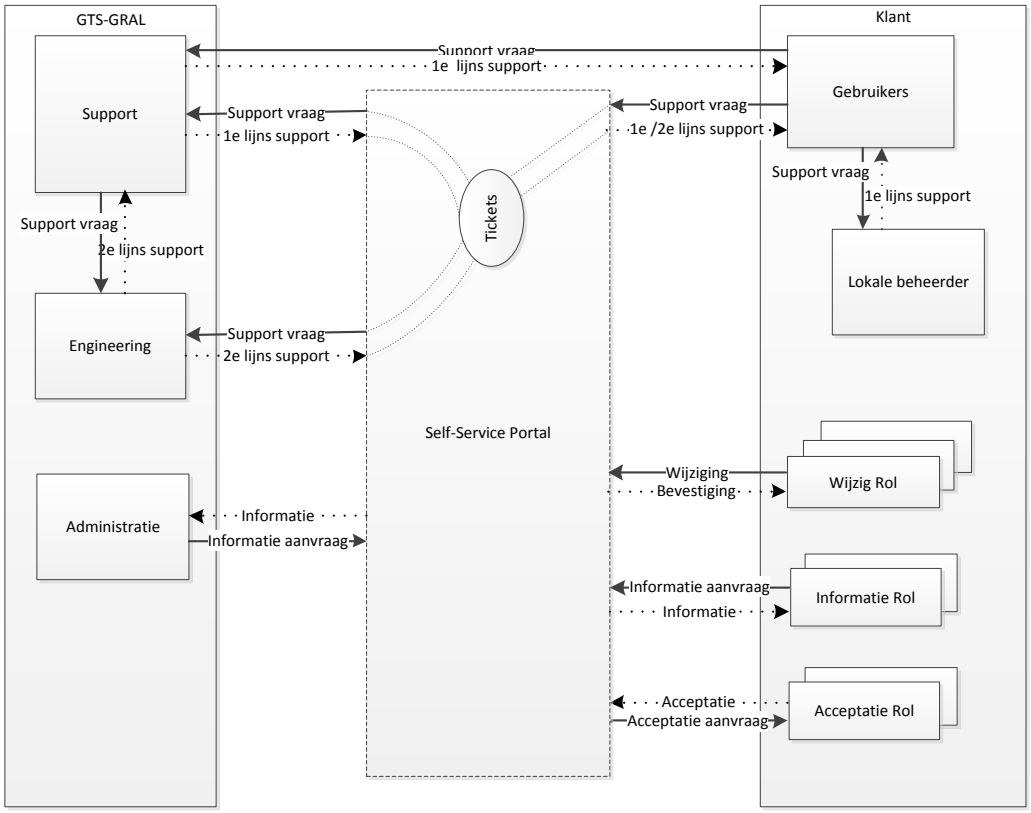
Binnen GTS-GRAL zal de Support Engineer altijd proberen eerst zelf een probleem aan te pakken. Lukt dat niet, vanwege te weinig rechten of kennis,

dan zal het probleem bij de System Engineers terecht komen die de benodigde ondersteuning geven. Is er een wijziging benodigd die organisatorische of financiële gevolgen heeft, dan wordt er door ons zelf contact gelegd met de persoon met de beslissersrol of deze wijziging inderdaad doorgevoerd zal gaan worden. Wie dit precies is, is vaak niet vastgelegd, dus soms is het een flinke puzzel of zoektocht om uit te zoeken welke persoon we hiervoor moeten vragen.

Deze beslisser krijgt aan het eind van de maand ook de factuur op zijn of haar bureau en wil hier nog wel eens extra informatie over hebben. Hierover wordt dan contact opgenomen met onze Administratie die de gegevens verzamelt en de benodigde informatie verstrekt aan de klant. Dit alles zijn handmatige acties.

7.2. Gewenste situatie

De grootste gewenste verandering is niet het definiëren van meer rollen voor de gebruikers, dat heeft alleen als gevolg dat het groeiend aantal mogelijkheden voor de klant overzichtelijk en beheersbaar blijft. Vooral het toevoegen van de Self Service Portal zal een grote verandering geven, wat ook blijkt uit de volgende figuur.



Figuur 6 Processen gewenste situatie

Het blijft uiteraard mogelijk voor gebruikers om een vraag direct bij onze Support Engineer neer te leggen of bij de Lokale beheerder. Maar door steeds meer functionaliteit beschikbaar te stellen via de Self Service Portal verwachten we dat ook de gebruikers hier steeds meer gebruik van gaan

maken. Zeker als ze merken dat wijzigingen gemakkelijker en sneller door te voeren zijn via de Portal dan door dit mondeling te bespreken.

Ook voor ons zelf zal het gemakkelijker moet worden indien medewerkers van de klant gebruik maken van de functionaliteit in de Self Service Portal. Bijvoorbeeld als het gaat om het accepteren van wijzigingen, zoals bij het toevoegen van personen aan een applicatie waar extra geld voor betaald moet worden i.v.m. licenties.

En ook het laatst genoemde punt in de paragraaf over de huidige sitatie, het opvragen van informatie, zou efficiënter kunnen gaan. Administratie hoeft niet meer handmatig overzichten te maken van in gebruik zijnde systemen en gebruikersaccounts, maar deze zal door de Self Service Portal beschikbaar gemaakt kunnen worden.

8. Product configuratie

Uit de projectopdracht die ik heb gekregen blijkt duidelijk dat er de wens is om de gewenste functionaliteit te realiseren door gebruik te gaan maken van de Microsoft System Center oplossingen Service Manager en Orchestrator. Deze oplossingen zijn beide gericht op grote bedrijven en op veel verschillende manieren in te richten.

In dit hoofdstuk beschrijf ik hoe deze twee oplossingen samen gebruikt kunnen worden om de gewenste functionaliteit te bieden. Maar ik zal beginnen met te bespreken wat de reden nou precies is dat we juist deze twee pakketten wilden gaan gebruiken voor dit project.

8.1. Waarom Microsoft System Center?

Microsoft System Center is de verzamelnaam van diverse oplossingen waarmee Microsoft omgevingen kunnen worden beheerd. Een greep uit de meest gebruikte System Center oplossingen zijn:

- **Operations Manager**: hiermee kunnen niet alleen Windows servers en computers worden gemonitord, maar ook Linux-gebaseerde systemen en zelfs netwerkapparatuur, zoals Cisco switches.
- **Configuration Manager**: hiermee kunnen grote groepen Windows machines geconfigureerd en beheerd worden door uitgebreid patch-management, distributie van software, het verzamelen van gegevens over de gebruikte hard- en software op de in het netwerk gebruikte systemen en diverse tools voor het op afstand beheren van machines.
- **Virtual Machine Manager**: met deze software kunnen Hyper-V hosts en de daarop geïnstalleerde Virtuele Machines (VMs) worden beheerd, nieuwe VMs geïnstalleerd en geconfigureerd worden en VMs live gemigreerd worden naar andere Hyper-V hosts.

Naast deze veelgebruikte oplossingen voor back-up (*Data Protection Manager*), het beheren van mobiele apparaten (*Mobile Device Manager),* het inrichten van beheerprocessen, grotendeels gebaseerd op ITIL (*Service Manager*) en één van de nieuwste oplossingen is Orchestrator (voorheen *Opalis*[1]): een oplossing waarmee zeer uitgebreide taken, op zeer diverse platformen kunnen worden geautomatiseerd door gebruik te maken van Runbook Automation[2].

[1] http://technet.microsoft.com/en-us/systemcenter/hh913943
[2] http://en.wikipedia.org/wiki/Runbook#Run_Book_Automation

Figuur 7 Verschillende onderdelen van System Center 2012[3]

8.1.1. Integratie

Voor de GTS-Online omgeving gebruikten we al bijna alle System Center oplossingen voordat ik begon met dit project. Ook Service Manager is al wel eens geïnstalleerd geweest in de omgeving, maar door gebrek aan tijd is de implementatie hiervan nooit echt van de grond gekomen. Echter, de aankondiging van Orchestrator, en de nauwe integratie ervan met Service Manager, wekte de interesse van verschillende medewerkers.

Naast de integratie tussen deze twee oplossingen integreren beide oplossingen gemakkelijk met de andere al beschikbare System Center pakketten, maar ook met andere onderdelen in een Windows omgeving, zoals bijvoorbeeld:

- Active Directory (centrale database waarin o.a. gebruikers- en groepsobjecten van een Windows domein zijn opgeslagen);
- Hyper-V servers (waarop de gehele GTS-Online omgeving op staat te draaien in de vorm van Virtuele Machines) en
- Exchange (groupware oplossing voor o.a. e-mail, agenda's, etc.).

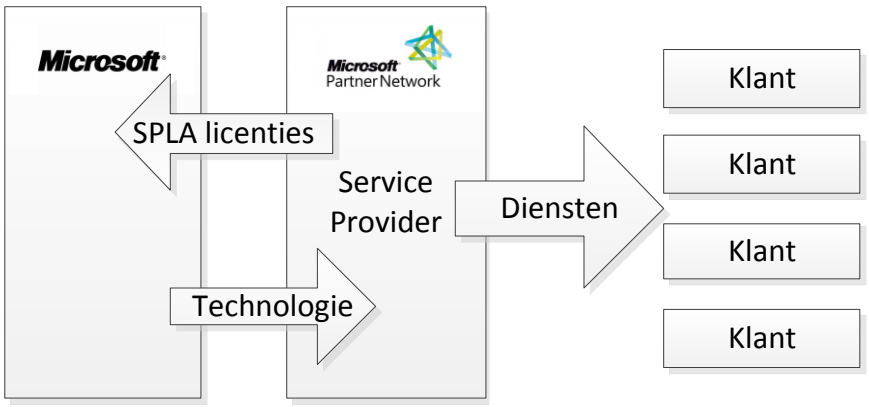
8.1.2. Licenties

Niet alleen de integratie tussen de verschillende oplossingen deed ons kiezen voor de combinatie van Service Manager en Orchestrator voor het verbeteren van onze dienstverlening richting onze klanten. Ook licentie technisch is het een logische stap. GTS-GRAL is een zogeheten Service Provider met haar GTS-Online omgeving: wij leveren diensten aan onze klanten waarbij de klanten zelf niet voor hun licenties hoeven te betalen.

[3] http://www.microsoft.com/en-us/server-cloud/system-center/datacenter-management-capabilities.aspx

Uiteraard moet voor iedere Office of Windows installatie wel een licentie betaald worden. Voor de klant zit dat in de prijs inbegrepen die zij aan ons betaald, GTS-GRAL betaald per maand de op dat moment in gebruik zijnde licenties aan Microsoft. Dit gebeurt door gebruik te maken van het SPLA-licentiemodel[4] van Microsoft, waarmee per maand voor de producten die in gebruik zijn wordt betaald.

Niet alleen Windows en Office licenties zijn hier bij inbegrepen. Ook de diverse System Center oplossingen kunnen hiermee worden betaald. Voor het gebruik van Service Manager en Orchestrator hoeft dus geen of weinig extra licentie geld te worden betaald, terwijl voor de meeste soortgelijke oplossingen van Microsofts' concurrenten vaak een stevig bedrag moet worden betaald.



Figuur 8 SPLA licentie model: de klant betaald alleen de diensten, geen licenties

8.1.1. Functionaliteit

Ook de functionaliteit die beschikbaar komt het installeren van de twee oplossingen heeft natuurlijk te maken gehad met de keuze. Ik zal van beide uitleggen wat de toegevoegde waarde is voor dit project.

8.1.1.1. Service Manager

Op dit moment gebruiken we al een zogeheten ticketsysteem. Problemen en vragen worden geregistreerd als ticket en worden vanuit dit ticketsysteem behandeld. Service Manager biedt nog veel meer functionaliteit dan zo'n standaard ticket systeem, waaronder:

- Verschillende soorten werkitems die beter aansluiten bij ITIL, zoals incidenten, problemen, changes en activiteiten;
- Een uitgebreide CMDB (configuratie management database) waar goed in kan worden bijgehouden wat de status is van de verschillende objecten (gebruikersaccounts, computers, servers, etc) is in onze omgeving;
- Self Service Portal. Bij ons huidige ticketsysteem zit ook een website waarmee gebruikers tickets kunnen aanmaken, maar hier zit niet de mogelijkheid in om deze meteen te koppelen aan items in de CMDB. Verder kunnen vanuit deze Self Service Portal ook Change Requests

[4] https://partner.microsoft.com/belux-nl/licensing/licensingprograms/40059322

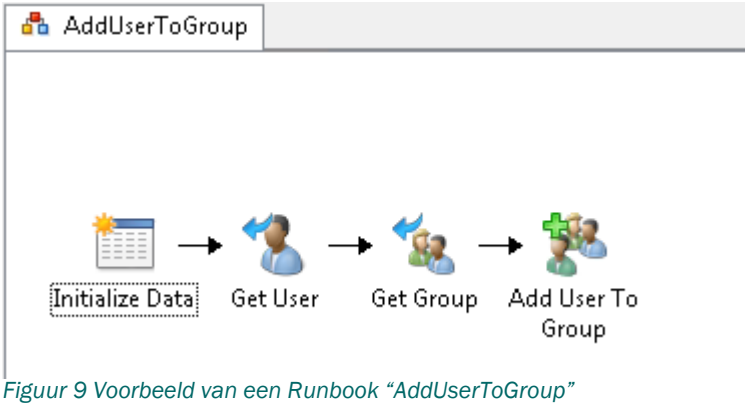
worden ingediend die door gebruik te maken van Orchestrator automatisch kunnen worden geïmplementeerd.

8.1.1.2. Orchestrator

Op dit moment worden veel wijzigingen gedaan door gebruik te maken van zeer veel losse scripts. De hoeveelheid versies is niet meer na te gaan en de precieze functionaliteit is soms ook lastig te achterhalen uit de scripts.

Met Orchestrator kan deze functionaliteit grotendeels worden opgenomen op een stuk overzichtelijkere manier. In Orchestrator maak je geen script, maar een Runbook, een soort van workflow van allerlei activiteiten die in chronologische volgorde worden afgewerkt. Veel van deze activiteiten zijn standaard beschikbaar en anders vaak uit te breiden met zogeheten Integration packs. Mocht er voor een bepaalde aanpassing geen standaard activiteit beschikbaar zijn, kan er altijd nog een stukje zelf gemaakt script worden uitgevoerd.

Vanuit een Workflow kunnen ook andere Runbooks worden gestart. Verder kunnen gemakkelijk parameters en andere gegevens worden doorgegeven van de ene naar de andere activiteit. Een Runbook wordt gestart met bepaalde parameters waarmee de rest van de activiteiten gevolgd worden.



Figuur 9 Voorbeeld van een Runbook "AddUserToGroup"

Zoals ook in bovenstaand voorbeeld te zien is, is een Runbook zelfs voor een leek te begrijpen. De functionaliteit van iedere activiteit wordt gauw duidelijk door de afbeelding en de titel. Ook het debuggen van een Runbook is vaak velen malen gemakkelijker dan wanneer er gebruik gemaakt wordt van een script.

8.2. Installatie

Ook al hebben de verschillende onderdelen in de System Center reeks diepe integratie mogelijkheden met elkaar, het zijn wel echt los te gebruiken en te installeren pakketten. De installatie van Service Manager en Orchestrator omvat dus ook twee losse installaties. Een uitgebreid verslag over deze installaties is te vinden in Bijlage 5.

8.2.1. Release Candidate & Release To Manufacture

Op het moment van installeren van de software was van beide pakketten slechts de Release Candidate[5] beschikbaar. Een Release Candidate komt na het bèta testen en is dus over het algemeen bugvrij en waarna ook geen extra functionaliteit zal worden toegevoegd. Een bèta test wordt over het algemeen met een gesloten groep testgebruikers uitgevoerd, terwijl een Release Candidate (vaak afgekort tot RC) voor een groter publiek ter beschikking komt.

Pas begin april is de RTM (Release To Manufacturer[6]) versie beschikbaar gekomen. Deze bevat een aantal verbeteringen t.o.v. de nu geïnstalleerde Release Candidates en zal naar pas na dit project worden geïnstalleerd, aangezien voor dit project de stabiliteit van deze omgeving op basis van de Release Candidates voldoende is gebleken.

8.3. Integratie tussen Service Manager en Orchestrator

Met een standaard installatie van Service Manager en Orchestrator is het direct mogelijk om vanuit Service Manager een link te leggen met Orchestrator. Die functionaliteit zit standaard in de software van Service Manager inbegrepen in de vorm van zogeheten “connectors”. De twee connectors die voor dit project belangrijk zijn, zijn de connector met Orchestrator en die met Active Directory. Verbindingen vanuit Orchestrator naar andere pakketten gebeurt op basis van “integration packs”.

Als de connectie is gelegd tussen de twee pakketten, is het mogelijk om vanuit Service Manager een runbook in Orchestrator te starten en vanuit Orchestrator weer aanpassingen te doen in Service Manager. Uitgebreide informatie over hoe deze verbinding gelegd wordt en de stappen die gedaan moeten worden alvorens een runbook gestart kan worden in Service Manager wordt besproken in Bijlage 5 en dan met name de paragrafen “Integratie tussen Service Manager, Orchestrator en Active Directory” en “Services in de Self Service Portal”.

8.4. Multi-tenancy

Voor onze omgeving is één van de belangrijke onderdelen het scheiden van de klantgegevens. Aangezien dit een veel voorkomend onderwerp is in de ICT is hier ook een algemene term voor: multi-tenancy. Multi-tentant letterlijk vertaald betekent: meerdere huurders en dit komt goed overeen met de werkelijkheid: klanten kunnen bij ons software, resources en ondersteuning hierop afnemen.

Doordat er zo efficiënt mogelijk moet worden omgegaan met de middelen, werken onze klanten allemaal in dezelfde omgeving, maar mogen daarbij elkaars gegevens uiteraard niet kunnen in zien. Ze mogen zelfs van elkaar niet weten dat ze bestaan en daardoor zijn er op veel niveaus beveiligingsinstellingen aangepast om dat mogelijk te maken.

Ook in Service Manager hebben we hiermee te maken. Aangezien gebleken is dat dit nogal lastig is om te configureren en er erg veel tijd in is gaan zitten

[5] http://nl.wikipedia.org/wiki/Release_Candidate
[6] http://nl.wikipedia.org/wiki/Release_to_manufacturer

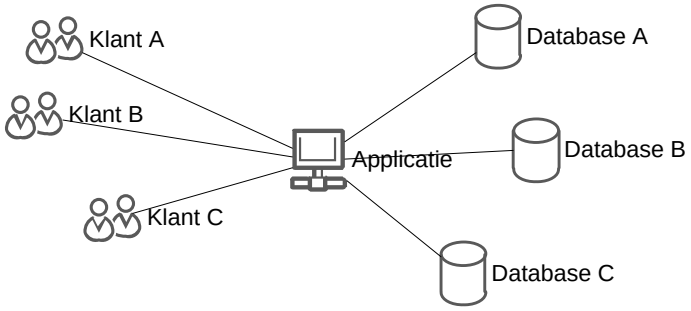
om dit op een eenduidige manier te lijf te gaan zal ik hier eerst in theorie op in gaan om vervolgens uit te leggen hoe ik dit heb opgelost voor Service Manager. Voor Orchestrator hoeft er geen enkele aanpassing gedaan te worden op dit moment, aangezien de runbooks alleen maar kunnen starten met bepaalde parameters en er geen klant specifieke gegevens in de runbooks zijn opgenomen. Het is dus niet mogelijk de runbooks zo te manipuleren dat deze op een of andere manier gegevens toont

8.4.1. Multi-tenancy in theorie

Multi-tenancy is in software op diverse manieren te configureren, Microsoft heeft hier een duidelijk artikel[7] over geschreven. In dit artikel wordt gesproken over drie manieren om de klantendata te scheiden:

1. Gescheiden databases
2. Dezelfde database, maar gescheiden schema's (groepen van tabellen, gescheiden op basis van beveiliging)
3. Dezelfde database, zelfde schema, maar de regels gescheiden door gebruik te maken van een extra kolom waarmee iedere regel kan worden geïdentificeerd als van een klant.

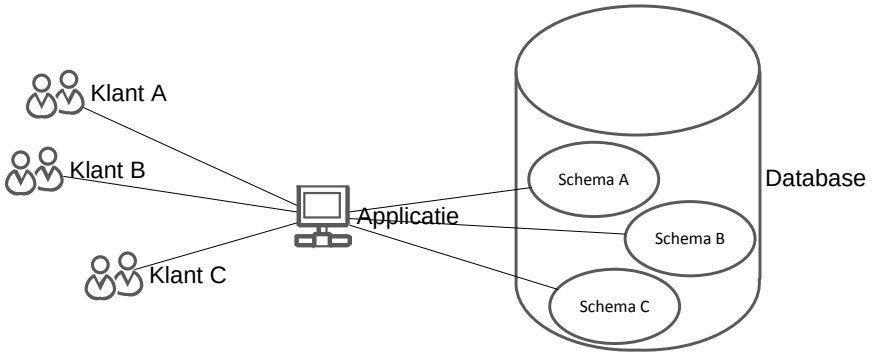
Gebruik maken van gescheiden databases is het gemakkelijkste om klantgegevens te scheiden, echter kost dat vaak bij onderhoud meer tijd en vaak meer licenties en capaciteit. Bij wijzigingen in het ontwerp van de database, door bijvoorbeeld extra functionaliteit, moeten deze wijzigingen op alle losse databases uitgevoerd worden. Ook updates in de database software dienen op alle losse databases uitgevoerd te worden.



Figuur 10 Gescheiden databases

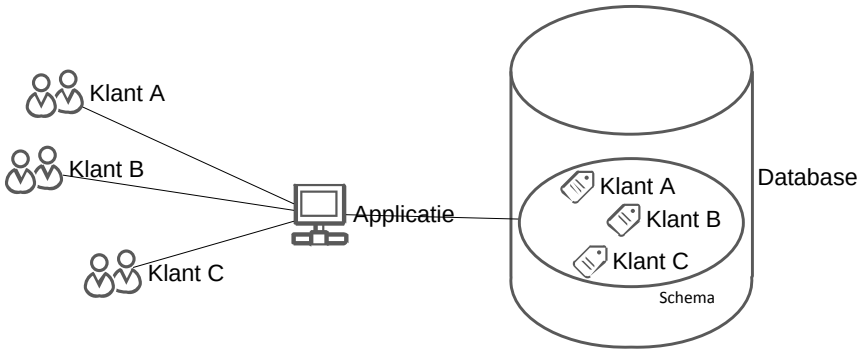
Het gebruik van één database geeft als voordeel dat de software gemakkelijker bijgewerkt kan worden, maar wijzigingen in de database dienen alsnog in de diverse schema's gedaan te worden. Verder moet er dus op er extra beveiliging ingesteld worden om te zorgen dat de klant alleen zijn eigen schema's kan benaderen en zien.

[7] http://msdn.microsoft.com/en-us/library/aa479086.aspx



Figuur 11 Zelfde database, gescheiden schema's

De derde oplossing is door alle klantgegevens in dezelfde database te zetten, in hetzelfde schema en in dezelfde tabellen, maar door de verschillende regels te scheiden met een extra kolom, bijvoorbeeld KlantID. Door gebruik te maken van een nummer in plaats van de naam van de klant is de enige manier om klanten niet direct inzage te geven in elkaars gegevens, maar de inhoud is uiteraard wel te bekijken.



Figuur 12 Zelfde database en schema, klantgegevens gescheiden door extra label

Het is met deze laatste constructie belangrijk om klanten niet direct toegang te geven tot de database en de daarbinnen horende tabellen, maar een front-end aan te bieden die alleen de gegevens weergeeft die de klant mag inzien. Verkeerd geschreven software kan dan alsnog gegevens beschikbaar stellen aan personen die deze niet mag in zien.

Er zijn echter ook voordelen, want er is veel minder server capaciteit nodig om de gegevens op te slaan en wijzigingen op de database en andere updates zijn veel gemakkelijker uit te voeren.

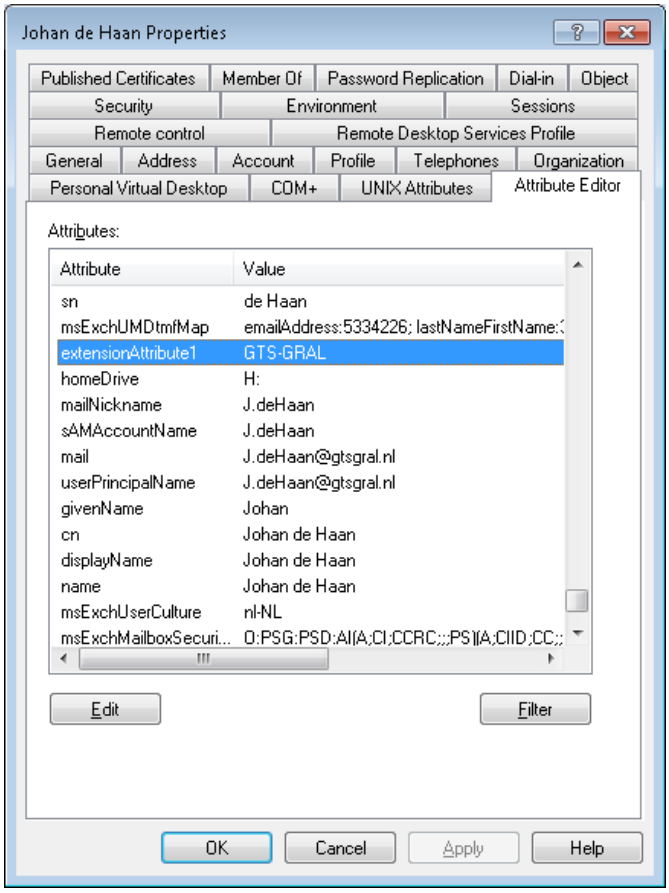
8.4.2. Multi-tenancy in Service Manager

Service Manager is "out-of-the-box" totaal niet geschikt voor een multi-tenant omgeving. Alle gebruikersaccounts, groepen en computers die geïmporteerd zijn in Service Manager komen allemaal in dezelfde pool van "Configuration Items" terecht. De enige manier om deze gegevens te scheiden is door een extra eigenschap te koppelen waarmee te ontdekken valt bij welke klant zo'n Configuration Item behoort.

Het scheiden van deze gegevens lijkt dus op de derde variant voor het scheiden van gegevens, zoals uitgelegd in de vorige paragraaf "Multi-tenancy

in theorie". Belangrijk is dus dat de software waarmee de klant zijn gegevens beheert alleen die items toont die bij deze klant hoort.

Het attribuut waarmee we de objecten van onze klanten in Active Directory identificeren is "extensionAttribute1" waarin de naam van de klant of een afkorting hiervan is opgenomen. Dit attribuut is ingevuld op zowel gebruikersaccounts als diverse andere objecten, zoals beveiligingsgroepen, en heeft voor de "klant" GTS-GRAL de waarde "GTS-GRAL".



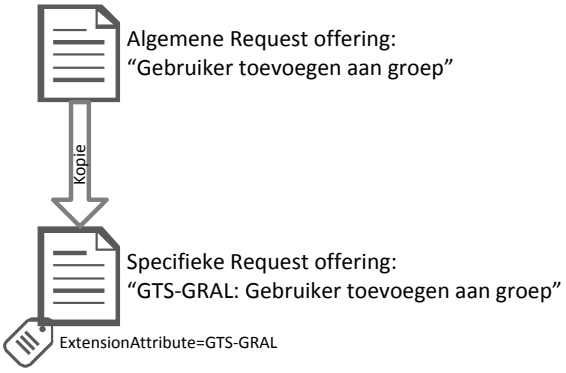
Figuur 13 ExtensionAttribute1 op het gebruikersaccount van Johan de Haan

Om de verschillende items in Service Manager te kunnen scheiden is zo'n zelfde attribuut "extensionAttribute1" aangemaakt waarin de klantnaam kan worden opgenomen. Deze attribuut wordt niet automatisch met de "Active Directory Connector" gesynchroniseerd, maar d.m.v. een eigen gemaakt PowerShell script die alleen maar de *extensionAttribute1* invult op basis van Domein en SAMAccountName die al wel gesynchroniseerd zijn met de Active Directory Connector. De methode die is gebruikt om *extensionAttribute1* te synchroniseren is uitgebreid besproken in Bijlage 5.

Gevolg van deze methode is dus dat, zoals al eerder uitgelegd in de paragrafen over "Multi-tenancy in theorie", de software verantwoordelijk is voor het scheiden van de klantgegevens. Bij het aanmaken van iedere Request Offering moet daardoor geconfigureerd worden dat er alleen Configuration Items (gebruikers, groepen en computers die beschikbaar zijn

in de CMDB van Service manager) beschikbaar mogen zijn op basis van *extensionAttribute1*, die dus gelijk moet zijn aan die van de ingelogde gebruiker. Wordt niet gedaan: dan komen er geen Configuration Items beschikbaar in de Request Offering: beter dan het weergeven van andermans gegevens!

In de praktijk bleek dat het niet mogelijk was om de *extensionAttribute1* van de op de Self Service Portal ingelogde gebruiker “at runtime” op te halen. Een aangeboden Request Offering moet dus specifiek voor een klant gemaakt worden. Om duidelijkheid te scheppen welke functies voor welke klant bedoeld is zal bij het ontwikkelen van een nieuwe Request Offering een soort algemeen “sjabloon” gemaakt moeten worden. Deze kan gekopiëerd worden en alleen door de naam te wijzigingen van de betreffende Request Offering en de waarde van de extensionAttribute1 kan met weinig inspanning de nieuwe aanvraag beschikbaar worden gemaakt voor een klant.



Figuur 14 Het aanpassen van “algemeen” Request Offering sjabloon naar een klantspecifieke Request Offering

8.5. Informatievoorziening

Naast het automatiseren van diverse veel voorkomende taken door gebruik te maken van Service Manager en Orchestrator, was ook een verbetering van de Informatievoorziening een onderdeel van mijn afstudeeropdracht. Uit de documentatie bleek dat het goed mogelijk was met Service Manager rapporten te maken die inzicht konden geven in de omgeving, in gebruik zijnde resources en rapportages over de aangemaakte incidenten en Service Requests.

Doordat ik erg veel tijd heb moeten besteden aan het uitzoeken van hoe multi-tenancy geïmplementeerd moest gaan worden in Service Manager, ben ik er niet aan toe gekomen hier erg veel aandacht aan te besteden. Wel bleek al snel dat ook het scheiden van klantgegevens in de rapportages lastig bleek. En al is dit wel mogelijk door gebruik te gaan maken van intensief maatwerk, dan nog bleken deze rapportages alleen in onze eigen management consoles beschikbaar en kunnen deze niet gemakkelijk worden opgevraagd via de Self Service Portal.

We hebben dus besloten dit deelproject op te schorten en hier later een goede oplossing voor te zoeken. Waarschijnlijk zal deze functionaliteit dan wel beschikbaar komen via de Self Service Portal, aangezien dit uiteindelijk gewoon een Sharepoint site is, waardoor een zelf geschreven web part of

andere web dienst gemakkelijk te integreren is. De juiste software hiervoor zal echter in een volgend project geselecteerd of ontwikkeld worden.

9. Modellen

Door het uitzoeken van hoe ik de producten moest configureren om deze samen te laten werken kreeg ik een steeds beter beeld van hoe een standaard Service Request moest gaan verlopen. Door het onderzoek naar hoe ik multi-tenancy moest gaan implementeren is dit beeld wel stevig aan verandering onderhevig geweest.

In het Functioneel Ontwerp (Bijlage 2) ga ik uitgebreid in op diverse modellen die ik heb gemaakt en ook hoe deze in werkelijkheid draaien in Orchestrator. Ik leg daar ook uit dat een aantal van de stappen die ik moet nemen in een Runbook in Orchestrator functioneel nodig zijn, maar de leesbaarheid niet ten goede komen. Ik heb er daarom voor gekozen de modellen op te zetten met Bizagi Process Modeler, waardoor ik deze op een iets hoger niveau kan uitleggen.

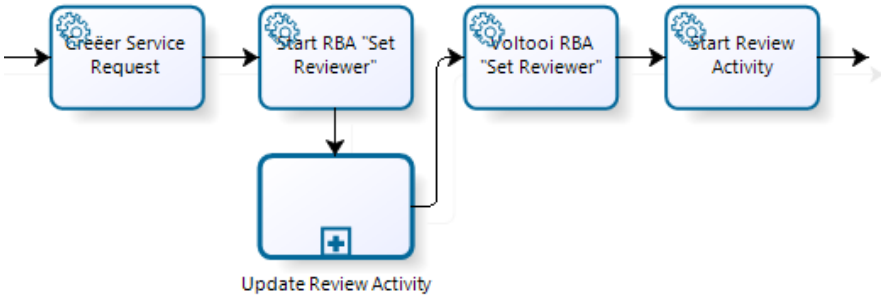
9.1. Algemeen Service Request

Bij het opzetten van de eerste modellen van een Service Request bleek een zelfde ontwerp steeds terugkomen. De volgende belangrijkste stappen komen daarbij vaak terug:

1. De gebruiker die een Service Request uitkiest in de Self Service Portal, deze invult en verstuurt.
2. De aanvraag moet soms wel, soms niet worden goedgekeurd door een eindverantwoordelijke vanwege organisatorische of financiële gevolgen.
3. Bij goedkeuring (of op het moment dat er geen goedkeuring nodig is) worden er één of meerdere runbooks gestart in Orchestrator die de wijziging doorvoeren.

Om dit zo generiek mogelijk op te zetten, bruikbaar voor alle klanten, heb ik een aantal aanpassingen moeten doen. Zo wordt de eindverantwoordelijke bijvoorbeeld pas na het invoeren van het Service Request bepaald op basis van gegevens van de persoon die het Service Request heeft aangemaakt.

Tussen stap 1 en stap 2, het invoeren en het goedkeuren van de gewenste wijziging komt dus eigenlijk nog een extra stap die alleen maar nodig is om het proces “multi-tenant” op te zetten. Die ziet er ongeveer als volgt uit:

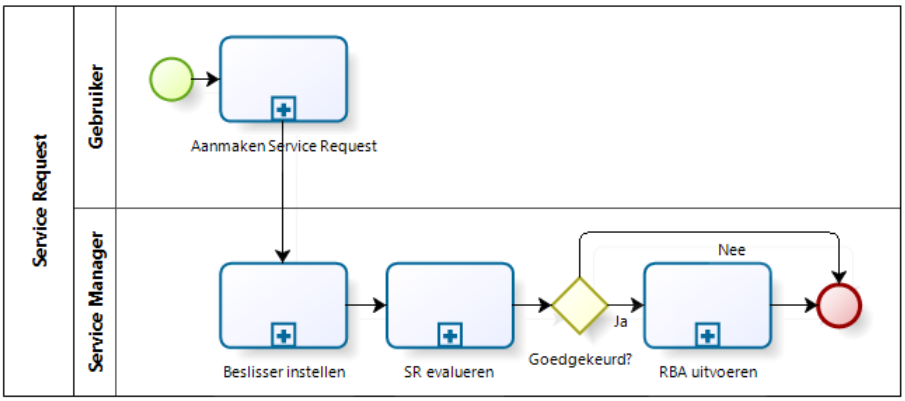


Figuur 15 Persoon instellen voor de goedkeuring van een Service Request

In bovenstaande afbeelding wordt na het aanmaken van het Service Request eerst een zogeheten Runbook Automation Activity (RBA) gestart die een

Runbook in Orchestrator initieert om de eindverantwoordelijke in te stellen voor dit Service Request: de persoon met de zogeheten beslissersrol voor de betreffende organisatie.

Een uitgebreide variant van het algemeen Service Request is te vinden in het Functioneel Ontwerp, maar op hoofdlijnen ziet deze er als gevolg van eerder genoemde toevoeging als volgt uit:



Figuur 16 Algemeen Service Request process

Ik heb de vele stappen die met elkaar te maken hebben samengevoegd tot sub processen om de leesbaarheid te vergroten.

9.2. Runbooks

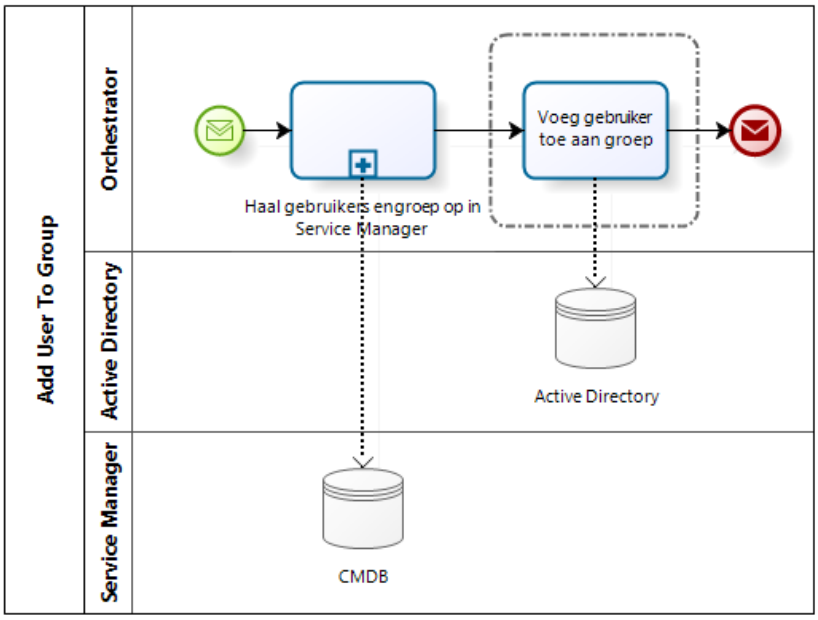
In het hiervoor besproken algemene Service Request wordt meestal aan het eind van het proces de wijziging zelf doorgevoerd door het starten van een runbook. Alle tot nu toe gemodelleerde taken zijn terug te vinden in hoofdstuk 4.2 in het Functioneel Ontwerp. Om te laten zien hoe de inhoud van een runbook eruit kan zien zal ik hieronder twee voorbeelden bespreken.

9.2.1. Voorbeeld 1: Gebruiker toevoegen aan groep

Sommige runbooks zijn ongelofelijk simpel in een model te vatten en blijken technisch een stuk lastiger om te implementeren. Een voorbeeld hiervan is het toevoegen van een gebruiker of meerdere gebruikers aan één of meerdere groepen in Active Directory.

Het toevoegen van een gebruiker kan door gebruik te maken van het eerder besproken algemeen Service Request proces. De gebruiker heeft een Service Request aangemaakt waarbij hij één of meerdere gebruikers heeft geselecteerd die lid moeten worden van een aantal Active Directory groepen. In werkelijkheid selecteert de gebruiker echter niet direct objecten in Active Directory, maar objecten die opgeslagen zijn in de Configuration Management Database (CMDB) van Service Manager.

Het runbook maakt daar dankbaar gebruik van door deze objecten eerst op te halen uit de CMDB en vervolgens in Active Directory aan elkaar te koppelen:



Figuur 17 Runbook "Add User To Group"

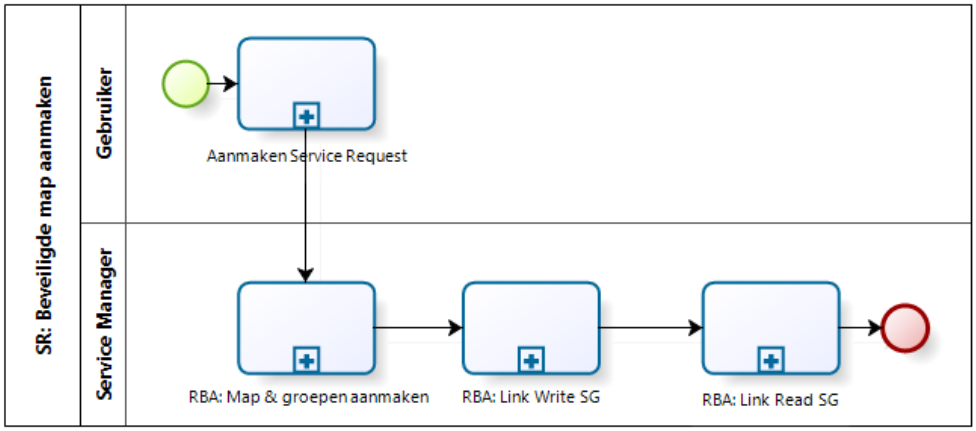
Om deze stappen uiteindelijk technisch voor elkaar te krijgen ziet het runbook er als volg uit:

Figuur 18 Runbook "Add User to Group"

Het runbook start alleen met gegevens van het Service Request. Daarmee worden de Groep- en Gebruikersobjecten opgehaald uit de CMDB van Service Manager. Deze gegevens worden vervolgens gebruikt om de gebruiker(s) toe te voegen aan de geselecteerde groep(en). Mochten er meer dan één gebruiker en/of groep zijn geselecteerd, dan heeft Orchestrator zelf al functionaliteit ingebouwd om een soort loop te creëren, zodat alle objecten aan de beurt komen.

9.2.2. Voorbeeld 2: Aanmaken beveiligde map

Het aanmaken van een beveiligde map bleek een stuk ingewikkelder. Het model van het algemeen Service Request heb ik daarbij moeten laten varen en ziet er als volgt uit:



Figuur 19 Service Request "Aanmaken beveiligde map"

Voor het aanmaken van een beveiligde map is eigenlijk nooit toestemming nodig, dus die stap is verwijderd, maar het proces bevat nu niet één Runbook Activiteit, maar uit drie. Eerst wordt naar aanleiding van de ingevoerde gegevens een map aangemaakt en twee beveiligingsgroepen in Active Directory: een groep met leesrechten en een groep met schijfrechten.

In de volgende twee stappen worden eerst de geselecteerde personen en/of groepen die schijfrechten moeten krijgen gekoppeld in de eerder aangemaakte groep in Active Directory, vervolgens wordt hetzelfde trucje gedaan met de groep met leesrechten.

De uitwerking van alle sub processen zijn weer terug te vinden in het Functioneel Ontwerp, maar duidelijk moet zijn dat een Service Request niet altijd op dezelfde manier in elkaar hoeft te zitten. Het model van het algemene Service Request is echter wel een goede houvast voor het opzetten van nieuwe taken.

10. Proof of Concept

Het installeren van zowel Service Manager en Orchestrator en al het onderzoek naar hoe ik deze pakketten wilde gaan gebruiken in de omgeving van GTS Online heeft geleid tot een werkelijke implementatie van de diverse onderdelen. Deze zijn verwerkt in een Proof of Concept (PoC) omgeving.

10.1. Rollen

Voor het implementeren van rollen heb ik gebruik gemaakt van de functionaliteit in Service Manager. Daarin kunnen gebruikersrollen worden aangemaakt die toegang verlenen tot specifieke objecten en operaties hierop. Aangezien onze klanten alleen via de Self Service Portal Incidenten en Service Requests kunnen aanmaken, zijn alleen de volgende selecties van belang:

- Welke configuration Items, zoals bijvoorbeeld gebruikers-, groeps- en computerobjecten kunnen worden gebruikt via deze rol
    - In onze omgeving zullen altijd die items worden gebruikt met het label van het eigen bedrijf.
- Catalog Item groups: welke Service Requests moeten er voor deze rol ter beschikking worden gesteld.
    - Voor iedere klant zal voor iedere beschikbare Service Request een kopie komen met een variant voor die klant.
    -

Deze rollen worden uiteindelijk gekoppeld aan Active Directory groepen. Op deze manier blijft Active Directory uitgangspunt voor onze omgeving, zoals dat nu ook is voor toegang tot bestanden, mappen en applicaties.

10.2. Proces verbetering

Door gebruik te maken van de Self Service Portal en het snel uitbreiden van de functionaliteit kan de benodigde interactie flink naar beneden. Helaas heb ik te weinig tijd gehad om de opgezette PoC omgeving door de klanten te laten testen. Intern hebben we al wel met succes diverse stukken functionaliteit kunnen testen.

De verwachting is dit snel in werking te zetten op het moment dat we de productieomgeving op gaan zetten. Ondertussen zijn al diverse ideeën toegevoegd aan de lijst met functionaliteit die straks in de productie omgeving ook geïmplementeerd moet gaan worden.

10.3. Functionaliteit

In de Service Manager is op dit moment onder andere de volgende functionaliteit verwerkt.

- Mogelijkheden voor alle gebruikers:
    - Aanmaken van algemeen incident
    - Volgen van eigen incidenten
    - Toegewezen activiteiten uitvoeren, zoals bijv. wijzigingen accepteren of handmatige acties.
- Beheerdersfunctionaliteit:
    - Gebruikersbeheer
        - Aanmaken van een gebruiker
        - Het uitschakelen van een gebruikersaccount

- Het resetten van een wachtwoord
- Het aanmaken van een beveiligingsgroep
- Het aanmaken van een distributiegroep
- Het toevoegen van een gebruiker aan beveiligs- of distributiegroep

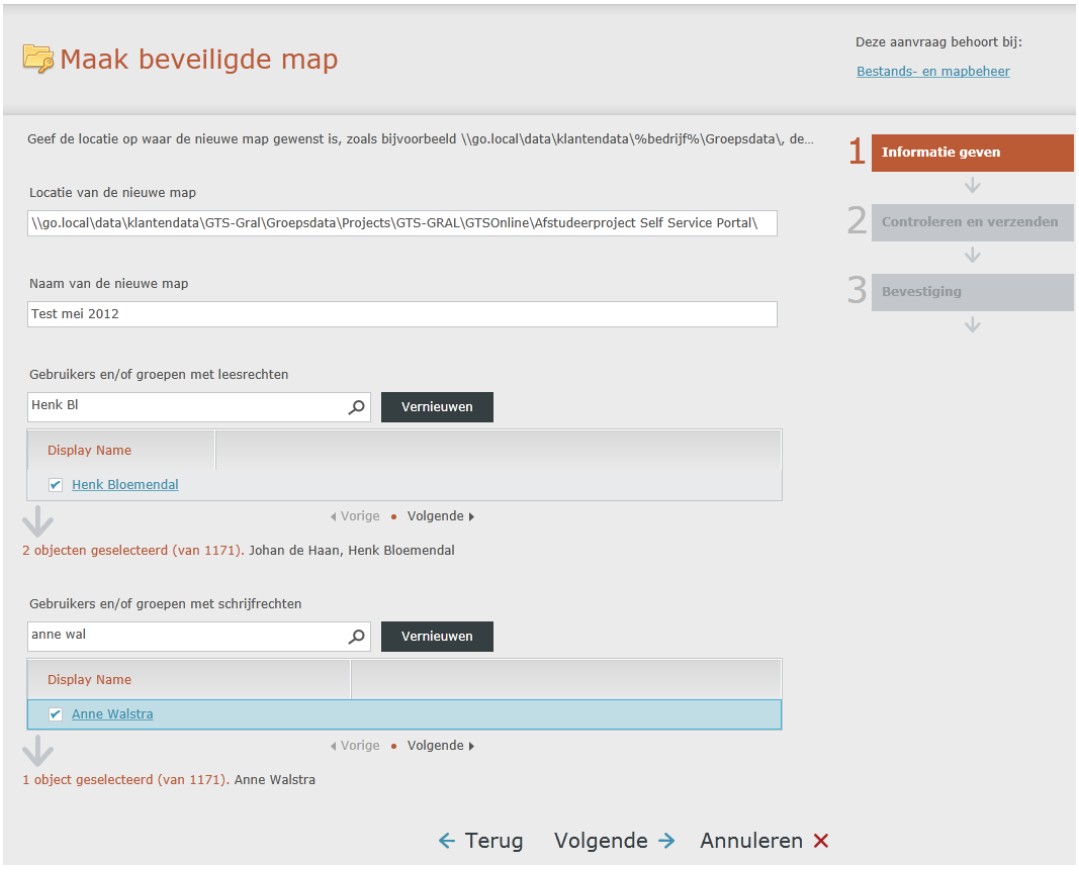
- Werkplekbeheer
  - Het aanmaken van een map
  - Het aanmaken van een beveiligde map
  - Het verwijderen van een computeraccount

Ook is er de mogelijkheid om aankondigingen te doen via een standaard Sharepoint webpart. Helaas bleek het niet mogelijk om in andere vormen van informatievoorziening te voorzien met de twee gekozen software pakketten, zoals al uitgelegd in 8.5 Informatievoorziening.

10.3.1. Voorbeeld: maak beveiligde map

Een goed voorbeeld van een Service Request via de Self Service Portal is het maken van een beveiligde map. Hiervoor heb ik eerst een aantal modellen gemaakt (zie bijlage 2 voor het functioneel ontwerp met o.a. dit model) op basis waarvan het Service Request en de benodigde runbooks zijn gemaakt.

Als de gebruiker de juiste rol toebedeeld heeft gekregen, krijgt hij/zij de mogelijkheid het volgende formulier in te vullen:



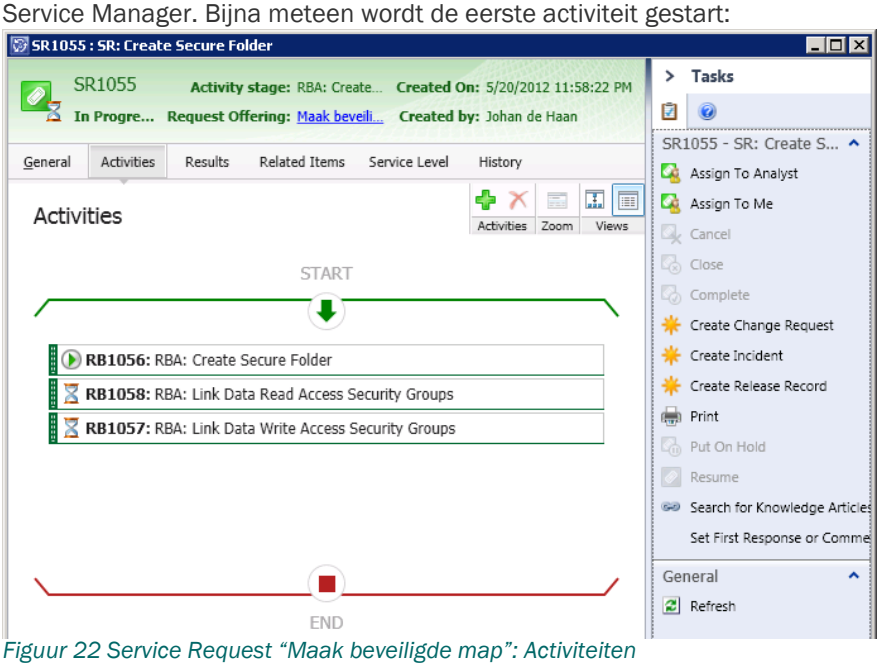
Figuur 20 Service Request "Maak beveiligde map" in de Self Service Portal

Hier kan de locatie van de nieuw te maken map worden opgegeven, de naam van de nieuw te maken map, de personen met leesrechten en de personen met schrijfrechten. Dit kunnen zowel gebruikers als groepen zijn en er kunnen meerdere personen of groepen geselecteerd worden.

Na het invoeren verschijnt een overzichtspagina waarin de ingevoerde wijzigingen worden weergegeven:

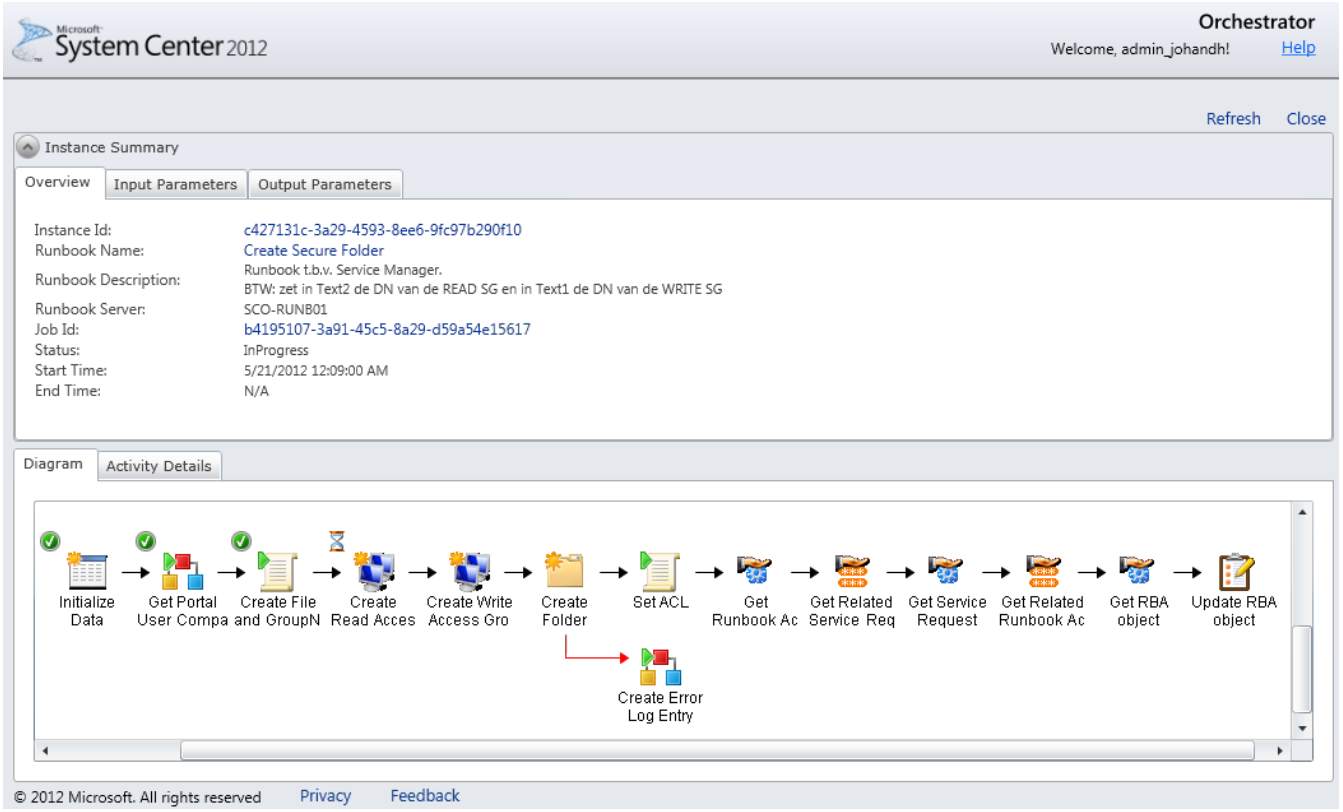
Figuur 21 Service Request "Maak beveiligde map" in de Self Service Portal

Bij het klikken op Verzenden wordt het Service Request aangemaakt in Service Manager. Bijna meteen wordt de eerste activiteit gestart:



Figuur 22 Service Request "Maak beveiligde map": Activiteiten

In werkelijkheid wordt de activiteit in Orchestrator uitgevoerd: het gaat hier namelijk om een Runbook Automation Activity. Over het algemeen wordt



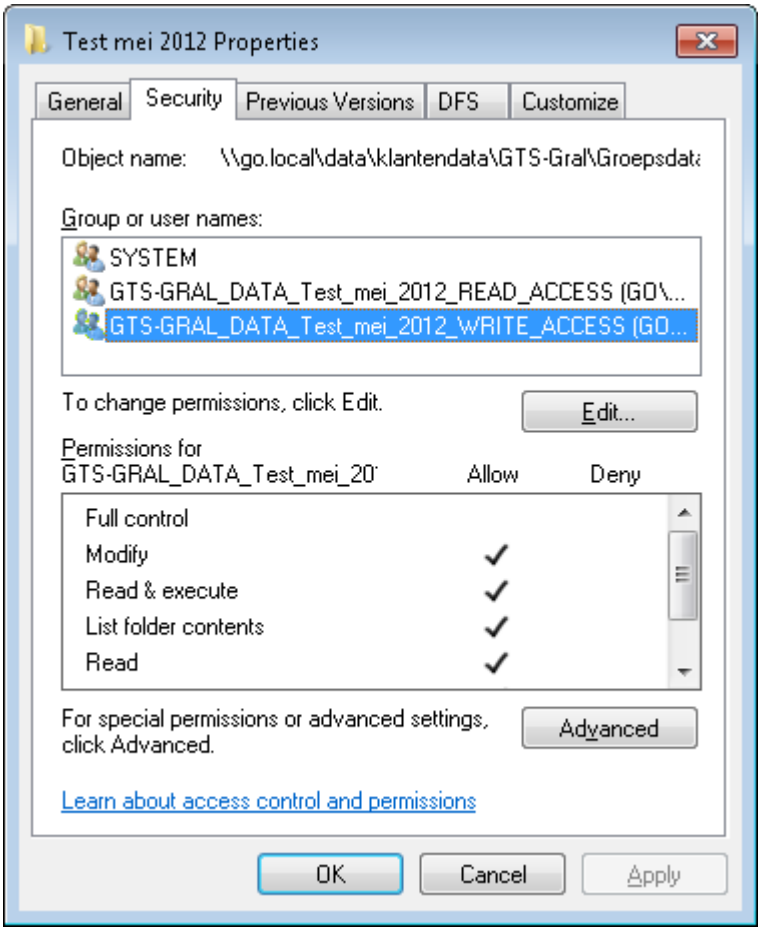
binnen een minuut het Runbook dat gekoppeld is aan de Runbook Automation Activity uitgevoerd:

Figuur 23 Runbook "Create Secure Folder"

Stap voor stap worden de benodigde acties uitgevoerd door het runbook. In bovenstaande voorbeeld zijn de eerste drie activiteiten al succesvol doorlopen en is de vierde zojuist gestart.

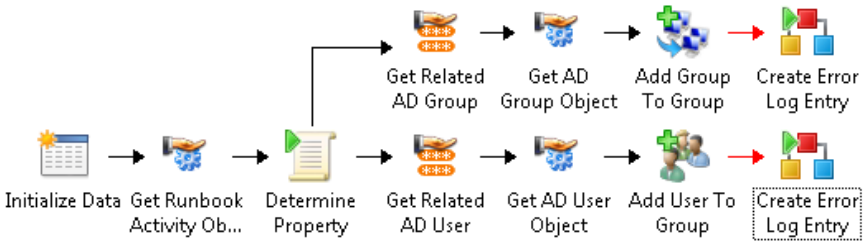
Mocht er ergens tijdens één van de activiteiten in het Runbook een fout ontstaan (er bestaat bijvoorbeeld al een groep met dezelfde naam) dan "mislukt" het runbook en zal de rest van het runbook en ook de rest van het Service Request niet worden uitgevoerd. Het Service Request krijgt dan uiteindelijk ook de status "Mislukt". Het is op dat moment beter om de klant ons te laten bellen dan dat er iets fout gaat op het systeem.

Als dit Runbook voltooid is, is de map aangemaakt, zijn de groepen aangemaakt in Active Directoryen is de beveiliging op de map aangemaakt. Ook worden de overige Runbook Activiteiten in Service Manager op de hoogte gebracht van de aangemaakte Active Directory groepen. Ik doe dit door de objecten in Service Manager te updaten, maar op zich zou ik dat ook kunnen door deze weg te schrijven naar een tekstbestand.



Figuur 24 Aangemaakte map met beveiliging door Runbook "Create Secure Folder"

Nadat deze stappen zijn gedaan wordt twee keer hetzelfde runbook uitgevoerd. De ene wordt echter gestart met de opdracht de "lees" groep te koppelen aan de eerder geselecteerde gebruikers en/of groepen, de ander krijgt de opdracht mee de "schrijf" groep te vullen:



Figuur 25 Runbook "Link Data Security Groups"

10.3.1.1. Conclusie

Op deze manier zijn alle stappen volledige geautomatiseerd uitgevoerd. Vanaf het moment dat de aanvraag is ingediend totdat deze volledig is uitgevoerd kost maximaal een kwartier en dit is dus een flinke verbetering ten opzichte van "ouderwets" handwerk waarbij het zo een dag kon duren voordat de map werkelijk werd aangemaakt.

11. Evaluatie

11.1. Product

Met het geleverde eindproduct ben ik zeer tevreden. Er is wel veel minder functionaliteit opgeleverd dan in verwacht op het moment dat ik het Plan van Aanpak opstelde. Dit komt vooral door tekortkomingen van de gebruikte software op punten waarvan we hadden aangenomen dat deze vanzelfsprekend zouden zijn. Zoals bijvoorbeeld de mogelijkheid om een multi-tenant implementatie te doen binnen Service Manager.

Het implementeren van een multi-tenant omgeving bleek niet mogelijk met een standaard installatie en ook door middel van maatwerk bleek dit niet gemakkelijk. Door het vele extra werk dat ik hier in heb gestopt, heb ik echter wel flink wat kennis opgedaan over de mogelijkheden en functionaliteit van de verschillende onderdelen in Service Manager. Daarmee kunnen we de te maken productieomgeving vele malen sneller opzetten en veel van het reeds gemaakte maatwerk 1 op 1 overzetten naar deze nieuwe omgeving.

Een ander probleem waar ik tegen aan ben gelopen is dat er toch wel wat fouten in de software bleken te zitten, welke te maken bleken te hebben met het feit dat de software nog niet officieel uit was gekomen. Zoals in hoofdstuk 8.2.1 beschreven heb ik gebruik gemaakt van Release Candidates en zeker bij de integratie met andere oplossingen bleken deze niet altijd even stabiel.

11.2. Proces

Ik heb nog niet eerder zo'n groot project in mijn eentje gedaan en ik moet zeggen dat het me ook wel enigszins is tegengevallen. Doordat ik met geheel nieuwe materie bezig was kon ik inhoudelijk lastig bij mijn collega's terecht. Ik heb wel veel gebruik gemaakt van diverse fora op Internet en andere media om vragen rondom het configureren van de producten beantwoord te krijgen. Op diezelfde manier heb ik ook al weer ervaring kunnen delen waaruit wel blijkt dat ik voldoende kennis heb opgedaan.

Een ander punt is dat je jezelf bij de les moet houden. Ik heb bijvoorbeeld bij het onderzoek naar hoe ik multi-tenancy moest gaan implementeren veel tijd gebruikt. Ik leek op een gegeven moment een beetje te verzanden in de niet werkende oplossingen. Op zo'n moment is het belangrijk overzicht te houden op het grote geheel, mijn leidinggevende had dat overigens op dit punt goed in de gaten.

11.3. Leerervaringen

Na de initiële installatie van de producten ben ik eerst druk bezig geweest te leren hoe de pakketten samenwerkten en hoe ik de eerste processen kon vatten in de software. Ik ging meteen uitzoeken hoe ik problemen technisch moest aanpakken. Achteraf merk ik hoeveel prettiger het was om uiteindelijk de processen eerst op een hoger niveau te modelleren, met de mogelijkheden van de producten in mijn achterhoofd, voordat ik me ging bezig houden met de technische implementatie ervan.

Een andere leerervaring is op een heel ander vlak: toen ik namelijk startte bij GTS-GRAL in november had ik totaal geen kennis over hoe de omgeving in

elkaar stak. Doordat ik zo intensief bezig ben geweest met het waarom en hoe van de gewenste functionaliteit heb ik nu veel beter inzicht van de omgeving en ook veel sneller dan wanneer ik het in de dagelijkse praktijk had moeten ontdekken.

11.4. Verbeterpunten

De punten die ik de volgende keer anders zou doen zijn de volgende:

- Minstens wachten op de RTM versie van software alvorens zo'n groot project aan te gaan.
    - Een Release Candidate is handig om de software onder de knie te krijgen, maar het is erg vervelend om er na een aantal uur debuggen achter te komen dat een fout in de software de boel zit te dwarsbomen en je de software wel goed geconfigureerd had.
    - Documentatie van de software is summier of niet aanwezig en dat heeft tot gevolg dat veel onderzoek uit "trial-and-error" bestaat. En het is prima als dat voor een klein onderdeel van het project nodig is, maar uiteindelijk ben ik zelf een groot gedeelte van de tijd op die manier bezig geweest.
- Uitgebreider pakketselectie onderzoek doen
    - Wat betreft licentievoordelen en het al in gebruik hebben van veel van de andere pakketten in dezelfde System Center reeks was het logisch om deze software te gebruiken voor deze toepassing. Uiteindelijk zijn we er wellicht wel iets te veel blind op gevaren.
    - De voor dit gekozen software is goed te gebruiken voor een groot deel van de gewenste toepassing, maar op sommige punten komt het toch echt tekort. Van te voren hadden we dat niet verwacht.
    - Misschien komt dit ook wel voort uit het feit dat we gebruik maakten van Release Candidates en documentatie niet tot nauwelijks beschikbaar was.
- Meer aan projectmanagement doen
    - Doordat je alleen werkt ben je minder bezig met het halen van mijlpalen en geplande opleverdata. Ik denk dat het juist dan nog belangrijker is data in te plannen waarop zaken af moeten zijn en ook druk hiervoor op te bouwen.

Bijlagen

Bijlage 1: Plan van Aanpak

Documentbeheer

Datum	Auteur	Omschrijving	Versie
16-12-2011	Johan de Haan	Initieel document	0.1
03-01-2011	Johan de Haan	Herschrijven Organisatie & Opdracht	0.2
04-12-2011	Johan de Haan	Projectactiviteiten & Projectorganisatie	0.3
06-01-2011	Johan de Haan	Toevoeging eisen met prioriteiten (MoSCoW)	0.9
13-01-2012	Johan de Haan	Verfijning van diversen n.a.v. intern overleg	1.0
19-01-2012	Johan de Haan	Toevoeging Gantt diagram (planning) + verfijning afbakening & producten	1.1

Inleiding

Dit document bevat het Plan van Aanpak voor de afstudeeropdracht van Johan de Haan, student aan de opleiding Informatica op de Hogeschool Utrecht. Deze opdracht zal uitgevoerd worden bij GTS-GRAL te Veenendaal en zal gaan over het opzetten van een Self Service Desk voor één van de diensten van deze organisatie.

Organisatie

GTS-GRAL heeft zijn oorsprong in Duitsland waar deze sinds 1988 als Server Based Computing specialist een vooraanstaande positie weten te verwerven in deze markt. In Nederland wordt in 1998 een dochteronderneming gestart: GTS-GRAL Nederland B.V.

GTS-GRAL Nederland is sinds 1998 volledig zelfstandig en heeft zijn kantoor in Veenendaal. Naast het leveren van diensten "on premise", intern bij de klant, levert GTS-GRAL steeds meer diensten direct vanuit de eigen omgeving. Dit gebeurt voornamelijk middels GTS-Online, een online werkplek omgeving welke gehost wordt vanuit een data center.

GTS-GRAL biedt met GTS-Online een (online) werkplek aan, waarmee altijd en overal gewerkt kan worden tegen dezelfde vaste kosten per maand voor bedrijven in het MKB. In dit bedrag zit alles inbegrepen: licenties voor diverse kantoor applicaties, toegang tot de e-mail via bijna elk denkbaar apparaat en helpdesk via website, e-mail of telefoon. Alleen bij het gebruik van eigen bedrijfssoftware of het huren van een werkplek wordt het bedrag hoger.

Opdracht

Situatie

De dienst GTS-Online is als basis heel erg robuust en schaalbaar opgezet. Of een klant nu 10 of 100 werkplekken afneemt, de capaciteit van de dienst kan gemakkelijk uitgebreid worden zonder ingrijpende veranderingen in het systeem. Aanpassingen op het systeem worden grotendeels met scripts gedaan, zodat deze iedere keer op dezelfde manier uitgevoerd worden.

Helpdesk

De migratie van een klant naar GTS-Online gebeurt in projectvorm en tijdens dit project worden er ook allerlei zaken ad-hoc geregeld. Een gebruiker erbij, een applicatie erbij, een printer minder, etc. En ook de maanden na een migratie komen dit soort, meer helpdesk-achtige vragen en wensen steeds meer voor, welke in een ticket systeem worden vastgelegd en van daaruit worden behandeld door verschillende medewerkers (medewerkers van de support afdeling en system engineers) van GTS-GRAL.

Dit soort aanpassingen kunnen vaak gedaan worden door aanpassingen op een of meerdere objecten in Active Directory, de centrale database van een Windows domein. In Active Directory zijn niet alleen alle gebruikersaccounts van een Windows domein te vinden, maar ook onder andere beveiligingsgroepen, computerobjecten en groepsbeleidobjecten. Door een gebruikersaccount lid te maken van een bepaalde beveiligingsgroep, kan bijvoorbeeld een snelkoppeling worden aangeboden of een printer worden geïnstalleerd.

De bedoeling is dat het komende jaar nog meer nieuwe klanten gebruiken zullen maken van onze GTS-Online dienst. Het aantal helpdeskvragen zal hierbij alleen maar toenemen. Om deze klanten allemaal goed van dienst te kunnen en blijven zijn, dienen zoveel mogelijk zaken die zij zelf zouden kunnen beheren geautomatiseerd te worden. Dit moet echter mogelijk gemaakt worden zonder dat dat gebruikers complete toegang krijgen tot de systemen, aangezien het om een multi-tentant omgeving gaat: één omgeving voor meerdere klanten.

Borging van informatie

Verder zijn er al wel een aantal systeembeheertaken geautomatiseerd, zoals het aanmaken van gebruikers en het uitrollen van nieuwe werkplekken. Maar deze scripts wijzigen regelmatig doordat regelmatig extra functionaliteit gewenst is of doordat instellingen bij de ene klant toch net weer wat anders moeten zijn dan bij de andere. Wat de verschillen precies zijn tussen deze scripts en de functionaliteit van veel stukken code in deze scripts is geen documentatie.

Informatievoorziening

Daarnaast groeit de vraag naar inzichtelijkheid over wat er door de klant in gebruik is: de klant betaalt namelijk per gebruiker, per maand, een bedrag, maar in sommige gevallen ook voor het aantal computers dat hij huurt of het aantal applicaties die hij afneemt. Deze inzichtelijkheid is niet alleen

belangrijk voor ons om te weten wat wij aan de klant moeten factureren, maar ook voor de klant om altijd te kunnen zien waar hij gebruik van maakt.

Afstudeeropdracht

De combinatie van het automatiseren van een aantal veelvoorkomende taken, het voor een deel beschikbaar maken van deze taken aan eindklanten en het inzichtelijk maken van de diensten en producten waar de klant gebruik van maakt, vormt de kern van mijn afstudeeropdracht.

Om de verschillende taken aan verschillende rollen te kunnen koppelen zal er eerst een uitwerking gemaakt moeten worden van de verschillende rollen die er bij GTS-GRAL en de organisatie van de klant (kunnen) zijn. Deze rollen zullen verderop in het project veelvuldig gebruikt worden om een workflow mee te kunnen maken.

De informatie over de (opnieuw) te automatiseren taken zal geborgd worden door de workflow ervan te documenteren en de functionele (welke informatie is er nodig) en niet-functionele eisen (waarom worden taken op een bepaalde manier opgelost en niet op een andere) er van vast te leggen. Deze documentatie zal eerst door de engineers van GTS-GRAL gecontroleerd worden op juistheid alvorens deze te implementeren.

Aangezien met deze software ook de mogelijkheid bestaat om andere helpdeskvragen en change requests te registeren en deze af te handelen, zal dit ook meteen worden meegenomen in de scope van het project.

Afbakening

De twee zaken waar het project in ieder geval om draait is het automatiseren van diverse taken en het verbeteren van de informatievoorziening. De zaken die daar volgens GTS-GRAL bij horen zijn hieronder weergegeven onder het kopje Functionaliteit.

Software

De software die ik zal gebruiken zijn de softwarepakketten Microsoft System Center Service Manager 2012 (SCSM) en Microsoft System Center Orchestrator 2012 (SCO). De licenties voor deze pakketten zijn al beschikbaar voor ons en daarnaast hebben deze twee pakketten een diepe integratie met de andere System Center producten die wij al gebruiken.

Functionaliteit

De hieronder opgestelde eisen of functionaliteiten kunnen echter worden herzien op het moment dat er tijdens het project tot een ander inzicht gekomen wordt. Dit zou bijvoorbeeld kunnen komen door een technische onmogelijkheid of juist een groeiende wens voor bepaalde functionaliteit die niet is opgenomen in onderstaande lijst. Er is afgesproken met de opdrachtgever dat dit geen probleem moet zijn en dit in goed overleg mogelijk is.

Voor de prioritering van het project wil ik gebruik maken van de *M*o*S*C*o**W*-methode. Hierbij staan de hoofdletters voor:

- *M*ust have: deze zaken dienen in ieder geval in het eindresultaat terugkomen;
- *S*hould have: deze zaken zijn zeer gewenst, maar zonder dit is het eindresultaat alsnog bruikbaar;
- *C*ould have: deze zaken zullen alleen geïmplementeerd worden als er voldoende tijd beschikbaar is;
- *W*ont have: dit zal zeer waarschijnlijk niet binnen de tijd van het project meegenomen worden, maar zou in de toekomst interessant kunnen zijn om te implementeren.

De lijst die hierop volgt is verder nog onderverdeeld in:

- Gebruikerstaken: dit zijn taken die iedere gebruiker in de organisatie tot zijn beschikking heeft, voornamelijk om het aantal telefoontjes te verminderen en de gebruiker meer inzicht te geven in de status van openstaande helpdesk vragen.
- Beheertaken: taken die alleen beschikbaar zijn voor bepaalde personen in de organisatie van de klant die vaak voordat zij gebruik gingen maken van de diensten van GTS-GRAL al systeembeheertaken hadden. Indien een specifieke beheertaak niet voor de klant beschikbaar is, is dit in onderstaande lijst aangegeven achter deze taak.
- Informatievoorziening: rapporten over de zaken die een klant in gebruik heeft. Deze zijn in de eerste plaats om inzicht te geven aan de klant, maar zal ook beschikbaar zijn voor GTS-GRAL om op basis hiervan de facturatie te kunnen doen.

Must

Hier valt ten minste onder:

- Configuratie van System Center Service Manager & Orchestrator
  - Basis installatie
  - Integratie tussen de twee software pakketten
  - Verschillende rollen definiëren binnen zowel de organisatie van de klant als die van GTS-GRAL
  - Role-based access configureren op basis van de eerder onderscheiden functies of rollen uit de organisaties van de klant en GTS-GRAL zelf
- Beheertaken:
  - Gebruikersbeheer
    - Aanmaken van een gebruiker
    - Verwijderen van een gebruiker
    - Wachtwoord resetten van een gebruiker
    - Toevoegen van een gebruiker aan een groep (bijvoorbeeld een e-mailgroep of beveiligingsgroep)
    - Verwijderen van een gebruiker uit een groep
  - Werkplekbeheer
    - Computeraccounts verwijderen
- Informatievoorziening:
  - Het kunnen weergeven van de aangemaakte gebruikers
  - Het kunnen weergeven van het aantal gebruikers in bepaalde groepen (i.v.m. betaalde licenties)
  - Het kunnen weergeven van aantal computers (i.v.m. mogelijk gehuurde werkplekken)

Should

Andere zaken die wenselijk zijn

- Gebruikerstaken:
  - Self-service portal voor alle gebruikers, geïntegreerd met Active Directory (AD) (huidige ticketomgeving is een extern gehoste website, zonder koppelingen met centrale databases als AD)
    - Incidenten/requests indienen;
    - Eigen incidenten/requests bekijken, verwijderen;
- Beheertaken:
  - Bestandsbeheer
    - Aanmaken van mappen
    - Wijzigen van rechten op mappen
    - Verwijderen van (met rechten beveiligde) mappen
  - Gebruikersbeheer
    - Algemene gegevens wijzigen (zoals bijv. naam, functiebeschrijving, telefoonnummer, etc)
    - E-mailadres(sen) toevoegen
    - Beveiligingsgroepen aanmaken
    - Distributiegroepen (voor in de e-mailomgeving) aanmaken
    - Distributiegroepen verwijderen
  - Nieuwe klant (bedrijf) toevoegen (alleen GTS-GRAL)
  - Gedeelde (resource) mailboxen beheren
    - E-mailadres(sen) toevoegen
    - Resource mailboxen verwijderen
  - Werkplekbeheer

        - Offline domain join (aanmelden van nieuwe computers in het domein)
- Informatievoorziening:
    - Informatie over geplande werkzaamheden in self-service portal

Could

Indien er voldoende tijd beschikbaar blijkt te zijn:

- Beheertaken:
    - Aanmaken resource mailboxen (gedeelte mailboxen) in Microsoft Exchange.
    - Wijzigen rechten resource mailboxen in Microsoft Exchange.
    - ActiveSync mobile device management
        - Op afstand wissen van bedrijfstelefoon
- Informatievoorziening
    - Rapportage over percentage beschikbaarheid van de diensten (bv. e-mail, werkplek, sharepoint) (i.v.m. SLA's)
    - CMDB (Configuration Management Database) met uitgebreidere informatie over verschillende assets (computers, telefoons, etc) en door wie deze in gebruik is en op welke locatie deze zijn.

Won't

Zaken die interessant zouden kunnen zijn, maar pas in een mogelijk volgend project geïmplementeerd zullen worden:

- Beheertaken:
    - Het integreren van System Center Service Manager (SCSM) met Virtual Machine Manager (VMM);
        - Aanmaken van Virtual Machines (alleen GTS-GRAL)
        - Wijzigen van Virtual Machines; (alleen GTS-GRAL)
        - Verwijderen van Virtual Machines; (alleen GTS-GRAL)
    - Het integreren van System Center Service Manager (SCSM) met Data Protection Manager (DPM, back-up oplossing)
        - Beheren restore jobs (alleen GTS-GRAL)
        - Beheren back-up jobs (alleen GTS-GRAL)

Producten

Aan het eind van het project zullen de volgende producten worden opgeleverd:

- Plan van Aanpak
- Functioneel ontwerp
- Proof of Concept
    - Documentatie
- Scriptie

Een aantal van de hierboven genoemde producten worden in de volgende alinea's nog wat verduidelijkt.

Proof of Concept

Het proof of concept is het belangrijkste product van dit project voor GTS-GRAL en bestaat uit zowel aan de gebruikerskant als aan de beheerderskant een interface of portal waarin de gedefinieerde taken beschikbaar zijn of rapporten in getoond worden. Om deze portals en bijbehorende taken te maken wordt gebruik gemaakt van Microsoft System Center Service Manager en Microsoft System Center Orchestrator.

Aan de gebruikerskant zal dit in de vorm zijn van een Self-Service Portal waarin de gebruiker zelf kan inzien wat de status van zijn/haar incidenten of aanvragen is, zelf oplossingen kan zoeken naar al bekende problemen en er pro-actief informatie getoond wordt over geplande werkzaamheden.

Aan de beheerderskant moeten zoveel mogelijk systeembeheertaken geautomatiseerd worden aan de hand van workflows en scripts, zodat iedere aanpassing op het systeem op dezelfde manier wordt uitgevoerd. Daarnaast moeten bepaalde beheerderstaken beschikbaar komen voor bepaalde personen in de organisatie van de klant, zodat niet alle aanpassingen door GTS-GRAL zelf uitgevoerd hoeft te worden. Dit zal worden gedaan op basis van role-based access: het ligt er aan welke rol het gebruikte account heeft of bepaalde taken wel of niet beschikbaar zijn voor een gebruiker.

Functioneel ontwerp

Daarnaast zullen alle te maken taken, indien nodig gemodelleerd, maar in ieder geval gedocumenteerd worden wat de functionele eisen (bijv. welke gegevens zijn er nodig om een taak uit te voeren) en niet-functionele eisen (bijv. waarom iets op een bepaalde manier moet worden opgelost en niet op een andere) zijn.

Voordat een taak gemaakt wordt met de software, moet deze volledig op papier uitgewerkt zijn, zodat de engineers van GTS-GRAL deze kunnen herzien indien nodig. Ook zal er bij veel taken een bepaalde workflow nodig zijn, zoals bijvoorbeeld een akkoord van een manager voor bepaalde zaken, en het is belangrijk dat dit soort zaken duidelijk worden voor alle betrokkenen.

Projectactiviteiten

Fasering

Het project is in grote lijnen op te delen in de volgende fasen, welke ik heb overgenomen uit DSDM:

Feasibility Study

In deze fase wordt er onderzoek gedaan naar de mogelijkheden van de te gebruiken tools en zal het afstudeervoorstel worden ingediend.

Business Study

In de fase zal onderzoek gedaan naar de mogelijkheden van de tools en de mogelijke implementatie hier van. Ten behoeve van het plan van aanpak wordt er een overzicht van de eisen opgesteld en de (deel)producten bepaald. Het plan van aanpak wordt ingediend.

Functional model iteration

Voor iedere taak zal er vastgelegd worden wat de functionele en niet-functionele eisen zijn en wat voor workflow er nodig is om de taak uit te voeren. Door middel van prototyping worden deze specificaties getoetst, nadat de specificaties zijn gecontroleerd door de engineers van GTS-GRAL Dit zal zowel voor de beheertaken, informatievoorziening als de gebruikerstaken gedaan worden.

Design and build iteration

In deze fase zullen de prototypes van de verschillende deelproducten verder uitgewerkt en al deels opgeleverd en steeds meer geïntegreerd worden tot een samenhangend geheel.

Implementation

In deze fase zullen de verschillende opgeleverde producten getest worden door geselecteerde gebruikers in de eigen organisatie en bij diverse klanten. Op dit moment kan er nog voor worden gekozen om (bepaalde onderdelen) opnieuw of anders op te zetten.

Planning

Het project zal uitgevoerd worden gedurende een periode van ongeveer 26 weken, waarbij er per week ongeveer 20 uur aan het project gewerkt kan worden op kantoor. Daarnaast zal ik nog 8 uur per week in mijn eigen tijd besteden aan het project, waarin ik voornamelijk verslagen en documentatie zal uitwerken.

Ik verwacht de hierop volgende planning aan te kunnen houden. Tussen haakjes staat in welke fase deze werkzaamheden vallen.

Periode	*Werkzaamheden*
November t/m half januari	• Afstudeervoorstel indienen (wk 47) • Onderzoek naar mogelijkheden van de te gebruiken software (wk 45, 46) • Plan van Aanpak opstellen (wk 48 - 4) • Plan van Aanpak indienen (wk 4)
Januari t/m half april	• Basis implementatie van de te gebruiken software (wk 4 - 7) • Uitwerken van de benodigde processen en uitzoeken hoe deze zo effectief mogelijk geïmplementeerd kunnen te worden in de te gebruiken software. (wk 8 - 15) • Implementeren van deze processen (wk 8 - 15) • Inrichten van de portals (wk 7)
April	• Portals beschikbaar maken voor testen (wk 14) • Mogelijke problemen oplossen t.b.v. werkend eindproduct (wk 14 - 18)
Mei	• Uitloop (wk 19 - 21) • Afronding scriptie (wk 19 - 21) • Inleveren scriptie op 29-05-2012 (wk 22)

Deze planning is ook in Bijlage 1 te vinden, in de vorm van een Gantt diagram.

Kwaliteitsbewaking

Het grootste risico aan het project is dat het opgeleverde eindproduct niet naar wens is van GTS-GRAL doordat deze niet goed bruikbaar en de kwaliteit onvoldoende is. Om dit te voorkomen zal er gedurende het gehele project regelmatig overleg worden gevoerd over de voortgang van het project.

De voortgang van het project zal dan ook niet alleen tijdens het tweewekelijks werkoverleg plaats vinden met de rest van mijn collega's, maar ook op een aantal nader te bepalen momenten met alleen mijn leidinggevende (tevens bedrijfsbegeleider). Ik wil dit overleg maandelijks inplannen om te voorkomen dat de verwachtingen van beide partijen teveel uiteen gaan lopen tijdens het project.

Ook zal het van te voren documenteren en modelleren van de taken die het systeem aan het project moet kunnen uitvoeren zorgen voor een stuk kwaliteitsbewaking. Deze modellen en bijbehorende documentatie kan voordat deze worden geïmplementeerd worden bekeken door mijn collega's en kunnen

Projectorganisatie

Dit project zal ik volledig zelfstandig uitvoeren. Uiteraard zal er echter wel overleg zijn met mijn directe collega's en leidinggevende om beslissingen te nemen over hoe bepaalde technische zaken geïmplementeerd dienen te gaan worden. De op te leveren producten dienen namelijk wel zo opgeleverd te worden dat deze in de toekomst, met het oog op nieuwe klanten met mogelijk andere wensen en eisen, ook gebruikt kunnen gaan worden.

Bedrijfsgegevens

GTS-GRAL Nederland BV

Adres:	Turbinestraat 3b
	3903 LV Veenendaal
Telefoonnummer:	0318-550884
Bedrijfsbegeleider:	Henk Bloemendal
E-mailadres begeleider:	h.bloemendal@gtsgral.nl

Persoonsgegevens

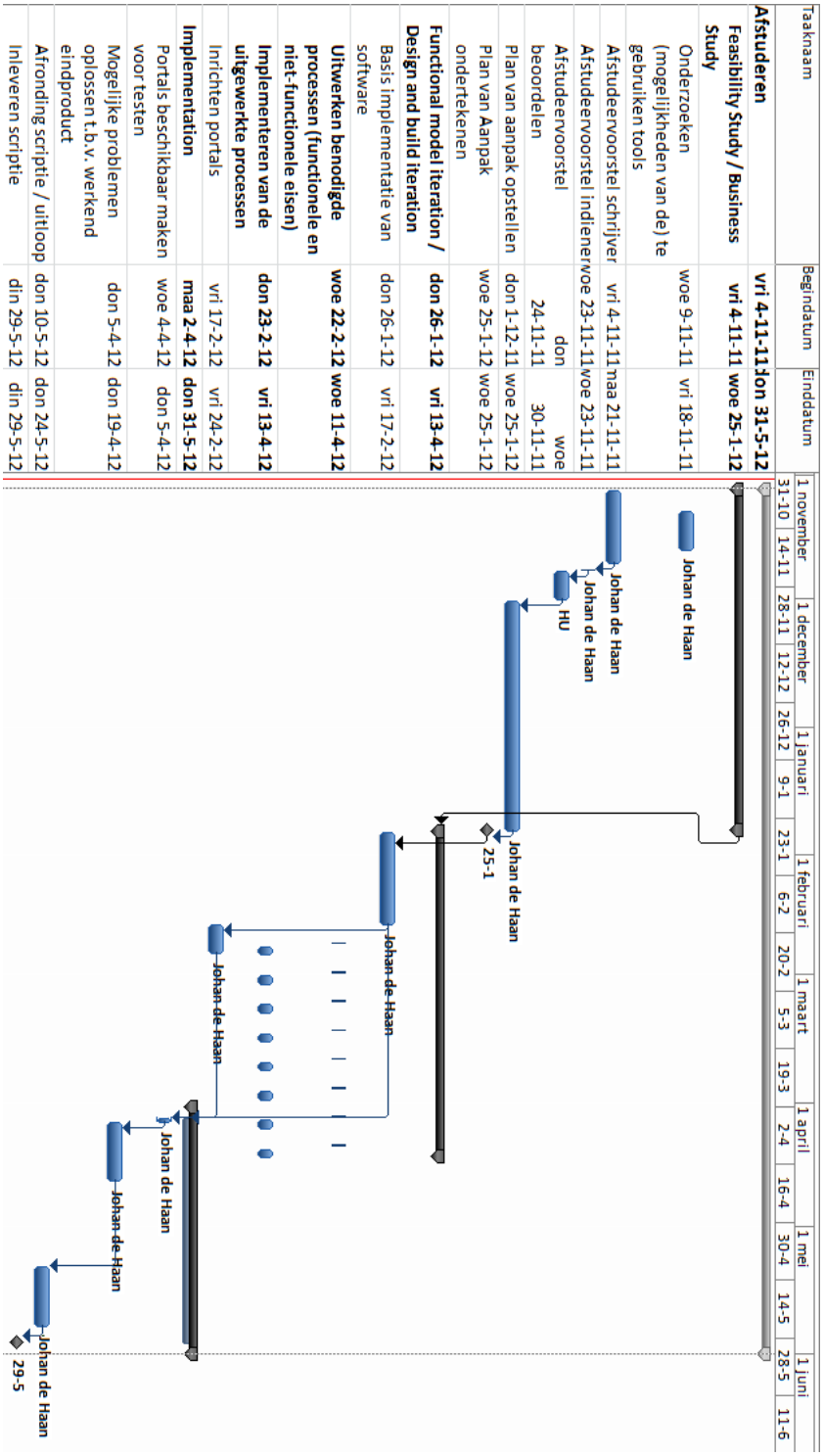
Mijn eigen gegevens zijn als volgt:

Naam:	Johan de Haan
Telefoonnummer:	0318-550884
Mobiel nummer	0628532362
Emailadres	j.dehaan@gtsgral.nl

Bijlagen Plan van Aanpak

Bijlage 1 (PvA): Planning

Taaknaam	Begindatum	Einddatum
Afstuderen	**vri 4-11-11**	**don 31-5-12**
Feasibility Study / Business Study	**vri 4-11-11**	**woe 25-1-12**
Onderzoeken (mogelijkheden van de) te gebruiken tools	woe 9-11-11	vri 18-11-11
Afstudeervoorstel schrijver	vri 4-11-11	naa 21-11-11
Afstudeervoorstel indienen	woe 23-11-11	woe 23-11-11
Afstudeervoorstel beoordelen	don 24-11-11	woe 30-11-11
Plan van aanpak opstellen	don 1-12-11	woe 25-1-12
Plan van Aanpak ondertekenen	woe 25-1-12	woe 25-1-12
Functional model iteration / Design and build iteration	**don 26-1-12**	**vri 13-4-12**
Basis implementatie van software	don 26-1-12	vri 17-2-12
Uitwerken benodigde processen (functionele en niet-functionele eisen)	**woe 22-2-12**	**woe 11-4-12**
Implementeren van de uitgewerkte processen	**don 23-2-12**	**vri 13-4-12**
Inrichten portals	vri 17-2-12	vri 24-2-12
Implementation	**maa 2-4-12**	**don 31-5-12**
Portals beschikbaar maken voor testen	woe 4-4-12	don 5-4-12
Mogelijke problemen oplossen t.b.v. werkend eindproduct	don 5-4-12	don 19-4-12
Afronding scriptie / uitloop	don 10-5-12	don 24-5-12
Inleveren scriptie	din 29-5-12	din 29-5-12



Bijlage 2 (PvA): Contract afstudeeropdracht

Datum:	25-01-2012
Naam student	Johan de Haan
Opleiding	Informatica
Variant:	Deeltijd
Adres student:	Schiestraat 56 3812KK Amersfoort
Studentnummer:	1523226
Telefoonnummer prive	0628532362
E-mailadres	Johan.dehaan@student.hu.nl
Naam bedrijf:	GTS-GRAL
Adres bedrijf:	Turbinestraat 3b 3903 LV Veenendaal
Naam bedrijfsbegeleider	Henk Bloemendal
Telefoonnummer bedrijfsbegeleider	0318-550884
E-mailadres bedrijfsbegeleider	h.bloemendal@gtsgral.nl
Afstuderen in:	Mei 2012

Ondergetekenden verklaren hiermee akkoord te gaan met de inhoud van bijgevoegd PvA.

Handtekeningen

Student:

Docentbegeleider:

Bedrijfsbegeleider*

*Door ondertekening van dit formulier verklaart de bedrijfsbegeleider minimaal een hbo- of vergelijkbare opleiding te hebben.

Bijlage 2: Functioneel ontwerp

Documentbeheer

Datum	Auteur	Omschrijving	Versie
27-12-2011	Johan de Haan	Initieel document	0.1.0
02-02-2012	Johan de Haan	Beschrijving huidige situatie (Rollen)	0.2.0
03-02-2011	Johan de Haan	Toevoeging RBAC (Rollen)	0.2.1
22-03-2012	Johan de Haan	Aanpassingen n.a.v. overleg P. van Rooijen d.d. 13-03-2012	0.3.0
16-04-2012	Johan de Haan	Betere scheiding Rollen & Processen in RBAC	0.4.0
26-04-2012	Johan de Haan	Hoofdstuk modellen gestart	0.5.0
27-04-2012	Johan de Haan	Algemeen Service Request proces	0.5.1
03-05-2012	Johan de Haan	Algemeen Service Request bijgewerkt met Runbooks	0.5.2
11-05-2012	Johan de Haan	Beheertaken (aanmaken, verwijderen gebruiker)	0.5.3
17-05-2012	Johan de Haan	Overige beheertaken gemodelleerd en beschreven	0.5.4
18-05-2012	Johan de Haan	Opgenomen in scriptie document	0.6.0

1. Inleiding

De opdracht voor dit afstudeerproject kan kort als volgt worden samengevat als “de combinatie van het automatiseren van een aantal veelvoorkomende taken, het voor een deel beschikbaar maken van deze taken aan eindklanten en het inzichtelijk maken van de diensten en producten waar de klant gebruik van maakt”. Aangezien een aantal taken duidelijk slechts voor bepaalde personen beschikbaar moeten komen, is het nodig hierin onderscheid te maken.

In dit functioneel ontwerp zal ik daarom voornamelijk aandacht schenken aan de volgende twee zaken:

- *Rollen*: we zullen een aantal rollen definiëren die grotendeels op basis waarvan vervolgens rechten kunnen worden verleend voor het uitvoeren van taken of het autoriseren van wijzigingen op het systeem. Ook het kunnen weergeven van diverse vormen van bepaalde informatie kunnen aan deze rollen toegewezen worden.
- *Processen*: op wat voor manier zal het introduceren van een Self Service Portal de huidige processen wijzigen en welke verbeteringen zijn daardoor mogelijk.
- *Taken*: wat is de volgorde van de activiteiten die uitgevoerd zullen worden die bij een taak horen. Bijvoorbeeld het autoriseren van een wijziging, het valideren van ingevoerde gegevens en het werkelijk uitvoeren van een activiteiten die tot deze wijziging leiden.

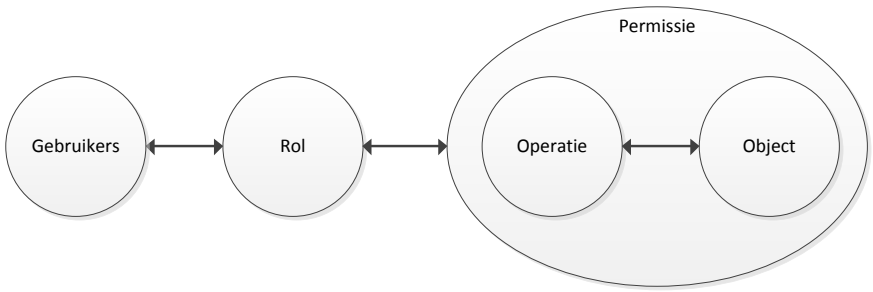
Op basis van de verschillende rollen en gemodelleerde taken kan de software vervolgens eenduidig worden ingericht, waardoor ook inzichtelijk wordt wie welke rechten heeft op de GTS-Online omgeving.

2. Rollen

De verschillende taken die beschikbaar dienen te gaan komen via de Self-Service portal, maar ook diverse vormen van informatievoorziening zullen niet voor iedereen beschikbaar moeten zijn. De toegang tot deze taken of informatie zal worden verleend op basis van de rol die een medewerker van de klant of GTS-GRAL is toebedeeld.

2.1. Role Based Access Control (RBAC)

Het op een overzichtelijk en efficiënte wijze verlenen en innemen van rechten wordt binnen IT systemen steeds vaker gedaan op basis van Role Based Access Control, afgekort met RBAC. RBAC is een algemeen gebruikte term voor het toekennen van permissies door gebruik te maken van rollen, maar is bijvoorbeeld ook gevat in een ANSI INCITS standaard 359-2004[8].



Figuur 26 RBAC

Zoals in bovenstaande afbeelding te zien is worden bij RBAC bepaalde permissies gekoppeld aan een rol en deze rol kan weer aan een gebruiker gekoppeld worden. Een permissie bestaat altijd uit het toestaan van een bepaalde operatie op een object, zoals bijvoorbeeld het lezen (operatie) van een bepaald document (object).

2.1.1. Dynamisch en onderhoudsvrij

Mocht een gebruiker er een collega bijkrijgen die dezelfde werkzaamheden dient te gaan doen, is het gemakkelijk om deze rechten over te zetten. De collega hoeft slechts dezelfde rollen toegekend te krijgen om dezelfde permissies op het systeem te hebben. En het ontnemen van bepaalde rechten kan net zo gemakkelijk: het ontkoppelen van de rol van het gebruikersaccount is voldoende om geen rechten meer te hebben.

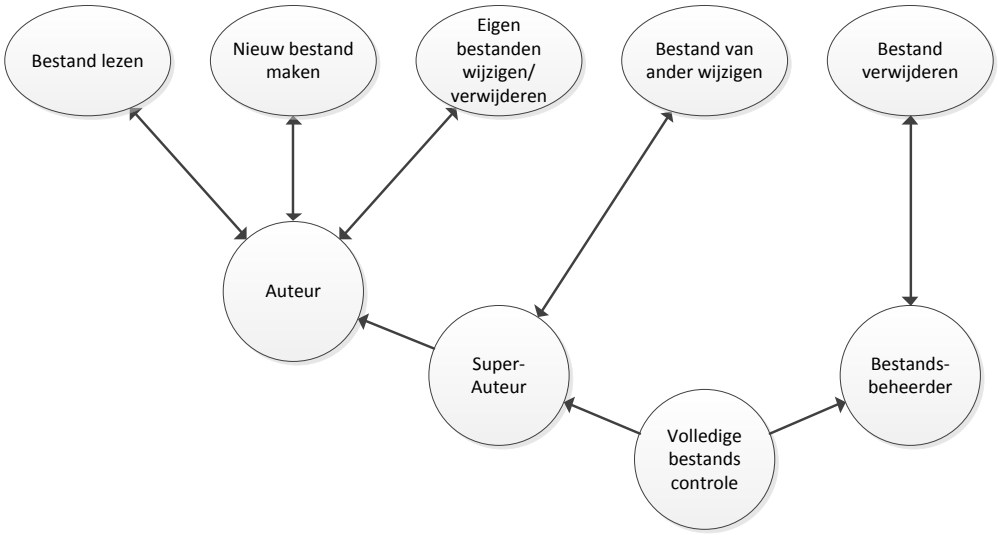
Een ander voordeel van RBAC is dat na het eenmaal toewijzen van rollen aan een bepaalde permissie er vervolgens nauwelijks of geen wijzigingen meer gedaan hoeven te worden in de rechten op een object. De permissies die zijn verleend op een object, bijvoorbeeld het mogen schrijven in tabel A in een CRM pakket voor de ene rol en alleen lezen voor een andere rol hoeft slechts één keer gezet te worden.

[8] Deze standaard is gemaakt op basis van voorstel van Ravi Sandhu, David Ferraiolo en Richard Kuhn, “The NIST Model for Role-Based Access Control: Towards a Unified Standard (http://csrc.nist.gov/rbac/EDACcompliance.pdf)

2.1.2. Overerving

Rollen binnen een RBAC omgeving kunnen elkaar vaak ook overerven. Daardoor kunnen er verschillende rollen gecombineerd worden tot een andere rol. Om dit duidelijk te maken volgt hieronder een voorbeeld, welke in de Figuur 2 schematisch is weergegeven.

In figuur 2 zijn de permissies worden weergegeven als ellipsen en de rollen als cirkels.



Figuur 27 Voorbeeld van overerving van permissies

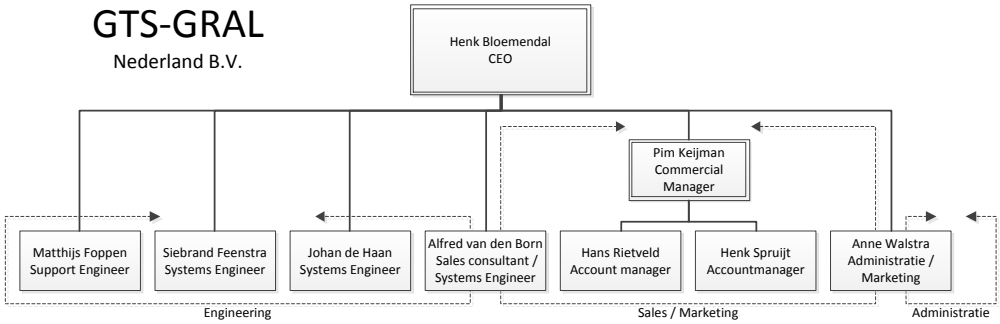
De rol “Auteur” bevat o.a. de permissies om bestanden te lezen, nieuwe bestanden aan te maken en eigen gemaakte bestanden te wijzigen of te verwijderen. De rol “Super-Auteur” is gekoppeld aan zowel de rol “Auteur” als de Permissie om bestanden van een ander te wijzigen. Een persoon die lid is van de rol “Super-Auteur” kan daardoor niet alleen bestanden van anderen wijzigen, maar heeft ook alle permissies die horen bij de rol “Auteur”. Ook twee rollen kunnen gecombineerd worden tot een andere rol, zoals in volgende afbeelding is weergegeven bij de rol “Volledige bestands controle”.

2.2. Rollen in de huidige situatie

Zowel binnen GTS-GRAL als bij de klant zijn nu al diverse rollen. Zo hebben we binnen GTS-GRAL al verschil tussen de rechten van een Support- en Systems Engineer. Maar ook bij de meeste van onze klanten zijn op dit moment al diverse rollen te omschrijven: zo zijn er de “gewone” gebruikers, een of meerdere personen die beslissingen nemen over organisatorische en financiële wijzigingen en vaak ook lokaal een beheerder voor kleine ICT-problemen.

2.2.1. Rollen binnen GTS-GRAL

Op dit moment is GTS-GRAL een redelijk platte organisatie. Dit blijkt ook uit het organigram van de organisatie:



Figuur 28

Support- en Systems Engineers
Uit het organigram blijkt echter al een scheiding tussen de medewerkers in de techniek (Engineering) en de rest van de organisatie (Sales/Marketing en Administratie). Maar binnen Engineering bestaat er ook verschil in rechten op de omgeving: zo kan een Support Engineer lang niet zoveel aanpassingen doen op de GTS-Online omgeving als een System Engineer.

Gewone gebruikers
Alle medewerkers van GTS-GRAL zijn overigens zelf gebruiker van de GTS-Online omgeving en komt de rest van de rollen grotendeels overeen met die van een klant. Het enige verschil is alleen dat de afdeling Administratie meer inzicht heeft binnen het systeem om tot een correcte facturering te kunnen komen.

2.2.2. Rollen bij de klant

Bij onze klanten kunnen ook een aantal duidelijke rollen aangewezen worden die op dit moment al aanwezig zijn bij de klant. Zo is er de “gebruikersrol”, een “beslissersrol” en een “lokale beheerdersrol”.

Lokale beheerder
Bij veel van onze klanten die op dit moment gebruik maken van onze GTS-Online dienst één of meerdere medewerkers in dienst die al jarenlang de IT ondersteuning doen. En ook als de organisatie zo klein is dat deze geen beheerder in dienst heeft, is er vaak één die de kar trekt op IT gebied.

Bij problemen op de werkplek, zijn deze personen dan ook vaak het eerste aanspreekpunt voor de gebruiker. Komen deze personen er niet uit of

hebben deze personen geen rechten om de benodigde aanpassingen zelf te doen, dan nemen zij telefonisch contact met ons op of maken een ticket aan in ons online helpdesk systeem. Terugkoppeling over een oplossing of bij vragen is deze persoon dan ook vaak voor ons het aanspreekpunt.

Gewone gebruikers

Om de lijnen kort te houden sturen we er al wel steeds meer op aan dat de medewerkers bij een klant direct contact met ons opnemen. Dit zorgt ervoor dat medewerkers sneller geholpen kunnen worden en dat er vaak minder ruis ontstaat over een probleem. Medewerkers kunnen dit telefonisch doen, maar ook door een ticket aan te maken in ons helpdesksysteem.

De rol van de lokale beheerder wordt daardoor erg klein: kleine problemen die met een paar simpele handelingen en binnen korte tijd opgelost kunnen worden (zgn. eerstelijns incidenten) komen steeds vaker direct bij ons binnen. En problemen die grotere aanpassingen of meer tijd vergt, de zogeheten tweedelijns incidenten, kan de lokale beheerder zelf niet doen omdat hij geen rechten heeft op onze omgeving en zal hij dit altijd bij ons moeten neerleggen.

Beslissersrol

Naast de hierboven beschreven gebruikers- en beheerdersrol zijn er vaak ook één of meerdere personen die over de (financiële en/of organisatorische) beslissingen gaan. Vaak is door bijvoorbeeld een gebruiker die een pakket wenst te gebruiken waarvoor een licentie nodig is, al aangekaart dat deze wens er is en is hier al (in)formeel toestemming voor verleend. Maar ook bij andere aanpassingen in het systeem die niet standaard zijn binnen de omgeving en waar dus extra tijd (en dus geld) aan gespendeerd dient te worden of een organisatorische wijziging vergt, wordt zo'n beslisser ingeschakeld.

2.3. Rollen in de gewenste situatie

In de situatie met een Self Service Portal moet er veel meer functionaliteit beschikbaar zijn voor de klant. Daardoor zullen veel (voornamelijk administratieve) zaken door de klant zelf uitgevoerd moeten kunnen worden. Het is de bedoeling dat de Self Service Portal de primaire locatie wordt als gebruikers problemen ervaren op IT-gebied.

Omdat de mogelijkheden voor de klant groeit van één (namelijk het aanmelden van een probleem middels ticket, e-mail of per telefoon) naar enkele tientallen, willen we deze meteen vanaf het begin af aan goed gaan scheiden. Het aantal rollen binnen de klant zal dus veel groter worden dan in de huidige situatie.

2.3.1. Rollen binnen GTS-GRAL

De rollen binnen GTS-GRAL zullen ongewijzigd blijven, aangezien de Support Engineer nog altijd de eerstelijns incidenten oplost en de Systems Engineers hierin ondersteunen indien nodig voor de zogeheten tweedelijns incidenten.

Wel zullen er stapsgewijs meer functies beschikbaar komen voor de Support Engineer(s) doordat taken beschikbaar komen d.m.v. de Self Service Portal die normaal met Administrator rechten zouden moeten worden uitgevoerd.

2.3.2. Rollen bij de klant

De te definiëren rollen zijn voor een groot deel een abstractie van de functionaliteiten die in de Self Service Portal aangeboden dienen te gaan worden zoals gebruikerstaken, beheerderstaken en bepaalde vormen van informatievoorziening. In de tabel op de volgende pagina zijn een aantal permissies (rijen) genoemd die aan verschillende rollen (kolommen) gekoppeld zouden kunnen worden.

Zoals al uitgelegd in het hoofdstuk over RBAC kunnen deze rollen ook overerven, zoals bijvoorbeeld de rollen “Accountbeheer HRM”, “Accountbeheer uitgebreid” en “Account- en groepsbeheer”. Dit zijn rollen die elkaar overerven (te zien aan de lichter weergegeven markeringen). Deze overervingen zijn extra duidelijk aangegeven met de iets dikkere lijn er om heen.

Naast het doorvoeren van wijzigingen binnen GTS-Online zijn er op dit moment ook twee rollen gedefinieerd die wijzigingen in het systeem dienen te accepteren. Bijvoorbeeld omdat het gaat om toegang tot bepaalde applicaties waar licenties voor beschikbaar moeten zijn, toegang tot privacy gevoelige informatie of toegang tot andere informatie die alleen beschikbaar moet zijn voor personen met een bepaalde functie.

Permissies	Gewone gebruiker	Accountbeheer HRM	Accountbeheer uitgebreid	Account- en groepsbeheer	Werkplekbeheer	E-mailbeheer	Informatievoorziening	Informatievoorziening CMDB	Applicatiebeheerder
Aanmaken ticket	X	X	X	X	X	X	X	X	X
Wijzigen ticket	X	X	X	X	X	X	X	X	X
Verwijderen ticket	X	X	X	X	X	X	X	X	X
Aanmaken gebruikersaccount		X	X	X					
Uitschakelen gebruikersaccount		X	X	X					
Verwijderen gebruikersaccount			X	X					
Wijzigen gebruikersaccount details			X	X					
Wachtwoord resetten gebruikersaccounts			X	X					
Toevoegen gebruikersaccount aan beveiligingsgroep				X					
Verwijderen gebruikersaccount uit beveiligingsgroep				X					
Distributiegroep toevoegen						X			
Distributiegroep verwijderen						X			
Accounts toevoegen aan distributiegroep				X		X			
Accounts verwijderen uit distributiegroep				X		X			
Resource mailbox aanmaken						X			
E-mailadres toevoegen aan resource mailbox						X			
Resource mailbox verwijderen						X			
Rechten wijzigen op resource mailbox						X			
Computeraccount verwijderen					X				
Computeraccount toevoegen (Offline domain join)					X				
Weergeven van aangemaakte gebruikers							X	X	
Weergeven van gebruikers in groepen							X	X	
Weergeven van aantal computers							X	X	
Weergeven van geplande werkzaamheden	X	X	X	X	X	X	X	X	X
Weergeven van CMDB								X	
SLA rapportage							X	X	
Toegang tot applicaties accepteren									X

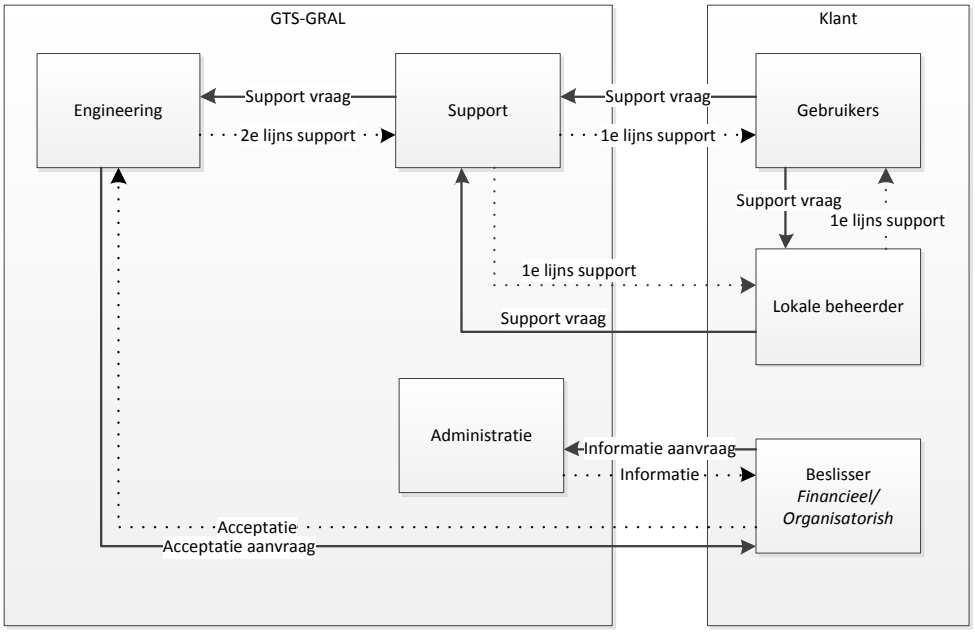
Figuur 29 Gewenste rollen en bijbehorende permissies

3. Proces verbetering

Zowel door de toevoeging van een Self Service Portal en door het uitsplitsen van de huidige rollen in veel kleinere onderdelen gaan de processen ook anders lopen.

3.1. Model huidige situatie

De rollen die gelden in de huidige situatie kunnen weergegeven worden in een onderstaand diagram, welke niet de gehele organisatie weergeeft, maar alleen de onderdelen die voor dit project van belang zijn:



Figuur 30 Processen huidige situatie

Duidelijk wordt uit dit diagram is de support vragen van de klant richting GTS-GRAL altijd eerst binnen komen bij de Support Engineers. Vragen van gebruikers worden ook regelmatig nog bij de lokale beheerder neergelegd, welke deze grotendeels dan bij ons aanmeldt.

De afdeling Support probeert uit te zoeken waar het probleem zit en deze, indien mogelijk, op te lossen. Als een vraag aanpassingen vergt op het systeem waarover deze medewerker geen kennis heeft of op dat onderdeel geen rechten heeft, zal een Systems Engineer worden ingeschakeld om naar het probleem te kijken en zal de tweedelijns ondersteuning worden gegeven.

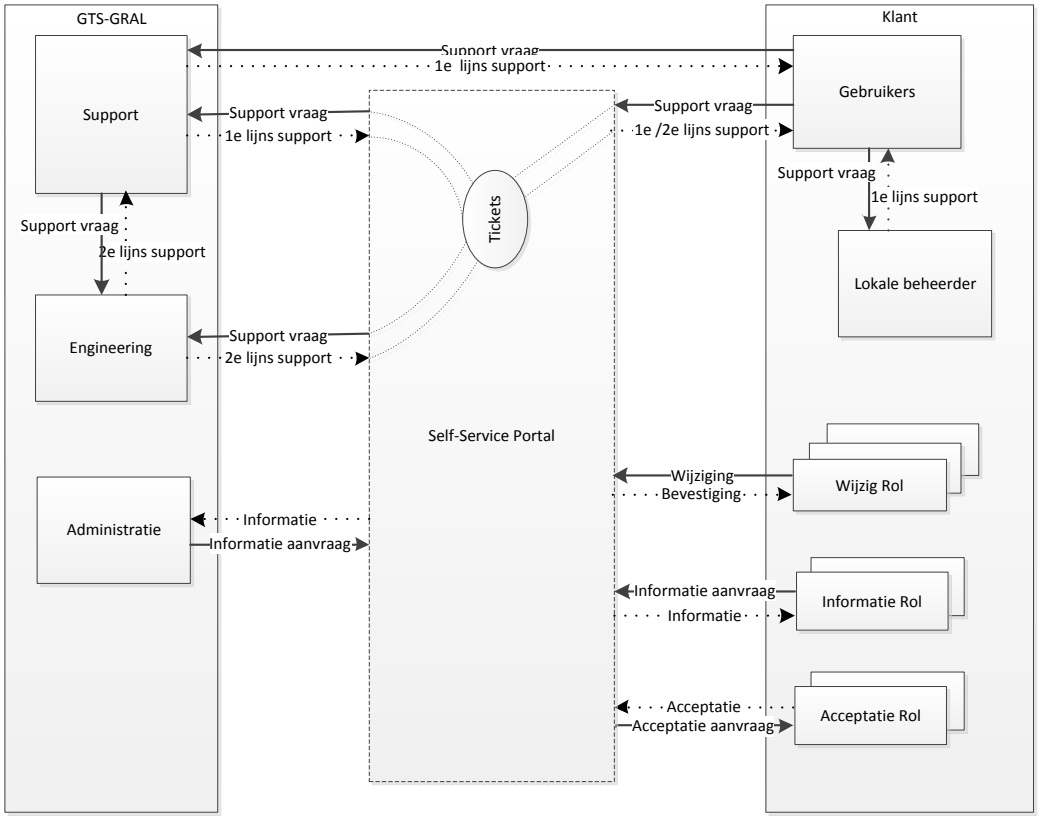
Is er een aanpassing nodig die financiële of organisatorische gevolgen heeft voor de klant, wordt hiervoor een akkoord gevraagd worden aan de beslisser(s) bij de klant. Deze beslissers hebben ook de bevoegdheid om informatie op te vragen over de diensten die zij bij ons gebruiken. Een voorbeeld: aangezien een klant o.a. betaald per werkplek per maand, is het belangrijk inzicht te hebben in het aantal werkplekken dat de klant op een bepaald moment in gebruik heeft. Dit soort informatie kan de afdeling Administratie (die deze informatie overigens ook zelf nodig heeft voor de facturering) uitzoeken en aan de klant verstrekken.

3.2. Model gewenste situatie

In de gewenste situatie gaat niet alleen de toevoeging van de vele verschillende rollen een wijziging geven in het eerder geschetste model. Ook de toevoeging van de Self Service Portal zorgt voor een grote wijziging. De Self Service Portal zorgt in wezen voor een extra laag tussen de klant en GTS-GRAL in.

Verder is de directe rol van de lokale beheerder is nog aanwezig voor de gebruikers bij een klant als het gaat om kleine problemen op de werkplek. Maar de lokale beheerder moet een veel kleinere rol gaan spelen in het aanmelden van problemen die door gebruikers bij hem gemeld worden, zodat de lijnen duidelijker worden voor de gebruiker.

Verder kunnen personen bij de klant al naar gelang de rollen die zijn toebedeeld meer of minder wijzingen doorvoeren, wijzigingen accepteren en informatie opvragen. In onderstaande figuur zijn al deze wijzigingen visueel weergegeven:



Figuur 31 Processen gewenste situatie

Het moet ook duidelijk worden uit bovenstaande model dat niet altijd alles via de Self Service Portal kan verlopen. Het is altijd mogelijk om direct een vraag neer te leggen bij Support, alleen al om de simpele reden dat gebruikers niet kunnen inloggen vanwege een vergeten wachtwoord en op dat moment ook geen toegang hebben tot de Self Service Portal.

3.3. Verbeteringen t.o.v. huidige situatie

Het invoeren van de Self Service Portal zal diverse verbeteringen moeten opleveren. Zo zullen naast het feit dat steeds maar vragen in de organisatie van de klant zelf opgelost kunnen worden ook de processen rondom wijzigingen soepeler moeten gaan verlopen.

Bijvoorbeeld als er “acceptatie” nodig is voor een wijziging, zal in plaats van dat een engineer van GTS-GRAL dit mondeling of per e-mail kenbaar maakt bij de betreffende persoon, de Self-Service portal deze vraag bij de juiste persoon beschikbaar maken.

Ook zal GTS-GRAL van de invoering van de Self Service Portal kunnen profiteren. Administratie hoeft niet meer handmatig een overzicht te maken van de gegevens van de klant, maar kan van een zelfde overzicht gebruik maken als de klant, zodat gegevens voor de facturering altijd overeenkomen met wat de gebruiker zien in zijn overzicht.

4. Modellen

De functionaliteit die beschikbaar moet komen in de Self Service Portal zal in de vorm zijn van Service Requests. Dit komt overeen met het onderdeel Change Management[9] in ITIL en is voor de gebruiker niets meer dan een formulier met de gewenste wijziging in het systeem. Deze wijziging dient, indien gewenst gevalideerd te worden door een verantwoordelijke, en vervolgens (handmatig of automatisch) aangepast te worden.

Een Service Request leidt dus altijd tot één of meerdere activiteiten die uitgevoerd dienen te worden om de gedane Service Request te voltooien. Voorbeelden van de belangrijkste activiteiten zijn:

- Review Activity: een eindverantwoordelijke wordt aangesteld om de aangevraagde aanpassing te valideren en akkoord te geven of te weigeren.
- (Runbook) Automation Activity: hiermee wordt over het algemeen de aanpassing gedaan, waarbij geen interactie nodig is: deze wordt automatisch uitgevoerd. In Service Manager gebruiken we hier de integratie met Orchestrator voor om automatisch een Runbook uit te voeren.
- Manual Activity: een handmatige activiteit. Sommige aanpassingen zijn te omslachtig om te automatiseren of niet wenselijk om deze te automatiseren en zullen handmatig uitgevoerd worden.

Er wordt in Bijlage 5 uitgebreid ingegaan op de integratie mogelijkheden tussen Service Manager en Orchestrator en ook over de werking van Runbooks. Wat voor dit functioneel ontwerp van belang is, is dat een Runbook een workflow is van scripts of activiteiten die automatisch worden uitgevoerd.

4.1. Algemeen Service Request proces

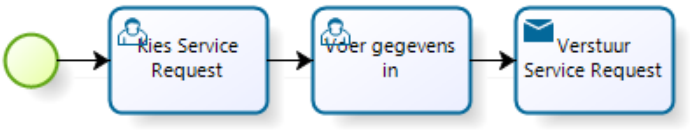
Uiteindelijk hebben de meeste functies die beschikbaar moeten komen via de Self Service Portal grotendeels dezelfde opbouw. Deze stappen zal ik eerst stuk voor stuk bespreken, vervolgens volgt een samenvattend model.

4.1.1. Start Service Request

Zo zal het proces altijd starten bij de gebruiker die kiest welke aanpassing hij/zij wil doen in de omgeving door een Service Request uit te kiezen in de Self Service Portal. Dit is uiteindelijk een formulier waarin alle gegevens worden opgevraagd om de benodigde gegevens te verzamelen.

Deze gegevens worden ingevoerd en waar nodig via de Self Service Portal gevalideerd (bijvoorbeeld een e-mailadres, cijfer of datum). De ingevoerde gegevens kunnen worden gecontroleerd en verstuurd.

9 http://en.wikipedia.org/wiki/Information_Technology_Infrastructure_Library#Change_management

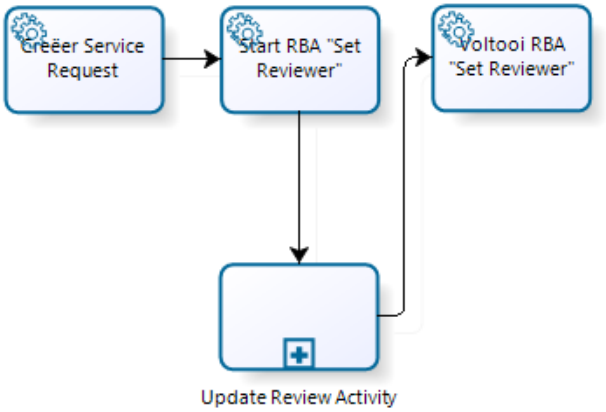


Figuur 32 Gebruiker maakt een Service Request aan

Op het moment van versturen wordt er een Service Request aangemaakt in Service Manager. Direct na het aanmaken van een Service Request zullen de geconfigureerde activiteiten worden gestart. Over het algemeen zullen dit drie activiteiten zijn:

4.1.2. Runbook Activity 1, "Bepalen van Reviewer"

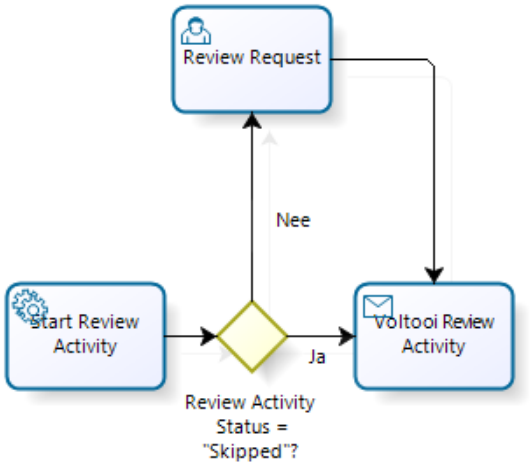
Er moest eerst bepaald worden of er een akkoord gegeven moet worden voor deze wijziging en wie dat akkoord zou moeten geven. Indien er geen akkoord nodig is (in het geval dat het geen financiële gevolgen heeft, bijvoorbeeld) dan zal de volgende activiteit worden overgeslagen door daarvan de status op "Skipped" te zetten. De wijzigingen worden gedaan door de Runbook "Set reviewer".



Figuur 33 Bepalen van Reviewer

4.1.3. Review Activity

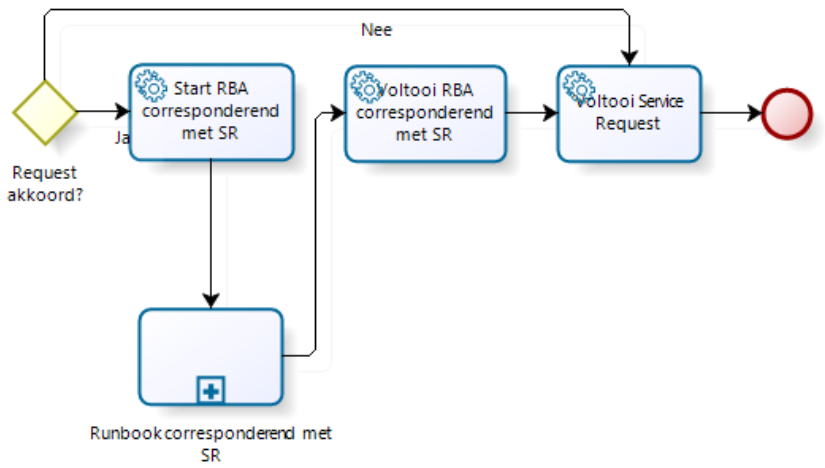
In deze activiteit wordt de hiervoor ingestelde “Reviewer” (dit kan ook een groep personen zijn) gevraagd akkoord te geven voor het Service Request. Deze activiteit wordt alleen gestart op het moment dat de status niet op “Skipped” is gezet door de vorige activiteit.



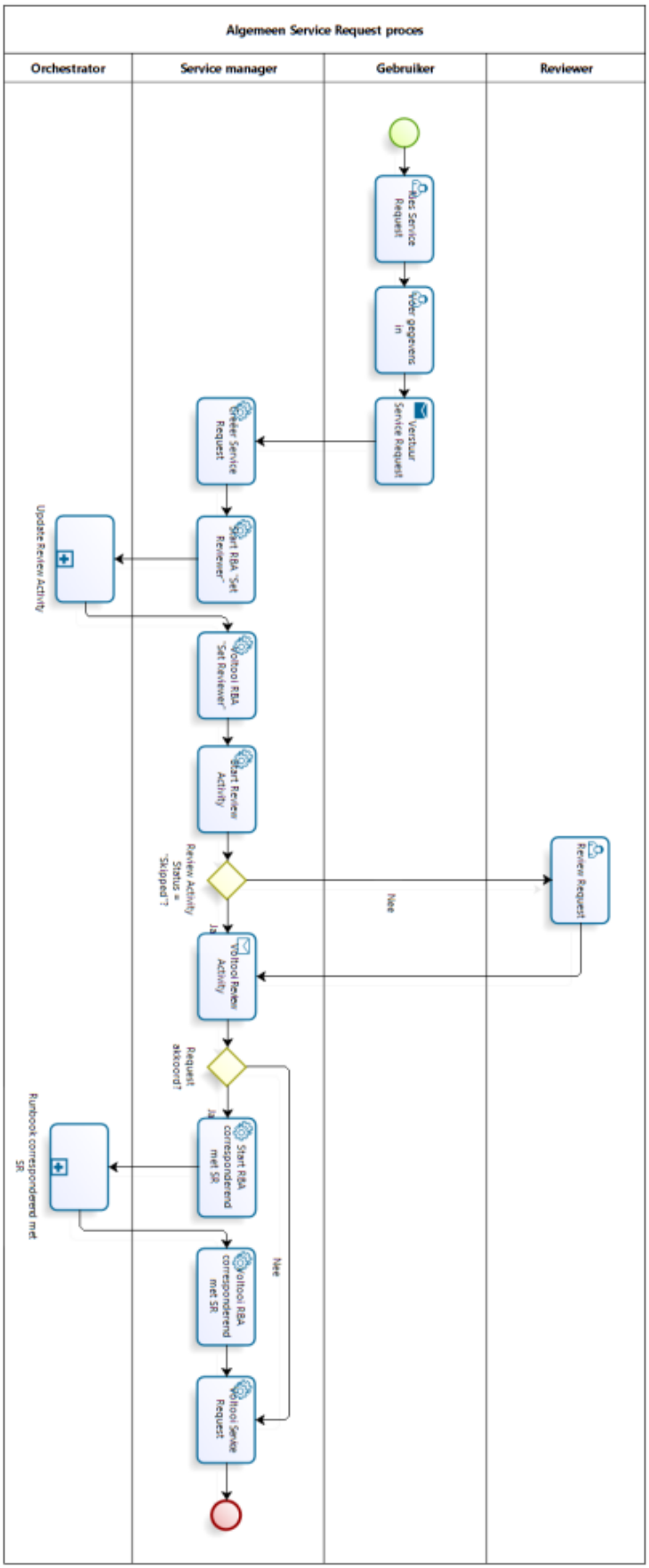
Figuur 34 Review Activity

4.1.4. Runbook Activity 2, corresponderend met Service Request

Het uitvoeren van de wijziging zelf door het starten van een Runbook in Orchestrator. Dit gebeurt uiteraard alleen indien de voorgaande activiteiten zijn doorlopen.



Al deze taken in een compleet model is weergegeven op de volgende pagina.



Figuur 35 Algemeen Service Request Proces

In de afbeelding op de vorige pagina is goed te zien welke processtappen op welk niveau worden uitgevoerd. De meeste stappen worden gedaan in Service Manager, maar hier blijkt niet de meeste tijd in te zitten. Vooral de te ontwikkelen stappen in Orchestrator zijn zeer tijdrovend. Een goed voorbeeld daarvan wordt duidelijk uit de stappen in het Orchestrator runbook “Set Reviewer”.

4.1.5. Runbooks

Er is ondertussen al een aantal keer gesproken over dat er een Runbook wordt uitgevoerd om de aanpassing te doen. Hierna volgen de twee hiervoor genoemde Runbooks met alle stappen en de functionaliteit van die stappen.

Zoals uit onderstaande voorbeelden blijkt, zijn veel activiteiten technisch nodig om bepaalde functionaliteit mogelijk te krijgenmaar vertroebelt dit het overzicht van de stappen die werkelijk genomen worden. Ik zal de rest van de modellen die ik zal maken op een iets hoger niveau maken, waarbij de kleine stappen die wel nodig zijn om iets mogelijk te maken achterwege blijven.

4.1.5.1. Runbook “Update Review Activity”

De Runbook Activity “Update Review Activity” zal regelmatig terugkomen. Dit komt omdat voor veel aanpassingen er akkoord nodig is van een eindverantwoordelijke. Bij het aanmaken of verwijderen van een gebruikersaccount, het toevoegen van een gebruiker een aan een applicatie waar extra licentiegeld voor betaald moet worden en nog een aantal van dit soort aanpassingen vereisen dat deze worden geverifieerd bij een daarvoor verantwoordelijke.

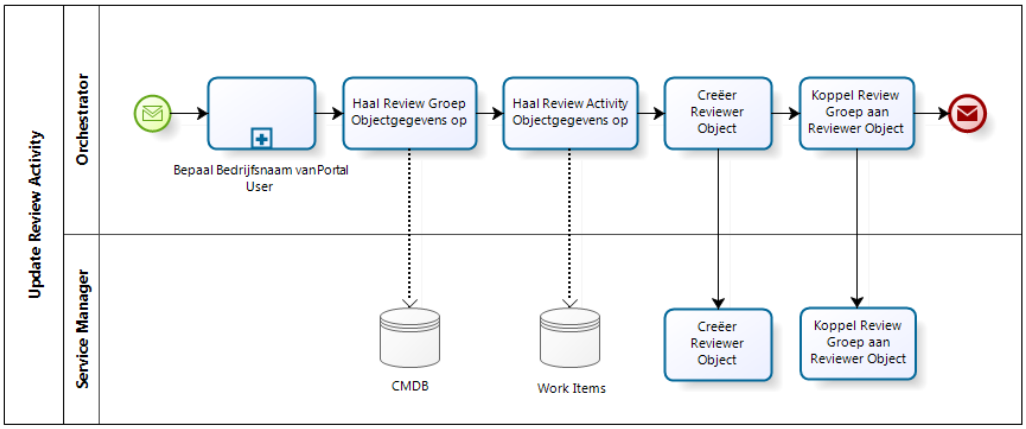
Het runbook “Update Review Activity” ziet er als volgt uit:

Figuur 36 Runbook “Update Review Activity”

De stappen die worden uitgevoerd zijn hieronder besproken.

Activiteit	Beschrijving	Input
Initialize Data	Hiermee wordt doorgaans een runbook gestart. Hier worden de benodigde parameters gedefinieerd.	Portal User Name *(gebruikersnaam van de gebruiker die het Service Request heeft gestart)* ActivityID *(ID van de Runbook Activity die dit Runbook heeft gestart)* Area *(indien dit een specifiek domein betreft, zoals HRM, kan deze worden meegegeven voor een specifieke "Review-groep")*
Invoke Runbook Get Portal User Company	Met de Portal User Name wordt een ander runbook gestart: "Get Portal User Company" om de naam van zijn bedrijf op te halen	Portal User Name uit "Initialize Data"
Create Approver Group Name	De naam van de groep die het Service Request moet reviewen wordt opgebouwd uit COMPANY_AREA_Approvers. Deze groep is eerder al aanemaakt per bedrijf en domein in Active Directory.	Company uit "Invoke Runbook Get Portal User Company" Area uit "Initialize data"
Get Group Object	De bijbehorende groep object wordt opgezocht in de Service Manager CMDB.	Approver Group Name uit "Create Approver Group Name"
Get Runbook Activity	De Runbook Activity die dit Runbook heeft geïnitieerd wordt opgehaald uit Service Manager	ActivityID uit "Initialize Data"
Get related Service Request	De SC Object GUID van het gerelateerde Service Request die eerder opgehaalde Runbook Activity wordt bepaald	SC Object GUID uit "Get Runbook Activity"
Get Service Request	Het Service Request zelf wordt opgehaald uit Service Manager	Related Object GUID uit "Get related Service Request"
Get related Review Activity	De SC Object GUID van het aan de Service Request gekoppelde Review Activity wordt bepaald	SC Object GUID uit "Get Service Request"
Get Review Activity	De Review Activity zelf wordt opgehaald	Related Object GUID uit "Get related Review Activity"
Create Related Object	Er wordt een object gemaakt van het type Reviewer en gekoppeld aan de Review Activity	SC Object GUID uit "Get Review Activity" Approver Group Name uit "Create Approver Group Name"
Create Reviewer Relationship	Er wordt een relatie gemaakt tussen de Approver Group en het Reviewer object	Object GUID uit "Related Group Object" SC Object GUID uit "Get Group Object"

Een aantal van voorgaand genoemde stappen zijn erg technisch, maar duidelijk is wel dat vanuit Orchestrator ook weer veel gecommuniceerd wordt met de CMDB van Service Manager. Een duidelijkere weergave van de stappen en de communicatie met de buitenwereld is weergeven in de volgende afbeelding.

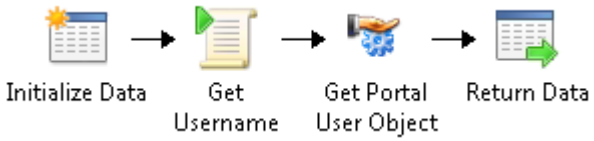


Figuur 37 Subproces "Update Review Activity"

Dit subproces “Update Review Activity” is een stuk duidelijker te lezen, aangezien ook duidelijk wordt welke gegevens opgehaald worden. Het subproces “Bepaal Bedrijfsnaam van Portal User” is ook weer een Runbook. Deze word in volgende paragraaf besproken.

4.1.5.2. Runbook “Get Portal User Company”

In het runbook “Update Review Activity" dat besproken werd in vorige paragrafen wordt ook nog een ander runbook gestart met de activiteit “Invoke Runbook Get Portal User Company”. Dit Runbook is erg kort en ziet er als volg uit:

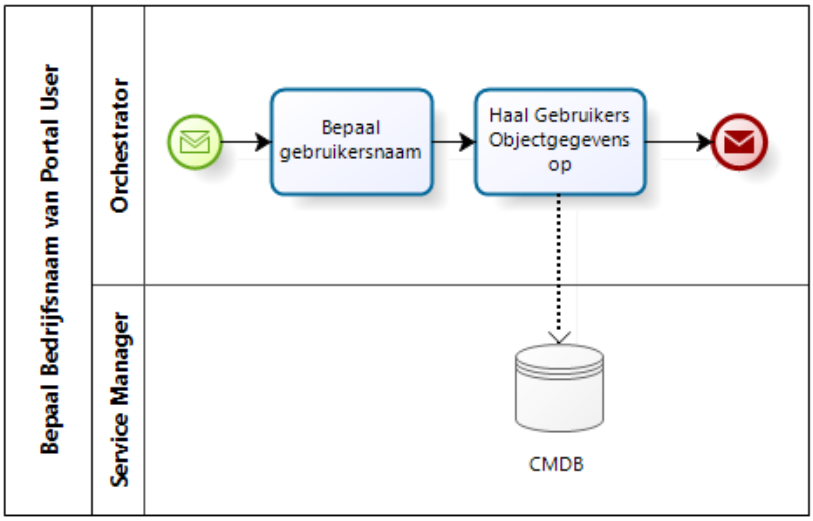


Figuur 38 Runbook "Get Portal User Company"

De stappen die in dit runbook worden genomen zijn als volgt:

Activiteit	Beschrijving	Input
Initialize Data	Hiermee wordt doorgaans een runbook gestart. Hier worden de benodigde parameters gedefinieerd.	Portal User Name *(gebruikersnaam van de gebruiker die het Service Request heeft gestart)*
Get Username	Met dit powershell script wordt blijft alleen de gebruikersnaam over (de Portal User Name bestaat uit DOMEIN\Username)	Portal User Name uit “Initialize Data”
Get Portal User Object	Het bij de username horende object wordt opgezocht in de Service Manager CMDB.	Portal User Name uit “Get Username”
Return Data	Met deze activiteit worden parameters weer teruggestuurd Deze activiteit geeft de Company terug op basis van extensionAttribute1.	extensionAttribute1 uit “Get Portal User Object”

Ook deze stappen heb ik omgezet naar een ander model, en zelfs dit korte proces wordt daarmee een stuk leesbaarder:



Figuur 39 Subproces "Get Portal User Company"

4.2. Beheertaken

In het hoofdstuk 7.1 is uitgebreid stil gestaan over het gehele proces van het indienen van een Service Request tot het afhandelen ervan, met mogelijk nog het valideren van het betreffende Service Request. Daarin is uiteraard nog niet opgenomen welke taken er aan het eind van het Service Request geautomatiseerd moeten worden. Deze zal ik hier behandelen.

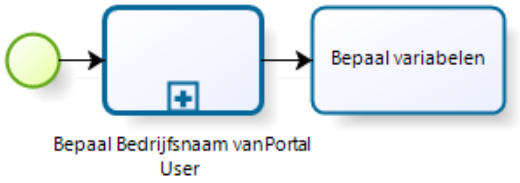
4.2.1. Aanmaken gebruiker

Voor het aanmaken van een gebruiker zijn de volgende gegevens nodig:

Parameter	Waarde
Portal User Name	Gebruikersnaam van de ingelogde gebruiker
Voornaam	Voornaam van de aan te maken gebruiker
Tussenvoegsel & Achternaam	Achternaam van de aan te maken gebruiker
E-mailadres	Deze wordt gebruikt voor: UPN -> gebruikersnaam@bedrijfsdomein.nl SAMAccountName -> GO\bedrijfsnaamgebruikersnaam
Wachtwoord	Het initiële wachtwoord dat wordt ingesteld voor de aan te maken gebruiker

4.2.1.1. Variabelen verzamelen

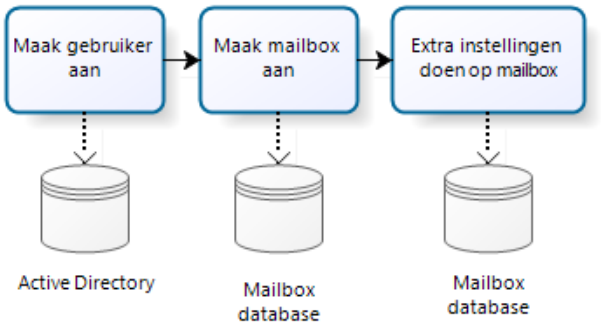
De bedrijfsnaam wordt opgemaakt uit de “Portal User Name”. Dit is de eerste stap die gedaan wordt. Vervolgens moeten eerst o.a. de UPN, sAMAccountname, en locatie waar het account moet worden opgeslagen worden gecreëerd.



Figuur 40 Variabelen verzamelen & instellen

4.2.1.2. Account & mailbox aanmaken

Volgende stap is om het gebruikersaccount aan te maken, een mailbox te creëeren en deze te koppelen en diverse bedrijfsnaam afhankelijke variabelen in te stellen. Ook moet het account meteen in een aantal groepen opgeslagen worden. Na het aanmaken moeten diverse instellingen gedaan worden. Zo moeten er een e-mailadres ingesteld worden, instelling voor het offline adresboek voor de gebruiker ingesteld worden en moet de e-mailadrespolicy vervolgens aangezet worden.

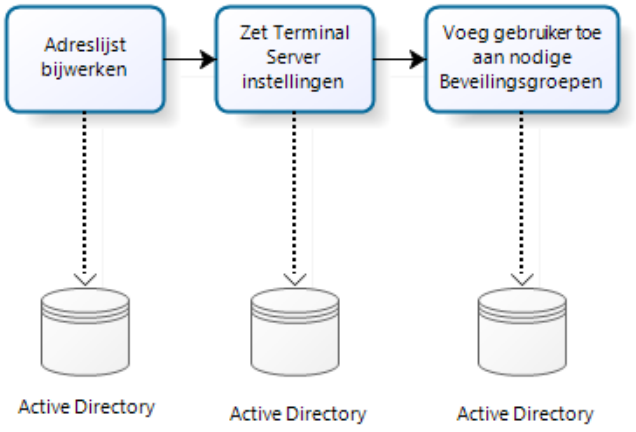


Figuur 41 Account & mailbox aanmaken

4.2.1.3. Active Directory bijwerken: Adreslijst, Terminal Server instellingen & beveiliging groepen

De adreslijst van het bedrijf moet vervolgens ook bijgewerkt worden, zodat de nieuwe gebruiker zichtbaar wordt voor de rest van het bedrijf. Voor het inloggen op onze omgeving moet de gebruiker in ieder geval lid zijn van de zogeheten “bedrijfsbeveiligingsgroep”. Deze heeft altijd de vorm “BEDRIJFSNAAM SG”. Deze groep regelt de rechten voor het inloggen op veel systemen en de rechten op gezamenlijke bestanden, de “Groepsdata”.

Daarnaast gebruikt bijna iedere klant Terminal Server en daarom wordt voor iedere gebruiker deze instellingen ingesteld. Dat zijn bijvoorbeeld de locatie van zijn Terminal Server profiel, de locatie van zijn persoonlijke map en het vinkje aangezet worden dat deze gebruiker mag inloggen middels Terminal Services.



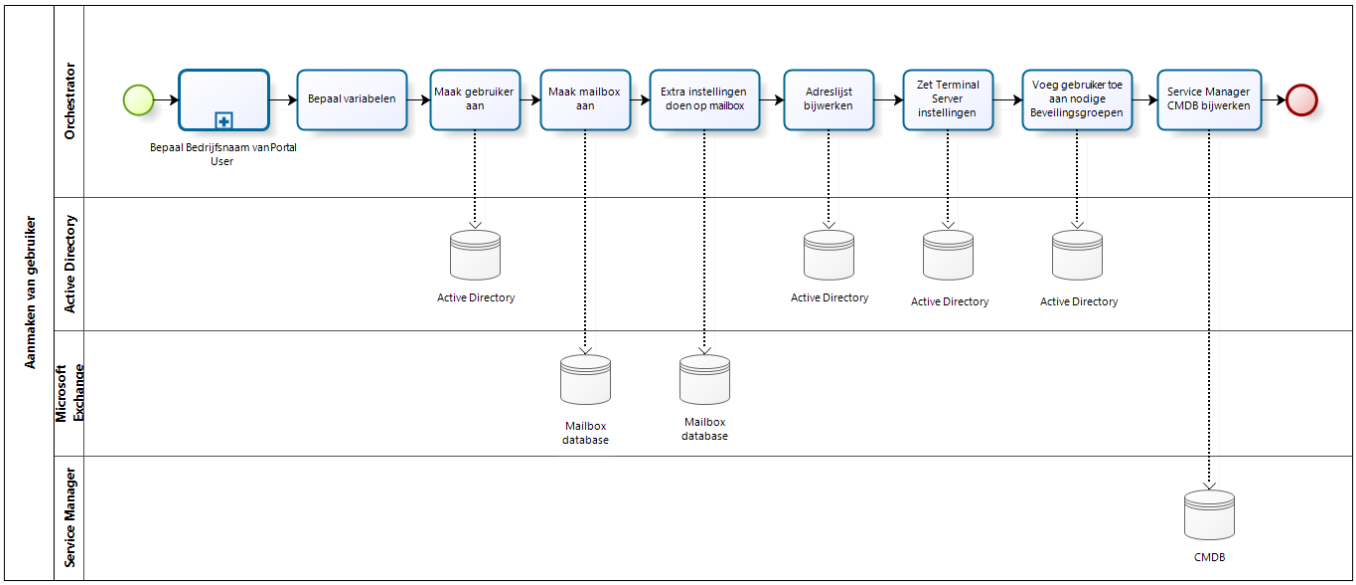
Figuur 42 Active Directory bijwerken

4.2.1.4. Service Manager bijwerken

Laatste stap is om de CMDB van Service Manager bij te werken door de connector te starten die synchroniseert met Active Directory. Helaas kan het bijwerken van de Custom Attribute extensionAttribute1 maar ééns in het uur bijgewerkt worden. Dus pas na een aantal uur nadat het Service Request is ingediend voor het aanmaken van een gebruikersaccount, kunnen verdere aanpassingen worden gedaan door de klant op dit nieuwe account.

4.2.1.5. Totaal

Alle stappen bij elkaar leiden tot het volgende model:



Figuur 43 Toevoegen van een gebruiker

4.2.2. Verwijderen gebruiker

Voor het verwijderen van een gebruiker zijn minimaal de volgende gegevens nodig:

Parameter	Waarde
Portal User Name	Gebruikersnaam van de ingelogde gebruiker
Gebruiker	Gebruikersnaam van de aan te verwijderen gebruiker
Datum Uit Dienst	Datum vanaf wanneer de betreffende gebruiker uit dienst gaat

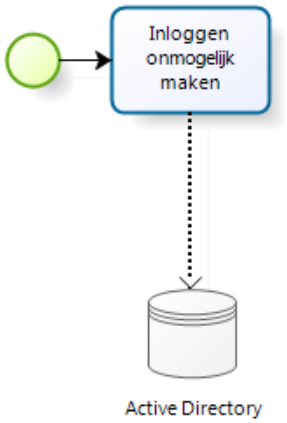
Daarnaast is het mogelijk dat het wenselijk is dat de gegevens van de gebruiker opgeslagen of benaderbaar zijn op het moment dat hij/zij uit dienst is. Dit zal per bedrijf verschillen en hier zullen we pragmatisch mee om moeten gaan. Het runbook zal echter wel alle functionaliteit moeten bevatten om alle mogelijke stappen te doorlopen. De volgende parameters zullen dan van belang zijn:

Parameter	Waarde
Persoonlijke map behouden	Ja/Nee
Gebruikersnaam andere gebruiker t.b.v. persoonlijke map	Indien persoonlijke map bewaard dient te blijven, moet hier worden gedefinieerd welke gebruiker toegang krijgt
Mailbox behouden	Ja/Nee
Gebruikersnaam andere gebruiker t.b.v. mailbox	Indien mailbox bewaard dient te blijven, moet hier worden gedefinieerd welke gebruiker toegang krijgt

Het verwijderen van een gebruiker op een bepaalde datum zal er voor zorgen dat er een extra activiteit zal moeten komen in het Service Request proces dat eerder besproken is (zie hoofdstuk 7.1). Na het valideren van het verwijderen van een gebruiker door de “reviewer”, zal er eerst een timer moeten gaan draaien tot de betreffende dag is aangebroken. Op dat moment zal het proces in Orchestrator gaan draaien in de vorm van een runbook. De stappen die daarin gedaan worden zijn als volgt:

4.2.2.1. Inloggen uitschakelen

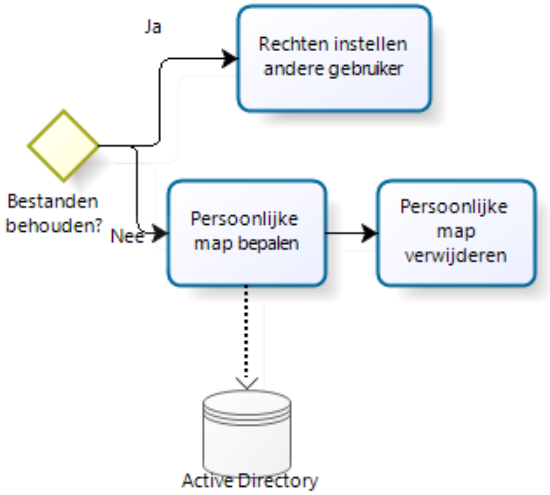
In Active Directory dient het account uitgeschakeld te worden, waardoor er meteen niet meer mee kan worden ingelogd. Er zijn twee manieren om dat te doen, maar wij doen hier “Disable account” aangezien het account naar alle verwachting niet meer beschikbaar hoeft te komen.



Figuur 44 Disable account in Active Directory

4.2.2.2. Bestanden wel/niet verwijderen

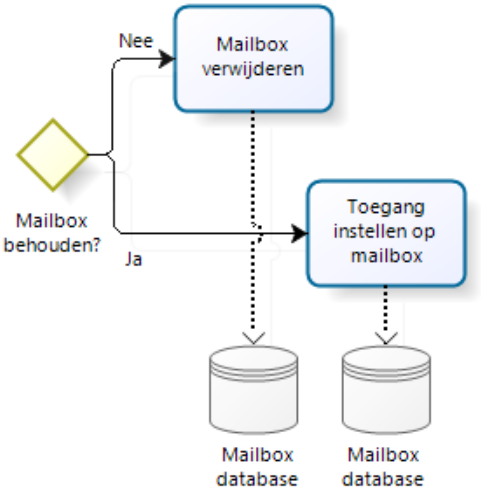
Vervolgens is er aangegeven of de bestanden verwijderd moeten worden. Indien dat het geval is, moet eerst bepaald worden a.d.h.v. gegevens uit Active Directory waar die staan om deze vervolgens te verwijderen. Anders is er aangegeven welke gebruiker rechten moet krijgen op deze map om de inhoud er van te kunnen benaderen.



Figuur 45 Bestanden wel/niet verwijderen

4.2.2.3. Mailbox wel/niet verwijderen

De volgende stap betreft de mailbox: moet die wel of niet verwijderd worden en zo nee: wie moet er rechten krijgen op de mailbox om deze te benaderen:



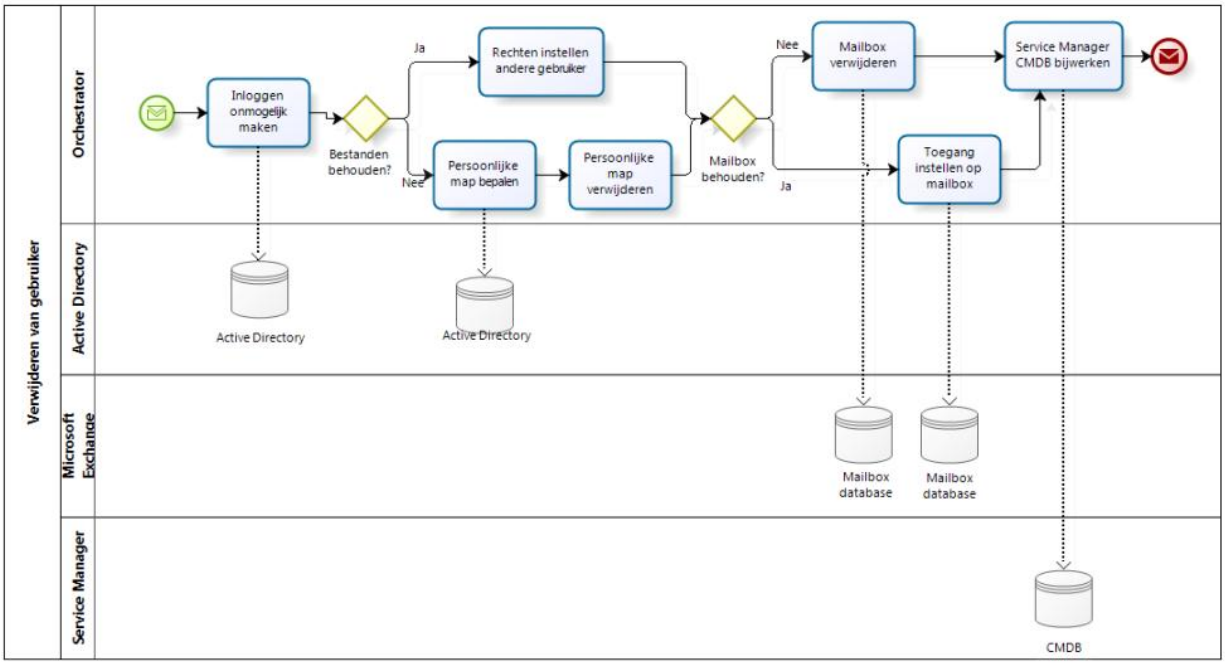
Figuur 46 Wel/niet verwijderen mailbox

4.2.2.4. Service Manager bijwerken

De laatste stap in het proces is het bijwerken van de CMDB van Service Manager: we willen niet dat deze gebruiker vanaf dat moment nog voorkomt in de database.

4.2.2.5. Totaal

Het hele proces ziet er als volgt uit:

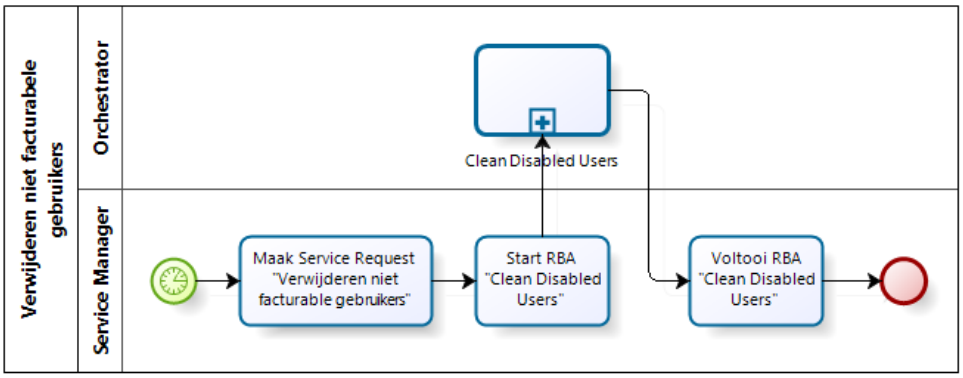


Figuur 47 Verwijderen van een gebruiker

4.2.2.6. Verwijderen niet facturable gebruikers

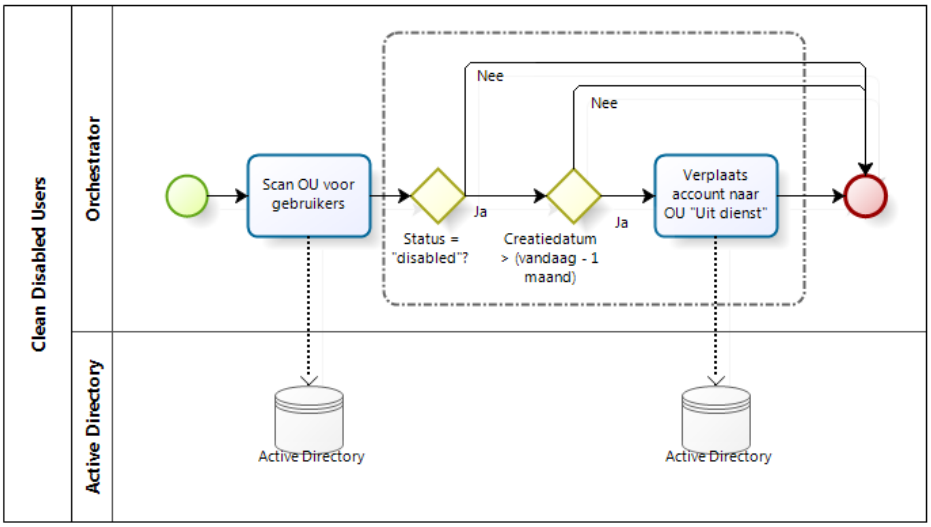
Verder geldt: de maand waarin een gebruiker verwijderd wordt, hoeft niet altijd betaald te worden. Wordt een gebruiker verwijderd voor de 15e, dan zal hier niet voor gefactureerd te worden, na de 15e dan zal dit wel het geval zijn. Wordt een gebruiker aangemaakt en dezelfde maand voor de 15e weer worden verwijderd, dan zal deze alsnog moeten worden gefactureerd. Hier dienen dus twee controles te draaien.

Eerst het proces in Service Manager. In Service Manager wordt iedere 15e van de maand een Workflow gestart die een Service Request aanmaakt. Deze heeft als enige taak het starten van een Runbook in Orchestrator:



Figuur 48 Workflow maakt Service Request "Verwijderen niet facturabele gebruikers"

Alle accounts worden gescand en indien de status "disabled" en de creatiedatum lager is dan vorige maand de 15e, zal het account worden verplaatst naar een andere locatie waardoor deze niet wordt meegenomen in de facturatie. Het vlak met de stippellijn geeft aan dat dit per gebruikersaccount wordt uitgevoerd. Zie hieronder het betreffende runbook:

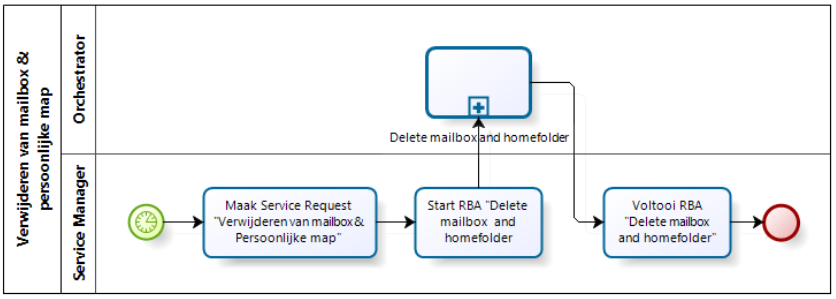


Figuur 49 Runbook "Clean Disabled Users"

4.2.2.7. Verwijderen mailbox en persoonlijke map

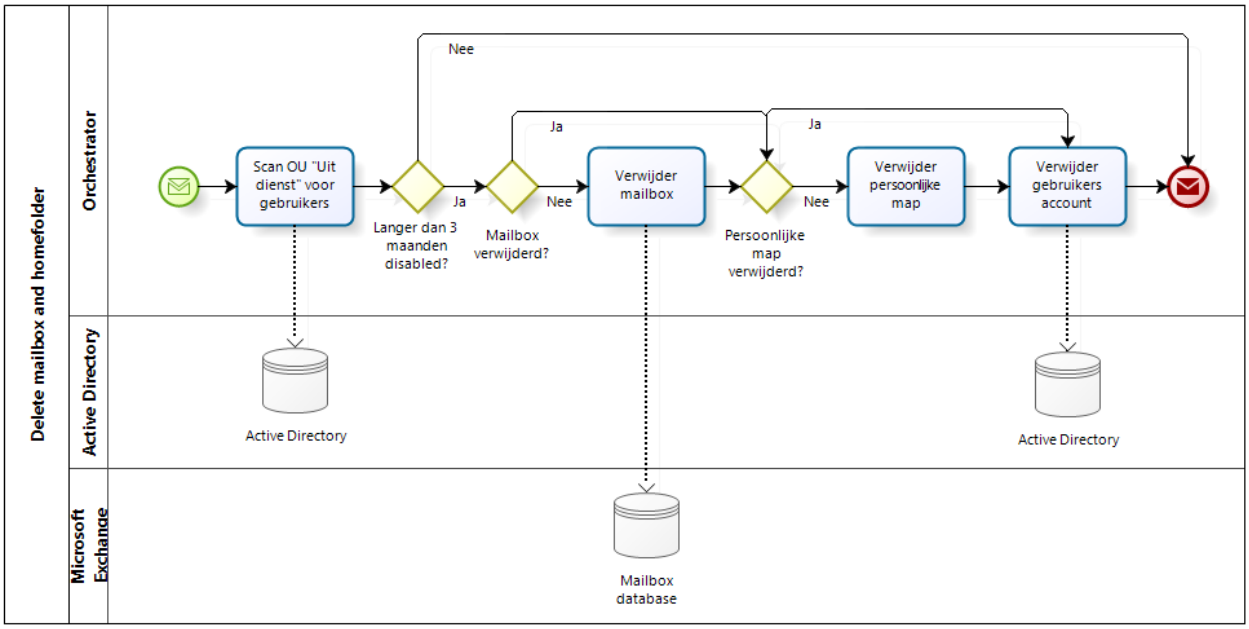
Indien een persoonlijke map of mailbox beschikbaar moet blijven nadat het bijbehorende account tot een gebruikersaccount 3 maanden uit dienst is. Dan zal er een andere workflow gaan draaien om de bestanden definitief te verwijderen om geen vervuiling van het systeem te krijgen.

Iedere maand dient er dus gecontroleerd worden of er nog accounts langer dan 3 maanden uitgeschakeld staan en of de bijbehorende bestanden al zijn verwijderd. Dit gebeurt door in Service Manager iedere maand een workflow te starten die een Service Request aanmaakt. In dit Service Request is slechts één activiteit opgenomen, namelijk het starten van een Runbook in Orchestrator die de hele operatie op zich neemt.



Figuur 50 Workflow van het maken van Service Request "Verwijderen van mailbox & persoonlijke map"

Het runbook dat wordt gestart, voert de volgende stappen uit:



Figuur 51 Runbook "Delete mailbox and homefolder"

Gebruikersaccounts die al langer dan 3 maanden de status “disabled” hebben worden gecontroleerd op mailbox en persoonlijke map. Indien deze nog bestaan worden deze verwijderd en vervolgens wordt in ieder geval het account definitief verwijderd.

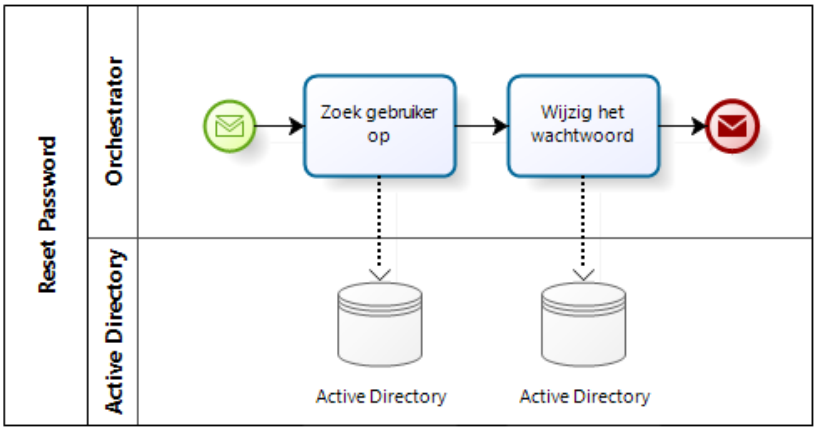
4.2.3. Wachtwoord resetten van gebruiker

Het resetten van een wachtwoord is één van de wat gemakkelijker taken om te maken. Deze Service Request behelst geen grote aanpassing en ook het valideren van de aanvraag is niet nodig. De personen die dit soort aanvragen op dit moment doen bij ons, zijn meestal voorheen ook de systeembeheerder geweest bij de klant en hadden dan dus ook de mogelijkheid om het wachtwoord te restten.

Het betreft dus een Service Request met slechts één taak: het uitvoeren van een Runbook. Daarvoor zijn wel de volgende gegevens nodig:

Parameter	Waarde
Gebruiker	Gebruikersnaam van de aan te passen gebruiker
Wachtwoord	Nieuw in te stellen wachtwoord

De te nemen stappen zijn ook redelijk kort: het account van de gebruiker moet worden opgezocht in Active Directory en vervolgens moet het wachtwoord worden gewijzigd naar het ingevoerde wachtwoord:



Figuur 52 Runbook "Reset Password"

4.2.4. Toevoegen van gebruiker aan groep

De volgende gegevens zijn nodig om een gebruiker toe te voegen aan een groep:

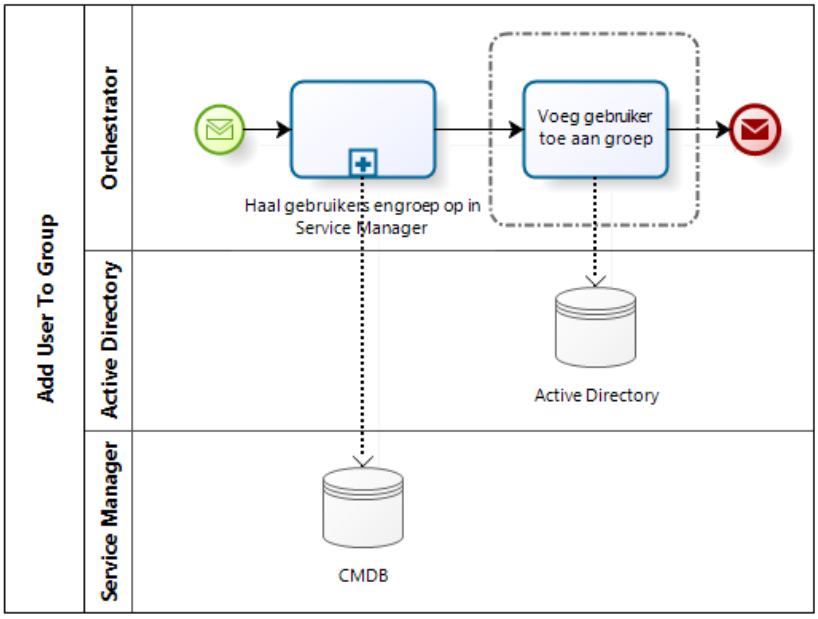
Parameter	Waarde
Gebruikers	Gebruikersna(a)m(en) van de aan de groep toe te voegen gebruiker(s)
Groep	De naam van de groep waar de gebruiker(s) lid van moeten worden

N.b.: zowel de groep als de gebruikers zullen in werkelijkheid niet direct worden meegegeven aan het uit te voeren Runbook, maar zullen worden gekoppeld aan het Service Request in Service Manager. Daarvandaan kunnen ze zonder problemen weer worden opgehaald door Orchestrator om vervolgens de acties uit te voeren.

Er zal één Runbook worden gemaakt waarmee zowel mutaties kunnen worden gedaan voor zowel “gewone” beveiligingsgroepen als distributiegroepen, maar ook indien lidmaatschap van de groep een extra

item voor op de factuur betekent. Indien het een beveiligingsgroep betreft voor een applicatie, dan zal er namelijk eerst een bevestiging worden gevraagd, zoals besproken in 7.1 Algemeen Service Request proces. Bij een gewone beveiligingsgroep of distributiegroep zal deze validatie niet hoeven plaats te vinden. Het verschil tussen een groep waarvoor moet worden betaald en waarvoor dat niet het geval is, wordt overigens gemaakt op basis van de locatie ervan in Active Directory.

Het proces verder is niet ingewikkeld:



Figuur 53 Runbook "Add user to group"

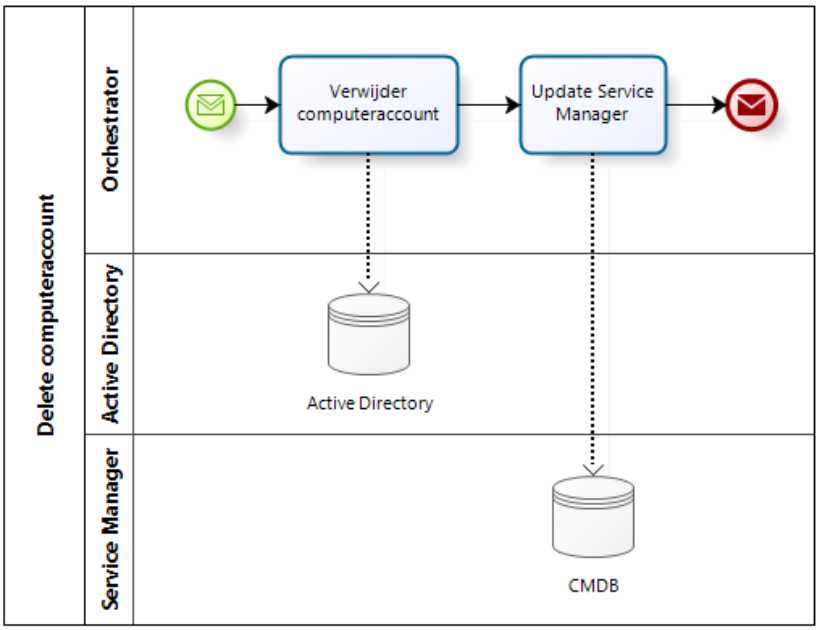
Eerst moeten de verschillende objecten worden opgehaald in Service Manager en vervolgens wordt er per gebruiker een actie uitgevoerd om deze lid te maken van de geselecteerde groep.

4.2.5. Computeraccount verwijderen

Het verwijderen van een computer account is soms nuttig vanwege het feit dat de klant betaald per gehuurde computer. Dit kunnen zowel laptops als desktops zijn. Mocht een computer niet opnieuw weer dienst gaan doen als werkplek, of een nieuwe naam krijgen, dan moet het oude computer object worden verwijderd uit Active Directory.

Parameter	Waarde
Computer	Naam van de computer die verwijderd moet worden.

Ook dit is weer een redelijk simpele handeling: het computeraccount moet opgezocht worden om deze vervolgens te verwijderen uit Active Directory. Vervolgens moet Service Manager ge-update worden om ervoor te zorgen dat het computeraccount niet meer beschikbaar is.



Figuur 54 Runbook "Delete Computeraccount"

4.2.6. Maak beveiligde map

Het aanmaken van een map bleek met Orchestrator kinderspel te zijn en standaard kan dit uiteraard ook via Verkenner op iedere werkplek waar de gebruiker rechten op heeft. Het maken van een beveiligde map is echter een stuk interessanter.

Om de rechten op een map overzichtelijk te houden, is het wenselijk om aan iedere beveiligde map alleen Active Directory groepen te koppelen welke vervolgens lees- of schrijfrechten krijgen. Als er dan personen uit dienst gaan en er komt iemand anders die dezelfde rechten moet krijgen, hoeven alleen de juiste Active Directory groepen gekoppeld te worden om dezelfde rechten te verkrijgen en daarnaast treedt er geen vervuiling op doordat de oude rechten van de gebruiker nooit worden verwijderd.

Doordat we vaak te maken hebben met personen die moeten kunnen schrijven, maar een andere groep personen die de gegevens in de

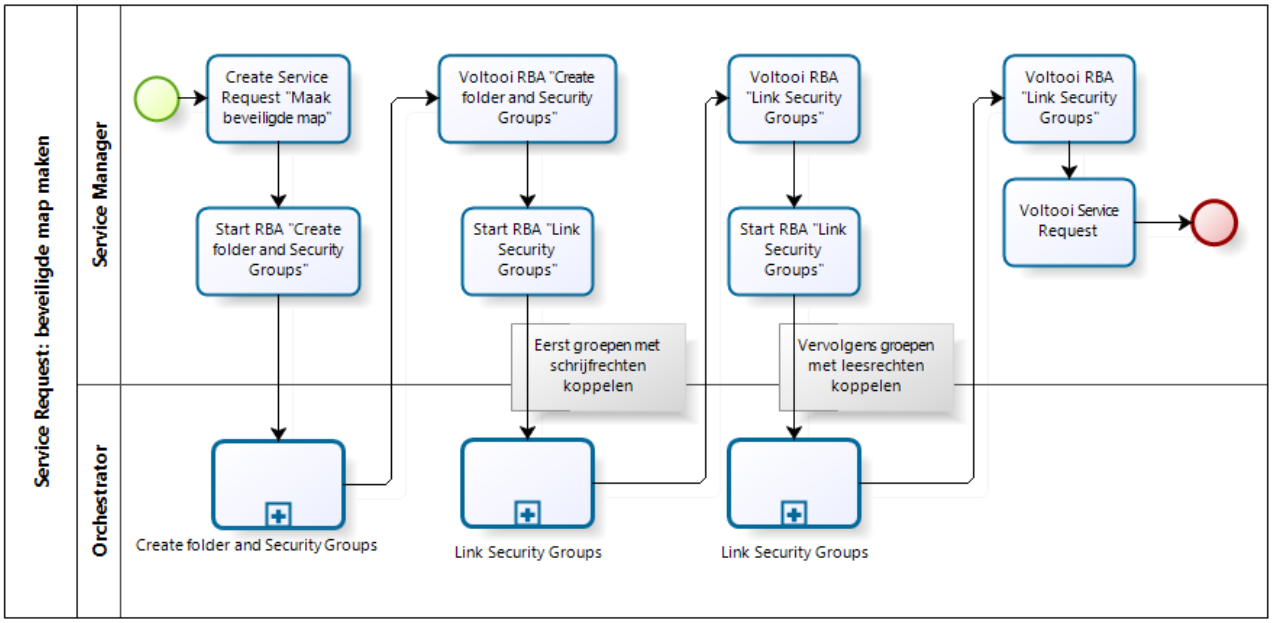
betreffende map alleen hoeft te lezen, zullen we standaard twee Active Directory groepen aanmaken die automatisch worden gekoppeld aan de nieuw aan te maken map: één groep met leesrechten, één met schrijfrechten. Deze groepen kunnen vervolgens in Active Directory gebruikt worden om voortaan de rechten in deze map te regelen.

De volgende gegevens zijn nodig om de map automatisch aan te kunnen maken:

Parameter	Waarde
Mapnaam	Naam van de map die aangemaakt moet worden
Locatie	De locatie waar de map zal moeten worden aangemaakt. Indien niets wordt meegegeven zal de groepsdata van de ingelogde gebruiker worden gebruikt.
Groep met leesrechten	De Active Directory beveiligingsgroep(en) en/of gebruiker(s) die lees rechten moet(en) krijgen op de map.
Groep met schrijfrechten	De Active Directory beveiligingsgroep(en) en/of gebruiker(s) die schrijf rechten moet(en) krijgen op de map.

4.2.6.1. Service Request “Beveiligde map aanmaken”

Doordat het wat lastig is om onderscheid te maken tussen groepen die lees- of schrijfrechten moeten krijgen, moet het standaard Service Request proces enigszins aangepast worden om de gewenste functionaliteit te krijgen. De stappen die nu in het Service Request gedaan moeten worden zijn als volgt:



Figuur 55 Service Request "Beveiligde map maken"

Er zijn drie runbooks die gedraaid moeten worden. Eerst moet de map worden aangemaakt, de bijbehorende Active Directory groepen aangemaakt worden (een aparte groep voor leesrechten en een aparte groep voor

schrijfrechten) en deze moeten vervolgens de juiste rechten krijgen op deze map.

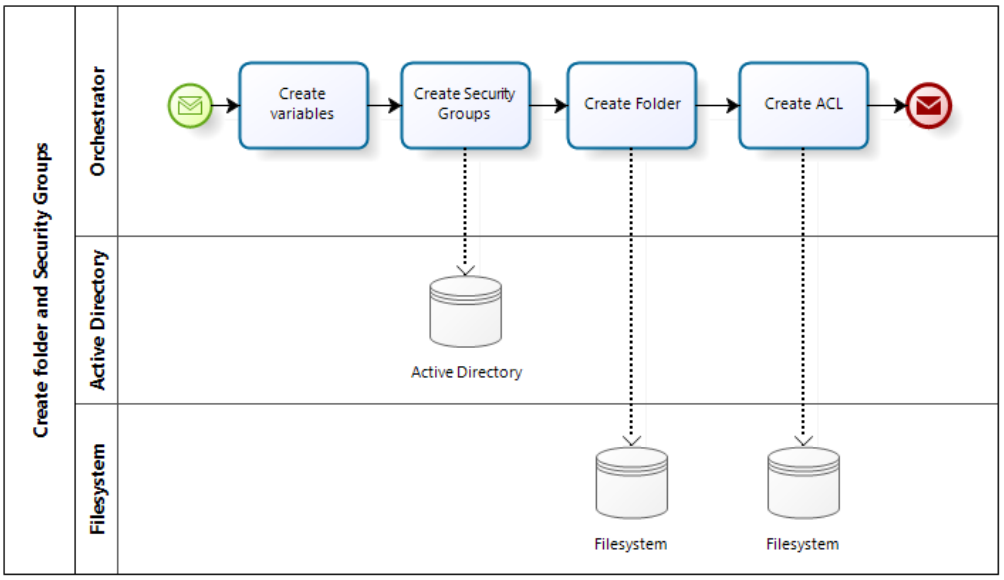
Daarna wordt twee keer hetzelfde runbook uitgevoerd, maar allebei met andere parameters. De eerste koppelt de opgegeven gebruiker(s) en Active Directory Security Groups aan de eerder aangemaakte groep die schrijfrechten heeft gekregen op de aangemaakte map. De tweede keer wordt dezelfde actie uitgevoerd, maar dan worden de gebruiker(s) en/of groep(en) aan de groep met leesrechten gekoppeld.

4.2.6.2. Runbook “Create Folder and Security Groups”

De parameters die nodig zijn voor dit runbook zijn als volgt:

Parameter	Waarde
Mapnaam	Naam van de map die aangemaakt moet worden
Locatie	De locatie waar de map zal moeten worden aangemaakt. Indien niets wordt meegegeven zal de groepsdata van de ingelogde gebruiker worden gebruikt.

Het runbook “Create Folder and Security Groups” ziet er als volgt uit:



Figuur 56 Runbook "Create folder and Security Groups"

Aan de hand van de aan te maken foldernaam worden er groepsnamen gemaakt in de activiteit “Create variables”. Die groepsnamen zullen er uit zien als:

- Leesrechten: BEDRIJF_DATA_FOLDERNAME_READ_ACCESS
- Schrijfrechten: BEDRIJF_DATA_FOLDERNAME_WRITE_ACCESS

Speciale tekens moeten eruit gefilterd worden, zodat zowel de bovengenoemde beveiligingsgroepen en de aan te maken map zonder problemen aangemaakt kunnen worden: tekens zoals / \ * ? < > | worden bijvoorbeeld niet toegestaan bij het aanmaken van een map.

Vervolgens worden de groepen aangemaakt, de map aangemaakt op de opgegeven locatie en wordt de toegang geregeld door een Access Control List op te bouwen en deze te koppelen aan de gemaakte map. Een Access Control List is een lijst van groepen en de bijbehorende rechten van deze groepen, welke d.m.v. PowerShell gemakkelijk toegepast kan worden op een map.

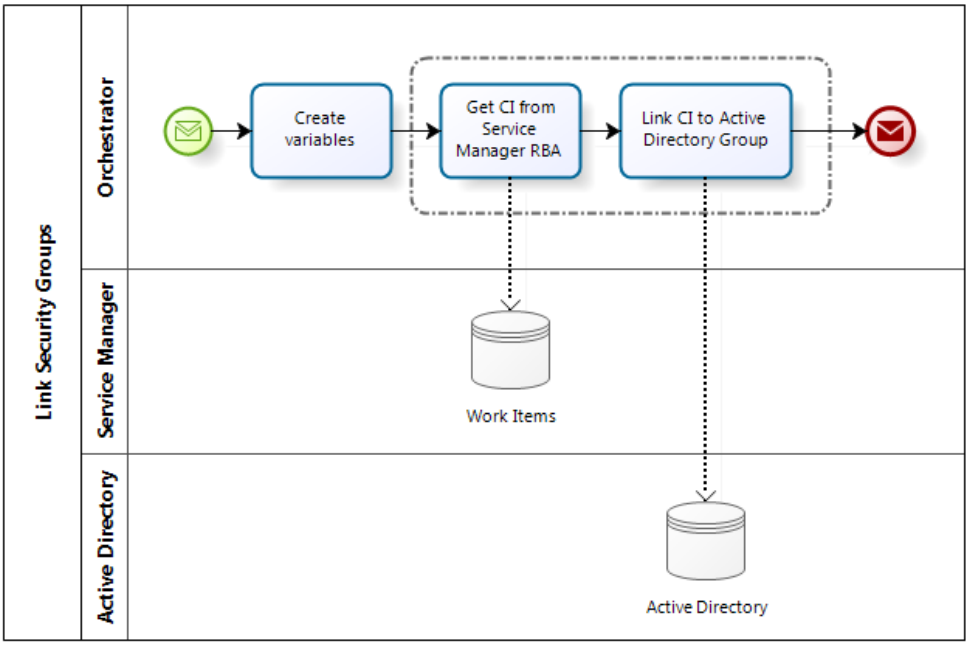
4.2.6.3. Runbook "Link Security Groups"

De parameters die nodig zijn voor dit runbook zijn als volgt:

Parameter	Waarde
Groep personen of groepen	De Active Directory beveiligingsgroep(en) en/of gebruiker(s) die lees rechten moet(en) krijgen op de map.
Welk type rechten	Lees- of schrijfrechten

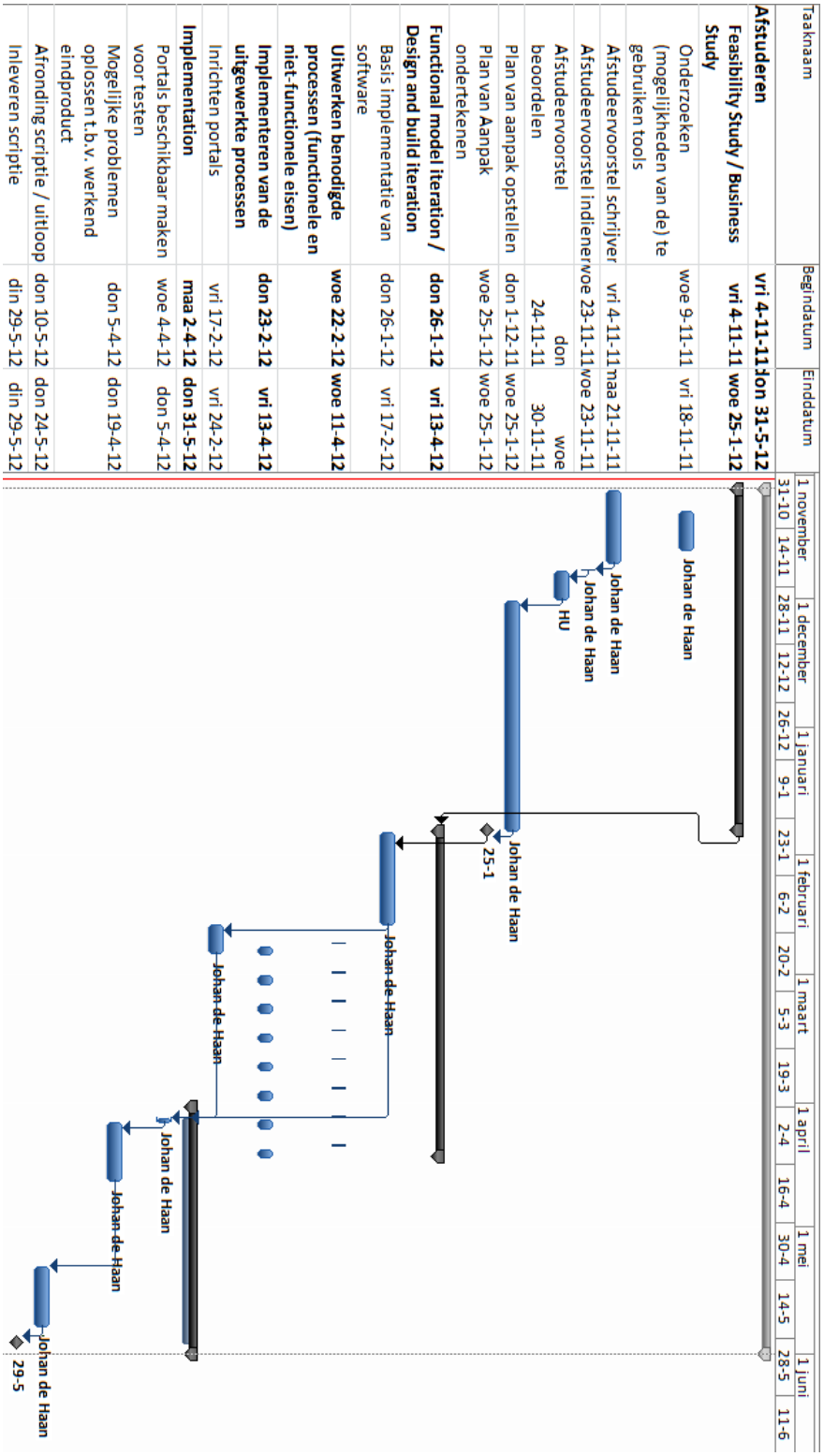
Bij het aanmaken van het Service Request kunnen er twee typen groepen items worden geselecteerd: één groep die leesrechten krijgt en één groep die schrijfrechten krijgt. Dit kunnen zowel Active Directory groepen zijn als gebruikersaccounts.

Met een slim trucje wordt de goede groep van Configuration Items opgehaald in Service Manager: de groep met leesrechten om te koppelen aan de "data lees" groep en de groep met schrijfrechten om deze te koppelen aan de "data schrijf" groep.

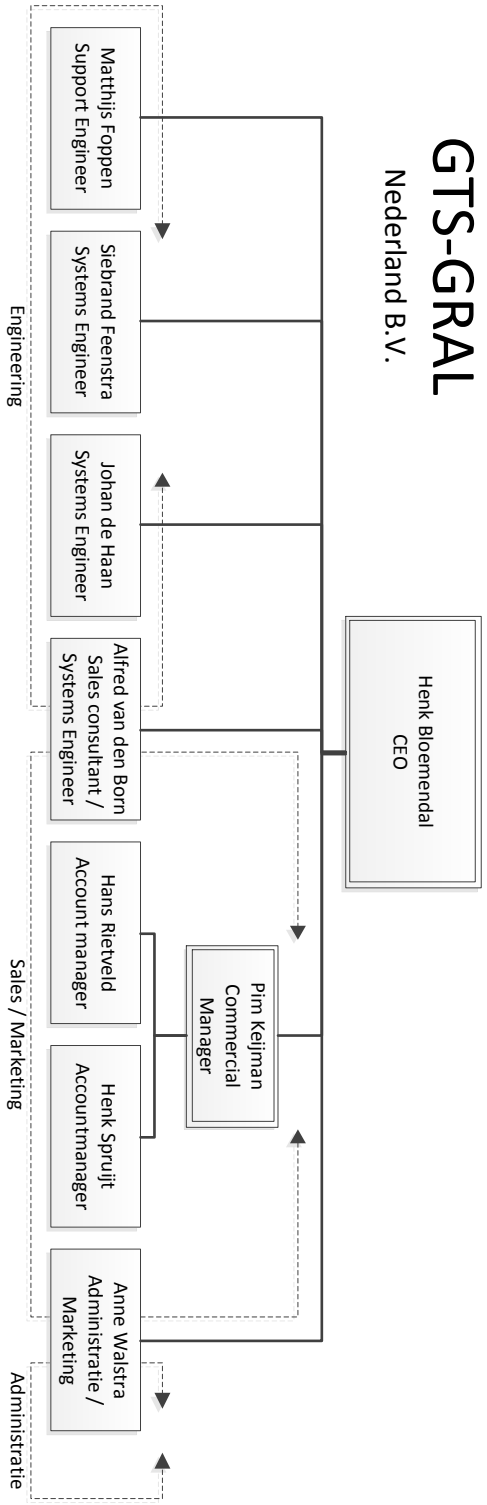


Figuur 57 Runbook "Link Security Groups"

Bijlage 3: Planning (Gantt diagram)



Bijlage 4: Organigram GTS-GRAL



Bijlage 5: Installatiebeschrijving System Center producten

Software

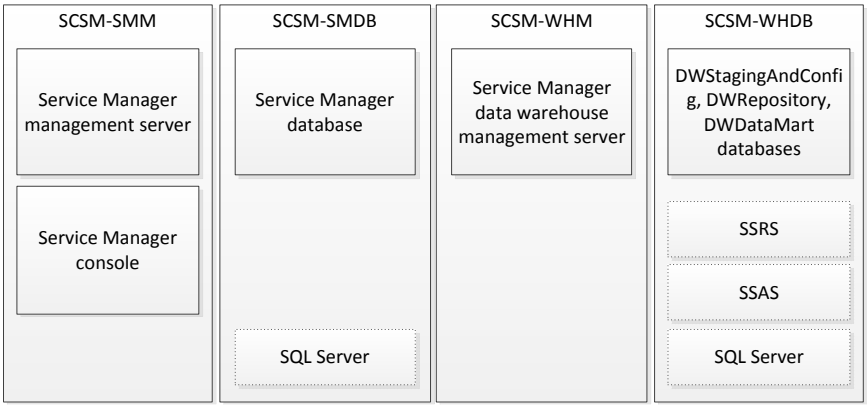
De software voor zowel System Center Service Manager 2012 (Service Manager) als die voor System Center Orchestrator 2012 (Orchestrator) zijn onderdeel geworden van de zogeheten Microsoft Private Cloud. De software voor deze Microsoft Private Cloud is vrij te downloaden[10] en als trial te gebruiken. Na 180 dagen wordt een licentie vereist om de software te blijven gebruiken.

System Center 2012 Service Manager

Voor het installeren van Service Manager zijn nog niet erg uitgebreide installatie handleidingen beschikbaar. Dat komt omdat van de laatste versie van Service Manager 2012 op het moment van schrijven nog maar een aantal weken een eerste Release Candidate (RC) beschikbaar is. Deze RC wordt ook ondersteund door Microsoft om in een productieomgeving te gebruiken[11].

Onderdelen van Service Manager

Om System Center Service Manager zo schaalbaar mogelijk te installeren wordt door Microsoft aanbevolen[12] de verschillende onderdelen van Service Manager op vier verschillende servers te installeren.



Figuur 58 Onderdelen van Service Manager

Zoals te zien is in bovenstaande figuur, moeten er twee database servers worden geïnstalleerd één voor Service Manager en één voor de Data Warehouse databases. Op de server met de Datawarehouse databases dienen ook de SQL Server Reporting Services (SSRS) en SQL Server Analysis Services (SSAS) worden geïnstalleerd. Verder zijn er nog twee management

[10] http://technet.microsoft.com/nl-nl/evalcenter/hh505660.aspx
[11] http://technet.microsoft.com/en-us/library/hh495600.aspx
[12] http://technet.microsoft.com/en-us/library/hh495582.aspx

servers nodig om de communicatie tussen de databases en het aanleveren van de gegevens uit de databases mogelijk te maken.

Minimaal twee servers

Het is wel mogelijk om Service Manager werkend te krijgen op minder systemen (minimaal twee servers), maar het is minimaal vereist dat de data warehouse management server en de Service Manager management server gescheiden worden geïnstalleerd. De bijbehorende databases zullen dan op deze beide servers geïnstalleerd worden[13]. Deze configuratie wordt door Microsoft niet aangeraden voor in een productieomgeving, maar alleen om de software te testen en te evalueren. Door deze op vier separate servers te installeren is de configuratie veel beter te schalen voor betere performance bij het groeien naar een grotere omgeving.

Gescheiden SQL Servers

Verder is het natuurlijk mogelijk om bijvoorbeeld de Service Manager database op een van de andere SQL Servers in de GTS-Online omgeving te installeren. Mocht er echter wat aan de hand zijn met zo'n SQL server dan is het wenselijk dat ook op zo'n moment een incident aangemaakt kan worden en Service Manager online is. Om dat risico te voorkomen is er voor gekozen om een aparte SQL Server te installeren voor zowel de Service Manager database als de Service manager data warehouse databases.

Self Service Portal

De Self Service Portal behoeft niet perse op een aparte server te worden geïnstalleerd. Dat komt omdat de Self Service Portal bestaat uit een aantal webparts die gebruikt kunnen worden in een al bestaande Sharepoint 2010 omgeving.

Webparts zijn kleine bouwstenen die gebruikt kunnen worden in bijna iedere Sharepoint pagina en gemaakt zijn in de programmeertaal ASP.NET. Een webpart staat dus los van de Sharepoint omgeving en kan dus gemakkelijk toegevoegd, verwijderd, maar ook bewerkt worden. Bij een update van zo'n webpart hoeft dat slechts eenmalig te gebeuren, waarna op alle plekken waar de webpart gebruikt is de webpart is bijgewerkt.

System Requirements

De complete GTS-Online omgeving is geïnstalleerd onder Microsoft Hyper-V[14]. Hyper-V is het virtualisatieplatform van Microsoft waardoor er meerdere virtuele besturingssystemen naast elkaar geïnstalleerd kunnen worden op één fysieke server en ze tegelijkertijd kunnen draaien.

Het installeren van Service Manager is geen probleem in een Hyper-V omgeving. Wel zijn er een aantal aanbevelingen gedaan, vooral voor het installeren van SQL Server in deze virtuele omgeving. Ook deze zaken zijn netjes gedocumenteerd op Microsoft Technet en zal ik dus niet dieper op in gaan, mede aangezien iedere omgeving verschillend is.

De verschillende Virtual Machines (VM) die onder Hyper-V zullen worden geïnstalleerd, hebben als besturingssysteem Windows Server 2008 R2 SP1.

[13] http://technet.microsoft.com/nl-nl/library/hh495485(en-us).aspx
[14] http://www.microsoft.com/nl-nl/Server-Cloud/windows-server/hyper-v.aspx

Daarnaast zijn voor een aantal onderdelen nog andere software pakketten benodigd, zoals .NET Framework, SQL Server of Windows Powershell. Een handig overzicht van de benodigde software[15] is hieronder weergegeven:

Onderdeel	Benodigde software
Voor alle onderdelen is deze software benodigd:	Microsoft Server 2008 R2 met SP1 Microsoft .NET Framework 3.5 with SP1 ADO.NET Data Services Update for .NET Framework 3.5 SP1 Windows PowerShell 2.0 Microsoft Report Viewer Redistributable
Database Servers	64-bit versie van SQL Server 2008 met SP1, SP2 of versie 2008 R2 SQL Server Reporting Services (alleen Datawarehouse Server) SQL Server Analysis Services (alleen Datawarehouse Server)
Self Service Portal	IIS 7.5 with IIS 6 metabase compatibility geïnstalleerd Self-signed SSL certificaat ASP.NET 2.0 Microsoft .NET Framework 4.0 Microsoft Analysis Management Objects Microsoft SharePoint Foundation 2010 Of Microsoft SharePoint Server 2010 Of Microsoft SharePoint 2010 for Internet Sites Enterprise Excel Services in SharePoint 2010 is nodig voor bepaalde rapportage.
Service Manager Console	32-bit of 64-bit edition van Windows Server 2008 met SP2 Windows Server 2008 R2 met SP1 Windows Server 2003 R2 met SP2 Windows 7 Professional of Windows 7 Ultimate Windows Vista Enterprise or Ultimate met SP2 Windows Powershell 1.0 of hoger Microsoft Report Viewer Redistributable Microsoft .NET Framework 3.5 met SP1 ADO.NET Data Services Update for .NET Framework 3.5 SP1
Browser waarmee de Self Service Portal geopend wordt.	Internet Explorer 8 of hoger Silverlight 4.0 of hoger

Hardware configuratie

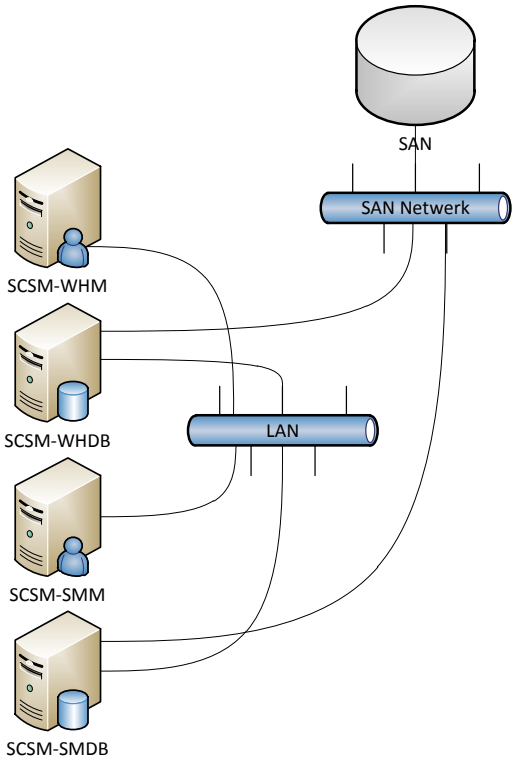
De aanbevelingen over het gebruik van de (virtuele) hardware liggen tussen de 1 á 2 processoren, 8GB RAM (behalve de Service Manager Console die met 2GB RAM uit de voeten kan) en 10 tot 400GB aan benodigde vrije ruimte

[15] Tabel grotendeels overgenomen van: http://www.petri.co.il/system-center-service-manager-2012-installation-requirements.htm

op de harde schijf. Specifieke configuratie per onderdeel staat uitgebreid beschreven[16] op Microsoft Technet.

De vier servers zijn allemaal in Hyper-V geconfigureerd. Iedere machine heeft initieel o.a. een 40GB hard disk gekregen, een viertal CPU's en in ieder geval één netwerkkaart. Verder hebben de database servers meerdere hard disks (volumes) direct op het SAN (Storage Area Network[17]) middels iSCSI[18], waarvoor twee extra netwerkkaarten zij geconfigureerd op deze machines.

In onderstaande figuur is op abstracte wijze weergegeven hoe de netwerkconfiguratie is.



Figuur 59

Duidelijk is dat het LAN en SAN netwerk compleet gescheiden zijn. In werkelijkheid heeft iedere server die één of meerdere volumes direct van het SAN gebruikt twee netwerkverbindingen naar het SAN, maar voor de overzichtelijkheid zijn deze verbindingen weggelaten in bovenstaande figuur.

System Center 2012 Orchestrator

Net als voor Service Manager is op het moment van schrijven slechts een Release Candidate beschikbaar van System Center 2012 Orchestrator (verder te noemen Orchestrator). Het is zeer waarschijnlijk dat deze Release Candidate zonder problemen bij het uitkomen van de definitieve versie ge-update kan worden, maar hierover heb ik geen toezeggingen kunnen vinden.

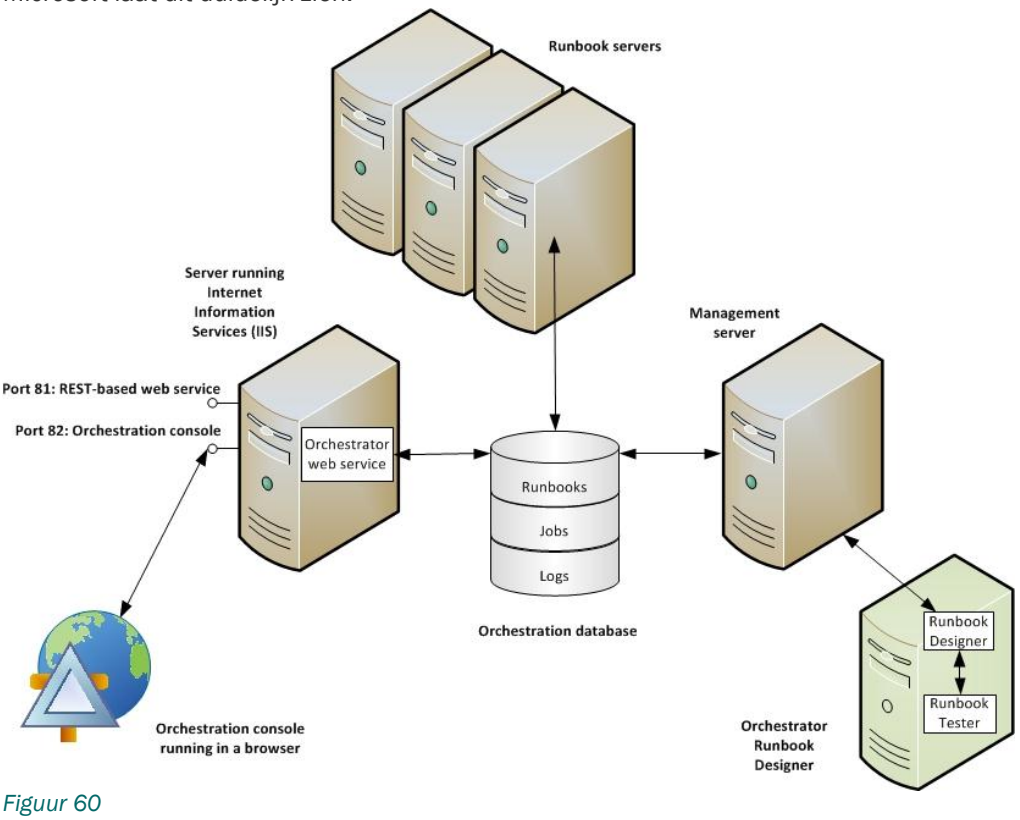
[16] http://technet.microsoft.com/nl-nl/library/hh524328(en-us).aspx
[17] http://nl.wikipedia.org/wiki/Storage_area_network
[18] http://nl.wikipedia.org/wiki/ISCSI

De belangrijkste informatie in Orchestrator, de zogeheten runbooks, zijn echter redelijk universeel en zouden dus, indien nodig, gemakkelijk over te zetten moeten zijn naar een andere omgeving.

Een runbooks is in wezen een workflow van activiteiten die in een opgegeven volgorde moeten doorlopen worden, waarbij gegevens van de ene activiteit naar een volgende kunnen worden doorgegeven. De activiteiten die uitgevoerd kunnen worden middels System Center Orchestrator zijn flink uit te breiden doordat er steeds meer zogeheten Integration Packs beschikbaar komen. Met deze Integration Packs kan gemakkelijk worden gecommuniceerd met andere Microsoft en niet-Microsoft producten, zoals bijvoorbeeld de andere System Center pakketten en VMware vSphere.

Onderdelen van Orchestrator

Orchestrator bestaat uit een aantal verschillende onderdelen die bijna allemaal direct in verbinding staan met de database. Alleen de Runbook Designer en Runbook Tester tools maken verbinding met de Management server en niet direct met de database.
De volgende afbeelding die te vinden is op de TechNet website[19] van Microsoft laat dit duidelijk zien:



Figuur 60

In de database zit alle relevante informatie opgeslagen over de gemaakte runbooks, verdere configuratie en logbestanden. De runbooks worden gemaakt en getest met de Orchestrator Runbook Designer, die communiceren met de database via de management server.

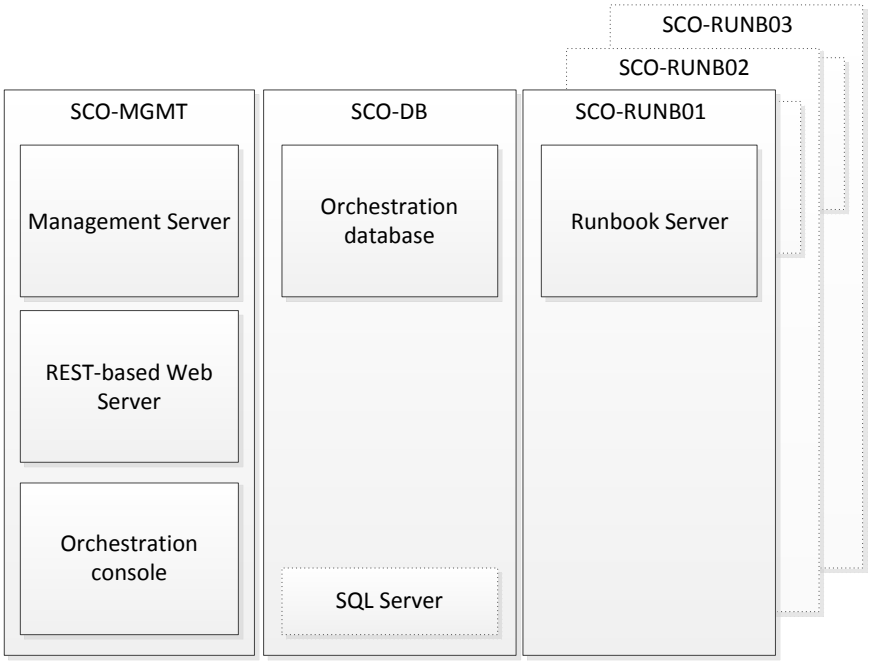
[19] http://technet.microsoft.com/en-us/library/hh420377.aspx

Verder kunnen er één of meerdere runbook servers gebruikt worden om de gemaakte runbooks uit te voeren. Hoe meer runbooks er tegelijkertijd moeten worden uitgevoerd, hoe verder dit moet worden opgeschaald.

Daarnaast draait er nog een Orchestrator web service waarmee alle informatie over de runbooks opgehaald kan worden en runbooks gestart en gestopt mee kunnen worden. Deze op REST (Representational State Transfer) gebaseerde web service haalt deze informatie op uit de database. Dit laatste is belangrijk: de status van de runbook servers kan alleen actueel worden opgehaald via de web service als de runbook server voldoende capaciteit heeft om zijn status netjes bij te houden in de database. Een gevolg is ook dat er enige vertraging is bij het communiceren tussen de web service en de Runbook servers.

Verder is het mogelijk een Orchestration console te draaien waardoor toegang mogelijk is via een webinterface en alle informatie die beschikbaar is over de runbooks via de web service opgevraagd kan worden.

Het is mogelijk om alle onderdelen van Orchestrator op één server te installeren. Voor de schaalbaarheid en betrouwbaarheid van de omgeving zullen we er echter voor kiezen om een losse database server te installeren en één losse runbook server. Op deze manier kan het aantal runbook servers gemakkelijk opgeschaald worden indien nodig. Initieel zullen we dus 3 servers installeren, zoals in onderstaande afbeelding is weergegeven.



Figuur 61 Verdeling van onderdelen van Orchestrator binnen onze omgeving

Wat in bovenstaande figuur niet is opgenomen, is de tool Runbook Designer. Dat is namelijk geen vereiste voor een werkende Orchestrator omgeving, maar wel nodig om de Runbooks te ontwikkelen en zo nodig te testen.

System Requirements

Voor ieder onderdeel is via TechNet[20] een overzicht beschikbaar van wat voor software en hardware eisen zijn voor de verschillende onderdelen van Orchestrator:

Onderdeel	Benodigde software
Voor alle onderdelen is deze software benodigd:	Microsoft Server 2008 R2 Microsoft .NET Framework 3.5 with SP1
Orchestrator database server	64-bit versie van SQL Server 2008 met SP1, SP2 of versie 2008 R2
Orchestrator web service	Internet Information Services (IIS) 7.0 Microsoft .NET Framework 4
Browser waarmee de Orchestrator console geopend wordt.	Silverlight 4.0 of hoger
Runbook designer	Kan ook op Windows 7 geïnstalleerd worden

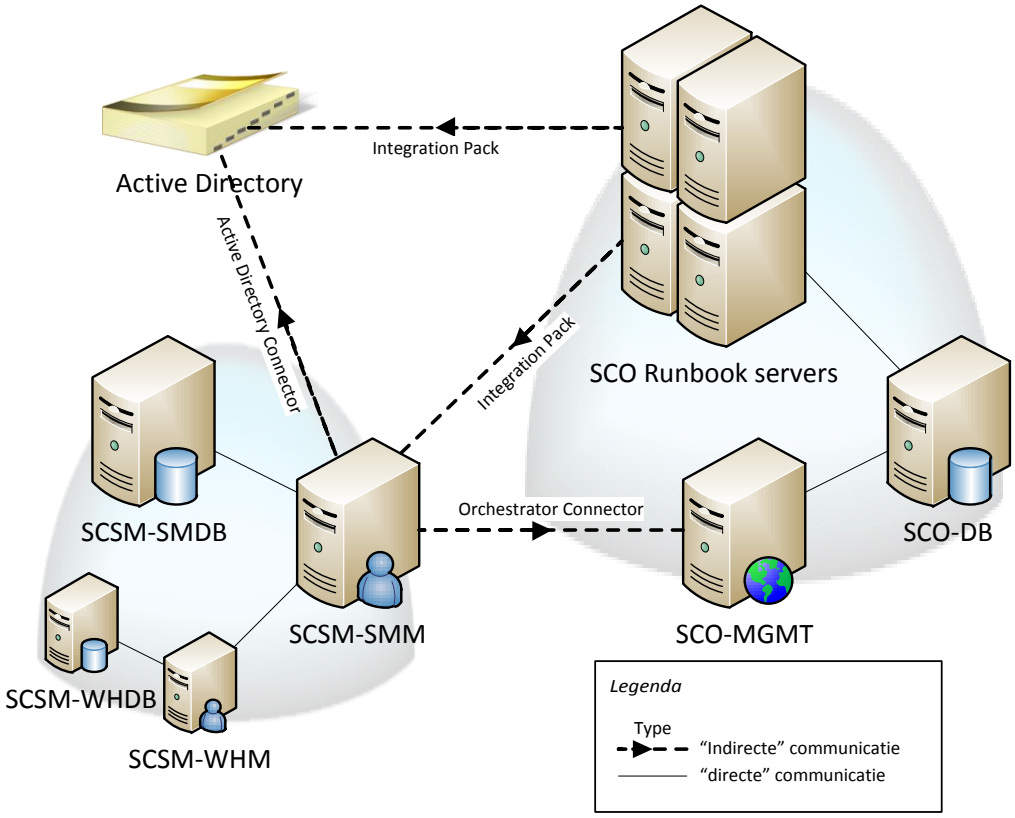
Verder is er voor ieder onderdeel ongeveer hetzelfde aan hardware vereist: minimaal 1GB (bij voorkeur 2GB) aan RAM, minimaal 200 MB vrij om de software te kunnen installeren en minstens een dual core processor met meer dan 2.1 GHz.

[20] http://technet.microsoft.com/en-us/library/hh420376.aspx

Integratie tussen Service Manager, Orchestrator en Active Directory

De integratie van Service Manager en Orchestrator werkt voor beide pakketten anders. Zo werkt Orchestrator met Integration packs die voor diverse pakketten (niet alleen andere pakketten in de System Center reeks, maar ook voor oplossingen van VMware, HP en IBM Tivoli) beschikbaar zijn en vanuit Service Manager wordt de koppeling gelegd met een ingebouwde connector.

De verbindingen die voor dit project van belang zijn, zijn in onderstaande afbeelding weergegeven:



Figuur 62 Communicatie tussen Orchestrator, Service Manager en Active Directory

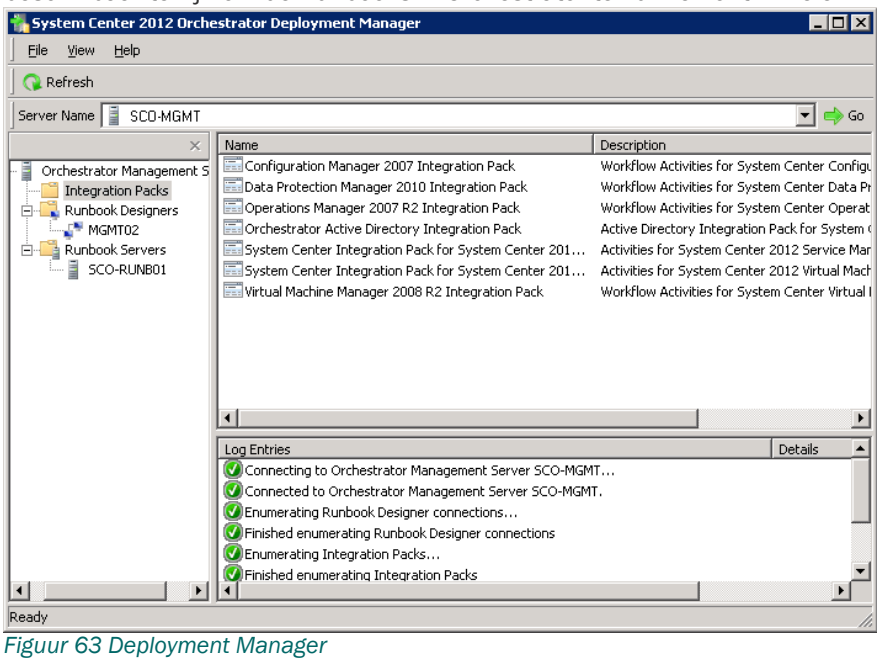
Van bovenstaande afbeeldingen zullen de hierboven weergegeven 'indirecte communicatie' lijnen uitgebreid worden besproken.

Orchestrator: Integration Packs

In Orchestrator wordt gebruik gemaakt van zogeheten Integration Packs, die niet alleen voor de nieuwste versie van Service Manager beschikbaar is. Zo bestaan er integration packs voor ieder System Center product dat op dit moment nog ondersteund wordt[21], maar ook voor bijvoorbeeld Active Directory, diverse HP pakketten, bepaalde onderdelen van IBM en VMware vSphere[22]. In deze integration packs zitten voor gedefinieerde activiteiten waarmee deze producten beheerd en geautomatiseerd kunnen worden.

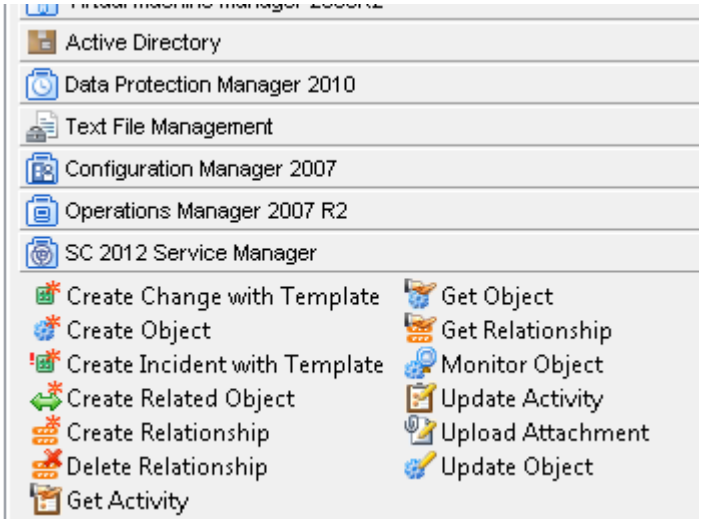
[21] http://technet.microsoft.com/en-us/library/hh830706.aspx
[22] http://technet.microsoft.com/en-us/library/hh295851.aspx

Deze integration packs kunnen worden geïmporteerd op de Management server met de daarop geïnstalleerde tool “Deployment Manager”. Met de Deployment Manager kunnen Integration Packs worden geïnstalleerd en vervolgens gedistribueerd naar de verschillende Runbook Servers. Daarnaast dient er een kopie van ieder Integration Pack op de Runbook Designer server beschikbaar te zijn om de Runbooks in Orchestrator te kunnen ontwikkelen.



Figuur 63 Deployment Manager

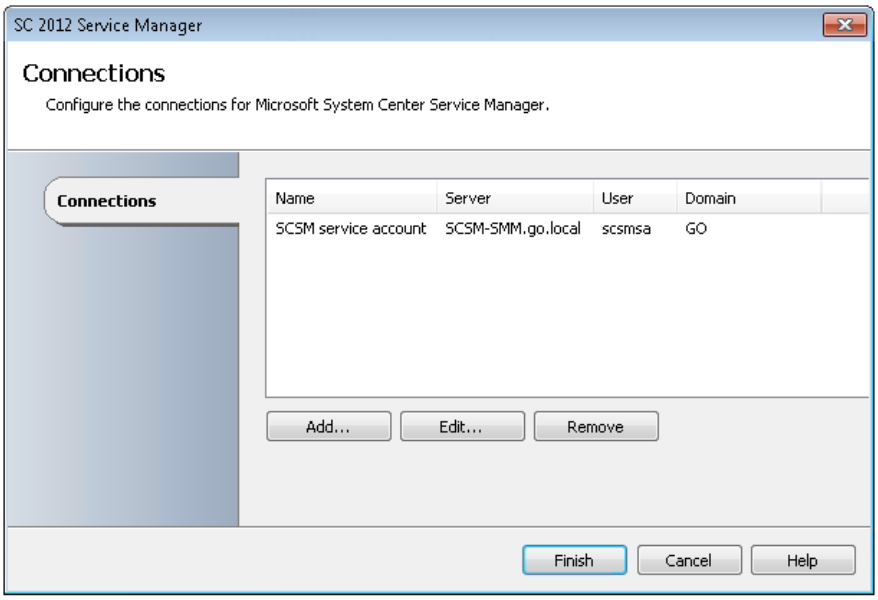
Nadat zo’n Integration Pack is geïnstalleerd komen er diverse standaard activiteiten beschikbaar die voor het gelijknamige pakket kunnen worden gebruikt.



Figuur 64 Integration pack “SC 2012 Service Manager”

In bovenstaande figuur zijn de activiteiten weergegeven die op dit moment in het Integration pack voor Service Manager zijn opgenomen. Voor deze activiteiten gebruikt kunnen worden, moet er wel eerst een verbinding

worden opgezet met de Service Manager Management Server. Eventueel kunnen er meerdere verbindingen worden gedefinieerd, maar dat is ons geval niet nodig.

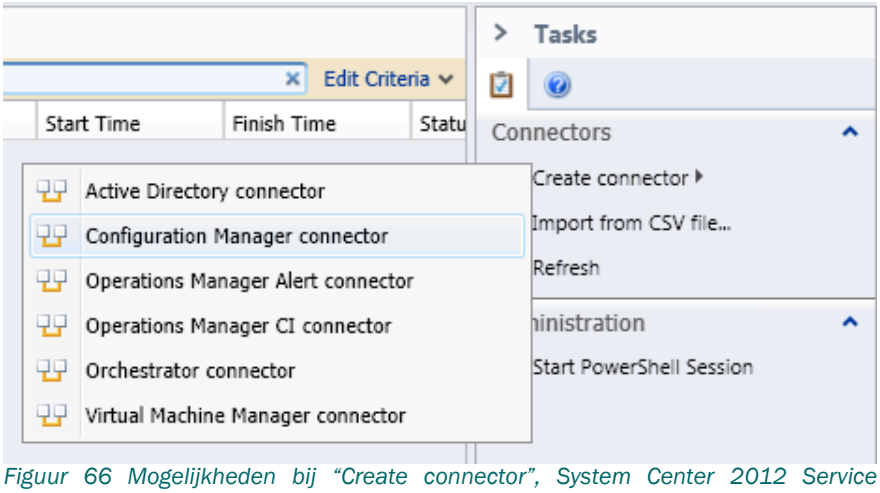


Figuur 65 Verbindingen voor het "SC 2012 Service Manager" Integration Pack

Bij het gebruiken van een activiteit uit een Integration Pack moet altijd een Verbinding te worden opgegeven waarvan gebruik gemaakt moet worden.

Service Manager: Connectors

In Service Manager werkt de interactie met andere pakketten met zogeheten "Connectors". Een aantal hiervan zit al ingebouwd in Service Manager, waaronder de "Active Directory connector" en de "Orchestrator connector" die ik in eerste instantie zal moeten gebruiken.



Figuur 66 Mogelijkheden bij "Create connector", System Center 2012 Service Manager

Orchestrator connector

De verbinding vanuit Service Manager naar Orchestrator is tweeledig: met een Orchestrator Connector kunnen de beschikbare Automation Runbooks

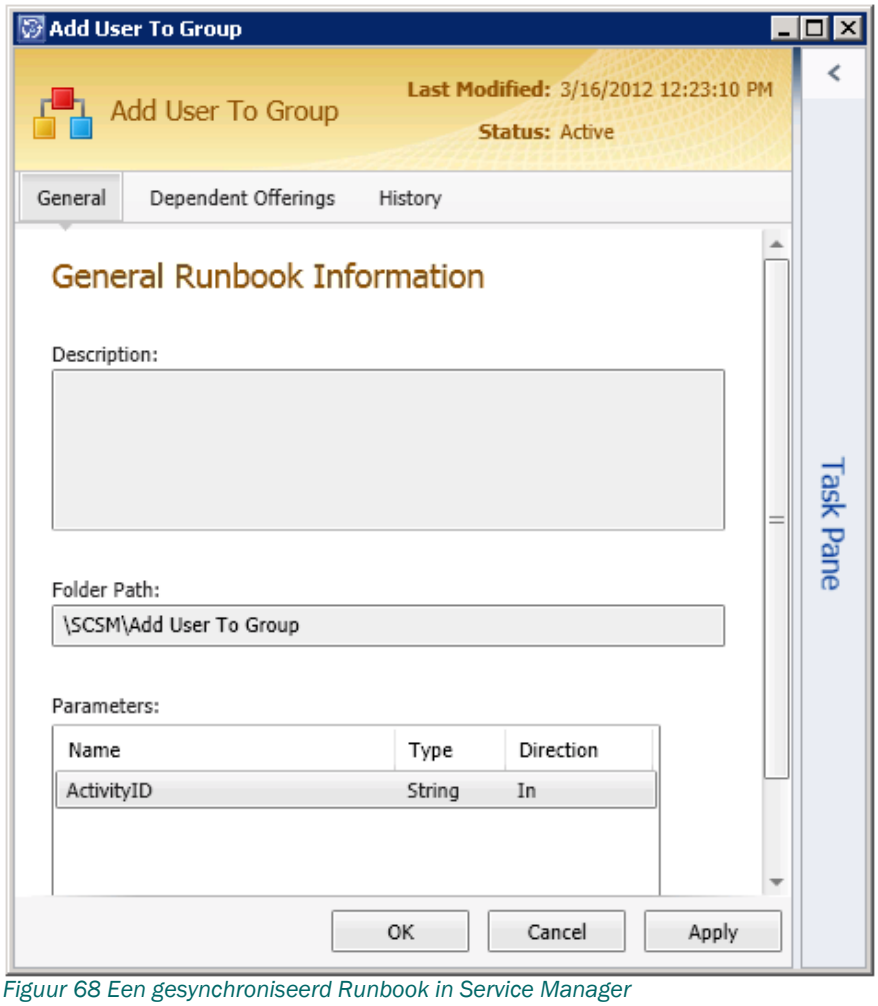
worden geïmporteerd in Service Manager. Deze kunnen vervolgens worden gebruikt in Service Requests in de vorm van zogeheten “Automation Runbook Activities”. Als zo’n Automation Runbook Activity wordt gestart, wordt het bijbehorende runbook geïnitieerd op de Orchestrator Web Service.

De Connector voor Orchestrator zit standaard ingebouwd en hoeft dus niet te worden geïnstalleerd. Het enige wat nodig is om de verbinding te leggen is het invoeren van de juiste URL’s naar de Orchestrator Web Service en Web Console en het account waarmee de gegevens opgehaald dienen te worden. Verder kan eventueel worden opgegeven van welke map de inhoud moet worden gesynchroniseerd.

Figuur 67 Configureren van de Orchestrator Connector

Als de Connectie werkt, worden automatisch de Runbooks en de bijbehorende gegevens geïmporteerd. Als er wijzigingen worden doorgevoerd in het Runbook worden deze voor zover mogelijk automatisch bijgewerkt, maar in de praktijk blijkt dit nog wel eens tegen te vallen.

Zo worden de Parameters die aan een Runbook kunnen worden meegegeven wel automatisch toegevoegd bij de eerste synchronisatie. Maar als hier later wijzigingen in worden gedaan (bijvoorbeeld een extra Input of Output parameter, of juist één minder), dan geeft dit regelmatig problemen en moet het runbook opnieuw worden aangemaakt om deze vervolgens goed te kunnen synchroniseren.



Figuur 68 Een gesynchroniseerd Runbook in Service Manager

Exchange connector

Op het moment van schrijven is er ook een nieuwe Exchange connector in de maak, welke ondersteuning biedt voor System Center 2012 Service Manager, want de huidige (versie 2) werkt niet met deze laatste versie[23]. Wanneer deze beschikbaar komt is op dit moment nog afwachten, maar is wel nodig om in onze omgeving bepaalde functionaliteit werkend te krijgen.

Zo kunnen niet alleen incidenten worden aangemeld worden via de e-mail, maar ook wijzigingen (d.m.v. service- en change requests) bevestigd worden via de e-mail. Dit laatste kan op dit moment alleen via de Service Manager Console waarop we op dit moment de gebruikers in onze omgeving liever geen toegang toe willen geven (i.v.m. de multi tenant omgeving, waardoor het makkelijk mogelijk is dat klanten elkaars gegevens kunnen inzien).

Custom workflow & klasse uitbreiding

Om in Active Directory de objecten van de verschillende klanten in te kunnen scheiden gebruiken we het attribuut “extensionAttribute1” op ieder relevant

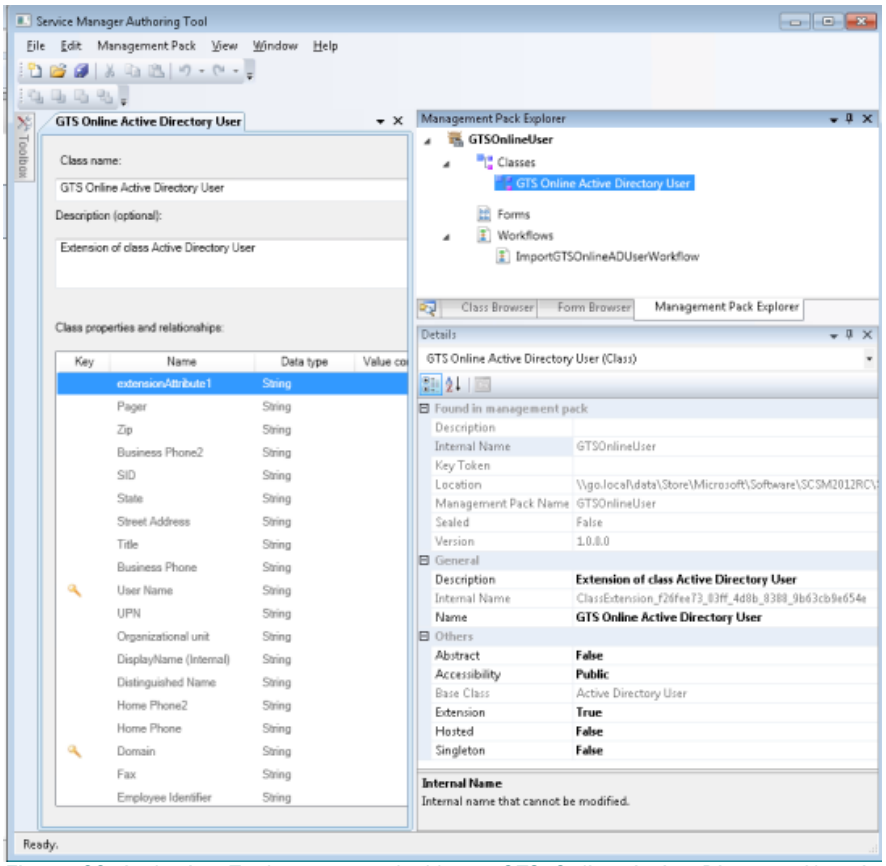
[23] http://blogs.technet.com/b/servicemanager/archive/2011/10/30/scsm-2012-public-beta-released.aspx

object in Active Directory om gegevens te kunnen scheiden. Voor de klant GTS-GRAL hebben alle gebruikersaccounts een “extensionAttribute1” met als waarde “GTS-GRAL”. Op dezelfde manier hebben al onze klanten een unieke waarde in die “extensionAttribute1” die niet alleen aan gebruikersaccounts, maar ook aan Computers, Beveiligingsgroepen en andere objecten in Active Directory gekoppeld kan worden.

In Service Manager willen de objecten, zogeheten Configuration Items, ook graag scheiden met datzelfde “extensionAttribute1”. In Service Manager worden Configuration Items aangemaakt op basis van voor gedefinieerde klassen en in deze standaard klassen bestaat die “extensionAttribute1” echter niet. Hiervoor heb ik dus een aantal aanpassingen moeten doen.

Service Manager Authoring Tool

Alle gebruikers die worden geïmporteerd met de Active Directory Connector worden aangemaakt op basis van de klasse ‘Active Directory User”. Deze klassen kunnen zelf niet uitgebreid worden, maar een andere klasse kan wel op basis aangemaakt worden en vervolgens zelf uitgebreid worden. Zo heb ik om de extensionAttribute1 te koppelen aan iedere gebruiker de klasse “Active Directory User” uitgebreid door gebruik te maken van de daarvoor beschikbare tool “System Center Service Manager Authoring Tool”[24].



Figuur 69 Authoring Tool waarmee de klasse GTS Online Active Directory User is gemaakt

[24] http://www.microsoft.com/Download/en/details.aspx?id=28726

Deze “extensionAttribute1” kan niet automatisch worden gesynchroniseerd door gebruik te maken van de “Active Directory Connector”. Er moest dus een andere manier worden verzonnen om deze waardes te kunnen synchroniseren.

Hiervoor heb ik ook gebruik gemaakt van de Authoring Tool door een eigen Workflow aan te maken. Een Workflow kan niet via de Service Manager Console aangemaakt, gewijzigd of verwijderd worden, maar alleen via de Authoring Tool. Een Workflow kan alleen in- of uitgeschakeld worden via de Console. Workflows binnen Service Manager zijn eigenlijk gewoon geplande taken die één of meerdere taken achter elkaar (vandaar de naam Workflow) uitvoeren.

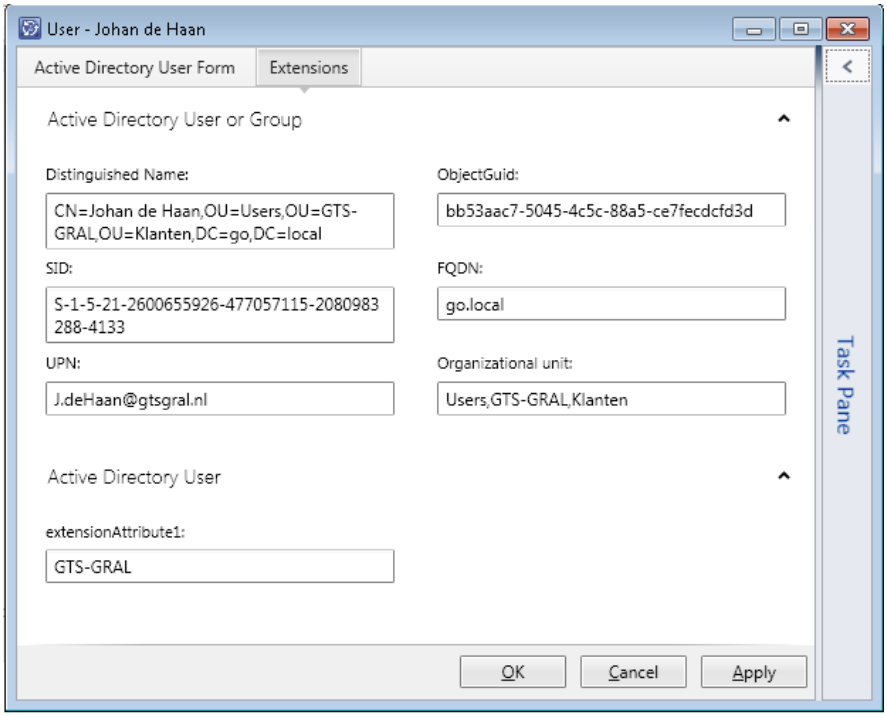
De workflow die ik gemaakt heb om het attribuut extensionAttribute te vullen in Service Manager, op basis van deze[25] blogpost van Microsoft, voert iedere nacht het onderstaande PowerShell script uit. Daarmee worden alle objecten opgehaald uit Active Directory die in de categorie “person” vallen. Van deze objecten worden vervolgens het domein, SAMAccountname en extensionAttribute weggeschreven in een CSV die gebruikt wordt om de data te importeren in Service Manager.

```
# Om later gebruik te kunnen maken van Import-SCSMInstance dient eerst de benodigde snap
in geladen worden
Add-PSSnapin smcmdletsnapin

# Om de objecten uit Active Directory op te halen moet de module ActiveDirectory geladen
worden.
import-module ActiveDirectory

# Alle objecten met de objectCategory “person” worden opgehaald en met alleen de
properties SAMAccountName, en extensionAttribute in een object 'OutputData' geplaatst.
Get-ADObject -Filter 'objectCategory -eq "person"' -SearchBase
'OU=Klanten,DC=GO,DC=LOCAL' -Properties CanonicalName, SAMAccountName,
extensionAttribute1 | Select-Object -property @{Name="Domain";Expression={"GO"}},
SAMAccountName, extensionAttribute1 | ConvertTo-CSV -NoTypeInformation -OutVariable
OutputData

# De inhoud van de variable ‘OutputData’ wordt uitgelezen en in een CSV bestand
opgeslagen.
$OutputData[1..($OutputData.Count-1)]|ForEach-Object {Add-Content -Value $_ -Path
"C:\Software\CSV\Users.csv"}

# Met onderstaande commando wordt de CSV ingelezen in Service Manager
Import-SCSMInstance -DataFileName "C:\Software\CSV\Users.csv" -FormatFileName
"C:\Software\CSV\Users.xml"
```

Figuur 70 PowerShell script waarmee iedere avond de extensionAttribute1 wordt gesynchroniseerd

25 http://blogs.technet.com/b/servicemanager/archive/2009/12/21/creating-an-ad-connector-using-powershell-and-csv-import.aspx

Op basis van de variabelen “GO” en “SAMAccountname” wordt de variable “extensionAttribute1” gesynchroniseerd met de al bestaande users in Service Manager (geïmporteerd d.m.v. Active Directory Connector):

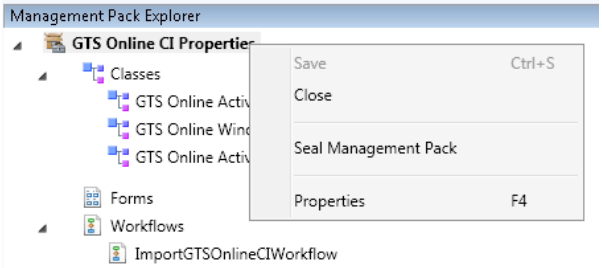


Niet alleen voor de gebruikers moet dit gemaakt worden, maar voor alle Configuration Items waar de klant gebruik van gaat maken via Service Manager. Ook voor Computers, Groepen en eventueel in de toekomst Printers, Software en andere objecten kan dit gemaakt worden.

Management Pack Sealen

Om te voorkomen dat dit soort wijzigingen gewijzigd worden heb ik het Management Pack waarin de wijzigingen gedaan zijn, nadat deze uitvoerig is getest, ‘gesealed’. Een Management Pack die geen seal bevat kan altijd bewerkt worden en keer op keer opnieuw worden geïmporteerd. Probleem hierbij is dat sommige wijzigingen die ondertussen zijn gedaan in Service Manager verwijderd worden.

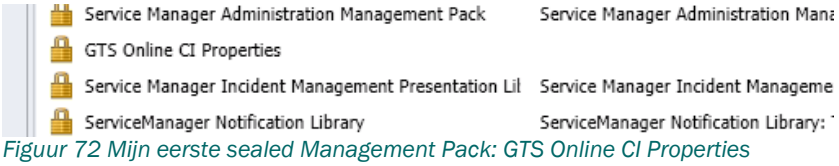
Een Management Pack kan gemakkelijk gesealed worden via de Service Manager Authoring Tool waarin het Management Pack ook gemaakt is.



Figuur 71 Seal Management Pack in Service Manager Authoring Tool

Om een Management Pack te 'sealen' is er alleen een zogeheten "Strong Name Key File" nodig die gemaakt kan worden met de tool die is opgenomen in de "Microsoft Windows SDK[26]". Deze tool heeft de passende naam "Strong Name Utility" en kan worden gebruikt worden om zo'n key file te maken.

Het importeren van een Sealed Management Pack heeft het voordeel dat deze niet zomaar aangepast kan worden door een nieuwe versie te importeren. Een Sealed Management Pack importeren kan alleen als er geen ander Management Pack met dezelfde naam beschikbaar is in Service Manager.



Figuur 72 Mijn eerste sealed Management Pack: GTS Online CI Properties

[26] http://www.microsoft.com/download/en/details.aspx?id=8279

Services in de Self Service Portal

Na de basis installatie van zowel Service Manager en Orchestrator en het configureren van de integratie tussen de twee oplossingen werd het zaak om de Self Service Portal te configureren. Zoals al eerder genoemd bestaat deze uit een aantal Webparts die geïnstalleerd kunnen worden op één of meerdere Sharepoint 2010 omgevingen. Deze webparts communiceren direct met de Service Manager database om gegevens op te halen of in te voeren.

Na het installeren van de Self Service Portal is er “out-of-the-box” meteen de mogelijkheid om een standaard aanvraag te doen, vergelijkbaar met het aanmaken van een incident, zoals in veel helpdesksystemen standaard mogelijk is. Om andere “services” aan te bieden dan alleen het aanmaken van zo’n standaard aanvraag, is er een stevige structuur neergezet door Microsoft.

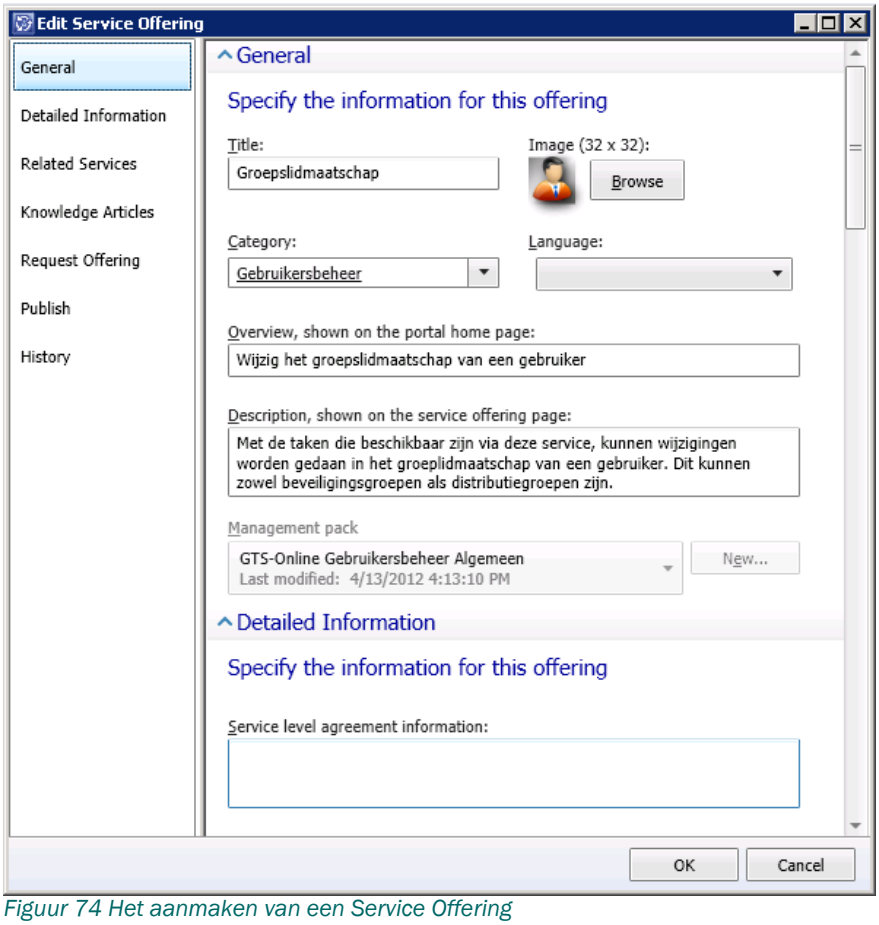
Voor het bespreken van de verschillende onderdelen in het proces is het gemakkelijker om te beginnen aan de kant van de gebruiker. Vanuit dit eindpunt ga ik steeds dieper in op de onderliggende onderdelen van een aangeboden stukje functionaliteit in de Self Service Portal.

Service Offering

We beginnen dus bij de Self Service Portal. Hierin zijn functies voor ingelogde gebruikers geordend per “Service Offering Category” (in de volgende afbeelding blauw omlijnd).

Figuur 73 Service Offering Category (blauw) en Service Offering (rood) in de Self Service Portal

Binnen een categorie vallen één of meerdere “Service Offerings”, zoals hierboven rood omlijnt: Groepslidmaatschap. Bij het openen van een Service Offering verschijnen de onderliggende Request Offerings (in wezen de aanvraagformulieren), bijbehorende kennisbank artikelen en informatie over Service Level Agreements (SLA) en mogelijke kosten. Een SLA is bijvoorbeeld dat bij het gebruik van deze functionaliteit, deze binnen één werkdag of binnen een bepaald aantal uur geïmplementeerd zal worden.



Figuur 74 Het aanmaken van een Service Offering

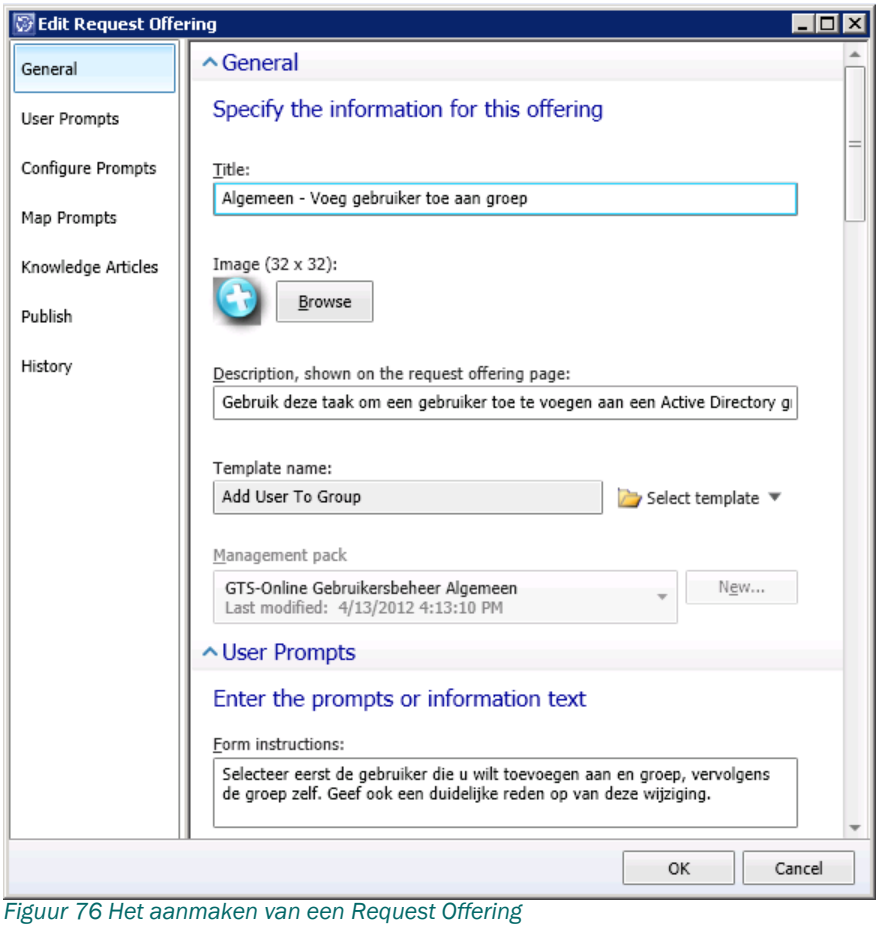
Request Offering

Een Service Offering (of naar het Nederlands vertaald: Serviceaanbieding) bevat op zijn beurt weer één of meerdere “Request Offerings” (aanvragen). Dit zijn in wezen de formulieren die de gebruiker kan invullen om een wijziging door te (laten) voeren.

Figuur 75 Service Offering (blauw) met onderliggende Requests Offerings (rood)

Iedere Request Offering bevat uiteraard informatie over wat deze aanvraag verandert in het systeem en er kan worden gedefinieerd welke informatie er

nodig is om een aanvraag succesvol te kunnen uitvoeren. Voor meer informatie kan er aan een aanvraag ook nog Knowledge Articles gekoppeld worden.



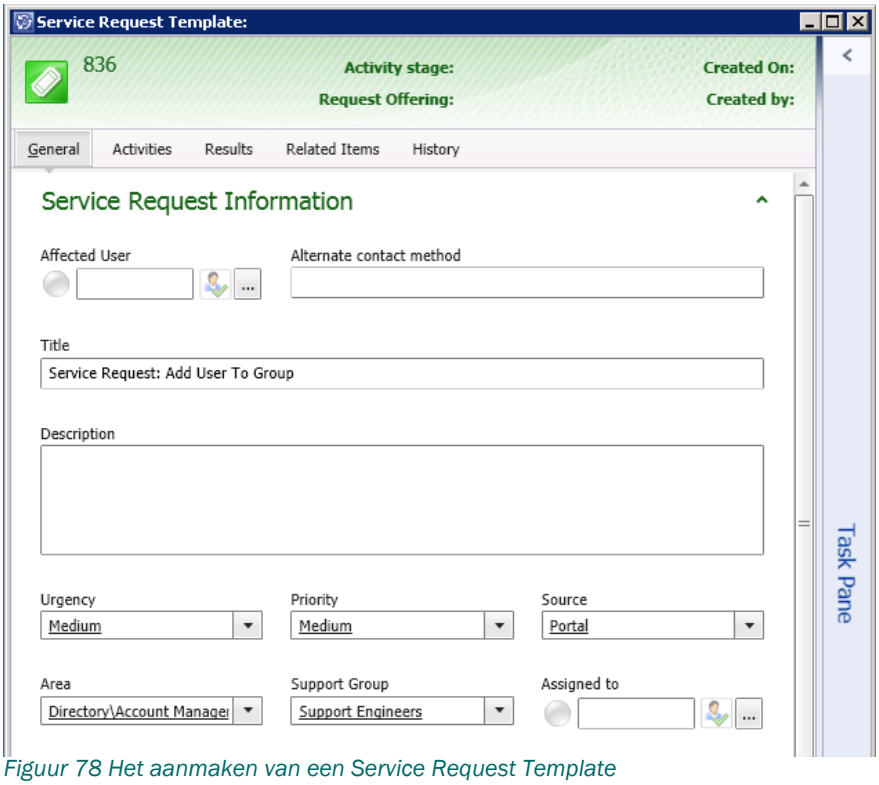
Figuur 76 Het aanmaken van een Request Offering

Zo is er bij het toevoegen van een gebruiker aan een beveiligingsgroep in Active Directory, zoals in bovenstaande afbeelding het geval is, minstens de naam van de gebruiker, de naam van de groep en een reden van de wijziging vereist. Om te voorkomen dat het uitvoeren van de aanvraag niet goed gaat kunnen de naam van de gebruiker en de groep alleen maar worden geselecteerd vanuit de ingebouwde CMDB van Service Manager, zoals op de volgende afbeelding als voorbeeld te zien is.

Figuur 77 Selecteren van items uit de CMDB van Service Manager

Service Request Template

Een Request Offering wordt gemaakt op basis van een eerder gemaakt Template. Een template dient wel gemaakt te zijn op basis van de klasse “Service Request”. In zo’n template worden standaard eigenschappen vastgelegd, zoals bijvoorbeeld de weer te geven naam, welke prioriteit de betreffende aanvraag heeft en in wat voor categorie deze valt:

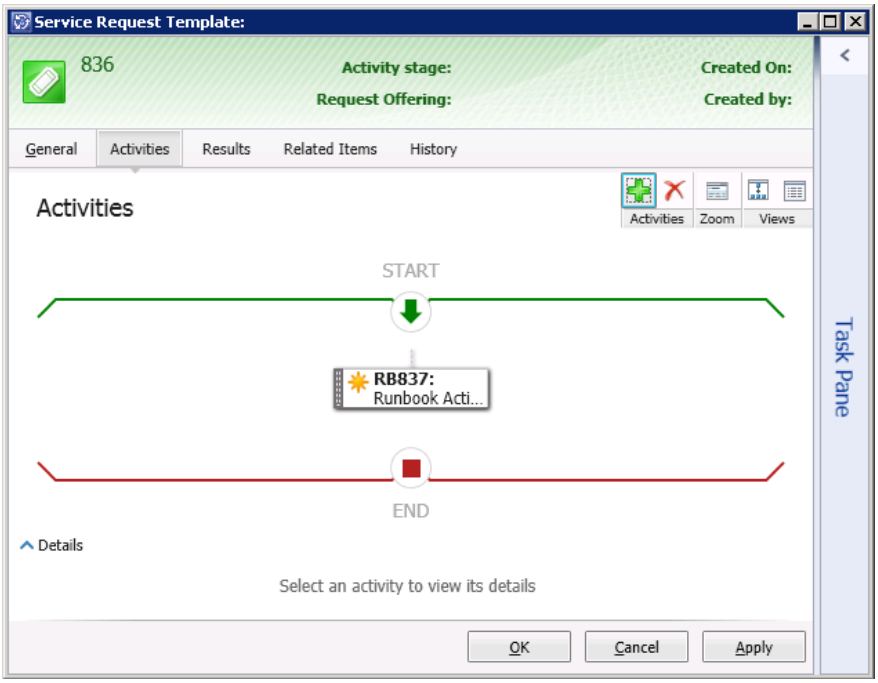


Figuur 78 Het aanmaken van een Service Request Template

Activity Template

Maar het belangrijkste in zo'n template zijn de activiteiten die uiteindelijk uitgevoerd moeten worden op het moment dat een aanvraag op basis van dit template wordt ingediend. Deze activiteiten kunnen handmatige activiteiten zijn, zoals het controleren van de ingevoerde informatie of het uitvoeren van een installatie, maar kunnen ook geautomatiseerde activiteiten zijn op basis van een runbook in Orchestrator.

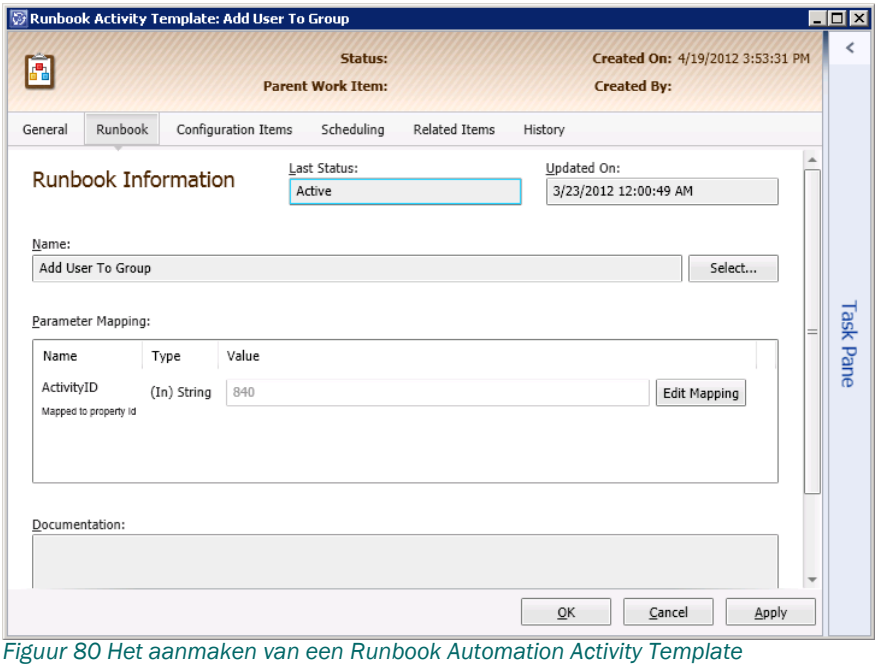
Dit laatste is voor ons uiteraard het meest interessante van deze activiteiten, want door steeds meer geautomatiseerde taken te maken hoeven er juist steeds minder handmatige handelingen worden gedaan naar aanleiding van vragen van gebruikers. Bij het toevoegen van een gebruiker aan een groep is slechts één activiteit nodig:



Figuur 79 Een Runbook Automation Activity als activiteit bij het aanmaken van een Service Request Template

Activiteiten die kunnen worden uitgevoerd zijn ook zelf weer op basis van eerder gedefinieerde templates, zoals een “Default Manual Activity” of een “Default Review Activity” template. Voor een geautomatiseerde activiteit op basis van een runbook uit Orchestrator is het nodig zelf een template te maken voor ieder Runbook dat gebruikt kan worden in Service Manager.

Zo’n activiteit wordt gemaakt op basis van de klasse “Runbook Automation Activity”. Ook bij een Runbook Automation Activity Template kunnen een aantal standaard waarden worden ingevoerd, maar voor dit template is het tabblad “Runbook” het belangrijkst. Daar kan het juiste Runbook geselecteerd worden waarna de in de runbook geconfigureerde Parameters beschikbaar komen die het runbook nodig heeft om mee te starten. Die parameters kunnen bij het uitvoeren van de Runbook Automation Activity automatisch worden ingevuld op basis van de op bij runtime bekende gegevens (zoals bijvoorbeeld het nummer van de activiteit zelf), maar kan ook later worden gevuld met waardes die worden ingevoerd in een Request Offering.

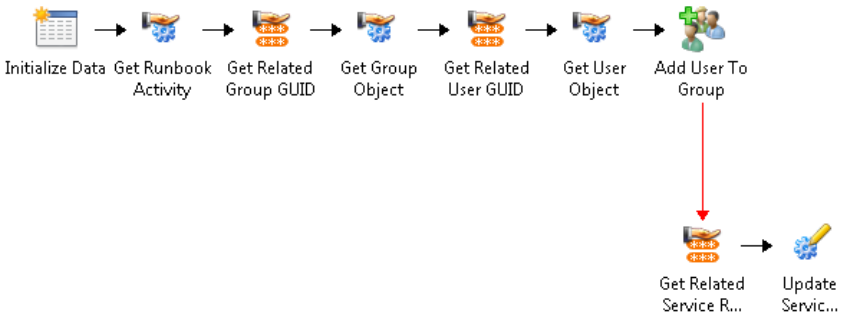


Figuur 80 Het aanmaken van een Runbook Automation Activity Template

Runbook

Voordat een Runbook Automation Activity Template gemaakt kan worden in Service Manager, moet er wel een runbook beschikbaar zijn die uitgevoerd kan worden. Dit is de eerste keer dat Orchestrator om de hoek komt kijken in dit verhaal, maar in werkelijkheid is dit het startpunt van waaruit de meeste aanvragen worden opgebouwd.

De runbook die ik heb gemaakt voor de aanvraag “voeg gebruiker toe aan een groep” is specifiek gemaakt voor gebruik in combinatie met een Runbook Automation Activity. Om dit runbook te kunnen starten is er slechts één parameter vereist: de ID van de Runbook Automation Activity uit Service Manager. Deze parameter wordt automatisch ingevuld bij het starten van de bijbehorende Runbook Automation Activity. De runbook ziet er als volg uit:



Figuur 81 Runbook “Add User To Group”

Met het meegegeven ID wordt het Runbook Automation Activity object opgehaald uit Service Manager. In de Request Offering hebben we aangegeven dat de geselecteerde gebruiker en groep moeten worden gekoppeld aan dit object. Met de activiteiten“Get Related Group GUID” en “Get Related User GUID” worden de GUIDs van deze gekoppelde items

opgehaald. Ieder object in de CMDB van Service Manager heeft een eigen GUID en daarmee kunnen de groeps- en gebruikersobjecten worden opgehaald. Met de informatie uit deze groeps- en gebruikersobjecten kan vervolgens met de activiteit “Add user To Group” de gebruiker aan de groep worden gekoppeld.

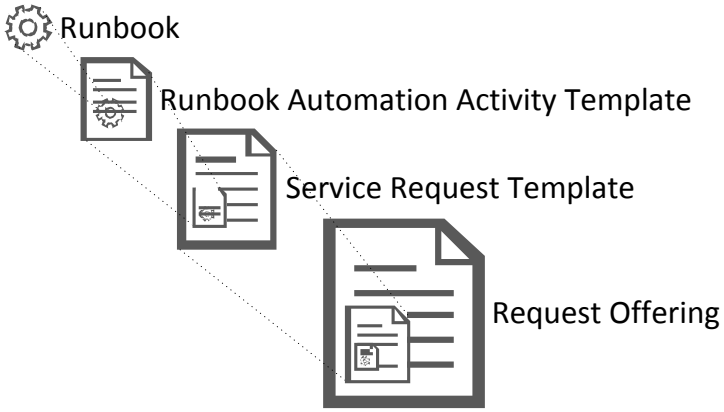
Als deze laatste activiteit gelukt is, dan zal er een signaal terug worden gestuurd naar de Runbook Automation Activity die het runbook heeft aangestuurd dat deze voltooid is en zullen de rest van de activeiten in de Service Request (mochten deze er zijn) worden doorlopen.

Mocht deze laatste activiteit onverhoopt niet goed gaan (de gebruiker is bijvoorbeeld al lid van deze groep), dan worden de activiteiten achter de rode lijn uitgevoerd. Deze activiteiten worden alleen ingevoerd op het moment dat de activiteit “Add user to group” een fout geeft. Deze twee activiteiten halen de objectgegevens op van de Service Request die de Runbook Automation Activity heeft aangestuurd, om deze vervolgens te updaten met de foutmelding die is gegenereerd door de activiteit “Add user to group” en de status op “Geannuleerd” te zetten.

Als deze laatste stap niet gedaan zou worden, zou de runbook de status “Mislukt” krijgen, vervolgens mislukt de Runbook Automation Activity en zal ook de Service Request de status “Mislukt” krijgen, zonder dat de gebruiker op de hoogte gebracht wordt van de reden van deze “mislukking”. Om Self Service te motiveren krijgt de gebruiker op deze manier een foutmelding te zien waaruit kan worden opgemaakt wat er fout is gegaan en de volgende keer dit te kunnen verbeteren.

Samenvattend

In de praktijk blijkt dat het grote aantal stappen in dit proces het erg lastig maakt om achteraf nog een aanpassing te doen. Het van te voren goed vastleggen van de stappen die genomen moeten gaan worden is essentieel om niet heel vaak een aanvraag opnieuw te moeten opzetten.



Figuur 82 Stappen van Runbook tot Request Offering

Er is ook voordeel: werkt een aanvraag goed en zijn alle onderliggende onderdelen generiek opgezet, dan kunnen deze gemakkelijk hergebruikt of voor een groot deel worden overgenomen naar een nieuwe taak. Op die manier zou bijvoorbeeld een Runbook Automation Activity template die een e-mail verstuurd met bepaalde informatie op heel veel plekken hergebruikt kunnen worden.