

Afstudeerscriptie

Project

‘Exchange 2010 ROC Nova College’

Student:	Ruud Beets
Studentnummer:	1546866
Datum:	28 mei 2011
E-mail:	ruud.beets@student.hu.nl
Eerste examinerator:	Roland Bijvank
E-mail:	roland.bijvank@hu.nl

Colofon

Titel	Afstudeerscriptie Project 'Exchange 2010 ROC Nova College'
Opgesteld door	Dhr. R.M. Beets
Datum	28-05-2011
Documentnaam	HU_Scriptie_RM_Beets_1546866_v1.0
Onderwerp	Afstudeerscriptie
Onderwijsinstelling	Hogeschool Utrecht, Nijenoord 1, Utrecht
Opleiding	HBO Systeembeheer Duaal
Studiejaar	2010 - 2011

Contactpersonen

Naam	Rol	Organisatie
Dhr. R. Beets	Student	ROC Nova College
Dhr. P. Loeber	Bedrijfsbegeleider	ROC Nova College
Dhr. R. Bijvank	Docentbegeleider	Hogeschool Utrecht

Revisies

Versie	Datum	Omschrijving
0.1	11-03-2011	Initiële versie
0.2	03-05-2011	Aangepaste versie
0.3	19-05-2011	Aangepaste versie
0.4	23-05-2011	Aangepaste versie
0.5	24-05-2011	Aangepaste versie
1.0	28-05-2011	Definitieve versie

Distributie lijst

Versie	Datum	Namen
0.4	23-05-2011	Dhr. P. Loeber
0.5	28-05-2011	Dhr. R. Bijvank
1.0	31-05-2011	Examencommissie

1 Voorwoord

Deze scriptie is geschreven door Ruud Beets in opdracht van Hogeschool Utrecht. Ik heb de opleiding *HBO Systeembeheer Duaal* gevolgd aan de faculteit Natuur & Techniek in Utrecht.

Na het volgen van deze driejarige opleiding is de laatste fase het schrijven van een scriptie. Op pagina 4 staat de *Managementsamenvatting* waarin ik het onderwerp van mijn scriptie verder toelicht.

Aan deze scriptie heb ik met veel inzet en plezier gewerkt. In overleg met mijn bedrijfsbegeleider Peter Loeber is er een keuze gemaakt in het afstudeeronderwerp. De samenwerking met Peter is prettig verlopen. Mede dankzij de ICT projectervaring van Peter heb ik in de afgelopen periode veel geleerd.

Verder gaat mijn dank uit naar mijn docentbegeleider Roland Bijvank voor de begeleiding gedurende de afstudeerperiode.

Inhoudsopgave

Colofon	1
1 Voorwoord	2
2 Managementsamenvatting	4
3 De opdrachtgever en de klant	5
3.1 ROC Nova College	5
3.2 Dienst ICT	5
3.3 De rol van de afstudeerder	6
4 Probleemstelling en opdracht	7
4.1 Globale probleemstelling	7
4.2 Opdrachtomschrijving	8
4.3 Op te leveren producten en onderzoeksresultaten	8
5 Plan van Aanpak en gebruikte methode	10
5.1 Aanleiding	10
5.2 Doelstelling	10
5.3 Huidige situatie en gewenste situatie	10
5.4 Afbakening	12
5.5 Deelnemers aan het project	12
5.6 Projectplanning	14
6 Functioneel ontwerp	16
6.1 Inleiding	16
6.2 Analyse van eisen uit de organisatie	16
6.3 Gebruikers- en informatie-eisen	18
6.4 Eisen aan applicaties	19
6.5 Eisen aan de datastromen	20
6.6 Eisen aan storage en databases	22
6.7 Eisen aan het netwerk	23
6.8 Analyse transitiefase	24
7 Technisch ontwerp	27
7.1 Algemene informatie	27
7.2 Ontwerp	29
7.3 Beveiliging van het netwerk	37
7.4 Overzicht fases	38
8 Implementatieplan en beschrijving	40
8.1 Implementatieplan	40
8.2 Beschrijving	40
8.3 Proof of Concept	43
8.4 Het testen van hardware en databases	43
9 Monitoring uptime	49
9.1 Monitoring	49
10 Conclusies en aanbevelingen	50
11 Evaluatie	51
12 Bronvermelding	52
13 Gebruikte Afkortingen	53
14 Overzicht gebruikte figuren en tabellen	54
Bijlage A - Veranderingsanalyse	55
Bijlage B - Overzicht overlegpunten	67
Bijlage C - Overzicht installatie documentatie	79
Bijlage D - Eindrapportage realisatiefase	116
Bijlage E - Handleiding Servicedesk Exchange Control Panel	120
Bijlage F - Importeren PST files	124
Bijlage G - Procedure uitfasering	125

2 Managementsamenvatting

Het project *Exchange 2010 ROC Nova College* heeft als doel een nieuw e-mailplatform te ontwerpen. De aanleiding voor dit project is dat het huidige Microsoft Exchange 2003 e-mailplatform end-of-lifetime is en qua prestaties en gebruikerservaring achterblijft bij applicaties als Microsoft Sharepoint 2010, die wel reeds zijn geïmplementeerd binnen het Nova College.

Tijdens de ontwerpfase wordt rekening gehouden met de eisen van de opdrachtgever. Deze eisen bestaan uit een hoge beschikbaarheid, voldoende groeimogelijkheden en de mogelijkheid om e-mail te archiveren. Door middel van een 'Proof of Concept' wordt het ontwerp in een testomgeving getoetst en geëvalueerd of de gewenste functionaliteiten aanwezig zijn. Vervolgens kan het ontwerp met eventuele aanpassingen in de productieomgeving worden geïmplementeerd.

Door gebruik te maken van een groep testgebruikers wordt de implementatie gemonitord en geëvalueerd. Indien de evaluatie positief is, zullen alle gebruikers van het Nova College op termijn van het nieuwe e-mailplatform gebruik gaan maken. Deze laatste migratieslag maakt geen deel uit van dit project.

Overzicht van de verwachte baten:

Het project *Exchange 2010 ROC Nova College* levert financieel gezien geen directe baten op.

Echter, qua functionaliteiten en eigenschappen van het nieuwe e-mailplatform kunnen we de volgende kwalitatieve baten onderscheiden:

- Een flexibeler en betrouwbaarder systeem dan het huidige e-mailplatform;
- Een sterk verbeterde gebruikerservaring ten opzichte van het huidige e-mailplatform;
- Opslag, archivering en handhaving van e-mail kunnen door het Nova College worden afgedwongen;
- Een vermindering van de beheerlast van het e-mailplatform voor de dienst ICT;
- Een grotere gebruikersproductiviteit, doordat er een aantal nieuwe functionaliteiten beschikbaar komen.

Voorafgaand aan het project is er een veranderingsanalyse uitgevoerd om te kunnen vaststellen welk product of welke productcombinatie het meest geschikt zou zijn als opvolger van het huidige platform. De uitkomst van deze analyse heeft de opdrachtgever doen besluiten om voor het alternatief '*Implementatie Exchange 2010 High Availability*' te kiezen.

Naar aanleiding van deze keuze is er een functioneel ontwerp opgesteld volgens de methode van *James D. McCabe*. Het functionele ontwerp is vervolgens vertaald naar een technisch ontwerp. Het technisch ontwerp is in eerste instantie geïmplementeerd in de bestaande testomgeving van het Nova College. Dit 'Proof of Concept' is getoetst op haalbaarheid en gewenste functionaliteiten. Na de bevredigende resultaten van de 'Proof of Concept' is het technisch ontwerp succesvol geïmplementeerd in de productieomgeving van het Nova College.

3 De opdrachtgever en de klant

3.1 ROC Nova College

Het Regionaal Opleidingen Centrum (ROC) Nova College verzorgt mbo beroepsopleidingen en volwassenenonderwijs in de regio IJmond, Haarlem, Haarlemmermeer, Amstelveen en de Duin- en Bollenstreek. Het Nova College is te vinden op 21 locaties verspreid over de regio. Bij het Nova College werken \pm 1.450 medewerkers. Het aantal ingeschreven cursisten telt ruim 15.000.

De organisatie van het Nova College bestaat uit drie organisatorische pijlers:

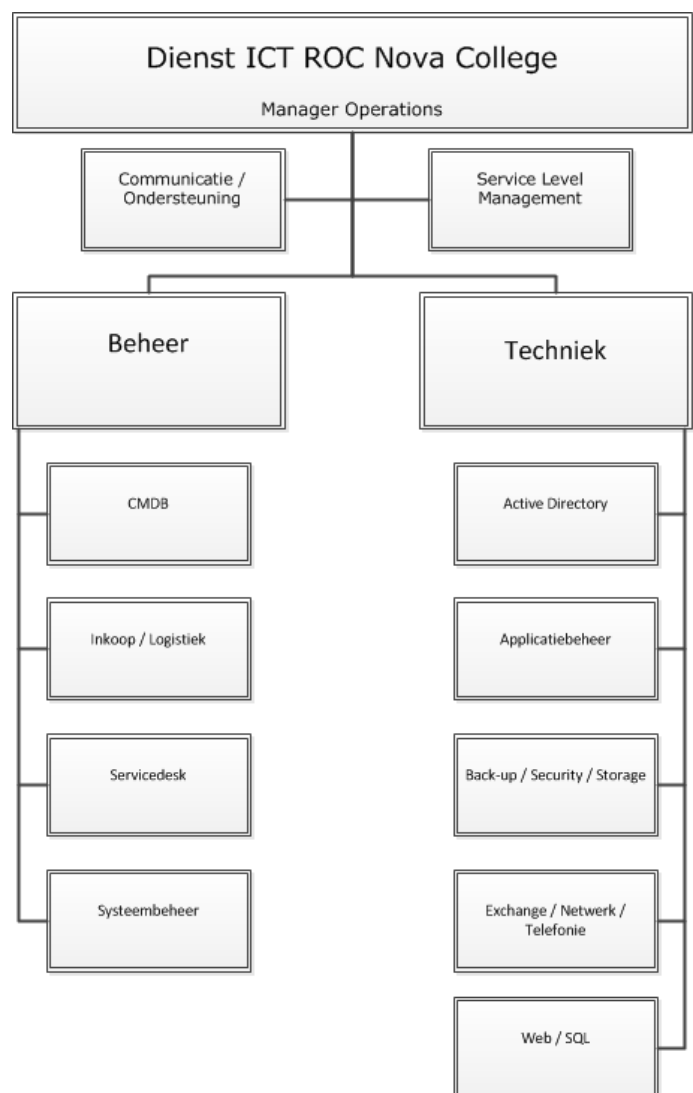
- Onderwijsunits;
- Bureau Bedrijfsvoering;
- Bestuursbureau.

3.2 Dienst ICT

De dienst ICT Beheer is onderdeel van het Bureau Bedrijfsvoering en verantwoordelijk voor de ontwikkeling en het beheer van de informatievoorziening van alle onderdelen van het Nova College. Deze voorzieningen bestaan uit: datacom- en telecomvoorzieningen, werkplekautomatisering, systeem- en netwerkbeheer, serverbeheer en technisch applicatiebeheer. De dienst ICT faciliteert gebruikersondersteuning via de ICT Servicedesk. Deze ondersteuning geldt alleen voor de medewerkers van het Nova College. De cursisten kunnen terecht bij de docent of Notebooksupport.

De dienst ICT bestaat uit drie teams: Coördinatie, Beheer en Techniek. De Manager Operations ICT stuurt, samen met 2 Teamleiders, 28 medewerkers aan. Met deze drie teams beheert de dienst ICT \pm 2.500 werkstations, \pm 800 laptops en \pm 200 servers.

In figuur 1 wordt het organogram de dienst ICT schematisch weergegeven.



Figuur 1 - Organogram Dienst ICT Nova College

3.3 De rol van de afstudeerder

Ik ben werkzaam bij de dienst ICT van het Nova College. Deze dienst valt samen met de diensten HRM, Marketing & Communicatie, Facilitaire Zaken, Cursisten Zaken, Informatie Management en Bedrijfsprocessen & Financiën onder het Bureau Bedrijfsvoering.

In juni 2002 ben ik bij het Nova College in dienst getreden als assistent-systeembeheerder. Mijn eerste werkzaamheden verrichte ik op de locatie Zijlweg in Haarlem bij de lokale afdeling systeembeheer.

Na het behalen van het diploma *MBO Netwerkbeheerder niveau 4* in 2004 ben ik gepromoveerd naar de functie van systeembeheerder. Naast het diploma MBO Netwerkbeheer ben ik ook in bezit van een MEAO diploma Economisch-Juridisch.

Vanaf 2005 werk ik als systeembeheerder op de locatie Garenkokerskade in Haarlem, op deze locatie is de dienst ICT gehuisvest. In maart 2011 ben ik gepromoveerd naar de functie van technisch specialist.

We werken op de locatie Garenkokerskade met ongeveer 25 personen aan verschillende taken. Deze taken lopen uiteen van inkoop van ICT apparatuur tot softwareontwikkeling.

De dienst ICT heeft alle hardware in eigen beheer, zoals servers, netwerkkapapparatuur en werkstations. Daarnaast ontwikkelen we software en andere digitale toepassingen. Ook voeren we regelmatig zelfstandig ICT projecten uit, zoals de implementatie van een Wireless netwerk en de uitlevering van 800 docentenlaptops.

Mijn taken bestaan uit het beheren van het datanetwerk, de telecom en VoIP omgeving en de e-mail en de Office Communications-omgeving. De genoemde taken zijn ondergebracht in de werkgroep *Exchange, Netwerk en Telefontie*. Deze werkgroep bestaat op dit moment uit drie medewerkers.

4 Probleemstelling en opdracht

4.1 Globale probleemstelling

Het Nova College heeft momenteel het groupware platform Microsoft Exchange 2003 als e-mailsysteem in gebruik. Dit platform draait bij het Nova College sinds 2004 op vier Windows Server 2003 servers. De hardware van deze vier servers is aan het einde van de daarvoor staande levenscyclus. Bovendien loopt de extended support op de software voor Exchange 2003 af in augustus 2014. De mainstream support voor Exchange Server 2003 is reeds op 14 april 2009 door Microsoft beëindigd.

De storageoplossing waarmee de huidige Exchange servers verbonden zijn, zit aan het plafond qua beschikbare ruimte. Er is het afgelopen jaar geïnvesteerd in extra opslagruimte in de vorm van een nieuw SAN systeem. Het heeft de voorkeur om deze nieuwe opslagruimte direct in combinatie met nieuwe servers in gebruik te nemen. Dit voorkomt dat de data van de mailboxen twee keer gemigreerd moet worden.

Op het Nova College is behoefte aan een hoger mailboxquotum voor medewerkers. Op dit moment kunnen de verzoeken om de mailboxgrootte uit te breiden niet worden gehonoreerd.

De dienst ICT constateert een wildgroei aan zogenaamde PST-bestanden. Een PST-bestand (personal storage table files) is een databestand die gebruikers zelf kunnen aanmaken. Het PST-bestand wordt vervolgens gevuld met e-mail uit de online mailbox. Hierdoor winnen gebruikers ruimte in hun online mailbox.

Er zijn echter een aantal serieuze problemen bij het beheer van de PST-bestanden. Deze problemen uiten zich in een aantal verschijnselen. Eén van de doelen die mij bij het schrijven van het projectplan voor ogen staat is het wegnemen van deze negatieve verschijnselen.

De geconstateerde verschijnselen:

- datacorruptie;
- onbeheerde bestanden;
- hoge kosten indien een mail moet worden teruggevonden;
- het niet kunnen afdwingen van een bewaartermijn voor e-mail;
- risico van data diefstal;
- dataverlies;
- geen overzicht van de e-mail data.

Om ook in de toekomst aan de wensen van de gebruikers op het gebied van e-mail opslag te kunnen voldoen, zal er aandacht worden besteed aan de vraag of er voldoende opslagmedia voorhanden is. Een onderzoek naar de uitbreidingsmogelijkheden van de huidige SAN infrastructuur zal tijdens het maken van het ontwerp aan de orde moeten komen. Met name de vraag of het mogelijk is een onderscheid maken tussen bepaalde dataopslag, de zogenaamde hot-storage en cold-storage, verdient aandacht.

Nadat de mogelijkheden van dataopslag duidelijk zijn zal er een migratieplan worden opgesteld. In dit plan staat beschreven hoe de PST-bestanden worden opgespoord en kunnen omgezet naar een beter beheerbare oplossing.

4.2 Opdrachtomschrijving

De genoemde constatering in de globale probleemstelling van paragraaf 4.1 heeft het management van de dienst ICT doen besluiten om het bestaande Exchange 2003 e-mailplatform te migreren naar het Microsoft Exchange 2010 platform. Na deze migratie moet het Nova College in staat zijn om de controle over e-mailfaciliteiten terug te krijgen. Dit kan door de behoefte aan het gebruik van PST-bestanden weg te nemen bij de gebruiker.

Exchange 2010 biedt hiervoor een duidelijke optie. Deze optie betreft de introductie van persoonlijke archieven binnen Exchange. Het gebruik van persoonlijke archieven stelt de gebruiker in staat om e-mailberichten op te slaan in een archief mailbox die toegankelijk is via Microsoft Outlook 2007 (update beschikbaar vanaf begin 2011), Microsoft Outlook 2010 en ook webbased via Microsoft Office Outlook Web App 2010.

Tijdens de afstudeeropdracht zullen mijn werkzaamheden bestaan uit onder andere het analyseren, het ontwerpen en inrichten van het Microsoft Exchange 2010 platform. Het nieuwe ontwerp en migratieplan zullen eerst in de bestaande testomgeving van het Nova College worden uitgevoerd. Aan de hand van een 'Proof of Concept' worden onder meer het gekozen ontwerp en de gehanteerde methoden en technieken getoetst.

Na een succesvol verlopen uitvoering van de 'Proof of Concept' in de testomgeving is de eerstvolgende stap een gedetailleerd projectvoorstel opstellen voor de realisatie van de totale oplossing in de productieomgeving. Het project zal worden opgedeeld in een vooronderzoek, een opstart-, een realisatie en een eindfase. Aan het eind van elke fase moet de stuurgroep van het project de resultaten beoordelen en al dan niet instemmen met het starten van de volgende fase.

Gedurende het project zal ik de rol van projectmanager vervullen. Drie collega's zullen onderdeel uitmaken van de projectgroep. De Manager Operations van de dienst ICT zal mij tijdens het uitvoeren van de afstudeeropdracht terzijde staan met adviezen rond de opbouw van het projectplan.

4.3 Op te leveren producten en onderzoeksresultaten

Het project levert de volgende producten op:

- Analyse van Eisen;
- Een functioneel ontwerp;
- Een technisch ontwerp;
- 'Proof of concept';
- Implementatieplan;
- Een PST-migratie werkprocedure voor systeembeheerders;
- Een handleiding beheer voor de ICT Servicedesk;
- Eindrapport realisatiefase;
- Procedure uitfasering;
- Presentatie;
- Alle documentatie gebundeld.

Tijdens het de uitvoering van dit project dient rekening te worden gehouden met:

- Flexibiliteit;
- Groeimogelijkheden;
- Schaalbaarheid;
- Toekomstgerichtheid;
- Beheersbaarheid.

De bovengenoemde kenmerken dienen tot uiting te komen in het ontwerp voor de vervanging van het huidige e-mailplatform van het Nova College. Door aandacht te besteden aan deze kenmerken tijdens het maken van het functionele ontwerp, kan de dienst ICT inspelen op toekomstige vraagstukken die vanuit de organisatie gesteld kunnen gaan worden.

5 Plan van Aanpak en gebruikte methode

5.1 Aanleiding

Het Nova College heeft momenteel het groupware platform Microsoft Exchange 2003 als e-mailsysteem in gebruik. Dit huidige systeem is end-of-lifetime. Het Nova College heeft aangegeven graag een geavanceerder e-mailsysteem te willen opzetten om zo aan de toenemende behoeftes van de gebruikers te kunnen voldoen. Deze behoeftes bestaan onder meer uit:

- Een betere toegang tot de mailbox indien een medewerker zich buiten het Nova College bevindt;
- Meer opslagruimte en betere archiveringsmogelijkheden;
- Een snellere responstijd bij het openen van een mailbox.

5.2 Doelstelling

Dit project heeft als doel een nieuw e-mailplatform te ontwerpen. Door middel van het uitwerken van een 'Proof of Concept' zullen de gewenste functionaliteiten worden gerealiseerd. De 'Proof of Concept' zal eerst in een testomgeving worden gerealiseerd, na een positieve evaluatie zal hetzelfde ontwerp in de productieomgeving worden geïmplementeerd.

De doelstelling van het project *Exchange 2010 ROC Nova College* is dat de opslag en het beheer van e-mail op een veiliger en beter gestructureerde wijze gaat plaatsvinden.

Het Exchange 2010 Nova College project moet een e-mailplatform voor het Nova College creëren dat voor de komende vijf jaar aan de wensen van de gebruikers kan voldoen.

5.3 Huidige situatie en gewenste situatie

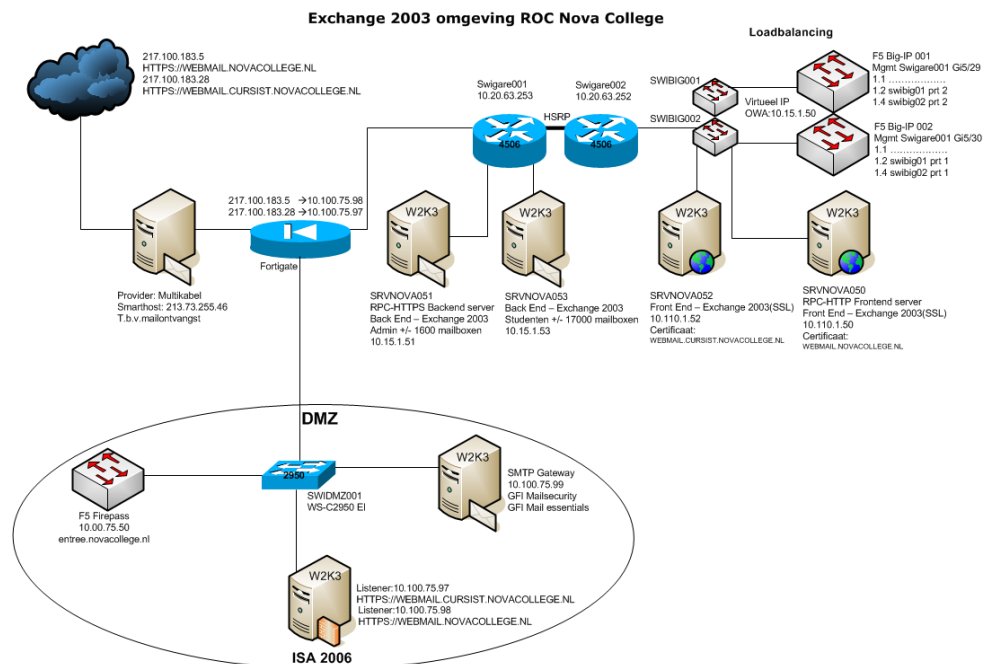
5.3.1 Huidige situatie

Het Nova College beschikt op dit moment over een Exchange Server 2003 Enterprise omgeving, draaiend op Windows Server 2003 SP2 servers.

De extended support op de software voor Microsoft Exchange 2003 loopt af in augustus 2014. De mainstream support voor Exchange Server 2003 is reeds op 14 april 2009 door Microsoft beëindigd.

De opstelling is samengesteld uit twee Front-End (FE) en twee Back-End (BE) servers waarop zich een totaal van ruim 20.000 mailboxen bevindt (zie figuur 2).

Het huidige Exchange 2003 ontwerp voorziet niet in redundant uitgevoerde databases. Elke mailboxserver heeft de beschikking over maar één exemplaar van een database. Indien een database door welke reden dan ook corrupt raakt, is de kans op dataverlies aanwezig. Momenteel hebben de eindgebruikers de beschikking over een relatief kleine mailbox. Met als gevolg het gebruik van PST-bestanden door de gebruikers.



Figuur 2 - Huidig e-mailplatform Nova College

Het gebruik van PST-bestanden brengt voor de organisatie veel nadelen met zich mee:

- datacorruptie;
- onbeheerde bestanden;
- hoge kosten indien een mail moet worden teruggevonden;
- het niet kunnen afdwingen van een bewaartermijn voor e-mail;
- risico van data diefstal;
- dataverlies;
- geen overzicht van de e-mail data.

5.3.2 Gewenste situatie

Het nieuwe e-mailplatform moet onder andere over de volgende eigenschappen beschikken:

- De mogelijkheid om grotere mailboxen (van 100 Mb naar 300 Mb) aan alle medewerkers aan te bieden;
- Voldoende groeimogelijkheden qua storagecapaciteit;
- Mogelijkheid tot archivering van e-mail;
- De e-mail moet kunnen worden benaderd met Microsoft Outlook 2007 en hoger;
- Een sterk verbeterde gebruikerservaring wat betreft het gebruik van de e-mail webinterface (Outlook Web App). Ongeacht via welke webbrowser deze benaderd wordt: IE6 en hoger, Firefox, Google Chrome of Safari;
- De e-mail moet toegankelijk zijn via smartphones met een OS van het type Apple iOS, Android en Windows Mobile 5 en hoger;
- Het ontwerp voorziet in een hoge beschikbaarheid van het e-mailplatform;
- Het nieuwe platform kan qua hardware en software support minimaal 5 jaar mee;
- Een goede beveiliging van het platform.

5.4 Afbakening

Dit project heeft invloed op de wijze van opslag en back-up van de e-mail. Tevens krijgen de gebruikers te maken met een aantal veranderingen op het gebied van de grafische interface van de Nova Webmail en manier van opslaan van hun e-mail. Door middel van een handleiding die op de SharePoint-website Nova Portal wordt gepubliceerd, worden de gebruikers geïnstrueerd hoe met de nieuwe interface gewerkt kan worden.

In dit project wordt niet meegenomen de migratie van de cursisten en medewerkers mailboxen. Verder wordt ook niet meegenomen de opsporing en migratie van alle PST-bestanden van de medewerkers. Wat wel onderdeel uitmaakt van dit project zijn het scheppen van voorwaarden die het mogelijk maken om dit uit te voeren.

- *Must have*: een ontwerp van het e-mailplatform, een getest ontwerp in de testomgeving door middel van een 'Proof of Concept';
- *Should have*: implementatie e-mailplatform in de productieomgeving;
- *Could have*: migratieplanning mailboxen;
- *Won't have now*: volledige uitfasering van het huidige e-mailplatform.

Het project kent de volgende doelstellingen en verantwoordelijkheden:

- Analyse van Eisen;
- Een functioneel ontwerp;
- Een technisch ontwerp;
- 'Proof of concept';
- Implementatieplan;
- Een PST-migratie werkprocedure voor systeembeheerders;
- Een handleiding beheer voor de ICT Servicedesk;
- Eindrapport realisatiefase;
- Procedure uitfasering;
- Presentatie;
- Alle documentatie gebundeld.

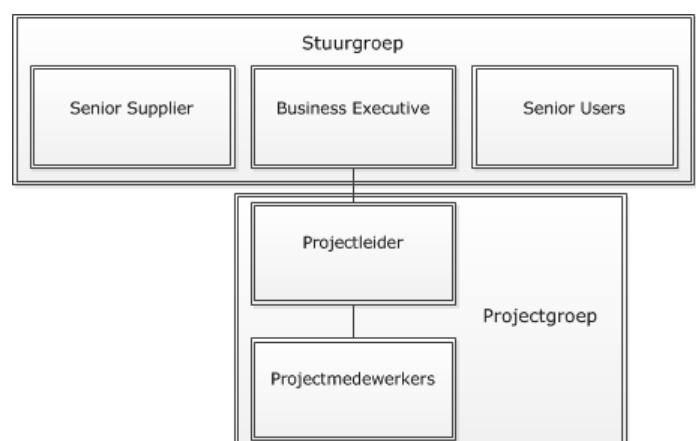
De volgende onderdelen maken geen deel uit van het project:

- Installatie en configuratie van de hardware componenten;
- Migratie van applicaties, anders dan in paragraaf 5.4 vermeld.

5.5 Deelnemers aan het project

5.5.1 Projectgroep

De projectgroep begeleidt de installatiefase en verzorgt de afstemming van alle werkzaamheden. De projectgroep mag beslissingen nemen binnen de door de stuurgroep vastgestelde begroting en planning. Indien er afwijkingen zijn of worden verwacht, worden deze gemeld aan de stuurgroep. Indien er beslissingen moeten worden genomen over voorgestelde oplossingen binnen het



Figuur 3 - Projectorganisatie

project, worden deze eveneens voorgelegd aan de stuurgroep. De projectmanager functioneert als schakel tussen de projectgroep en de stuurgroep.

5.5.2 Stuurgroep

De stuurgroep neemt beslissingen over de planning, het budget en vragen vanuit de projectgroep. Tevens wordt de voortgang van het project door de stuurgroep bewaakt. Een andere taak van de stuurgroep is om formeel de eindproducten te accepteren.

5.5.3 Vergaderfrequentie

De projectgroep komt tijdens de start van het project bijeen. Tijdens de projectperiode komt de projectgroep eenmaal per week bij elkaar voor overleg. Verder zal er tijdens de uitvoering van het project een wekelijks overleg worden gevoerd tussen de projectleider en de stuurgroep in de vorm van het reguliere Techniekoverleg.

Samenstelling Stuurgroep		
Rol	Naam	Verantwoordelijkheden
Business Executive	Peter Loeber	<ul style="list-style-type: none"> ○ Eindverantwoordelijke voor het project ○ Eigenaar van de Business Case ○ Besluitvorming stuurgroep ○ Accorderen
Senior Users	Peter Zandvliet Ruud Lok	<ul style="list-style-type: none"> ○ Verantwoordelijk voor de eisen die aan de producten gesteld moeten worden en voor een eenduidig standpunt namens de diverse belanghebbenden
Senior Supplier	Gert Wenning	<ul style="list-style-type: none"> ○ Aanspreekbaar op de kwaliteit van de door de Suppliers geleverde producten en voor de tijdige oplevering hiervan

Samenstelling Projectgroep		
Rol	Naam	Verantwoordelijkheden
Projectleider	Ruud Beets	<ul style="list-style-type: none"> ○ Dagelijkse leiding van het project ○ Opleveren van de diverse producten ○ Rapporteren aan de stuurgroep ○ Communicatie naar alle betrokkenen binnen het project en alle gerelateerde projecten ○ Toezien op kwaliteitscontroles en indien nodig escaleren
Projectmedewerkers	Leo Noordermeer Paul Kieft Pieter Hulscher	<ul style="list-style-type: none"> ○ Opleveren diverse producten volgens afspraak ○ Rapporteren aan de projectmanager ○ Verzorgen communicatie naar de gebruikers

5.5.4 Voorwaarden aan derden

Tijdens de uitvoering van het project is de projectgroep afhankelijk van bepaalde werkgroepen binnen de dienst ICT van het Nova College. De projectleider zal de activiteiten waaruit deze afhankelijkheden bestaan tijdig afstemmen met de diverse werkgroepen. Indien de voortgang van het project hinder ondervindt van het niet tijdig nakomen van de afspraken, kan er worden geëscaleerd naar de stuurgroep.

5.6 Projectplanning

In de projectplanning wordt aangegeven wanneer welke producten worden opgeleverd en wat de eventuele kosten zullen zijn. De planning kan tijdens het project worden aangepast wanneer er sprake is van nieuwe ervaringen en/of nieuwe feiten.

5.6.1 Aanpak en fasering

Definitiefase

- Voorbespreking met de opdrachtgever, Manager Operations ICT. In dit gesprek zullen een aantal zaken duidelijk moeten worden. Als eerste de verdeling van de verantwoordelijkheden en als tweede of de benodigde resources voorhanden zijn. Ook zullen de huidige situatie, de globale probleemstelling en het gewenste resultaat aan de orde komen;
- De door de opdrachtgever gestelde voorwaarden aan het ontwerp worden samengevat in een Analyse van Eisen;
- Indien dit is afgestemd kan er een start worden gemaakt met het verzamelen van gegevens en het definiëren van de globale probleemstelling. Ook wordt er een activiteitenoverzicht samengesteld;
- Deze informatie wordt samengevoegd in het Plan van Aanpak.

Ontwerpfase

- Om een goed beeld te krijgen van de huidige situatie wordt er een beschrijving van de huidige e-mailsysteem gemaakt. (*Beschrijving huidige situatie*);
- Het maken van een functioneel ontwerp dat de problemen, genoemd in de globale probleemstelling, kan oplossen. Vervolgens wordt het functioneel ontwerp vertaald naar een technisch ontwerp. Door middel van het uitvoeren van een 'Proof of Concept' wordt het technisch ontwerp uitgetest in een testomgeving;
- Het resultaat is:
 - Een functioneel ontwerp;
 - Een technisch ontwerp;
 - Een 'Proof of Concept' testomgeving;
 - Een beschrijving van de huidige e-mailsysteem.

Voorbereidingsfase

- Indien de 'Proof of Concept' succesvol is, gaan we verder met de voorbereiding om het technisch ontwerp in de productieomgeving te implementeren. Dit houdt onder meer in het aankopen van hardware en licenties, het scheppen van randvoorwaarden en het opstellen van een implementatieplan;
- Het opstellen van handleidingen voor de gebruikers met betrekking tot het nieuwe product;
- In samenwerking met de dienst Marketing & Communicatie de gebruikers informeren over de veranderingen waar zij mee te maken krijgen;
- Het resultaat is een implementatieplan.

Realisatiefase

- Het implementeren van de oplossing volgens het implementatieplan en het eventueel verbeteren van de bedachte oplossing;
- Verplaatsen van mailboxen van testgebruikers in de productieomgeving van het Exchange 2003 naar het Exchange 2010 platform;
- Evaluatie met de testgebruikers;
- Verplaatsen van PST-bestanden van testgebruikers in de productieomgeving naar het Exchange 2010 platform;
- Evaluatie met de testgebruikers;
- Het inrichten van monitoring en onderhoudsprocedures voor het nieuwe e-mailplatform;
- Het opstellen van procedures en handleidingen voor de ICT Servicedesk en systeembeheerders;
- Het resultaat is:
 - Een eindrapport met daarin de bevindingen van het projectteam tijdens de realisatiefase;
 - Een procedure voor de systeembeheerders;
 - Een handleiding voor de ICT Servicedesk.

Nazorgfase

- Troubleshooting;
- Evaluatie;
- Procedure opstellen voor de uitfasering van het huidige e-mailplatform;
- Het voorbereiden van een presentatie;
- Het resultaat is een presentatie en een procedure uitfasering.

6 Functioneel ontwerp

6.1 Inleiding

Voor het creëren van een ontwerp voor het nieuwe e-mailplatform gebruiken we de methode van James D. McCabe. Deze methode is in eerste instantie ontwikkeld voor het ontwerpen van netwerken. Ik heb voor deze methode gekozen omdat een groot aantal onderdelen één op één toepasbaar zijn bij het maken van een ontwerp voor een nieuw e-mailplatform.

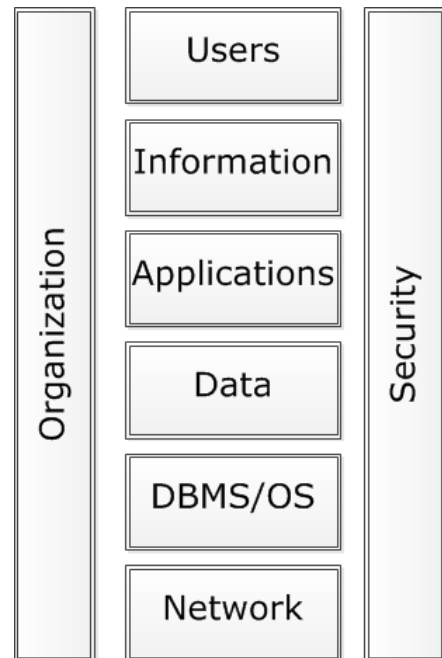
McCabe gebruikt in zijn methode een systeembenadering, het is juist deze benadering die voor dit project uitermate geschikt is. McCabe gaat uit van een aantal niveaus: users – applications – devices – networks. Op alle niveaus speelt security een duidelijke rol. Om de beveiliging te waarborgen wordt dit op elk niveau vanuit een andere invalshoek gewaarborgd.

De systeembenadering zoals weergegeven wordt in figuur 4, zullen wij gebruiken om een logisch ontwerp op te stellen.

McCabe gebruikt voor het opzetten van een systeem de volgende fases:

- Vooronderzoek;
- Analyse;
- Architectuur;
- Ontwerp.

Deze fasering zullen wij in grote lijnen overnemen.



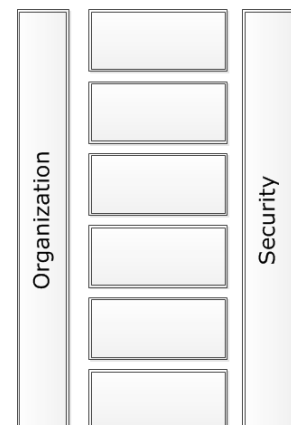
Figuur 4 - De systeembenadering van James D. McCabe

6.2 Analyse van eisen uit de organisatie

Om een goed beeld te krijgen van de eisen die aan het nieuwe e-mailplatform gesteld worden, kunnen deze het beste onderverdeeld worden in een aantal niveaus.

De systeembenaderingsmethode van James McCabe gaat ervan uit dat we de eisen verzamelen op elk niveau van het systeem. Op het hoogste niveau vinden we de eisen met betrekking tot de gebruikers beveiliging en op het laagste niveau het netwerk in de vorm van perimeter beveiliging.

In figuur 5 wordt aangegeven op welke plaats in het systeem van McCabe de eisen thuishoren. Aangezien alle niveaus betrokken zijn bij het functioneren van het nieuwe e-mailplatform kunnen we concluderen dat er organisatorische maatregelen noodzakelijk zijn



Figuur 5 - Organisatie

voor een adequate beveiliging. Om verantwoord beheer van het systeem te kunnen waarborgen dienen minimaal de volgende beheersprocessen te worden ingevuld:

- **Autorisatiebeheer**

Er zijn veel gegevens binnen het platform met een vertrouwelijk karakter. Het op de juiste wijze uitdelen, wijzigen en intrekken van autorisaties is hierbij van cruciaal belang. Er kan hier onderscheid gemaakt worden tussen het configureren op tactisch/operationeel en business/ICT niveau.

- **Configuratiebeheer**

Er zijn diverse redenen om het belang van configuratiebeheer aan te geven. Wanneer we beheer uitvoeren over hardware en software is het raadzaam om informatie bij te houden om bijvoorbeeld:

- a) Te kunnen achterhalen welke afspraken en contracten er zijn afgesloten ten aanzien van de software of het apparaat dat een storing veroorzaakt;
- b) In geval van diefstal van gegevens te kunnen herleiden wie welke rechten heeft verstrekt.

- **Incidentbeheer**

Aan het nieuwe e-mail platform worden bepaalde eisen gesteld met betrekking tot de beschikbaarheid. Mocht zich een storing voordoen dan is het belangrijk om duidelijke procedures te hebben om deze storing zo snel mogelijk te kunnen verhelpen.

- **Wijzigingsbeheer**

Wanneer er wijzigingen worden aangebracht aan de productie omgeving kan dit een storing veroorzaken. Het bijhouden van wijzigingen is erop gericht om op een gestructureerde en doordachte manier wijzigingen aan te brengen. Tevens kan het voorbereiden van wijzigingen er toe bijdragen dat er een noodprocedure of roll-back scenario beschikbaar is, mocht een aangebrachte wijziging een storing veroorzaken.

- **Operationeel beheer**

Alle hardware en software hebben tegenwoordig periodiek onderhoud nodig. Dit kan zijn in de vorm van een nieuw servicepack, nieuwe firmware, security updates of een bug-fix. Logging en monitoring zijn hierin essentieel.

- **Beveiligingsbeheer**

De wereld om ons heen staat niet stil. Beveiliging is daarom een dynamisch geheel. Elke dag komen er nieuwe dreigingen op ons af. Dreigingen in de vorm van per e-mail verspreide virussen of het verouderen van bestaande beveiligingstechnieken. Het is reëel om aan te nemen dat de beveiliging en de daarvoor geldende eisen periodiek zullen veranderen. Als organisatie moet je hierop kunnen anticiperen. Een procesmatige aanpak is daarom vereist.

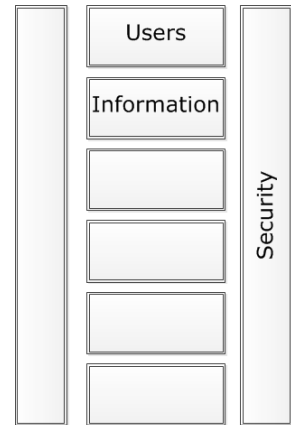
6.3 Gebruikers- en informatie-eisen

Informatie is wat iedere organisatie nodig heeft. Zonder informatie kunnen de medewerkers van een organisatie niet functioneren. Het is belangrijk om ervoor te zorgen dat de informatie aan een aantal eisen voldoet.

We willen dat de informatie altijd voldoet aan een aantal eisen. Informatie moet zijn:

- Toegankelijk;
- Betrouwbaar;
- Bruikbaar;
- Up to date;
- Juist.

Hoe en welke systemen ervoor zorgen dat de informatie aan de genoemde eisen voldoet word in een later stadium beschreven.



Figuur 6 - Gebruikers- en informatie eisen

De informatie dient altijd door middel van de juiste autorisatie beschikbaar te zijn voor bepaalde eindgebruikers, een groep of een proces.

Figuur 6 laat zien op welke plaats in het systeem van McCabe deze eisen thuishoren.

De volgende tabel geeft een overzicht van de gebruikers- en informatie-eisen weer:

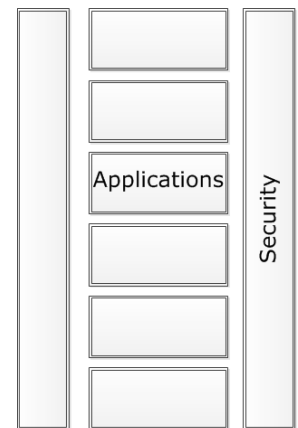
I1	Het verstrekken van informatie aan alle eindgebruikers verloopt altijd via een authenticatieprocedure
I2	Informatieverstrekking binnen de gebruikte applicaties wordt geregeld door gebruik te maken van Role Based Authentication (RBACS)
I3	Direct inloggen op fysieke systemen wordt alleen toegestaan voor medewerkers in de werkgroepen Netwerk en Back-up van de Dienst ICT van het Nova College.
I4	Informatieverstrekking aan eindgebruikers: er wordt niet gekozen voor een factor 2 authenticatie om de e-mail te kunnen benaderen. Deze vorm van authenticatie wordt alleen bij het aanmelden op het domein m.b.v. van een docentenlaptop afgedwongen
I5	Het nieuwe systeem moet een jaarlijkse beschikbaarheid hebben van minimaal 99,5%. Indien we uitgaan van vier storingen per jaar komt de verwachte MTBF (Mean Time Between Failures) op een gemiddelde periode van 2188 uur (± 3 maanden)
I6	De verwachte MTTR (Mean Time Till Repair) binnen het service window (kantooruren) dient niet boven de 2 uur uit te komen

Tabel 1 - Gebruikers- en informatie eisen

Onder eindgebruikers wordt verstaan: medewerkers van de ondersteunende diensten, docenten en cursisten.

6.4 Eisen aan applicaties

Voordat we kunnen beginnen met het inrichten van een e-mailplatform gebaseerd op Exchange 2010 moeten de onderliggende systemen aan een aantal eisen voldoen.



Figuur 7 - Applicatie

Hier volgt een overzicht van de belangrijkste eisen:

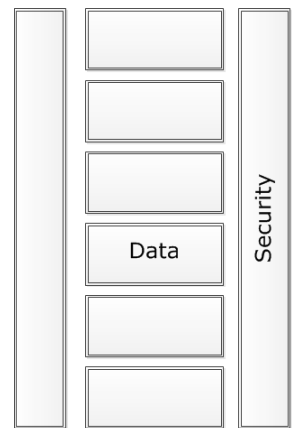
	Component	Benodigd
A1	Bestaande Exchange versie	<ul style="list-style-type: none"> Exchange Server 2003, of hoger en in native mode
A2	Active Directory forest	<ul style="list-style-type: none"> Active Directory Windows Server 2003 forest functionaliteit versie, of hoger en in native mode
A3	Global Catalog / Active Directory Schema Master	<ul style="list-style-type: none"> The Global Catalog Servers en de Active Directory Schema Master moeten minimaal over het OS Windows Server 2003 SP1 beschikken
A4	Link State updates	<ul style="list-style-type: none"> Moeten worden uitgezet op alle Exchange Server 2003 servers
A5	Een besturingssysteem op hardware met een 64-bit processor	Eén van de volgende: <ul style="list-style-type: none"> 64-bit edition of Windows Server 2008 Standard with Service Pack 2 (SP2) 64-bit edition of Windows Server 2008 Enterprise with SP2 64-bit edition of Windows Server 2008 R2 Standard with SP1 64-bit edition of Windows Server 2008 R2 Enterprise with SP1 Windows Server 2008 Datacenter Windows Server 2008 R2 Datacenter
A6	Outlook cliënt en Entourage cliënt ondersteuning	<ul style="list-style-type: none"> Outlook 2010 Outlook 2007 Outlook 2003 Entourage 2008 for Mac, Web Services Edition Outlook for Mac 2011

Tabel 2 - Eisen aan applicaties

6.5 Eisen aan de datastromen

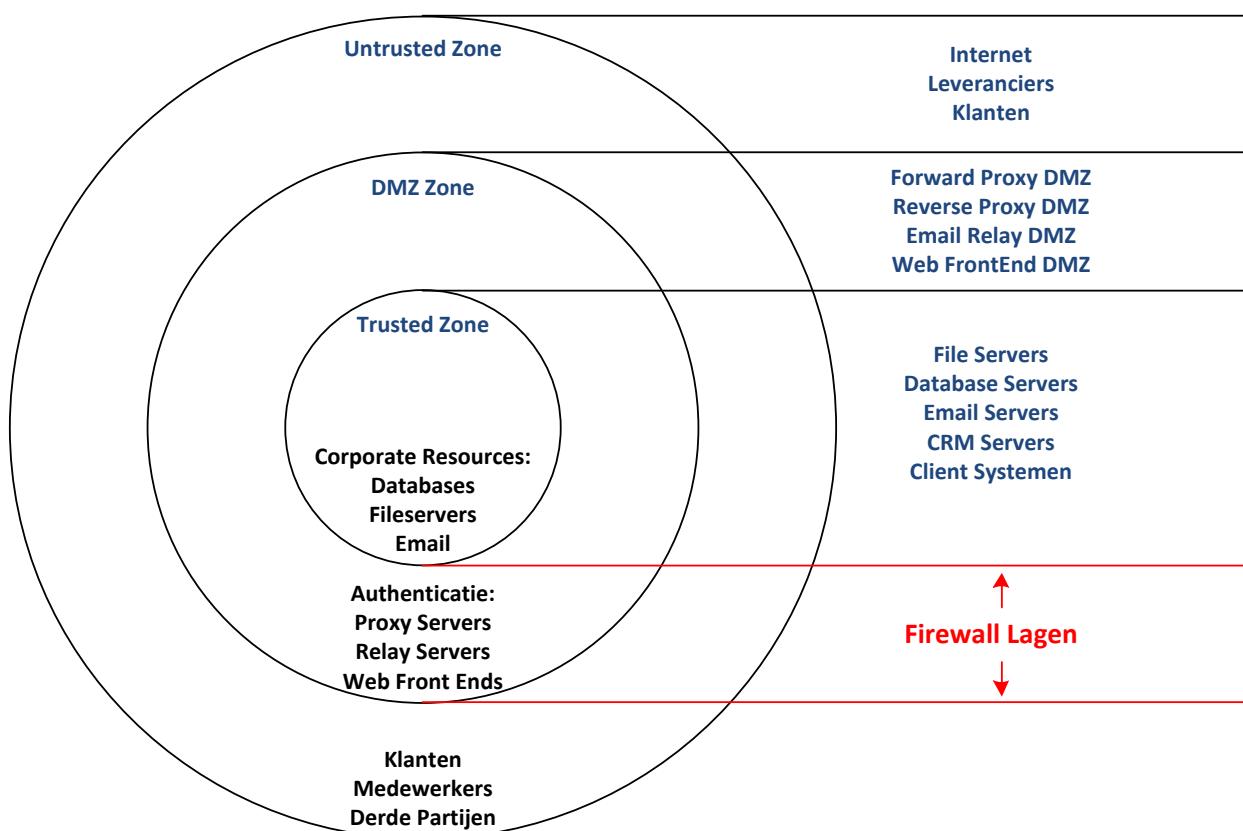
Figuur 9 geeft een overzicht van de zones die de datastromen dienen te passeren wanneer er wordt gecommuniceerd tussen eindgebruikers en servers. Bij het opstellen van het datastroom ontwerp voor het Nova College is het een voorwaarde dat een datastroom nooit twee zones in één keer passeert. Deze benadering voorkomt dat gebruikers van buitenaf direct bij een server van het interne (veilige) netwerk kunnen komen.

Een datastroom dient dus altijd via een DMZ (DeMilitarized Zone) in- of uit de organisatie te worden getransporteerd. In de praktijk betekent dit dat er Forward- en Reverse Proxies voor web verkeer worden ingezet. Het in- en uitgaande e-mail verkeer verloopt via een zogenaamde SMTP-mailgateway die in de DMZ zone is geconfigureerd.



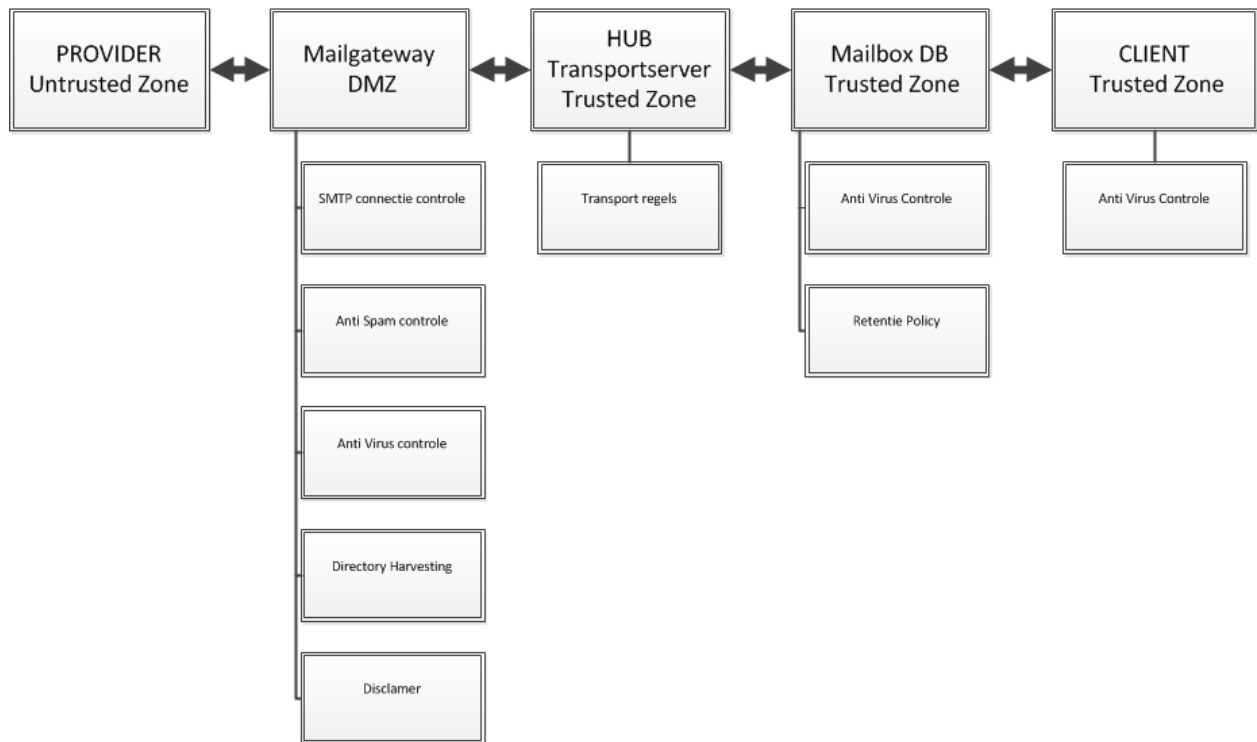
Figuur 8 - Datastromen

Figuur 8 geeft aan op welke plaats in het systeem van McCabe deze eisen terug te vinden zijn.



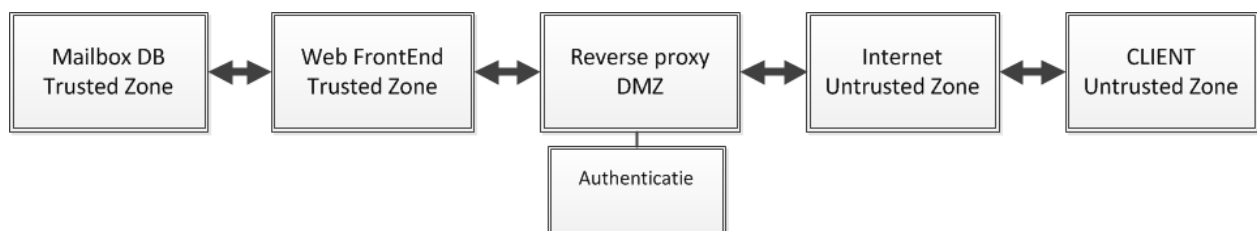
Figuur 9 - Globale datastromen

Het onderstaande figuur laat het proces zien dat een e-mail bericht doorloopt als het de organisatie binnen komt of verlaat. Een e-mail bericht kan ook intern (binnen de Trusted Zone) blijven.



Figuur 10 - Datastromen e-mail processing

Het onderstaande figuur geeft de datastromen weer indien een eindgebruiker gebruik maakt van een webbrowser om zijn e-mail te raadplegen.



Figuur 11 - Datastromen web verkeer

In tabel 3 worden alle datastromen die binnen het e-mail platform kunnen ontstaan weergegeven.

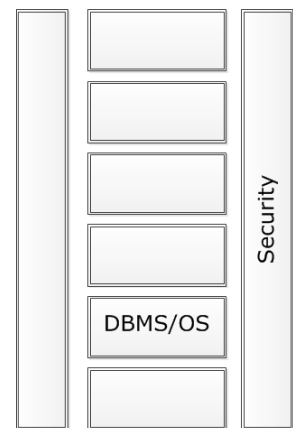
D1	Een e-mail wordt door de provider aangeboden aan de Mailgateway server in de DMZ
D2	De e-mail wordt door de gateway server naar een HUB Tansportserver gestuurd
D3	De e-mail wordt door de HUB Tansportserver afgeleverd aan een Mailbox DB server
D4	Een MAPI cliënt haalt de e-mail op, en slaat hem op in de offline storage file
D5	Een e-mail wordt door Mailgateway server in de DMZ aan de provider aangeboden
D6	De e-mail wordt door de HUB Tansportserver naar gateway server gestuurd
D7	De e-mail wordt door de Mailbox DB server aan HUB Tansportserver afgeleverd
D8	Een MAPI cliënt stuurt een e-mail naar de Mailbox DB server
D9	Een web cliënt maakt verbinding met de Reverse proxy
D10	De Reverse proxy maakt verbinding met een Directory server
D12	De Reverse proxy maakt verbinding met de Web FrontEnd server
D13	De Web FrontEnd server maakt verbinding met Mailbox DB server

Tabel 3 - Datastromen

6.6 Eisen aan storage en databases

Onderstaande eisen zijn opgesteld aan de hand van productdocumentatie van leverancier Microsoft in combinatie met informatie over de eindgebruikers in de huidige omgeving.

De informatie over de eindgebruikers is op diverse manieren verzamelt; handmatig, door het uitvoeren van scripts en het raadplegen van rapportages. Hierdoor is inzicht verkregen in het aantal in het aantal gebruikers, het mailverkeer, mailboxquota's en de huidige bezettingsgraad van de mailboxen. Met behulp van deze informatie zijn drie gebruikersprofielen opgesteld. Het eerste profiel betreft de 2.000 eindgebruikers die werkzaam zijn bij het Nova College. Het tweede profiel betreft de 500 zogenaamde intensieve gebruikers, deze kenmerken zich door intensief gebruik van e-mail applicaties en een hoog datagebruik. Deze groep krijgt de beschikking over grote mailboxen en een MAPI-client die tijdens kantooruren continue online zoekacties uitvoert. Het derde profiel betreft de ruim 20.000 cursisten die momenteel ingeschreven staan.



Figuur 12 - DBMS/OS

Per profiel worden waardes zoals mailboxgrootte, wel of geen archieffunctie, wel of geen desktop search engines, gemiddelde berichtgrootte en mailfrequentie opgegeven.

Als alle zojuist genoemde informatie beschikbaar is kan deze gebruikt worden om de *Exchange 2010 Mailbox Server Role Requirements Calculator* in te vullen. Leverancier Microsoft heeft deze applicatie beschikbaar gesteld. Deze applicatie gebruiken we om een goede inschatting te maken van de benodigde hardware.

De calculator berekend het minimale aantal IOPS (het gemiddelde aantal input/output bewerkingen per seconde) waaraan de gebruikte storage oplossing zal moeten voldoen. De storage oplossing is de belangrijkste pijler onder een e-mailplatform en verdient daarom veel aandacht.

In tabel 4 zien we een overzicht van de eisen aan de DBMS-OS.

D1	Het platform dient een hoge beschikbaarheid te kunnen garanderen. Bij de gebruikerseisen is reeds een percentage genoemd
D2	De individuele mailboxservers dienen de in de <i>Exchange 2010 Mailbox Server Role Requirements Calculator</i> te berekenen aantal IOPS aan te kunnen
D3	Het platform dient over voldoende redundantie te beschikken om Single Points of Failure uit te sluiten
D4	Het platform dient te voorzien in betrouwbare databases
D5	Het platform dient schaalbaar te zijn
D6	Binnen het platform dient de mogelijkheid voor mail archivering aanwezig te zijn
D7	Er dient onderscheid gemaakt te worden tussen diverse storage lagen

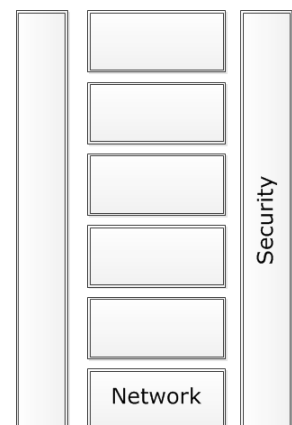
Tabel 4 - Eisen aan DBMS-OS

6.7 Eisen aan het netwerk

Onder het netwerk verstaan we:

- De bekabeling van het LAN;
- De netwerkinterfaces van de servers;
- Netwerkkapparatuur zoals switches, routers, firewalls en loadbalancers.

De scheiding tussen bepaalde segmenten, loadbalancing en netwerksnelheden worden in deze paragraaf besproken. De gebruikte protocollen die binnen de TCP/IP stack vallen behoren ook tot het netwerk.



Het netwerk waarin het nieuwe e-mailplatform wordt geïnstalleerd moet voldoen aan de volgende eisen: **Figuur 13 - Netwerk**

N1	Netwerk delay binnen het LAN mag maximaal 20 milliseconden bedragen
N2	Servers dienen in een apart netwerksegment te worden ondergebracht
N3	Toegang tot het e-mail platform vanaf het cursistennetwerksegment wordt beperkt door gebruik te maken van diverse Access Lists op de routers
N4	Servers binnen het e-mail platform moeten een redundante netwerkinterface hebben
N5	Netwerkkapparatuur moet gemonitord worden met SNMP-agents. De SNMP-strings zijn alleen bekend binnen de afdeling ICT
N6	Het LAN van het e-mail platform dienst minimaal te beschikken over een snelheid van 1000Mbps
N7	Binnen de LAN-infrastructuur is hardwarematige redundante loadbalancing mogelijk

Tabel 5 - Eisen aan het netwerk

6.8 Analyse transitiefase

Op dit moment gebruikt het Nova College een Exchange Server 2003 e-mailplatform. In het jaar 2007 is de versie Exchange Server 2007 door de leverancier Microsoft uitgebracht. Destijds heeft het management van het Nova College besloten om geen transitie traject in te zetten naar deze versie.

De huidige situatie is als volgt: er is een Exchange Server 2003 e-mailplatform, Exchange Server 2007 wordt overgeslagen. Er wordt een transitie gedaan naar Exchange Server 2010.

De beste manier om dit te doen is Exchange Server 2010 te integreren in de bestaande Exchange Server 2003 omgeving. Dit wordt een "intra-organizational migration" genoemd.

De overgang van Exchange Server 2003 naar Exchange Server 2010 in dezelfde Active Directory-forest heet transitioning. Bouw van een nieuw Active Directory-forest met een nieuwe Exchange Server 2010 organisatie en het verplaatsen van mailboxen van de oude Active Directory naar de nieuwe Active Directory wordt in de white papers van Microsoft 'migreren' genoemd.

Om het nieuwe platform te kunnen integreren met het oude platform zijn er een aantal zaken die we even op een rijtje moeten zetten:

- De huidige servers kunnen niet worden geüpgraded;
- De huidige Exchange 2003 WebFrontEnds kunnen geen Exchange 2010 mailboxen ten behoeve van Outlook Web Acces publiceren;
- De transitie wordt uitgevoerd per mailbox.

Bovenstaande feiten zorgen ervoor dat dat het noodzakelijk is de twee e-mailplatform tijdelijk naast elkaar te laten draaien.

De servers van het nieuwe platform worden geïnstalleerd in hetzelfde Windows Server 2003 Active Directory-domein als het huidige Exchange Server 2003 e-mailplatform. Op deze wijze is het verplaatsen van de mailboxen van Exchange Server 2003 naar Exchange Server 2010 minder complex. Wij kiezen voor een transitie omdat dit het beste past in de huidige strategie van de Dienst ICT

6.8.1 Analyse webmail URLs

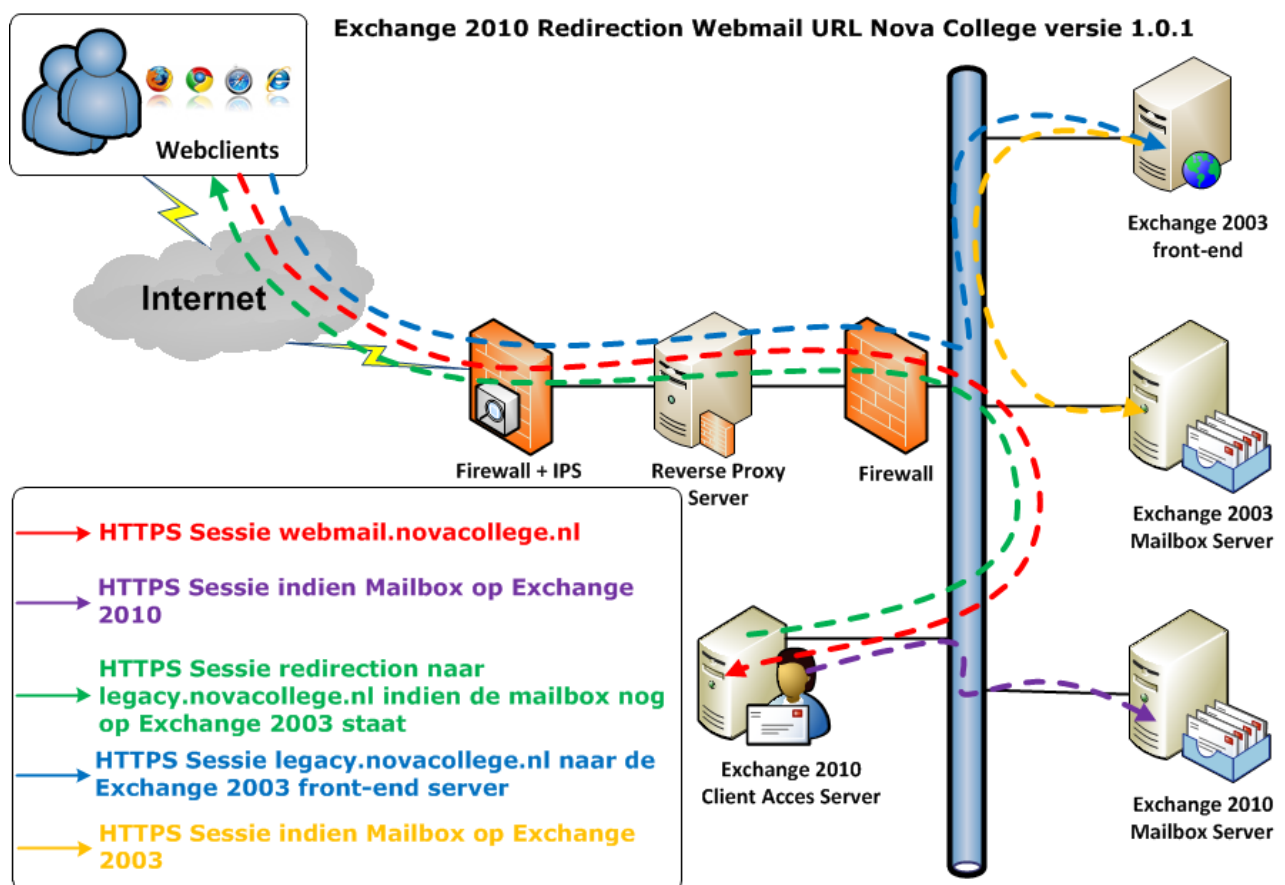
Wanneer er een begin gemaakt wordt met een transitieproces Exchange 2003 naar Exchange 2010 is één van de eerste veranderingen die plaatsvindt de volgende:

- Alle cliënt verbindingen verlopen voortaan via een Exchange Server 2010 Client Access Server.

Indien de mailbox van de eindgebruiker nog op een Exchange Server 2003 Mailbox Server staat dan wordt het cliëntverzoek doorgestuurd naar de Exchange Server 2003 front-end server. Deze front-end server handelt vervolgens het verzoek af.

Dit betekent automatisch dat de URLs van de Exchange-omgeving moeten worden aangepast voordat er een mailbox transitie kan plaatsvinden:

- <https://webmail.novacollege.nl> – Deze URL wordt gebruikt door alle internet-cliënts die verbinding maken met de Exchange-omgeving. Deze naam is niet anders dan in de Exchange Server 2003 omgeving, maar zal nu wijzen naar de Exchange Server 2010 Client Access Server;
- <https://autodiscover.novacollege.nl> – Deze URL wordt gebruikt door Outlook 2007 en Outlook 2010 cliënts voor autodiscover doeleinden (Autodiscover is een hulpmechanisme dat eindgebruikers buiten de eigen organisatie in staat stelt om op eenvoudige wijze een Outlook profiel te configureren);
- <https://legacy.novacollege.nl> – Dit wordt de nieuwe URL voor de Exchange Server 2003 front-end servers (bestaande omgeving). De URL van de Exchange Server 2003 front-end servers moet dus worden aangepast.



Figuur 14 - Redirection van de webmail URL

In figuur 14 zien we de weergave van een cliënt verzoek vanaf het internet voor het openen van een mailbox in een webbrowser, ook wel webmail genoemd. Alle verzoeken komen uit bij de nieuwe 2010 Client Access Server. Indien de mailbox van de eindgebruiker al op een Exchange 2010 mailboxserver staat dat handelt de 2010 Client Access Server het verzoek verder af.

Indien de mailbox van de eindgebruiker nog niet is verplaatst en dus nog op een 2003 mailboxserver staat, dan verzorgt de 2010 Client Access Server een redirection naar een andere URL. In de huidige situatie moet de URL doorverwezen worden naar: legacy.novacollege.nl. In de adresbalk van de eindgebruiker verandert de URL webmail.novacollege.nl naar legacy.novacollege.nl.

Op deze wijze kunnen beide omgevingen een periode naast elkaar draaien zonder dat de eindgebruiker een andere URL hoeft te gebruiken.

Voorwaarde voor een bovenstaand scenario is het gebruik van een zogenaamd SAN SSL certificaat. SAN staat voor Subject Alternative Name, ook wel bekend als Unified Communications SSL Certificaat (UCC SSL). Een standaard SSL Certificaat beveiligt slechts één Fully Qualified domeinnaam. Bij een SAN Certificaat kunnen in het 'Alternative Name-veld' echter meerdere alternatieven voor de common name worden geplaatst.

Om het bovenstaande ontwerp te kunnen implementeren is er een certificaat nodig met de volgende drie common names:

- webmail.novacollege.nl;
- legacy.novacollege.nl;
- autodiscover.novacollege.nl.

Het certificaat moet worden aangevraagd bij een officiële Certificate Authority (CA), om te voorkomen dat eindgebruikers een waarschuwing krijgen dat het SSL certificaat niet wordt vertrouwd.

7 Technisch ontwerp

Om invulling te geven aan het technisch ontwerp zullen we aandacht besteden aan onder meer:

- Ontwerp;
- Benodigde software;
- Benodigde hardware;
- Beveiliging van het netwerk.

7.1 Algemene informatie

Bij het uitkomen van het product Microsoft Exchange 2010 zijn er veel nieuwe ontwerp mogelijkheden en configuratie opties bijgekomen om rekening mee te houden. Het aantal serverrollen in Exchange 2010 is flink uitgebreid ten opzichte van Exchange 2003. Het Exchange 2003 ontwerp kan daardoor niet overgenomen worden. Er moet een nieuw technisch ontwerp worden gemaakt.

7.1.1 Serverrollen

Voordat we kunnen beginnen met het maken van een ontwerp is het verstandig om de vijf serverrollen die Exchange 2010 gebruikt te kunnen onderscheiden. We zetten ze even op een rijtje:

- Client Access Server Role - Via de Client Access Server (CAS) maken de gebruikers verbinding met de Exchange-omgeving. De CAS server zet vervolgens een connectie op met de mailbox server waar de mailbox van de eindgebruiker op geplaatst is. Vergeleken met Exchange 2003 is dit een grote verandering. Hierin maakte de cliënt nog direct verbinding met de mailbox server. Naast deze aanpassing is de CAS server ook verantwoordelijk voor het aanbieden van de Autodiscover service, Outlook Web App, ActiveSync en POP3, IMAP connecties;
- Mailbox Server Role - Op de mailbox server zijn de databases geplaatst ten behoeve van mailboxen en public-folders. Sinds Exchange 2010 kennen we geen storage groups meer maar alleen nog maar databases. De mailboxdatabases kunnen in een Database Availability Groups (DAGs) geplaatst worden waardoor men een 'High Availability' mailboxdatabase omgeving kan creëren. Er kunnen maximaal 16 mailbox servers lid zijn van de DAG. In dit geval zal op alle 16 servers een kopie aanwezig zijn van de database. De servers onderling monitoren elkaar om eventuele problemen te detecteren. Zo blijft de database ook beschikbaar als er een probleem ontstaat op 1 van de mailbox servers;
- Hub Transport Role - De HUB Transport server is onder andere verantwoordelijk voor het verzenden en ontvangen van berichten. Dit geldt voor berichten binnen en van buiten de organisatie. Hiervoor wordt gebruik gemaakt van send en receive connectors. Op de HUB server wordt ook ingesteld voor welke domeinen de Exchange server mail mag ontvangen. Daarnaast kunnen op de HUB Transport server transport rules aangemaakt worden. Transport Rules maken het mogelijk om bijvoorbeeld gepersonaliseerde handtekeningen toe te voegen aan berichten, berichten te kopiëren naar een journal mailbox of berichten te weigeren;

- Unified Messaging Role - Met de Unified Messaging (UM) Server wordt het mogelijk om in de standaard mail omgeving voicemail berichten te ontvangen. Deze kunnen vervolgens afgeluisterd worden middels Outlook/OWA of via de subscriber access. Subscriber Access biedt eindgebruikers de mogelijkheid via een speciaal telefoonnummer toegang te krijgen tot hun mailbox;
- Edge Transport Role - De Edge Transport Server is een server welke in de DMZ geplaatst wordt en in tegenstelling tot alle overige rollen geen lid is van het domein. Middels een Edge-Subscription wordt er een verbinding opgezet tussen de HUB Transport server en een Edge Transport Server. Deze subscription zorgt er voor dat de correcte send en receive connectors worden aangemaakt op beide servers. Daarnaast zal de Edge Transport Server informatie ontvangen van de HUB Transport server waaronder: wat zijn de ingestelde accepted domains en welke gebruikers bestaan er binnen de Exchange omgeving. Dit laatste wordt gebruikt door de anti-spam agents welke geactiveerd zijn op de Edge Transport server. Hiermee kan een e-mail die gericht is aan een niet bestaand persoon direct al op de Edge Transport worden geweigerd in plaats van pas op de HUB Transport server.

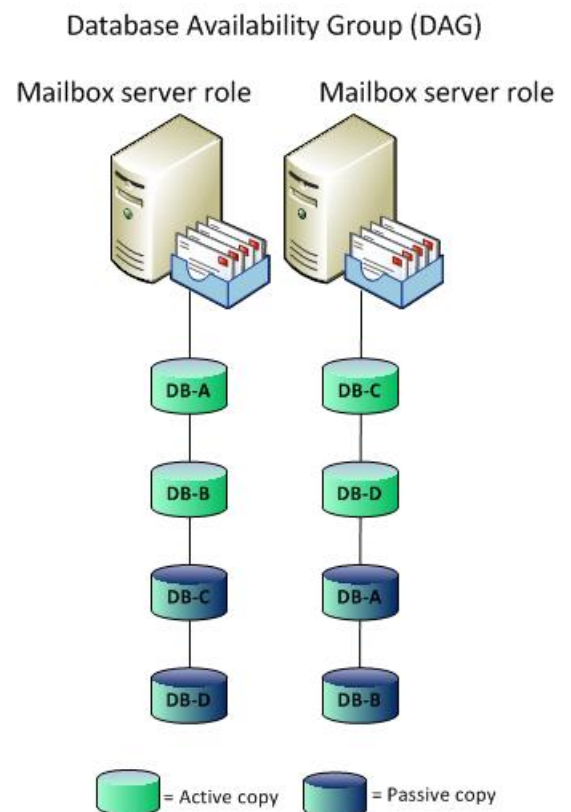
7.1.2 High Availability

7.1.2.1 Databases

Om aan de functionele eis van een hoge beschikbaarheid van het e-mailplatform te kunnen voldoen kiezen we bij het maken van het ontwerp voor een "High Availability" inrichting van de mailbox servers. Door gebruik te maken Database Availability Groups (DAG) binnen Exchange 2010 kunnen we de downtime als gevolg van updates en onvoorziene storingen aanzienlijk reduceren. In figuur 15 zien we een simpele weergave van een DAG architectuur. Elke mailboxserver beheert zowel actieve als passieve kopieën van bepaalde databases. Wanneer één van de twee afgebeelde servers zou uitvallen worden de passieve kopieën op de nog actieve server automatisch geactiveerd. Op deze wijze blijven de mailboxen van de eindgebruikers beschikbaar.

7.1.2.2 Client Acces

Om op het gebied van de Client Access ook redundantie in te bouwen wordt er gekozen voor twee CAS servers. Microsoft raad aan om beide servers achter een hardware loadbalancer te plaatsen. Het Nova College beschikt over een loadbalance oplossing van de firma F5. Navraag bij de leverancier heeft ons geleerd dat de bestaande apparatuur, mits voorzien van softwareversie v10.1 of later, loadbalancing van Exchange 2010 ondersteund. Bij het configureren van zogenaamde iRules op de loadbalancer dient gebruik te worden gemaakt van de deployment guide "Deploying F5 with MS Exchange Server 2010" versie 1.5 uitgegeven door fabrikant F5.

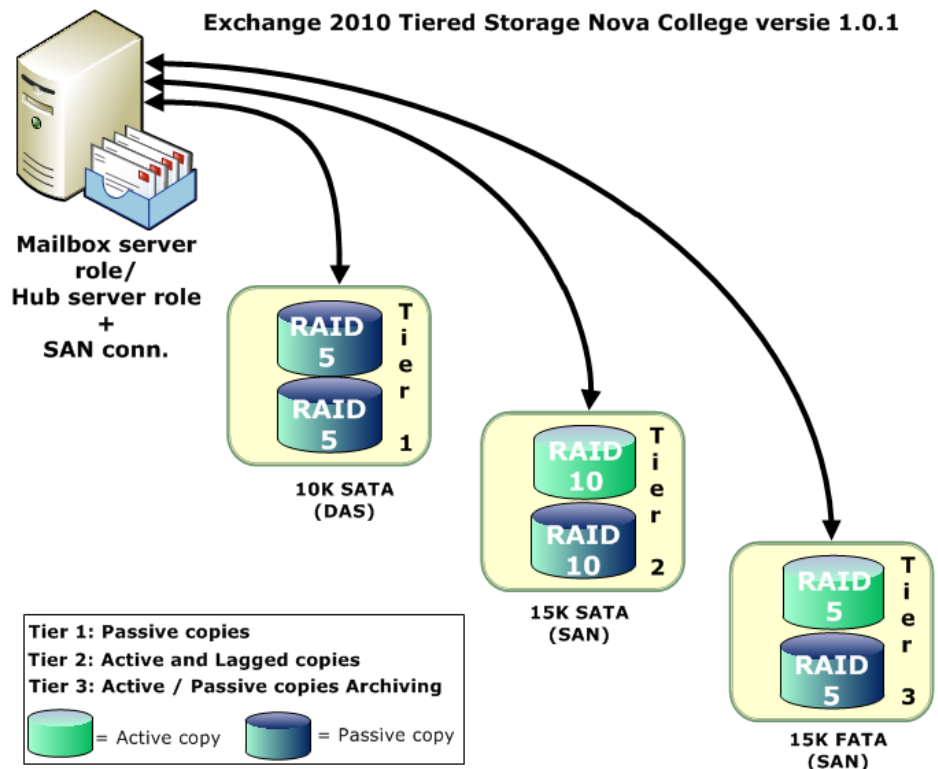


Figuur 15 - DAG

7.1.3 Archivering en Tiered Storage

Archivering is ook één van de functionele eisen. Vaak wordt dit gedaan met 3rd party producten. Exchange 2010 biedt nu ook archiveringsfunctionaliteit, waardoor eindgebruikers via Outlook 2007/2010 en via Outlook Web App toegang hebben tot hun mailbox en hun archief. PST bestanden kunnen gemigreerd worden naar het archief, waardoor het gebruik van PST's niet meer nodig is.

Met de komst van Service Pack 1 voor Exchange 2010 is het mogelijk om de primaire mailbox en archive mailbox in afzonderlijke databases te plaatsen. Dit heeft als voordeel dat er storage tiering kan worden toegepast.



Figuur 16 - Tiered Storage

Met behulp van storage tiering kan een onderscheid gemaakt worden tussen diverse storage lagen. Het Nova College beschikt over een nieuwe SAN oplossing voorzien van SATA drives. In dit SAN bevinden zich ook goedkopere storage lagen voorzien van FATA drives. Door de archive mailboxen te plaatsen in een database op FATA storage kunnen we de duurdere storage laag blijven gebruiken voor de databases die de primaire mailboxen bevatten. Op deze manier maken we onderscheid tussen verschillende storage lagen, zie figuur 16.

7.2 Ontwerp

Microsoft biedt met de introductie van Exchange 2010 vijf serverrollen aan. Van deze vijf rollen zullen we er bij het maken van het ontwerp voor het nieuwe e-mailplatform er maar drie gebruiken.

De twee rollen die niet geïmplementeerd worden zijn:

- De Unified Messaging Role wordt niet gebruikt omdat het Nova College een soortgelijke oplossing van Cisco in gebruik heeft. Het management van het Nova College is tevreden met deze oplossing en heeft besloten de Unified Messaging van Microsoft voornamelijk niet te willen gaan gebruiken;

- De Edge Transport Role wordt niet gebruikt omdat de huidige SMTP mailgateway qua functionaliteit niet afwijkt van deze nieuwe Edge Server van Microsoft. Ook in het kader van het spreiden van antivirus vendors is het raadzaam om deze SMTP mailgateway intact te laten.

Van de drie rollen die wel geïmplementeerd worden kunnen we er twee combineren. De Mailbox Server Role en de Hub Transport Role kunnen we combineren op een server omdat deze rollen zich in hetzelfde netwerk segment bevinden. De CAS servers worden in het kader van "High Availability" achter een loadbalancer geplaatst, dit brengt automatisch met zich mee dat ze ook in een ander netwerksegment komen te staan. Het plaatsen van een server achter een loadbalancer brengt beperkingen met zich mee qua bereikbaarheid, wat het combineren van rollen bemoeilijkt. Bij het combineren van meerdere rollen op één server dient men rekening te houden met de hardware prestaties van de aan te schaffen hardware.

Om te bepalen hoeveel gecombineerde Mailbox/Hub Transport servers we nodig hebben moeten we kijken naar de eisen. Eén van de eisen is 'High Availability' dit houdt dus automatisch in dat er meer dan één server nodig is. Wanneer we uitgaan van twee servers kunnen we gebruik maken van een Database Availability Group met meerdere kopieën van een database. Met maar twee servers is er geen failover mogelijkheid als we één van de twee servers uit moeten schakelen of rebooten vanwege onderhoud. Daarom is het een 'Best Practice' vanuit leverancier Microsoft om bij een 'High Availability' scenario uit te gaan van minimaal drie servers voor de Mailbox Role.

7.2.1 Software

Voor de opbouw van het Exchange 2010 e-mailplatform wordt de volgende software gebruikt:

Type	Omschrijving
Operating System	Windows Server 2008 R2 Enterprise with Service Pack 1 (x64) - DVD (English)
Server	Exchange Server 2010 Service Pack 1 (x64) - DVD (English)
Rollup	Update Rollup 3-v3 for Exchange Server 2010 Service Pack 1 (KB2529939)

Tabel 6 - Software overzicht

7.2.2 Hardware

Wanneer we de door Microsoft beschikbaar gestelde Exchange 2010 Mailbox Server Role Requirements Calculator stap voor stap invullen komen we uit op de volgende aanbevolen waarden per server:

- Recommended RAM Configuration: 32GB
- Mailbox Role CPU Megacycle Requirements: 15297
- Total Database Required IOPS: 979

Wanneer we naar de specificaties van een standaard Nova College HP server kijken zien we het volgende: HP server ProLiant DL380 G6 E5540 2,53 GHz dual quad-core high-efficiency rackserver, 2 x 1 Gbps network adapter x64 type with 8 processor cores. Het aantal megacycles per core van dit type server is 4600 → 8 cores x 4600 = 36800 CPU Megacycles. 36800 CPU megacycles is ruim voldoende, deze server wordt standaard geleverd met 8GB RAM aan intern geheugen. Navraag bij de leverancier leert ons dat hij ook geleverd kan

worden met 32GB RAM intern geheugen. De keuze voor dit type server brengt het voordeel met zich mee dat er van dit type altijd één reserve op voorraad is bij Dienst ICT.

De keuze voor de Mailbox / Hub Transport servers:

3 x HP server ProLiant DL380 G6 E5540 2,53 GHz quad-core 32GB RAM high-efficiency rackserver, 2 x 1 Gbps network adapter.

De hardware specificatie voor de Client Access Servers is eenvoudiger te bepalen. Microsoft raad in hun documentatie op technet.microsoft.com 2 GB RAM per core aan, met een minimum van 8 GB per server. Het geheugen gebruik op een Client Acces server heeft een lineaire relatie met het aantal cliënt connecties en belasting per transactie. Op basis van de huidige aanbevelingen van 2 GB RAM per core processor zal een Client Acces server op zowel het geheugenverbruik als op het processorverbruik evenredig worden belast. De aanbevelingen van Microsoft zijn gebaseerd op de Exchange 2010 feature, RPC Client Access. Deze feature vereist meer RAM en processorkracht om de extra belasting aan te kunnen.

De keuze voor de Client Acces server: 2 x HP server ProLiant DL380 G6 L5420 2,5 GHz quad-core 8 GB high-efficiency rackserver, 2 x 1 Gbps network adapter. Ook deze keuze brengt het voordeel met zich mee dat er van dit type altijd één reserve op voorraad is bij de Dienst ICT.

7.2.3 Waarom geen virtualisatie?

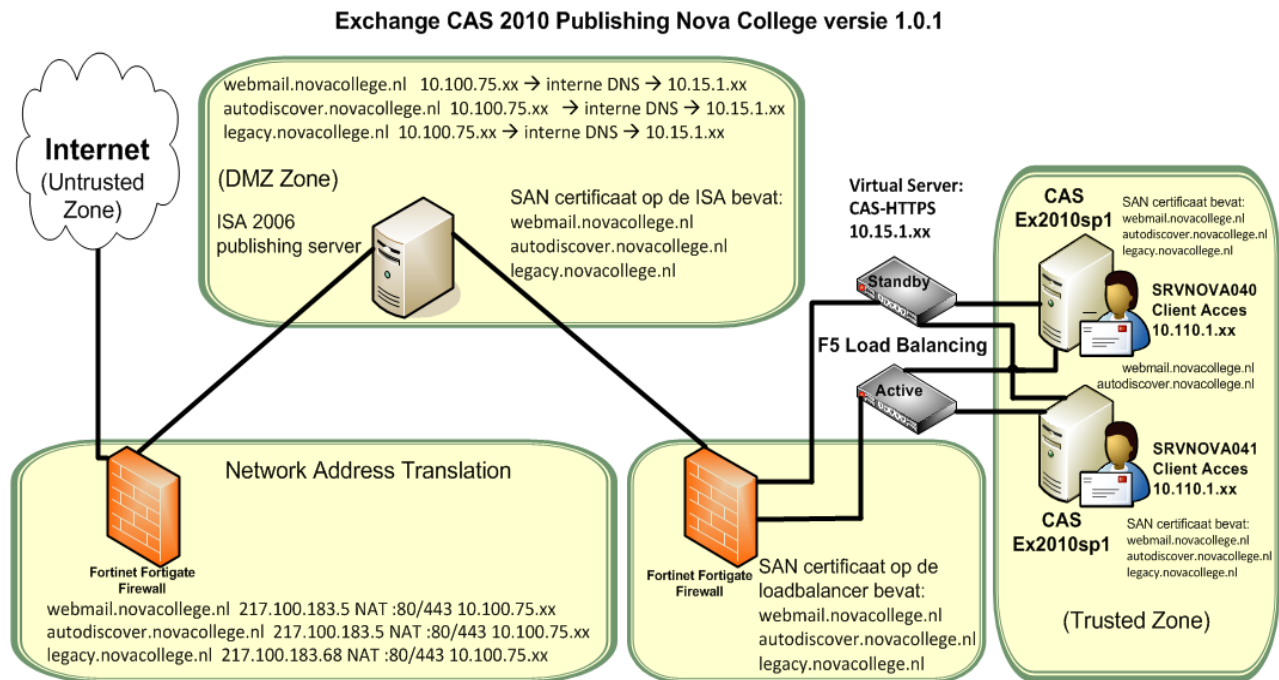
Een trend die al een aantal jaren geleden werd ingezet binnen de ICT wereld is het virtualiseren van servers. Door het kunnen plaatsen van diverse servers op één hardware systeem kunnen kosten worden gereduceerd. Binnen de ICT infrastructuur van het Nova College hebben we ook de beschikking over een virtualisatie platform in de vorm van VMware ESX.

De eerste gedachte bij het maken van een ontwerp ging uit naar het installeren van het nieuwe e-mail platform op dit VMware platform. Echter stuitte we op één belangrijk bezwaar. In de Exchange 2010 Best Practice Guide van Microsoft staat letterlijk dat Exchange 2010's Database Availability Groups (DAGs) geen 'virtual platform high availability' ondersteunen. Microsoft ondersteund de combinatie van Exchange 'High Availability' oplossingen (DAGs) in combinatie met hypervisor-based clustering (VMware) niet. In een notitie citeert Microsoft een quote van VMware: 'VMware ondersteund momenteel geen VMware VMotion or VMware DRS voor Microsoft Cluster nodes'.

Uit bovenstaande uitleg van beide fabrikanten kunnen we afleiden dat een Exchange 2010 Database Availability Group onderwater een cluster server is. Microsoft Cluster nodes worden ten tijde van dit schrijven door VMware nog niet ondersteund.

7.2.4 Exchange CAS 2010 Publishing design

Omdat bij de transitie het een voorwaarde is dat het oude en het nieuwe e-mail platform een periode naast elkaar draaien is het noodzakelijk om te starten met het inrichten van de Client Access Servers. In figuur 17 zien we twee nieuwe Exchange 2010 CAS servers die achter de F5 loadbalancers zijn geplaatst. In de functionele eisen van het netwerk wordt beschreven dat de diverse netwerk componenten in gescheiden zones moeten worden opgenomen. In figuur 17 zien we deze onderverdeling van zones terug.



Figuur 17 - Exchange CAS 2010 Publishing Nova College

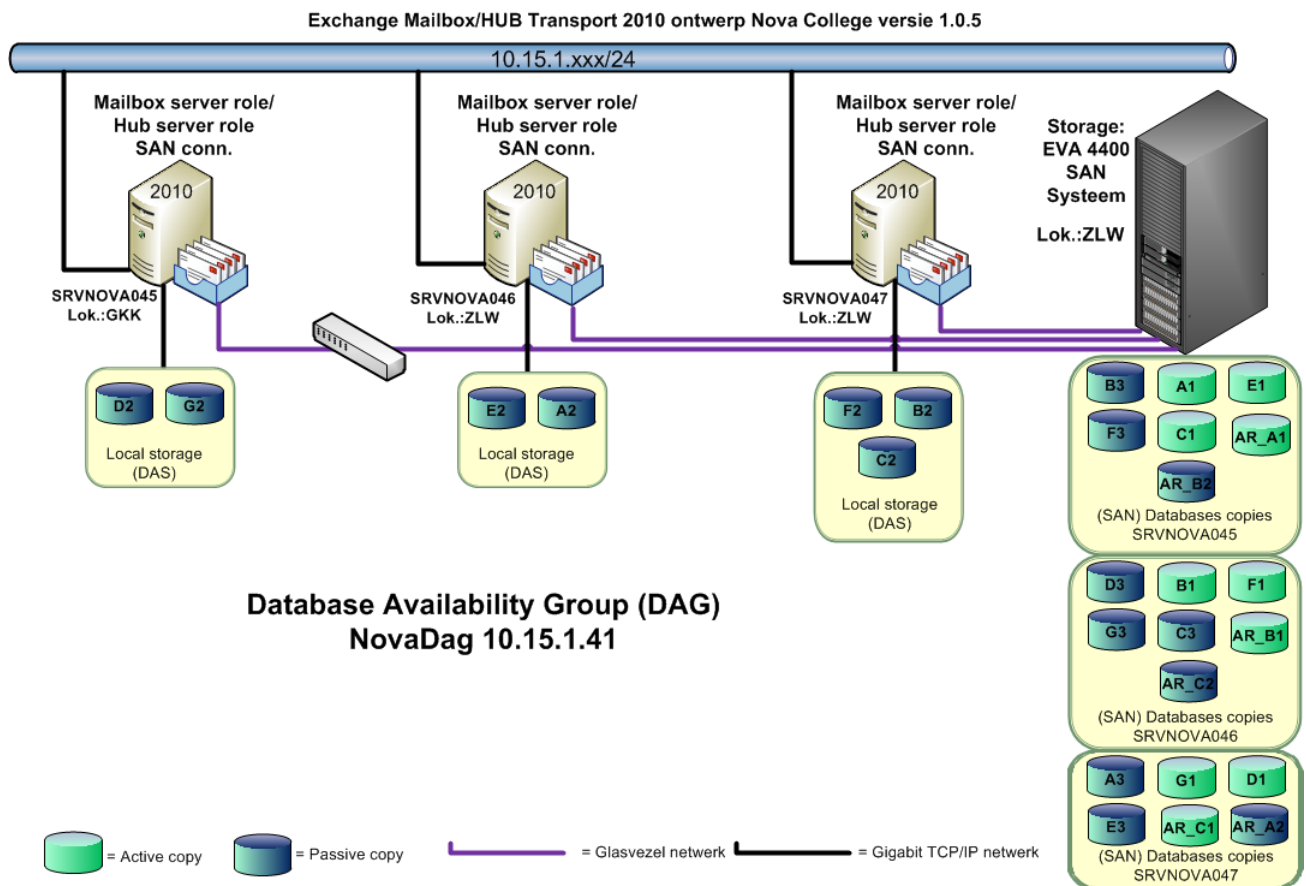
7.2.5 Exchange Mailbox / HUB Server design

In figuur 18 ziet we een weergave van het Mailbox / HUB Server design. Eerder hebben we al bepaald om uit te gaan van drie servers. De keuze voor drie vloeit voort uit de functionele eis om een e-mailplatform met een hoge beschikbaarheid te bouwen.

De Dienst ICT van het Nova College heeft sinds kort de beschikking over een nieuwe storage oplossing in de vorm van een HP EVA 4400 Storage Area Network (SAN) systeem. De connectie vanaf een server naar dit SAN systeem verloopt via het Fibre Channel protocol over een separaat glasvezel netwerk. Het bestaande TCP/IP netwerk wordt door gebruik te maken van dit glasvezel netwerk niet extra belast.

Door gebruik te maken van een Database Availability Group kunnen we meerdere kopieën van een database binnen het e-mailplatform creëren. Een Database Availability Group bestaat altijd uit minimaal twee mailboxservers. Elke kopie van een database is direct gekoppeld aan één mailboxserver. In ons geval kunnen we dus maximaal drie kopieën van een database aanmaken omdat we drie mailboxservers in het ontwerp hebben opgenomen. Wanneer er een kopie wordt gecreëerd binnen de Database Availability Group dient er een activatie preferentie te worden opgegeven. Dit is van belang bij een fail-over van een mailboxserver, want de database met de hoogste preferentie die nog beschikbaar is wordt op dat moment de actieve kopie.

Binnen dit ontwerp is er gekozen om de databases met de hoogste preferentie op het SAN te plaatsen. In de paragraaf 8.3 wordt beschreven wat de reden van deze keuze is.



Figuur 18 - Exchange Mailbox/HUB Transport 2010 ontwerp Nova College

Binnen een Database Availability Group zijn er binnen dit ontwerp drie kopieën van een database beschikbaar:

1. Een actieve kopie die de eindgebruikers benaderen: In figuur 18 worden deze databases met een letter in combinatie met het nummer 1 weergegeven;
2. Een passieve kopie die continue up to date wordt gehouden door middel van log shipping. In figuur 18 worden deze databases met een letter in combinatie met het nummer 2 weergegeven;
3. Een lagged kopie, in figuur 18 worden deze databases met een letter in combinatie met het nummer 3 weergegeven;

Log shipping is een term die door Microsoft wordt gebruikt om aan te geven dat de transactie log files met daarin transacties (bijvoorbeeld de in-en uitgaande e-mail) van de actieve database naar de passieve database wordt gekopieerd, zie figuur 19. Als het bestand gevuld is, wordt deze door de Exchange Replication Service naar de DAG partners gekopieerd om aldaar te worden geïnspecteerd. Na goedkeuring worden de transacties in de log file afgespeeld op de passieve mailbox database. De grootte van deze log file is 1 MB.

Als voorbeeld voor de werking van log shipping nemen we een DAG met twee mailbox servers. In DAG termen is er sprake van een actieve database kopie en een passieve database kopie. De voor de actieve kopie gegenereerde logfiles worden gekopieerd naar de passieve kopie. Op de server die de passieve kopie herbergt worden de logfiles geïnspecteerd en na goedkeuring worden de transacties verwerkt. In figuur 19 staan de aanwezige logfiles vermeld. We zien dat dat de eerste 3 logfiles (EX0000000001-EX0000000003) gekopieerd zijn; EX0000000001-EX0000000002 zijn geïnspecteerd en

verwerkt, EX0000000003 moet nog worden verwerkt. Nieuw binnengekomen transacties worden in het geheugen gebufferd. Als de Limiet (1MB) van de logfile grootte is bereikt worden de transacties weggeschreven in een nieuwe logfile, EX0000000004.

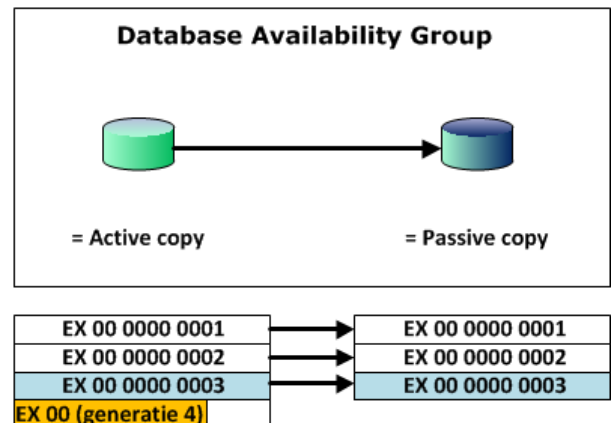
We kunnen uit bovenstaande argumentatie concluderen dat er kans op verlies van informatie is bij uitval van de actieve kopie. Dit komt door het feit dat de Exchange Replication Service alleen volle logfiles repliceert en er dus bij uitval informatie in een deels gevulde logfile verloren kan gaan. Om dit nadelige effect tegen te gaan is het replicatie mechanisme in Exchange 2010 met de komst van Service Pack 1 uitgebreid met continuous replication block mode.

Als block mode geactiveerd is wordt elke transactie direct naar de passieve kopieën gerepliceerd. De transacties worden dus zowel op de actieve als de passieve kopieën gebufferd. Omdat op de passieve en de actieve kopie logfiles worden gegenereerd bij het bereiken van de grootte van 1 MB, kan de passieve kopie het gebruikelijke proces volgen van logfile inspectie en het afspelen van transacties.

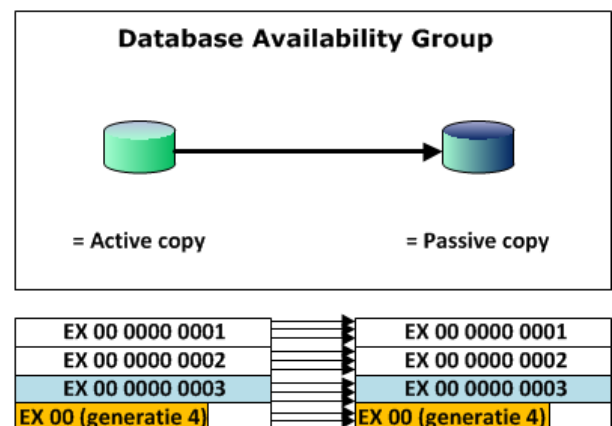
Het voordeel van block mode is dat er minder kans op verlies van informatie is, omdat niet gelogde transacties ook parallel gebufferd worden op de passieve kopieën. In block mode wordt tijdens een fail-over de gebufferde informatie verwerkt als onderdeel van het recovery proces. De gebufferde informatie op de passieve kopie wordt in een (deels gevulde) logfile weggeschreven, waarna reguliere recovery met gebruikmaking van aanwezige logfiles kan plaatsvinden.

Dit proces heeft ook een nadeel. De Exchange Replication Service genereert meer netwerkverkeer aangezien elke transactie direct over het netwerk wordt verzonden in plaats van in batches via een logfile. Het verzenden via een 1 MB logfile is nu eenmaal efficiënter vanwege de lagere overhead. De extra netwerk overhead is relatief gezien een beperkt nadeel voor een nagenoeg instant replicatie.

De schakeling tussen file en block mode gebeurt automatisch. Initieel wordt er replicatie file mode gebruikt. Wanneer de passieve kopieën synchroon zijn gaat de replicatie over op block mode. Als de passieve kopieën te veel af gaan wijken, bijvoorbeeld doordat de mailbox server het te druk heeft en de copy queue teveel logfiles bevat, dan valt de replicatie terug op file mode.



Figuur 19 - Log shipping d.m.v. replicatie file mode



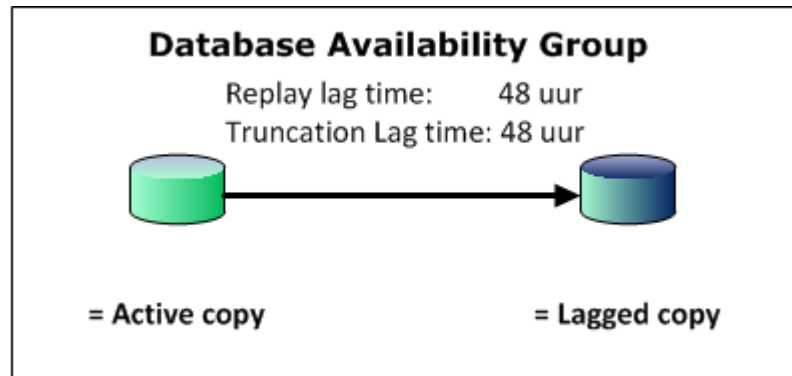
Figuur 20 - Log shipping d.m.v. block mode

7.2.6 Lagged database kopieën

Naast de actieve en passieve databases in een DAG is er binnen dit ontwerp ook voor gekozen een zogenaamde lagged copies te configureren. Met deze lagged copy functionaliteit is het mogelijk om de zojuist genoemde log bestanden vertraagd af te spelen in een passieve database. Hiermee wordt de mogelijkheid gecreëerd om toch een Point-In-

Time recovery uit te voeren wanneer er bijvoorbeeld logische corruptie optreedt in de database. De maximale retentietijd bedraagt 14 dagen. In dit ontwerp is gekozen voor een retentie tijd van twee dagen.

Een andere optie die kan worden ingesteld is de Truncation Lag Time. Deze parameter geeft aan hoe lang de logfiles nog bewaard moeten blijven nadat de logfiles met de passieve database zijn gerepliceerd. Dit kan zeer handig zijn indien je een actieve database wilt herstellen met niet geïnfecteerde logfiles. In dit ontwerp is gekozen voor een bewaartermijn van twee dagen.



Figuur 21 - Lagged Mailbox Database Copy

7.2.7 Indeling databases

Op basis van het huidige aantal eindgebruikers en de nieuw vastgestelde mailboxlimieten per gebruikersgroep kunnen we een indeling maken van de databases. In Exchange 2010 worden de limieten afgedwongen per database, het is dus verstandig de mailboxen van eindgebruikers waarvoor dezelfde limieten gaan gelden in dezelfde database te plaatsen.

In tabel 7 vind u een overzicht van alle databases met daarin de volgende gegevens:

- **Activatie preferentie per server:** preferentie 1 staat voor de actieve database, preferentie 2 staat voor de passieve database en preferentie 3 staat voor de lagged database;
- **DB locatie:** geeft het fysieke pad aan waar de database op de server wordt opgeslagen;
- **Logs:** geeft het fysieke pad aan waar logfiles op de server wordt opgeslagen;
- **Maintenance:** geeft aan of er op de betreffende database onderhoud in de vorm van online defragmentatie moet word uitgevoerd;
- **Limits:** geeft de quota per mailbox aan in de volgorde: Issue warning at, Prohibit send at, Prohibit send and recieve at;
- **Deleted items/mb retention time:** geeft aan welke periode de verwijderde items nog beschikbaar blijven in de mailbox, mb retention time geeft aan hoe lang een mailbox nog beschikbaar blijft indien de bijbehorende account uit de active directory wordt verwijderd.

ROC Nova College Databases indeling Exchange 2010 versie 2.2							
		srvnova045 (GKK)	GB	srvnova046 (ZLW)	GB	srvnova047 (ZLW)	GB
DAS	Omschrijving	Medewerkers A-Z [D2]		Groups-Resource [E2]		Cursisten I-P [F2]	
	DB naam	MBDB_Medewerkers		MBDB_Groups_Resource		MBDB_Cursisten_I-P	
	Activate Preference	2		2		2	
	DB locatie	E:\Medewerkers\Medewerkers.edb	500	I:\Groups_Resource\Groups_Resource.edb	20	M:\Cursisten_I-P\Cursisten_I-P.edb	195
	Logs	F:\Medewerkers\	25	J:\Groups_Resource\Logs	5	N:\Cursisten_I-P\Logs	5
	Maintenance	ja		ja		ja	
	Limits	260-280-300 MB		260-280-300 MB		80-90-100MB	
	Deleted items/mb retention time	14 dagen		14 dagen		14 dagen	
	Omschrijving	Heavy Users [G2]		Cursisten Q-Z [A2]		Cursisten A-H [B2]	
DB naam	MBDB_HeavyUsers		MBDB_Cursisten_Q-Z		MBDB_Cursisten_A-H		
Activate Preference	2		2		2		
DB locatie	S:\HeavyUsers\HeavyUsers.edb	500	O:\Cursisten_Q-Z\Cursisten Q-Z.edb	195	K:\Cursisten_A-H\Cursisten_A-H.edb	195	
Logs	T:\HeavyUsers\	25	P:\Cursisten_Q-Z\Logs	5	L:\Cursisten_A-H\Logs	5	
Maintenance	ja		ja		ja		
Limits	950-975-1000 MB		80-90-100MB		80-90-100MB		
Deleted items/mb retention time	14 dagen		14 dagen		14 dagen		
Omschrijving					Klassikaal [C2]		
DB naam					MBDB_Klassikaal		
Activate Preference					2		
DB locatie					G:\Klassikaal\Klassikaal.edb	5	
Logs					H:\Klassikaal\Logs	5	
Maintenance					ja		
Limits					80-90-100MB		
Deleted items/mb retention time					14 dagen		
SAN	Omschrijving	Klassikaal [C1]		Cursisten A-H [B2]		Cursisten Q-Z [A3]	
	DB naam	MBDB_Klassikaal		MBDB_Cursisten_A-H		MBDB_Cursisten_Q-Z	
	Activate Preference	1		2		3	
	DB locatie	G:\Klassikaal\Klassikaal.edb	5	K:\Cursisten_A-H\Cursisten_A-H.edb	195	O:\Cursisten_Q-Z\Cursisten_Q-Z.edb	195
	Logs	H:\Klassikaal	5	L:\Cursisten_A-H\Logs	5	P:\Cursisten_Q-Z\Logs	5
	Maintenance	ja		ja		ja	
	Limits	80-90-100MB		80-90-100MB		80-90-100MB	
	Deleted items/mb retention time	14 dagen		14 dagen		14 dagen	
	Omschrijving	Groups-Resource [E1]		Cursisten I-P [F1]		Medewerkers A-Z [D1]	
	DB naam	MBDB_Groups_Resource		MBDB_Cursisten_I-P		MBDB_Medewerkers	
	Activate Preference	1		1		1	
	DB locatie	I:\Groups_Resource\Groups_Resource.edb	20	M:\Cursisten_I-P\Cursisten I-P.edb	195	E:\Medewerkers\Medewerkers.edb	500
	Logs	J:\Groups_Resource\	5	N:\Cursisten_I-P\Logs	5	L:\Medewerkers\Logs	25
	Maintenance	ja		ja		ja	
	Limits	260-280-300 MB		80-90-100MB		260-280-300 MB	
	Deleted items/mb retention time	14 dagen		14 dagen		14 dagen	
Omschrijving	Cursisten A-H [B3]		Heavy Users [G3]		Groups-Resource [E3]		
DB naam	MBDB_Cursisten_A-H		MBDB_HeavyUsers		MBDB_Groups_Resource		
Activate Preference	3		3		3		
DB locatie	K:\Cursisten_A-H\Cursisten A-H.edb	195	S:\HeavyUsers\HeavyUsers.edb	500	I:\Groups_Resource\Groups_Resource.edb	20	
Logs	L:\Cursisten_A-H\	5	T:\HeavyUsers\	25	J:\Groups_Resource\Logs	5	
Maintenance	ja		ja		ja		
Limits	80-90-100MB		950-975-1000 MB		260-280-300 MB		
Deleted items/mb retention time	14 dagen		14 dagen		14 dagen		
Omschrijving	Cursisten I-P [F3]		Medewerkers A-Z [D3]		Heavy Users [G2]		
DB naam	MBDB_Cursisten_I-P		MBDB_Medewerkers		MBDB_HeavyUsers		
Activate Preference	3		3		2		
DB locatie	M:\Cursisten_I-P\Cursisten_I-P.edb	195	E:\Medewerkers\Medewerkers.edb	500	S:\HeavyUsers\HeavyUsers.edb	500	
Logs	N:\Cursisten_I-P	5	F:\Medewerkers\Logs	25	T:\HeavyUsers\	25	
Maintenance	ja		ja		ja		
Limits	80-90-100MB		260-280-300 MB		950-975-1000 MB		
Deleted items/mb retention time	14 dagen		14 dagen		14 dagen		
Omschrijving	Cursisten Q-Z [A1]		Klassikaal [C3]		Archive Q-Z [AR_C1]		
DB naam	MBDB_Cursisten_Q-Z		MBDB_Klassikaal		MBDB_Archive_Q-Z		
Activate Preference	1		3		1		
DB locatie	O:\Cursisten_Q-Z\Cursisten_Q-Z.edb	195	G:\Klassikaal\Klassikaal.edb	5	Q:\Archive_Q-Z\Archive_Q-Z.edb	500	
Logs	P:\Cursisten_Q-Z	5	H:\Klassikaal\Logs	5	R:\Archive_Q-Z	25	
Maintenance	ja		ja		ja		
Limits	80-90-100MB		80-90-100MB		80-90-100MB		
Deleted items/mb retention time	14 dagen		14 dagen		14 dagen		
Omschrijving	Archive A-H [AR_A1]		Archive I-P [AR_B1]		Archive A-H [AR_A2]		
DB naam	MBDB_Archive_A-H		MBDB_Archive_I-P		MBDB_Archive_A-H		
Activate Preference	1		1		2		
DB locatie	Q:\Archive_A-H\Archive_A-H.edb	500	Q:\Archive_I-P\Archive_I-P.edb	500	Q:\Archive_A-H\Archive_A-H.edb	500	
Logs	R:\Archive_A-H	25	R:\Archive_I-P	25	R:\Archive_A-H	25	
Maintenance	ja		ja		ja		
Limits	950-975-1000 MB		950-975-1000 MB		950-975-1000 MB		
Deleted items/mb retention time	14 dagen		14 dagen		14 dagen		
Omschrijving	Archive I-P [AR_B2]		Archive Q-Z [AR_C2]				
DB naam	MBDB_Archive_I-P		MBDB_Archive_Q-Z				
Activate Preference	2		2				
DB locatie	Q:\Archive_I-P\Archive_I-P.edb	500	Q:\Archive_Q-Z\Archive_Q-Z.edb	500			
Logs	R:\Archive_I-P	25	R:\Archive_Q-Z	25			
Maintenance	ja		ja				
Limits	950-975-1000 MB		950-975-1000 MB				
Deleted items/mb retention time	14 dagen		14 dagen				

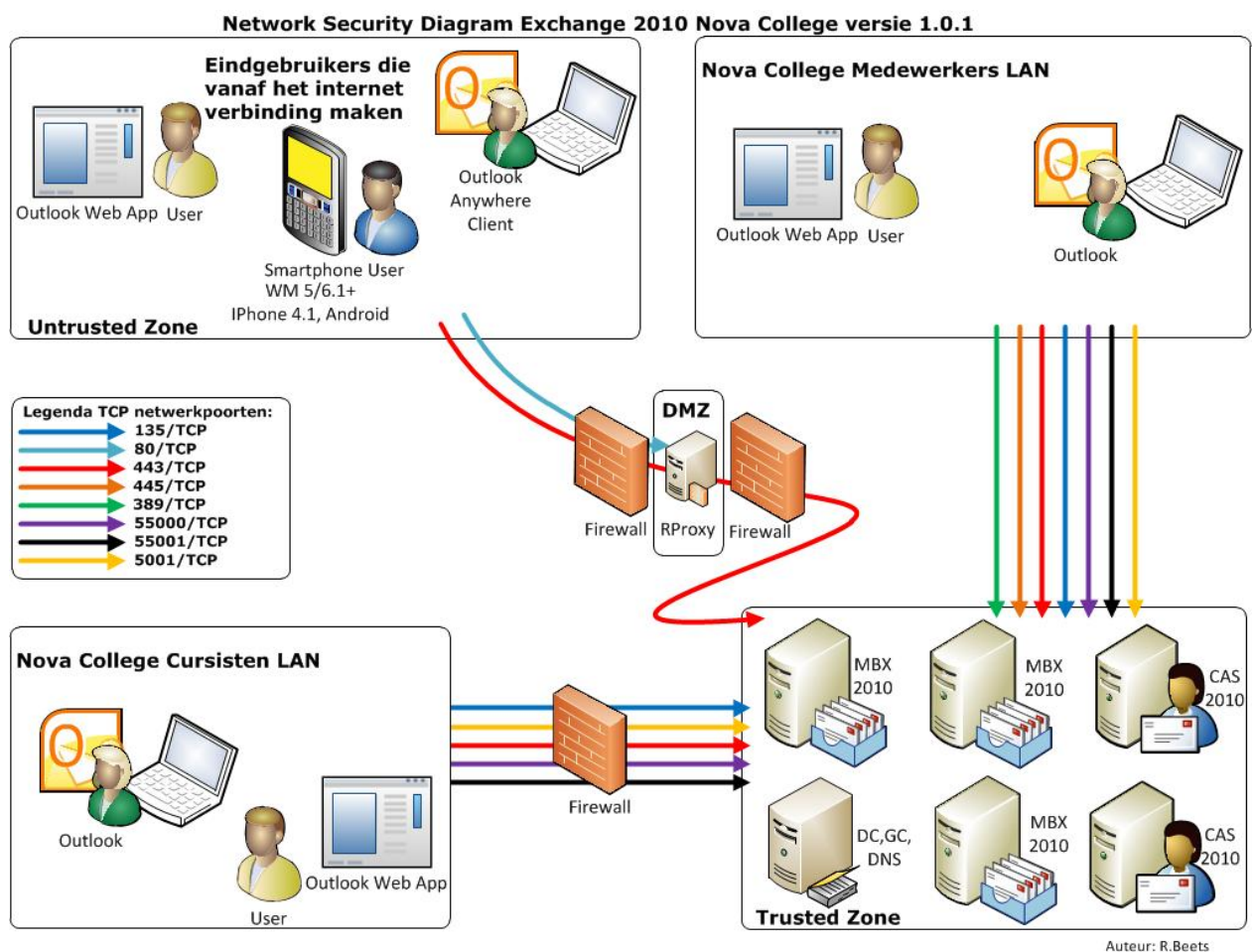
auteur: R.Beets 4-5-2011

auteur: R.Beets 4-5-2011

Tabel 7 - Database indeling

7.3 Beveiliging van het netwerk

In onderstaand diagram wordt aangegeven welke netwerkpoorten er tussen de verschillende LAN segmenten worden gebruikt. Standaard wordt er voor de communicatie tussen de Client Access Servers en de cliënten een dynamische reeks TCP poorten gebruikt. Omdat ook de cursisten met behulp van de mail cliënt Outlook 2007/2010 vanuit het Nova College cursisten LAN verbinding moeten maken met Client Access Servers, zou eigenlijk de gehele dynamische reeks van de poorten 6005 tot 59530 op de firewall open moeten staan. Omdat het openen van een groot aantal poorten op de firewall qua security risico's niet acceptabel is, hebben we naar een alternatief gezocht. Dit alternatief bestaat uit het fixeren van de uitgaande poorten op de Client Access Servers. Door middel van een aanpassing in register van het besturings systeem van de Client Access Servers kunnen de communicatie poorten worden beperkt tot twee, poort 55000 en poort 55001.



Figuur 22 - Network Security Diagram

Vanuit het internet worden alleen sessies via poort 443 (HTTPS) toegestaan. HTTPS is een combinatie van het Hypertext Transfer Protocol met het SSL/TLS protocol en voorziet in het encrypten van de communicatie en veilige identificatie van een webserver.

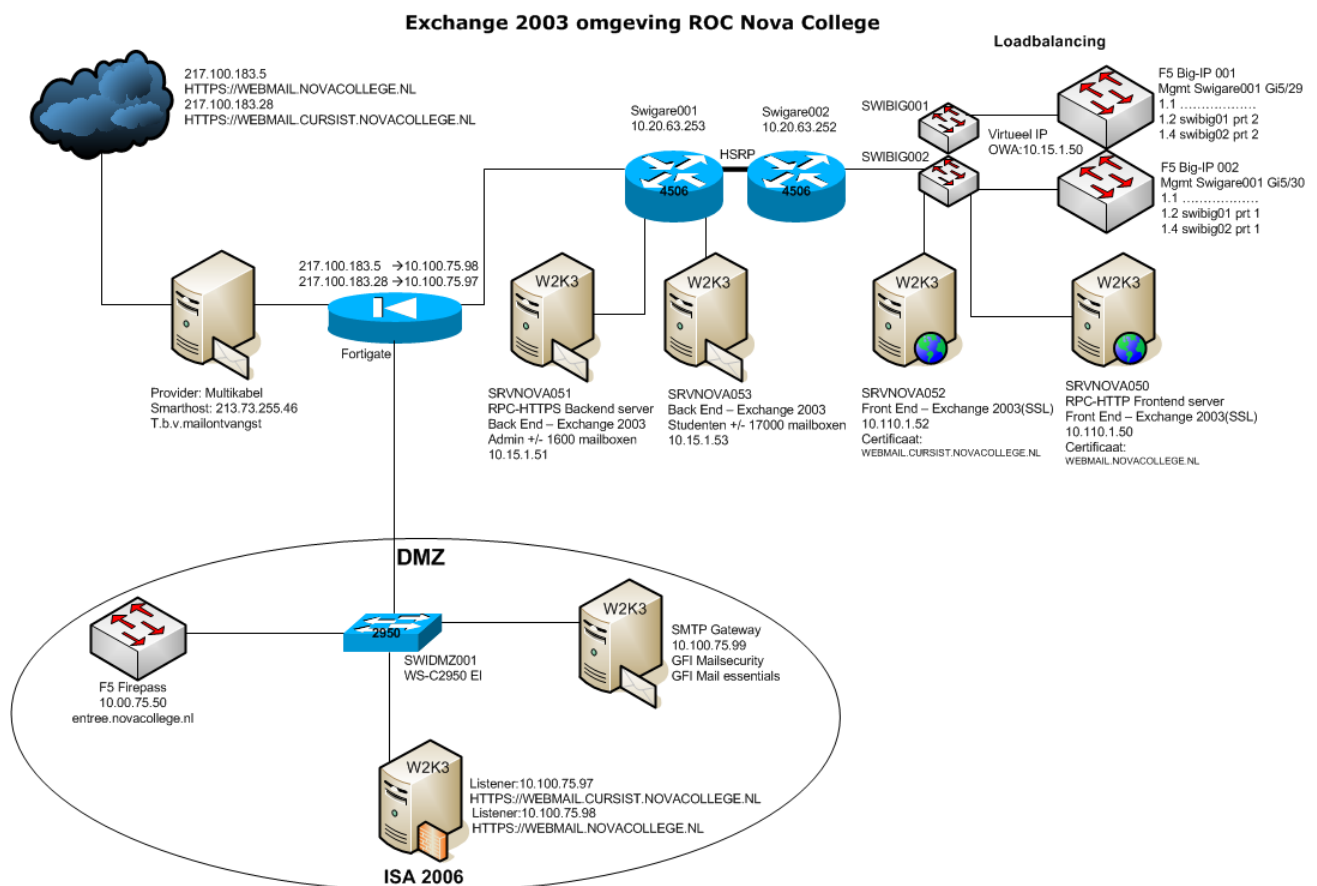
Indien een cliënt verbinding wil maken via poort 80 (HTTP), dan redirect de Reverse Proxy Server in de DMZ de aanvraag naar HTTPS. Intern wordt de redirection van HTTP naar HTTPS door de hardware loadbalancer verzorgd.

Binnen de configuratie van de Client Acces Servers kan per web directory worden aangegeven of er wel of geen encryptie wordt afgedwongen.

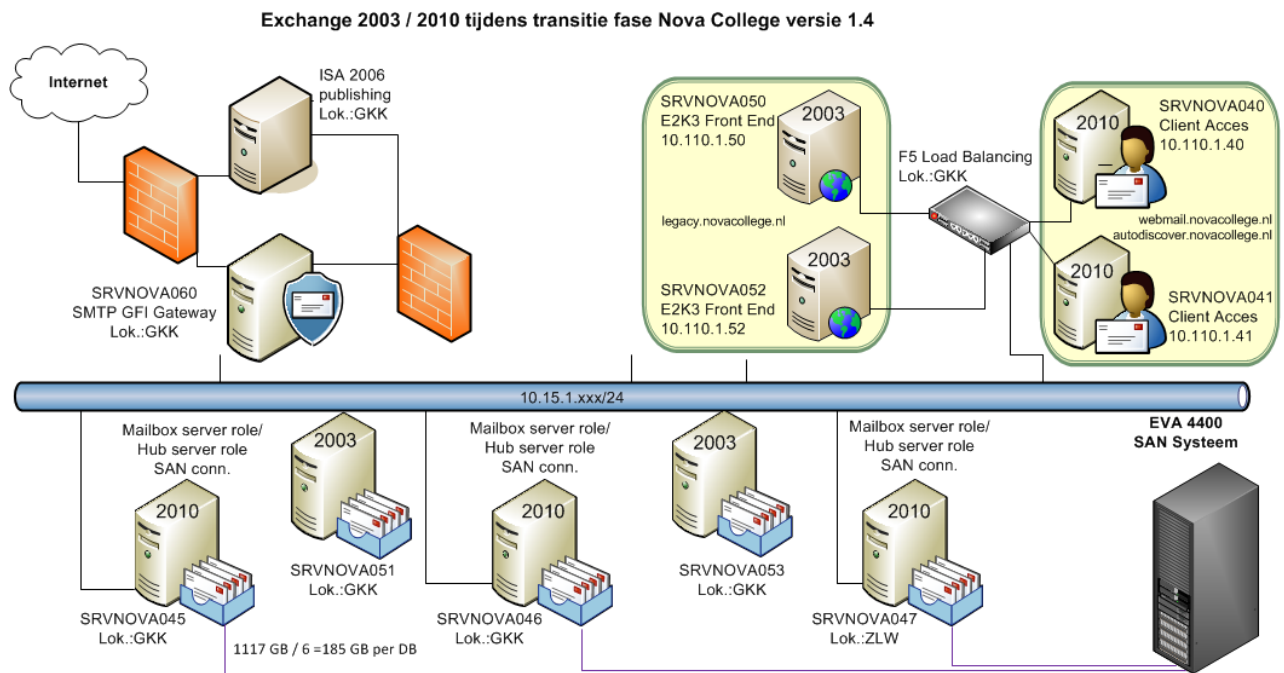
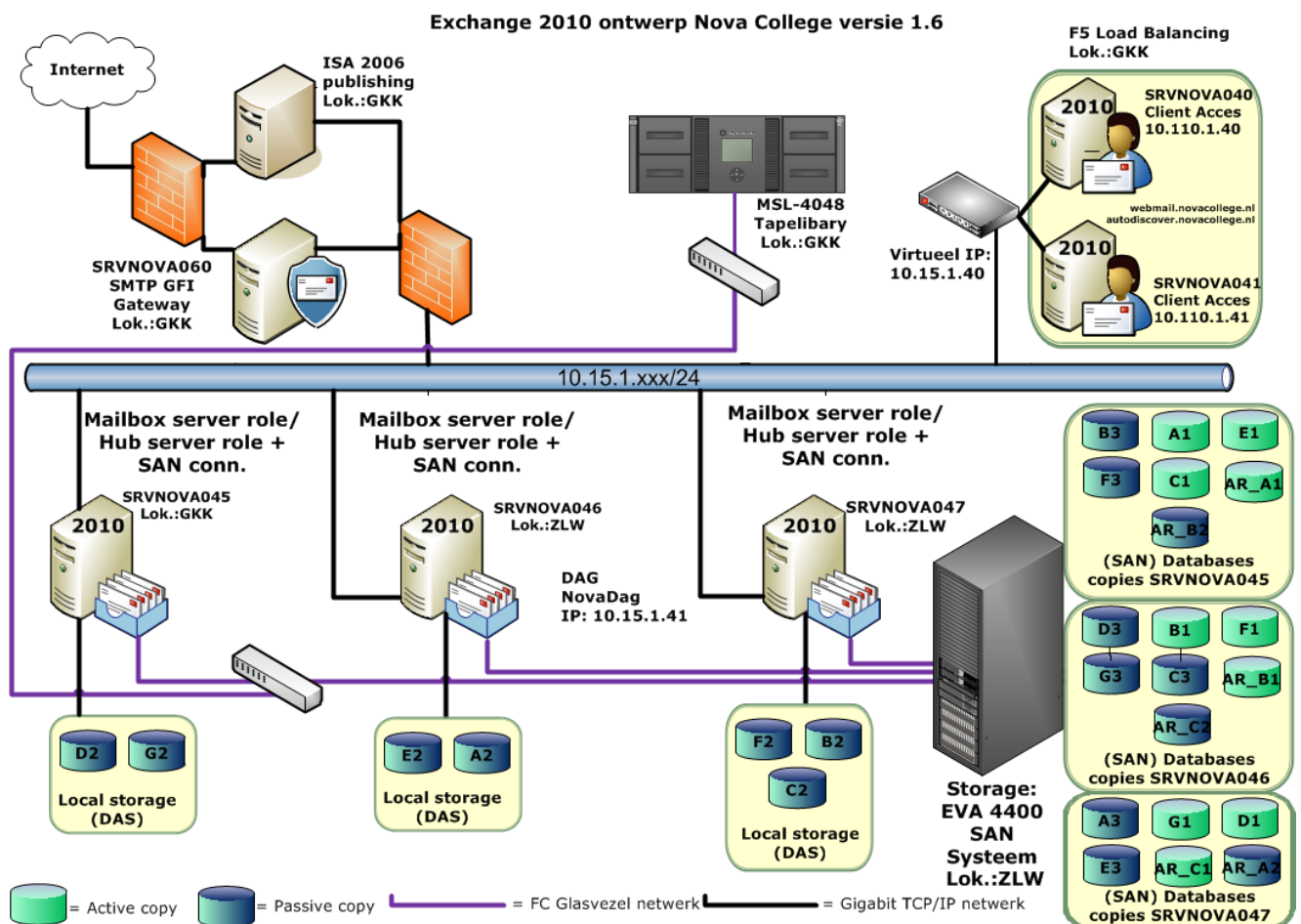
Er dient op alle directories gekozen te worden voor een SSL beveiliging van minimaal 128 bits. De certificaten die het Nova College gebruikt zijn 256 bits SSL certificaten. SSL staat voor Secure Sockets Layer en is tegenwoordig de meest gebruikte manier voor het aangaan van beveiligde elektronische transacties op het internet. De methode gebruikt public key cryptografie om beveiligd de sessiesleutel te genereren en uit te wisselen. De sessiesleutel wordt gebruikt voor symmetrische versleuteling. De SSL-functies in een Exchange webserver kunnen niet gebruikt worden voordat er een servercertificaat is aangekocht bij een Certificate Authority en is configureert voor de betreffende websites.

7.4 Overzicht fases

Indien we voorgaande stadia van het ontwerp en de uitgangssituatie op een rijtje zetten komen we tot de volgende drie overzichten:



Figuur 23 - Het huidige e-mail platform

**Figuur 24 - Het e-mail platform tijdens de transitie fase****Figuur 25 - Het e-mail platform na de transitiefase**

8 Implementatieplan en beschrijving

8.1 Implementatieplan

De implementatie zal uit verschillende fases bestaan. Er zal worden gestart met het implementeren van het ontwerp in een testomgeving (Proof of Concept). Deze testomgeving is qua functionaliteit een kopie van de ICT productieomgeving die bij het Nova College in gebruik is. De gebruikte hardware in de testomgeving wijkt echter af in vergelijking met de productie omgeving. De geïnstalleerde systemen in de testomgeving blijven in de toekomst beschikbaar.

De implementatie bestaat uit verschillende fasen:

Exchange 2010 High Level Deployment Plan	
1.	Huidige infrastructuur controleren
2.	Ontwerp eisen verzamelen
3.	Bouwen Exchange 2010 Servers
4.	Active Directory Preparatie
5.	Installatie
6.	Client Acces Server Configuratie
7.	Mailbox/HUB Server Configuratie
8.	Testen
9.	Mailboxen verplaatsen
10.	Post transitie fase
11.	Deinstalleren Exchange 2003

Tabel 8 - Implementatieplan

8.2 Beschrijving

8.2.1 Huidige infrastructuur controleren

- 2 Windows 2008 R2 DC
 - 2 Windows 2008 R2 GC
 - 4 Exchange 2003 servers
 - 1 Windows 2008 R2 SMTP gateway
 - 1 Windows 2003 SP2 ISA 2006 SP1 server*
- *(ISA 2006 ondersteund geen SAN certificaten)

Alle servers zijn gesitueerd in één site maar in verschillende subnetten.
De cliënten gebruiken Outlook 2007 en 2010.

8.2.2 Ontwerp eisen verzamelen

- 3 Exchange 2010 Hub/MBX servers in een enkelvoudige DAG
- Hub/MBX rol gecombineerd
- 2 Exchange 2010 CAS servers achter hardware loadbalancer
- 5 Exchange 2010 servers in "main site"
- Enkele DAG Active Passive

- FSW op CAS

8.2.3 Bouwen Exchange 2010 Servers

- Staging fysieke hardware
- Aanmaken LUN's op DAS
- Aanmaken LUN's op SAN
- Installatie Windows 2008 R2
- Installatie SP1 for Win2008 R2
- Installatie Windows Updates
- Toevoegen aan het novacollege.intern domein
- Installatie Exchange 2010 filter pack
- Installatie rollen en dot net framework 3.5 feature vanaf de server manager
- Teaming van de netwerk adapters
- Toewijzen van statische IP adressen

8.2.4 Active Directory Preparatie

- Voer de ExBPA uit op een Exchange 2003 server en bekijk de resultaten
- Los de gerapporteerde problemen in ExBPA op
- Log in met een account met adminschemarechten
- Voer de onderstaande commando's uit op een Ex2010SP1 machine die de setup bestanden uitgepakt heeft staan
- Setup /pl
- Setup /ps
- Setup /pd
- Setup /pad

8.2.5 Installatie

- Pak het Ex2010Sp1 setup bestand uit, en klik op setup.exe
- Klik op Automatically install all windows role and features necessary for ex2010 setup
- Vul webmail.novacollege.nl in als external name space
- Installeer de Hub/Mailbox/CAS rollen
- Installeer Forefront protection for Exchange

8.2.6 Client Acces Server Configuratie

- Maak CAS array
- Configureren F5 HLB
- Maak CSR voor SAN cert
- Ontvang SAN cert van externe CA
- Import SAN cert via IIS
- DNS wijzigingen voor legacy OWA url
- Configureren OWA redirection voor Ex2003 gebruikers
- Open poorten van Ex2010 servers om firewall (indien nodig)
- Vervang de interne OWA met webmail.novacollege.nl op CAS
- Configureren autodiscover uri parameter om naar HLB te wijzen op CAS
- ISA-server configureren regels webpublicatie
- ISA regels overschakelen

8.2.7 Mailbox/HUB Server Configuratie

- Verwijder standaard Exchange 2010 DBs

- Maken en configureren nieuwe DB in Ex2010
- Maak DAG / FSW op CAS
- Maak DAG netwerk en Statische routes
- Voeg DB in DAG
- Maak de Public folder database
- Maak test mailboxen in Ex2003 en 2010
- Configureren retention policies and tags
- Installeer Back-up en testen
- Maak Receive connector voor SMTP-relay
- Wijzig Offline adresboek

8.2.8 Testen

- Connectiviteit test met CAS-array
- MAPI testen met Outlook 2003/2007/2010
- OWA OA EAS met smartphones testen
- DAG Replicatie testen
- Back-up terugzetten testen
- Test SMTP-relay-toepassingen
- Test mailbox verplaatsingen
- Test inkomende en uitgaande e-mailstroom en connectiviteit
- Test smartphones e-connectiviteit, het zoeken naar adressen en agenda sync na de migratie
- Test interne externe e-mailstroom

8.2.9 Mailboxen verplaatsen

- Transitie: mailboxen verplaatsen
- Pilot transitie
- Tier 1 mailbox verplaatsen
- Oplossen mailbox migratie problemen
- Tier 2 postvakverplaatsing
- Speciale mailbox verplaatsen
- Definitieve mailbox verplaatsing

8.2.10 Post transitie fase

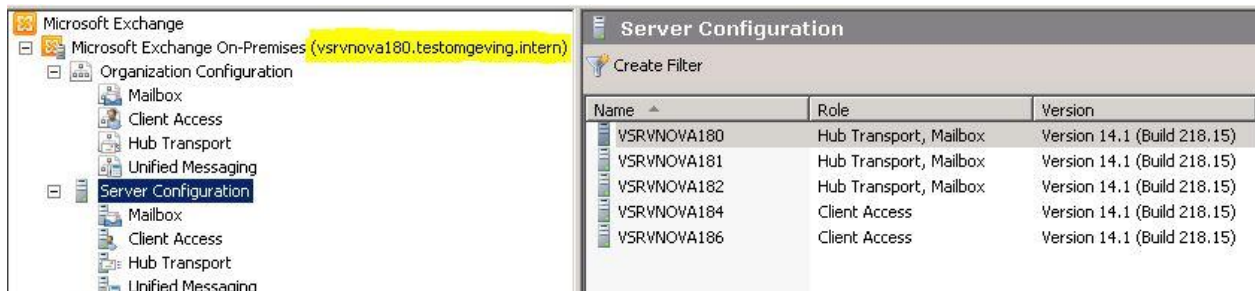
- Creëer Send connectors op de Ex2010 HUB servers
- Configureer TLS en verander de cost
- Routeer binnenkomende mail direct naar Ex2010
- Verwijder internet connector op Ex2003
- Update standaard email adres policy
- Verplaats replica van public folders naar Ex2010
- Verwijder Ex2003 openbare mappen

8.2.11 Deinstalleren Exchange 2003

- Tijdelijk uitzetten Ex2003 Servers
- Oplossen van problemen die verband houden met Exchange 2003
- Verwijder de Recipient Update service van Ex2003
- Verwijder de Interop routing-groep
- Dismounten en verwijderen van de Ex2003 DBs
- Verwijderen van Exchange 2003
- Uitzetten van de Windows 2003 servers

8.3 Proof of Concept

In de testomgeving is het volledige technische ontwerp geïmplementeerd aan de hand van het stappenplan uit hoofdstuk 8.2 "Implementatieplan en beschrijving". Tijdens deze implementatie zijn installatiehandleidingen gemaakt die tijdens de implementatie in de productie omgeving zijn gebruikt. Deze handleidingen vindt u in de bijlagen terug.



The screenshot shows the Microsoft Exchange Server Configuration console. On the left, the 'Server Configuration' node is selected under 'Microsoft Exchange On-Premises (vsvnova180.testomgeving.intern)'. The main pane displays a table of servers:

Name	Role	Version
VSRVNOVA180	Hub Transport, Mailbox	Version 14.1 (Build 218.15)
VSRVNOVA181	Hub Transport, Mailbox	Version 14.1 (Build 218.15)
VSRVNOVA182	Hub Transport, Mailbox	Version 14.1 (Build 218.15)
VSRVNOVA184	Client Access	Version 14.1 (Build 218.15)
VSRVNOVA186	Client Access	Version 14.1 (Build 218.15)

Figuur 26 - Overzicht servers testomgeving

Aan de hand van een puntenlijst zijn alle functionaliteiten getest. Deze puntenlijst heeft dezelfde opzet als de lijst die voor de oplevering van de productieomgeving is gebruikt. Deze puntenlijst is terug te vinden in bijlage D.

8.4 Het testen van hardware en databases

Een cruciaal onderdeel tijdens de implementatie van een Exchange 2010 e-mailplatform is het testen van het maximaal haalbare aantal IOPS van de gebruikte servers in combinatie met de daaraan gekoppelde storage oplossing. IOPS staat voor (Input/Output Operations Per Second, en wordt uitgesproken als i-ops). Deze test wordt na fase 3 'Bouwen Exchange 2010 Servers' uitgevoerd. In de ontwerpfase hebben we met behulp van de *Exchange 2010 Mailbox Server Role Requirements Calculator Versie 14.4* een berekening gemaakt van het aantal benodigde IOPS per server. In de onderstaande tabellen worden de waardes ingevuld per gebruikersklasse (Tier).

Bij het Nova College kunnen we globaal drie gebruikersgroepen onderscheiden:

- Tier 1: de administratieve medewerkers en docenten;
- Tier 2: de cursisten;
- Tier 3: de unit directeuren, diensthoofden, opleidingsmanagers, brede docenten en andere medewerkers/diensten die vanwege hun werkzaamheden grote hoeveelheden mails verwerken.

Tier-1 User Mailbox Configuration	Value
Total Number of Tier-1 User Mailboxes / Environment	1750
Projected Mailbox Number Growth Percentage	10%
Total Send/Receive Capability / Mailbox / Day	50 messages
Average Message Size (KB)	75
Mailbox Size Limit (MB)	300
Personal Archive Mailbox Size Limit (MB)	1024
Deleted Item Retention Window (Days)	14
Single Item Recovery	Enabled
Calendar Version Storage	Enabled
IOPS Multiplication Factor	1,00
Megacycles Multiplication Factor	1,00
Desktop Search Engines Enabled (for Online Mode Clients)	No
Predict IOPS Value?	Yes
Tier-1 User IOPS / mailbox	0,00
Tier-1 Database Read-Write Ratio	3:2

Tabel 9 - Tier 1 Gebruikersprofiel

Tier-2 User Mailbox Configuration	Value
Total Number of Tier-2 User Mailboxes / Environment	20000
Projected Mailbox Number Growth Percentage	10%
Total Send/Receive Capability / Mailbox / Day	50 messages
Average Message Size (KB)	50
Mailbox Size Limit (MB)	100
Personal Archive Mailbox Size Limit (MB)	0
Deleted Item Retention Window (Days)	14
Single Item Recovery	Disabled
Calendar Version Storage	Disabled
IOPS Multiplication Factor	1,00
Megacycles Multiplication Factor	1,00
Desktop Search Engines Enabled (for Online Mode Clients)	No
Predict IOPS Value?	Yes
Tier-2 User IOPS / mailbox	0,00
Tier-2 Database Read-Write Ratio	3:2

Tabel 10 - Tier 2 Gebruikersprofiel

Tier-3 User Mailbox Configuration	Value
Total Number of Tier-3 Mailboxes / Environment	250
Projected Mailbox Number Growth Percentage	10%
Total Send/Receive Capability / Mailbox / Day	100 messages
Average Message Size (KB)	150
Mailbox Size Limit (MB)	1024
Personal Archive Mailbox Size Limit (MB)	2048
Deleted Item Retention Window (Days)	14
Single Item Recovery	Enabled
Calendar Version Storage	Enabled
IOPS Multiplication Factor	1,00
Megacycles Multiplication Factor	1,00
Desktop Search Engines Enabled (for Online Mode Clients)	No
Predict IOPS Value?	Yes
Tier-3 User IOPS / mailbox	0,00
Tier-3 Database Read-Write Ratio	3:2

Tabel 11 - Tier 3 Gebruikersprofiel

Exchange Environment Configuration	Value
Global Catalog Server Architecture	64-bit
Server Multi-Role Configuration (MBX+CAS+HT)	No
High Availability Deployment	Yes
Number of Mailbox Servers Hosting Active Mailboxes / DAG	3
Number of Database Availability Groups	1
Mailbox Database Copy Configuration	Value
Total Number of HA Database Copy Instances (Includes Active Copy) within DAG	2
Total Number of Lagged Database Copy Instances within DAG	1
Number of HA Database Copy Instances Deployed in Secondary Datacenter	0
Number of Lagged Database Copy Instances in Secondary Datacenter	0
Exchange Data Configuration	Value
Data Overhead Factor	20%
Mailbox Moves / Week Percentage	1%
Dedicated Maintenance / Restore LUN?	Yes
LUN Free Space Percentage	20%
Log Shipping Network Compression	Enabled
Log Shipping Compression Percentage	30%
Exchange I/O Configuration	Value
I/O Overhead Factor	20%
Additional I/O Requirement / Server	0,00

Tabel 12 - Server voorkeuren

Indien de bovenstaande tabellen in de *Exchange 2010 Mailbox Server Role Requirements Calculator* worden ingevuld geeft de calculator een aantal aanbevelingen. In tabel 13 kunnen we zien dat het aantal Mailbox Role CPU Megacycle Requirements 15297 bedraagt. Deze waarde hebben we eerder gebruikt om de hardware te selecteren. In tabel 14 vinden we een andere belangrijke waarde namelijk de Total Database Required IOPS per server: 979.

Server Configuration	/ Primary Datacenter Server (Single Failure)
Recommended RAM Configuration	32 GB
Server Total Available Adjusted Megacycles	592474
Mailbox Role CPU Megacycle Requirements	15297
Mailbox Role CPU Utilization	3%
Possible Storage Architecture	RAID

Tabel 13 - Mailbox Server Requirements

Host IO Requirements	/ Database	/ Server
Total Database Required IOPS	245	979
Total Log Required IOPS	54	210
Database Read I/O Percentage	60%	--

Tabel 14 - Host IO Requirements

Om het aantal IOPS per server te testen maken we gebruik van de *Microsoft Exchange Jetstress 2010* tool. Met deze tool kunnen we veel I/O genereren en zo het effect nabootsen van een druk belaste Exchange database. Daarnaast houdt deze tool tijdens het uitvoeren

van een test een Performance monitor en een Event viewer bij. Op deze manier kunnen we achteraf zien wat het effect van de test op de server geweest is.

Het gebruik van de tool vergt wel enige configuratie op de betreffende mailboxservers. In de *Jetstress Field Guide v1.0.0.6* staat beschreven hoe alles ingesteld moet worden. Bij het uitvoeren van een stresstest met de *Jetstress 2010* tool worden een aantal parameters zoals de storagelocatie en het aantal te gebruiken threads gevraagd. In de Field Guide wordt aangeraden om met één thread per database te beginnen. En successievelijk het aantal threads op te bouwen totdat de I/O Database Reads Average Latency (msec) boven de 20 msec uitkomt. Deze 20 msec is de bovengrens voor het goed kunnen functioneren van een Exchange database.

Microsoft Exchange **Jetstress 2010**
Performance Test Result Report
Test Summary
Overall Test Result **Pass**
Machine Name SRVNOVA045
Test Description **test3**
Jetstress Version 14.01.0225.017
ESE Version 14.01.0270.001
Operating System Windows Server 2008 R2
Enterprise (6.1.7600.0)
Database Sizing and Throughput
Achieved Transactional I/O per Second:
690,759
Jetstress System Parameters
Thread Count 3 (per database)

Transactional I/O Performance		
MSEExchange Database ==> Instances	I/O Database Reads Average Latency (msec)	I/O Database Writes Average Latency (msec)
Instance384.1	18,448	94,544
Instance384.2	14,027	76,186
Instance384.3	7,662	13,666
Instance384.4	7,603	12,737
Instance384.5	7,656	12,969
Instance384.6	7,683	11,990
Instance384.7	8,310	11,979
Instance384.8	13,837	74,269

Tabel 15 – Test3

In tabel 15 ziet u de uitkomst van test3 met een belasting van drie threads op de databases. De overall uitslag is een Pass, wanneer we kijken naar de behaalde IOPS zien we een waarde van 690. Deze waarde is volgens eerdere berekeningen niet voldoende.

Als we kijken naar de oorzaak zien we dat drie databases de oorzaak zijn van deze lage score. De databases met de instance nummers 384.1 en 384.2 blijken bij drie threads al bijna op de maximale Reads Average Latency van 20 msec te zitten. Ook de database met instance nummer 384.8 heeft een afwijkende score. Wanneer we kijken naar de fysieke plaatsing van de databases zien we het volgende patroon:

MSEExchange Database ==> Instances	Fysieke Plaatsing Database	I/O Database Reads Average Latency (msec)	I/O Database Writes Average Latency (msec)
Instance384.1	DAS (RAID5)	18,448	94,544
Instance384.2	DAS (RAID5)	14,027	76,186
Instance384.3	SAN (RAID10)	7,662	13,666
Instance384.4	SAN (RAID10)	7,603	12,737
Instance384.5	SAN (RAID10)	7,656	12,969
Instance384.6	SAN (RAID10)	7,683	11,990
Instance384.7	SAN (RAID10)	8,310	11,979
Instance384.8	SAN (RAID5)	13,837	74,269

Tabel 16 – Fysieke plaatsing DBs

In tabel 16 zien we dat de databases die fysiek op DAS (lokaal op de server) zijn geplaatst, aan hun maximum qua prestaties zitten. De database instance 384.8 die fysiek op het SAN in een RAID5 FATA configuratie staat, presteert gemiddeld.

Om te zien of de huidige configuratie het aantal van 10 Threads aan kan, voeren we wederom een test uit: test10. De overall uitslag is een Fail, wanneer we kijken naar de behaalde IOPS zien we wel een waarde van 1324. Maar deze waarde mogen we niet gebruiken omdat de een aantal databases boven de maximale Reads Average Latency van 20 msec zitten.

Microsoft Exchange **Jetstress 2010**

Performance Test Result Report

Test Summary

Overall Test Result **Fail**

Machine Name SRVNOVA045

Test Description **test10**

Jetstress Version 14.01.0225.017

ESE Version 14.01.0270.001

Operating System Windows Server 2008 R2

Enterprise (6.1.7600.0)

Database Sizing and Throughput

Achieved Transactional I/O per Second:

1324,296

Jetstress System Parameters: Thread

Count 10 (per database)

Transactional I/O Performance

MSExchange Database ==> Instances	I/O Database Reads Average Latency (msec)	I/O Database Writes Average Latency (msec)
Instance6800.1	43,441	178,826
Instance6800.2	28,469	140,631
Instance6800.3	9,248	42,998
Instance6800.4	9,122	41,891
Instance6800.5	9,198	41,773
Instance6800.6	9,307	40,665
Instance6800.7	9,649	39,323
Instance6800.8	28,302	143,065

Tabel 17 – Test10

Om te kunnen bepalen of we de aanbevolen waarde van 979 IOPS kunnen halen voeren we test12 uit met alleen databases in een RAID10 configuratie die fysiek op het SAN staan. De overall uitslag is een Pass, wanneer we kijken naar de behaalde IOPS zien we een waarde van 4289. De maximale Reads Average Latency zit nog ruim onder de 20 msec.

Microsoft Exchange **Jetstress 2010**

Performance Test Result Report

Test Summary

Overall Test Result **Pass**

Machine Name SRVNOVA045

Test Description **test12**

Jetstress Version 14.01.0225.017

ESE Version 14.01.0270.001

Operating System Windows Server 2008

R2 Enterprise (6.1.7600.0)

Database Sizing and Throughput

Achieved Transactional I/O per Second:

4289,691

Jetstress System Parameters: Thread Count 12 (per database)

Transactional I/O Performance

MSExchange Database ==> Instances	I/O Database Reads Average Latency (msec)	I/O Database Writes Average Latency (msec)
Instance5868.1	11,787	16,084
Instance5868.2	14,542	15,462
Instance5868.3	11,133	13,835
Instance5868.4	11,188	12,529
Instance5868.5	11,248	11,059

Tabel 18 – Test12

8.4.1 Conclusie storage tests

Wanneer we alle testen in ogenschouw nemen kunnen we het volgende concluderen:

- Databases op Direct Attached Storage (DAS) in een RAID5 configuratie zijn in de geteste hardware configuratie niet geschikt als actieve database in ons Exchange 2010 ontwerp. Daarentegen kunnen ze prima functioneren als passieve copy;
- Databases op een Storage Area Network (SAN) in een RAID10 SATA configuratie zijn in de geteste hardware configuratie uitermate geschikt als actieve database in ons Exchange 2010 ontwerp;
- Databases op een Storage Area Network (SAN) in een RAID5 FATA configuratie zijn in de geteste hardware configuratie uitermate geschikt als actieve archief database in ons Exchange 2010 ontwerp.

Naar aanleiding van bovenstaande testresultaten is het ontwerp uit paragraaf 7.2.5 "Exchange Mailbox / HUB Server design" op bepaalde punten aangepast.

9 Monitoring uptime

In het plan van aanpak is gesproken over de verwachte uptime van het nieuwe platform. Het volgende is destijds geformuleerd:

Bij het ontwerp van het nieuwe e-mailplatform moet rekening worden gehouden met de volgende eisen:

- *Het nieuwe systeem moet een betrouwbaar platform worden. Het doel is om een jaarlijkse beschikbaarheid van minimaal 99,5% te kunnen aanbieden;*
- *De verwachte MTTR (Mean Time Till Repair) binnen het service window (kantooruren) mag niet boven de 2 uur uitkomen;*
- *Indien we uitgaan van vier storingen per jaar komt de verwachte MTBF (Mean Time Between Failures) op een gemiddelde periode van 2188 uur (± 3 maanden).*

Het huidige e-mailplatform is nu regelmatig offline. Dit heeft te maken met onder meer:

- *Werkzaamheden aan het Storage Area Network (uitbreiding en firmware updates t.b.v. de dataopslag);*
- *Werkzaamheden aan de servers (updates).*

Het nieuwe ontwerp zal erin moeten voorzien dat downtime als gevolg van genoemde werkzaamheden tot een minimum kan worden beperkt.

9.1 Monitoring

Om het nieuwe platform te kunnen monitoren is er op elke nieuwe Exchange 2010 Server een SCOM cliënt geïnstalleerd. SCOM staat voor System Center Operations Manager en is een product van Microsoft. SCOM monitort een server op diverse punten, waaronder diskfouten en beschikbare ruimte op de disks.

Met behulp van SCOM is het ook mogelijk om elke vijf minuten een test te laten uitvoeren met betrekking tot de Outlook Connectivity. Deze test kijkt of de e-mailomgeving nog goed bereikbaar is (end-to-end). De uitkomst van deze testresultaten wordt gebruikt om een periodiek overzicht te publiceren van de uptime van het platform.

10 Conclusies en aanbevelingen

De verschillen in architectuur tussen Exchange 2003 en Exchange 2010 zijn groot. Ongeacht de omvang van het bestaande Exchange 2003 platform is het aan te raden om de transitie zorgvuldig te plannen. De volgorde bij een dergelijk project is cruciaal voor het slagen ervan. Wanneer het idee opgevat wordt om over te gaan naar een ander e-mailplatform, is het aan te bevelen om de volgende volgorde van handelen aan te houden:

1. Doe niets;
2. Ga eerst lezen en begrijpen...;
3. Dan plannen...;
4. Dan testen...;
5. Daarna pas migreren.

Wanneer begonnen wordt met het maken van een ontwerp voor een nieuw e-mailplatform moet rekening gehouden worden met de consequenties voor de eindgebruikers. De gevolgen in de vorm van downtime van het e-mailplatform moeten zo veel mogelijk beperkt blijven. Tijdens de implementatie zijn er echter twee momenten waarbij downtime onvermijdelijk is. Het eerste moment betreft het implementeren van de nieuwe Client Access Servers. Tijdens deze actie worden de DNS records omgezet naar een andere bestemming. Het repliceren van de DNS records en het testen van de correcte werking van de Client Access Servers bedraagt ongeveer een dagdeel. Het tweede moment waarbij de eindgebruiker geen toegang tot de eigen mailbox heeft, is het moment waarbij het zogenaamde "move mailbox request" wordt uitgevoerd. De bestaande Exchange 2003 mailbox van de eindgebruiker gaat offline tijdens deze actie, het verplaatsen van een 150 MB mailbox bedraagt 15 minuten. Na deze 15 minuten is de inhoud van de mailbox overgezet naar een Exchange 2010 mailbox en komt de mailbox weer online. De oude Exchange 2003 mailbox wordt tijdens de genoemde actie opgeruimd.

De uitdaging tijdens de uitvoering van het project zat hem in het feit om zoveel mogelijk de overlast voor de eindgebruiker te beperken. De diversiteit aan mogelijkheden die een eindgebruiker tegenwoordig heeft om de mailbox te benaderen maakt de uitvoering gecompliceerd en niet zonder risico's. De risico's bestaan uit bijvoorbeeld het niet meer kunnen benaderen van mailboxen tijdens de co-existentie fase via mobile devices met besturingssystemen als Android en Apple IOS. Het is daarom van groot belang en aan te bevelen om alle stappen die tijdens de implementatie worden uitgevoerd te documenteren. Deze documentatie maakt het mogelijk om, telkens wanneer er een tussentijds testresultaat negatief is, een stapje terug te doen in het implementatieproces.

De Exchange 2010 functies Outlook Anywhere en Autodiscover zijn paradepaardjes van Microsoft. Outlook Anywhere maakt het mogelijk om Outlook buiten de eigen organisatie te gebruiken en de Autodiscover functie maakt het configureren van deze functie door de eindgebruiker zelf zeer eenvoudig. Echter, het configureren van deze twee functies is uitermate lastig en gecompliceerd. Bij het feit dat er geen duidelijke handleiding van Microsoft beschikbaar is, waarin alle stappen duidelijk beschreven staan, zet ik echt vraagtekens. Gelukkig zijn er veel internet blogs beschikbaar over Exchange 2010. Deze blogs worden gevuld door collega ICT'ers. Door de informatie op deze blogs te combineren en juist te interpreteren met betrekking tot de eigen infrastructuur kunnen veel vragen worden beantwoord. Het is daarom ook aan te bevelen om te wachten met implementatie van een serverproduct totdat het enige tijd op de markt is en er een Service Pack voor beschikbaar is. Dit voorkomt dat je als ICT'er niet voor elk probleem zelf het wiel opnieuw hoeft uit te vinden.

11 Evaluatie

De combinatie van het uitgevoerde project, het schrijven van deze scriptie en het uitvoeren van de normale dagelijkse werkzaamheden hebben geleid tot een zeer drukke maar ook zeer leerzame periode. Door middel van het opstellen van een gedetailleerde planning en nakomen van deze planning, met regelmatig wat extra inspanning in de vorm van overuren, is het gelukt om voor de gestelde deadline een nieuw werkend e-mailplatform op te leveren.

De risico's die het uitgevoerde project met zich mee bracht in de vorm van ongeplande downtime van het e-mailplatform of dataverlies zijn uitgebleven. Dit is te danken aan het continue bijhouden van uitgevoerde wijzigingen en het achter de hand houden van roll-back scenario's.

Gedurende dit project heeft de rol van projectleider mijn interesse gewekt. Met name het delegeren van werkzaamheden en het maken van afspraken met diverse partijen over de oplevering van deze werkzaamheden waren zeer leerzaam.

Nu ik aan het einde van mijn afstudeeropdracht ben gekomen hoop ik mijn opleiding af te ronden. Mijn honger naar de kennis van techniek in combinatie met projectmanagement en de theorie hierachter is nog niet gestild. Ik ga mij dan ook zeker oriënteren op nieuwe mogelijkheden.

Ruud Beets
Zuid-Scharwoude, 28 mei 2011

12 Bronvermelding

Boeken:

McCabe, J. (2007). *Network Analysis, Architecture, and Design*, Third Edition. Morgan Kaufmann, Burlington, USA.

Harris, S. (2009). *CISSP All-in-One Exam Guide*, Fifth Edition. McGraw-Hill, Columbus, USA.
Stanek, W (2003). *Microsoft Exchange Server 2003 Administrator's Pocket Consultant*. Microsoft Press, Redmond, USA.

Glenn, W. (2007). *Microsoft Exchange Server 2007 Administrator's Companion, Second Edition*. Microsoft Press, Redmond, USA.

Lammle, T. (2007). *Studyguide CCNA: Cisco Certified Network Associate Study Guide, Sixth Edition, Exam 640-802*. John Wiley & Sons Inc, Hoboken, NJ, USA.

Torell, W./Avelar, V. (2004). *Mean Time Between Failure: Explanation and Standards*. American Power Conversion, USA.

Wesselius, J. (2010). *Exchange 2010 - A Practical Approach*. Red Gate Books, Cambridge, UK.

Internet:

Masterson, J. (2010). *White Paper: Exchange 2007 Autodiscover Service*. Geraadpleegd op 4 mei 2011, [http://technet.microsoft.com/en-us/library/bb332063\(EXCHG.80\).aspx](http://technet.microsoft.com/en-us/library/bb332063(EXCHG.80).aspx)

Microsoft Corporation (2010). *Exchange 2010 Understanding the Autodiscover Service*. Geraadpleegd op 4 mei 2011, [http://technet.microsoft.com/nl-nl/library/cc737383\(WS.10\).aspx](http://technet.microsoft.com/nl-nl/library/cc737383(WS.10).aspx)

Walther, H. (2010). *Uncovering Exchange 2010 Database Availability Groups (DAGs)*. Geraadpleegd op 10 maart 2011, http://www.msexchange.org/articles_tutorials/exchange-server-2010/high-availability-recovery

Anderson, P. (2009). *Installing Exchange Server 2010*. Geraadpleegd op 8 maart 2011, http://www.msexchange.org/articles_tutorials/exchange-server-2010/migration-deployment

Shudnow, A. (2010). *Exchange 2010 RTM High Availability Load Balancing Options*. Geraadpleegd op 9 maart 2011, <http://www.shudnow.net/2010/03/17/exchange-2010-rtm-high-availability-load-balancing-options>

Rooij de, M. (2011). *MsExchQueryBaseDN and Exchange 2010 SP1*. Geraadpleegd op 8 maart 2011, <http://eightwone.com/2011/04/05/msexchquerybasedn-and-exchange-2010-sp1>

Microsoft Corporation (2007). *De integratie van DNS met Active Directory*. Geraadpleegd op 5 april 2011, [http://technet.microsoft.com/nl-nl/library/cc737383\(WS.10\).aspx](http://technet.microsoft.com/nl-nl/library/cc737383(WS.10).aspx)

Microsoft Corporation (2009). *Getting Started With Exchange 2010*. Geraadpleegd op 4 maart 2011, <http://technet.microsoft.com/en-us/library/bb124265.aspx>

13 Gebruikte Afkortingen

CAS	Client Acces Server.
DAS	Direct Attached Storage, interne harddisk of gekoppeld aan computer
EVA	HP StorageWorks Enterprise Virtual Array.
HBA	Host bus adapters om servers aan het SAN te koppelen.
HTTP	HyperText Transport Protocol. Een protocol voor het transporteren van hypertext-documenten oftewel HTML-bestanden. Gebruikt door een web-server. Dit protocol wordt gebruikt om een internet-pagina in te laden en te bekijken.
HTTPS	Secure HTTP. Protocol voor versleutelde HTTP overdracht, gericht op de beveiliging van gegevens. De S staat voor Secure.
IDS	Intrusion Detection Systems. Software die ongewenst bezoek aan computernetwerken moet detecteren.
IOPS	Input/Output Operations Per Second. Wordt uitgesproken als i-ops. Het geeft het gemiddelde aantal input/output bewerkingen per seconde weer.
IPS	Intrusion Prevention System. Een intrusion prevention systeem controleert de toegang tot een netwerk op basis van de inhoud van het verzoek en niet zozeer op poorten of IP-adressen.
LAN	Computernetwerk binnen een gebouw of een bedrijf. Toch kan een LAN meer dan alleen een kantoorgebouw beslaan. De LAN-techniek maakt netwerken met een reikwijdte van 10 km mogelijk.
LUN	Logical Unit Number, SCSI-apparaatklassen verdeling na de ID-toekenning.
MSA	HP StorageWorks Modular Smart Array.
NAT	Network Address Translation. Methode die specifiek bedoeld is om meerdere gebruikers dezelfde internettoegang te laten gebruiken. Hierbij wordt gebruik gemaakt van de mogelijkheid van het IP-protocol om het IP-adres te veranderen in een ander IP-adres.
NFS	Network File System, a distributed file system network protocol developed by Sun Microsystems.
SAN	Storage Area Network, systeem bestaande uit veel harddisks en een intelligente controller, doorgaans via speciale snelle verbinding verbonden met server.
SAN	Subject Alternative Name. Bij een SAN beveiligings certificaat kunnen in het 'Alternative Name-veld' echter meerdere alternatieven voor de common name worden geplaatst.
SMTP	Simple Mail Transfer Protocol. Een standaard voor het uitwisselen van e-mails tussen servers in een netwerk (inclusief Internet).
SSL	Secure Sockets Layer.
TCO	Total Cost of Ownership.
TCP/IP	Transmission Control Protocol/Internet Protocol. TCP is verantwoordelijk voor de betrouwbare verzending van gegevens van het ene knooppunt op het netwerk naar het andere. TCP brengt een verbindingsgeoriënteerde sessie, of virtueel circuit, tot stand tussen twee computers.
TLS	Transport Layer Security.
UTP	Unshielded Twisted Pair.
VLAN	Virtual Local Area Network. Een VLAN bestaat uit een groep eindstations en switches die zich fysiek in één of meerdere netwerken, of zelfs gebouwen, kunnen bevinden, maar toch logisch gezien één enkele gemeenschappelijke LAN vormen. In een netwerk kunnen meerdere VLAN's naast elkaar bestaan.
WAN	Wide Area network, wereld- of regio-omspannend computernetwerk, vaak een aaneenschakeling van LANs.

14 Overzicht gebruikte figuren en tabellen

Figuur 1 - Organogram Dienst ICT Nova College	5
Figuur 2 - Huidig e-mailplatform Nova College	11
Figuur 3 - Projectorganisatie	12
Figuur 4 - De systeembenadering van James D. McCabe	16
Figuur 5 - Organisatie	16
Figuur 6 - Gebruikers- en informatie eisen	18
Figuur 7 - Applicatie	19
Figuur 8 - Datastromen	20
Figuur 9 - Globale datastromen	20
Figuur 10 - Datastromen e-mail processing	21
Figuur 11 - Datastromen web verkeer	21
Figuur 12 - DBMS/OS	22
Figuur 13 - Netwerk	23
Figuur 14 - Redirection van de webmail URL	25
Figuur 15 - DAG	28
Figuur 16 - Tiered Storage	29
Figuur 17 - Exchange CAS 2010 Publishing Nova College	32
Figuur 18 - Exchange Mailbox/HUB Transport 2010 ontwerp Nova College	33
Figuur 19 - Log shipping d.m.v. replicatie file mode	34
Figuur 20 - Log shipping d.m.v. block mode	34
Figuur 21 - Lagged Mailbox Database Copy	35
Figuur 22 - Network Security Diagram	37
Figuur 23 - Het huidige e-mail platform	38
Figuur 24 - Het e-mail platform tijdens de transitie fase	39
Figuur 25 - Het e-mail platform na de transitiefase	39
Figuur 26 - Overzicht servers testomgeving	43
Tabel 1 - Gebruikers- en informatie eisen	18
Tabel 2 - Eisen aan applicaties	19
Tabel 3 - Datastromen	22
Tabel 4 - Eisen aan DBMS-OS	23
Tabel 5 - Eisen aan het netwerk	23
Tabel 6 - Software overzicht	30
Tabel 7 - Database indeling	36
Tabel 8 - Implementatieplan	40
Tabel 9 - Tier 1 Gebruikersprofiel	44
Tabel 10 - Tier 2 Gebruikersprofiel	44
Tabel 11 - Tier 3 Gebruikersprofiel	44
Tabel 12 - Server voorkeuren	45
Tabel 13 - Mailbox Server Requirements	45
Tabel 14 - Host IO Requirements	45
Tabel 15 - Test3	46
Tabel 16 - Fysieke plaatsing DBs	46
Tabel 17 - Test10	47
Tabel 18 - Test12	47

Bijlage A - Veranderingsanalyse

Inleiding

Voorafgaand aan de start van dit project is er een veranderingsanalyse uitgevoerd. In gesprekken met de opdrachtgever en gebruikers zijn eisen verzameld die in de analyse worden gebruikt.

Deze veranderingsanalyse is gebruikt om te kunnen bepalen welke variant van de beschikbare e-mailplatformen van Microsoft het meest geschikt is als opvolger van het huidige Microsoft Exchange 2003 platform. De diverse alternatieven zijn met behulp van de beschikbare productdocumentatie met elkaar vergeleken. De keuze voor Microsoft als leverancier van het nieuwe e-mailplatform vloeit voort uit het feit dat deze leverancier het beste aansluit bij de huidige strategie van de dienst ICT Nova College.

Bij deze vergelijking zijn alternatieven zoals Gmail en Hotmail buiten beschouwing gelaten. Ook zogenaamde off-premise alternatieven zoals Office 365 en Exchange 2010 in de cloud worden niet meegenomen in deze analyse. De reden hiervoor is dat de opdrachtgever heeft aangegeven deze alternatieven om een aantal redenen niet te willen implementeren.

Een aantal van deze redenen zijn:

- Het is niet altijd eenvoudig om: cloud diensten te gaan gebruiken, over te stappen naar een andere cloud provider of van een cloud dienst af te stappen;
- De dienst moet afgenomen worden zoals deze is en kan niet op maat gemaakt worden;
- Back-up en archivering is een aandachtspunt;
- De eisen aan de internetverbinding worden hoger;
- De betrouwbaarheid van de aanbieder blijft een vraagteken;
- Juridische implicaties zijn niet altijd helder.

Inhoudsopgave - Bijlage A

1	Problemen	57
2	Belangengroepen - Problemen	58
3	Probleemgroepentabel	59
4	Het veranderingskader	60
5	Veranderingsbehoeften, problemen en doelen	61
6	Maatregelen versus alternatieven	62
7	Scoringstabel veranderingsbehoeften versus alternatieven	63
8	Tabel bedrijfseconomische beoordeling	64
9	Kostenoverzicht bedrijfseconomische beoordeling	65
10	Keuze van het alternatief	66

1 Problemen

Code	Problemen
P1	Verouderde hardware
P2	Support software loopt af
P3	Datacorruptie als gevolg van gebruik PST bestanden
P4	Te kleine mailboxen
P5	Een hoge beschikbaarheid is niet gewaarborgd
P6	Beheer kost veel tijd (reductie TCO)
P7	Geen archiverings mogelijkheden
P8	Openen van mail en agenda's duurt te lang (20 á 30 seconden)
P9	De huidige Web interface is niet gebruikersvriendelijk en intuïtief

2 Belangengroepen - Problemen

Belangengroepen							
B7 Werkgroep Back-up restore							
B6 Werkgroep serverbeheer							
B5 Cursisten							
B4 Medewerkers							
B3 Management Dienst ICT							
B2 Servicedesk							
B1 Werkgroep e-mailbeheer							
Problemen	B1	B2	B3	B4	B5	B6	B7
Verouderde hardware						X	
Support software loopt af	X					X	
Datacorruptie als gevolg van gebruik PST bestanden	X			X			X
Te kleine mailboxen	X	X		X	X		X
Een hoge beschikbaarheid is niet gewaarborgd	X		X				X
Beheer kost veel tijd (reductie TCO)			X				X
Geen archiverings mogelijkheden				X			
Openen van mail en agenda's duurt te lang				X	X		
Web interface is niet gebruikersvriendelijk en intuïtief				X	X		
Wijze van betrekken							
- Informeren		X		X	X		
- interviews			X	X			
- participeren	X	X	X			X	X
- projectleiding	X						
- bekostiging			X				

3 Probleemgroepentabel

<i>Probleemgroepen</i>					
G3 Beheersbaarheid					
G2 Uitbreiden functionaliteiten					
G1 Kostenbeperkende maatregelen					
Problemen	G1	G2	G3		
Verouderde hardware			X		
Support software loopt af			X		
Datacorruptie als gevolg van gebruik PST bestanden			X		
Te kleine mailboxen		X	X		
Een hoge beschikbaarheid is niet gewaarborgd			X		
Beheer kost veel tijd (reductie TCO)	X				
Geen archiverings mogelijkheden		X			
Openen van mail en agenda's duurt te lang (20 á 30 seconden)	X	X			
De huidige Web interface is niet gebruikersvriendelijk en intuïtief	X	X			
Prioriteit probleemgroepen	G	G	H		
Legenda: H = hoog G = gemiddeld L = laag					

4 Het veranderingskader

Doelstellingen

Code	Doelstellingen
D1	Waarborgen hogere beschikbaarheid
D2	Meer functionaliteit
D3	Reductie beheerskosten

Inventarisatie veranderingsbehoeften

Code	Veranderingsbehoeften
V1	Continuering hard- en software ondersteuning
V2	Uitbannen PST bestanden
V3	Grotere mailboxen
V4	Waarborgen hoge beschikbaarheid
V5	Archiverings mogelijkheden
V6	(Beheers) kosten reduceren
V7	Prestatieverbetering e-mailplatform
V8	Verbeteren webinterface

5 Veranderingsbehoeften, problemen en doelen

Veranderingsbehoeften								
V8 Verbeteren webinterface								
V7 Prestatieverbetering e-mailplatform								
V6 (Beheers) kosten reduceren								
V5 Archiverings mogelijkheden								
V4 Waarborgen hoge beschikbaarheid								
V3 Grotere mailboxen								
V2 Uitbannen PST bestanden								
V1 Continuerend hard- en software ondersteuning								
Problemen	V1	V2	V3	V4	V5	V6	V7	V8
Verouderde hardware	X							
Support software loopt af	X							
Datacorruptie als gevolg van gebruik PST bestanden		X						
Te kleine mailboxen			X		X			
Een hoge beschikbaarheid is niet gewaarborgd				X		X		
Beheer kost veel tijd (reductie TCO)						X		
Geen archiverings mogelijkheden						X		
Openen van mail en agenda's duurt te lang							X	
Web interface is niet gebruikersvriendelijk en intuïtief								X
Prioriteit veranderingsbehoeften	H	H	G	G	G	G	G	G
Legenda: H = hoog G = gemiddeld L = laag	V1	V2	V3	V4	V5	V6	V7	V8

6 Maatregelen versus alternatieven

Alternatieven					
A5 Huidige situatie handhaven					
A4 Implementatie Exchange 2010 “High Availability”					
A3 Implementatie Exchange 2010					
A2 Implementatie Exchange 2007 + 3rd party archiving					
A1 Implementatie Exchange 2007					
Maatregelen	A1	A2	A3	A4	A5
Vervangen van de hardware	X	X	X	X	
Vervangen van de software	X	X	X	X	
Grotere mailboxen aanbieden	X	X	X	X	
Een “High Availability” platform implementeren				X	
TCO reduceren			X	X	
Een archiving oplossing implementeren		X	X	X	
Een beter presterend e-mailplatform implementeren	X	X	X	X	
Een gebruiksvriendelijkere webinterface implementeren			X	X	
Niets doen					X

7 Scoringstabel veranderingsbehoeften versus alternatieven

(probleemoplossend vermogen)

Alternatieven					
A5 Huidige situatie handhaven					
A4 Implementatie Exchange 2010 "High Availability"					
A3 Implementatie Exchange 2010					
A2 Implementatie Exchange 2007 + 3rd party archiving					
A1 Implementatie Exchange 2007					
Veranderingsbehoeften	A1	A2	A3	A4	A5
Continuering hard- en software ondersteuning	+	+	++	++	-
Uitbannen PST bestanden	+	++	++	++	-
Grotere mailboxen	++	++	++	++	-
Hoge beschikbaarheid	-	-	-	++	-
Archiverings mogelijkheden	-	++	++	++	-
(Beheers) kosten reduceren	+	-	+	++	-
Prestatieverbetering e-mailplatform	+	+	++	++	-
Verbeteren webinterface	+	+	++	++	-
Totaalscore	6,5	7,5	10	12	0
Legenda: - = 0 pnt. +/- = 0.5 pnt. + = 1 pnt. ++ = 1.5 pnt.					

8 Tabel bedrijfseconomische beoordeling

Alternatieven					
A5 Huidige situatie handhaven					
A4 Implementatie Exchange 2010 "High Availability"					
A3 Implementatie Exchange 2010					
A2 Implementatie Exchange 2007 + 3rd party archiving					
A1 Implementatie Exchange 2007					
Initiële kosten	A1	A2	A3	A4	A5
Aanschaf servers	28	28	28	36	0
Uitbreiding SAN	3	5	4	5	0
Netwerkbekabeling	0,4	0,4	0,4	0,5	0
Aanpassingen netwerkapparatuur	1	1	1	1,2	0
Kosten kleine veranderingen	1	1	1	1	0
Totaal initiële kosten	35,4	35,4	35,4	43,7	0
Bedrijfskosten					
Kosten beheer	30	30	25	20	30
Jaarlijkse licentie/software fee	1,6	6,6	1,6	2	1,5
Stroomverbruik servers	2,4	2,4	2,4	3	3
Afschrijving apparatuur (20% per jaar)	5,6	5,6	5,6	7,2	0
Totaal bedrijfskosten	39,6	44,6	34,6	32,2	34,5
Legenda: Getallen x1000 in euro's ex. BTW De bedrijfskosten zijn en weergegeven per jaar					

9 Kostenoverzicht bedrijfseconomische beoordeling

Om enig inzicht te verkrijgen in de kosten die in de 'Tabel bedrijfseconomische beoordeling' zijn gebruikt, volgt hieronder een duiding van de gebruikte bedragen.

Aanschaf apparatuur

- Aanschaf 1 Front-end server €6.000,-
- Aanschaf 1 Back-end server €8.000,-

Met uitzondering van alternatief 4 worden zijn er twee Front-end en twee Back-end servers benodigd. Alternatief 4 heeft één extra Back-end server in het ontwerp.

Uitbreiding SAN

Afhankelijk van de hoeveelheid data dat moet worden opgeslagen variëren deze kosten. De kosten bestaan hoofdzakelijk uit de aanschaf van licenties.

Netwerkbekabeling

Extra servers betekent ook meer netwerkbekabeling. De kosten bestaan uit de aanschaf van Cat6 patchkabels en glasvezelbekabeling.

Aanpassingen netwerkapparatuur

Deze kosten bestaan uit de aanschaf van Gbic modules om de servers met het SAN te koppelen.

Kosten kleine veranderingen

De kosten bestaan uit de aanschaf van labels en rangeerpanelen.

Kosten beheer

Deze kosten zijn gebaseerd op basis van de kosten van een beheerder met een volledig dienstverband (1 FTE). Alternatief 5 heeft een beheerlast van 1 FTE. De andere alternatieven hebben dezelfde beheerlast of een percentage hiervan.

Jaarlijkse licentie/software fee

De jaarlijkse kosten van 1 Exchange Server licentie via een onderwijsovereenkomst bedraagt €400,-. Een 3rd party archiving licentie kost €5.000,- per jaar.

Stroomverbruik servers

Het stroomverbruik is berekend met behulp van de *HP Power Advisor* tool maal het geldende KW/h tarief.

10 Keuze van het alternatief

Aan de hand van de hiervoor beschreven analyses kan een keuze gemaakt worden uit de verschillende alternatieven. Bij de verschillende analyses kwamen de volgende alternatieven als beste naar voren:

- Tabel 7 'Veranderingsbehoeften versus veranderingsalternatieven': alternatief 4;
- Tabel 8 'Bedrijfseconomische beoordeling': alternatief 5.

Indien we alle analyses tezamen bestuderen blijken de alternatieven 2, 3 en 4 het meest geschikt om een keuze uit te maken. Alternatieven 1 en 5 komen als minst geschikte naar voren.

Na overleg met de opdrachtgever is besloten om alternatief 4 verder uit te werken.

Bij de bedrijfseconomische beoordeling komt alternatief 5 bij de initiële kosten als voordeligste naar voren. Echter het handhaven van dit alternatief brengt grote risico's op het gebied van continuïteit met zich mee, omdat zowel hard- als software verouderd is.

Bijlage B - Overzicht overlegpunten

Overzicht puntenlijsten

Tijdens de projectperiode hebben de leden van het projectteam regelmatig overleg gevoerd. Dit overleg was in wekelijks ingepland op de woensdagmorgen. Verder was de projectleider wekelijks aanwezig bij het zogenaamde techniek overleg waarbij naast vertegenwoordigers van alle techniek werkgroepen ook de coördinator techniek aanwezig is. Tijdens deze bijeenkomsten informeerde de projectleider de coördinator techniek over de status en voortgang van het project.

Naast de reguliere bijeenkomsten heeft er een aantal malen een ad-hoc overleg plaats gevonden. Deze bijeenkomsten waren noodzakelijk omdat er anders te veel tijd overheen zou gaan totdat het volgende reguliere overleg zou plaatsvinden.

Inhoudsopgave - Bijlage B

Puntenlijst Ex2010 overleg 14 Maart 2011	69
Puntenlijst Ex2010 overleg 15 Maart 2011	70
Puntenlijst Ex2010 overleg 30 Maart 2011	72
Puntenlijst Ex2010 overleg 20 April 2011	73
Puntenlijst Ex2010 overleg 4 Mei 2011	75
Puntenlijst Ex2010 overleg 10 Mei 2011	76

Puntenlijst Ex2010 overleg 14 Maart 2011

1. Fysieke plaatsing servers
 - 1.1. CAS servers 2x (moeten achter de load balancer op GKK)
 - 1.1.1. Plaatsing?
 - 1.1.2. Spanningsvoorziening?
 - 1.2. Mailbox servers 3x, waarvan één server op de GKK
 - 1.2.1. SAN koppeling?
 - 1.2.2. Patchkabels?
 - 1.2.3. KVM switch/kabels?
- Mailbox servers 3x, waarvan twee servers op de Zijlweg
 - 1.2.4. SAN koppeling?
 - 1.2.5. Patchkabels?
 - 1.2.6. KVM switch/kabels?
2. Commvault backup
 - 2.1. Windows 2008 R2
 - 2.2. Exchange 2010
3. Opruimen 19.000 oude mailboxen cursisten (Johan/Frido)
4. Aanmaken 2010 mailboxen d.m.v. scripting (Johan/Frido)
5. Exchange 2010 CRM plugin? (Lennart van Velzen)

Puntenlijst Ex2010 overleg 15 Maart 2011

Onderwerp: Uitsluitingen t.b.v. virusscanners

Info:

File-Level Antivirus Scanning on Exchange 2010

File-level scanners are frequently used. However, if they are configured incorrectly, they can cause problems in Exchange 2010. The following problems may occur when you use file-level scanners with Exchange 2010:

File-level scanners may scan a file when the file is being used or at a scheduled interval. This can cause the scanners to lock or quarantine an Exchange log or a database file while Microsoft Exchange tries to use the file. This behavior may cause a severe failure in Microsoft Exchange and may also cause -1018 errors.

If you're deploying file-level scanners on Exchange 2010 servers, make sure that the appropriate exclusions, such as directory exclusions, process exclusions, and file name extension exclusions, are in place for both memory-resident and file-level scanning Mailbox server role

E: t/m J: Hier staan de databases

L: en verder Hier staan de logfiles

C:\Program Files\Microsoft\Exchange Server\V14\

C:\Windows\System32\Inetsrv

C:\Program Files (x86)\Microsoft Forefront Protection for Exchange Server

Client Access server role

SRVNOVA040

SRVNOVA041

C:\Windows\inetpub\temp\IIS Temporary Compressed Files

C:\Windows\System32\Inetsrv De IIS systemfiles in deze directory

C:\Windows\inetpub\Logs\Logfiles\W3SVC1

C:\Program Files\Microsoft\Exchange Server\V14\

Alleen op SRVNOVA040 C:\FSW

Process Exclusions

Many file-level scanners now support the scanning of processes, which can adversely affect Microsoft Exchange if the incorrect processes are scanned. Therefore, you should exclude the following processes from file-level scanners.

- .config
- .dia
- .wsb

Database-related extensions

- .chk
- .log
- .edb
- .jrs
- .que

Offline address book-related extensions:

- .lzx

Content Index-related extensions

.ci .wid .001
.dir .000 .002

GroupMetrics

- .dsc
- .bin
- .xml

Forefront Protection for Exchange Server-related extensions

.avc .dt .lst
.cab .fdb .mdb
.cfg .fdm .ppl
.config .ide .set
.da1 .key .v3d
.dat .klb .vdb
.def .kli .vdm

The file name extensions listed for Forefront Protection for Exchange Server are the signature files from various antivirus directory engines. In most cases, these file name extensions don't change, but file name extensions may be added in the future as third-party antivirus vendors update their antivirus signature files.

Puntenlijst Ex2010 overleg 30 Maart 2011

- Aanmaken archive database
- Aanmaken PST bestanden
- PST naar Archive verplaatsen
- Wijzigen archive database per user
- Bepalen quota mb
- Bepalen quota arcive mb
- Enablen van users voor archiving - Hoe?
- Wijze van aanmaken nieuwe mailboxen
- Wijze van aanmaken nieuwe archive mailboxen
- archive database enkel uitvoeren - hoeveel - backup ja/nee
- retention policies / tags

Puntenlijst Ex2010 overleg 20 April 2011

Aanpassingen inlogscript t.b.v. Exchange 2010:

Paul:

outlook.novacollege.intern i.p.v.
srvnova051 en srvnova053

Leo:

ACL's aanpassen andere lokaties dan GKK

Ruud:

- Mailboxquota's

Per database de quota instellen:

Medewerkers: Huidige Q.: 80-90-100 mb. Nieuw: 260-280-300 mb

Heavy Users: Huidige Q.: 300 tot 600 mb. Nieuw: 950-975-1000 mb

Nu alleen op DAS: prestaties laten te wensen over.....

Cursisten (3x)/Klassikaal: Huidige Q.: 20-30-40 mb. Nieuw ... - ... - ... mb

Groepen: Huidige Q: 80-90-100 mb. Nieuw ... - ... - ... mb

Archives: Nieuw: 950-975-1000 mb

- Forefront security for Exchange 2010 installeren op de mailboxservers
- Handleidingen en communicatie
- Doorgeven aan Frido gegevens voor het aanmaken nieuwe accounts:

Database namen:

Archive database namen etc.

Paul:

PST import / verplaatsen mailboxen

- Uitzoeken PST import mogelijkheden:

<http://www.red-gate.com/products/exchange-administration/pst-importer-2010>

- Uitzoeken mogelijkheden hoe het verplaatsen mailboxen in Exchange het makkelijkste kan:

<http://thoughtsofanidleind.wordpress.com/2010/12/03/tweaking-the-mailbox-replication-service-configuration-file/>

http://www.msexchange.org/articles_tutorials/exchange-server-2010/management-administration/moving-mailboxes-exchange-2010-part4.html

Leo:

- Controleren NOD32 settings op alle 5 de Exchange 2010 servers.

Met name de excepties nog eens opzoeken voor Exchange 2010 en nakijken of na laten kijken op de servers.

- Uitzoeken hoe je een van een normale database een lagged copy maakt, voorstel voor periode.

- Retentie policies, default 14 dagen op een mailbox, moeten we hier iets aan veranderen?

Algemeen:

Procedure bij onderhoud aan servers.

Updating Exchange 2010 SP1 DAG Members

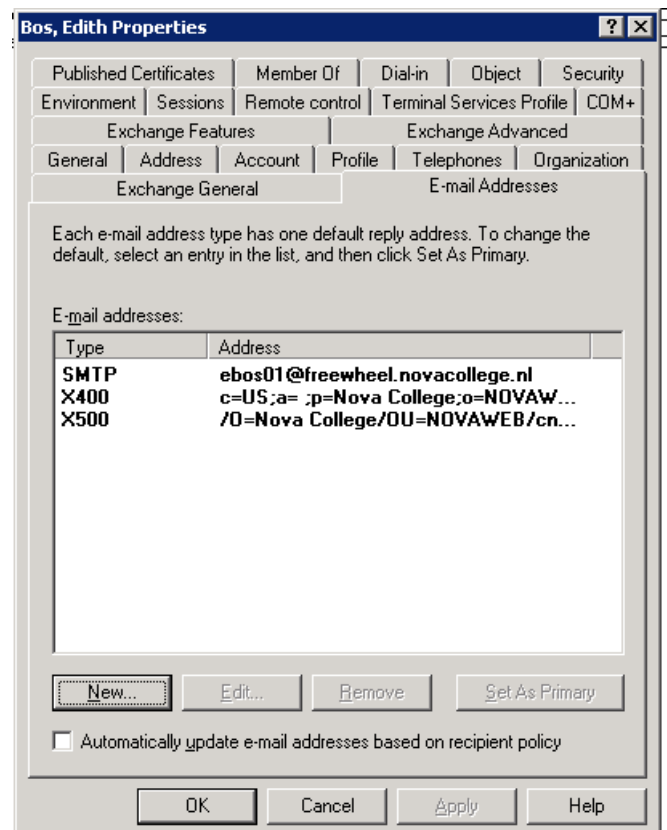
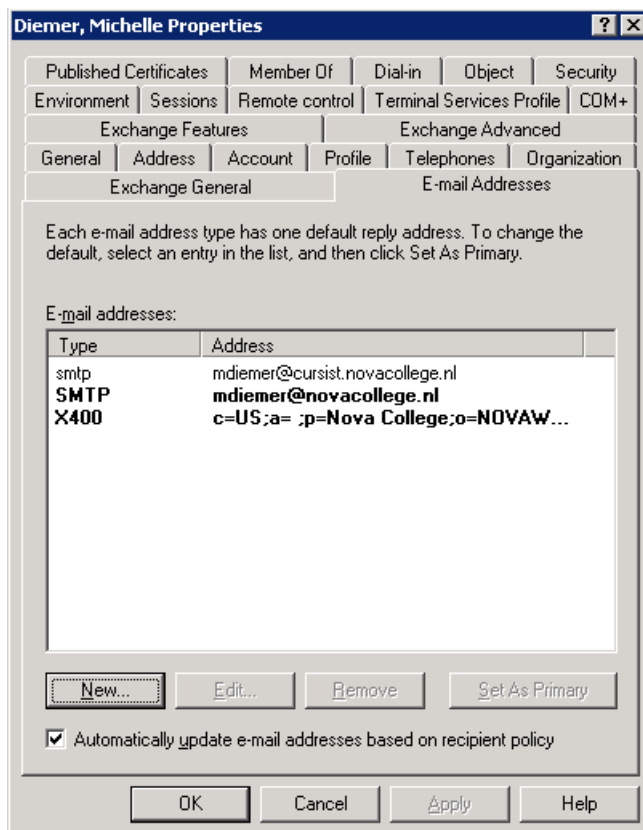
<http://eightwone.com/2011/04/13/updating-exchange-2010-sp1-dag-members>

- 1.Appoint (next) DAG member;
- 2.Move away all active copies on that DAG member;
- 3.Prevent copies from activating on that DAG member;
- 4.Perform maintenance, e.g. down or upgrade DAG member;
- 5.Enable possible activation on that DAG member again;
- 6.Optionally redistribute database copies.

Beheer vanaf eigen werkstation: EM Tools + Rollup 3v3 installeren en je eigen account de juiste rechten geven (organization management)

Puntenlijst Ex2010 overleg 4 Mei 2011

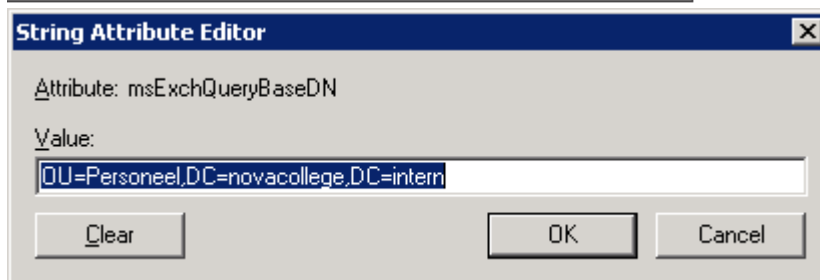
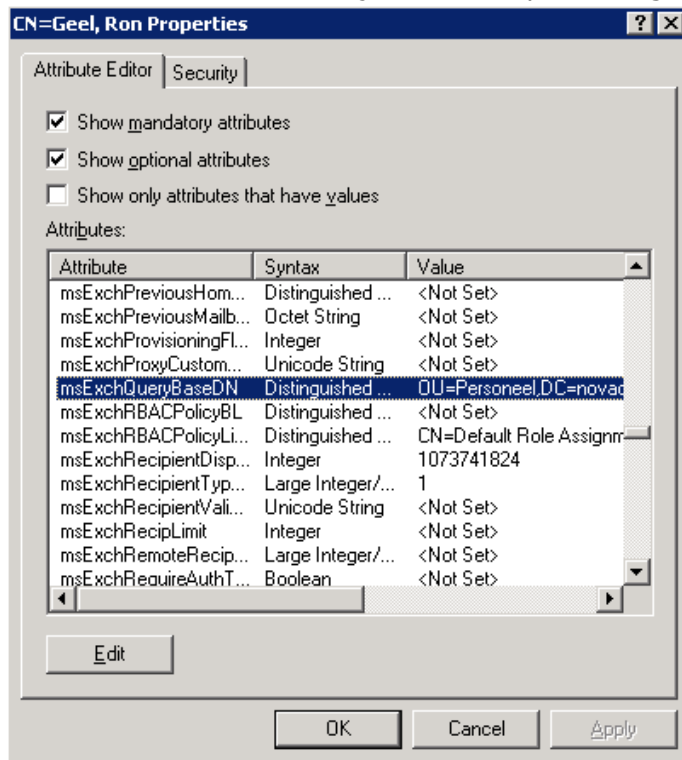
- Recipient Policies cursisten omgeving functioneren niet correct (zie bijgevoegde screenshots)
- Indien een cursistenmailbox verplaatst wordt van Ex2003 naar Ex2010 krijgt de cursist er een verkeerde alias bij, deze alias wordt meteen primary!
- Vraag aan Leo of hij dit uit wilt zoeken en wilt oplossen



Puntenlijst Ex2010 overleg 10 Mei 2011

Het msExchQueryBaseDN attribute Bij het ROC Nova College

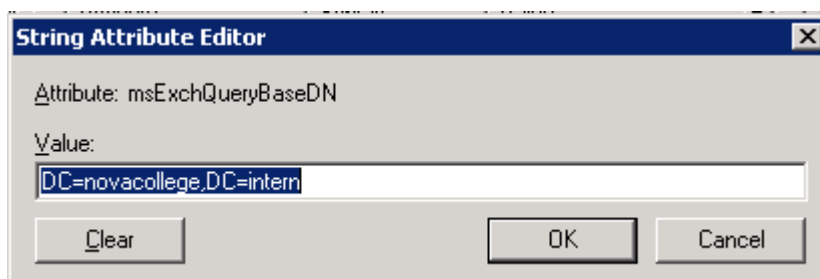
Testuser Ron Geel heeft zijn mailbox op Exchange 2010:



OU=PersoneelDC=novaccollege,DC=intern

**Outlook 2007: GAL niet beschikbaar
Personeel**

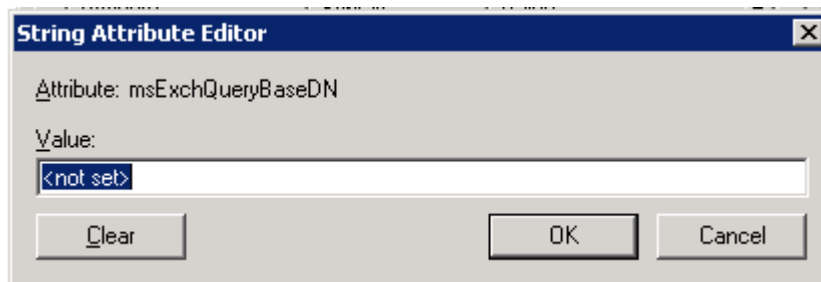
OWA2010: Alleen info OU



DC=novacollege,DC=intern

Outlook 2007: GAL niet beschikbaar

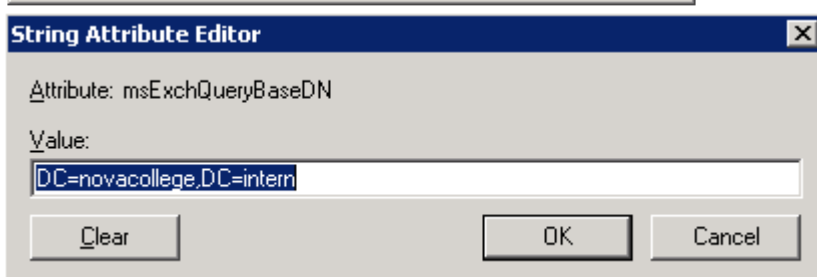
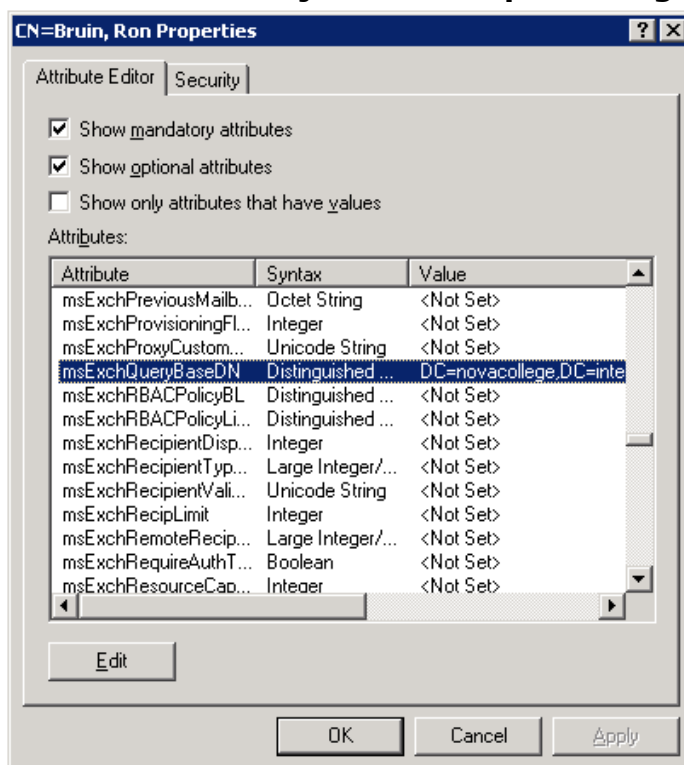
OWA2010: Foutmelding



Outlook 2007: GAL plus de andere bestaande adreslijsten zoals Cursisten, Docenten en Personeel

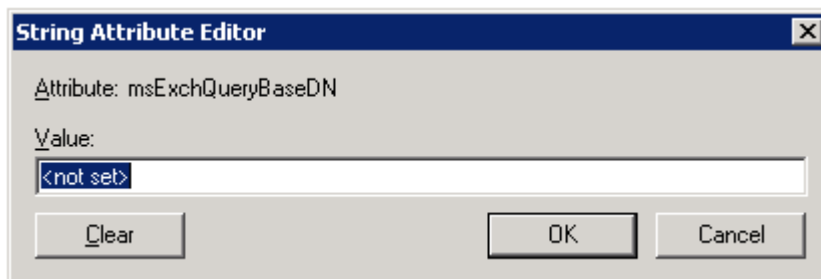
OWA 2010: GAL plus de andere bestaande adreslijsten zoals Cursisten, Docenten en Personeel

Ron Bruin heeft zijn mailbox op Exchange 2003



DC=novacollege,DC=intern

Outlook 2007: GAL plus de andere bestaande adreslijsten zoals Cursisten, Docenten en Personeel.
OWA 2003: GAL



Outlook 2007: GAL plus de andere bestaande adreslijsten zoals Cursisten, Docenten en Personeel.
OWA 2003: GAL

Conclusie:

Het msExchQueryBaseDN attribute wijzigen naar <not set> lost het probleem van het niet zien van de GAL binnen Exchange 2010 SP1 op. Maar heeft als consequentie dat alle gebruikers alle emailadressen zien in de adreslijst.

Binnen de Exchange 2003 omgeving hadden we ingesteld dat de cursisten de adressen van de medewerkers niet konden zien:

(msExchQueryBaseDN attribute : OU=Cursisten,DC=novacollege,DC=inter).

Deze waarde dient met de overgaan naar Exchange 2010 dus verwijderd te worden.

Dit betekent dus dat de cursisten dan ook de e-mail adressen van de medewerkers kunnen zien.

Noot: Mail sturen naar medewerkers door de cursisten was handmatig wel altijd al mogelijk.

Verzoek aan Paul of hij het msExchQueryBaseDN attribute wijzigen naar: <not set>.

Bijlage C - Overzicht installatie documentatie

Tijdens de uitvoering van het project Exchange 2010 Nova College zijn er een aantal installatie handleidingen samengesteld. Hier volgen de installatie handleidingen in chronologische volgorde waarin ze samengesteld zijn.

Inhoudsopgave - Bijlage C

Ex2010 Installatie handleiding testomgeving	81
Installatieverslag Ex2010 CAS Nova College	89
Integratie CAS Ex2010 server Nova College	100
Installatie 1^e HUB server	102
Installatie Mailbox servers	105
DNS instellen AutoDiscovery	113
Instellen MsExchQueryBaseDN en Ex2010 SP1	115

Ex2010 Installatie handleiding testomgeving

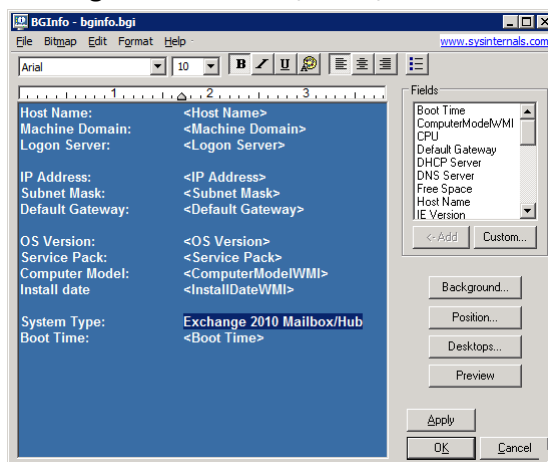
Versie	1.0.1
Auteur	Paul Kieft
Datum	01-04-2011
Aangepast door	Ruud Beets
Datum	03-04-2011



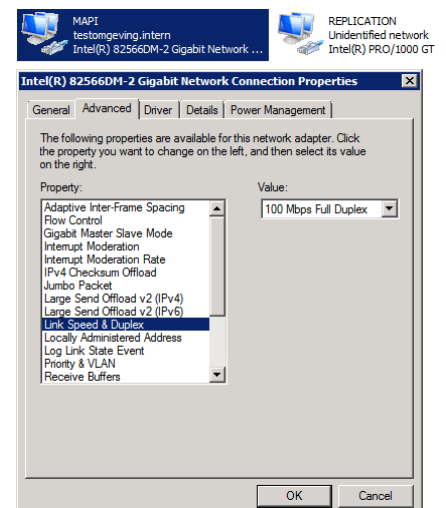
Microsoft®
Exchange Server 2010

Voorbereidingen Exchange 2010 installatie

1. Besturingssysteem installatie Windows 2008 R2 met de met **AutoInstallW2K8R2 DVD v1.0.2**.
2. Wijzig het wachtwoord van het lokale administrator account **adminnova** in 3kk...
3. Wijzig de computer naam.
4. Start BGInfo met het icoon op de desktop en type achter System Type: **Exchange 2010 Mailbox / HUB / CAS**.

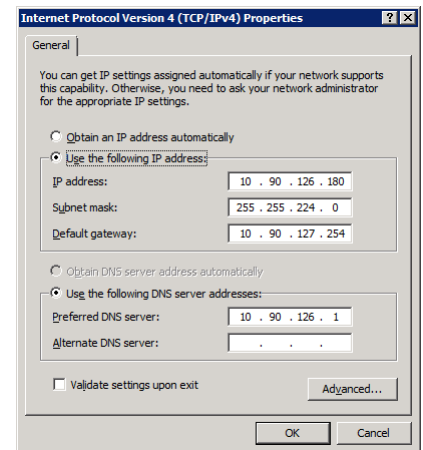


5. Schakel User Account Control (UAC) uit en activeer meerdere RDP sessies door het register bestand **DisableUAC_MultiRDP.reg** uit te voeren.
6. Hernoem de netwerkkaarten naar **MAPI** (intern netwerk) en **REPLICATION** (heartbeat)[Alleen bij MB servers] en zet de snelheid van de netwerkkaarten op **100MBFull** (voor de testomgeving).



7. TCP/IPv4 voor de MAPI netwerkkaart configureren.
Subnet mask **255.255.224.0**, Gateway **10.90.127.254**,
DNS server **10.90.126.1**.

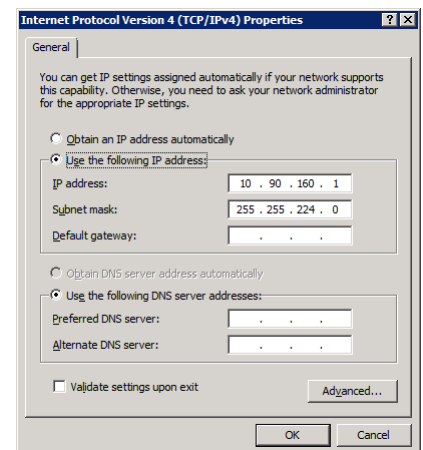
SRVNOVA180	MailBox/HUB	10.90.126.180
SRVNOVA181	MailBox/HUB	10.90.126.181
SRVNOVA182	MailBox/HUB	10.90.126.182
SRVNOVA184	Cas	10.90.126.184
SRVNOVA186	Cas	10.90.126.186



8. De **REPLICATION** (heartbeat) netwerkkaarten configureren op de Mailbox/HUB servers.

TCP/IPv4 voor de **REPLICATION** netwerkkaart configureren.
Alleen een IP-adres opgeven, geen Subnet mask, Gateway en DNS server.

SRVNOVA180	MailBox/HUB	10.90.160.1
SRVNOVA181	MailBox/HUB	10.90.160.2
SRVNOVA182	MailBox/HUB	10.90.160.3



Open de eigenschappen van de REPLICATION netwerkkaart,
de-selecteer **File and Printer Sharing for Microsoft Networks**.

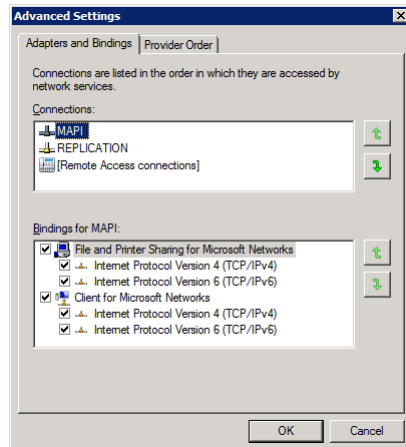
Open het tabblad DNS, de-selecteer **Register this connection's addresses in DNS**

Open het tabblad WINS, de-selecteer **Enable LMHOSTS lookup** en selecteer **Disable NetBIOS over TCP/IP**.

In het scherm **Network Connections**, kies **Advanced** en selecteer **Advanced Settings...**

het scherm **Adapters and Bindings**. Zet de **MAPI netwerkkaart bovenaan de lijst** door op de

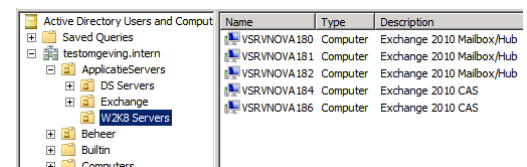
groene pijl te klikken.



9. Internet Explorer proxy instellen **10.90.126.20:8080**.

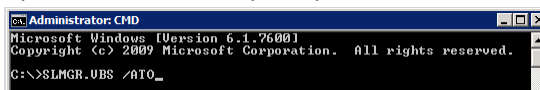
10. **Windows Update** uitvoeren en de beschikbare updates installeren.

11. Maak de server lid van het **TESTOMGEVING.INTERN** domein, verplaatst het computer account naar de **OU Applicatie Servers\W2K8 Servers** en herstart de server.

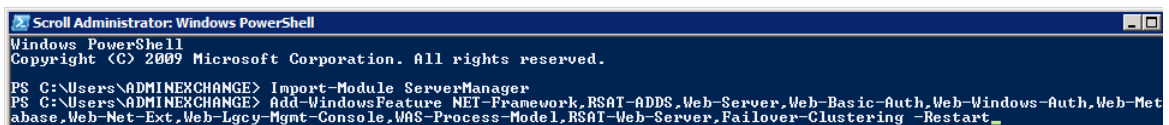


12. Activeer Windows 2008 R2 via KMS server.

Open een command prompt als Administrator en type: **SLMGR.VBS /ATO**.



13. Installeer de Exchange 2010 prerequisites, open de Power Shell commando Shell als administrator.



Type:

Import-Module ServerManager

Mailbox/HUB Servers:

Add-WindowsFeature NET-Framework,RSAT-ADDS,Web-Server,Web-Basic-Auth,Web-Windows-Auth,Web-Metabase,Web-Net-Ext,Web-Lgcy-Mgmt-Console,WAS-Process-Model,RSAT-Web-Server,Failover-Clustering -Restart

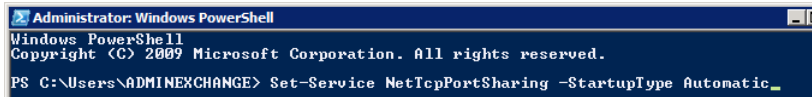
(met Failover-Clustering-Services voor de Mailbox Servers i.v.m. het aanmaken van een DAG)

CAS Servers:

Add-WindowsFeature NET-Framework,RSAT-ADDS,Web-Server,Web-Basic-Auth,Web-

Windows-Auth,Web-Metabase,Web-Net-Ext,Web-Lgcy-Mgmt-Console,WAS-Process-Model,RSAT-Web-Server,Web-ISAPI-Ext,Web-Digest-Auth,Web-Dyn-Compression,NET-HTTP-Activation,RPC-Over-HTTP-Proxy –Restart

14. (Alleen nodig bij een toekomstig DAG-member) Verander de **Startup Type** van de **Net TCP Port Sharing Service**. Open de Power Shell commando Shell als administrator en type: **Set-Service NetTcpPortSharing -StartupType Automatic**

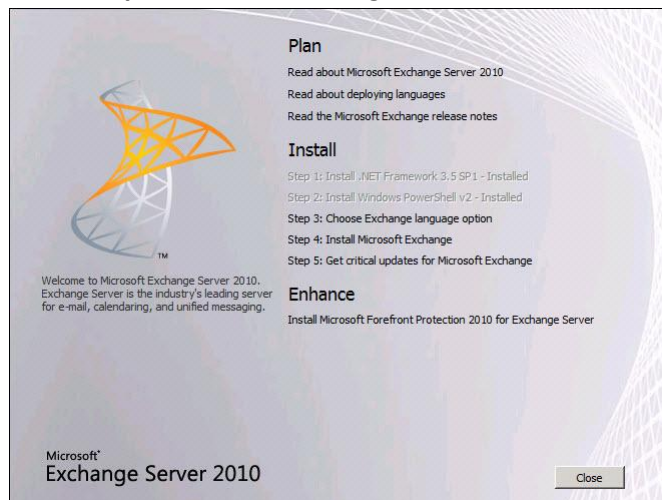


15. Installeer het **Microsoft Filter Pack v1.0** (FilterPackx64.exe) op de Mailbox/HUB servers.

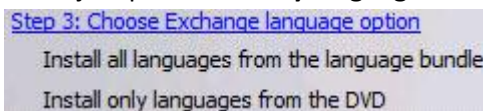
Exchange 2010 CAS Installatie

Het account dat de **eerste Exchange 2010 installatie** uitvoert **moet lid zijn** van de groepen **Enterprise/Schema Admins**, omdat het Active Directory schema wordt aangepast.

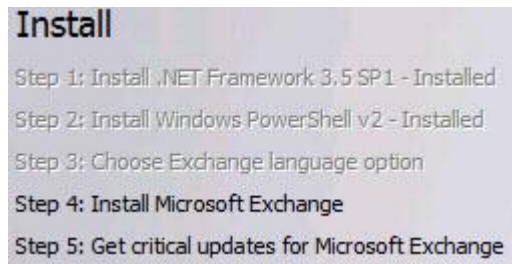
1. Login met het **TESTOMGEVING\ADMINEXCHANGE** account op de **Exchange 2010 CAS server**.
2. Start **Setup.exe** van de Exchange DVD.



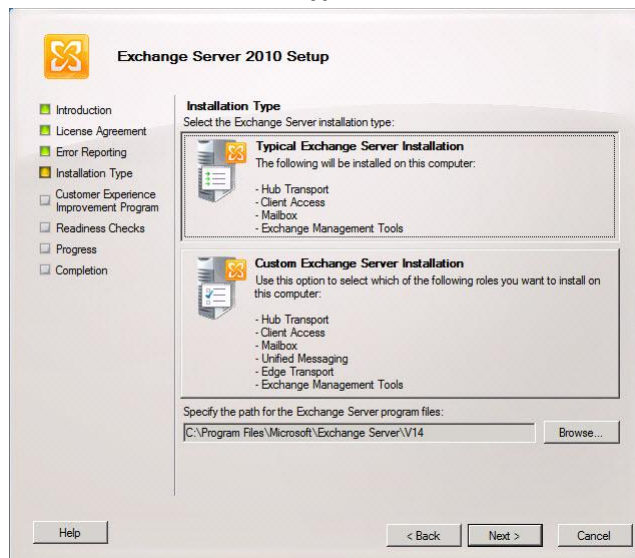
3. Kies bij Step 3 **Install only languages from the DVD**.



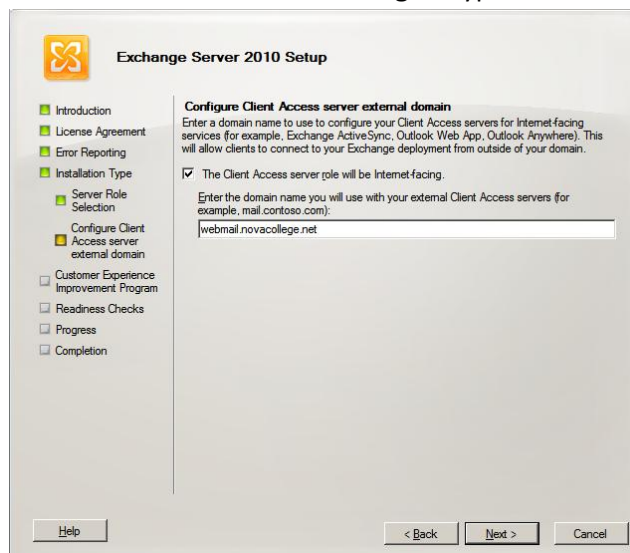
4. Klik op Step 4 **Install Microsoft Exchange**.



5. Het scherm **Introduction**, klik op **Next**.
 6. Het scherm **License Agreement**, selecteer **I Accept the terms...** en klik op **Next**.
 7. Het scherm **Error Reporting**, selecteer **No** en klik op **Next**.
 8. Het scherm **Installation Type**, Kies voor **Custom Exchange Server Installation**.



9. Selecteer alleen de server rol: **Client Access Role**.
 10. Het scherm **Configure Client Access server external domain**, selecteer **The Client Access server role will be Internet facing** en type **webmail.novacollege.net**.



11. Het scherm **Customer Experience Improvement Program**, selecteer **I don't wish to join...**

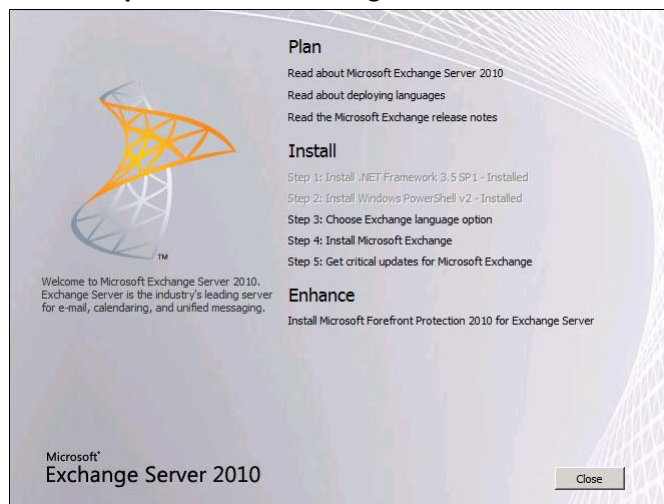
12. Controleer de meldingen van de **Readiness Checks**, klik op **Install**.
13. Installeer **Update Rollup 2 for Exchange Server 2010**, (KB979611)
<http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=6d3ae3e0-3982-46d6-9e9c-7d7d63fae565>
(Deze update vervangt Update Rollup 1)
14. Activeer Exchange 2010, open de Power Shell commando Shell als administrator en type:
Set-ExchangeServer -Identity VSRVNOVA180 -ProductKey XXXXX-XXXXX-XXXXX-XXXXX



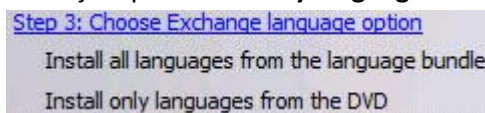
Exchange 2010 Mailbox/HUB Installatie

Op de eerste Exchange 2010 Mailbox server moet een **Routing Group Connector** worden geconfigureerd. Selecteer in het scherm **Mail Flow Settings** de **Exchange 2003 server VSRVNOVA130**.

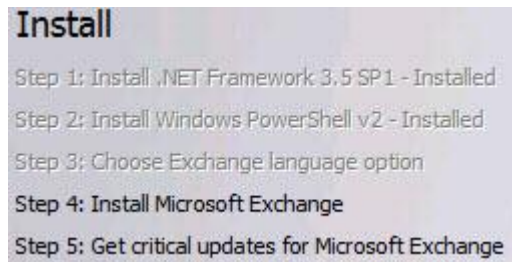
1. Login met het **TESTOMGEVING\ADMINEXCHANGE** account op de **Exchange Mailbox/HUB server**.
2. Start **Setup.exe** van de Exchange DVD.



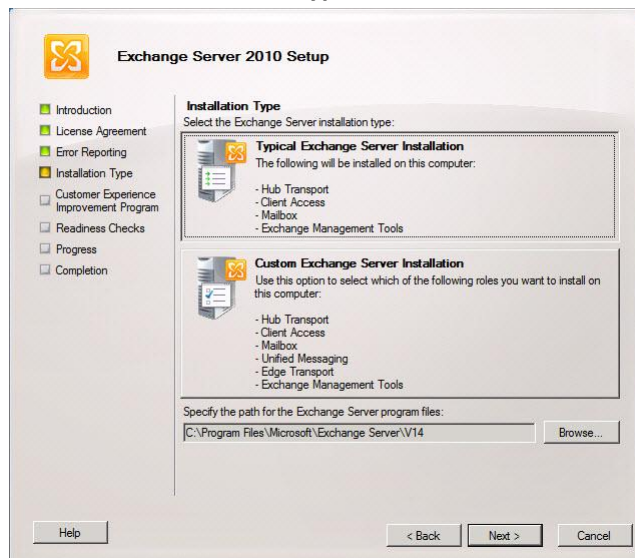
3. Kies bij Step 3 **Install only languages from the DVD**.



4. Klik op Step 4 **Install Microsoft Exchange**.



5. Het scherm **Introduction**, klik op **Next**.
6. Het scherm **License Agreement**, selecteer **I Accept the terms...** en klik op **Next**.
7. Het scherm **Error Reporting**, selecteer **No** en klik op **Next**.
8. Het scherm **Installation Type**, Kies voor **Custom Exchange Server Installation**.



9. Selecteer de server rollen: **Mailbox en Hub Transport Role**.
10. Het scherm **Customer Experience Improvement Program**, selecteer **I don't wish to join...**
11. Controleer de meldingen van de **Readiness Checks**, klik op **Install**.
12. Installeer **Update Rollup 2 for Exchange Server 2010**, (KB979611)
<http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=6d3ae3e0-3982-46d6-9e9c-7d7d63fae565>
(Deze update vervangt Update Rollup 1)
13. Activeer Exchange 2010, open de Power Shell commando Shell als administrator en type:
Set-ExchangeServer -Identity VSRVNOVA180 -ProductKey XXXXX- XXXXX-XXXXX-XXXXX

Exchange 2010 Database Availability Group

Als de **File Share Witness (FSW)** op een **NIET-Exchange server** wordt geplaatst moet de **Exchange Trusted Subsystem groep** worden toegevoegd aan de lokale Administrators groep.

Het aanmaken van een DAG met de naam NOVA-DAG

Open de Exchange Management Shell als administrator en type:

```
New-DatabaseAvailabilityGroup -Name Nova-DAG -WitnessServer VSRVNOVA186 -WitnessDirectory  
"c:\FSW" -DatabaseAvailabilityGroupIPAddresses 10.90.126.183 -Verbose
```

Links

Windows Server 2008 R2 operating system prerequisites;

[http://technet.microsoft.com/nl-nl/library/bb691354\(en-us\).aspx](http://technet.microsoft.com/nl-nl/library/bb691354(en-us).aspx)

Exchange Remote Connectivity Analyzer

<https://www.testexchangeconnectivity.com>

Installing Exchange Server 2010 in Mixed Mode Environment;

<http://msexchangegeek.com/2009/10/27/installing-exchange-server-2010-in-mixed-mode-environment-part-1/>

Exchange 2010 Beta1: Bunch of FAQs, Tips & Known Issues;

<http://exchangeshare.wordpress.com/2009/05/03/exchange-2010-beta1-bunch-of-faqs-tips-known-issues/>

Configuring Exchange 2010 Database Availability Groups

<http://howtoexchange.wordpress.com/2009/12/06/configuring-exchange-2010-database-availability-groups/>

Database Availability Group (DAG)

<http://www.exchange-genie.com/2009/04/database-availability-group-dag-exchange-2010/>

Installatieverslag Ex2010 CAS Nova College



<i>Auteurs:</i>	Paul Kieft, Ruud Beets
<i>Versie</i>	1.0.3
<i>Datum</i>	10-05-2011

Inleiding

Het Nova College heeft een start gemaakt met de overgang naar Exchange 2010. Er zijn twee Exchange 2010 SP1 CAS servers geïnstalleerd.

Tijdens de testperiode constateerden we de volgende zaken:

Indien de beide CAS server achter de F5 BIG IP loadbalancers worden geplaatst werkt het volgende:

- Het publiceren van de OWA URL webmail.novacollege.nl en de redirection naar URL legacy.webmail.novacollege.nl. De redirection is nodig voor gebruikers die hun mailbox nog op een 2003 mailboxserver hebben staan.

Het volgende werkt niet:

- Active Sync
- Outlook Anywhere (RPC over https)

Indien we de CAS server achter de loadbalancers vandaan halen werkt het volgende:

- Het publiceren van de OWA URL webmail.novacollege.nl en de redirection naar URL legacy.webmail.novacollege.nl. Deze redirection is nodig voor gebruikers die hun mailbox nog op een 2003 mailboxserver hebben staan.
- Active Sync

Het volgende werkt mogelijk wel*:

- Outlook Anywhere (RPC over Https)
-

*Het testen van Outlook Anywhere is zeer lastig omdat er bepaalde aanpassingen gedaan moeten worden in de productieomgeving. Dit kan dus alleen tijdens vooraf bepaalde service windows.

In het resterende deel van dit document is de installatie procedure beschreven zoals wij die hebben uitgevoerd.

16. Besturingssysteem installatie Windows 2008 R2 met de met **AutoInstallW2K8R2 DVD v1.0.7**.

17. Creëer een 'Fault tollerant' HP Team, team naam: **HP Network Team #1**, team type selection: **Network Fault Tolerance (NFT)**.

Hernoem de netwerkkaarten -> kaart 1: **NIC01**, kaart 2: **NIC02**, kaart 3: **HPTeam01**.

Zet de snelheid van beide NICs op **1 GB Full Auto**.

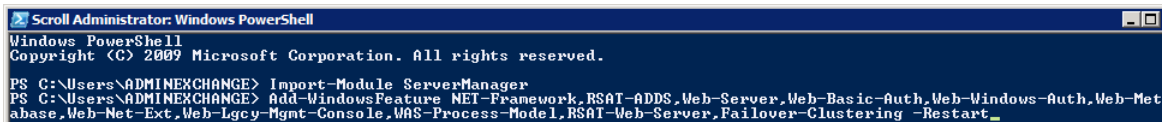
18. Open de **eigenschappen** van de **HP Team (HPTeam01)** netwerkkaart en configureer de IPv4 instellingen en disable LMHosts lookup (tabblad WINS).

Server	IP address	Subnet Mask	Default Gateway	DNS Servers
SRVNOVA040	10.110.1.40	255.255.255.0	10.110.1.3	10.15.1.103/10.15.1.104
SRVNOVA041	10.110.1.41	255.255.255.0	10.110.1.3	10.15.1.103/10.15.1.104

19. Verander de computer naam in **SRVNOVA040/SRVNOVA041**, open **BGInfo** en type achter System Type: **Exchange 2010 CAS**.
20. Schakel User Account Control (UAC) uit en activeer meerdere RDP sessies door het register bestand **DisableUAC_MultiRDP.reg** uit te voeren.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system], "EnableLUA"=dword:00000000
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server]",
fSingleSessionPerUser"=dword:00000000
```
21. **Windows Update** uitvoeren en de beschikbare updates installeren.
22. **Herstart** de server, de server zal na de automatische installatie nog 1 keer automatisch inloggen. Maak de server lid van het **TESTOMGEVING.INTERN** domein en verplaatst het computer account naar de **OU Applicatie Servers\W2K8 Servers**.
23. Activeer Windows 2008 R2 via KMS server.
 Open een command prompt als Administrator en type: **SLMGR.VBS /ATO**.
24. Installeer de Exchange 2010 CAS prerequisites, open de **Power Shell commando Shell als administrator**.
 Knip/plak of type:
Import-Module ServerManager

 Knip/plak of type:
Add-WindowsFeature NET-Framework,RSAT-ADDS,Web-Server,Web-Basic-Auth,Web-Windows-Auth,Web-Metabase,Web-Net-Ext,Web-Lgcy-Mgmt-Console,WAS-Process-Model,RSAT-Web-Server,Web-ISAPI-Ext,Web-Digest-Auth,Web-Dyn-Compression,NET-HTTP-Activation,RPC-Over-HTTP-Proxy –Restart



25. Verander de **Startup Type** van de **Net TCP Port Sharing Service**. Open de Power Shell commando Shell als administrator en type: **Set-Service NetTcpPortSharing -StartupType Automatic**.

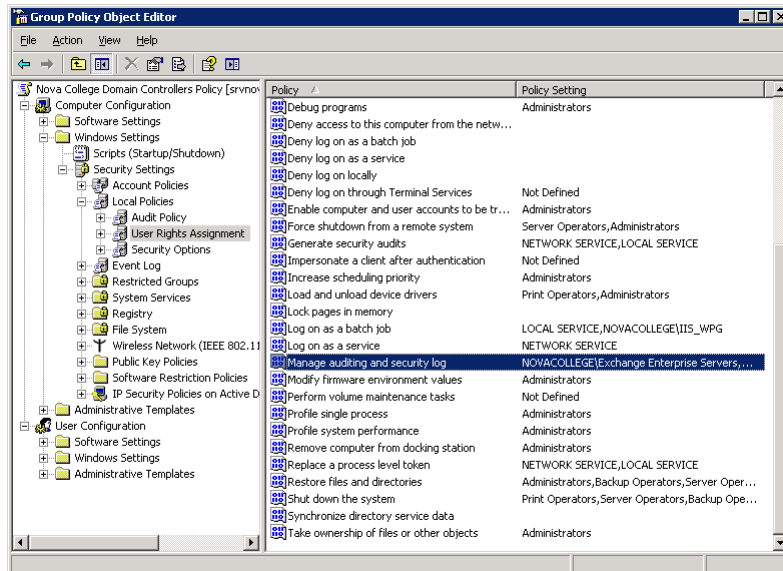
Exchange 2010 CAS Installatie

1. Kopieer de inhoud van de Exchange 2010 DVD naar **D:\Exchange2010_DVD**. Download de laatste Exchange 2010 Update Rollup (versie 4, [Exchange2010-KB982639-x64-en.msp](#)) en plaatst deze in de directory **D:\Exchange2010_DVD\Updates**. (In juni 2010 kwam SP1 voor Exchange 2010 uit, SP1 is inmiddels geïnstalleerd op CAS servers).
2. Controleer of het account AdminNova lid is van de groepen **Enterprise Admins** en **Schema Admins** en login op de betreffende server met het **AdminNova** account.

3. Maak het computer account van de betreffende server lid van de **Exchange Domain Servers** groep.

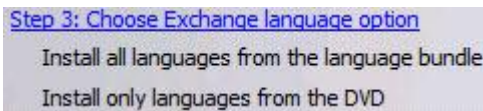
De **MSExchangeADTopology** service heeft rechten nodig om het **auditing en security log** van **domain controllers** te beheren.

De rechten worden bepaald door de **Domain Controllers Group Policy -> Computer Configuration -> Windows Settings -> Local Policies -> User Rights Assignment -> Manage auditing and security log**.



4. Start **D:\Exchange2010_DVD\Setup.exe**

Kies bij Step 3 **Install all languages from the Language bundle** en download de language bundle from internet.



Let Op: Zorg voor het downloaden van de language bundle dat er geen virusscanner is ingeschakeld.

5. Klik op Step 4 **Install Microsoft Exchange**

Het scherm **Introduction**, klik op **Next**.

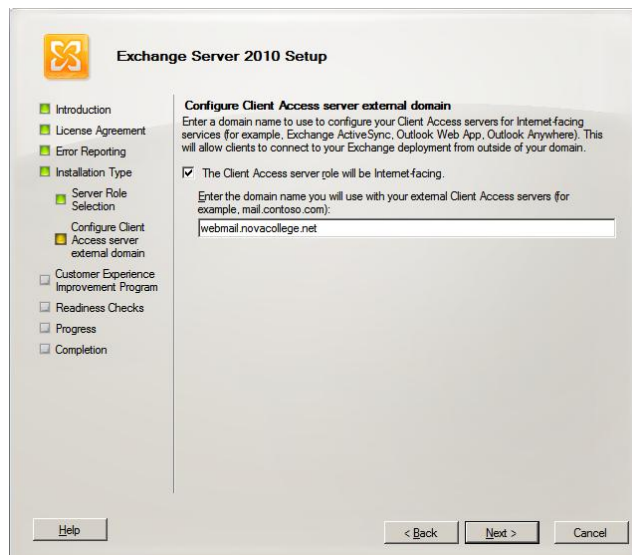
Het scherm **License Agreement**, selecteer **I Accept the terms...** en klik op **Next**.

Het scherm **Error Reporting**, selecteer **No** en klik op **Next**.

Het scherm **Installation Type**, Kies voor **Custom Exchange Server Installation**.

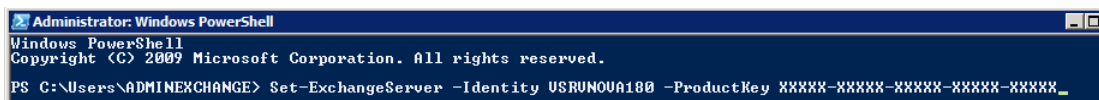
Selecteer alleen de server rol: **Client Access Role** en de **Management Tools**.

6. Het scherm **Configure Client Access server external domain**, selecteer **The Client Access server role will be Internet facing** en type **webmail.novacollege.net**.



7. Het scherm **Customer Experience Improvement Program**, selecteer **I don't wish to join...**
Controleer de meldingen van de **Readiness Checks**, klik op **Install**.

8. Activeer Exchange 2010, open de Power Shell commando Shell als administrator en type:
Set-ExchangeServer -Identity SRVNOVA040 -ProductKey XXXXX-XXXXX-XXXXX-XXXXX



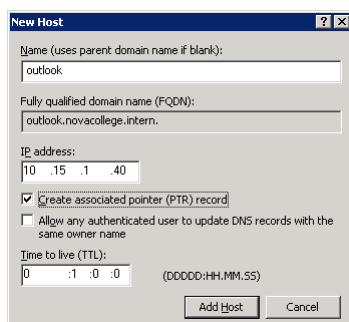
9. Voeg het **AdminExchange** account toe aan de groep **Exchange Organization Administrators**.

CAS Array aanmaken

Open de Power Shell commando Shell als administrator en type:

New-ClientAccessArray -Name "CAS array NOVA" -Fqdn "outlook.novacollege.intern" -Site "Nova_GK_Servers"

DNS record aanmaken. Open op een domain controller het **DNS management console -> Forward Lookup Zones -> Novacollege.intern**, maak een **New Host (A..)** record aan, Name: **outlook**, IP-Address: **10.15.1.40**, selecteer **Create associated pointer (PTR) record** en klik op **Add Host**.



Bron: http://www.msexchange.org/articles_tutorials/exchange-server-2007/planning-architecture/uncovering-new-rpc-client-access-service-exchange-2010-part1.html

Statische RPC port instellen

Port_55000.reg

Op beide CAS servers het register bestand uitvoeren **Port_55000.reg** om de RPC port te veranderen in 55000.

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\MSExchangeRPC\ParametersSystem],
"TCP/IP Port"=dword:0000d6d8

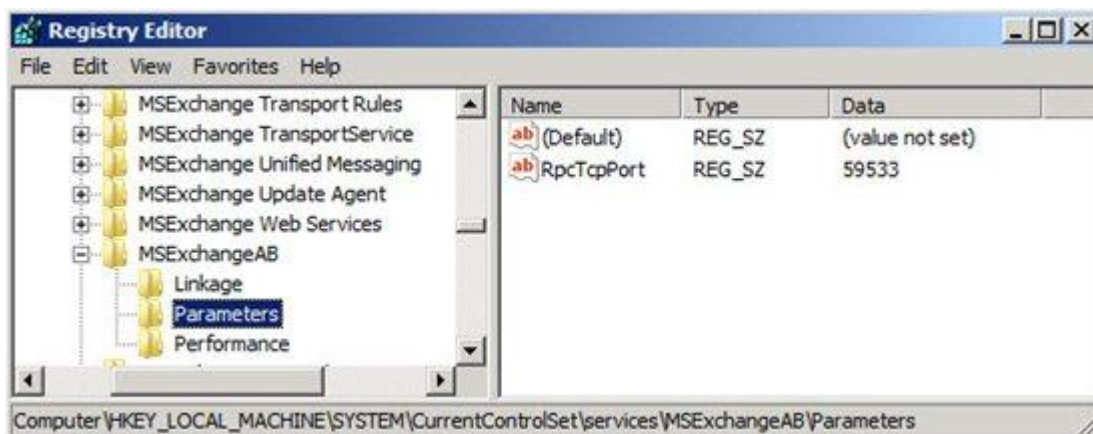
Bron: http://www.msexchange.org/articles_tutorials/exchange-server-2007/planning-architecture/uncovering-new-rpc-client-access-service-exchange-2010-part2.html

Port_55001.reg (nieuw methode van aanpassen bij gebruik SP1)

With Exchange 2010 SP1, you no longer use the “Microsoft.exchange.addressbook.service.exe.config” file to assign a static RPC port to the Exchange Address Book Service. Instead this configuration setting is controlled using the registry. To set a static RPC port for the Exchange Address Book Service, create a new

REG_SZ registry key named “RpcTcpPort” under:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\MSExchangeAB\Parameters



Configuring static port for the Exchange Address Book Service in Exchange 2010 SP1

Important

When upgrading from Exchange 2010 RTM to SP1, you need to set this key manually after the upgrade.

Note

Microsoft recommends you set this to a unique value between 59531 and 60554 and use the same value on all Exchange 2010 Client Access servers in any one AD site.

When you've configured the port, it's required to restart the Microsoft Exchange Address Book service in order for the changes to be applied.

Bron: <http://social.technet.microsoft.com/wiki/contents/articles/configuring-static-rpc-ports-on-an-exchange-2010-client-access-server.aspx>

Standaard Domain instellen

Standaard domeinnaam opgegeven die gebruikt wordt bij het inloggen via OWA.

Open het **Exchange Management shell** en voer het onderstaande commando uit.

```
set-OwaVirtualDirectory "SRVNOVA040\OWA (Default Web Site)" -LogonFormat UserName -DefaultDomain novacollege.intern  
set-OwaVirtualDirectory "SRVNOVA041\OWA (Default Web Site)" -LogonFormat UserName -DefaultDomain novacollege.intern
```

Exchange2003 OWA URL

Set-OwaVirtualDirectory SRVNOVA040\owa* -Exchange2003Url <https://legacy.novacollege.nl/exchange>

Bron: <http://technet.microsoft.com/en-us/library/ee332348.aspx>

Outlook certificaat foutmelding

Na het toevoegen van een nieuw certificaat kan Outlook 2007/2010 een certificaat foutmelding geven; Open het Exchange Management shell en voer de onderstaande commando's uit.

Proxy instellen:

Op beide Exchange CAS servers het onderstaande **netsh** commando uitvoeren, zodat certificaten geverifieerd kunnen worden via internet.

```
netsh winhttp set proxy proxy-server="http=proxy.novacollege.intern:8080;  
https=proxy.novacollege.intern:8080" bypass-list= "10.*;*.novacollege.intern"
```

Heropen het Exchange Management console om de status van de certificaten te controleren.

Als de proxy instellingen juist zijn en het werkt nog steeds niet, leeg de OCSP/CRL cache met het commando: **certutil -urlcache ocsf delete** en **certutil -urlcache crl delete**

Bekijken van de huidige proxy instellingen: **netsh winhttp show proxy**

Bron: <http://support.microsoft.com/kb/979694>

Algemene instellingen:

CAS Instellingen bekijken:

Get-ClientAccessServer -Identity SRVNOVA040 | FL

AutoDiscoveryURI veranderen:

```
Set-ClientAccessServer -Identity SRVNOVA040 -AutoDiscoverServiceInternalUri  
https://webmail.novacollege.nl/Autodiscover/Autodiscover.xml
```

```
Set-ClientAccessServer -Identity SRVNOVA041 -AutoDiscoverServiceInternalUri  
https://webmail.novacollege.nl/Autodiscover/Autodiscover.xml
```

Interne URL veranderen:

```
Set-WebServicesVirtualDirectory -Identity "SRVNOVA040\EWS (Default Web Site)" -InternalUrl  
https://webmail.novacollege.nl/EWS/Exchange.asmx -BasicAuthentication:$True
```

```
Set-WebServicesVirtualDirectory -Identity "SRVNOVA041\EWS (Default Web Site)" -InternalUrl  
https://webmail.novacollege.nl/EWS/Exchange.asmx -BasicAuthentication:$True
```


Interne URL offline address book veranderen:

Set-WebServicesVirtualDirectory -Identity "SRVNOVA040\EWS (Default Web Site)" -InternalUrl
https://webmail.novacollege.nl/OAB

Set-WebServicesVirtualDirectory -Identity "SRVNOVA041\EWS (Default Web Site)" -InternalUrl
https://webmail.novacollege.nl/OAB

Bron: <http://www.shudnow.net/2007/08/10/outlook-2007-certificate-error/>

DNS Records aanmaken

Nieuwe DNS records intern:

webmail.novacollege.nl → 10.15.1.40

autodiscover.novacollege.nl → 10.15.1.40

legacy.novacollege.nl → 10.15.1.50

Nieuwe DNS records extern:

webmail.novacollege.nl → 217.100.183.5 NAT :80/443 10.100.75.98

autodiscover.novacollege.nl → 217.100.183.5 NAT :80/443 10.100.75.98

legacy.novacollege.nl → 217.100.183.68 NAT :80/443 10.100.75.68

IP adressen

Public		URL	Intern	DMZ
217.100.183.68		legacy.novacollege.nl	10.15.1.xx	10.100.75.xx
217.100.183.5		webmail.novacollege.nl	10.15.1.xx	10.100.75.xx
217.100.183.5		autodiscover.novacollege.nl	10.15.1.xx	10.100.75.xx

SAN certificaat

Het SAN certificaat welke we in gebruik hebben bevat de volgende namen:

- legacy.novacollege.nl
- webmail.novacollege.nl
- autodiscover.novacollege.nl

Exchange 2003 Hotfix voor synchronisatie Mobiele Apparaten

Onderstaande hotfix is uitgevoerd op beide backend servers.

Enable Integrated Windows Authentication on Exchange 2003 MSAS Virtual directory, Event ID 1036.

Bron: <http://support.microsoft.com/kb/937031>

Enable Outlook Anywhere (for the purposes of this document, the default authentication settings are assumed):

Enable-OutlookAnywhere -Server: -ExternalHostName:mail.contoso.com -SSLOffloading \$false

<http://msexchangeteam.com/archive/2009/11/20/453272.aspx>

You will then schedule Internet protocol client downtime (please note that this downtime window should be relatively small - enough time for you to make the change and validate that everything works as desired) and perform the following steps:

- You will reconfigure External DNS and/or your reverse proxy infrastructure's publishing rules to have the mail.contoso.com namespaces point to CAS2010.
- Users with mailboxes on an Exchange 2003 server who try to use Exchange ActiveSync through an Exchange 2010 Client Access server will receive an error and be unable to synchronize unless Integrated Windows authentication is enabled on the Microsoft-Server-ActiveSync virtual directory on the Exchange 2003 server. This allows the Exchange 2010 Client Access Server and the Exchange 2003 back end server to communicate using Kerberos authentication.

To enable this authentication change on Exchange 2003 you need to either:

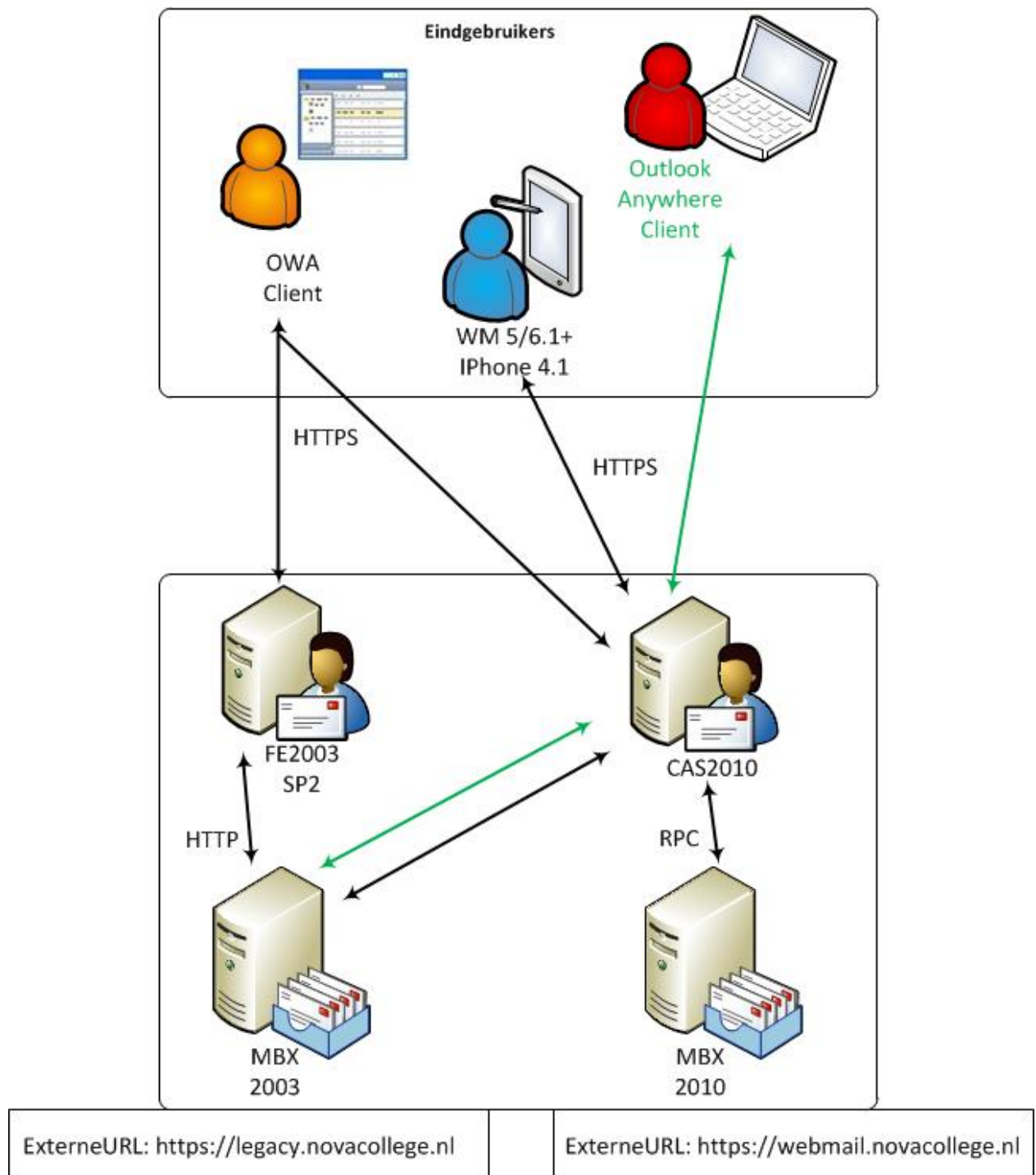
- Install <http://support.microsoft.com/?kbid=937031> and then use the Exchange System Manager to adjust the authentication settings of the ActiveSync virtual directory. Repeat this for each Exchange 2003 mailbox server in your organization.
- Or, set the *msExchAuthenticationFlags* attribute to a value of 6 on the Microsoft-Server-ActiveSync object within the configuration container on each Exchange 2003 mailbox server. An example script is provided at <http://technet.microsoft.com/en-us/library/cc785437.aspx>.

Note: It is important that you do not use IIS Manager to change the authentication setting on the Microsoft-Server-ActiveSync virtual directory as the DS2MB process within the System Attendant will overwrite the settings that are stored in Active Directory.

- Disable Outlook Anywhere by utilizing the Exchange System Manager and selecting the "Not part of an Exchange managed RPC-HTTP topology" radial button on the RPC-HTTP tab of the Front-End server's properties. Optionally, you can also remove the RPC over HTTP proxy component (refer to your Windows Server documentation for more information).

Important: This requires an up-front investment in CAS2010 architecture as all Outlook Anywhere clients will utilize CAS2010 once you transition the Outlook Anywhere endpoint. Be sure to follow all proper scalability planning documentation when deploying CAS2010 to ensure that you do not create a bottleneck in your CAS infrastructure due to Outlook Anywhere clients.

- Test all client scenarios and ensure they function correctly:



ISA2006

De drie URLs worden via een ISA 2006 server gepubliceerd. Voor de redirection van webmail.novacollege.nl naar legacy.novacollege.nl verzorgt de ISA server de SSO.

Load balancing

De beide Exchange CAS servers worden geloadbalanced via de F5 BIG-IP loadbalancer.

De Big-IP's zijn in februari 2011 voorzien van firmware versie 10.1.0 (Build 3341.0)

De deployment handleiding die we gevolgd hebben is versie 1.2 “Deploying F5 with Microsoft Exchange Server 2010”. We hebben de “one pool” optie (vermeld op blz. 1-40 en verder) gebruikt.

Integratie CAS Ex2010 server Nova College

1. Uitgangssituatie: SRVNOVA040 (CAS1) niet achter de loadbalancers:
[IP *srvnova040* is tijdelijk: 10.15.1.42]

- ❖ DNS record aanpassen op **srvnova003**
 - webmail → 10.15.1.42
 - autodiscover → 10.15.1.42
- ❖ **ISA srvnova014** publishing rules aanpassen
 - Autodiscover (activeren – ip adres controleren)
 - Webmail (controleren)
 - Legacy (controleren)
- ❖ webmail testen, *webmail.novacollege.nl* (extern)
- ❖ outlookanywhere testen, *autodiscover.novacollege.nl* (extern)
- ❖ active sync testen (extern)
 - WMobile
 - Android
 - Iphone 4.1

2. Situatie: SRVNOVA040 (CAS1) samen met SRVNOVA041 (CAS2) achter de loadbalancers:

- ❖ DNS record aanpassen op **srvnova003**: webmail en autodiscover naar 10.15.1.40 (=virtuele adres op big-ip loadbalancer)
 - webmail → 10.15.1.40
 - autodiscover → 10.15.1.40
- ❖ IP adres **srvnova040** aanpassen naar 10.110.1.40/24 gw 10.110.1.3
- ❖ Kabels **srvnova040** omsteken naar swibig001 prt9 en swibig002 prt9

- ❖ Op BIG IP controleren of de regels juist zijn geconfigureerd en actief zijn.
- ❖ webmail testen, *webmail.novacollege.nl* (extern)
- ❖ webmail testen, *webmail.novacollege.nl* (**intern**) (SSO ?)
- ❖ outlookanywhere testen, *autodiscover.novacollege.nl* (extern)
- ❖ active sync testen, (extern)
 - o WMobile
 - o Android
 - o Iphone 4.1
 - Joop SMS-en: "Backup On srvnova051"

Installatie 1^e HUB server

Achtergrondinformatie:

Exchange Server 2003 uses Routing Groups to determine the proper way to route messages while Exchange Server 2010 uses Active Directory sites for routing. These are not compatible with each other so a legacy Routing Group Connector will be created within Exchange Server 2010. This legacy connector connects Exchange Server 2010 with Exchange Server 2003 so messages can be sent between the two Exchange versions. During setup of the first Hub Transport Server an Exchange Server 2003 Hub Server needs to be selected.

This is the server the legacy Routing Group Connector will connect to: Exchange Server 2003 Hub Server: **SRVNOVA051**

When an Exchange Server 2010 Hub Transport server is installed into an existing Exchange Server 2003 environment, it installs a special Legacy, or Interop, Routing Group Connector. This Interop Routing Group Connector is responsible for sending messages between Exchange Server 2003 and Exchange Server 2010 and vice versa.

When you move mailboxes to Exchange Server 2010 and a new message arrives on the Exchange Server 2003 front-end server, this server will check Active Directory and find the user's mailbox is on Exchange Server 2010. The message will be routed through the Interop Routing Group Connector to the new Hub Transport Server, and the message will be delivered in the Exchange Server 2010 Mailbox Server – nice and simple.

Similarly, when a user with a mailbox on Exchange Server 2010 composes a message for a mailbox on Exchange Server 2003, the message is routed from the Hub Transport Server, through the Interop Routing Group Connector, to the Exchange Server 2003 front-end server. From there it will be delivered to the user's mailbox on the Exchange Server 2003 Mailbox server – also nice and simple.

As this is a completely stable system, it is up to the system administrator to decide when the mail flow is switched from delivery at the Exchange Server 2003 server to the Exchange Server 2010 Hub Transport Server. There are no hard requirements when to switch the message flow.

Exchange 2010 Mailbox/HUB Installatie:

Prerequisites for a server that will host the Hub Transport and Mailbox server roles:

Import-Module ServerManager

Add-WindowsFeature NET-Framework (voor alleen de management tools)

Add-WindowsFeature NET-Framework,RSAT-ADDS,Web-Server,Web-Basic-Auth,Web-Windows-Auth,Web-Metabase,Web-Net-Ext,Web-Lgcy-Mgmt-Console,WAS-Process-Model,RSAT-Web-Server - Restart

As per Microsoft Recommendation we need to download and install the recommended updates from Microsoft Site.

Op de eerste Exchange 2010 Mailbox server moet een Routing Group Connector worden geconfigureerd. Selecteer in het scherm Mail Flow Settings de Exchange 2003 server SRVNOVA051

1. Login met het NOVACOLLEGE\ADMINEXCHANGE account op de SRVNOVA045.
2. Start Setup.exe.
3. Kies bij Step 3 Install only languages
4. Klik op Step 4 Install Microsoft Exchange.
5. Het scherm Introduction, klik op Next.
6. Het scherm License Agreement, selecteer I Accept the terms... en klik op Next.
7. Het scherm Error Reporting, selecteer No en klik op Next.
8. Het scherm Installation Type, Kies voor Custom Exchange Server Installation.



9. Selecteer de server rollen: Mailbox en Hub Transport Role.
10. Het scherm Customer Experience Improvement Program, selecteer I don't wish to join...
11. Controleer de meldingen van de Readiness Checks, klik op Install.

12. Activeer Exchange 2010, open de Power Shell commando Shell als administrator en type:
Set-ExchangeServer -Identity SRVNOVA045 -ProductKey XXXXX- XXXXX-XXXXX-XXXXX
Exchange 2010 Database 2011 Availability Group

Als de File Share Witness (FSW) op een NIET-Exchange server wordt geplaatst moet de Exchange Trusted Subsystem groep worden toegevoegd aan de lokale Administrators groep.

Het aanmaken van een DAG met de naam NOVA-DAG
Open de Exchange Management Shell als administrator en type:
New-DatabaseAvailabilityGroup -Name Nova-DAG -WitnessServer SRVNOVA054 -WitnessDirectory
"c:\FSW" -DatabaseAvailabilityGroupIPAddresses 10.15.1.41 -Verbose

Op de gateway, bij relaying, de eerste 2010 mailboxserver toevoegen.

Links:

Windows Server 2008 R2 operating system prerequisites;
[http://technet.microsoft.com/nl-nl/library/bb691354\(en-us\).aspx](http://technet.microsoft.com/nl-nl/library/bb691354(en-us).aspx)

Exchange Remote Connectivity Analyzer

<https://www.testexchangeconnectivity.com>

Installing Exchange Server 2010 in Mixed Mode Environment;

<http://msexchangegeek.com/2009/10/27/installing-exchange-server-2010-in-mixed-mode-environment-part-1/>

Exchange 2010 Beta1: Bunch of FAQs, Tips & Known Issues;

<http://exchangeshare.wordpress.com/2009/05/03/exchange-2010-beta1-bunch-of-faqs-tips-known-issues/>

Configuring Exchange 2010 Database Availability Groups

<http://howtoexchange.wordpress.com/2009/12/06/configuring-exchange-2010-database-availability-groups/>

Database Availability Group (DAG)

<http://www.exchange-genie.com/2009/04/database-availability-group-dag-exchange-2010>

Installatie Mailbox servers

Voor de servers srvnova045, srvnova046, srvnova047:

- Setup.exe runnen
- Language: DVD.....
- Mailbox optie kiezen

Installatie DAG:

- New DAG (Organization Configuration → Mailbox)
- Right click Mailbox and select New Database Availability Group
- DAG name : NovaDAG
- FSW : [\\srvnova040\NovaDAG](#)
- C:\NovaDAG

Of:

New-DatabaseAvailabilityGroup -Name NovaDAG -WitnessServer srvnova040 -WitnessDirectory C:\NovaDAG -DatabaseAvailabilityGroupIPAddresses 10.15.1.41

Indien geen rechten:

Pre-stage Cluster Network Object (CNO):

1. Open Active Directory Users and Computers.
2. Expand the forest node.
3. Right-click the organizational unit (OU) in which you want to create the new account, select New and then select Computer.
4. In New Object - Computer, type the computer account name for the CNO in the Computer name box. This is the name that you'll use for the DAG itself. Click OK to create the account.
5. Right-click the new computer account, and then click Disable Account. Click Yes to confirm the disable action, and then click OK.

Assign permissions to the CNO

1. Open Active Directory Users and Computers.
2. If Advanced Features aren't enabled, turn them on by clicking View, and then clicking Advanced Features.
3. Right-click the new computer account, and then click Properties.
4. In <Computer Name> Properties, on the Security tab, click Add to add either the computer account for the first node to be added to the DAG or to add the Exchange Trusted Subsystem USG (universal security group):

To add the Exchange Trusted Subsystem, type Exchange Trusted Subsystem in the Enter the object names to select field. Click OK to add the USG. Then select the Exchange Trusted Subsystem USG and in Permissions for Exchange Trusted Subsystem field, select Full Control in the Allow column. Click OK to save the permission settings.

To add the computer account for the first node to be added to the DAG, click Object Types. In the Object Types dialog box, clear the Built-in security principals, Groups, and Users check boxes. Select the Computers check box. Click OK. In the Enter the object names to select field, type the name of the first Mailbox server to be added to the DAG, and then click OK. Then, select the first node's computer account, and in the Permissions for <NodeName> field, select Full Control in the Allow column. Click OK to save the permission settings.

Use the Shell to manage database availability group membership:

```
Add-DatabaseAvailabilityGroupServer -Identity NovaDAG -MailboxServer srvnova045
Add-DatabaseAvailabilityGroupServer -Identity NovaDAG -MailboxServer srvnova046
Add-DatabaseAvailabilityGroupServer -Identity NovaDAG -MailboxServer srvnova047
```

Info:

- replay lag time, de tijd dat gewacht moet worden voordat de logs worden gereplayed op de andere mailbox server
- truncation lag time, de tijd dat gewacht moet worden voordat de logs getruncate worden op de andere mailbox server

When using DAG in Exchange 2010 , You can configure the replay lag time and a truncation lag time for Mailbox database copies .

Setting a replay lag time enables you to take a database copy back to a specific point in time. Setting a truncation lag time enables you to use the logs on a passive database copy to recover from the loss of log files on the active database copy.

Replay lag time is a property of a mailbox database copy that specifies the amount of time, in minutes, to delay log replay for the database copy. The replay lag timer starts when a log file has been replicated to the passive copy and has successfully passed inspection. By delaying the replay of logs to the database copy, you have the capability to recover the database to a specific point in time in the past.

Some findings :

- the replay lag time is an administrator-configured value, and by default, it's disabled.
- The replay lag time setting has a default setting of 0 days, and a maximum setting of 14 days.
- Lagged copies are designed to prevent loss of data in the case of DB corruption.
- corruption case in exchange 2010 is very rare to happen , Exchange 2010 use some protection mechanism to prevent from DB corruption

Truncation Lag Time is a property of a mailbox database copy that specifies the amount of time, in minutes, to delay log deletion for the database copy after the log file has been replayed into the

database copy. The truncation lag timer starts when a log file has been replicated to the passive copy, and successfully passed inspection, and has been successfully replayed into the copy of the database. By delaying the truncation of log files from the database copy, you have the capability to recover from failures that affect the log files for the active copy of the database.

Eigen conclusie:

- *Replay lag time: Bepaald of de database kopie meteen wordt geupdate of dat er nog even gewacht moet worden, zodat de kopie deze periode gebruikt kan worden voor een restore.*
- *Truncation Lag Time: Het bewaren van de logfiles op de passieve kopie voor een bepaalde tijd i.p.v. ze meteen te laten verwijderen. Dit biedt de mogelijkheid om de actieve database te herstellen mochten problemen met de logfiles van de actieve database zijn.*

In this example, a copy of mailbox database DB1 is being added to a Mailbox server named MBX3. Replay lag time and truncation lag time are left at the default values of zero, and the activation preference is configured with a value of 2.

Add-MailboxDatabaseCopy -Identity DB1 -MailboxServer MBX3 -ActivationPreference 2

In this example, a copy of mailbox database DB2 is being added to a Mailbox server named MBX4. Replay lag time and truncation lag time are left at the default values of zero, and the activation preference is configured with a value of 5. In addition, seeding is being postponed for this copy so that it can be seeded using a local source server instead of the current active database copy, which is geographically distant from MBX4.

Add-MailboxDatabaseCopy -Identity DB2 -MailboxServer MBX4 -ActivationPreference 5 – SeedingPostponed

In this example, a copy of mailbox database DB3 is being added to a Mailbox server named MBX5. Replay lag time is set to 3 days, and truncation lag time is left at the default value of zero, and the activation preference is configured with a value of 4.

Add-MailboxDatabaseCopy -Identity DB3 -MailboxServer MBX5 -ReplayLagTime 3.00:00:00 - ActivationPreference 4

Summary: 2 item(s). 2 succeeded, 0 failed.

Elapsed time: 00:00:04

New MBDB_Medewerkers

Completed

Exchange Management Shell command completed:

**new-mailboxdatabase -Server 'SRVNOVA045' -Name 'MBDB_Medewerkers' -EdbFilePath
'E:\Medewerkers\Medewerkers.edb' -LogFolderPath 'F:\Medewerkers'**

Elapsed Time: 00:00:01

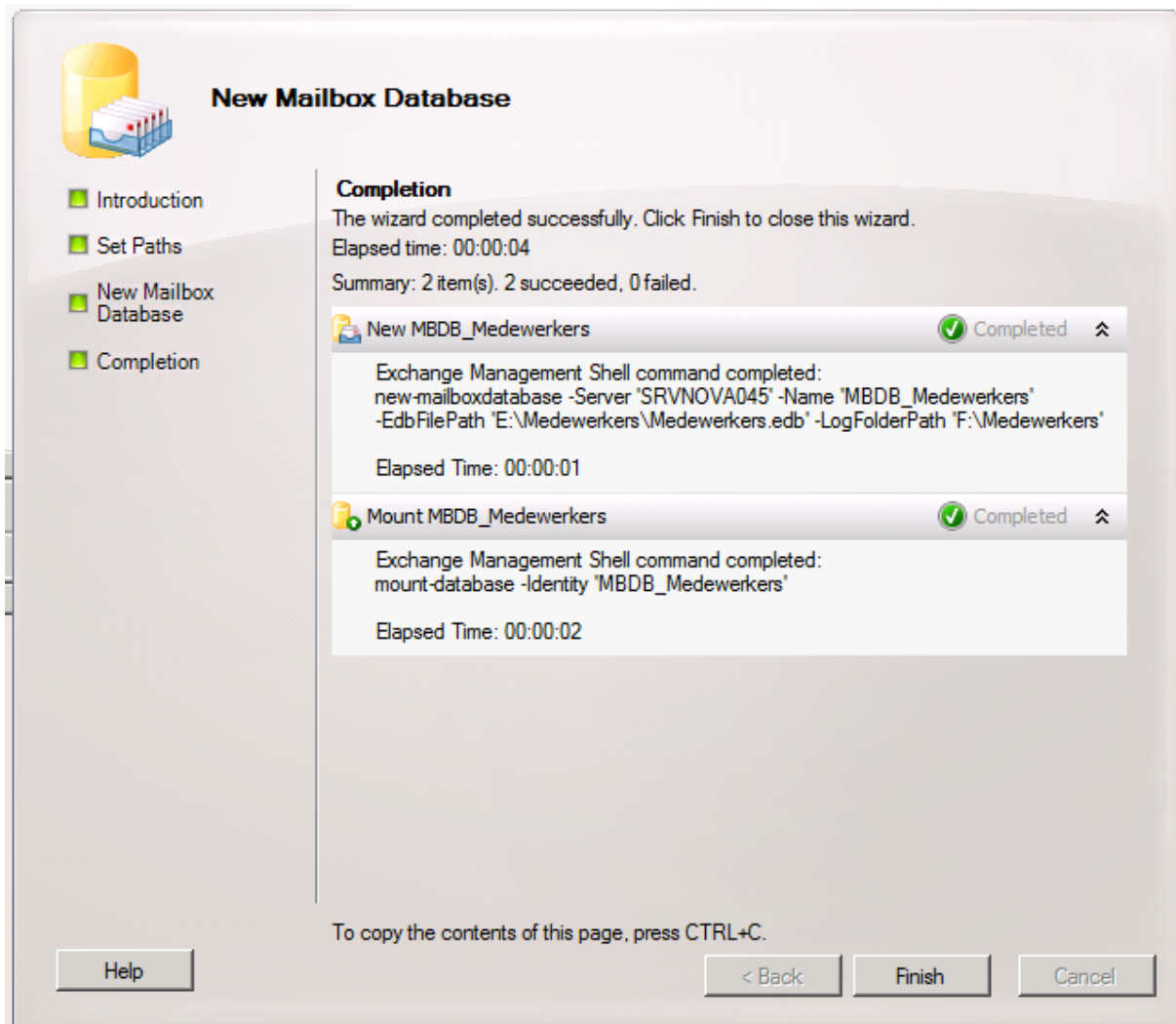
Mount MBDB_Medewerkers

Completed

Exchange Management Shell command completed:

mount-database -Identity 'MBDB_Medewerkers'

Elapsed Time: 00:00:02



Summary: 1 item(s). 1 succeeded, 0 failed.

Elapsed time: 00:00:25

MBDB_Medewerkers

Completed

Exchange Management Shell command completed:

Add-MailboxDatabaseCopy -Identity 'MBDB_Medewerkers' -MailboxServer 'SRVNOVA046' -ActivationPreference '2'

Elapsed Time: 00:00:25

Summary: 1 item(s). 1 succeeded, 0 failed.

Elapsed time: 00:00:10

Korte, Chris

Completed

Exchange Management Shell command completed:

'novacollege.intern/Personeel/TestAccounts/Korte, Chris' | New-MoveRequest -TargetDatabase 'MBDB_Medewerkers'

Elapsed Time: 00:00:10

Instellen security settings IIS7

Virtuele directory authenticatie voor Exchange 2010 CAS en Mailbox Servers

In de IIS manager op de **CAS servers** (SRVNOVA040, SRVNOVA041) hebben we de **authenticatie van de virtuele directories** ingesteld volgens de onderstaand tabel.

Exchange Server 2010 met de CAS Role:

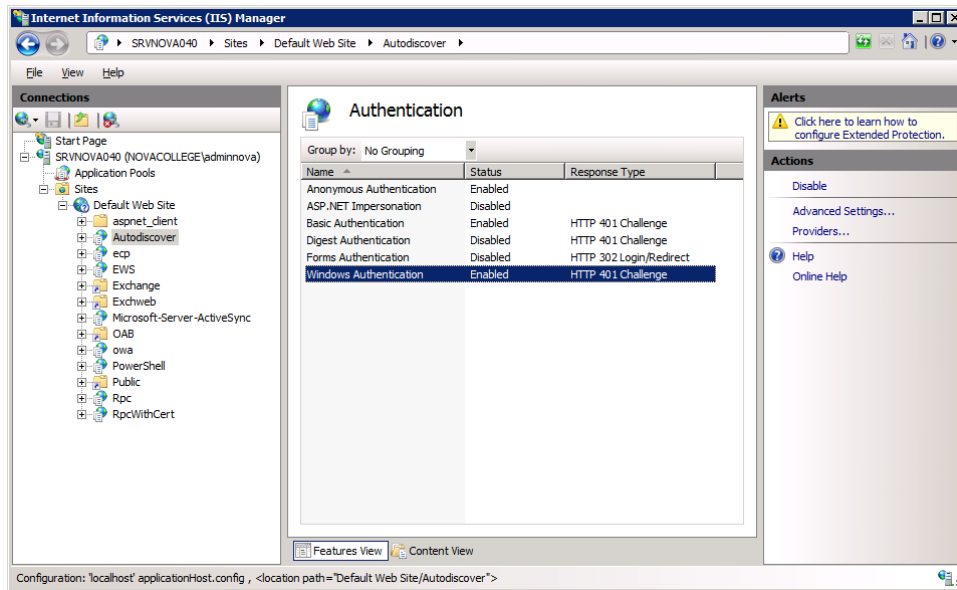
Location	Authentication	Windows Authentication Kernel-Mode	SSL Setting
Default Web Site	Anonymous		Required
aspnet_client	Anonymous		Required
Autodiscover	Anonymous / Basic / Windows Authentication	Enabled	Required
ECP	Anonymous / Basic		Required
EWS	Anonymous / Windows Authentication	Enabled	Required
Exchange (2003)	Basic / Windows Authentication		Required
Exchweb (2003)	Basic / Windows Authentication		Required
Microsoft-Server-ActiveSync	Basic		Required
OAB	Windows Authentication	Enabled (Grayed out)	<u>Not Required</u>
OWA	Basic		Required
Powershell	Anonymous		<u>Not Required</u>
Public (2003)	Basic / Windows Authentication		Required
RPC	Basic / Windows Authentication	Enabled	Required
RpcWithCert	<u>All options Disabled</u>		Required (128bit not enabled)

Exchange Server 2010 met de Mailbox role:

Location	Authentication	SSL Setting	Management
Default Web Site	Anonymous	Required	IIS Management Console
PowerShell	Anonymous	<u>Not Required</u>	Exchange Management Shell

Back-up van de IIS virtuele directory authenticatie instellingen van SRVNOVA040:

Location	Authentication
Default Web Site	Anonymous/ Basic
aspnet_client	Anonymous
Autodiscover	Anonymous / Basic / Windows
ECP	Anonymous / Basic
EWS	Anonymous / Basic / Windows
Exchange	Anonymous
Exchweb	Anonymous
Microsoft-Server-ActiveSync	Basic
OWA	Basic
Powershell	Anonymous
RPC	Basic
RpcWithCert	Basic / Windows
OAB	Windows Authentication

De IIS manager op SRVNOVA040:

Bron: <http://blogs.technet.com/b/msaad/archive/2010/09/24/default-authentication-methods-in-exchange-2010-cas-and-mailbox-servers.aspx>

IIS Virtual Directory Kernel-Mode Authentication

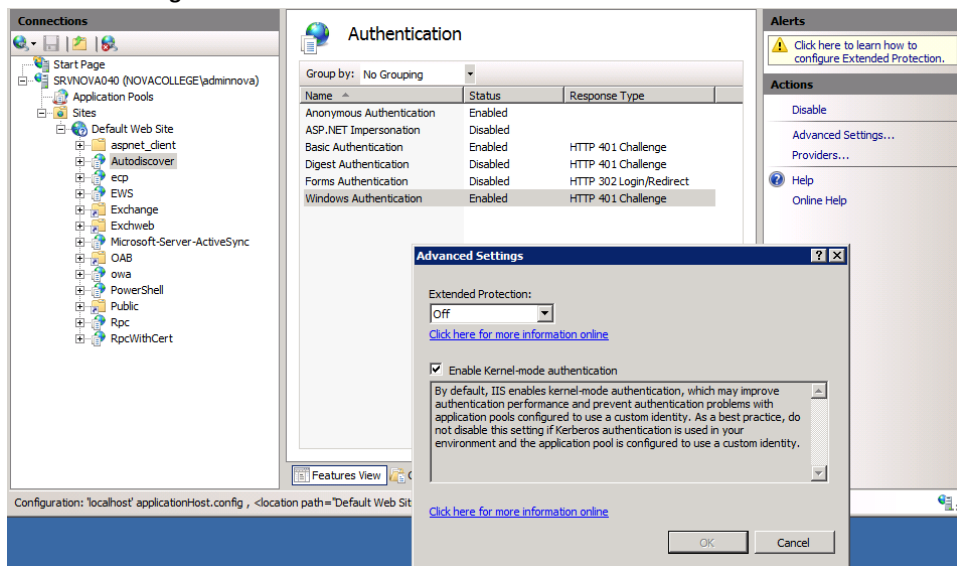
De authenticatie van de virtuele directories is goed geconfigureerd, maar Outlook vraagt nog steeds naar een gebruikersnaam en wachtwoord bij de auto configuratie van Outlook en na handmatige configuratie na het open van Outlook.

Om dit probleem te verhelpen hebben we op de onderstaande virtuele directories **kernel-mode authentication** geactiveerd.

Open de **Internet Information Services (IIS) Manager**, onder de **Default Website**, selecteer de betreffende virtuele directory, dubbelklik op het **Authentication** icoon, klik met de rechtermuisknop op **Windows Authentication** en selecteer **Advanced Settings** en Activeer **Kernel-Mode Authentication**.

Voer deze acties uit voor de onderstaande directories:

- **Autodiscover**
- **EWS**
- **RPC**
- **OAB**

Advanced Settings Kernel-Mode Authentication:

Bron: http://www.experts-exchange.com/Software/Server_Software/Email_Servers/Exchange/A_2300-Outlook-continually-prompting-for-username-and-password.html

DNS instellen AutoDiscovery

SRV Record aanmaken voor t.b.v. autodiscovery Outlook and Exchange 2010

De Autodiscover service gebruikt het e-mailadres of het domein account van de gebruiker om Outlook te configureren voor een Exchange Server.

Procedure: verwijder alle HOST (A) of CNAME records voor de Autodiscover service in de externe DNS zone.

Gebruik de volgende parameters om het nieuwe **SRV record** te creëren.

Domain name: novacollege.nl

Service: _autodiscover

Protocol: _tcp

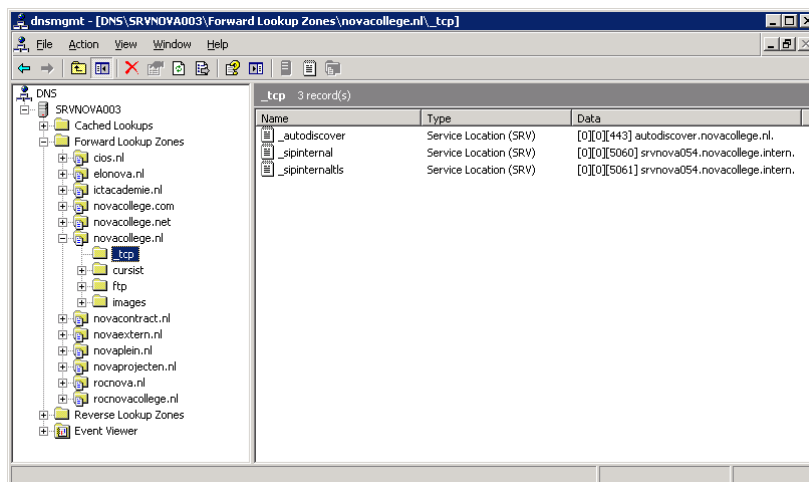
Priority: 0

Weight: 0

Port Number: 443

Host: autodiscover.novacollege.nl

Autodiscover Service Record op SRVNOVA003.



Bron: <http://blog.link2exchange.com/srv-record-settings-for-autodiscover-setup-for-outlook-and-exchange-2007/>

RPCproxy poorten instellen voor RPC over HTTP

De waarde van de registersleutel **HKEY_LOCAL_MACHINE\Software\Microsoft\Rpc\Rpcproxy\ValidPorts** is standaard onjuist.

De Exchange Service Host service schrijft de juiste RPC proxy poorten elke 15 minuten naar de register sleutel

HKEY_LOCAL_MACHINE\Software\Microsoft\Rpc\Rpcproxy\ValidPorts_AutoConfig_Exchange.

Herstart de Exchange Service Host service om de **ValidPorts_AutoConfig_Exchange** te updaten.

Op beide CAS servers (SRVNOVA040, SRVNOVA041) hebben we de inhoud van de register sleutel

ValidPorts_AutoConfig_Exchange geplakt in de **ValidPorts** sleutel en aangevuld met volgens waardes:

SRVNOVA001:6004;SRVNOVA001:593;srvnova001.novacollege.intern:6004;SRVNOVA002:6004;SRVNOVA002:593;srvnova002.novacollege.intern:6004; webmail.novacollege.nl:593

De inhoud van de **HKEY_LOCAL_MACHINE\Software\Microsoft\Rpc\Rpcproxy\ValidPorts** ziet er nu als volgt uit:

outlook:6001-6002;outlook:6004;

outlook.novacollege.intern:6001-6002;outlook.novacollege.intern:6004;

SRVNOVA040:60016002;SRVNOVA040:6004;SRVNOVA040.novacollege.intern:6001-6002;SRVNOVA040.novacollege.intern:6004;

SRVNOVA041:6001-6002;SRVNOVA041:6004;SRVNOVA041.novacollege.intern:6001-

6002;SRVNOVA041.novacollege.intern:6004;SRVNOVA045:6001-6002;SRVNOVA045:6004;SRVNOVA045.novacollege.intern:6001-6002;SRVNOVA045.novacollege.intern:6004;

SRVNOVA046:6001-6002;SRVNOVA046:6004;SRVNOVA046.novacollege.intern:6001-6002;SRVNOVA046.novacollege.intern:6004;

SRVNOVA047:6001-6002;SRVNOVA047:6004;SRVNOVA047.novacollege.intern:6001-6002;SRVNOVA047.novacollege.intern:6004;

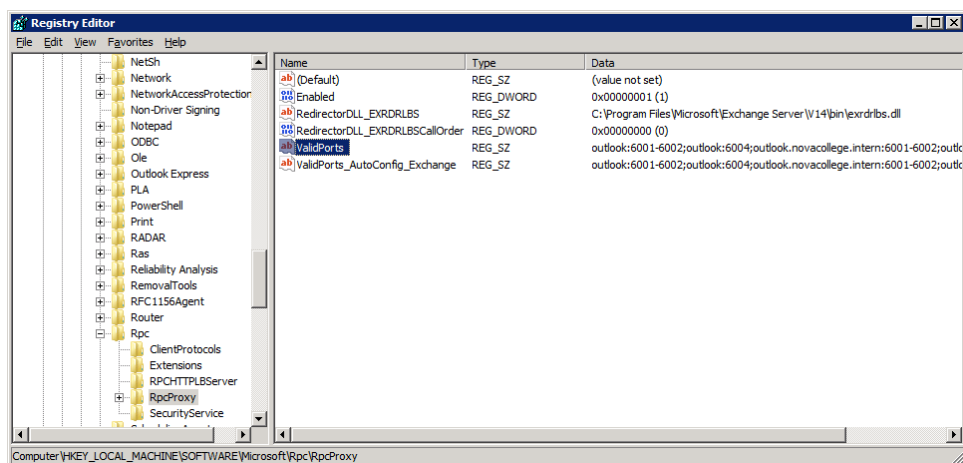
srvnova051:6001-6002;srvnova051:6004;srvnova051.novacollege.intern:6001-6002;srvnova051.novacollege.intern:6004;

srvnova053:6001-6002;srvnova053:6004;srvnova053.novacollege.intern:6001-6002;srvnova053.novacollege.intern:6004;

SRVNOVA001:6004;SRVNOVA001:593;srvnova001.novacollege.intern:6004;

SRVNOVA002:6004;SRVNOVA002:593;srvnova002.novacollege.intern:6004;

webmail.novacollege.nl:593



Foutoplossing

1. Controleer of Outlook Anywhere de poorten 6001, 6002 en 6004 gebruikt. Type in een command prompt **netstat -ano**
2. Controleer of het RPC over HTTP component is geïnstalleerd en goed werkt. Type in de Internet Explorer <https://localhost/rpc/rpcproxy.dll>, de service werkt als er lege pagina verschijnt .

Bron: <http://uc-technology.blogspot.com/2011/03/troubleshooting-outlook-anywhere-in.html>

Instellen MsExchQueryBaseDN en Ex2010 SP1

Het msExchQueryBaseDN attribuut kan worden gebruikt om voor bepaalde gebruikers het algemene adresboek te beperken. In Exchange 2010 Service Pack 1 kan het instellen van het msExchQueryBaseDN attribuut tot gevolg hebben dat Outlook 2007 en 2010 een leeg adresboek tonen en andere adresboeken worden onzichtbaar.

Exchange 2010 Service Pack 2 zal waarschijnlijk een functie bevatten die het mogelijk maakt om het algemene adresboek op te splitsen. Meer informatie op <http://blogs.msdn.com/b/dgoldman/archive/2011/01/28/the-official-stance-on-address-list-segregation.aspx>

Het zal nog enige tijd duren voordat Exchange 2010 Service Pack 2 beschikbaar zal zijn. Tot die tijd wordt aanbevolen om het msExchQueryBaseDN attribuut leeg te maken voor alle gebruikers met een mailbox op een Exchange 2010 server.

Het onderstaande commando leegt het msExchQueryBaseDN attribuut.

Open de Exchange Management Shell en type:

```
get-mailbox -organizationalunit "OU=Dienst_IFS,OU=Personeel,DC=novacollege,DC=intern" | Foreach { $dn = "LDAP://" +  
$_distinguishedname;$obj = [ADSI]$dn;$obj.PutEx(1,"msExchQueryBaseDN",0);$obj.setinfo() }
```

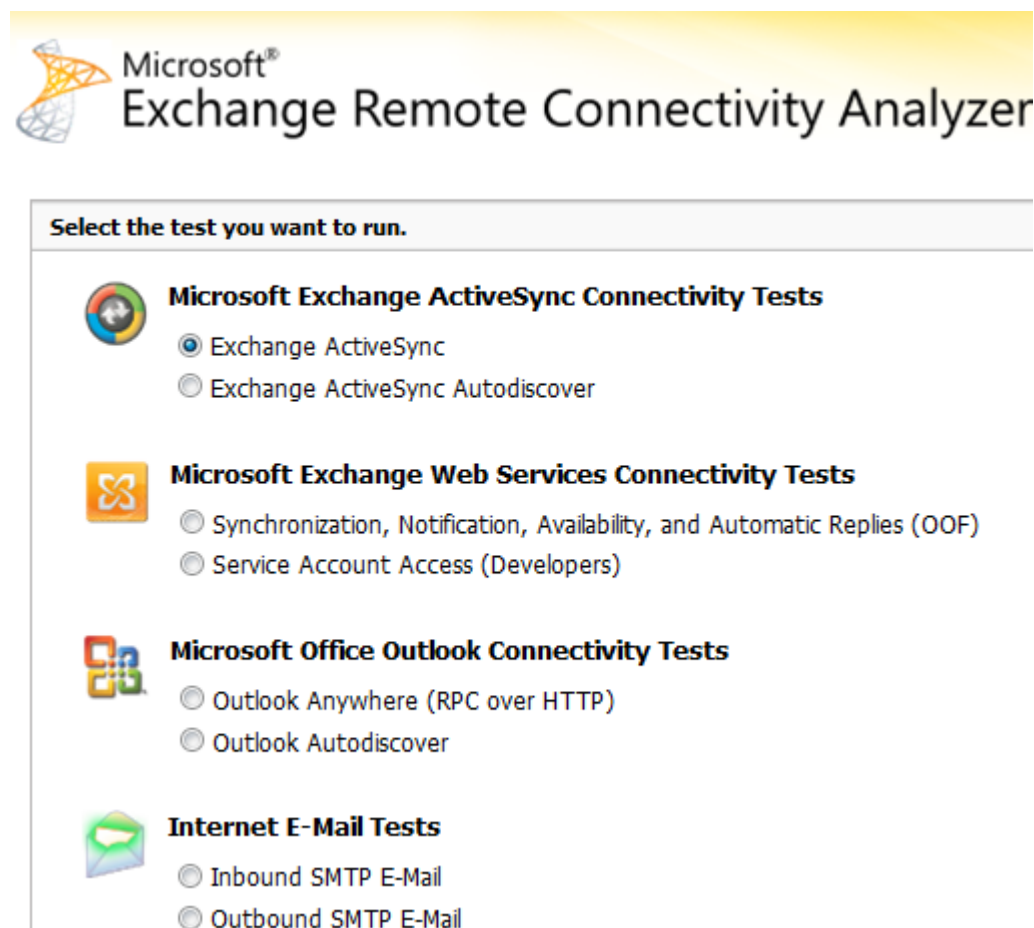
Bron: <http://eightwone.com/2011/04/05/msexchquerybasedn-and-exchange-2010-sp1/>

Bijlage D - Eindrapportage realisatiefase

Aan het einde van het project zijn een aantal testen uitgevoerd met daarin alle facetten en functionaliteiten waaraan het nieuwe e-mailplatform zou moeten voldoen. Door deze testen uit te voeren kan de opdrachtgever zien wat er wel en wat er nog niet werkt. Dit document is na de projectperiode naar de opdrachtgever verzonden. Zie tabel 19.

Een belangrijke tool om de een Exchange 2010 e-mailplatform te testen is de Exchange Remote Connectivity Analyzer. Met deze tool wordt als het ware een remote cliënt gesimuleerd. Er kan uit acht testscenario's worden gekozen. De resultaten van de twee belangrijkste tests zijn weergegeven in figuur 28 en 30.

Bij de RPC/HTTPS test laat de analyzer een waarschuwing zien, deze waarschuwing kan genegeerd worden. De analyzer probeert eerst connectie te maken zonder encryptie, zit wordt niet toegestaan. Met gebruik van encryptie slaagt de test vervolgens wel.



Figuur 27

Opleverdocument Exchange 2010 SP1 productieomgeving Nova College dd. 13-05-2010			
Testitems	Voldoet		
	Ja	Nee	Restpunt
Mailflow:	X		
Mailflow 2003 intern --> 2010 intern	X		
Mailflow 2010 intern --> 2003 intern	X		
Mailflow 2003 --> extern	X		
Mailflow 2010 --> extern	X		
Mailflow extern --> 2003	X		
Mailflow extern --> 2010	X		
Mobile Devices	X		
Mail ontvangen/versturen. Taken. Agendafunctie	X		
WM 5.1	X		
WM 6.0 en hoger	X		
Android 3.0	X		
Apple IOS 4.1	X		
Autodiscover	X		
Intern XP - Office 2007	X		
Intern XP - Office 2010	X		
Intern W7 - Office 2007	X		
Intern W7 - Office 2010	X		
Extern XP - Office 2007	X		
Extern XP - Office 2010	X		
Extern W7 - Office 2007	X		
Extern W7 - Office 2010	X		
RPC over HTTPS (Outlook Anywhere)	X		
Extern XP - Office 2007	X		
Extern XP - Office 2010	X		
Extern W7 - Office 2007	X		
Extern W7 - Office 2010	X		
Exchange 2010 Archive zichtbaar in Outlook client	X		
Intern XP - Office 2007	X		
Intern XP - Office 2010	X		
Intern W7 - Office 2007	X		
Intern W7 - Office 2010	X		
Extern XP - Office 2007	X		
Extern XP - Office 2010	X		
Extern W7 - Office 2007	X		
Extern W7 - Office 2010	X		
OWA 2010 (Outlook Web Acces)	X		
Archive zichtbaar	X		
Adreslijst zichtbaar			x ¹
Outlook 2010	X		
Mail - Agenda's - Adreslijst zichtbaar	X		
Outlook 2007	X		
Mail - Agenda's - Adreslijst zichtbaar	X		
Local MB move request 2003 --> 2010	X		
Aanmaken Archives	X		
Functioneren retentie policy tbv archive	X		
Office Communicator 2007 integratie	X		
¹ - Actie: Indien Werkgroep Web/SQL de spaties achter de displaynamen heeft verwijderd, past werkgroep AD het msExchQueryBaseDN attribute aan voor de OU Personeel.			

Tabel 19 - opleverdocument



Connectivity Test Successful with Warnings

Test Details



Testing RPC/HTTP connectivity.

The RPC/HTTP test completed successfully.

► Test Steps

Figuur 28 – RPC/HTTPS test



Testing NSPI "Check Name" for user rpaars@novacollege.nl against server outlook.novacollege.intern.
The test passed with some warnings encountered. Please expand the additional details.



[Tell me more about this issue and how to resolve it](#)

Additional Details

NspiBind returned ecNotSupported. This typically indicates that your server requires RPC encryption. ExRCA will attempt the NSPI test again with encryption.

Figuur 29 – Warning



Connectivity Test Successful

Test Details



ExRCA is attempting to test Autodiscover for rpaars@novacollege.nl.

Autodiscover was tested successfully.

► Test Steps

Figuur 30 – Autodiscover test

Een andere test die uitgevoerd is betreft het controleren of het gebruikte SSL certificaat valide is:

digicert Your Success is Built on Trust™ 1. supp

SSL Certificates Code Signing Certificates Enterprise Support Reseller About Us Login

SSL Certificate Check Install

SSL Installation Diagnostics - Check SSL Certificate

Welcome to DigiCert SSL Help. If you are having a problem with your SSL certificate installation, please enter the name of your server below and we will attempt to diagnose the problem and verify proper SSL installation.

Server Address (Ex: www.digicert.com)

webmail.novacollege.nl

Check Server

- ✓ **DNS resolves 'webmail.novacollege.nl' to 217.100.183.5**
- ✓ **SSL certificate**
Common Name = webmail.novacollege.nl
Subject Alternative Names = webmail.novacollege.nl, autodiscover.novacollege.nl, legacy.novacollege.nl
Issuer = USERTrust Legacy Secure Server CA
Serial Number = 8D8BC67A450E53FDD584F6BB59F31D30
SHA1 Thumbprint = 181924165B04D1D86D68B40AF068F2481355CEF4
Key Length = 2048 bit
Signature algorithm = SHA1+RSA (good)
Secure Renegotiation: Supported
- ✓ **This certificate does not use a vulnerable Debian key (this is good)**
- ✓ **SSL Certificate expiration**
The certificate expires August 10, 2013 (810 days from today)
- ✓ **Certificate Name matches webmail.novacollege.nl**

SERVER CERTIFICATE
Subject webmail.novacollege.nl
Valid from 11/Aug/2010 to 10/Aug/2013
Issuer USERTrust Legacy Secure Server CA

INTERMEDIATE CERTIFICATE
Subject USERTrust Legacy Secure Server CA
Valid from 26/Nov/2009 to 01/Nov/2015
Issuer Entrust.net Secure Server Certification Authority

Figuur 31

Uit bovenstaande test blijkt dat het gebruikte certificaat aan de gestelde eisen voldoet.

Bijlage E - Handleiding Servicedesk Exchange Control Panel

Exchange 2010 bevat een aantal nieuwe features. Een van deze features is het Exchange Control Panel, hiermee kan een servicedesk diverse items aanpassen. Daarnaast kunnen gebruikers welke lid zijn van specifieke groepen compliance zoekacties starten vanuit het Exchange Control Panel.

Het inlogscherf is exact hetzelfde als dat van de OWA in Exchange 2010. Wanneer je eenmaal bent ingelogd krijg je onderstaand scherm te zien:



Figuur 32

Zoals te zien is zijn er diverse opties:

- Users, hiermee wordt een overzicht getoond van de gebruikers van Exchange en kan men details van de gebruikers opvragen en eventueel items wijzigen;
- Public groups, hiermee is het mogelijk public groups aan te maken en eventueel te wijzigen;
- External contacts, hiermee is het mogelijk externe contacten aan te maken en te wijzigen;
- Administrator roles, hiermee wordt een overzicht getoond van alle beschikbare administratieve rollen en kan men gebruikers toewijzen aan deze groepen;
- User roles, hiermee wordt een overzicht getoond van alle beschikbare gebruikers rollen en kan men gebruikers toewijzen aan deze groepen en kunnen de rechten van de rollen ingesteld worden.

Wanneer men bijvoorbeeld de details van een gebruik opvraagt is onderstaand scherm te zien:



Figuur 33

Zoals te zien is kan bijna alles aangepast worden, in dit geval komt dit omdat we als administrator zijn ingelogd. Zijn we als gebruiker ingelogd dan kunnen we wel alle gegevens bekijken maar niet alles wijzigen. Hiermee zien we gelijk een nieuwe feature Mail Tips. Hiermee kunnen berichten ingesteld worden die gebruikers te zien krijgen wanneer er een mail naar deze gebruiker wordt gestuurd. Een voorbeeld hiervan is het volgende: een gebruiker stelt zijn/haar out-of-office in, normaliter zou de verzender dit pas weten wanneer hij een bericht verstuurd en vervolgens de OOF melding terugkrijgt. Met Mail Tips wordt direct wanneer de gebruiker wordt geselecteerd een bericht bovenaan de mail weergegeven met hierin een melding dat de ontvanger zijn/haar out-of-office aan heeft staan. Hiermee is ook direct zichtbaar of een gebruiker online is en zo ja of deze bezet is.

Als we verder kijken naar de optie public groups dan zien we dat we eenvoudig een nieuwe groep aan kunnen maken.



Figuur 34

Zoals je ziet is het vrij eenvoudig en is dit natuurlijk een extra mogelijkheid naast het aanmaken van een groep via de Exchange Management Console/Exchange Management Shell.

De volgende mogelijkheid is external contacts. Hiermee kunnen we contacten aanmaken welke geen Exchange mailbox hebben op de server maar welke je wel in je adressenlijst wil hebben of wil gebruiken om mail te forwarden.



Figuur 35

Administrative Roles, standaard bevat Exchange 2010 een aantal standaard rollen:

**Figuur 36**

Wanneer de optie wordt geselecteerd zal een overzicht van deze rollen worden weergegeven. Aan de rechterzijde van het scherm wordt een overzicht getoond van de rechten die deze rol heeft. In het geval van de delegated setup alleen view-only configuration. Daarnaast is het met deze optie gemakkelijk om gebruikers aan deze groep toe te voegen.

**Figuur 37**

Met User Roles is het mogelijk in te stellen wat gebruiker wel en niet mogen in de Outlook Web App. Hiermee kan bijvoorbeeld voorkomen worden dat gebruikers alle velden kunnen wijzigen van hun eigen gebruikersaccount.

**Figuur 38**

Naast deze opties is het mogelijk de optie reports te kiezen. Met deze optie is het mogelijk om te zoeken in een mailbox om te zoeken naar berichten welke verstuurd is in de afgelopen 2 weken.

**Figuur 39**

Het is ook mogelijk om compliance zoekopdrachten uit te voeren in Exchange. Dit kan ook via de ECP door de optie mailbox searches te selecteren. Wanneer je deze optie gaat vergelijken met de delivery reports zul je zien dat de resultaten van deze zoekopdracht complete berichten plaatst in een mailbox. Aangezien deze zoekopdrachten uitgevoerd kunnen worden op alle mailboxen dan het resultaat van deze zoekopdracht wel enige tijd op zich laten wachten. Via de ECP is het echter mogelijk om te zien wat de status van deze zoekopdracht is.



Figuur 40

Zoals je kunt zien zijn er al aardig wat mogelijkheden in de ECP: gebruikers aanmaken, groepen aanmaken.

Bijlage F - Importeren PST files

Handleiding:

"Importeren PST files naar een Personal Archive Mailbox in Exchange 2010 SP1"

Eén van de beperkingen van Exchange 2010 RTM was dat er geen administratieve manier bestond om historische (PST) gegevens naar het online archief te verplaatsen. Eén van die methodes die wel bestond was het handmatig slepen van mails uit PST's naar het online archief, maar dit was niet praktisch voor grote organisaties of middelgrote bedrijven.

Met de komst van Exchange 2010 SP1 zijn er een aantal dingen veranderd. We hebben nu de beschikking over de ingebouwde functionaliteit om historische gegevens te importeren vanuit de PST-bestanden en rechtstreeks naar het persoonlijke gebruikersarchief of primaire mailbox te verplaatsen. Dit kan via het New-MailboxImportRequest cmdlet. Dit cmdlet maakt het mogelijk voor een beheerder om een bulk import- en export van PST-bestanden uit te voeren zonder het gebruik van een Outlook cliënt.

Om een PST-bestand te importeren of een PST-bestanden te exporteren, moet de beheerder de juiste machtigingen hebben binnen Exchange.

Er is standaard geen RBAC Rol Group die de juiste machtigingen biedt voor deze functionaliteit. Dus wat doen we

We moeten eerst een nieuwe rol groep aanmaken die de toegang tot de *-MailboxImportRequest en *-MailboxExportRequest cmdlets verkrijgt.

New-RoleGroup "Mailbox Import-Export Management" -Roles "Mailbox Import Export"

En vervolgens een systeembeheerder toevoegen aan deze groep:

Add-RoleGroupMember "Mailbox Import-Export Management" -Member <user account>

Vervolgens moeten we bepalen waar het PST bestand zich bevindt:

Bijvoorbeeld: \\SRVNOVA099\HOMEDIRS\PSR9999\EXCHANGE\2009.pst

Nu kunnen we het New-MailboxImportRequest cmdlet gebruiken. Om het bestand naar een archive te kunnen importeren moeten we de switch **-IsArchive** gebruiken.

```
New-MailboxImportRequest -Mailbox "Ron Paars" -FilePath
\\SRVNOVA099\HOMEDIRS\PSR9999\EXCHANGE\2009.pst -IsArchive
```

Nu worden de mails naar de root van de archive mailbox verplaatst

Controleren of de import geslaagd is: **Get-MailboxImportRequest**

Optie om een target folder op te geven:

```
New-MailboxImportRequest -Mailbox "Ron Paars" -FilePath
\\SRVNOVA099\HOMEDIRS\PSR9999\EXCHANGE\2009.pst -IsArchive -
TargetRootFolder "Oude mail 2009"
```

Bijlage G - Procedure uitfasering

- Creëer Send connectors op Ex2010 HUB server;
- Configureer TLS en verander de cost;
- Routeer binnenkomende mail direct naar Ex2010;
- Verwijder internet connector op Ex2003;
- Update standaard email adres policy;
- Verplaats replica van public folders naar Ex2010;
- Verwijder Ex2003 openbare mappen;
- Multifunctionele scan- en printmachines zoals OCE of CANON voorzien van een valide SMTP benaming (PRTNOVA001@novacollege.intern) et cetera;
- Nieuwe interne SMTP server definiëren;
- DNS interne SMTP omzetten;
- Bridgehead functie srvnova051 overdragen naar Ex 2010 HUB servers;
- Tijdelijk uitzetten Ex2003 Servers;
- Oplossen van problemen die verband houden met Exchange 2003;
- Verwijder de Recipient Update service van Ex2003;
- Verwijder de Interop routing-groep;
- Dismounten en verwijderen de Ex2003 DBs;
- Verwijderen van Exchange 2003;
- Uitzetten van de Windows 2003 servers.