# High Level Technical Design

## Project Optimalisatie Infra

| | |
|---|---|
| *datum* | 23 juli 2013 |
| *op verzoek van* | VNOG |
| *versie* | 1.0 |
| *documentreferentie* | RP20120601JSl(High Level Technical Design)v1.0.docx |


| | | | | | |
|---|---|---|---|---|---|
| *bezoekadres* | Haagse Schouwweg 8b<br>2332 KG Leiden | *telefoon* | 071 - 579 70 10 | *banknummer* | 57.84.75.014 |
| | | *fax* | 071 - 579 70 11 | *bank* | ABN Amro |
| *postadres* | Haagse Schouwweg 8b<br>2332 KG Leiden | *e-mail* | info@peopleware.nl | *KvK* | 27362503 |
| | | *internet* | www.smartictsolutions.nl | *BTW nummer* | NL814547412B01 |

## Disclaimer

# Documentenbeheer

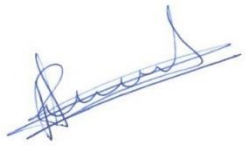
Versiebeheer

| Versie | Auteur | Aanpassingen | Datum |
|---|---|---|---|
| 1.0 | Johan Sleeuwenhoek | Final | 12-06-2013 |
| | | | |

Document review & distributie

| Naam reviewer | Organisatie | E-mail adres | Review datum |
|---|---|---|---|
| Roland van Meggelen | Icento | r.vanmeggelen@icento.nl | 07-06-2012 |
| Hans Damen | VNOG | h.damen@vnog.nl | 27-06-2012 |
| Dennis van den Akker | Icento | d.vandenakker@icento.nl | 27-06-2012 |
| Ferdinand Feenstra | Icento | f.feenstra@icento.nl | 27-06-2012 |
| Hans Damen | VNOG | h.damen@vnog.nl | 02-07-2012 |
| Bob Weber | VNOG | b.weber@it-value.nl | 02-07-2012 |

Documentgoedkeuring

| Naam | Handtekening | Datum |
|---|---|---|
| R. van Meggelen |  | 23-7 2013 |
| | | |
| | | |

# Verklarende woordenlijst

De terminologie in de ICT-branche is niet altijd eenduidig, daarom is hieronder een woordenlijst opgenomen.

| Begrip | Omschrijving |
|---|---|
| SAN | Storage Area Network. Een architectuur die centrale storage aanbiedt aan servers door middel van een eigen netwerk.<br>Een dedicated netwerk voor het transporteren van data. Vaak bestaat een SAN uit fibre channel en/of netwerk switches. |
| NAS | Network Attached Storage. Storage die aan het bedrijfsnetwerk gekoppeld is en benaderd kan worden door clients. |
| DAS | Direct Attached Storage. Storage die direct gekoppeld is aan een server. |
| SSD | Solid State Drive. Een disk zonder bewegende delen. Kenmerken van SSD zijn: Een snelle toegangs- en zoektijd, een hoge IO en een hoge kostprijs. Doordat er geen bewegende delen in zitten is de MTBF ook erg hoog. Ook is de capaciteit van een SSD disk niet zo groot als die van traditionele disken. |
| JBOD | Just a Bunch Of Disks. Een array van disken zonder bescherming tegen uitval van schijven. (RAID level). |
| RAID | Redundant Array of Independant Disks. JBOD met een beschermingsniveau tegen de uitval van een of meerdere disks.<br>RAID0 = Striping (JBOD)<br>RAID1 = Mirroring<br>RAID0+1 = Striped mirror set<br>RAID10 = Mirrored stripe set<br>RAID5 = parity disk<br>RAID6 = 2 parity disks<br>RAID50 = mirrored RAID5 set |
| LUN | Logical Unit Number. Een disk die door het SAN aangeboden wordt. |
| iSCSI | Storage over ethernet. Het aanbieden van storage aan een server op block niveau door middel van het ethernet protocol. |
| Deduplicatie | Technologie om ruimte te besparen op de storage. Kopieën van dezelfde (stukken van) data worden maar een maal opgeslagen op schijf. |
| Thin provisioning | Een methode om de lege ruimte op schijven optimaal te gebruiken. Dit gebeurt door middel van virtualisatie. Kort gezegd wordt de lege ruimte op een LUN niet gekoppeld aan een fysieke schijf. Pas wanneer de lege ruimte wordt beschreven wordt er fysieke diskruimte toegekend. |
| Storage Virtualisatie | Een laag tussen de fysieke disken en de logische disken. Deze laag biedt meer flexibiliteit en mogelijkheden in het aanbieden van storage, zoals snapshots, restores, etc. |
| BYO | Bring Your Own. Het aanbieden van de diensten op dusdanige wijze dat gebruikers eigen devices (smartphones, tablets, etc.) eenvoudig kunnen koppelen aan de infrastructuur. |
| CYO | Choose Your Own. De gebruikers laten kiezen tussen een aantal voorgeschreven combinaties van devices. Dit kan in de vorm van een budget met een lijst met goedgekeurde devices of in de vorm van een aantal vaststaande configuraties. |
| Information Workers | Alle gebruikers van ICT. Opgedeeld in drie groepen: Knowledge Workers, Task Workers en Data Entry Workers. |
| Knowledge Workers | De Knowledge Workers werkt met ideeën en managen teams. Ze creëren, verbruiken, transformeren en analyseren data. Ze moeten informatie snel en eenvoudig kunnen vinden. Knowledge Workers bouwen en verbeteren business processen |
| (Structured) Task Workers | De Task Worker werkt met data en informatie. Ze creëren en gebruiken informatie. Ze moeten informatie snel en eenvoudig kunnen vinden, editen en opslaan. Globaal gezien omvat deze groep ongeveer 80% van alle medewerkers van een organisatie. |
| Data Entry Workers | De Data Entry Worker creëert en gebruikt informatie volgens vastgelegde procedures en formulieren. |

# Inhoudsopgave

# Hoofdstuk 1 Inleiding

## 1.1 Aanleiding

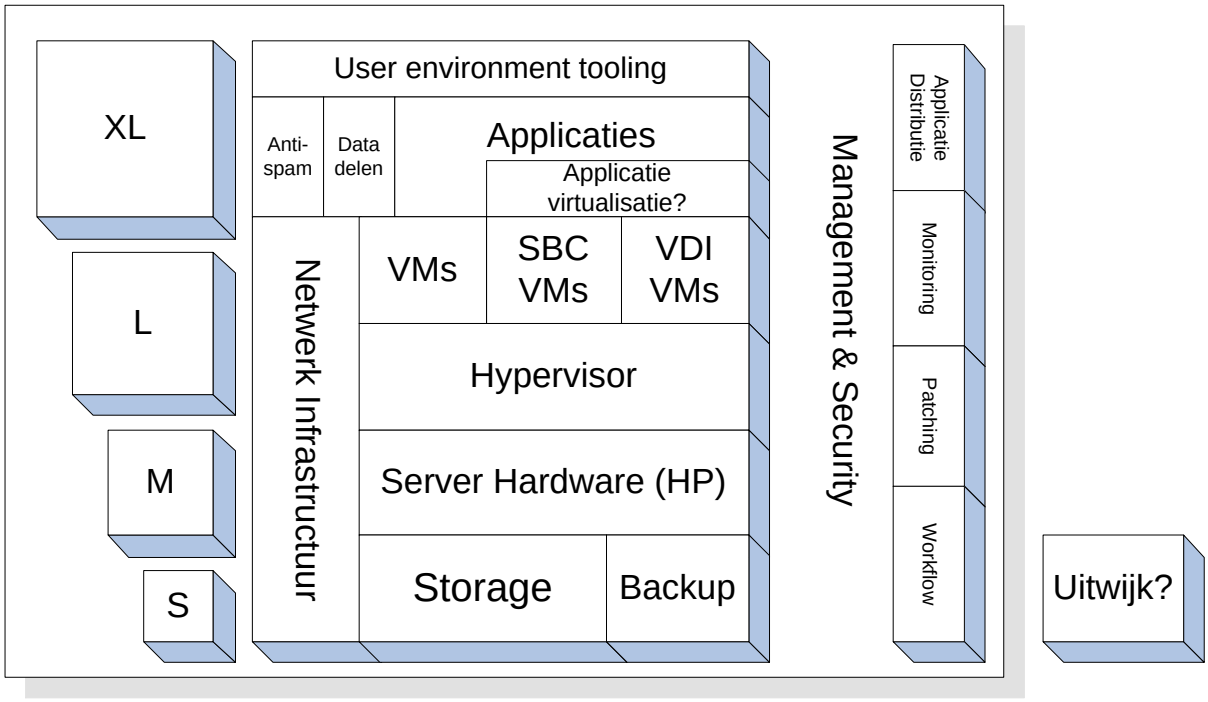
De infrastructuur van de VNOG heeft zijn capaciteit op enkele punten bereikt. Bij het ontwerp van de huidige architectuur is geschaald voor drie jaar. Deze termijn is bijna verstreken.

## 1.2 Probleemstelling

Het doel van dit document is het opstellen van een High Level Technical Design voor de nieuwe infrastructuur. Dit document beschrijft het ontwerp en de keuzes die gemaakt zijn.

# Hoofdstuk 2 Architectuur

Het ontwerp voor de nieuwe omgeving is gebaseerd op de volgende architectuur zoals deze in de expertgroep is behandeld.




In de volgende hoofdstukken worden de diverse elementen uit de architectuur uitgewerkt.

## 2.1 Integratie OIV

Operationele Informatievoorziening (OIV) is de 'warme' tak van de VNOG. De Kantoorautomatisering (KA) is de 'koude' tak. OIV voorzien in de informatie die de brandweer nodig heeft in de operatie. 3 jaar geleden was de OIV omgeving nog een onbekende. Inmiddels is deze uitgekristalliseerd. Ze bestaat uit een aantal VMWare ESXi servers met daarop diverse VMs, waaronder Linux systemen. Doordat de ESX systemen los van elkaar draaien en niet in cluster, is er een overcapaciteit aan de VMWare kant, zie paragraaf VMWare. De OIV omgeving kan geïntegreerd worden met de KA omgeving. Op deze wijze kan de beschikbaarheid van de OIV omgeving verbeterd worden en worden de beschikbare resources optimaal ingezet.

# Hoofdstuk 3 Naamconventie

Een eenduidige naamconventie van de systemen en active componenten bij de VNOG is essentieel om de omgeving goed te kunnen beheren. Het voorkomt verwarring over componenten en miscommunicatie.

## 3.1 Domein

| NETBIOS naam | FQDN naam |
|---|---|
| **VNOG** | vnog.intra |

## 3.2 Site namen

| Code | Volgnummer | Plaatsnaam |
|---|---|---|
| ***3 karakters*** | *2 karakters* | *Volledig* |
| **APE** | 01-99 | Apeldoorn |

Voorbeeld:
APE01 voor de eerste site in Apeldoorn.

## 3.3 Werkstations

| Type | Volgnummer |
|---|---|
| ***1 karakter*** | *2 karakters* |
| **L = Laptop**<br>**D = Desktop** | 0001-9999 |

Voorbeeld:
L0004 is laptop nummer vier.
D0018 is desktop nummer 18.

## 3.4 Printers

| Type | Verdieping | Locatie | Volgnummer |
|---|---|---|---|
| ***1 karakter*** | *1 karakter* | *4 karakters* | *2 karakters* |
| **P = Laserprinter**<br>**K = Kleurenprinter** | Etage nummer | Omschrijving van de Locatie. | 01-99 |

Voorbeeld:
P4VERG01 is de printer in de vergaderzaal op de 4e verdieping.
K5GANG03 is de derde kleurenprinter op de gang van de 5e verdieping.

## 3.5 Randapparatuur

| Code | Volgnummer | Plaatsnaam |
|---|---|---|
| ***1 karakter*** | *karakters* | *2 karakters* |
| **N = Netwerk**<br>**M = SAN devices** | Omschrijving van de functionaliteit. | 01-99 |

Voorbeeld:
NFW01 voor de eerste firewall.
NSW04 voor de 4e switch.
MSA01 voor de productie SAN.
MSW01 voor de 2e SAN switch.

### 3.6 Servers

| Type | Functionaliteit | Volgnummer |
|---|---|---|
| ***1 karakter*** | *2 karakters* | *2 karakters* |
| **V = Virtuele server**<br>**S = Fysieke server**<br>**T = Testserver** | Omschrijving van de functionaliteit. | 01-99 |

Voor de omschrijving van de functionaliteit wordt de volgende tabel gehanteerd.

| Afkorting | Functionaliteit |
|---|---|
| **AP** | Applicatie |
| **BA** | Backup |
| **CD*** | Citrix Datacollector server |
| **CL*** | Citrix License server |
| ~~**CX**~~ | ~~Citrix~~ |
| **DB** | Database |
| **DC** | Domain Controller |
| **EX** | Exchange |
| **FP** | File en Print |
| **FW** | Firewall |
| **GE** | Geoserver |
| **LB** | Load Balancer |
| **LO** | Locatie server |
| **MA** | Management |
| **PX** | Citrix Gateway appliance |
| **SA** | SAN Storage |
| **SD** | Security Device |
| **SS** | Stepping Stone |
| **SP*** | Sharepoint |
| **SW** | SAN Switch |
| **VS** | Hypervisor |
| **WB** | Webserver |
| **WI** | Citrix Web Interface |
| **XA*** | Citrix XenApp server |
| **XD*** | Citrix XenDesktop Delivery Controller |

~~XX~~ = legacy
* Nieuw

Voorbeeld:
VDB01 is de eerste virtuele databaseserver.
SDC02 is de tweede fysieke domain controller.
TAP02 is de tweede test applicatie server.

### 3.7 Gebruikers

| Achternaam | Voorletter |
|---|---|
| ***2-19 karakters*** | *1 karakter* |
| **Maximaal 19 karakters** | Initiaal |

NB: bij dubbele of lange namen kan systeembeheer de naam bepalen.

Voorbeeld:
Cleefg is de loginnaam van Gerry van Cleef.
Sleeuwenhoekj is de loginnaam voor Johan Sleeuwenhoek.

### 3.8 Administrator accounts

| Functie | Punt | Voornaam |
|---|---|---|
| ***3 karakters*** | *1 karakter* | *2-16 karakters* |
| **adm** | . | voornaam |

Voorbeeld:
adm.gerry is de administrator login van Gerry van Cleef.
adm.johan is de administrator login voor Johan Sleeuwenhoek.

### 3.9 Service accounts

| Functie | Punt | Omschrijving |
|---|---|---|
| ***3 karakters*** | *1 karakter* | *2-16 karakters* |
| **svc** | . | Een omschrijving van de functie |

Voorbeeld:
svc.exchange is het service account voor Exchange.
svc.decos is het service account voor Decos.

### 3.10 E-mail addressen

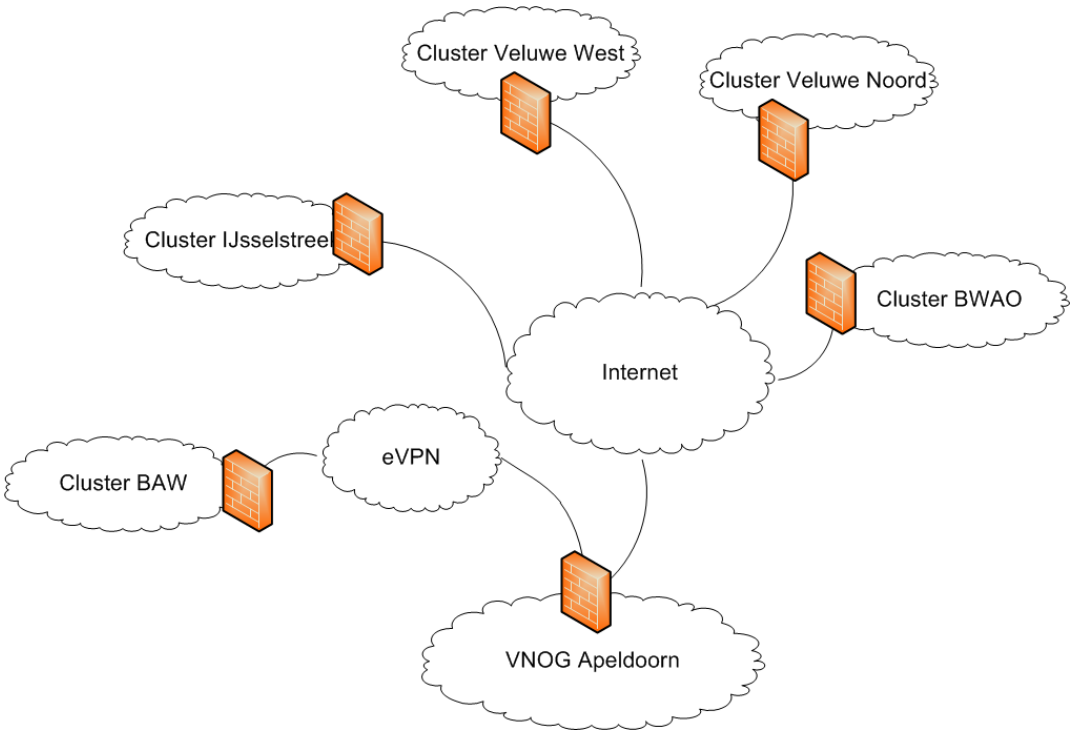
| Voorletter | | Achternaam | | Domein | | |
|---|---|---|---|---|---|---|
| ***1 karakter*** | | *xx karakters* | | *xx karakters* | | *Toplevel domain* |
| **g** | . | vancleef | @ | vnog | . | nl |
| **g** | . | vancleef | @ | veiligheidsregio-nog | . | nl |
| **g** | . | vancleef | @ | bwao | . | nl |

NB: elke gebruikers krijgt 2 e-mail addressen. Een eventueel tussenvoegsel wordt voluit na de punt opgenomen in het email adres. Het @bwao.nl is optioneel en zal niet automatisch worden toegekent aan nieuwe gebruikers.

Voorbeeld:
Gerry van Cleef wordt g.vancleef@vnog.nl en g.vancleef@veiligheidsregio-nog.nl.
Johan Sleeuwenhoek wordt j.sleeuwenhoek@vnog.nl en j.sleeuwenhoek@veiligheidsregio-nog.nl.

# Hoofdstuk 4 Netwerk services

In dit hoofdstuk worden de onderwerpen IP adressering, DNS, WINS, DHCP, en Time service behandeld. Deze ontwerpkeuzes stammen uit het ontwerp van de huidige infrastructuur en zijn hier opgenomen ter volledigheid van dit document. Bijgaande afbeelding geeft een overzicht van de netwerk infrastructuur.




**Figuur 1 Netwerk infrastructuur**

Bijgaand een overzicht van de kantoorlocaties van de VNOG.

| Cluster | Adres |
|---|---|
| **Hoofdkantoor VNOG/meldkamer** | Europaweg 79<br>7336 AK Apeldoorn |
| **Cluster BAW (Achterhoek West)** | C. Missetstraat 6<br>7005 AB Doetinchem |
| **Cluster Veluwe West** | Burgemeester de Meesterstraat 3<br>3846 AA Harderwijk |
| **Cluster BWAO (Achterhoek Oost)** | Raadhuisstraat 7<br>7131 CL Lichtenvoorde |
| **Cluster IJsselstreek** | Gerard Doustraat 129<br>7204 EW Zutphen |
| **Cluster Veluwe Noord** | Oostendorperstraatweg 8<br>8081 RK Elburg |
| **Cluster EVA (Epe, Voorst, Apeldoorn)** | Deventerstraat 21 (centerpoint-gebouw)<br>7311 BH Apeldoorn |

### 4.1 IP nummerplan

Om problemen te voorkomen met de politie die in de 10 range, en de GMA die in de 172.16 range opereert, is er gekozen voor de 172.17 t/m 172.31 range. Voor alle andere netwerken (DMZ, interconnect, untrusted e.d.) zal de 192.168 range gebruikt worden.

| Lokatie | Range | Subnetmask | Max aantal hosts |
|---|---|---|---|
| **Nieuwbouw** | 172.17.0.0 – 172.17.255.255 | 255.255.0.0 | 65534 |
| **Cluster BAW** | 172.18.0.0 – 172.18.34.255 | 255.255.224.0 | 8190 |
| **Cluster Veluwe West** | 172.18.32.0 – 172.18.63.255 | 255.255.224.0 | 8190 |
| **Cluster BWAO** | 172.18.64.0 – 172.18.95.255 | 255.255.224.0 | 8190 |
| **Cluster IJsselstreek** | 172.18.96.0 – 172.18.127.255 | 255.255.224.0 | 8190 |
| **…** | … | …. | … |
| **Cluster 104** | 172.31.224.0 – 172.31.255.255 | 255.255.224.0 | 8190 |

Dit ontwerp biedt de mogelijkheid voor 13 x 8 = 104 clusters.

De IP range voor de DMZ en Interconnect netwerken hoeft niet zo groot te zijn en kan gekozen worden uit de 192.168.0.0/16 range.

| Range | Naam | Subnetmask | Max aantal hosts |
|---|---|---|---|
| **192.168.60.0/24** | Private DMZ | 255.255.255.0 | 254 |
| **192.168.70.0/24** | Interconnect | 255.255.255.0 | 254 |
| **192.168.75.0/24** | Public DMZ | 255.255.255.0 | 254 |

De IP range voor de eVPN verbindingen hoeft niet zo groot te zijn gekozen uit de 172.31.0.0/16 range.

| Locatie | Subnet | IP Adres A'doorn | IP Adres Cluster | VLAN |
|---|---|---|---|---|
| **Cluster BAW** | 172.31.224.0/24 | 172.31.224.254/24 | 172.31.224.1/24 | 801 |
| **Cluster IJsselstreek** | 172.31.225.0/24 | 172.31.225.254/24 | 172.31.225.1/24 | 802 |
| **…** | … | … | … | … |

### 4.2 Subnets

Binnen de gekozen range kan er een opdeling gemaakt worden in subnets. Bijgaande tabel geeft een overzicht van de subranges met de type devices.

| Subnet | Subnet mask | Devices |
|---|---|---|
| **172.17.2.0/24** | 255.255.255.0 | Network management |
| **172.17.5.0/24** | 255.255.255.0 | Beheer (admins, iLo, etc.) |
| **172.17.10.0/24** | 255.255.255.0 | Backoffice (servers) |
| **172.17.16.0/21** | 255.255.248.0 | Frontoffice (werkstations) |
| **172.17.24.0/24** | 255.255.255.0 | Printer |
| **172.17.25.0/24** | 255.255.255.0 | Opleiding |
| **172.17.30.0/24** | 255.255.255.0 | Backup |
| **172.17.50.0/24** | 255.255.255.0 | Guest |

De default gateway van elk subnet is het laatste host IP adres van de range.

Voorbeeld:
172.17.10.0/24 → GW: 172.17.10.254
172.17.16.1/21 → GW: 172.17.23.254

### 4.3 VLAN configuratie

Door gebruik te maken van Virtual LAN technologie kunnen verkeerstromen gescheiden worden. Om componenten uit verschillende VLAN's toegang te geven tot elkaar wordt gebruik gemaakt van Inter VLAN routing. Toegang en restricties tussen VLANs kunnen worden bereikt d.m.v. VLAN Access Lists (ACL).
De volgende VLANs worden gedefinieerd. De nummering loopt op naarmate het netwerk minder belangrijk is vanuit beveiligingsoogpunt.

| VLAN | Subnet + mask | Naam | Omschrijving |
|---|---|---|---|
| **2** | 172.17.2.0/24 | Network management | Network management, Netwerk/Cisco componenten |
| **5** | 172.17.5.0/24 | Beheer | Beheer (admins, iLo, etc.) overige infra |
| **10** | 172.17.10.0/24 | BackOffice | Backoffice, servers en IT gerelateerde werkstations |
| **16** | 172.17.16.0/22 | FrontOffice WLAN | Frontoffice WLAN, werkstations |
| **20** | 172.17.20.0/22 | FrontOffice LAN | Frontoffice LAN, werkstations |
| **24** | 172.17.24.0/24 | Printer | Printers en scanners |
| **25** | 172.17.25.0/24 | Opleiding | Opleidingsomgeving |
| **30** | 172.17.30.0/24 | Backup | Backup netwerk |
| ~~**31**~~ | ~~172.17.31.0/24~~ | ~~VMotion~~ | ~~VMotion netwerk~~ |
| **32** | 172.17.32.0/24 | iSCSI | iSCSI netwerk, wordt gebruikt op de NSW04 |
| **40** | 172.17.40.0/24 | Voice | Alle telefonie IP devices. |
| **50** | 172.17.50.0/24 | Guest | Pre- NAP Guest VLAN. |
| **60** | 192.168.60.0/24 | DMZ | Private DMZ gekoppeld aan ISA |
| **70** | 192.168.70.0/24 | Interconnect | Netwerk tussen de Firewall en de ISA. Hier mogen geen andere devices opkomen. Internet services worden op dit VLAN aangeboden |
| **71** | ? | ? | OVOS, RBS netwerk |
| **75** | 192.168.75.0/24 | Public DMZ | Public DMZ gekoppeld aan de externe firewall |
| **77** | ? | Koppelvlak | Koppelvlak |
| | | | |
| **80** | 195.7.142.64/28 | Untrusted | Directe toegang tot de internetverbinding |
| **100** | 172.17.100.0/24 | Test LAN | Netwerk voor testdoeleinden |
| **110*** | 172.17.110.0/24 | TMG NLB | TMG unicast NLB verkeer |
| **111*** | 172.17.111.0/24 | Hyper-V heartbeat | Hyper-V Cluster heartbeat |
| **112*** | 172.17.112.0/24 | Hyper-V CSV | Hyper-V CSV |
| **113*** | 172.17.113.0/24 | Hyper-V Live Migration | Hyper-V Live Migration |
| **114*** | 172.17.114.0/24 | TMG Internal | TMG connectie naar interne netwerk |
| **115*** | 192.168.115.0/24 | TMG External | TMG connectie naar DMZ netwerk |

~~Xx~~ te verwijderen VLAN
* Nieuw VLAN

### 4.4 DNS

Er moet een ontwerpbeslissing worden genomen ten aanzien van de gehanteerde naamgeving die voor de DNS structuur gaat worden gebruikt. De volgende overwegingen spelen bij deze keuze een rol:

- **Identiteit:** Een DNS domeinnaam kan worden gebruikt om de identiteit van het bedrijf te benadrukken. Dit is met name belangrijk op het Internet. Voor Intranet is dit belang een stuk minder groot en zijn er technisch geen voor- of nadelen verbonden aan het al dan niet kiezen voor een domeinnaam die overeenkomt met de naam van de organisatie;
- **Beheer:** de keuzes voor verschillende DNS domeinnamen hebben verschillende impact op de mate van beheer. In het geval gekozen wordt voor identieke domein namen voor zowel het interne als externe DNS domein, zal er een grote verantwoordelijkheid liggen bij de beheerorganisatie. Het aanbrengen van een goede scheiding tussen interne en externe geclassificeerde informatie vereist een relatief grote beheerinspanning waarbij de kans op fouten relatief groot is. In het geval het interne DNS domein niet dezelfde naam heeft als het externe DNS domein, is de kans op fouten op dit gebied geminimaliseerd omdat visuele verschillen aanwezig zijn;
- **Beveiliging:** De beveiliging van informatie binnen de VNOG omgeving is van groot belang. Er moet voorkomen worden dat ongeautoriseerde toegang tot informatie mogelijk wordt. Deze eis is het beste te implementeren binnen een DNS model met gescheiden interne en externe naamgeving;
- **Hanteerbaarheid:** Vanuit gebruikersoogpunt moet de naamgeving zinvol zijn, zodat informatie waarin de DNS naamgeving verwerkt is, zoals bijvoorbeeld URL's, een extra betekenis krijgt;
- **Registratie:** Het verdient aanbeveling om – indien mogelijk – gebruikte DNS namen te registreren bij de daartoe bevoegde instanties. Indien dit niet wordt gedaan, bestaat de mogelijkheid dat het domein wordt geregistreerd door een niet aan VNOG gelieerde organisatie. Uit beheeroogpunt is dit niet een gewenste situatie.

Met betrekking tot de interne DNS domeinnaam zijn er een tweetal opties.

1. Maak de interne DNS domeinnaam gelijk aan de externe naam 'vnog.nl'.
2. Maak de interne DNS domeinnaam ongelijk aan de externe DNS domein naam.

De eerste ontwerpkeuze is dat de interne DNS domeinnaam niet gelijk wordt aan de externe DNS domeinnaam. Deze keuze is de meest optimale keuze wanneer de aspecten beheer en security worden beoordeeld. Ten aanzien van de aspecten hanteerbaarheid en registratie is er geen argumentatie die anders aangeeft.

**Ontwerpbeslissing:**

- De intern DNS domeinnaam wordt gescheiden van de externe DNS domeinnaam.

Deze beslissing is gebaseerd op de volgende punten:

- Huidige infrastructuur;
- Best practice.

In vervolg op de eerste ontwerpkeuze zal er een DNS naam moeten worden vastgesteld. De interne DNS domeinnaamgeving moet worden vastgesteld aan de hand van dezelfde bovenstaande overwegingen, waarbij hanteerbaarheid en registratie de belangrijkste factoren zijn.

De tweede ontwerpkeuze is dat de interne DNS root-domeinnaam wordt gesteld op 'vnog.intra'.

- Zichtbaar verschil;
- De veelgebruikte root-domeinnaam .local kan door sommige DNS systemen (voornamelijk Sun) niet goed worden opgepakt.

**Ontwerpbeslissing:**

- Interne DNS domein naam AD root domein is: vnog.intra.

Deze beslissing is gebaseerd op de volgende punten:

- Huidige infrastructuur;
- Best practice.

Het gekozen DNS ontwerp staat toe dat wanneer er organisatorische redenen zijn om andere DNS subdomeinen te introduceren, dit mogelijk is.

De basis van de VNOG is het interne DNS domein 'vnog.intra'. De DNS naamgeving vormt de basis voor de Active Directory domein naamgeving. In Active Directory zijn er ook mogelijkheden om bepaalde beheertaken binnen het domein te kunnen delegeren. Indien tijdens het Active Directory ontwerp gekozen wordt voor een structuur met meerdere domeinen in een forest, dan zijn de objecten binnen het Active Directory forest eenvoudig te verhuizen tussen de domeinen binnen het forest.

| Zone | Doel | Type |
|---|---|---|
| **.[root]** | Root zone | AD integrated |
| **vnog.intra** | Container voor Active Directory domein | AD integrated |

Voor reverse lookup wordt in het forest root domein de volgende zone aangemaakt:

| Zone | Doel | Type |
|---|---|---|
| **172.in-addr.arpa** | Reverse lookup zone voor de VNOG | AD integrated |

### 4.5 WINS

Hoewel Windows primair DNS gebruikt voor naamresolutie, is WINS nog steeds noodzakelijk in complexe omgevingen waar NetBIOS enabled applicaties gebruikt worden. In een complexe gerouteerde omgeving, waarbij gebruik gemaakt wordt van Windows NT of Windows 9.x clients en/of er wordt gebruik gemaakt van applicaties die het NetBIOS protocol gebruiken, dan is de aanwezigheid van WINS noodzakelijk. Het NetBIOS protocol is niet routable, dit betekent dat zonder de WINS service geen naamresolutie gedaan kan worden naar computers in een ander subnet. Gezien de nieuwe omgeving en met de kennis van de huidige omgeving is het inrichten van een WINS infrastructuur niet nodig.

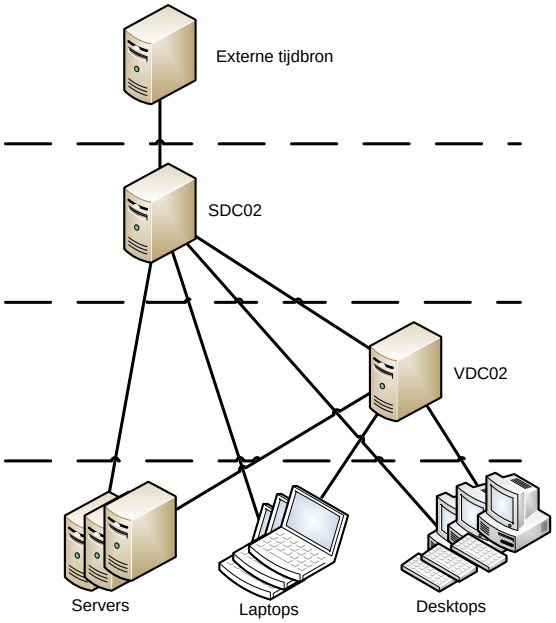
**Ontwerpbeslissing:**
- WINS wordt niet ingericht.

Deze beslissing is gebaseerd op de volgende punten:
- Huidige infrastructuur;
- Best practice.

Mocht overhoopt blijken dat er nog legacy applicaties of operating systemen zijn die WINS vereisen kan dit eenvoudig geimplementeerd worden. Beide DC's zullen dan tevens WINS server worden voor het domein VNOG.

## 4.6 Time Service

De fysieke domaincontroller worden ingezet als primary time server. Deze server synchroniseert met een externe tijdserver. De virtuele domaincontroller zal synchroniseren met de fysieke domeincontrollers. De resterende servers en clients zullen de tijd synchroniseren met de domaincontrollers. Schematisch ziet dit er als volgt uit.



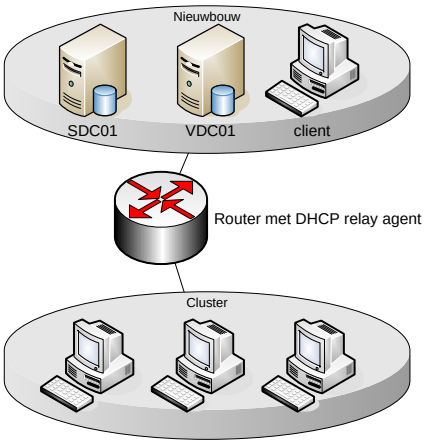

**Figuur 2 Time services**

Aangezien Hyper-V een eigen tijdsynchonisatiemethode onderhoudt met de VMs, wordt voor de tweede domaincontroller de tijdsynchronisatie met Hyper-V uitgeschakeld door middel van het volgende commando.

```
reg add HKLM\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\VMICTimeProvider
/v Enabled /t reg_dword /d 0
```

## 4.7 DHCP

In onderstaande figuur is de topologie voor de VNOG weergegeven. Op de centrale locatie wordt de DHCP service geïnstalleerd op beide domein controllers.




**Figuur 3 DHCP infrastructuur**

Om de DHCP service ook op de clusters aan te kunnen bieden gebruik wordt op alle relevante routers de UDP helper (DHCP relay agent) ingeschakeld.

**Ontwerpbeslissing:**
- UDP helper (DHCP relay agent) wordt gebruikt op clusterlocaties.

Deze beslissing is gebaseerd op de volgende punten:
- Huidige infrastructuur.

De leaseperiode bepaalt de periode waarin een client van een IP adres gebruik kan maken zonder een nieuwe aanvraag te doen. Een korte periode genereert meer netwerkverkeer maar garandeert een snelle vrijgave van IP adressen. Omdat de IP range van de VNOG over voldoende IP adressen beschikt kan worden volstaan met een leaseperiode van 7 dagen het geen het netwerkverkeer beperkt.

**Ontwerpbeslissing:**
- Lease periode is 7 dagen.

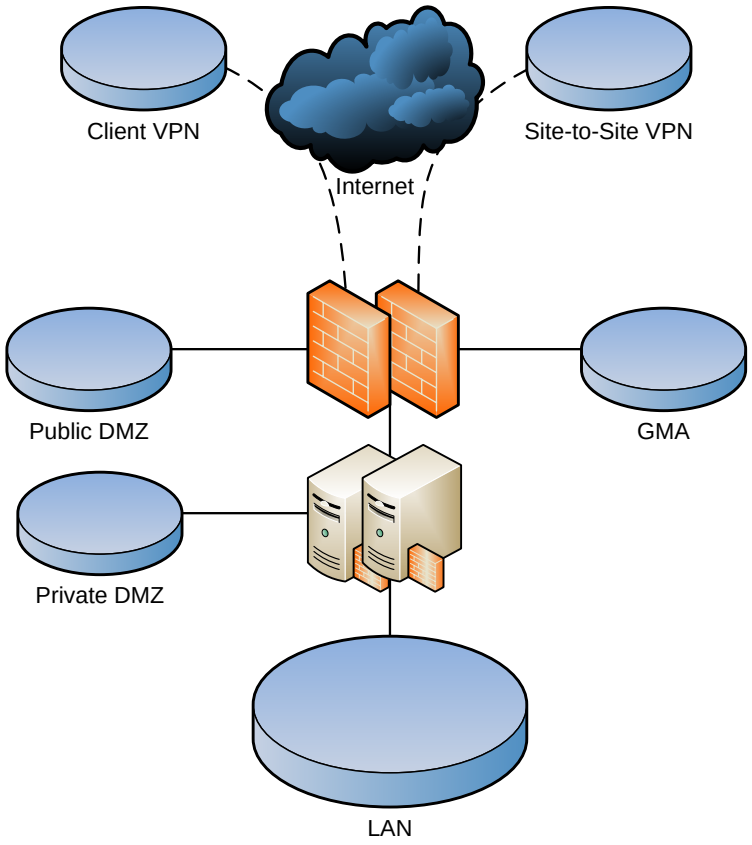
Deze beslissing is gebaseerd op de volgende punten:
- Huidige infrastructuur.

De DHCP instellingen die worden geconfigureerd bij de server opties worden standaard overgenomen door alle scopes. Als een zelfde parameter zowel bij de server opties als bij de scope opties opgegeven wordt, dan wordt de optie die in de scope staat uitgevoerd.
Voor de infrastructuur wordt één scope gedefinieerd.

| | Optie | Instelling |
|---|---|---|
| **003** | Router | 172.17.23.254 |
| **06** | DNS Servers | 172.17.10.1, 172.17.10.101 |
| **15** | DNS Domain name | vnog.intra |

# Hoofdstuk 5 Firewall

De Juniper SSG-140 is nu in gebruik. De SSG-140 zal worden ingezet als front-end firewall. Er wordt een redundante firewall configuratie geplaatst bij de VNOG met een dubbele front-end firewall en een Microsoft TMG array als back-end firewall. VPN tunnels naar andere clusters en locaties zullen tussen op de front-end firewall worden gemaakt.



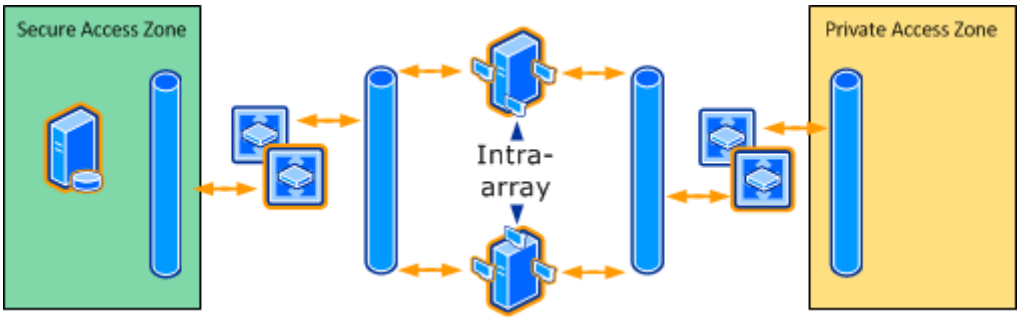

**Figuur 4 Firewall infrastructuur**

## 5.1 Juniper firewall

De SSG-140 zal in een active-passive HA opstelling worden geplaatst. Koppelingen met extranet partijen zoals de GMA worden op de frontend firewall gemaakt.

## 5.2 Microsoft Forefront Threat Management Gateway

TMG 2010 is de opvolger van ISA 2006. Het bestaande ISA cluster wordt gemigreerd naar een virtueel TMG cluster en ingezet als back-end firewall. Zie bijgaande afbeelding voor de architectuur.




**Figuur 5 TMG architectuur**

Voor unicast NLB in een apart VLAN is gekozen als best practice en aanbeveling van Microsoft boven multicast eventueel in combinatie met IGMP. Er is voor twee nodes gekozen voor hoge beschikbaarheid en een enkele node kan de load aan van de berekende capaciteit.

**Ontwerpbeslissing:**
- Unicast NLB in apart VLAN.

Deze beslissing is gebaseerd op de volgende punten:
- Best practice.

Voor de TMG array worden de volgende IP ranges gebruikt.

| Network | IP range | VLAN |
|---|---|---|
| **Internal** | 172.17.114.0/24 | 114 |
| **External** | 192.168.115.0/24 | 115 |

Voor beheer van de omgeving is er een aparte Forefront TMG 2010 Enterprise Management Server (EMS) waarop de configuratie wordt opgeslagen. De Forefront TMG 2010 nodes halen de configuratie informatie vanaf de EMS op en bewaren lokaal een read-only kopie.
De EMS is een virtuele server.

**Ontwerpbeslissing:**
- EMS vitueel uitvoeren.

Deze beslissing is gebaseerd op de volgende punten:
- Best practice.

TMG 2010 moet hoog beschikbaar ingericht worden hier zijn Enterprise licenties voor TMG noodzakelijk. Voor de EMS servers hoeven geen licenties aangeschaft te worden, deze zitten in de Enterprise versie van TMG.

| Software | Editie | aantal |
|---|---|---|
| **TMG 2010** | Enterprise | 2 licenties |

# Hoofdstuk 6 Directory

Active Directory Domain Services (ADDS) is de directory service van het Windows Server 2008 R2 besturingssysteem. Het is de Microsoft directory implementatie afgeleid van het bestaande X.500 model. De gegevens die binnen ADDS worden gebruikt door een groot aantal componenten van het Windows Server 2008 R2 besturingssysteem en de daarop aanwezige services. Een aantal van de functies die met behulp van ADDS worden gerealiseerd zijn functies als authenticatie, autorisatie en het bieden van directory services. Het maakt het gebruik mogelijk van organisatiebrede toepassingen zoals E-mail. ADDS is daarmee het fundament van de infrastructuur en de daarop geboden services. Een correcte architectuur en inrichting van ADDS is dan ook cruciaal voor een succesvolle inrichting.

## 6.1 Ontwerpbeslissingen

**Ontwerpbeslissing:**
- Huidige domain level wordt bijgewerkt naar Windows Server 2008 R2.

Deze beslissing is gebaseerd op de volgende punten:
- Best practice;
- Toekomstbestendigheid infrastructuur.

Het huidige Active Directory ontwerp blijft als volgt.

| Beslissing | Keuze |
|---|---|
| **Forest (voor productie)** | Single Forest |
| **Domain (voor productie)** | Single Domain |
| **Root domain** | vnog.intra |
| **NETBIOS Naame** | VNOG |
| **Wanneer is er sprake van een site** | voor elke groep IP-subnetten die met elkaar verbonden zijn via WAN-snelheid verbindingen |
| **Site replicatie protocol** | RPC |
| **Site** | IP subnets in LAN |
| **Replicatie interval** | 30 minuten |
| **Domain Controller plaatsing** | In het datacenter worden twee DC's geïnstalleerd, de SDC02 en de VDC02 |
| **Global Catalog** | Iedere eerste DC op een site wordt Global Catalog server. |
| **FSMO rollen** | De FSMO rollen worden als volgt verdeeld over de DC's in het datacenter:<br>SDC02: Domain Naming Master, Schema Master<br>VDC02: PDC Emulator, RID Master, Infrastructure Master |
| **Bridgehead Server** | Bridgehead servers worden automatisch door de KCC aangewezen. |

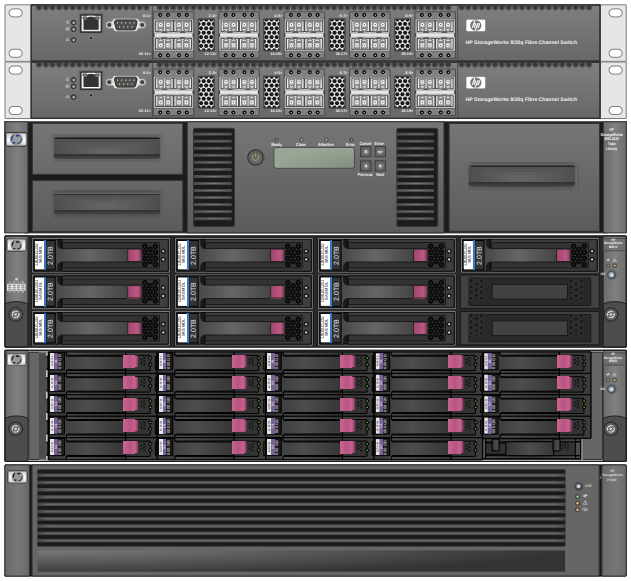
De OU structuur ziet er als volgt uit:

| Beslissing | Keuze |
|---|---|
| **Basis Structuur** | Centrale beheerstructuur |
| **Objecten Structuur** | Op basis van afdeling en applicatie |
| **Delegatie** | Mogelijk per Organisational Unit |
| **Laag 1 OU-structuur** | Builtin, VNOG, Computers, Domain Controllers en Users |
| **Laag 2 OU-structuur** | VNOG: Admins, Computers, Groups, Printers, Servers, Users |
| **Laag 3 OU-structuur** | Computers: Desktops, Laptops en Specials. Groups: Application, Distribution en Security.<br>Users: Centralisten, Concern, Achterhoek, Externen, GHOR, ICT, NW-Veluwe, Rcc Accounts en Test. |

# Hoofdstuk 7 Storage

## 7.1 SAN

De storage is opgebouwd uit een HP EVA6300 en de bestaande MSL2024 tapelibrary met de volgend configuratie:




**Figuur 6 Storage configuratie**

Er zijn drie type storage te onderscheiden, te weten:

- **Primary** of **Tier 1** storage. Dit zijn de 24 600GB 10k schijven in de HP EVA P6300;
- **Nearline** of **Tier 2** storage, Dit zijn de 10 2TB 7.2k schijven in de HP EVA P6300;
- **Backup** of **Tier 3** storage bestaat uit de MSL2024 tapelibrary met LTO4 drive.

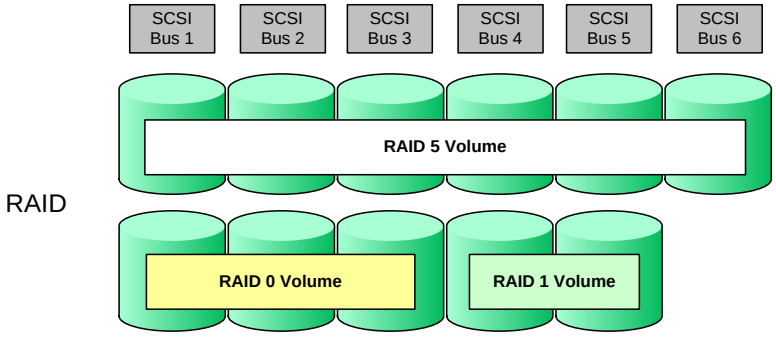
Deze oplossing biedt de volgende IOPS en capaciteit.

| Tier | Type | Storagetype | Aantal | IOPS per disk | Bruto capaciteit | Netto RAID1 | Netto RAID5 |
|---|---|---|---|---|---|---|---|
| **1** | Primary | 600GB 10k | 24 | 100~130 | 14,4 TB | 7,2 TB | 12,6 TB |
| **2** | Nearline | 2TB 7.2k | 10 | 75~100 | 20 TB | 10 TB | 18 TB |

## 7.2 Storage virtualisatie

Een HP EVA als SAN heeft als grootste voordeel t.o.v. een HP MSA dat er storage virtualisatie toegepast kan worden. Dit wordt gedaan met o.a. Virtual RAID (VRAID) sets.

Bij de traditionele manier van inrichten van opslag omgevingen wordt een specifiek aantal disk drives aangewezen om een bepaalde mate van redundantie te bieden (zo ook bij de HP MSA die VNOG nu in gebruik heeft). Hierbij geldt dat een RAID 0+1 set een hoge mate van redundantie biedt maar het dubbele aantal schijven vereist t.o.v. de benodigde netto capaciteit. Een RAID 5 biedt lagere mate van redundantie, maar vereist slechts één schijf meer dan voor de gewenste capaciteit nodig is (N+1 redundantie). RAID 0 kent geen redundantie maar biedt, in vergelijking met RAID 1 en RAID 5, de hoogste performance.



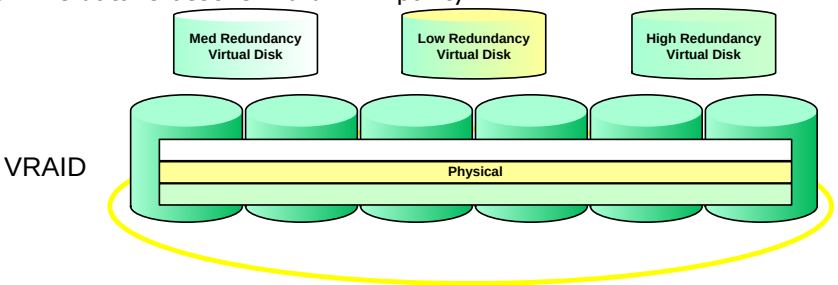

**Figuur 7 RAID sets**

De genoemde traditionele RAID techniek vergt een goede planning van de gewenste situatie voordat volumes geconfigureerd worden. Het uitvoeren van wijzigingen in bestaande omgevingen is tijdrovend en vergt de inzet van specialisten. Een zekere mate van flexibiliteit kan worden verkregen door het toepassen van virtualisatie op server niveau. Deze software biedt de mogelijkheid om de door het array aangeboden volumes op te nemen in een storage pool per server.

Een Enterprise Virtual Array (HP EVA) maakt gebruik van de VRAID techniek. Op basis van benodigde capaciteit en gewenste redundantie bepaalt de controller hoeveel en welke disk drives benodigd zijn om dit te realiseren. Er bestaat geen direct verband tussen een geconfigureerd volume en de onderliggende schijven.

Ten behoeve van redundantie worden drie niveaus onderscheiden:

- **VRAID0**: Geen fouttolerantie;
- **VRAID1**: Alle data is gedupliceerd binnen het storage systeem. Dit is de hoogste fout tolerantie;
- **VRAID5**: Alle data is beschermd d.m.v. parity.



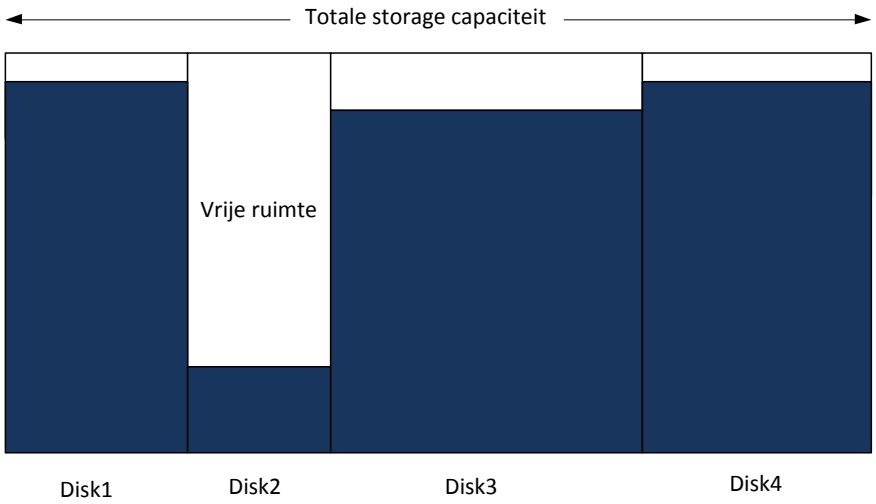

**Figuur 8 VRAID technologie**

**Ontwerpbeslissing:**
- HP EVA storage virtualisatie wordt ingezet.

Deze beslissing is gebaseerd op de volgende punten:
- Verhogen flexibiliteit van de inzet van storage.

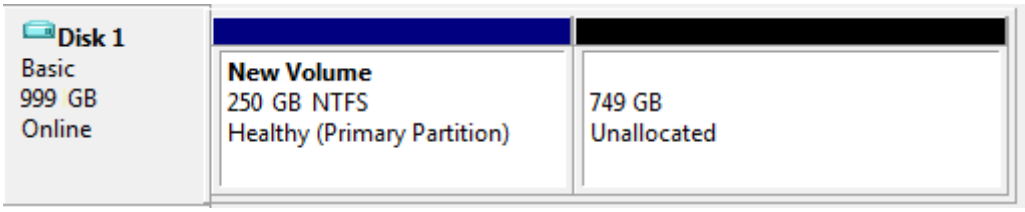
### 7.3 Thin provisioning

Zoals uit het aanbestedingsdocument blijkt wil de VNOG wil meer flexibiliteit in de nieuwe storage oplossing. Nu is er nog op enkele plaatsen vrije ruimte beschikbaar, maar deze kan niet ingezet worden zonder dat er complexe migraties uitgevoerd moeten worden. Dit omdat deze vrije ruimte al gealloceerd is. Bijgaande tekening verduidelijkt dit.




**Figuur 9 Niet flexibele storageoplossing**

Met de introductie van thin provisioning is het monitoren van de SAN omgeving essentieel om te voorkomen dat deze uit storagecapaciteit loopt. Ook is het Microsoft NTFS filesysteem niet geoptimaliseerd[1] voor thin provisioning. Om deze risico's te verkleinen wordt thin provisioning ingericht volgens het Just In Time (JIT) principe. Hierbij worden de data LUNs met behulp van thin provisioning aangeboden, maar worden deze op OS niveau kleiner gepartitioneerd. Zie bijgaande afbeelding:




**Figuur 10 Partitionering**

Hiermee wordt voorkomen dat processen of gebruikers datavolumes volledig in gebruik nemen en daarmee het SAN onderuit halen.

**Ontwerpbeslissing:**
- Thin provisioning inzetten om flexibiliteit in de storageoplossing te verkrijgen;
- Just In Time (JIT) gebruiken om risico's te verlagen.

Deze beslissing is gebaseerd op de volgende punten:
- Realisatie flexibele storageoplossing;
- Risicoverlagend.

[1] Zie http://support.microsoft.com/kb/959613

Het volgende overzicht geeft de verschillen tussen beide oplossingen weer:

| | Thin provisioning | JIT provisioning |
|---|---|---|
| **Overcommitment** | Ja | Ja, maar begrenst. |
| **Server monitoring** | Passief, middels trendrapportages | Actief, middels SCOM |
| **SAN monitoring** | Ja, door overcommitment is monitoring cruciaal | Nee, minder noodzakelijk door OS partitionering. |
| **Risico** | SAN storage vol. | Server: Disk vol. |

De provisioning factor die wordt gebruikt is 4. Dit houdt in dat de aangeboden LUNs die aangeboden worden vier maal groter worden aangeboden dan dat deze gesized zijn. De partitie die aangemaakt wordt op dit LUN zal een factor vier kleiner zijn dan dat er gesized is. Bijvoorbeeld:

| LUN | Sizing | LUN size | Partitie |
|---|---|---|---|
| **Exchange DB** | 200 GB | 800 GB | 50 GB |

**Ontwerpbeslissing:**
- Thin provisioning factor is 4 t.o.v. sizing;
- Partitioneringsfactor is 4 t.o.v. sizing.

Deze beslissing is gebaseerd op de volgende punten:
- Peopleware best practice;
- Risicoverlagend.

Het vergroten van de partitie kan eenvoudig uitgevoerd worden met diskpart.

```
C:\Windows\system32>diskpart

Microsoft DiskPart version 6.1.7601
Copyright (C) 1999-2008 Microsoft Corporation.
On computer: LAPTOP11

DISKPART> list volume

  Volume ###  Ltr  Label       Fs     Type       Size     Status     Info
  ----------  ---  -----------  -----  ----------  -------  ---------  --------
  Volume 0     D                       DVD-ROM         0 B  No Media
  Volume 1     C                NTFS   Partition    186 GB  Healthy    Boot
  Volume 2     E   New Volume   NTFS   Partition    250 GB  Healthy

DISKPART> select volume 2

Volume 2 is the selected volume.

DISKPART> extend size=250000

DiskPart successfully extended the volume.

DISKPART> list volume

  Volume ###  Ltr  Label       Fs     Type       Size     Status     Info
  ----------  ---  -----------  -----  ----------  -------  ---------  --------
  Volume 0     D                       DVD-ROM         0 B  No Media
  Volume 1     C                NTFS   Partition    186 GB  Healthy    Boot
* Volume 2     E   New Volume   NTFS   Partition    500 GB  Healthy
```

Voor bepaalde type LUNs wordt er geen gebruik gemaakt van thin provisioning vanuit performanceoogpunt of omdat dit geen toegevoegde waarde biedt. Bijgaand overzicht geeft aan wanneer er wel en wanneer er geen thin provisioning wordt ingezet.

| Type LUN | Thin Provisioning | Reden |
|---|---|---|
| **Hyper-V CSV volumes** | Nee | Best practice. Thin provioning biedt geen storage winst aangezien VHD bestanden fixed size uitgevoerd worden. |
| **FailoverCluster Quorum** | Nee | Geen winst bij dit kleine volume |
| **DPM Storage Pool** | Nee | Best practice. |
| **Resterende volumes** | Ja | |

### 7.4 Uitbreiding SAN

Voor een uitbreiding van de primary storage zal een additionele drive enclosure aangeschaft moeten worden. Bijgaand een overzicht voor de uitbreiding met 8 * 600 GB:

| | Artikelcode | Aantal |
|---|---|---|
| **M6612 3.5-inch SAS Drive Enclosure** | AJ832A | 1 |
| **M6625 600GB 6G SAS 10K 2.5in HDD** | AW611A | 8 |
| **P6300/P6500 Drive Enclosure JW Support** | HA110A3 Q25 | 1 |
| **P6300/P6500 HDD Support HW Support** | HA110A3 Q26 | 8 |

Vervolgens kunnen er nog 16 * 600 GB disken geplaatst worden voordat de enclosure vol is en een nieuwe geplaatst moet worden.

### 7.5 GPT vs MBR

Data LUNs worden mbv GUID Partition Table (GPT) geformatteerd. Dit heeft de volgende voordelen ten opzichte van de traditionele Master Boot Record (MBR) partitionering:

- Partities groter dan 2 TB mogelijk;
- Partitieinformatie op 2 locaties opgeslagen;
- GUID is uniek, ook over clusternodes heen;

# Hoofdstuk 8 Datacenter

## 8.1 Servers

Voor VM's en fysieke servers wordt Windows Server 2008 R2 SP1 Standard geïnstalleerd. Doordat er op de Hypervisor Datacenter editie licenties worden ingezet kunnen er een onbeperkt aantal VM's met Windows Server op draaien, ongeacht versie of editie. Waar nodig zal Enterprise ingezet worden.

**Ontwerpbeslissing:**
- OS versie is Windows Server 2008 R2 SP1;
- OS Editie is Standard tenzij Enterprise nodig is.

Deze beslissing is gebaseerd op de volgende punten:
- 2008 R2 SP1 is de meest moderne versie beschikbaar;
- Enterprise Edition is niet noodzakelijk voor alle servers.

### 8.1.1 KMS service

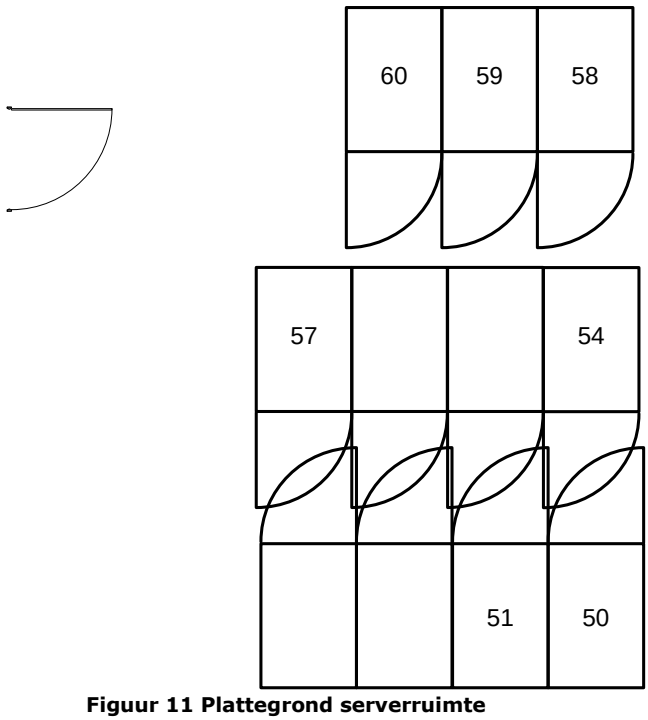
Ten aanzien van de Microsoft licenties wordt er een KMS service ingericht op de virtuele domaincontroller.

**Ontwerpbeslissing:**
- Een centrale KMS server op de licentieserver (Remote Desktop Services en Citrix).

Deze beslissing is gebaseerd op de volgende punten:
- Voorkeur en ervaring VNOG.

## 8.2 Serverruimte

Bijgaand een plattegrond voor de serverruimte met de relevante racks.




**Figuur 11 Plattegrond serverruimte**

## 8.3 Rackindeling

Zie volgende pagina.

| H.E. (U) | Kast 60 front | Kast 60 back | Kast 59 front | Kast 59 back | Kast 58 front | Kast 58 back | Kast 57 | Kast 54 | Kast 51 | Kast 50 |
|---|---|---|---|---|---|---|---|---|---|---|
| **47** | Geleidepanel | HP switch | Geleidepanel | KVM switch | Geleidepanel | | Geleidepanel | Geleidepanel | | Geleidepanel |
| **46** | Patchpanel | NSW04 | Patchpanel | | Patchpanel | | Patchpanel | Patchpanel | | Patchpanel |
| **45** | Patchpanel | | Patchpanel | ** Geleidepanel | Patchpanel | ** Geleidepanel | Patchpanel | Patchpanel | | Patchpanel |
| **44** | | | | ** HP SAN switch | | ** HP SAN switch | | | | |
| **43** | | | | | | | | | | NDS02 |
| **42** | | | | | | | | | | plaat |
| **41** | | | | | | | | | | ** NCG01 |
| **40** | | | | | | | | SVS05 | | |
| **39** | | | | | | | | | | |
| **38** | | | | | | | | | | |
| **37** | | | | | | | | | | |
| **36** | | | SVS10 | | | | | | | NRT01 |
| **35** | | | | | | | | | | NPS01 |
| **34** | | | SVS08 | | SVS09 | | | | | NFW01 |
| **33** | | | | | | | | | | NFW02 |
| **32** | | | | | | | SVI01 | MSA05 | | Avaya G450 |
| **31** | | | | | | | TAPEDRIVE (OUD) | | | |
| **30** | | | | | | | | | | |
| **29** | | | | | | | | | | |
| **28** | | | | | HP 6300 EVA | | plaat | | | |
| **27** | | | | | | | | | | |
| **26** | | | | | | | | | | |
| **25** | | | | | | | | | | |
| **24** | | | | | | | | | | |
| **23** | TAPEDRIVE | | | | | | | | | |
| **22** | | | LAPTOP | | | | | | | |
| **21** | SBA02 | | | | | | | | | |
| **20** | | | | | | | | | | |


*bezoekadres* Haagse Schouwweg 8b
2332 KG Leiden
*postadres* Haagse Schouwweg 8b
2332 KG Leiden

*telefoon* 071 - 579 70 10
*fax* 071 - 579 70 11
*e-mail* info@peopleware.nl
*internet* www.smartictsolutions.nl

*banknummer* 57.84.75.014
*bank* ABN Amro
*KvK* 27362503
*BTW nummer* NL814547412B01

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **19** | SBA01 | | | | | | | | | |
| **18** | | | | | | | | | | |
| **17** | SDC02 | | MSA01 | | | | | | | |
| **16** | | | | | | | | | | |
| **15** | | | | | MSA02 | | | | | |
| **14** | SVS22 | | | | | | | | | |
| **13** | | | MSW02 | | MSW01 | | | | | |
| **12** | MSA06 | | ** SVS31 | | ** SVS34 | | | | | |
| **11** | | | | | | | | | | |
| **10** | | | ** SVS32 | | ** SVS35 | | | | | |
| **9** | VNOGHOST4 | | | | | | | | | |
| **8** | | | ** SVS33 | | ** SVS36 | | | | | |
| **7** | VNOGHOST3 | | | | | | | SFW01 | NMS01 | |
| **6** | | | SVS01 | | SVS03 | | | | | |
| **5** | | | | | | | SFW02 | SCP01 | NMS02 | |
| **4** | VNOGHOST1 | | SVS03 | | SVS04 | | | | | |
| **3** | | | | | | | SDC01 | SMA01 | NMS03 | |
| **2** | SVS11 | | | | | | | | | |
| **1** | | | | | | | | | | |

# Hoofdstuk 9 Hypervisor

## 9.1 Operating System

De Hyper-V servers worden ingericht met Windows Server 2008 R2 Datacenter Core Edition. Door het gebruik van de Core versie wordt voorkomen dat er onnodige patches geïnstalleerd moeten worden. Tevens wordt voorkomen dat er per ongeluk software op de Hyper-V nodes geïnstalleerd wordt.

**Ontwerpbeslissing:**
- OS versie is Windows Server 2008 R2 SP1;
- OS type is Windows Server Core;
- OS editie is Datacenter.

Deze beslissing is gebaseerd op de volgende punten:
- Core heeft een kleinere 'footprint' en daardoor een betere beveiliging tegen aanvallen en beveiligingslekken;
- Datacenter editie is prijstechnisch het interessants.

## 9.2 Disk ontwerp

Bij het creëren van VHD bestanden kan er gekozen worden tussen Dynamic en Fixed size. Bij Dynamic disks moet er bij het wegschrijven van data door het OS twee acties ondernomen worden. Eerst moet de VHD uitgebreid worden, daarna kan de data weggeschreven worden. Dit levert een extra IO penalty op voor het SAN.

**Ontwerpbeslissing:**
- Alleen Fixed size VHDs;
- Uitzondering voor de VDI oplossing.

Deze beslissing is gebaseerd op de volgende punten:
- Best Practice Microsoft en Citrix;
- Performance penalty bij Dynamic disks.

### 9.2.1 CSV volumes

Om de VHD bestanden van de VM's onder te brengen worden CSV volumes gebruikt. Deze LUNs zijn 1 TB groot. Initieel worden er vier CSV volumes aangeboden. Data volumes van bijvoorbeeld Exchange en SQL worden door middel van pass-through direct aangeboden aan de VM. De keuze hiervoor is gebaseerd op:
- Performancewinst ten opzichte van CSV volumes;
- De mogelijkheid om thin provisioning in te zetten voor datavolumes;

**Ontwerpbeslissing:**
- CSV volumes zijn 1 TB.

Deze beslissing is gebaseerd op de volgende punten:
- Peopleware best practice;
- Beste beheer←→ performance verhouding.

### 9.2.2 VHD bestanden

De schijven worden als VHD ingericht op CSV volumes. De data schijven E:, F:, etc. worden als pass-through disken aangeboden voor de IO intensieve componenten zoals Exchange en SQL.

**Ontwerpbeslissing:**

- VM VHD's op CSV volumes;
- IO intensieve DATA volumes (E: t/m Y:) middels pass-through.

Deze beslissing is gebaseerd op de volgende punten:

- Performancewinst pass-through is 2-3%.

# Hoofdstuk 10 E-mail

In de huidige infrastructuur zijn er een aantal verstoringen geweest aan de Exchange 2007 omgeving. Bij het ontwerp van de nieuwe Exchange 2010 omgeving moet er een hogere beschikbaarheid gerealiseerd worden voor de e-mailomgeving.

## 10.1 Database Availabillity Group

Om de beschikbaarheid te vergroten is het een logische stap om van Exchange 2007 naar een Exchange 2010 DAG cluster te migreren. Aangezien Exchange 2010 minder IO intensief is dan zijn voorgangers belast dit de storage minder.

Hyper-V Live migration wordt ondersteund voor een DAG cluster, maar vanuit de ervaring van Peopleware kan er het beste een shutdown en cold boot plaatsvinden om een DAG nodes naar andere Hyper-V node over te brengen. Doordat de DAG de mailbox stores in de lucht houdt, betekend dit dat er geen onderbreking is in de dienstverlening als er een DAG node uitgeschakeld wordt. In de situatie dat de Hyper-V node waar een van de DAG nodes op draait uitvalt zal Exchange een failover van de mailbox databases uitvoeren naar de andere DAG node, waarna de uitgevallen DAG node op een andere beschikbare Hyper-V node opgestart wordt.

**Ontwerpbeslissing:**
- Hoge beschikbaarheid d.m.v. DAG cluster;
- Live Migration wordt uitgeschakeld voor DAG nodes.

Deze beslissing is gebaseerd op de volgende punten:
- Failover mogelijkheid bij uitval en onderhoud van een mailbox server;
- Peopleware best practice.

## 10.2 Exchange rollen

De Exchange rollen worden als volgt verdeeld:

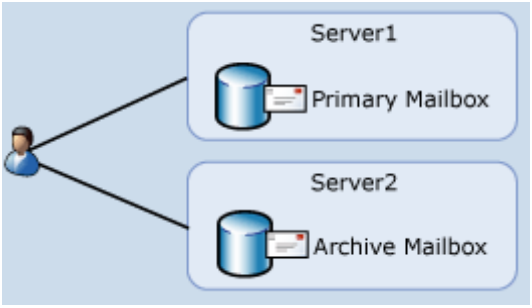
| | Node 1 | Node 2 |
|---|---|---|
| **Mailbox** | Ja | Ja |
| **Hub** | Ja | Ja |
| **Client Access** | Ja | Ja |
| **Edge** | Nee | Nee |
| **Unified Messaging** | Nee | Nee |

**Ontwerpbeslissing:**
- Beide DAG nodes krijgen MBX, HUB en CAS rol;
- Edge role wordt niet ingezet;
- Unified Messaging role wordt niet ingezet.

Deze beslissing is gebaseerd op de volgende punten:
- Failover mogelijkheid bij uitval en onderhoud van een mailbox server;
- Edge role wordt uitgevoerd door anti-spam appliance;
- Unified messaging role niet nodig.

### 10.2.1 Archive Mailbox

Exchange 2010 biedt een oplossing waarbij een gebruiker 2 mailboxen krijgt, één primaire mailbox en een archief mailbox. Omdat deze in gescheiden databases op een andere server bewaard kunnen worden blijft de database waar de primaire mailbox in staat klein, door het zetten van een lage quota, en zijn restore acties minder arbeidsintensief. De quota op de archief mailbox kan zeer ruim worden gezet. Ook kan er een policy worden aangemaakt die automatisch de mail ouder dan een vooraf ingestelde periode verplaatst naar de archief mailbox. Deze database kan dan op Nearline storage aangeboden worden. Bijgaande afbeelding verduidelijkt dit principe.



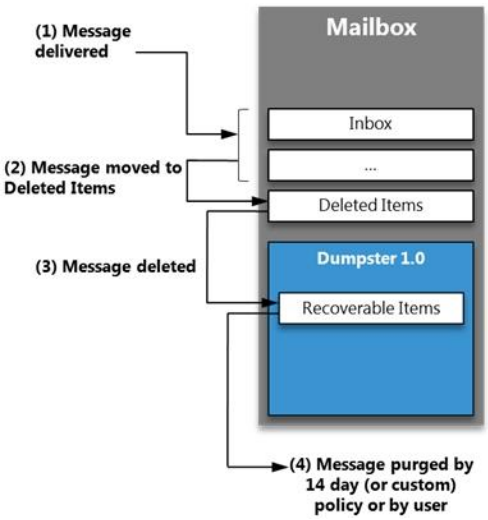

**Figuur 12 Archive Mailbox**

**Ontwerpbeslissing:**
- Inrichten Archive mailbox database voor selecte groep gebruikers;
- Exchange Enterprise CALs aanschaffen.

Deze beslissing is gebaseerd op de volgende punten:
- Verkleint doorlooptijd restoreverzoeken.
- Exchange Enterprise CAL noodzakelijk voor gebruikers die een Archive Mailbox krijgen.

### 10.2.2 Single Item Restore

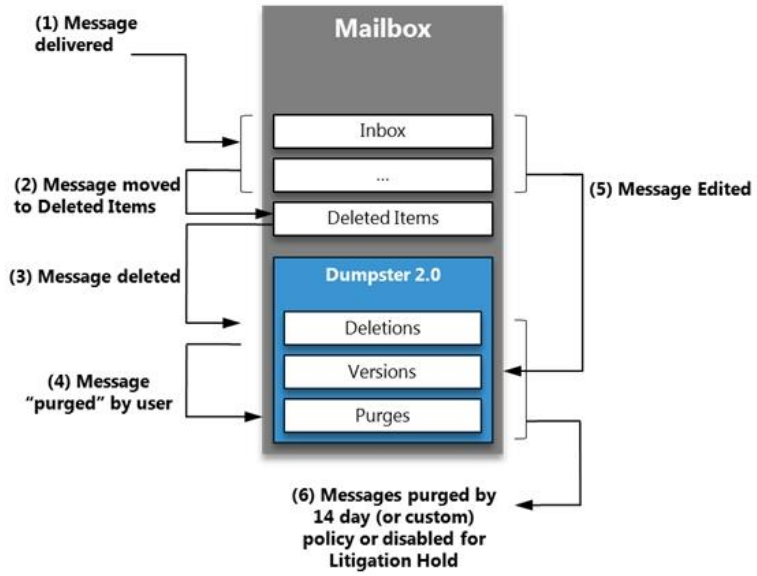
Verder is in Exchange 2010 de dumpster opnieuw ontworpen. De dumpster is een plaats in een Exchange Database waar verwijderde data geplaatst wordt. Pas na het verlopen van het Deleted Item Retension Window worden de verwijderde items definitief uit de Exchange database verwijderd. In Exchange 2007 staat dit window op 14 dagen. Zie bijgaande afbeelding.




**Figuur 13 Dumpster v1.0**[2]

[2] Zie The Exchange Team Blog - Single Item Recovery in Exchange Server 2010.

In Exchange 2010 is de dumpster bijgewerkt tot versie 2.0. Het nieuwe ontwerp van de dumpster voorkomt dat berichten definitief uit de database verwijderd kunnen worden door gebruikers. Pas wanneer het Deleted Item Retention Window verloopt worden berichten definitief uit de database verwijderd. Zie bijgaande afbeelding.




**Figuur 14 Dumpster 2.0**

Daarnaast houdt de dumpster ook wijzigingen in berichten vast, denk aan het verwijderen van attachments en het wijzigen van afspraken.

Gebruikers hebben nog steeds de mogelijkheid om verwijderde items terug te halen. Het terughalen van items die door de gebruiker uit de dumpster zijn verwijderd (de 'deleted deleted items') kan door beheer uitgevoerd worden zonder dat er een restore van een mailbox database noodzakelijk is.

**Ontwerpbeslissing:**
- Single Item Recovery activeren.

Deze beslissing is gebaseerd op de volgende punten:
- De doorlooptijd van mailbox restoreverzoeken verlagen.

Verder kan er op een mailbox Litigation Hold worden geactiveerd. Hiermee worden er door het Mailbox Records Management proces geen berichten meer verwijderd uit te mailbox.

**Ontwerpbeslissing:**
- Litigation Hold niet activeren.

Deze beslissing is gebaseerd op de volgende punten:
- Nadelige impact op storage. Er wordt helemaal niets meer uit de mailbox verwijderd.

### 10.3 Brick-level backup

Aangezien Microsoft brick-level backups niet meer adviseert voor Exchange kan er het beste gekozen worden voor een archiveringsoplossing. Hierdoor blijven de Exchange databases klein en kan er sneller een restore worden uitgevoerd.

**Ontwerpbeslissing:**
- Er wordt geen brick level backup uitgevoerd.

Deze beslissing is gebaseerd op de volgende punten:
- Best Practice Microsoft;
- Door het enablen van Single Item Recovery zal het aantal restoreverzoeken omlaag gaan.

### 10.4 Sizing

Om een archief mailbox aan te maken is een Exchange Enterprise CAL nodig. Aangezien de VNOG alleen Exchange Standard CAL's heeft zal deze optie wel geconfigureerd worden, maar niet voor alle gebruikers. Alleen de gebruikers met een mailbox boven de limiet van 1 GB zullen een archief mailbox krijgen.

Om de sizing[3] te berekenen is gebruik gemaakt van de volgende waardes.

| Onderwerp | Waarde |
|---|---|
| **Server Multi-Role Configuration (MBX+CAS+HT)** | Ja |
| **Server Role Virtualization** | Ja |
| **High Availability Deployment** | Ja |
| **Number of Mailbox Servers Hosting Active Mailboxes / DAG** | 2 |
| **Number of Database Availability Groups** | 1 |
| **Total Number of HA Database Copy Instances (Includes Active Copy) within DAG** | 2 |
| **Total Number of Lagged Database Copy Instances within DAG** | 0 |
| **Data Overhead Factor** | 20% |
| **Mailbox Moves / Week Percentage** | 1% |
| **Dedicated Maintenance / Restore LUN?** | Ja |
| **LUN Free Space Percentage** | 20% |
| **I/O Overhead Factor** | 20% |
| **Additional I/O Requirement / Server** | 0 |
| **Site Resilient Deployment** | Nee |
| **Maximum Database Size Configuration** | Default |
| **Number of Databases** | 3 (+1 voor Archives, +1 voor Public Folders) |
| **Backup Methodology** | Hardware VSS |
| **Backup Frequency** | Weekly Full/Daily Incremental |
| **Database and Log Isolation Configured** | Ja |
| **Backup/Truncation Failure Tolerance** | 3 |
| **Network Failure Tolerance (Days)** | 0 |
| **Disk Configuration** | 600 GB, 10K FC |
| **Cores per Mailbox server** | 2, SPECint2006: 241/12 cores * 2 cores = 40 |
| **Hypervisor CPU Adjustment Factor** | 10% |

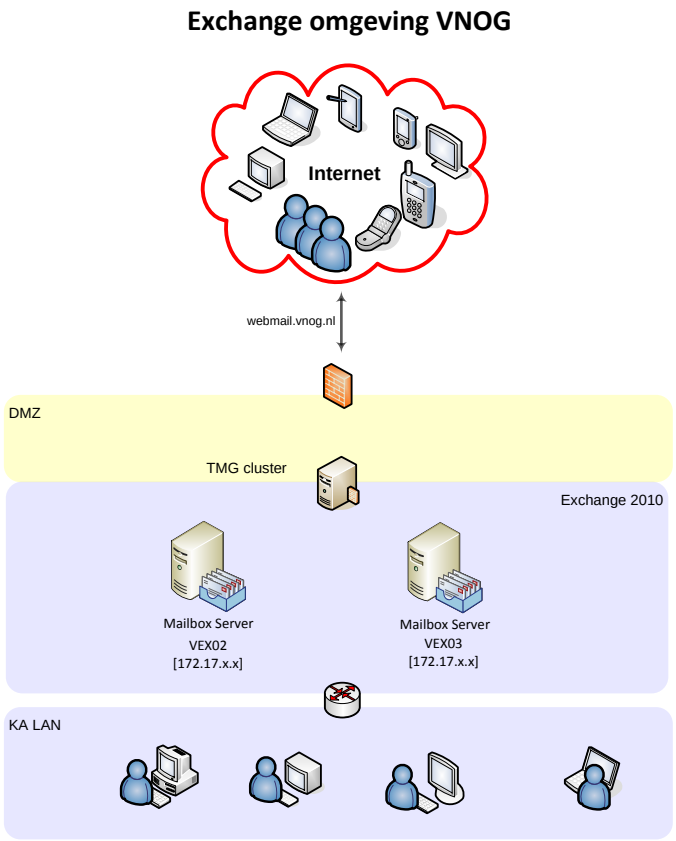
[3] Voor de berekening van de specificaties voor deze server is gebruik gemaakt van de "Exchange 2010 Mailbox Server Role Requirements Calculator" versie 18.9.

Er worden twee type gebruikers gedefinieerd:

| Type | Standaard | Heavy |
|---|---|---|
| **Total Number of Tier-1 User Mailboxes / Environment** | 250 | 100 |
| **Projected Mailbox Number Growth Percentage** | 20% | 50% |
| **Total Send/Receive Capability / Mailbox / Day** | 100 | 200 |
| **Average Message Size (KB)** | 75 KB | 75 KB |
| **Mailbox Size Limit (MB)** | 1024 MB | 1024 MB |
| **Personal Archive Mailbox Size Limit (MB)** | 0 MB | 8192 MB[4] |
| **Deleted Item Retention Window (Days)** | 14 | 14 |
| **Single Item Recovery** | Ja | Ja |
| **Calendar Version Storage** | Ja | Ja |
| **IOPS Multiplication Factor** | 1 | 1 |
| **Megacycles Multiplication Factor** | 1 | 1 |
| **Desktop Search Engines Enabled (for Online Mode Clients)** | Nee | Nee |
| **Predict IOPS Value?** | Ja | Ja |

## 10.5 Infrastructuur

De e-mail infrastructuur zal er als volgt uitzien.




**Figuur 15 Exchange infrastructuur**

[4] Berekening in twee stappen uitgevoerd om de Archive DB size te berekenen: een maal zonder archief, een maal met archief.

# Hoofdstuk 11 Desktop

Het ontwerp voor de Desktop is gebaseerd op Citrix technologie. Het design is onderverdeeld in componenten/bouwblokken. Per component/paragraaf kan er een keuze gemaakt worden, waarbij Peopleware een advies geeft. De keuze bepaalt de opbouw en configuratie van de nieuwe Citrix omgeving.

## 11.1 Basis ontwerp

Het Citrix XenApp + XenDesktop design is gebaseerd op meerdere Citrix farms bestaande uit een aantal componenten. De componenten kunnen verdeeld worden in een algemeen deel (database, licenties en beheer) en de kern.

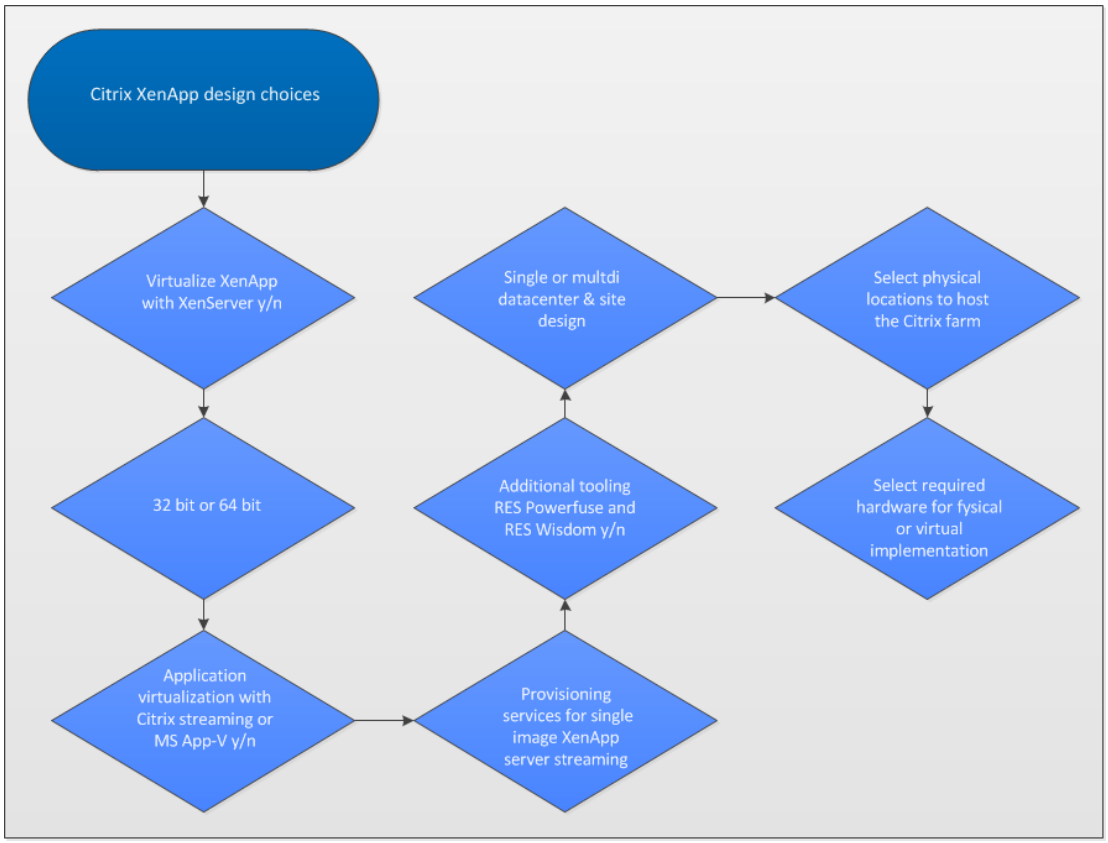
De kern bestaat uit enerzijds XenApp Applicatie servers die applicaties aanbieden naar gebruikers. Daarnaast zijn XenDesktop controllers aanwezig welke virtuele desktops aanbieden naar VDI gebruikers. De optionele componenten zoals Provisioning Services, beveiligde externe toegang, netwerk optimalisatie en virtualisatie services kunnen toegevoegd worden aan het logische design.

| Component type | Fysiek component |
|---|---|
| **Algemeen** | Citrix Licentieserver |
| **Algemeen** | Microsoft Terminal Server Licentieserver |
| **Algemeen** | Data collector (eerste XenApp server in de farm) |
| **Algemeen** | XenApp Datastore database |
| **Algemeen** | XenApp Configuration & Loggin database |
| **Algemeen** | XenDesktop Datastore database |
| **Algemeen** | Web Interface |
| **Kern** | XenApp Applicatie Servers |
| **Kern** | XenDesktop Controllers |
| **Optioneel** | Citrix Provisioning Server |
| **Optioneel** | Citrix Branch Repeater (optioneel) |
| **Optioneel** | Citrix Access Gateway (optioneel) |
| **Optioneel** | Virtualisatie Platform (optioneel) |
| **Clients** | Thin clients, Fat clients (laptops en desktops) of allebei, verbinden naar de Citrix Web Interface of Citrix Access Gateway |

| Logische Componenten | Omschrijving |
|---|---|
| **XenApp Farm** | Een logische groep van XenApp servers |
| **XenDesktop Farm** | Een logische groep van XenDesktop Controllers |
| **Zone** | Een groep XenApp server in hetzelfde subnet/site |
| **Silo** | Een groep XenApp servers binnen een farm met een overeenkomstig doel, zoals dezelfde applicatie set aanbieden of specifieke applicaties voor een aparte groep gebruikers (thuis werkers, externen, enz.) |

## 11.2 Ontwerp methode

Onderstaande flowchart toont een overzicht in hoofdlijnen van de ontwerpkeuzes.




**Figuur 16 Ontwerpkeuzes Citrix**

### 11.3 Fysiek of virtueel

De eerste stap in het ontwerpen en bouwen van een Citrix XenApp omgeving is het kiezen voor XenApp op fysieke hardware of virtueel op een hypervisor. XenApp applicatie servers (Windows server 2008 R2 + Terminal Service rol + Citrix XenApp 6.5 services) kunnen geïmplementeerd worden op fysieke hardware of als virtuele machines.

De traditionele 32-bit Citrix applicatie servers zijn gelimiteerd tot 2 cores CPU en 4GB geheugen (2 GB Kernel en 2GB User). Door toevoeging van PAE (Physical Address Extensions) kan tot 64GB geadresseerd worden, maar de Kernel en User memory space blijven beperkt tot 2GB ieder. Dit betekent minimale winst voor de gebruikers sessies. Het aanbieden van applicaties voor een grote groep gebruikers zal hoge eisen stellen aan de hardware (30-50 sessies per server, afhankelijk van soort/type applicaties).

De moderne 64-bit Citrix applicatie server ondersteunt quadcore CPU's en 32GB+ geheugen. Het 64-bit platform vereist dat alle applicaties draaien 64-bit mode of in 32-bit emulatie mode (WoW64). Er zijn applicaties (16 bit bijvoorbeeld) die werken in 32-bit Citrix omgevingen, maar niet met 64-bit Citrix. De 64-bit implementatie vereist minder fysieke hardware ten op zichte van een 32-bit implementatie kan meer sessies aanbieden (100+ sessies, afhankelijk van het soort applicaties en de aanwezige interne geheugen). XenApp 6.5 vereist Windows 2008 R2, dat betekent 64-bit.

De 64-bit implementatie kan meer dan 2 cores adresseren, maar het aantal extra sessies voor de 3e en 4e core zal 30% en 20% zijn. Het virtualiseren van XenApp servers draagt bij aan een effectiever gebruik van Multi-core hardware.

**Ontwerpbeslissing:**
- 2 cores per XenApp server.
- 10 GB RAM per XenApp server.

Deze beslissing is gebaseerd op de volgende punten:
- Effectiviteit 3e en 4e core is laag.
- Geheugentoewijzing is best practice Peopleware bij soortgelijke omgevingen.

Testen wijzen uit dat Intel Nehalem CPU's het beste geschikt zijn voor virtualisatie van Citrix XenApp servers.

De Citrix servers met een andere rol dan gebruikers hosten, zoals Web Interface, License Server en SQL database zijn goed te virtualiseren of op fysieke hardware aan te bieden.

| +/- | Fysieke hardware |
|---|---|
| + | Hoogst mogelijke performance |
| + | Geen overhead door virtualisatie laag (hypervisor) |
| + | Geen virtualisatie platform dat beheert moet worden |
| - | Minder flexibel tov gevirtualiseerde servers |
| - | Als Windows/Citrix hangt/vastloopt zal een grote hoeveelheid gebruikers geen sessie meer hebben |
| - | Geen live migratie mogelijkheden voor server/hardware onderhoud. |
| - | In de situatie met 32-bit Windows/Citrix zal alleen 2 cores en 4GB geheugen gebruikt worden. Recente hardware met quad core en het geheugen boven de 4GB wordt niet optimaal benut. |
| - | Met 64-bit Windows/Citrix kunnen meer dan 2 cores en 4GB geheugen gebruikt worden voor beter rendement en prestaties van de hardware. Quad core gebruik is mogelijk. De applicaties moeten geschikt zijn voor 64-bit architectuur of 32-bits emulatie mode (WoW64). |

| +/- | Virtuele machines |
|---|---|
| + | Flexibel. |
| + | Live migration maakt herallocatie mogelijk van VM's naar een andere hyper-visor ter bevordering van bijvoorbeeld hardware onderhoud. |
| + | Erg goede performance op hypervisor . |
| + | Schaalbaarheid van VM's maakt het uitbreiden van XenApp servers eenvoudiger. |
| + | Beschikbaarheid omgeving neemt toe, data staat centraal opgeslagen. Door toepassing van N+1 regel is er overcapaciteit beschikbaar, zodat in het geval van uitval fysieke host, de virtuele machines verdeeld worden over de aanwezige fysieke hosts. |
| + | hypervisor ondersteund quad core of dual quad core. |
| + | Betere benutting van hardware, aangezien er een aantal virtuele XenApp servers kan draaien op een fysieke host. Intel Nehalem CPU's vereist voor optimaal gebruik CPU. |
| - | Het virtualisatie platform vereist management en onderhoud. |
| - | Kleine overhead door virtualisatie laag (hypervisor). |

Het virtualiseren van XenApp applicatie servers zorgt voor maximale flexibiliteit. Virtualisatie van XenApp applicatie servers en bijbehorende rollen zorgt voor efficiënt en optimaal gebruik van hardware.

Aangezien de hypervisor niet alleen voor Citrix gebruikt wordt, maar ook voor de rest van de infrastructuur valt de keuze op Microsoft Hyper-V. Deze hypervisor biedt de beste prijs-functionaliteit verhouding voor de VNOG. Er zijn geen additionele licenties nodig om HA en support te verkrijgen op het Hyper-V platform.

**Ontwerpbeslissing:**
- De Citrix XenApp omgeving wordt gevirtualiseerd op Hyper-V. Dit betekent voor VNOG het gebruik maken van de Hyper-V omgeving voor de SBC omgeving en VDI omgeving.

Deze beslissing is gebaseerd op de volgende punten:
- Hyper-V vormt de basis van de infrastructuur.
- XenServer vereist additionele licenties voor high availability en support.
- Zie de voor- en nadelenlijst.

### 11.4 32 of 64 bits

Citrix XenApp 6.5 vereist een 64-bits Operating System. Dit betekent Windows 2008 R2.
Het gebruiken van een 64-bits Citrix server heeft vele voordelen t.o.v. 32-bits implementatie (XenApp 4.5) die nu aanwezig is bij de VNOG.

| +/- | X86 32-bits Citrix/Windows server |
|---|---|
| - | Maximaal 2GB Kernel geheugen kan toegewezen worden aan applicaties |
| - | Dual processor core is het maximum dat gebruikt wordt, met een quad core processor worden alleen maar 2 cores gebruikt |
| - | Aantal gelijktijdige sessies is lager d.m.v. OS beperkingen |
| + | Kan 16-bit applicaties gebruiken |
| + | 32-bits applicaties hoeven niet in emulatie mode te draaien, minder compatibiliteits issues voor oudere applicaties |

| +/- | X64 64-bits Citrix/Windows server |
|---|---|
| + | Windows Server Standard Edition ondersteunt standaard tot 32GB geheugen, geen Enterprise nodig |
| + | Geen 2GB Kernel geheugen limiet |
| + | Quad core support |
| + | Meer gelijktijdige sessies mogelijk op een XenApp server |
| - | 32-bit applicaties draaien in 32-bit WoW64 mode, sommige applicaties kunnen hier niet mee omgaan |
| - | 16-bit applicaties worden niet meer ondersteund |
| - | 64-bit printer drivers moeten beschikbaar zijn op de printserver |

Windows Server 2008 R2 wordt ingezet, dit betekent een 64-bit architectuur en compatibiliteit voor 32-bit applicaties. Er wordt aangeraden om Office 2010 (64 bits versie) te gebruiken als vervanger van Office 2003. Office 2010 32 bit heeft ongeveer 1,5 maal meer geheugen nodig. Office 2010 is backwards compatibel met Office 2003. Daarnaast wordt Office 2003 niet meer ondersteund door Microsoft[5].

**Ontwerpbeslissing:**
- 64 bit XenApp omgeving.
- Office 2010 64 bit ter vervanging van Office 2003.

Deze beslissing is gebaseerd op de volgende punten:
- Citrix XenApp 6.5 vereist 64 bit OS.
- Office 2003 wordt niet meer ondersteund.

Voor de oude 16-bit applicaties zal een oplossing gezocht moeten worden. De voorkeur hierbij is om deze te upgraden. In het geval dat dit niet mogelijk is kan door het gebruik van een 32-bit XenApp silo deze applicatie worden aangeboden.

**Ontwerpbeslissing:**
- 16 bit applicaties upgraden of vervangen.

Deze beslissing is gebaseerd op de volgende punten:
- 16 bit applicaties werken niet op 64 bit Windows systemen.

[5] ie artikel: http://support.microsoft.com/lifecycle/?p1=2488

## 11.5 Application publishing en virtualization

Op een XenApp server zijn er meerdere manieren om een applicatie te ontsluiten naar de gebruiker.

### 11.5.1 Application publishing

Dit is de standaard server based computing methode om applicaties aan te bieden binnen Citrix. De applicatie werkt op de terminal server en de eindgebruiker ziet de applicatie in een seamless window. Voor de gebruiker is het net alsof de applicatie lokaal op de machine geïnstalleerd staat.

### 11.5.2 Desktop publishing

Er kan gekozen worden om een compleet bureaublad (desktop) aan te bieden, getoond in een volledig scherm. De desktop is actief op de terminal server en de gebruiker ervaart dit alsof het zijn lokale desktop is. Published applications kunnen binnen de published desktop aangeboden worden.

**Ontwerpbeslissing:**
- Aanbieden van een compleet bureaublad.

Deze beslissing is gebaseerd op de volgende punten:
- Gebaseerd op huidige omgeving VNOG.

### 11.5.3 Citrix server-side streaming application virtualization

Application streaming wordt uitgevoerd op de terminal server, waarbij de applicatie geladen wordt in een geïsoleerde virtuele schil. De applicatie heeft geen weet van het feit dat het in een 'bubbel' werkt. Alle bestanden, register settings, tijdelijke bestanden, enz. worden geïsoleerd van het besturingssysteem. De voordelen zijn: geen applicatie conflicten, DLL conflicten en het besturingssysteem blijf schoon en snel. De applicaties die geladen worden in een ' bubble' kunnen standaard niet communiceren met andere applicaties. Het is mogelijk om gestreamde applicaties aan elkaar te koppelen, dit wordt inter-isolation genoemd.

Applicaties zoals antivirus of VPN clients zijn niet geschikt om te virtualiseren. Ook applicaties welke extra hardware eisen hebben, bijvoorbeeld USB dongles, kunnen niet gevirtualiseerd worden. De virtuele applicatie (technische term Streaming Profile ) staat op een centrale opslag, opvraagbaar vanuit het netwerk. Dezelfde virtuele applicatie kan gepubliseerd worden op de XenApp servers. In het geval van een applicatie update hoeft er maar één centraal image profiel aangepast te worden i.p.v. het updaten van de applicatie op iedere XenApp server.

### 11.5.4 Citrix client-side streaming

Een virtuele applicatie kan rechtstreeks aangeboden aan de client device (werkplek) zonder interventie van de XenApp server. De applicatie wordt geladen op de werkplek zelf en maakt gebruik van de resources van de werkplek i.p.v. de XenApp server.
Aangezien de applicatie gevirtualiseerd is zullen er geen bestanden lokaal geïnstalleerd worden en geen register wijzigingen gemaakt worden, de applicatie wordt alleen in de cache gezet. De beheerder kan zelf bepalen hoe lang de applicatie offline (zonder netwerktoegang) beschikbaar mag zijn, zonder een verbinding te hebben met de online Citrix omgeving.

### 11.5.5 Microsoft App-V server-side streaming application virtualization

Citrix XenApp is geschikt voor integratie met Microsoft App-V (applicatie virtualisatie).
De App-V client moet op de XenApp server geïnstalleerd zijn, zodat er gebruik gemaakt kan worden van de virtuele App-V applicaties.
De applicaties die geladen worden in een ' bubbel' kunnen standaard niet communiceren met andere applicaties. Het is mogelijk om gestreamde applicaties aan elkaar te koppelen, dit wordt inter-package genoemd. Dit vergt aanpassingen.
Note: de App-V infrastructuur vereist een sequencer en management server.

### 11.5.6 Keuze

Gebruik zoveel mogelijk server-side streaming met App-V of Citrix streaming voor de XenApp servers. Applicaties die niet geschikt zijn voor virtualisatie worden lokaal op de XenApp server geïnstalleerd. Indien applicaties afhankelijkheden hebben met vele andere applicaties wordt aangeraden deze in de basis laag (OS + XenApp) te installeren.

Peopleware adviseert om basis software zoals Office 2010, Acrobat Reader, Java, Silverlight, enz lokaal te installeren. Maatwerk kan lokaal geïnstalleerd worden, maar er moet getest worden of de packages geschikt zijn om onder besturingssysteem Windows 2008 R2 te werken. De kans is aanwezig dat de packages opnieuw gemaakt moeten worden.

Dit heeft consequenties voor applicaties die niet werken onder het besturingssysteem Windows 2008 R2. Deze applicaties dienen opnieuw gepackaged te worden of er moet een alternatief gezocht worden.

**Ontwerpbeslissing:**

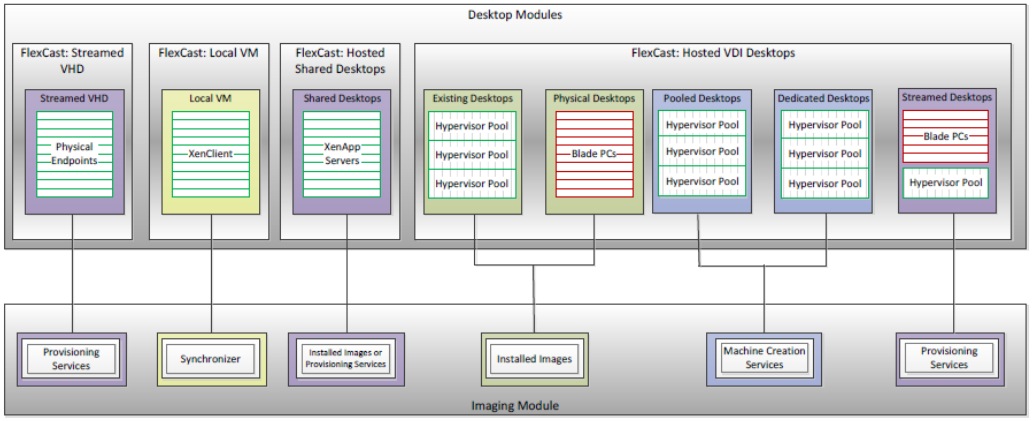
- Applicaties worden lokaal op de XenApp servers geïnstalleerd.

Deze beslissing is gebaseerd op de volgende punten:

- Ervaringen bij de VNOG uit het verleden. De applicatieset van de VNOG blijkt moeilijk te virtualiseren te zijn.

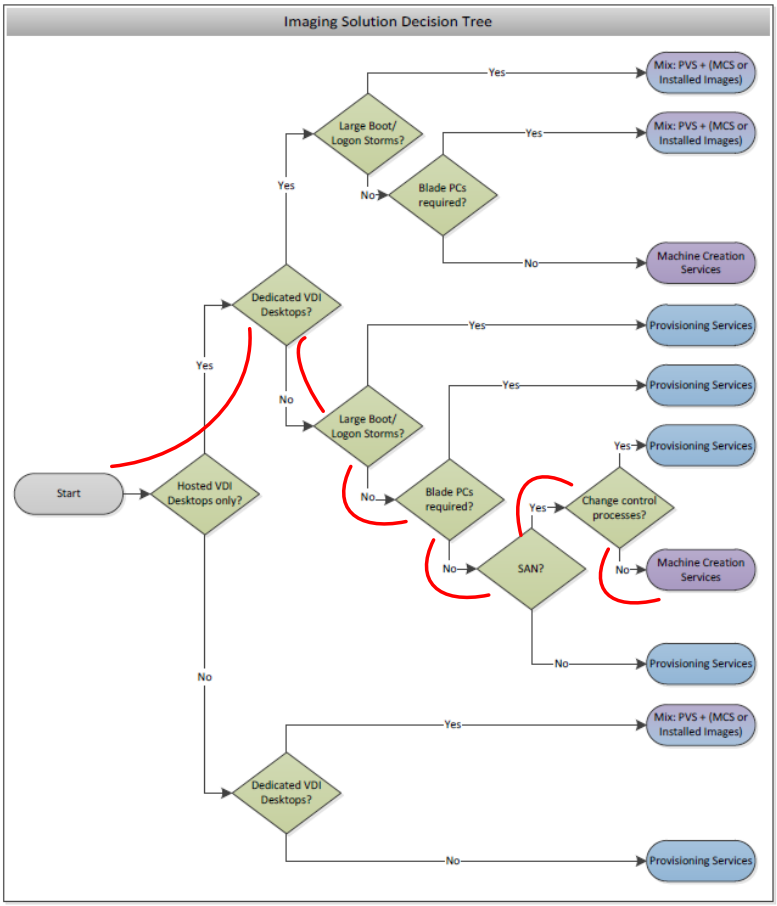
## 11.6 Provisioning of Machine Creation Services

Er zijn drie methodes om VDI desktops uit te rollen. Zie bijgaande afbeelding:




**Figuur 17 FlexCast opties (Bron: Citrix)**

De Installed Images methode is niet van toepassing, aangezien de VDI Desktops op de Hyper-V Pool aangeboden worden. Er moet een keuze gemaakt worden tussen Machine Creation Services (MCS) en Provsioning Services (PVS). Om te kiezen welke methode het beste van toepassing is kan gebruik gemaakt worden van de volgende flowchart.




**Figuur 18 Imaging flowchart (Bron: Citrix)**

De keuzes zijn als volgt:

- Hosted VDI Desktops only? **Yes**. Er wordt alleen gebruik gemaakt van VDI op het Hyper-V cluster;
- Dedicated VDI Desktops? **No**. Alle gebruikers krijgen dezelfde VDI desktop aangeboden, er worden geen VDI Desktops toegewezen aan gebruikers, er wordt een pool aangemaakt;
- Large Boot/Logon Storms? **No**. Aangezien de VDI oplossing klein wordt opgezet zal de IO impact van de oplossing geen Logon Storm opleveren;
- Blade PCs required? **No**. Er worden geen VDI desktops direct op blade hardware aangeboden;
- SAN? **Yes**. Er wordt gebruik gemaakt van SAN storage voor de VDI oplossing;
- Change Control processes? **No**. Bij grotere omgevingen heeft het change proces grote impact op de betrouwbaarheid van de oplossing. Bij het aanmaken van VDI desktop kunnen er dan problemen optreden.

Er zal worden gekozen voor een Machine Creation Services (MCS) oplossing. Peopleware adviseert om MCS (Machine Creation Services) te gebruiken als uitrol mechanisme voor virtuele desktops. MCS is laagdrempelig voor beheer ten opzichte van Provisioning en vereist geen extra servers naast de XenDesktop controllers.

**Ontwerpbeslissing:**
- MCS methode om Desktops aan te bieden.

Deze beslissing is gebaseerd op de volgende punten:
- Volgens Citrix flowchart.

Mocht de VNOG in de toekomst besluiten om volledig op VDI te gaan werken, dan zal de keuze er mogelijk anders uitzien. Op een later tijdstip kan altijd overgestapt worden op een Provisioning Services (PVS) oplossing.

**Ontwerpbeslissing:**
- Bij een groei boven de 50 VDI desktops voldoet de MSC oplossing niet meer. PVS zal dan ingericht moeten worden.

Deze beslissing is gebaseerd op de volgende punten:
- Peopleware best practice.

### 11.7 Provisioning Server (Optioneel)

Citrix Provisioning Services kan gebruikt worden om servers operationeel te maken en te laten opstarten door één golden image. Indien de aanwezige infrastructuur op XenServer is gebouwd, kan Provisioning server gebruikt worden om de image te streamen naar de virtuele XenApp servers. Het is ook mogelijk om een image te streamen naar een XenApp server, draaiend op fysieke hardware (traditioneel, niet virtueel).

Het voordeel van één golden image dat het updaten en wijzigen van een XenApp server maar één keer hoeft. Na de aanpassing van het golden image booten de XenApp server van het image en zijn zij up to date. Citrix noemt dit Single Image Management. Het image is read-only, hierdoor is na iedere herstart van de server de machine in originele staat. Ongecontroleerde wijzigingen en tijdelijke bestanden behoren tot het verleden.

Voor XenApp server provisioning is het best practice om standard image vDisks te gebruiken met de write cache (tijdelijke opslag wijzingen) op een centrale opslag of lokale storage.

Peopleware adviseert om gebruik te maken van de XenApp Prep methode, dat wil zeggen er één XenApp machine volledig opgebouwd wordt en deze als template gebruikt wordt voor de andere XenApp servers.

**Ontwerpbeslissing:**
- XenApp Prep methode inzetten als XenApp installatiemethode.

Deze beslissing is gebaseerd op de volgende punten:
- Peopleware best practice voor omgevingen zonder Provisioning.

### 11.8 3rd party tooling (Optioneel)

De volgende tools worden aanbevolen voor de Citrix omgeving tbv beheer en uitrol.

#### 11.8.1 RES Automation Manager (Wisdom)
Met RES Automation Manager kan er een uniform draaiboek gemaakt worden waarmee je XenApp servers kan inrichten inclusief applicaties, enz.
RES Automation Manager zorgt ervoor dat er eenduidig servers uitgerold kunnen worden, wat heel belangrijk is om XenApp servers identiek te houden.
http://www.ressoftware.com/products/automation-manager/automation-manager

#### 11.8.2 RES Workspace Manager (Powerfuse)
RES Workspace Manager integreert met de XenApp omgeving, waardoor management eenvoudiger wordt. RES Workspace Manager beheert de toegang naar alle applicaties, beveiligingsinstellingen, policies, toegangscontrole, enz. Eén van de extra features is de Zero-profile techniek, dit zorgt voor een aanzienlijke kortere aanmeldtijd op de XenApp omgeving.
http://www.ressoftware.com/products/workspace-manager/user-workspace-management

Icento adviseert om gebruik te maken van RES Automation Manager (Wisdom) en RES Workspace Manager (Powerfuse) om XenApp servers uit te rollen en de applicaties te ontsluiten naar de eindgebruikers. Om de aanmeldtijd naar de Citrix omgeving te verkorten zal de Zero-profile techniek geïmplementeerd moeten worden.

**Ontwerpbeslissing:**
- Er worden geen 3rd party tools gebruikt voor de opbouw van XenApp en XenDesktop servers. De opbouw van de server images zal meer tijd in beslag nemen, ook zal het beheer en onderhoud hiervan meer tijd vergen.
- Desktop zal met behulp van GPO's worden opgebouwd.

Deze beslissing is gebaseerd op de volgende punten:
- De klant moet hiervoor extra investeren en kiest ervoor om de XenApp omgeving en XenDesktop image op te bouwen zonder deze tooling.

### 11.9 Datacenter Ontwerp

Om redundancy te creëren aan de Citrix farm kan het verspreid worden over twee of meer datacenters. Dit kan een actief deel van de farm zijn of een standby deel. Door het configureren van een aparte zone per locatie/datacenter voor de XenApp servers, kun je een primary en secondary backup zone maken voor iedere zone. Als een zone niet beschikbaar is kunnen de gebruikers verbinden naar de backup zone op de andere locatie.

Icento adviseert om de XenApp omgeving single datacenter design op te bouwen, idem voor de XenDesktop omgeving.

**Ontwerpbeslissing:**

- Single datacenter design. Eén zone voor XenDesktop en één voor XenDesktop.

Deze beslissing is gebaseerd op de volgende punten:

- In lijn met de aanwezige onderliggende infrastructuur.

### 11.10 Beschikbaarheid

Citrix XenApp en XenDesktop bestaan uit componenten welke een single point of failure kunnen veroorzaken. Als hoge beschikbaarheid een vereiste is en de Citrix farm verspreid is over meerdere datacenters, dan betekent dit dat meerdere componenten beschikbaar moeten zijn in beide datacenters.

| Paragraaf | Vereiste voor hoge beschikbaarheid | Keuze |
|---|---|---|
| **Citrix Licentieserver** | 1 x actieve server + 1 virtueel of fysiek cold standby. De grace periode voor licenties is 30 dagen. De licentieserver is onderdeel van de hypervisor infrastructuur. In het geval van hostuitval zal de Licentieserver actief gemaakt worden op een andere host. | Cold standby niet nodig ivm grace periode van 30 dagen. Dit is afdoende. |
| **Microsoft Terminal server License Server** | 2 actieve servers verspreid over meerdere locaties of 2 op één locatie | Niet inzetten. Restore procedure voor bestaande server inzetten. |
| **Data Collector** | De Data collector rol binnen een zone zal bij uitval van een XenApp server verhuizen naar een vooraf ingestelde XenApp server. In een farm met meerdere zones heeft iedere zone zijn eigen Data collector. | Wordt ingezet. |
| **Datastore database XenApp** | Implementeer SQL clustering of replicatie technologie. Als de Datastore niet beschikbaar is blijft de XenApp server functioneren omdat deze de local host cache raadpleegt voor configuratie informatie voor een periode tot 30 dagen. | Geen SQL cluster beschikbaar. Restore procedure icm Hyper-V failover. |
| **Datastore database XenDesktop** | Implementeer SQL clustering of replicatie technologie. Als de Datastore niet beschikbaar is, is XenDesktop niet beschikbaar voor gebruikers. http://support.citrix.com/article/CTX128328 | Geen SQL cluster beschikbaar. Restore procedure icm Hyper-V failover. |
| **Web Interface** | Configureer meerdere WI's op één locatie of op meerdere locaties en gebruik load balancing | Er worden twee WI's ingericht in het datacenter. |
| **XenApp Server** | Publiceer voor één zone alle applicaties op meerdere XenApp server, voor meerdere zones spreid je de XenApp servers en definieer je een zone per locatie | Wordt ingezet. |
| **XenDesktop Delivery Controller** | Configureer twee XenDesktop controllers, zodat de VDI's hoger beschikbaar zijn in geval van XenDesktop controller uitval. | Wordt ingezet. |
| **XenServer** | Voeg de XenServer feature pack toe voor HA functionaliteit. | Niet van toepassing. |
| **Citrix Access Gateway** | 2de Citrix CAG standby of load balancing instellen | Er wordt 1 fysieke appliance ingezet. |

#### 11.10.1 Licentieserver

Het Citrix licentiemodel is gebaseerd op licentiebestanden welke geïnstalleerd worden op een Citrix licentieserver. Licentiebestanden kunnen op de Citrix website gemaakt worden. Bij het genereren van een licentiebestand wordt er gevraagd om de hostname van de licentieserver. De naam kan uit hoofdletters of kleine letters bestaan, dit moet identiek over genomen worden aangezien het licentie bestand identiek moet zijn ten opzichte van de hostname.

Aangezien het licentie bestand hostname gevoelig is kan er maar één licentieserver zijn. Daarom is het raadzaam een kopie van de server offline beschikbaar te hebben i.v.m. uitval van de licentieserver. Bij voorkeur gevirtualiseerd. Standaard is er een 30 dagen grace periode voor het geval de licentieserver onbereikbaar wordt door uitval. Er is genoeg tijd om een tweede licentieserver operationeel te brengen.

### 11.10.2 Data collector

De eerste XenApp server is de Data collector. Als de server onderuit gaat wordt de Data collector rol overgedragen aan een vooraf gedefinieerde XenApp server. Dit proces is volledig automatisch, geen handmatige actie vereist.

### 11.10.3 Datastore

De Datastore (standaard Microsoft SQL server) kan hoog beschikbaar gemaakt worden door middel van generieke SQL functionaliteiten, zoals clustering of replicatie.

**Ontwerpbeslissing:**
- Er wordt geen SQL clustering ingezet

Deze beslissing is gebaseerd op de volgende punten:
- SQL clustering is niet beschikbaar binnen de VNOG.

### 11.10.4 Web Interface

De Web Interface kan hoog beschikbaar gemaakt worden door middel van meerdere Web Interfaces op meerdere servers, gebruik makend van Windows Server Network Load Balancing (NLB). Deze methode gebruikt load balancing, ook kan er hardware matige load balancing toegepast worden door middel van de Citrix Netscaler.

**Ontwerpbeslissing:**
- Er worden twee WI's ingericht.

Deze beslissing is gebaseerd op de volgende punten:
- Best practice Citrix.

### 11.10.5 Hoge beschikbaarheid

Standaard bieden de XenApp applicatie servers een hoge beschikbaarheid. Meerdere XenApp server kunnen een vaste set applicaties aanbieden, een statisch load balancing mechanisme verdeeld de gebruiker sessies over de beschikbare XenApp servers. In het geval van het uitvallen van een XenApp server bieden de overige XenApp servers toegang tot de applicaties.

Best practices tonen aan dat er overcapaciteit aanwezig moet zijn, zodat bij uitval van één XenApp server er voldoende resources zijn om dit op te vangen. Dit geldt ook voor nood onderhoud.

**Ontwerpbeslissing:**
- Hogere beschikbaarheid door middel van virtualisatie van Citrix omgeving op het Hyper-V cluster.

Deze beslissing is gebaseerd op de volgende punten:
- Eisen VNOG.

### 11.11 Citrix XenApp en XenDesktop Farm

De eerste XenApp server vereist het creëren van een farm naam. Als de farm gemaakt is het mogelijk extra XenApp servers toe te voegen aan de farm. Op farm niveau kan je instellingen zetten die standaard voor iedere XenApp server gelden. Gebruik een eenvoudige en duidelijke naam voor de farm. Voor test en acceptatie doeleinden wordt aangeraden een aparte farm aan te maken. Denk aan OTA (Ontwikkel / Test / Acceptatie).

De XenApp Productie farm naam heet VNOG-XAPROD en de Ontwikkel / Test / Acceptatie farm heet VNOG-XAOTA.

**Ontwerpbeslissing:**
- Creëer twee XenApp farms, één voor Productie en de andere voor Ontwikkel / Test / Acceptatie.

Deze beslissing is gebaseerd op de volgende punten:
- Scheiding tussen test en productie.

Bij XenDesktop werkt het anders. De XenDesktop Controller kan meerdere Golden images aansturen, dit betekent dat een productie Golden image gebruikt wordt, terwijl parallel een ´OTA Golden image´ opgebouwd kan worden voor test doeleinden.

De XenDesktop Productie farm heet VNOG-XDPROD.

**Ontwerpbeslissing:**
- Bouw één XenDesktop omgeving met verschillende Golden images, zoals een productie image en een aparte OTA image.

Deze beslissing is gebaseerd op de volgende punten:
- Peopleware best practice.

### 11.12 Zone

Een XenApp zone bestaat uit een groep servers in hetzelfde subnet. Het wordt gebruikt om de juiste (minst drukke) XenApp server te vinden voor het bouwen van een gebruikers sessie. Voor XenDesktop is zone niet van toepassing.

**Ontwerpbeslissing:**
- Creëer één zone voor de XenApp omgeving.

Deze beslissing is gebaseerd op de volgende punten:
- Best practice.

### 11.13 Silo's

Voor het aanbieden van specifieke applicaties kan er een groep XenApp server ingericht worden. Iedere XenApp server biedt dezelfde set aan applicaties aan. In Server Based Computing termen wordt dit een silo genoemd. Creëer een silo als dit een vereiste is voor een specifieke applicatie, taak, groep of architectuur.

In de huidige omgeving zijn er silo's ingericht voor de volgende applicaties:

- Beaufort (PIS);
- Defacto CAPP (Opleidingen);
- Decos beheertools;
- PDF converter.

Creëer een applicatie silo voor de standaard applicaties. Isoleer applicaties waarvan bekend is dat zij moeilijk integreren met andere applicaties en veel meer van de hardware vragen (geheugen verbruik / CPU). De kans groot dat een slecht functionerende Citrix XenApp server ontstaat wanneer deze applicaties niet geïsoleerd worden.

| XenApp Applicatie silo | Uitleg |
|---|---|
| **Published Desktop** | Eén XenApp server is dedicated datacollector, dus effectief zijn er dertien XenApp servers. |

De XenApp Applicatie silo is hoog beschikbaar, als een Hyper-V host uitvalt, kan de VM herstart worden op een andere ESX host. De 14 XenApp applicatie silo servers zijn verspreid over het Hyper-V cluster.

**Ontwerpbeslissing:**

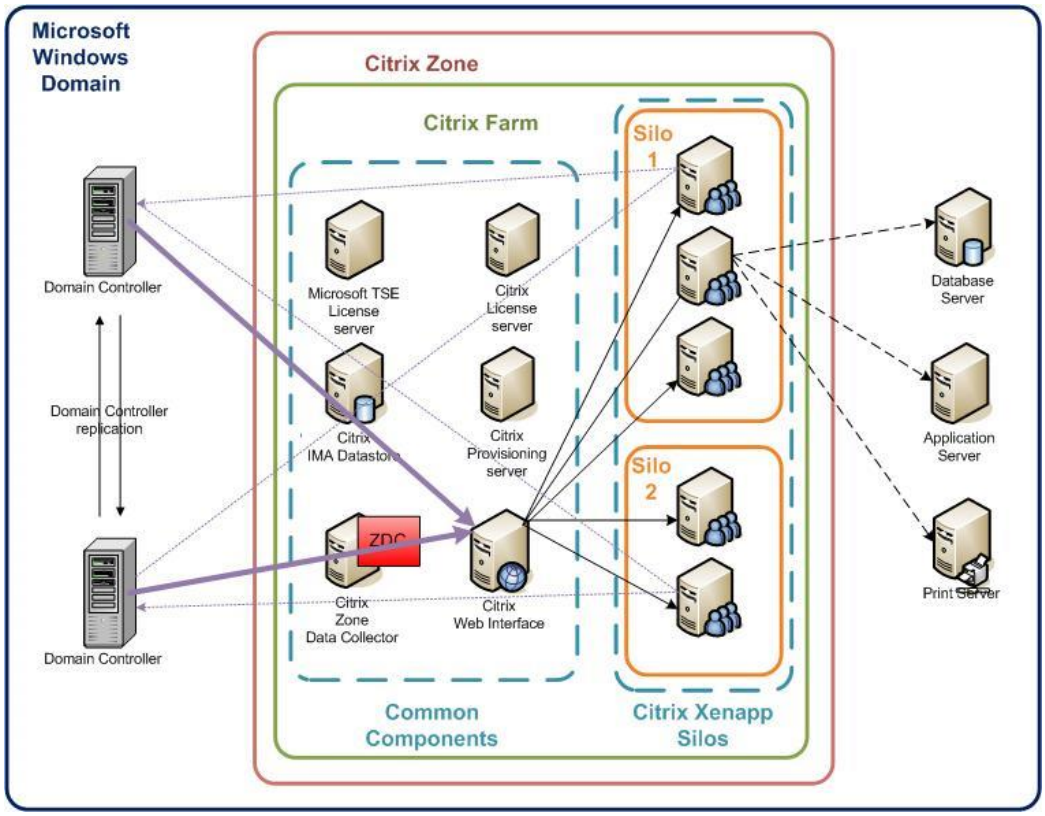
- Eén applicatie silo met daarin de applicaties die voor iedereen beschikbaar moet zijn..

Deze beslissing is gebaseerd op de volgende punten:

- Deze silo vormt de basisinfrastructuur waar alle gebruikers op werken.

### 11.14 Active Directory services

Citrix servers maken gebruik van een specifieke set Group Policies. Best practice is het creëren van een aparte Active Directory OU voor de XenApp servers met hierin eventueel een onderverdeling per rol. Iedere XenApp server biedt dezelfde set aan applicaties aan. De beschikbaarheid van Published Applications en Published Desktops wordt geregeld op basis van groep lidmaatschap in Active Directory. Configureer iedere applicatie met de benodigde groep.




**Figuur 19 Relatie Citrix en AD**

**Ontwerpbeslissing:**

- Integreer met Active Directory en creëer een aparte OU. Maak gebruik van AD groepen voor toegang tot applicaties.

Deze beslissing is gebaseerd op de volgende punten:

- Best practice.

### 11.15 Terminal Server en Client Access Licenties

Citrix XenApp is gebaseerd op Microsoft Remote Desktop Server services. Microsoft vereist voor het gebruik van iedere gebruiker of device een bedrag aan licenties voor toegang tot een RDS server. De RDS Client Access Licentieserver vereist een Windows 2008 besturingssysteem. Deze server geeft toegang tot de Microsoft RDS servers en beheert de licenties.

Er kan geen andere 'oudere' (Windows 2000, 2003) Microsoft licentieserver gebruikt worden. De oude licenties dienen geupgrade te worden. Wel is het zo dat Windows 2003 Terminal Servers gebruik kunnen maken van licenties van de Windows 2008 RDS licentieserver. Dit betekent backwards compatible. Het is gangbaar om deze rol te combineren met de Citrix Licentieserver rol, beide vereisen weinig load van de server.

De licenties zijn niet concurrent als bij Citrix, maar per user met een houdbaarheid van 60 dagen. Dit betekent in de praktijk dat je meer RDS user CALs hebt dan Citrix concurrent user CALs. Schaf voldoende RDS CALs aan voor Windows 2008 en upgrade bestaande CALs tot Windows 2008. Installeer twee licentieservers voor beschikbaarheid in grote Citrix landschappen.

Zet de RDS licentie rol op een virtuele server samen met de Citrix licenties en zorg voor een hoge beschikbaarheid, zodat bij Hyper-V host uitval de virtuele machine gestart kan worden op een andere host. Maak ook een VM backup, zodat je eventueel de VM opnieuw kan toevoegen op een Hyper-V host.

**Ontwerpbeslissing:**
- Combineer de RDS licentieserver met de Citrix licentieserver.

Deze beslissing is gebaseerd op de volgende punten:
- Best Practice.

### 11.16 Citrix licenties en licentieserver

Citrix biedt vier varianten voor XenApp 6.5, namelijk: Fundamentals, Advanced, Enterprise en Platinum.
Voor XenDesktop 5.6 heeft Citrix vier varianten, namelijk: Express, VDI, Enterprise en Platinum. Ook moet er bij XenDesktop een keuze gemaakt worden voor: Concurrent user, user license of device license.

Zie voor alle XenDesktop features onderstaande link:
http://support.citrix.com/article/CTX128328

Installeer een licentieserver met hierop de benodigde licenties, geschikt voor het aantal concurrent Citrix sessies. Het wordt geadviseerd om gebruik te maken van Subscription Advantage bij de aanschaf van Citrix licenties. Dit geeft de mogelijkheid om kosteloos te upgraden naar nieuwere versies.

**Ontwerpbeslissing:**
- Bestaande 200 XenApp Enterprise[6] licenties verhogen naar 230.

Deze beslissing is gebaseerd op de volgende punten:
- 80% concurrency voor 350 gebruikers – 50 XenDesktop licenties.

Voor XenDeskstop worden concurrent Platinum licenties ingezet, zodat je tot een maximaal gelijktijdige gebruikers toegang kan bieden tot XenDesktop. Daarnaast heb je gelijk Access Gateway Universal licenses in bezit, waardoor je dezelfde hoeveelheid gebruikers externe toegang (Telewerk) kan bieden naar XenApp/XenDesktop.

**Ontwerpbeslissing:**
- 50 XenDesktop Platinum CCU licenties.

Deze beslissing is gebaseerd op de volgende punten:
- XenDesktop licenties bevat ook een XenApp licentie.

### 11.17 Subscription advantage (SA) op licenties

Het Subscription Advantage programma zorgt ervoor dat Citrix klanten snel en kosten efficiënt verder kunnen bouwen op de bestaande Citrix infrastructuur met de laatste product updates.
Bij de aanschaf van Citrix licenties met Subscription Advantage geeft het recht op 1 jaar support op de laatste Citrix updates, zoals bijvoorbeeld een toekomstige opvolger van XenApp 6.5 of XenDesktop 5.6.

De voordelen op een rij:
- Voorspelbaar budget voor Citrix upgrades door het jaar;
- Bescherming van de investering op de aangeschafte Citrix;
- Op de hoogte blijven van het laatste nieuws en relevante informatie voor SA leden;
- Verlopen subscriptions kunnen hernieuwd worden.

Het advies is om licenties aan te schaffen en/of te upgraden met Subscription Advantage

**Ontwerpbeslissing:**
- Citrix licenties worden aangeschaft met Subscription Advantage.

Deze beslissing is gebaseerd op de volgende punten:
- Zie voordelen.

[6] Zie voor alle XenApp features onderstaande link:
http://www.citrix.com/site/resources/dynamic/additional/Citrix_XenApp_6.5_Comparative_Feature_Matrix.pdf

### 11.18 Datastore

De Datastore is de database welke alle instellingen opslaat van de Citrix omgeving.
Ondanks dat er meerdere Database leveranciers ondersteund is het gebruik van Microsoft SQL server gemeengoed voor het hosten van de Datastore, zeker voor grote Citrix omgevingen.
Voor kleine farms of een proof of concept omgeving kan de Datastore gehost worden op een server met SQL 2008 Express geïnstalleerd.

| Schaal | Servers | Applicaties | Databases |
|---|---|---|---|
| **Small** | 1-50 | 1-100 | Access, SQL, SQL Express, Oracle, DB2 |
| **Medium to Large** | 51-100 | 100-1000 | MS SQL, Oracle, DB2 |
| **Large enterprise** | 100+ | 1000+ | MS SQL, Oracle, DB2 |

Minimale disk ruimte voor een Datastore is ongeveer 20MB voor iedere 100 XenApp servers.

Voor het geval dat de Datastore niet beschikbaar is kan de XenApp server verder functioneren op basis van de "local host cache" (LHC), lokaal aanwezig met configuratie informatie voor een periode tot 30 dagen. De LHC bevat een gedeelte van de informatie welke aanwezig is op de Datastore. XenDesktop functioneert niet meer als SQL niet beschikbaar is.

Ondanks SQL 2008 Express geschikt is voor omgevingen tot 50 XenApp servers, is het toch raadzaam om een SQL server te gebruiken. Het spreiden van de SQL rol is best practice Citrix. SQL 2008 is minimaal vereist voor XenDesktop, zie http://support.citrix.com/article/CTX114501.
XenApp 6.5 kan ondergebracht worden op een SQL 2005 SP4 instance. Het inzetten van een dedicated SQL instance biedt de volgende voordelen:

- Datastore is een gedeelde database, waar alle XenApp servers van afhankelijk zijn, best practice om deze centraal aan te bieden op een dedicated SQL 2005 SP4 of SQL 2008 server;
- Patch beleid wordt belangrijker ivm aanwezige rollen op XenApp server waar ook SQL express database op draait;
- XenApp stabiliteit is in het algemeen minder in vergelijking tot een datastore op een dedicated SQL server;
- Troubleshooting is in het algemeen lastiger in geval van problemen;
- XenApp servers worden dagelijks herstart ivm memory leaks, in het geval van XenApp local database (Express) moet je de volgorde van reboot nauwkeurig bepalen.

**Ontwerpbeslissing:**

- SQL 2008 R2 SP1 Express wordt gebruikt voor de XenDesktop datastore.
- De bestaande SQL 2005 SP4 instance op VDB01 wordt ingezet voor XenApp.

Deze beslissing is gebaseerd op de volgende punten:

- Er hoeft geen licentie aangeschaft te worden.

### 11.19 Data collector

De data collector verzamelt alle dynamische informatie, zoals aantal sessies, actieve licenties, beheerders, beschikbare servers, load op servers, enz. De data collector regelt ook de master browser rol binnen de zone.

Iedere zone binnen een farm vereist een data collector. Ook al is het zo dat meerdere XenApp server geschikt zijn voor de rol er kan maar één actief zijn binnen een zone. Standaard is de eerste server in de farm "most preferred", oftewel de data collector rol. Andere servers staan ingesteld op "default preference".

Voor een grote XenApp farm is het een gegeven om geen applicaties of desktop aan te bieden op de XenApp server met de data collector rol.

**Ontwerpbeslissing:**
- Maak de eerste XenApp server data collector en publiseer geen applicaties of desktops.

Deze beslissing is gebaseerd op de volgende punten:
- Citrix best practice.

### 11.20 XenApp applicatie servers

De XenApp applicatie server publiseren applicaties en/of desktop aan gebruikers. Hiervoor is minimaal één XenApp server nodig. Het aantal XenApp servers hangt af van:
- het aantal gebruikers dat gebruik maakt van de omgeving;
- het aantal aan te bieden applicaties;
- soort applicatie (3D intensief, maatwerk);
- virtuele XenApp server of fysiek, op een virtuele server kunnen minder sessies aanbieden.

Voor het streamen van applicaties naar client devices dient minimaal één XenApp server als streaming applicatie hub. Het is raadzaam een proof of concept omgeving op te zetten welke identiek is aan de productie omgeving om het aantal te behalen sessies te testen. Minimaal één XenApp server is vereist voor het opzetten van een farm. Stel voldoende XenApp servers beschikbaar voor het aantal gebruikers. Stel voldoende XenApp servers beschikbaar voor het aantal gebruikers, gebaseerd op veilige waardes.

| Sizing informatie | Omschrijving |
|---|---|
| **Sessies per XenApp server: 25 – 30 concurrent sessies** | Het aantal sessies hangt sterk af van de type applicaties. Applicaties die veel geheugen en/of CPU gebruiken beïnvloeden het aantal te behalen sessies negatief. Virtualiseren van XenApp servers genereert een overhead van 7% aan minder te halen sessies. |
| **64-bits platform:** | 64-bit Windows adresseert meer dan 4 GB geheugen, door meer geheugen toe wijzen kun je meer sessies aanbieden. |

**Ontwerpbeslissing:**
- XenApp servers worden geschaald voor 25-30 gebruikers.

Deze beslissing is gebaseerd op de volgende punten:
- Peopleware best practice.

### 11.21 Citrix Branch Repeater (optioneel)

Een Citrix Branch Repeater kan ingezet worden om ICA verkeer te versnellen over het WAN naar bijkantoren. Eén Branch Repeater wordt geplaatst in het datacenter, de ontvangende Repeater wordt geplaats op een remote locatie om optimaal ICA accelaratie te verkrijgen. De client device kan rechtstreeks gebruik maken van de ICA acceleratie door de Repeater plug-in te installeren. Sommige Thin Client fabrikanten hebben de client Repeater plug-in geïntegreerd in de embedded software, zoals Wyse bijvoorbeeld.

Citrix adviseert het gebruik van de Branch Repeater op plaatsen in het netwerk waar de aanwezige bandbreedte niet toereikend is. Branch Repeater kan tot 50% besparen op de vereiste bandbreedte. Gebruik een Branch Repeater op locaties waar de aanwezige bandbreedte onvoldoende is. In sommige gevallen kan zelfs de bandbreedte onvoldoende zijn voor de Branch Repeater. De enige manier om dit op te lossen is een (fysieke) lijn upgrade.

**Ontwerpbeslissing:**
- De VNOG kiest ervoor om eerst zonder Branch Repeater te opereren.

Deze beslissing is gebaseerd op de volgende punten:
- De verbindingen naar de diverse kantoren zijn overgezet naar E-VPN.

### 11.22 Citrix Access Gateway (optioneel)

De Citrix Access Gateway kan ingezet worden om een betrouwbare externe toegang te bieden naar de Citrix XenApp servers. Alleen ge-encrypte scherm informatie, toets aanslagen en muis klikken gaan de lijn over via het internet over SSL. Citrix adviseert het gebruik van de Citrix Access Gateway voor externe beveiligde toegang tot XenApp.

Zet twee Citrix Netscaler VPX standard in om een hoog beschikbare Telewerk dienst op te leveren. De Netscaler VPX is virtueel en is lager in aanschaf ten opzichte van een Citrix Netscaler MPX 5500 Standard met 3 jaar garantie. Door de virtuele appliance op verschillende Hyper-V hosts te zetten elimineer je een Single Point of Failure. De load balancing feature door de inzet van twee Netscaler virtual appliances geeft op applicatie niveau een hogere beschikbaarheid, immers de Web Interface die bereikt moet worden wordt gecontroleerd op XML beschikbaarheid. Mocht de dienst niet actief zijn, wordt automatisch de andere Web Interface gebruikt. Deze vorm van beschikbaarheid kan NLB niet bieden.

Two factor authenticatie is vereist om een beveiligde manier toegang te geven aan de thuiswerk mogelijkheid voor VNOG. Peopleware adviseert om van de bestaande Safeword hardware token authenticatie over te stappen op SMS token authenticatie. Deze mogelijkheid verlaagt de beheerslast en verhoogt het gebruikersgemak.

De klant kiest voor 1 Citrix Netscaler MPX 5500 Cluster + Safeword SMS authentcatie.
De beschikbaarheid van de Telewerk dienst is minder hoog door de Single Point of Failure door de inzet van een MPX 5500.

**Ontwerpbeslissing:**
- Er wordt een Netscaler MPX 5500 ingezet met Safeword token authenticatie;
- Optioneel wordt SMS token authenticatie ingezet;
- Access Gateway Universal licenties nodig voor XenApp Enterprise gebruikers.

Deze beslissing is gebaseerd op de volgende punten:
- VNOG heeft een voorkeur voor hardware appliances.
- Safeword is reeds in gebruik.

### 11.23 Beheer rechten Citrix omgeving

In de Citrix omgeving dien je in te stellen welke personen volledige rechten nodig hebben voor het uitoefenen van de beheer functie. Andere personen zoals helpdeskmedewerkers kunnen rechten krijgen voor het meekijken in een sessie, sessies afmelden etc. De rechten wijs je toe op basis van de vereiste bevoegdheden, dit noem je een rol. Aan de rol koppel je een Active Directory groep.

Stel de rechten zorgvuldig in, verkeerd instellen kan leiden tot ongecontroleerde acties in een productie omgeving. De medewerkers dienen de juiste kennis te bezitten voor het uitoefenen van de XenApp beheer taken.

| Groep | Rechten |
|---|---|
| **Manage Citrix Servers** | Local Admin on XenApp servers |
| **Citrix Admins** | Full Citrix admin rights XenApp servers |
| **Citrix Helpdesk** | Shadow session, reset session, view rights |

**Ontwerpbeslissing:**
- Richt een delegatie model in volgens voorbeeld.

Deze beslissing is gebaseerd op de volgende punten:
- Peopleware best practice.

**Ontwerpbeslissing:**
- Shadow session is mogelijk zonder digitale toestemming

Deze beslissing is gebaseerd op de volgende punten:
- VNOG best practice. De toestemming wordt mondeling verkregen.

### 11.24 Schaalbaarheid

De Citrix XenApp is schaalbaar. De applicaties zijn aan te bieden op meerdere XenApp servers. Uitbreiden van de Citrix farm is te allen tijde mogelijk. Zorg voor extra capaciteit door middel van extra XenApp servers en een realistische sizing per server op basis van stress tests en bestaande gegevens (bijvoorbeeld soort applicaties) van de klant.

De berekening is gemaakt op basis 80% concurrency in relatie tot 350 gebruikers, maakt 280 gebruikers. Hier wordt er 1 spare server bij opgeteld en een data collector server. Op basis van 25 gebruikers per server zijn er afgerond 14 XenApp servers nodig.

| Aantal servers | aantal gebruikers per server | Totaal |
|---|---|---|
| **12** | 25 | 300 |
| **+1 (N+1)** | 25 | 25 |
| **13** | | **325** |

**Ontwerpbeslissing:**
- Er zijn 14 XenApp servers nodig.

Deze beslissing is gebaseerd op de volgende punten:
- 80% concurrency;
- N+1 model;
- 1 dedicated data collector.

### 11.25 Monitoring

Citrix heeft de module Edgesight voor het monitoren van de gebruikers ervaring. Dit component is optioneel en wordt geleverd bij XenApp Platinum of XenDesktop Platinum.

De Citrix omgeving kan gemonitord worden door middel van Microsoft System Center Operation Manager (SCOM). Op de SCOM omgeving dien je een Citrix extension pack toe te voegen.

Monitor de omgeving door het toevoegen van de Citrix management pack aan de Microsoft System Center Operation Manager (SCOM). De performance en capacitieit is meetbaar via SCOM. Implementeer EdgeSight om gebruikersbeleving te toetsen door de XenApp servers te meten en eventuele pijnpunten te verhelpen.

**Ontwerpbeslissing:**
- Citrix monitoring door middle van SCOM.

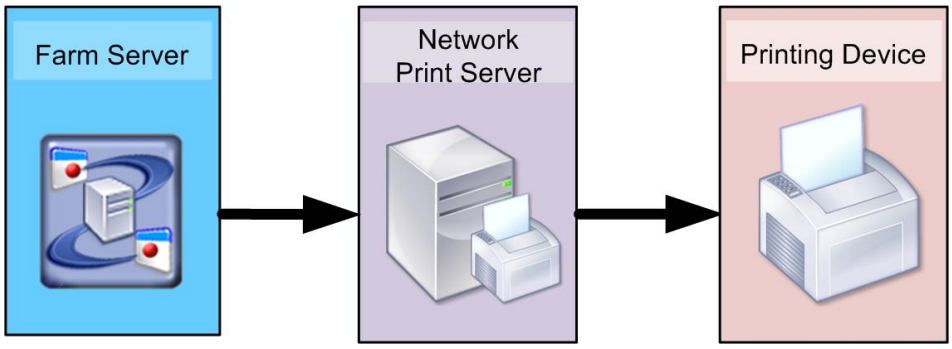
Deze beslissing is gebaseerd op de volgende punten:
- Onderdeel van project;
- Geen additionele investeringskosten.

### 11.26 Printing

Er zijn een aantal manieren om te printen vanuit een Citrix sessie.

#### 11.26.1 Sessie printer(s)

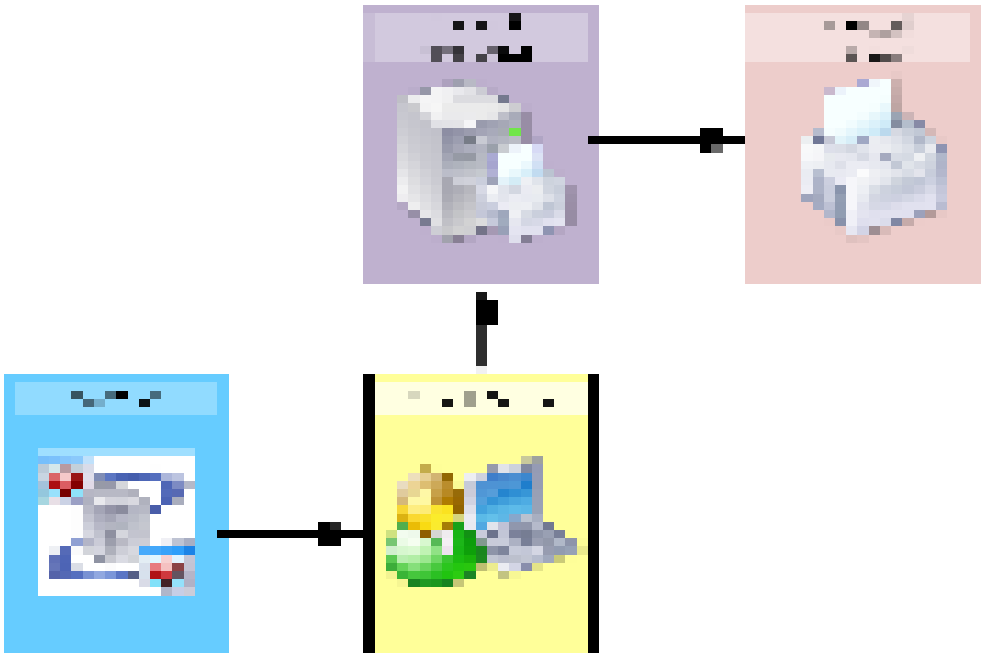
Één of meerdere netwerk printers wordt aangeboden in de Citrix sessie.




**Figuur 20 Session printing**

### 11.26.2 Autocreated printer naar netwerk printer

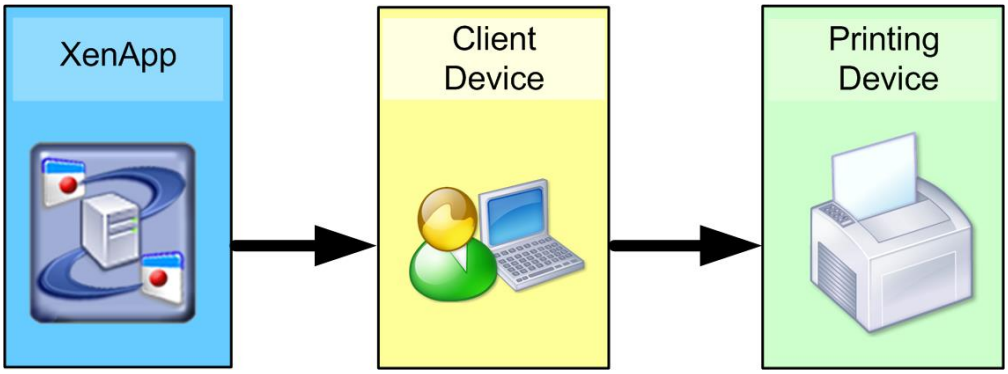
Aanwezige printers op de client device worden meegenomen naar de Citrix sessies.



**Figuur 21 Autocreated printer naar netwerk printer**

### 11.26.3 Autocreated printer naar lokaal aangesloten printer

Rechtstreeks gekoppelde printer wordt meegenomen naar de Citrix sessie.




**Figuur 22 Autocreated printer naar lokaal aangesloten printer**

### 11.26.4 Keuze

Welke methode gebruikt gaat worden hangt af van
- Afhankelijkheden applicatie;
- Locatie werkplek;
- Bandbreedte;
- Plaatsing print server.

Kortom, gebruiker A (helpdesk) kan baat hebben bij optie 1 en gebruiker B. (HR) bij optie 3 bij het printen van vertrouwelijke documenten.

**Ontwerpbeslissing:**
- De printmethode worden dynamisch toegepast op basis van rollen.

Deze beslissing is gebaseerd op de volgende punten:
- Geen eenduidige printbehoefte.

De printer deployment gebeurd op de werkplek. De Citrix Universal Printer driver wordt gebruikt voor ieder type printer, tenzij er technische beperkingen zijn waardoor er voor specifieke drivers gekozen wordt. Het spoelen van de opdracht gebeurd op de werkplek, waardoor op het LAN de print opdracht

Printer drivers kunnen alleen geïnstalleerd worden door een beheerder op de XenApp servers. XenApp printer instellingen worden bewaard op de lokale werkplek en niet in het Terminal server profiel. Het is best practice om het aantal drivers tot een minimum te houden i.v.m. instabiliteit door slecht geschreven drivers.

**Ontwerpbeslissing:**
- Maak gebruik van zo min mogelijk print drivers. Bij voorkeur gebruik HP Universal Print Drivers en Citrix Universal Print Drivers.

Deze beslissing is gebaseerd op de volgende punten:
- Best practice.

## 11.27 Load Balancing

Load balancing regels kunnen ingesteld worden om de gebruikers te verdelen over XenApp servers. Er zijn drie opties, namelijk standard, advanced en custom. Het doel is om de XenApp servers dusdanig te belasten zodat de gebruikers een optimale gebruikersbeleving hebben. De XenApp server kun je als het ware begrenzen op het aantal users of applicaties.

**Ontwerpbeslissing:**
- Er wordt gebruik gemaakt van de Advanced load evaluator .

Deze beslissing is gebaseerd op de volgende punten:
- Verdeling van de load op basis van CPU, geheugen en page file gebruik.

### 11.28 Reboot schedule

Standaard policy in XenApp omgeving is het regelmatig herstarten van de servers om het RAM te schonen i.v.m. mogelijke memory leaks en applicatie errors. Eén uur van te voren worden de logons dichtgezet op de servers die in reboot mode gaan en gebruikers worden geïnformeerd om af te melden en aan te melden naar een andere XenApp server (die niet in herstart gaat, of al geweest is).

Herstart de XenApp servers dagelijks. Hiermee blijven de XenApp servers snel en stabiel.
Zorg voor een gestaffelde reboot plan, zodat er te allen tijde XenApp servers beschikbaar zijn.

Aangezien de meldkamer gebruik maakt van de XenApp omgeving mogen deze sessies niet verbroken worden. Hiervoor worden XenApp servers met actieve sessies niet herstart.

**Ontwerpbeslissing:**
- Niet actieve XenApp servers worden dagelijks herstart. De 'even' servers om 3:00, de 'oneven' servers om 4:00.

Deze beslissing is gebaseerd op de volgende punten:
- Peopleware best practice.
- VNOG eisen t.a.v. XenApp omgeving van de meldkamer.

### 11.29 Profielen

Microsoft biedt een aantal profiel types aan die gebruikt kunnen worden in een Windows Terminal Services omgeving, namelijk:
- Lokale profielen – snel, maar wordt niet op netwerk opgeslagen en dit vervuilt de XenApp servers;
- Mandatory profielen – statisch profiel, wijzigingen worden niet bewaard, voordeel is het klein houden van het profiel;
- Roaming profielen – dynamisch profiel, wijzigingen worden centraal opgeslagen en zijn voor alle XenApp servers beschikbaar, nadeel is dat de profielen groot worden en de aanmeld tijd vertragen.

Citrix biedt met Citrix Profile manager een product aan die de profielen up to date houdt met gebruik van applicatie silo's. Standaard probleem met roaming profielen en silo's is het 'last write wins' principe. Hierdoor kunnen net ingestelde instellingen overschreven worden door de laatste afmelding van een Citrix sessie. Citrix Profile manager lost dit op door iedere wijziging direct op te slaan naar het netwerk, waardoor de laatste instellingen altijd beschikbaar zijn.

**Ontwerpbeslissing:**
- Implementeer Citrix profile manager in XenApp omgeving.

Deze beslissing is gebaseerd op de volgende punten:
- Peopleware best practice bij implementaties zonder 3rd party tooling.

### 11.30 Windows server versie

Microsoft heeft meerdere versies van het besturingssysteem Windows Server 2008 R2 welke geschikt zijn voor het aanbieden van de Terminal Services rol met daarop Citrix XenApp.
De volgende versies zijn beschikbaar:

- Standard editie x64;
- Enterprise editie x64;
- Datacenter editie x64.

De Standard en Enterprise editie bieden de vereiste functionaliteit voor het gebruiken van Remote Desktop Services en XenApp. De Datacenter editie is niet nodig.

De Datacenter licenties die op het Hyper-V cluster horen geven de mogelijkheid om zelf te kiezen welke editie er op de VM's gedraaid wordt.

**Ontwerpbeslissing:**

- Windows 2008 R2 x64 Enterprise wordt gebruikt als besturingssysteem voor XenApp 6.5 Enterprise.

Deze beslissing is gebaseerd op de volgende punten:

- Volgens de ontwerpbeslissing ten aanzien van VM's op het Hyper-V cluster.

### 11.31 Backup

Het dagelijks backuppen van de XenApp server is niet nodig, aangezien de XenApp server statisch is.

- Profielen - De profielen zijn dynamisch en worden bij het afmelden verwijderd
- Applicaties – Deze worden aangeboden d.m.v. Streaming of rechtstreeks installeren
- OS updates – Dit zijn changes waarvoor je een aparte backup maakt
- Citrix patches – Dit zijn changes waarvoor je een aparte backup maakt

Backup overzicht Citrix componenten:

| Backup | Component |
|---|---|
| **Ja** | Citrix License Server |
| **Ja** | Microsoft Terminal Server License Server |
| **Ja** | Data-collector (eerste XenApp server in de farm) |
| **Ja** | Data-store Database |
| **Ja** | Web Interface |
| | |
| **Nee** | XenApp Applicatie Servers |
| **Ja** | XenDesktop Delivery Controller |
| **Ja** | Citrix Provisioning Server (optioneel) |
| | |
| **Nee** | Citrix Branch Repeater (optioneel) |
| **Nee, alleen kopie van de configuratie noodzakelijk** | Citrix Access Gateway (optioneel) |
| **Ja** | Virtualisatie Platform (optioneel) |

Backup volgens de tabel

**Ontwerpbeslissing:**

- Backup volgens de tabel.

Deze beslissing is gebaseerd op de volgende punten:

- Peopleware best practice.

### 11.32 Citrix Clients

Gepubliceerde applicaties en desktops kan je op twee manieren ontsluiten:
- Door middel van de Citrix Web Interface;
- Door middel van de the PNAgent interface (applicatie wordt toegevoegd aan het startmenu van de gebruiker).

De Citrix Receiver 3.2 Enterprise wordt geïmplementeerd op de client device om toegang te geven aan gepubliceerde applicaties of desktops door middel van de PNAgent en de Web Interface.

Verschillende clients zijn beschikbaar als download via de global Citrix site.
Als alternatief kan de Citrix client aangeboden worden via Merchandising server of via de Web Interface.

1. Push de Citrix Receiver client door middel van SCCM naar de werkplekken.
2. Push de Citrix Receiver client via de Web Interface voor thuiswerkers. Bij het eerste keer aanmelden wordt de client geïnstalleerd.

Voeg Citrix Receiver 3.2 toe aan de werkplek en verwijder de aanwezige client.

**Ontwerpbeslissing:**
- Citrix Reciever 3.2 Enterprise middels PNAgent en Web Interface.

Deze beslissing is gebaseerd op de volgende punten:
- .

### 11.33 Web Interface en Services site

Voor interne toegang vanaf een kantoor locatie word de aanmelding op de Web Interface geregeld d.m.v lokaal geïnstalleerde Citrix Receiver 3.2 Enterprise. De standaard layout wordt gebruikt.

Two factor authenticatie op basis van AD + Safeword token. Optioneel SMS authenticatie.

**Ontwerpbeslissing:**
- Voor externe toegang vanaf https://telewerk.vnog.nl wordt two factor authenticatie toegepast.

Deze beslissing is gebaseerd op de volgende punten:
- Best practice.

### 11.34 Antivirus software

Antivirus software is belangrijk om XenApp servers en VDI werkplekken te beschermen tegen virussen. Antivirus instellingen worden toegepast op basis van Citrix best practice artikel http://support.citrix.com/article/CTX127030

Peopleware adviseert om Citrix artikel CTX127030 en Microsoft best practice artikel 822158 toe te passen om de performance optimaal te houden van de XenApp omgeving. Standaard Antivirus instellingen hebben namelijk een grote negatieve impact op de performance wat resulteert in minder XenApp sessies en gebruikersbeleving.

**Ontwerpbeslissing:**
- Antivirus inrichting Citrix volgens CTX12703 en Microsoft KB822158.

Deze beslissing is gebaseerd op de volgende punten:
- Peopleware best practice.

# Hoofdstuk 12 Beheer

## 12.1 Virtueel vs Fysiek

Het uitgangspunt 'Virtueel tenzij…' is van toepassing bij dit ontwerp. In dat kader zijn alle voor de monitoring benodigde System Center virtualisatiekandidaten, mits deze servers niet te IO-intensief zijn. DPM valt af, aangezien deze een afhankelijkheid heeft met de tapelibrary.

**Ontwerpbeslissing:**
- De SCOM, SCCM en SCVMM omgevingen worden virtueel uitgevoerd.
- DPM wordt op een fysieke server uitgevoerd.

Deze beslissing is gebaseerd op de volgende punten:
- De minimale IOPS die de disks kunnen leveren;
- De gebruikmaking van de resources op de Hyper-V hosts dient onder de 75% te blijven;
- De benodigde resources (CPU, RAM en diskruimte) dienen gealloceerd te worden.

## 12.2 Database server

De diverse System Center componenten hebben SQL Server 2008 SP1 over hoger nodig om te kunnen werken. Hiervoor wordt een virtuele databaseserver ingericht.

Aangezien SCOM, SCCM en SCVMM ieder een dedicated Reporting server nodig hebben wordt deze rol drie maal ingericht door middel van instances.

**Ontwerpbeslissing:**
- De databaseserver krijgt 4 vCPU's en 16 GB geheugen;
- Voor een optimale performance dienen de databases op een eigen LUN te staan.

Deze beslissing is gebaseerd op de volgende punten:
- Berekening[7] gemaakt met de volgende cijfers: 150 Agents en 100 Network devices;
- Belasting SCCM en SCVMM is minimaal vergeleken met SCOM.

[7] Berekening gemaakt m.b.v. System Center 2012 Operations Manager Sizing Helper Tool v1.xls

## 12.3 Operations Manager

### 12.3.1 Management Group naam

Een SCOM omgeving moet een Management Group naam hebben.

**Ontwerpbeslissing:**
- De Management Group heet: **VNOGSCOM**

Deze beslissing is gebaseerd op de volgende punten:
- De naam wordt overgenomen uit de bestaande inrichting;
- De Management Group naam kan achteraf niet worden gewijzigd en moet daarom zorgvuldig worden gekozen.

### 12.3.2 Managementserver

De managementserver bezit alle configuratie informatie voor System Center Operations Manager. Een System Center Operations Manager implementatie heeft minimaal één managementserver nodig. Alle agent en statusinformatie wordt naar de managementserver verstuurd. Vervolgens "update" de managementserver de informatie die opgeslagen staat op de SCOM database.

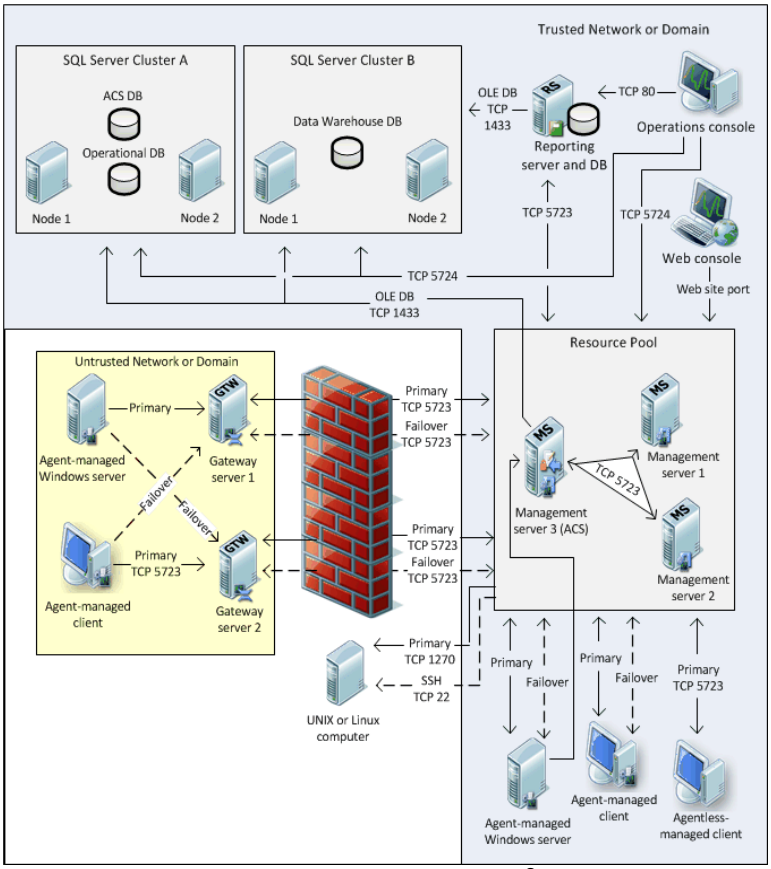
Er wordt geen tweede management server ingezet voor HA functionaliteit, was wel best practice is. HA wordt verkregen doordat de VM op een VMWare cluster draait.

**Ontwerpbeslissing:**
- Er wordt één Managementserver ingezet.

Deze beslissing is gebaseerd op de volgende punten:
- De omgeving vereist één server;
- Een HA server wordt weggelaten, aangezien er gebruik wordt gemaakt van Hyper-V clustering functionaliteit.
- Een SCOM infrastructuur is flexibel.

### 12.3.3 Operations Manager topologie

De onderstaande afbeelding toont de SCOM elementen met hun onderlinge relatie.




**Figuur 23 SCOM topologie[8]**

### 12.3.4 OperationsManager database

De OperationsManager database bevat alle configuratiegegevens over een SCOM omgeving. Daarnaast bevat het de monitoring data van deze omgeving. De data bestaat uit de status en de historie van de laatste zeven dagen. Het zogenaamde grooming proces schoont de database op.

| Onderwerp | Waarde |
|---|---|
| **SCOM DB: Number of Days for Data Retention** | 7 |
| **Number of Server Computers** | 150 |
| **Number of Network Devices** | 100 |
| **Number of APM-enabled Computers** | 0 |
| **Total Size (MB)** | 4925,38 |
| **Total Size (GB)** | 4,81 |
| **Total Size (GB) with 50% Buffer** | 7,21 |
| **Benodigde IOPS** | 250 |
| **Data volume type** | RAID5 |
| **Data volume size (GB)** | 50 |
| **Log volume type** | RAID1+0 |
| **Log volume size (GB)** | 10 |

[8] Bron: Deployment Guide for System Center 2012 - Operations Manager, april 2012, Microsoft.

### 12.3.5 DataWarehouse Database

De OperationsManagerDW database bevat alle historische gegevens over een SCOM omgeving. De data bestaat uit de status en de historie van het laatste jaar. Het zogenaamde grooming proces schoont de database op.

| Onderwerp | Waarde |
|---|---|
| **SCOM DW: Number of Days for Data Retention** | 365 |
| **Number of Server Computers** | 150 |
| **Number of Network Devices** | 100 |
| **Number of APM-enabled Computers** | 0 |
| **Total Size (MB)** | 198959,13 |
| **Total Size (GB)** | 194,30 |
| **Total Size (GB) with 10% Buffer** | 213,73 |
| **Benodigde IOPS** | 500 |
| **Data volume type** | RAID5 |
| **Data volume size (GB)** | 450 |
| **Log volume type** | RAID1+0 |
| **Log volume size (GB)** | 50 |

### 12.4 Configuration Manager

De SCCM inrichting bestaat uit één Primary Site. Deze wordt gehost in het datacenter in Apeldoorn. Er wordt geen Central Administration Site ingericht, aangezien deze niet nodig is voor de grootte van de omgeving.

**Ontwerpbeslissing:**
- De inrichting bestaat uit één Primary Site.

Deze beslissing is gebaseerd op de volgende punten:
- Best Practice.

De server krijgt de volgende SCCM rollen.
- Site server;
- Component server;
- Management point;
- Distribution point;
- State migration point;
- Software update point;
- System Health Validation point;
- Fallback status point.

De SQL database van SCCM wordt geplaatst op de centrale System Center database server, de VDB04. Deze krijgt de volgende SCCM rollen:
- Site database sever;
- Reporting services point;

**Ontwerpbeslissing:**
- Database en Reporting componenten op separate SQL Server.

Deze beslissing is gebaseerd op de volgende punten:
- Performance Best Practice.

Naast de basisinrichting van SCCM worden de volgende functionaliteiten ingericht:
- Windows Updates, het beheren van Microsoft updates en patches;
- Operating System Deployment (OSD), het installeren van een OS;
- Software Distributie, het distribueren van OS en software;
- Compliance, het controleren of de werkplekken en servers in de infrastructuur voldoen aan de standaard.

Er worden drie OSD's gemaakt, te weten:
- Windows 7 Professional voor laptops;
  - Toshiba Satellite Pro P300;
  - HP XX (nader te bepalen);
- Windows 7 voor desktops;
  - HP dx2400;
  - HP YY (nader te bepalen);
- Windows Server 2008 R2 Enterprise voor VM's;
- Windows Server 2008 R2 Standard voor HP DL380.

Voor de uitrol van Windows 7 en Server 2008 is een KMS productcode nodig. Uitrol m.b.v. MAK productcodes is niet mogelijk. Zie paragraaf 8.1.1.

### 12.5 Virtual Machine Manager

Met System Center Virtual Machine Manager wordt het Hyper-V cluster beheerd. Daarnaast kan SCVMM gebruikt worden om V2V en P2V migraties uit te voeren.

**Ontwerpbeslissing:**
- SCVMM wordt virtueel geïnstalleerd.

Deze beslissing is gebaseerd op de volgende punten:
- Supported door Microsoft.

De SQL server wordt geïnstalleerd op de dedicated database server voor System Center.

Om de load opnieuw te verdelen nadat de uitgevallen node weer online is gebracht kan gebruik worden gemaakt van Performance Resource Optimization (PRO) tips. Hierbij geeft SCOM advies over de verdeling van VM's over de beschikbare Hyper-V nodes.

**Ontwerpbeslissing:**
- Database en Reporting componenten op separate SQL Server.

Deze beslissing is gebaseerd op de volgende punten:
- Full versie SQL nodig om PRO Tips te kunnen gebruiken.

### 12.6 Data Protection Manager

DPM wordt ingericht op een fysieke server. Om op Hyper-V niveau backups te maken wordt de Hyper-V rol op dit systeem geïnstalleerd.


**Figuur 24 D2D2T met DPM (Bron: Microsoft Technet)**

#### 12.6.1 Tape Library

Om de backup op tape te schrijven wordt de bestaande HP MSL 2024 gebruikt.

| Item | Waarde |
|---|---|
| **Tapedrive** | HP LTO Gen. 4 |
| **Aantal** | 1 |
| **Compressie waarde (praktijk)** | 1,3 |
| **Maximale toevoersnelheid voor backupserver** | 120 Mb/s uncompressed |
| **Aantal streams per tapedrive** | 8 |
| **Gemiddelde backupstream (afhankelijk van backupclient en datatype)** | 15 Mb/s |

**Ontwerpbeslissing:**
- Genereer een rapportage waarin de te wisselen tapes worden aangegeven.

Deze beslissing is gebaseerd op de volgende punten:
- Beheergemak.

### 12.6.2 DPM Clients

DPM zal op Hyper-V niveau backups maken van de omgeving. Voor VM's met pass-throught LUNs en fysieke servers zal de DPM client op de server geinstalleerd worden.

### 12.6.3 Disaster Recovery

Voor de gehele infrastructuur zal een disaster recovery procedure geschreven worden.

### 12.6.4 Snapshots

In totaal kan de DPM server maximaal 9000 express full backups en file recovery point snapshots aan. Incremental synchronizations worden niet meegeteld. Bijgaand de berekening van het aantal snapshots wat er nodig is. Per volume kunnen er maximaal 64 Recovery Point gemaakt worden. Maximaal 8 scheduled recovery point per Protection Group per dag.

| Server | Aantal | Express Full (dag) | Recovery point (dag) | Incremental Syncronization (min) | Retention (dag) | Snapshots |
|---|---|---|---|---|---|---|
| **Fileserver** | 1 | - | 8 | - | 7 | 56 |
| **Exchange** | 1 | 4 | - | 15 | 7 | 28 |
| **SQL** | 3 | 4 | - | 60 | 7 | 84 |
| **VM's** | 70 | 1 | - | 60 | 7 | 490 |
| **TOTAAL** | | | | | | 658 |

### 12.6.5 Storage Pool en Sizing

Initieel wordt de storage pool twee zo groot als de te beschermen data. De LUNs worden aangeboden als RAID5. Dit levert op alle vlakken voldoende bescherming. Zie bijgaande tabel.

| Disk Configuration | Capacity | Cost | Reliability | Performance and Scalability |
|---|---|---|---|---|
| **JBOD** | 4 | 4 | 1 | 4 |
| **RAID 0** | 4 | 4 | 1 | 4 |
| **RAID 1** | 1 | 1 | 4 | 3 |
| **RAID 5** | 3 | 3 | 3 | 3 |
| **RAID 10** | 1 | 1 | 4 | 4 |

Om de benodigde capaciteit te berekenen is gebruik gemaakt van de "System Center Data Protection Manager 2010 Storage Requirements Calculator For Hyper-V". Hierbij zijn de volgende waardes ingegeven.

| Onderwerp | Waarde |
|---|---|
| **Number of Hyper-V Nodes** | 6 |
| **Number of Cluster Shared Volumes (CSV) in a Cluster** | 4 |
| **Number of Virtual Machines (VMs) on each CSV** | 15 |
| **Average size of a Virtual machine** | 80 GB |
| **Average RAM allocated per virtual machine** | 4 GB |
| **Average expected churn in a day(% of file size)** | 10% |
| **Backup Frequency** | Dagelijks |
| **Retention Range (days)** | 7 |
| **Hardware Snapshot enabled?** | Ja |

Hieruit volgt de volgende configuratie.

| | |
|---|---|
| **Recommended Number of cores / DPM Server** | 8 |
| **Recommended RAM Configuration / DPM Server** | **18 GB** |
| **Server Architecture** | 64 bits |
| **Replica Volume Size** | 7200 TB |
| **Recovery Volume Size** | 3454 TB |
| **Total Storage per DPM Server** | **10,65 TB** |
| | |
| **Storage required for DPM install bits** | 1 GB |
| **Stoarge required for SQL install bits** | 2 GB |
| **Storage required for DPM Config DB** | 12 GB |
| **Storage required for DPM diagnostic log files** | 1 GB |
| **Recommended Page File size** | 43 GB |
| **Total Internal Disk Storage for DPM** | **59 GB** |

**Ontwerpbeslissing:**

- LUNs maximaal 1,5 TB.

Deze beslissing is gebaseerd op de volgende punten:

- Zie http://technet.microsoft.com/en-us/library/hh757941.

# Hoofdstuk 13 Antivirus

Voor de implementatie van Symantec Endpoint Protection 12.1 (SEP) wordt een centrale beheerserver ingericht vanwaar de SEP inrichting en de policies worden beheerd.

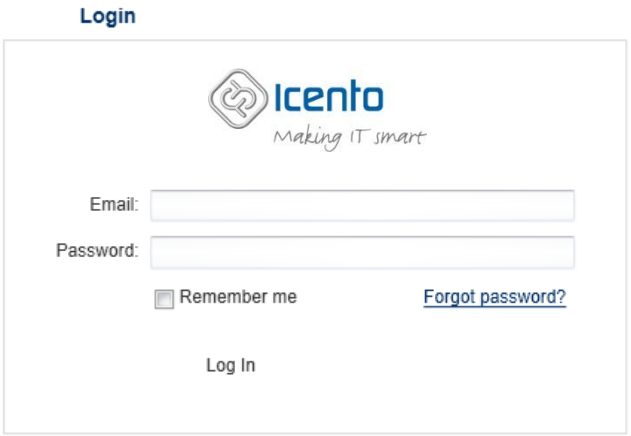
# Hoofdstuk 14 Delen van documenten

## 14.1 Sharepoint

SharePoint wordt als basis ingericht waarbij het logo van VNOG in SharePoint wordt geplaatst en tevens wordt er één Document Library aangemaakt om documenten te kunnen delen. Wanneer mensen documenten met elkaar willen delen dan kan dat door met een Active Directory account in te loggen. Vervolgens kan via het internet SharePoint benadert worden om documenten te delen. Wanneer een persoon een externe is en geen VNOG Active Directory account heeft dan moet VNOG een account aanmaken voor deze persoon en de credentials toesturen. Ook is het mogelijk om met algemene – functionele – externe accounts te werken.

## 14.2 Citrix File Share

Wanneer VNOG de wens heeft om externe gebruikers toegang te geven tot documenten met hun eigen (externe) e-mailadres – bijv. Gmail of Hotmail – dan kan VNOG Citrix File Share inzetten. Dit is een Public Cloud oplossing. VNOG is in control om externe toe te voegen met hun e-mailadres waarmee ze kunnen inloggen. Tevens kan VNOG zelf rechten toekennen per gebruiker. Voor Citrix File Share kan ook een VNOG logo gebruikt worden. Zie onderstaande afbeelding van de Icento Citrix File Share oplossing:




**Figuur 25 Citrix File Share**

Voor VNOG kan de URL dan zijn: https:/vnog.sharefile.com/