# WDS

## Welke 2 grote bestanden heb je nodig om een image van Windows 7, 8, 10 of Windows Server 2008, 2012 uit te kunnen rollen naar clients toe?

Install.wim = dit is een compressed file met daarin de OS image die je doorgeeft aan de client pc. Hiermee word dan de OS geinstalleerd op de client.

Boot.wim =

1) Boot images zijn images waarin je je client boot om je OS installatie uit te voeren.

2) Boot.wim installeert Windows PE. Dit is een klein OS dat Windows 10 installeert of deployt.

3) de Boot.wim versie moet gelijk of nieuwer zijn dan de versie van het install image.

Unattended.xml = dit is een antwoord file waarin alle aangepaste settings staan van een windows setup.

## Wat is het verschil tussen role based en feature based installation bij WDS?

Role based = een role is een service die de server aan anderen kunnen gebruiken. Bv dhcp: hier geeft de server ip addressen die de clients dan kunnen gebruiken.

Feature based = een feature die de server zelf gebruikt zoals bijvoorbeeld fail over clustering.

## Waarvoor dient de Transport server rol bij WDS?

De transport server role is een deel van de windows deployment service. Deze rol bevat enkel de core networking onderdelen. Deze dienen voor het voor het versturen van de data door gebruik te maken van multicasting op een stand-alone-server.

## Heb je altijd een dhcp server nodig om WDS te kunnen laten functioneren?

Ja, je hebt een DHCP server met een actieve scope op het netwerk nodig omdat Windows deployment service gebruikt maakt van PXE. PXE heeft een DHCP server nodig om te kunnen werken. Verder heeft WDS nog DNS, NTFS volume, een user die lid is van de lokale administrator groep op de server en de WDS-server moet lid zijn van een domein of zelf domein-controller zijn.

## Wat is PXE boot? Hoe functioneert dat?

PXE boot = Preboot Execution Environment of Pre-Execution Environment

Pxe is een manier om een computer op te starten zonder gebruik te maken van een harde schijf of een boot-diskette. De client haalt software van een computer af die daarvoor geconfigureerd is.

Ze maken gebruik van verschillende netwerkprotocollen:

-IP =internetprotocol word gebruikt om computernetwerken met elkaar te laten communiceren op netwerken, zoals het internet.

-UDP= User Datagram Protocol is het protocol dat snel gegevens door kan sturen maar niet de garantie kan bieden dat alles zal aankomen.

-DHCP Dynamic Host Configuration Protocol IP verkrijgen van de server.

-TFTP Trivial File Transfer Protocol: bestandsoverdracht protocol dat gebruikt wordt om een computer via een netwerk te laten starten.

Hoe?

1. De NIC van de client verstuurd een DHCP broadcast.
2. De DHCP server ontvangt de broadcast en antwoord met de standaard informatie zoals(IP, subnet mask, gateway, DNS,..) ook stuurt deze informatie over de locatie van de TFTP server en de boot image.
3. De client stuurt een PXE request naar de TFTPserver voor de boot image te krijgen.
4. De TFTP verstuurd de boot image en de client voert het uit.

## Wat is een image group? Heb je meerdere boot images nodig in WDS of kan je met één boot image alle andere besturingssystemen installeren? Hoe komt dat?

Een image group dient om op een overzichtelijke manier in de WDS de install.wim images te organiseren. Per image group wordt er ook een resources.wim aangemaakt, hierin worden alle resources die voor meerdere images hetzelfde zijn maar 1 keer opgeslagen. Al de verschillende images verwijzen dan naar de resource.wim file waardoor geheugen word uitgespaard.

WDS kan gebruikt worden met maar 1 enkele boot image, deze boot image moet recenter of even recent zijn dan de Windows dat je wil installeren.

Dit komt doordat de boot.wim file je de Windows PE omgeving geeft. Alle operating systems kunnen deze gebruiken zolang als de boot versie recenter of even recent is al de install.wim. Hierbij moet je wel een 32bit boot.wim gebruiken om beide 32 bit en 64 bit install.wim files te deployen. Moest je een 64bit boot.wim gebruiken kan je enkel 64bit install.wim files deployen.

<https://social.technet.microsoft.com/Forums/ie/en-US/ec32faf5-6488-4dcc-a3e6-dce284f200c7/wds-when-to-use-different-install-and-boot-images?forum=windowsserver2008r2general>

## Waarvoor dient unattend.xml? Wat kan je hierin allemaal configureren? Met welke tool heb je jouw unattend.xml gegenereerd?

Unattend.xml is een answer file, dit houdt in dat i deze file de settings worden bijgehouden die nodig zijn de setup van Windows. Hierin kan je configureren hoe disks gepartitioneerd moeten worden, de locatie waar de Windows image geïnstalleerd moet worden, de product key, toetsenbord, taal,…

Windows answer file generator

# Remote apps

## Wat is een streaming application? Op welke 2 manieren kan je deze streaming application aan de eindgebruiker aanbieden? Voor welke applicaties zou jij deze streaming application afraden en aanraden?

Wat?

Dit is een applicatie die wordt gestreamd vanaf een server. Taditioneel geïnstalleerde applicaties moet op elke client appart gemanaged en geüpdatet worden. App virtualisatie laat toe een administrator 1 instantie van de app te monitoren. Daarna word de app beschikbaar gesteld voor de clients. De server zend dan net genoeg informatie door naar de client zodat de applicatie kan starten. Daarna streamt de server de rest van de applicatie in de achtergrond terwijl de client werkt.

Hoe?

Via een group policy -> url van de rdweb in te geven bij remote app and desktop connections.

Daarna de policy toepassen op de user in het domein.

Via de webbrowser door de url van rdweb in te geven.

<https://www.youtube.com/watch?v=xwKK2qsVph4>

afraden/aanraden

afraden:

Voor grafische zware applicaties. Omdat alle pixels naar de client moeten worden gestuurd waardoor je veel bandbreedte gebruikt.

Voor bepaalde applicaties waarvoor er benodigde driverinstallaties zijn.

Aanraden:

Voor applicaties waarbij er belangrijke gegevens aan te pas komen. Als de lokale computer crashed dan gaan er geen belangerijke gegevens verloren omdat de app nooit geïnstalleerd was op de pc zelf

# WSUS

## Welke policies heb je nodig om Wsus te laten functioneren op een client? Zijn dat user policies of computer policies?

1. Configure automatic updating -> enablen -> auto download and notify for install
2. Specify intranet Microsoft update -> enable (pad+poortnummer)
3. Enable client side targeting -> dit zorgt ervoor dat de ou’s van de computer terecht komen in de overeenkomstige computergroups bij WSUS.

Dit zijn allemaal computer policies dat wil zeggen dat ze toegepast worden op de computer ongeacht welke user er inlogt.

## Kan je in WSUS automatisch alle updates doorsturen naar groepen? Hoe doe je dit?

Ja dit doe je door een computer toe te voegen aan een computer groep in WSUS en daarna voeg je de policies toe aan de computergroep

Configure automatic updating -> enable en pad + poortnummer

Specify intranet Microsoft update service location -> enable + pad + poortnummer

## Welke klassen van updates heb je binnen WSUS? Welke zou jij ALTIJD automatisch verdelen via WSUS? Raad jij ook aan om servers automatisch te laten updaten? Waarom wel/niet? Welke updates zou jij niet zomaar automatisch approven (denk aan grootte van update)?

1. Critical updates -> bugfixen zonder security relevantie
2. Security updates -> fixen van security vulnerability
3. Defnition updates -> updaten van virus definities
4. Update rollup -> meerdere hotfixes te samen
5. Service pack -> meerdere hotfixen maar voor een applicatie
6. Tool -> een feature dat een andere product helpt
7. Feature pack -> nieuwe product features
8. Update -> update voor een applicatie of file.
9. Upgrade -> upgrade voor een windows 10 feature of functionaliteit.
10. Drivers -> software componenten voor nieuwe hardware te ondersteunen.

Ik zou critical update, security updates en definitie update altijd automatisch laten verdelen via WSUS. De security en definitie updates om de security van de clients up to date houden en de critical updates voor de hotfix van verschillende office pakketten en betere performance van de client.

De server zou ik nooit automatisch laten updaten. Bij nieuwe updates zou de domein beheerder eerst moeten opzoeken wat de updates allemaal gaan veranderen en kijken of het nodig is om te updaten. Ook kan de domein beheerder kiezen wanneer hij de update gaat doen. Want nadat de updates geïnstalleerd zijn moet de server herstarten zodat de updates kunnen worden toegepast. Nu kan de domein beheerder er voor zorgen welke servers even uit liggen zodat de andere servers de rollen op zich kunnen nemen zodat het netwerk beschikbaard blijft.

De service packs en feature packs zou ik nooit automatisch laten doorvoeren omdat deze groot kunnen zijn waardoor er veel bandbreedte gebruikt kan worden. Ook moet er worden nagekeken of deze onderdelen en features ook wel nuttig zijn binnen het domein.

## Wat is de functie van WSUS in een domein? Welke voordelen heb je om WSUS in een domein te installeren en gebruiken?

WSUS zorgt ervoor dat systemen binnen een domein makkelijk en overzichtelijk kunnen worden bijgewerkt met de laatste updates.

de security van de systemen blijft up to date en het geeft garantie dat alles goed blijft functioneren.

Besparen van bandwidth doordat de clients de update van de centrale WSUS server halen en niet allemaal van het internet. Enkel 1 systeem haalt de update van het internet (WSUS server).

Je kan meerdere systemen in 1 klik laten updaten dan dat je alle systemen apart moest laten updaten.

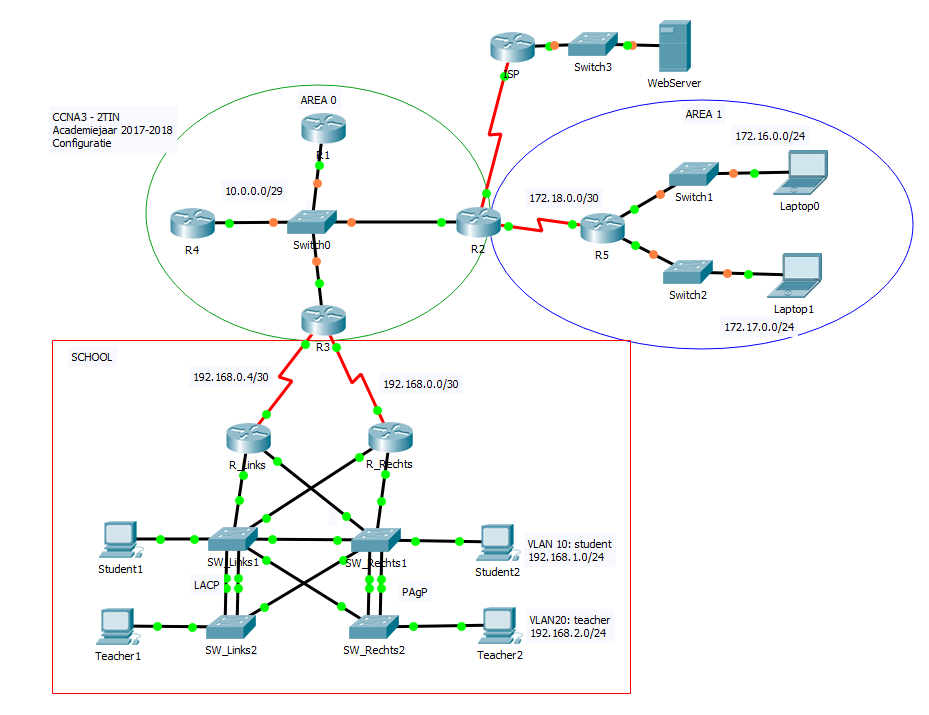
De domein beheerder kan kiezen welke update hij doorlaat en welke hij weigert. Hierdoor kan men gebugde updates makkelijk tegenhouden.

# Fail over clustering

Downtime = tijd dat een dienst niet meer functioneerd. (zeer kostelijk)

Redundancy = dienst of apparaat dat functie overneemt van een niet-functionerend apparaat.

Vb: UPS, fail over server, fail over blades

Single point of failure = 1 toestel dat een of service kan beperken.

Vb 1 router, 1 switch,..

Replication: gegevens op meerdere plaatsen continu synchroniseren met als doel redundancy te verkrijgen bij failure.

Vb ads,dns,namespace,replication group

Fail-over clustering: redundancy tussen 2 verschillende systemen om downtime te vermijden.

Cluster: verschillende systemen die 1 dezelfde service hosten.

Cluster bevat meerdere fysieke of virtuele servers of services waarbij 1 systeem online is

Node: 1 totaal systeem of service data autonoom kan opstarten. Een cluster bevat minimum 2 nodes die onafhankelijk functioneren. 1 node is actief, de andere node staat in fail-over modus (klaar om over te nemen bij falen van de actieve node)

Fail-over: het automatisch opstarten van een identieke backup serivce op een ander systeem na faling van het actieve systeem zonder manuele interventie, waarbij de gebruiker geen of weinig downtime ondervindt.

## Waarom cluster?

Cluster bied de garantie dat een service altijd online blijft zonder downtime. Dit is zeer belangrijk bij bv ziekenhuizen, datacenters, vliegtuigradars,…

## Vereisten cluster?

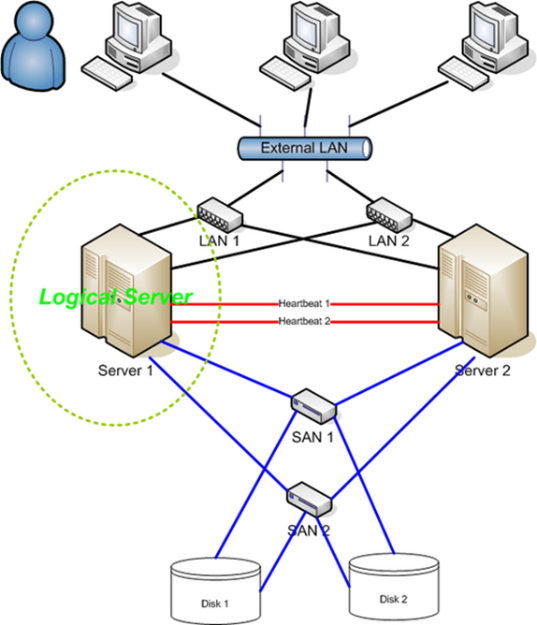
* Geen single point of failure (stroom, storage, network connecties)
* Meerdere onafhankelijke systemen met een heart beat netwerk en redundante netwerk verbindingen tussen storage, nodes en ISP.

Clustering als back up system?

Nee, De gewiste bestanden op 1 node worden ook verwijderd op de andere nodes.

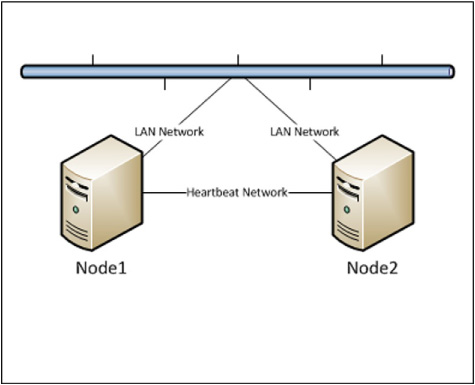
## Wat is een heart beat netwerk?

Heart beat netwerk is een privaat netwerk tussen 2 nodes dat test of de actieve ode nog functioneert en eventueel het fail-over commando doorstuurt. Het netwerk is volledig gescheiden van lan of san netwerk. Ook kan er gebruik gemaakt worden om false fail-over te voorkomen.



## Wat is false fail-over?

Wanneer de heartbeat link kapot is gegaan zal de 2de node denken dat de eerste node is uitgevallen. Deze node wilt dan de 1ste node overnemen maar doordaat enkel de verbinding is kapot gegaan en niet de eerste node zullen er nu 2 nodes tegelijkertijd dezelfde service draaien.



# Back up

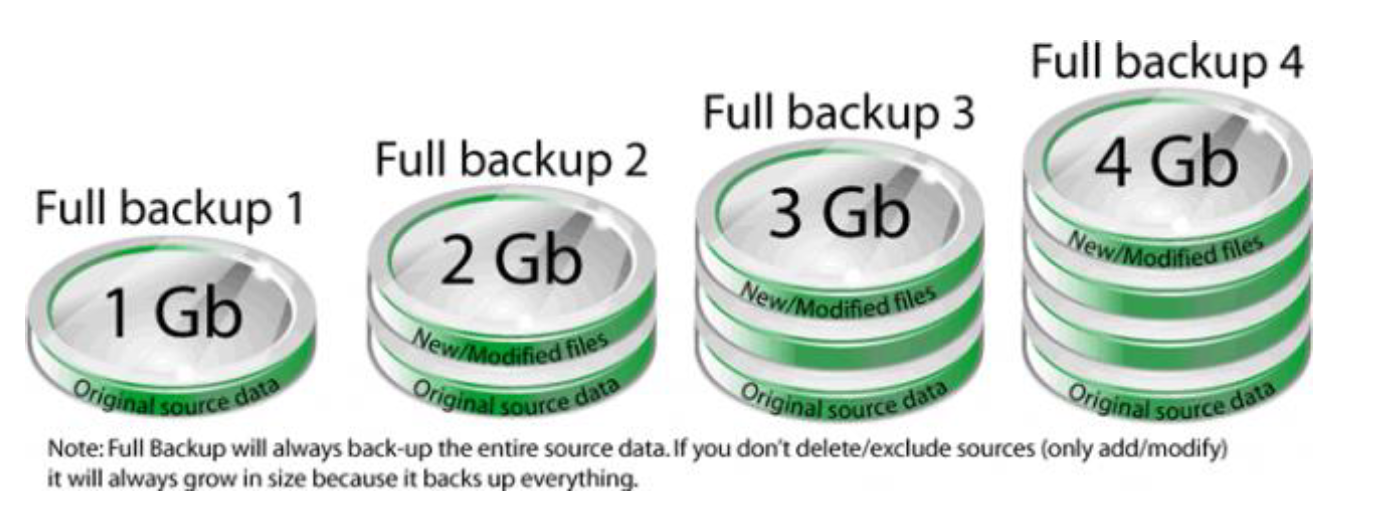
## Wat is een back up?

Een back up is een kopie van gegevens die zich op een gegevensdrager of binnen een applicatie bevinden om deze te kunnen herstellen mochten ze beschadigd raken.

Korte termijn 🡪 harde schijven

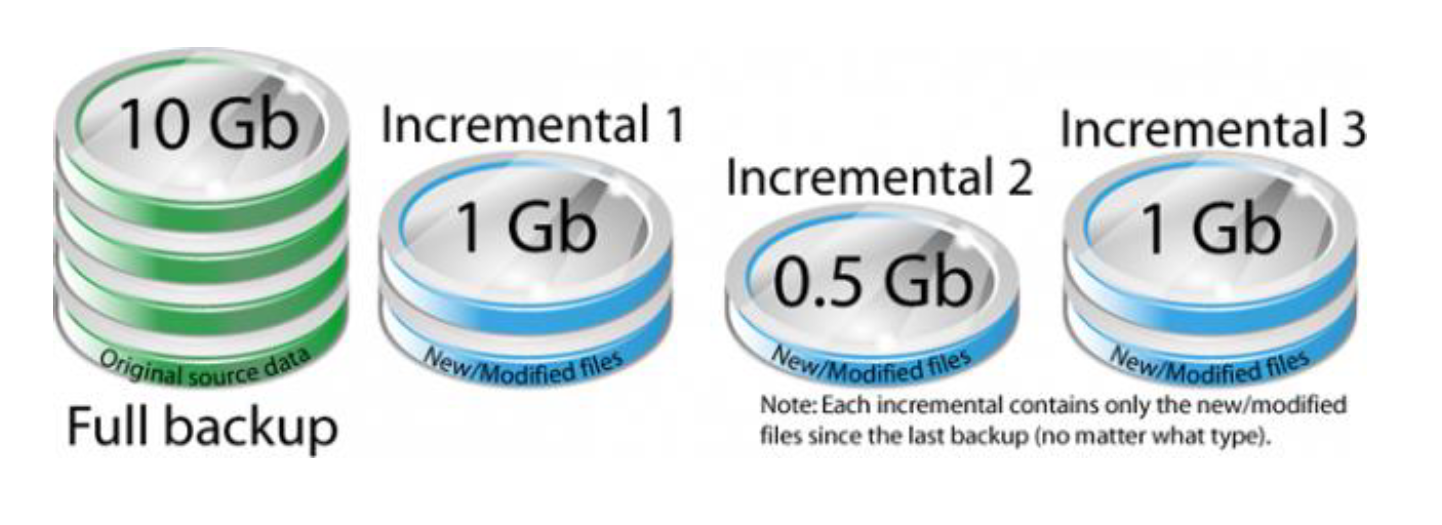
Lange termijn 🡪cartridges

## Full backup



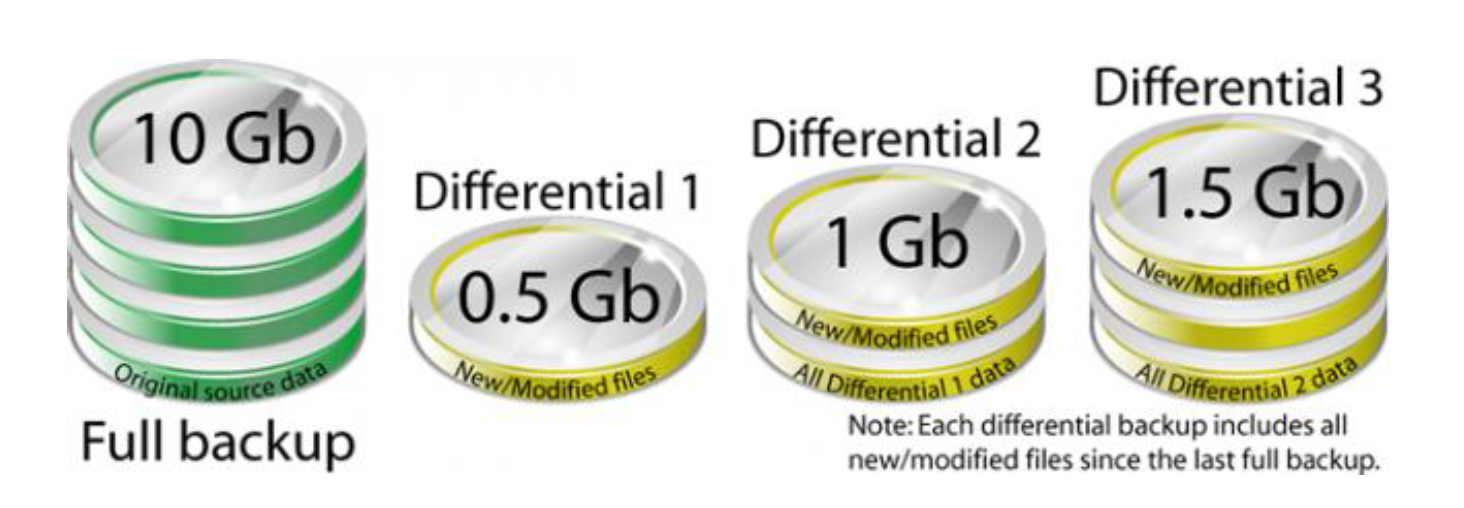
Slaat iedere keer het volledige bestand op. Nadeel veel geheugen.

## Incremental back up



Slaat elke keer enkel de bestanden die je heb bewerkt op. Nadeel als incremental 2 corrupt is dan moet je terug opnieuw beginnen bij incremental 1

## Differential backup



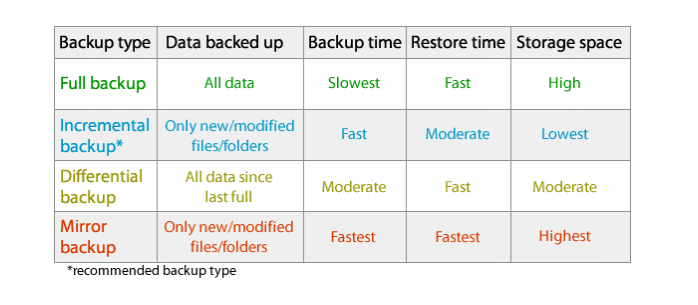
Slaat 1 grote back up met daarna telkens alle updates samen te voegen.

## Mirror backup

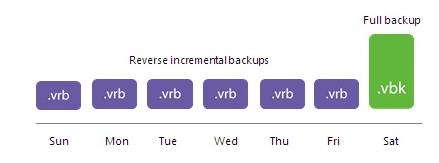


Mirror image compressed het vorige en voegt er dan de nieuwe files bij toe.

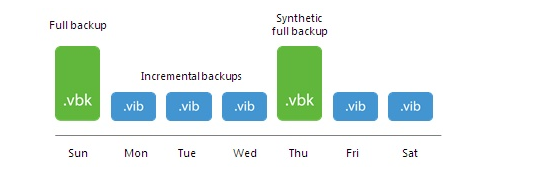
## Voor nadelen



## Reverse incremental backup



## Forward incremental backup



# Monitoring

Waarom monitoring?

* Zekerheid dat alle applicaties en servers up en running zijn
* Voorkomen van mogelijke problemen op voorhand
* Opvolging van gemiste problemen

# Virtualizatie

## Wat is virtualizatie?

Virtualizatie is 1 computer de job laten doen van meerdere computers door het delen van de hardware over meerdere omgevingen

## Geschiedenis server concept?(virtualizatie)welke voordelen zijn er bij het nieuwe model?

Bij de traditionele systemen kocht men hardware aan voor een server te bouwen. Op deze server draaide een OS en daarop draaide dan verschillende services/applications.

Oude model voordelen/nadelen

* 1 OS per machine
* Software and hardware moesten afgestemd zijn.
* Meerdere applicaties/services zorgde voor conflicten.

Bij de nieuwe systemen kocht men hardware aan voor een server te bouwen. Op deze server draait dan een hypervisor. Hierop draaien dan meerdere OS’en en op die OS’en draaien dan verschillende services/applications

Nieuw model voordelen/nadelen

* Hardware onafhankelijk🡪 het maakt niet uit op welke hardware de VM draait want de hardware die de VM gebruikt wordt gevirtualiseerd als ook de drivers.
* Elke VM is geïsoleerd 🡪 elke VM word in een apart hokje gestoken. Hierdoor werken ze individueel als VM op een host systeem. Moest 1 van de VM’s corrupt geraken beinvloed dit de andere VM’s niet.
* Encapsulatie🡪 een hele VM kan in een file gestoken worden door behulp van encapsulation.

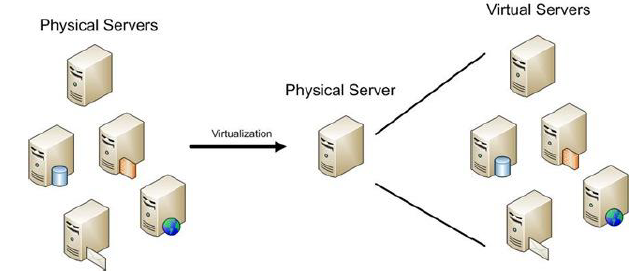
## Voordelen virtualizatie

* Optimaal hardware gebruik

Doordat er meerdere VM servers kunnen laten draaien met meerdere rollen op de server kunnen we 1 hardware optimaler gebruiken. Vroeger waren er servers zoals DHCP servers die maar 4% gebruikte van zijn hardware.

* Server consolidatie

Meerdere services op 1 server laten draaien.



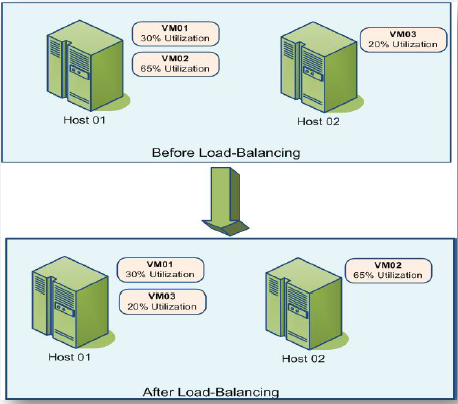
* Lagere provisioning time

Provisioning is het klaarmaken van server om applicaties te kunnen runnen. Services voorzien bv het installeren van een .net framework

De provisioning time bij virtualisatie is verlaagt omdat men met templates van cleane servers kan werken.

* Load balancing

men kan gemakkelijk load balancen met virtuele machines omdat de machines niet afhankelijk zijn van hun hardware. Men kan de hoge hardware gebruikende machines apart zetten zodat in de piek momenten de servers niet gaan crashen.



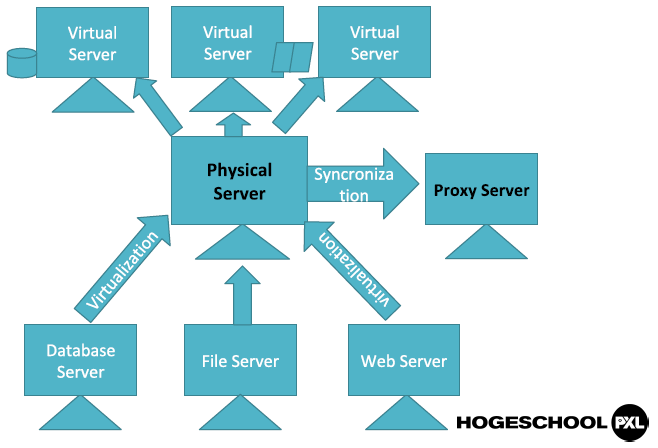
## Nadelen virtualizatie

### Physical to virtual

De conversie van een bestaande fysieke machine naar een virtuele machine.(os ,setting, data)

### Physical failures become “serious”

Als de fysieke server uitvalt en de data corrupt word, dan zijt ge alles kwijt. #openstackserver #critical-kernel fout #wegermee



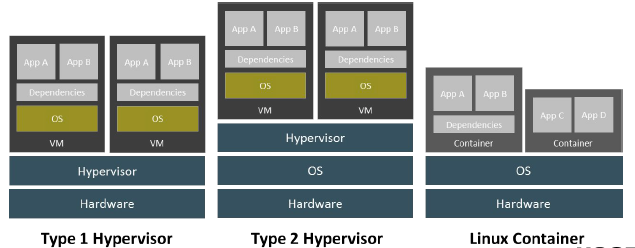
## Hoe kies je welke hypervisor je nodig hebt?

Je moet kijken wat uw hardware support, wat de vendor support is en kijken welke appliccaties en apparatuur specefiek op een platform moeten draaien.

# Docker

## Containers

Containers zijn lichter voor op een server te draaien. Binnen in docker gaan de container de host OS kernel en root filesystem sharen wanneer het mogelijk is.



Docker maakt gebruik van ‘libcontainer’ technologie

## What is docker?

Docker is een container technology waarmee je een applicatie in een package gaat steken en daar een lightweight removable image van te maken. Die image kan je dan steken in container. Die container ga je dan runnen met lxc/, libvirt/, libcontainer/,…

Bv webservers, fileservers,…

## Docker security

Intrinsic security of containers

* Kernel namespaces

De namespace isoleert de applicatie zijn zicht van zijn runnende omgeving. Dit betekent dat een process draaiend in 1 container niet een andere process in een andere container kan zien of aanraken. (isolatie van een virtuele machine)

* Control Groups

Control groups verzekeren dat elke container zijn deel van de ram/cpu krijgt. Dus 1 container kan het hele systeem niet omzeep krijgen door alle cpu power af te pakken van alle andere containers. Dit kan handig zijn bij DDOS aanvallen.

Security of docker daemon

* Door de root users van een container te mappen met een niet-root user van je docker daemon. Moest een hacker aan de root privileges van een container komen. Kan hij enkel die container om zeep krijgen en niet alle andere.
* De docker daemon laten runnen zonder root privileges en het delegeren van die operaties met die privileges naar goed inde gaten gehouden processen.

## Voordelen docker

Portability over machines

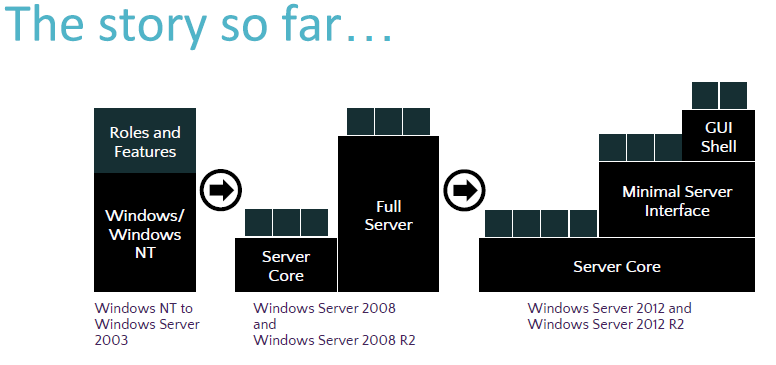
* Men kan gebruik maken van dezelfde container over meerdere container-based omgevingen.
* Live migration: men kan de container verplaatsen naar een andere server zonder downtime.

Isoleren van de service of applicatie

Copy-on-write mechanics

* Alle containers maken gebruik van dezelfde files. Als 1 van deze containers een aanpassing maakt in deze files dan word er een kopie gemaakt van die files met de aanpassing.

## Windows server 2016



Servercore = zonder GUI

* Minder CPU usage
* Minder ruimte voor OS te runnen
* Nadeel alles in CLI/powershell

## Nano server?

Nano server is een klein operating systeem gebaseerd op windows server 2016. Dit OS voor het gebruik van de host OS layer voor container virtualizatie.

# Cloud computing

## Service models

### SaaS

(voor normale consument)

Gehoste apps die enkel toegankelijk zijn via het internet

Providers: XBOX live, gmail, google docs, office 365

### Paas

(voor developers)

Gehoste development platform voor het deployen van SaaS apps. ,(applicatie server, webservers,…)

Providers: windows azure, google app engine, apache stratos,..

### IaaS

(voor IT departement)

Huren van IT infrastructuur. (servers)

Leveren van servers in een makkelijk te gebruiken manier. De consument moet zich niets meer aantrekken van networking, hard drives, processoren, geheugen,…

Men kan gewoon een remote desktop connectie maken naar de server en beginnen met het installeren van de software op de machines.

Providers: amazon AWS, cegeka, microsoft azure

(de mottige openstack servers van de pxl alleen dat die bij pxl stond)