# Hoe zet u virtualisatie slim in bij forensische onderzoeksomgevingen?

ir. Ronald van Vugt
ronald@netwell.eu

# Aanleiding

- Deze presentatie is ontstaan naar aanleiding van een nieuw architectuur ontwerp voor een nieuwe forensische onderzoeksomgeving voor een opsporingsdienst
- Dit ontwerp is uiteindelijk in een PoC gebouwd en getest
- Data Expert was hier betrokken en zo is het contact ontstaan

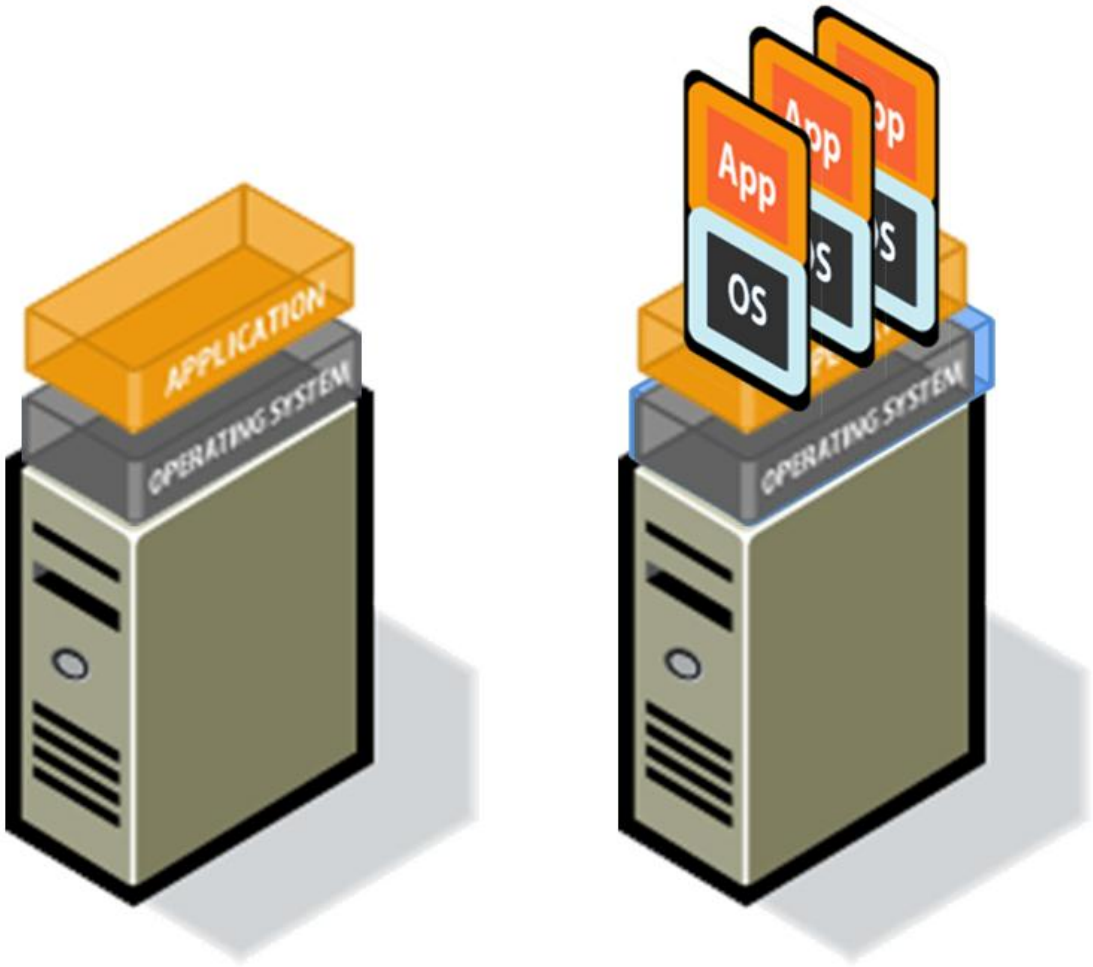
# Agenda

- Wat is virtualisatie?
- Opbouw forensische onderzoeks omgeving
- Slim gebruik van virtualisatie

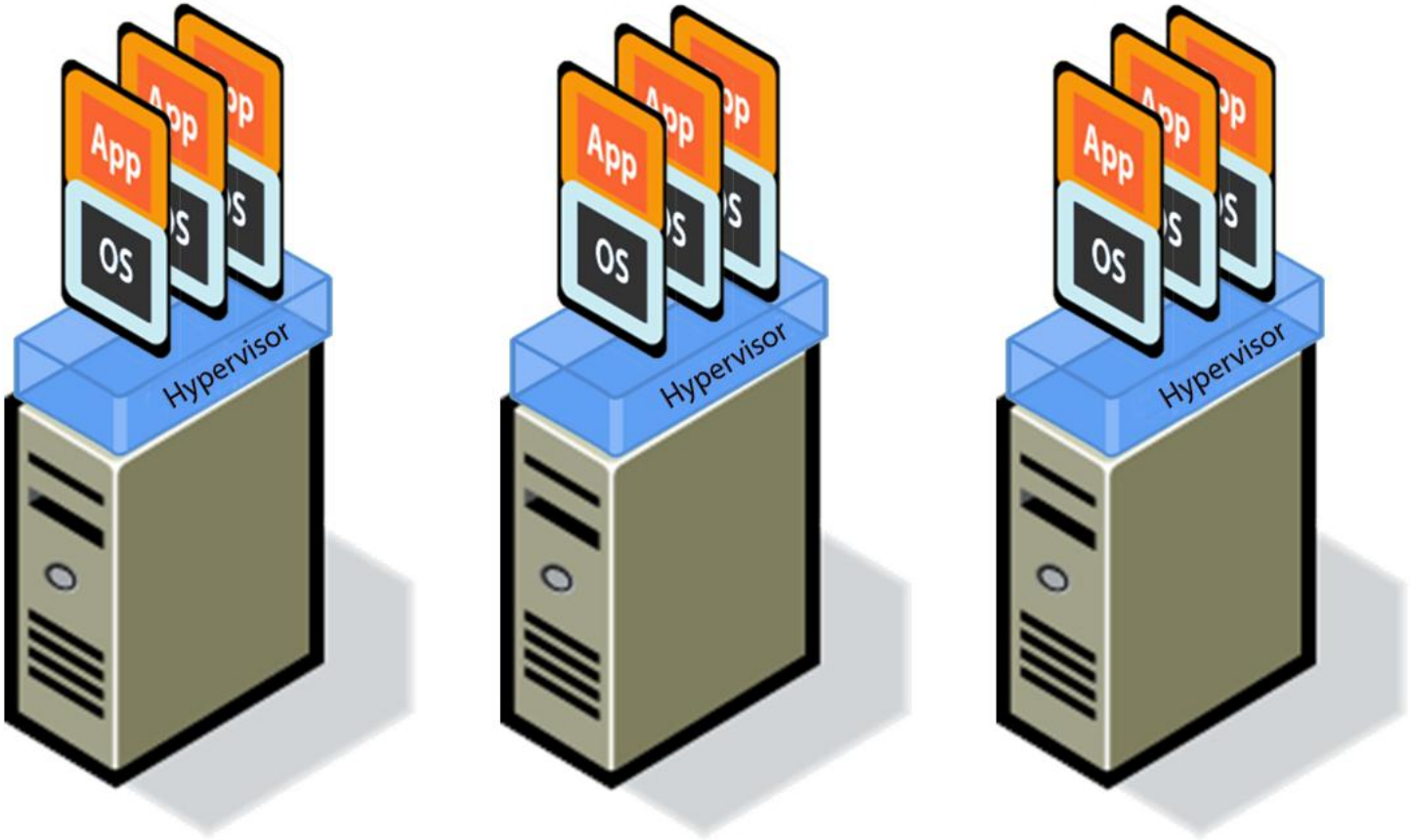
# Vormen van Virtualisatie

- Server
- Desktop
- Applicatie virtualisatie
  - Streaming van applicaties
  - Terminal server
- Tientallen andere vormen
  - Storage virtualisatie, netwerk virtualisatie, etc.

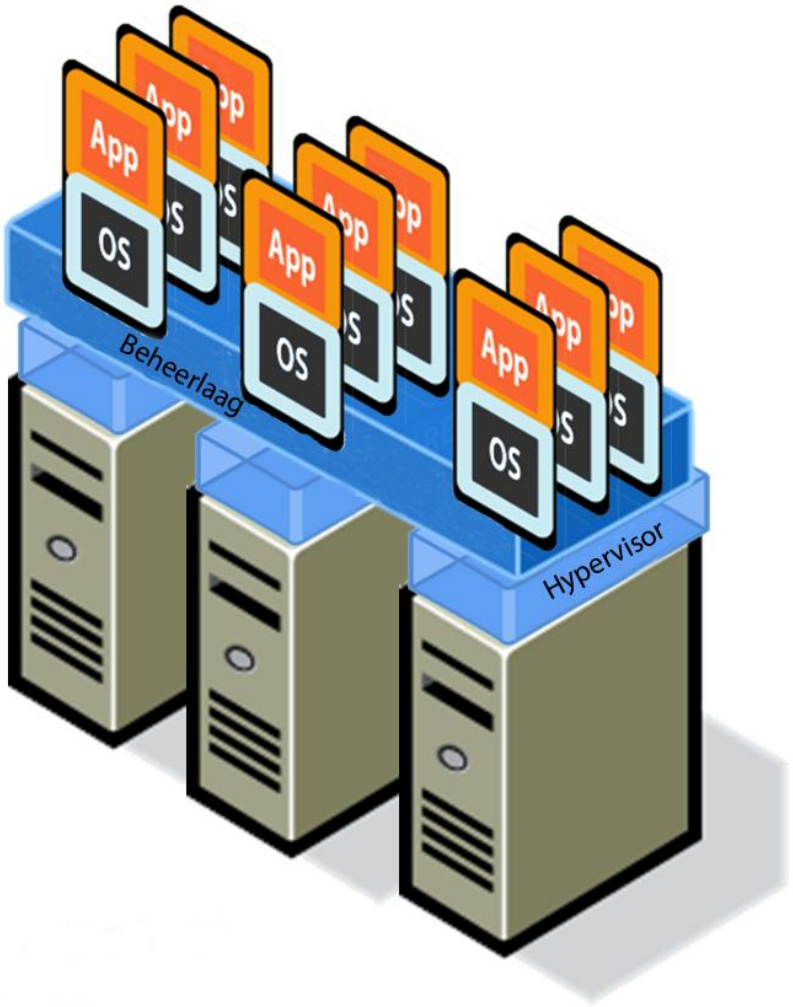
# Wat is virtualisatie?



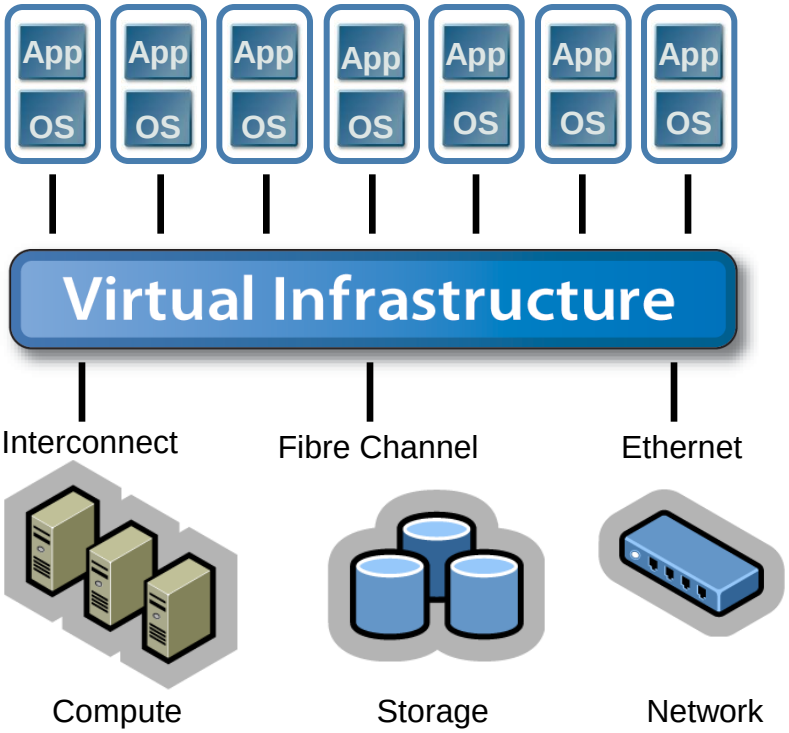
# Wat is virtualisatie?



# Wat is virtualisatie?



# Wat is virtualisatie?



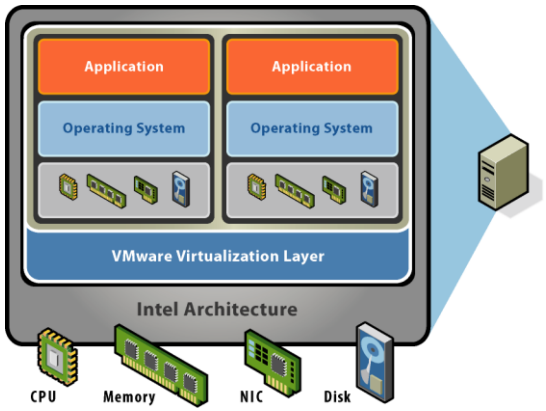

Bij server virtualisatie is er een pool van resources beschikbaar die:

- extreem flexibel inzetbaar is
- waarbij resources inzetbaar zijn afhankelijk van de behoefte

Zonder server virtualisatie is er een pool van resources die inflexibel gekoppeld zijn aan een stukje behoefte

# Wat is virtualisatie?

## Partitioning

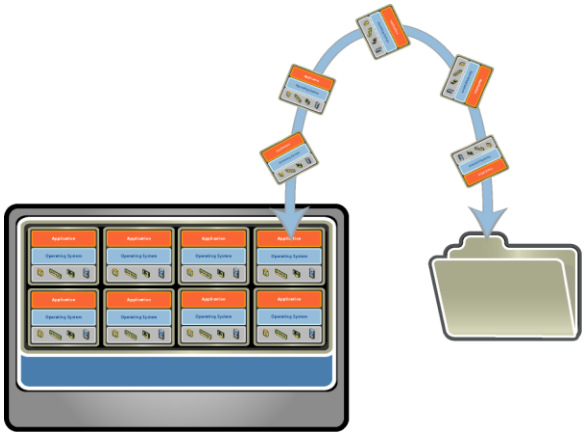



- Draai meerdere OS'en op één fysieke server
- Volledig gebruik van de server resources
- Applicatie is cluster-ready voor failover en redundancy, ook als de applicatie zelf niet cluster-ready is

## Isolation

- Afscherming op hardware niveau
- Controle over CPU, geheugen, disk en netwerk resources per Virtuele Server
- Gegarandeerde service levels

## Encapsulation

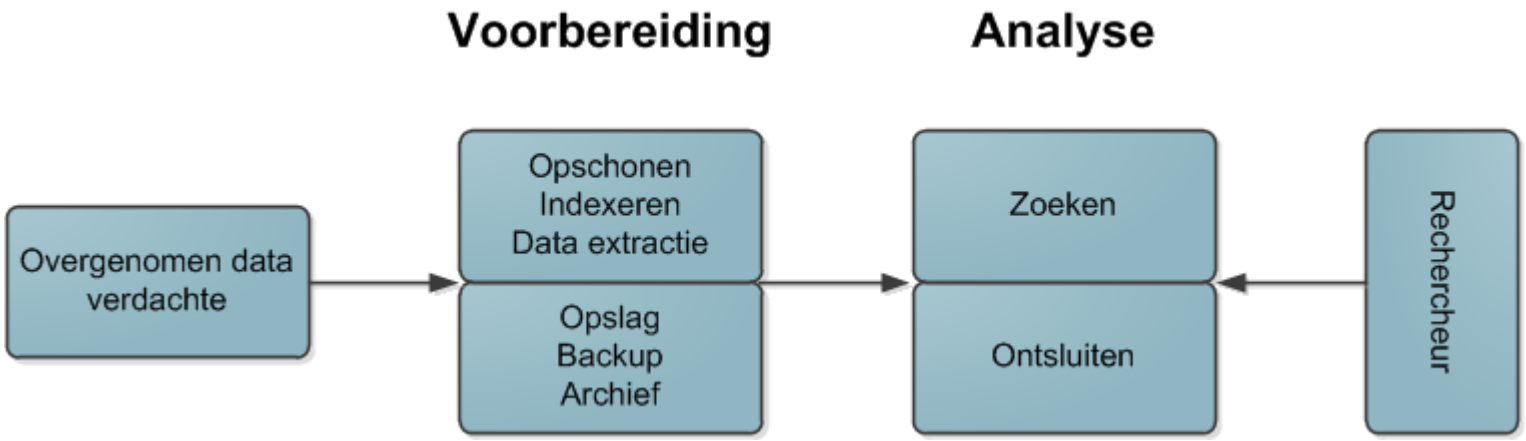


- Volledige state van de VM is encapsulated: geheugen, disk images, I/O status
- VM state kan worden opgeslagen in een file – checkpointing, "Suspend / Resume"
- Een VM kan eenvoudig gerepliceerd of hergebruikt worden door een file-copy

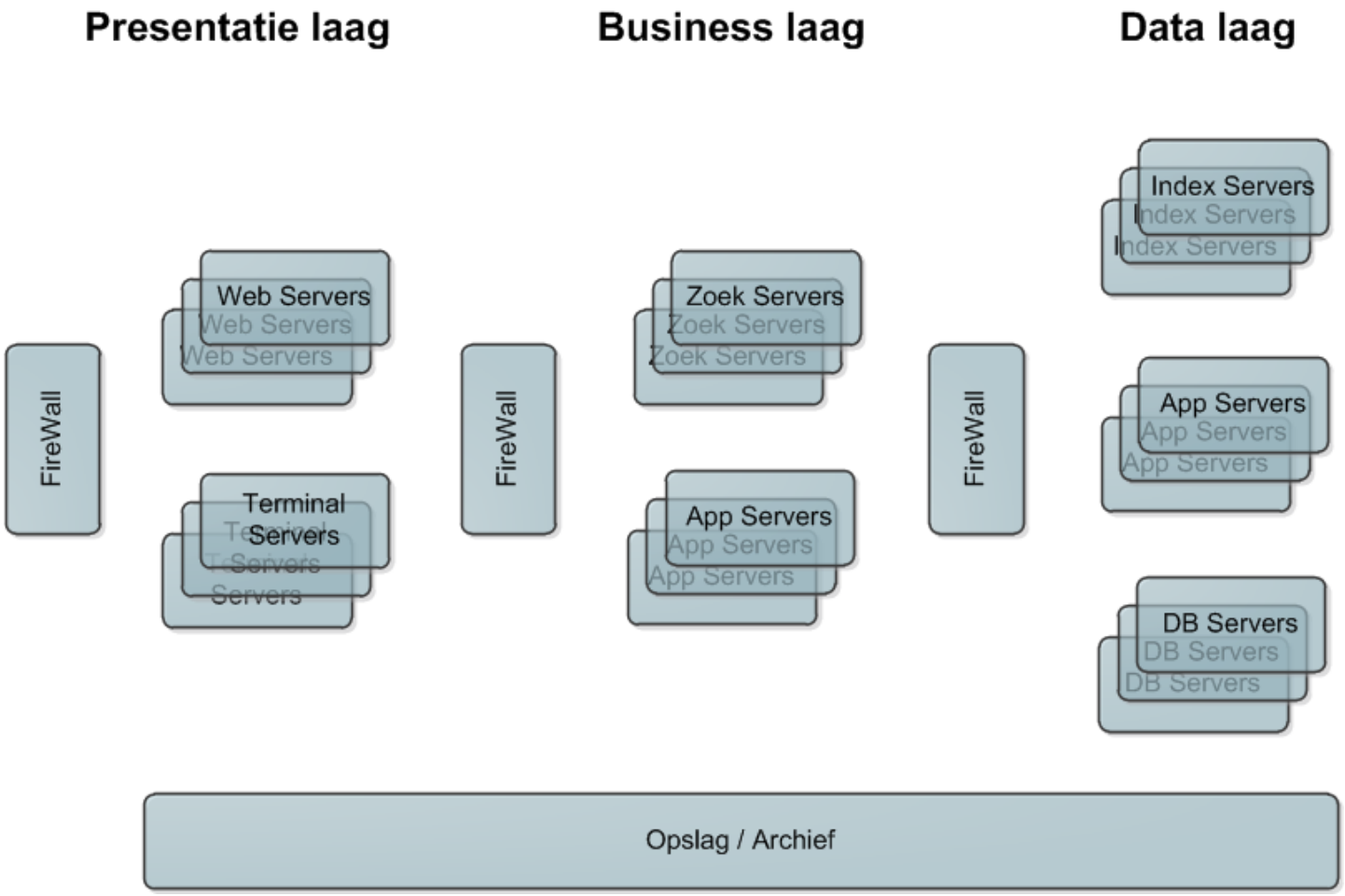
# Welke voordelen biedt dit?

- Zeer snelle uitrol servers
- 100% gelijke productie en testomgevingen
- Eenvoudige rollback
- Hardware onafhankelijk
- Heel eenvoudig backups maken van volledige operationele servers
- Uitwijk relatief eenvoudig
- Automatische beschikbaarheid

# Forensische tools



# Globale architectuur



# Slim gebruik virtualisatie

- Huidige processoren bieden heel veel capaciteit en veel cores per CPU
- Huidige processoren zijn geoptimaliseerd voor virtualisatie
- Geheugen is geen echte beperking meer
- Windows is niet echt geschikt voor scale-up, maar veel meer voor scale-out

# Slim gebruik virtualisatie

- Wat is nodig voor een tool:
  - Schaalbaarheid: naar behoefte moeten er index, zoek en applicatie servers bij- en afgeschakeld kunnen worden
  - Zeer efficiënte opslag en geen dubbele opslag
  - Bevriezen originele dataset
  - Maximale beschikbaarheid
  - Uniforme en schaalbare ontsluiting
  - Logische netwerk scheiding

# Slim gebruik virtualisatie

- Schaalbaarheid:
  - Virtualisatie zorgt voor een ‘one-click’ deployment in minuten
  - Virtualisatie zorgt voor een optimaal gebruik van de fysieke servers, waardoor veel minder fysieke servers nodig zijn
  - Schaalbaar kan ook gevonden worden in Cloud Technologieën om tijdelijk extra capaciteit beschikbaar te krijgen

# Slim gebruik virtualisatie

- Opslag:
  - Door middel van snapshot technologie mogelijkheid om meerdere subsets van datasets te maken en de originele dataset onaangetast te laten
  - Door middel van Thin Disks technologie exact fysiek opslaan wat nodig is, zonder ‘slack’

# Slim gebruik virtualisatie

- Beschikbaarheid:
  - Automatisch herstart virtuele servers op andere fysieke server bij uitval van een fysieke server (maar met downtime en mogelijk gegevensverlies en inconsistentie)
  - Er zijn geavanceerde technieken beschikbaar waarbij er parallel een virtuele server meedraait en die operationeel wordt bij een disaster zonder downtime, gegevensverlies en geen risico inconsistentie

# Slim gebruik virtualisatie

- Ontsluiting:
  - Terminal Server oplossingen draaien gevirtualiseerd veel efficiënter, dat wil zeggen meer concurrent gebruikers per fysieke server door het draaien van meerdere virtuele terminal server servers per fysieke server
  - Als Terminal Server oplossingen niet mogelijk is, gebruik van VDI oplossingen om elke onderzoeker een eigen virtuele desktop te geven

# Slim gebruik virtualisatie

- Logische netwerkscheiding:
  - Virtualisatie biedt de mogelijkheid om virtuele netwerken aan te maken
  - Hierdoor kan op netwerk niveau geregeld worden dat iemand alleen toegang heeft tot de juiste servers
  - Dit biedt ook mogelijkheden om verschillende partijen gebruik te laten maken van dezelfde onderzoeksomgeving

# Vragen