Generieke gemeentelijke Infrastructuur modellen

&

Naar de Cloud

LOOK BEYOND

Over mijzelf

- 10+ jaar ervaring als infrastructuur / cloud architect
- CCSP (cloud security) gecertificeerd
- Ervaring binnen overheid:
  - Gemeente Utrecht (project Ucloud)
  - Ministerie van Veiligheid en Justitie
  - Provincie Overijssel, Utrecht en Drenthe
  - Nu: Gemeente Haarlemmermeer

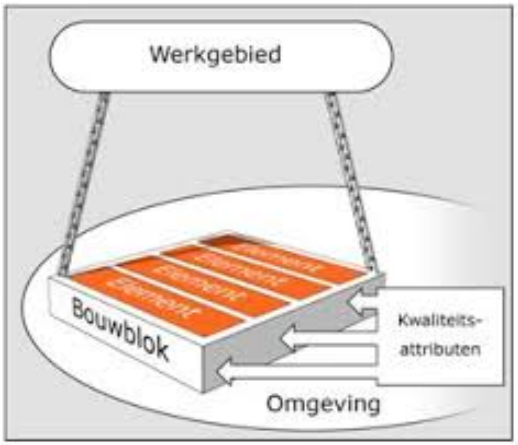
LOOK BEYOND

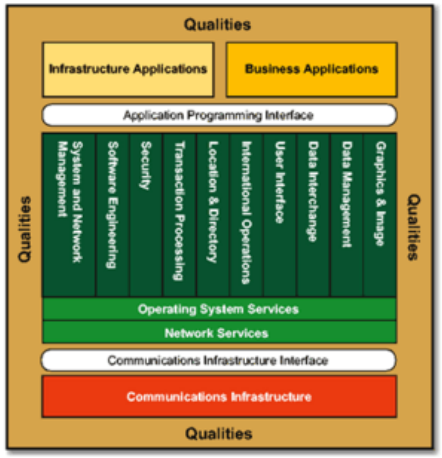
Onderwerpen

- Infrastructuurmodellen
- Patronen
- Infrastructuurmodellen
- Infrastructuurontwikkelingen
- Cloud computing
- Wat kan Collectief?
- Aanpak Cloud Haarlemmermeer

LOOK BEYOND

Bestaande infrastructuur modellen





OIAr :

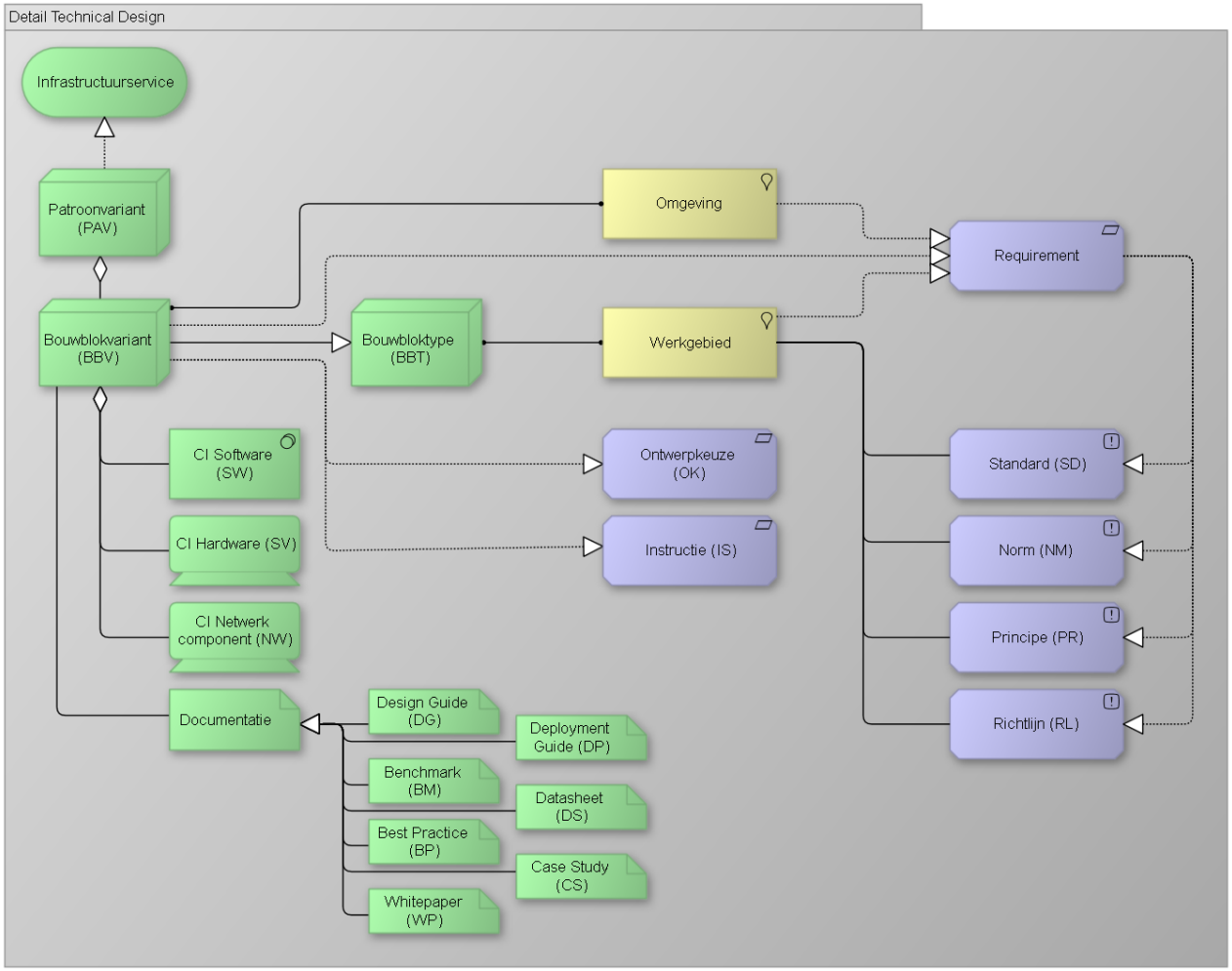
- Generieke infra patronen
- Infrastructuur functionaliteit

TOGAF III-RM :

- Beschrijving componenten
- Relaties tussen componenten

LOOK BEYOND

Metamodel op basis van OIAm



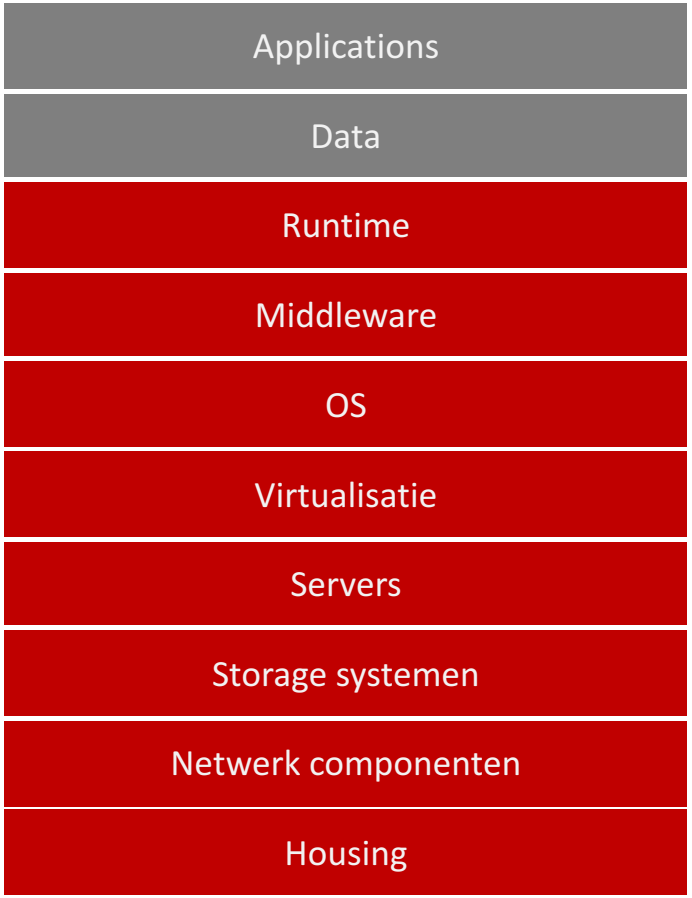
LOOK BEYOND

Waar bestaat het generiek referentiemodel voor technische infrastructuur uit?

- 33 werkgebieden
- 220 generieke bouwblokken
- Generieke bouwblokken voorzien van Wikipedia definitie
- (open) Standaarden gekoppeld aan werkgebieden
- BIG-normen gekoppeld aan werkgebieden

LOOK BEYOND

Wat beschouwen we tot technische infrastructuur?



LOOK BEYOND

33 werkgebieden en 220 Bouwblokken

Security Information and Event Management
Alerting
Compliance
Correlation
Dashboards
Data Aggregation
Forensic Analysis
Retention

Application Integration
Enterprise Service Bus
File transport
Layer 7 Switching
Message Oriented Middleware
Message Passing
Message Queuing
Web Services

Virtual Desktop Infrastructure
Connection Broker
Desktop Pool Provisioning
Pool Management
User Entitlement
Virtual Desktop
Virtual Printing

Backup & Restore
Continuous Data protection
On-line Back-up
Off-line Backup
Near-line Backup
Snapshot Backup

Configuration Management
Hardware Inventory
Software Inventory
License Manager
Asset Management

Device Management
Thin Client Management
Mobile Device Management

Collaboration
Content Repository
Web Content Management
Mail client access
Mail Transport
Instant Messaging

Server Based Computing
Remote Applications
Remote Desktop Connection
Remote Desktop Gateway
Terminal Server

Zone Protection
Anti Malware Inspection
DDoS Mitigation
Data Leakage Prevention
Deep Packet Inspection
Firewalling
Intrusion Detection
Intrusion Prevention
Network Access Control List
Network Address Translation
URL Filtering
Virtual Private Networking
Virus scanning
Anti Spam

Client Realm
Mobile Phone
Smart Phone
Tablet
Laptop
Thin-client
Personal Computer

Multi media
Streaming Media

Application Distribution
Application Store
Self Service Portal
Application Packaging
Application Streaming
Automated Application Installation
Application Deployment
Application Virtualization

Networking
Fiber Channel over Ethernet
Host Configuration
IP Address Management
LAN Switching
Link Aggregation
Link-State Routing
Multi Layer Switching OSI 3/4
Name Resolution
Network Access Control
Network Time Services
Power over Ethernet
Routing
Traffic Shaping
Virtual Extensible LAN
Virtual Routing & Forwarding
WAN
WAN Optimization
Wireless LAN

Mobile Application Management
App Wrapping
Mobile Application Store
Secure Workspace

Transaction Processing
Transaction Processing - System

Data warehousing
Extract Transform & Load
Operational Data Store
Data Mining
Online Analytical Processing

Server Computing
Blade Enclosure
Blade Server
Dynamic Resource Allocation
Hypervisor
I/O Virtualization
Physical Server
VM High Availability
VM Live Migration
Virtual Chargeback
Virtual Server

Data Center Infrastructure Management
Capacity Planning
Deployment
Energy Efficiency
Management Packs
Patch Management
Remote Administration
Run book Automation

Peripherals
Barcode Reader
Computer Display
Computer Mouse
Graphic Tablet
Image Scanner
Keyboard
LCD projector
Network Printer
Touch screen
USB Flash Drive
Webcam

Database Management
RDBMS
Data Security
Database Activity Monitoring

Application Processing
Application Server
Web Content Server

Storage
Data Compression
Data De-duplication
Direct Attached Storage
Disk Storage Replication
Distributed File System
Flash Hypervisor
Flash Storage
Hard Drive
Logical Unit
Network Attached Storage
Network File System
Optical Storage
Solid State Storage
Storage Area Network

Network Management
Out-of-band Management
Network Analysis
Bandwidth Management
Traffic Analysis
Network Automation
Quality of Service

Fabric based Infrastructure (convergence)
IP Address Automation
Orchestration
Server Provisioning
Storage Naming
Hybrid Cloud Enabling

Workspace Management
Profile Management
Context Awareness
Dynamic Printer Mngt

Document Management
Check-in / out
Versioning
Document Search
Metadata Management

Physical
Air
Cables
Cell Site
Equipment Room
Fiber Optics
Furniture
Power
Rack
Uninterruptible Power Supply

Application Delivery Networking
Web application Firewall
Reverse proxy
Application Acceleration
Web Application Portal
Connection Multiplexing
Data Compression
Data Caching
Internet Connection Sharing
Web Application Portal
L4 Load Balancing
L7 Load Balancing
PCoIP Proxy
SSL Acceleration
SSL Termination Proxy
TCP Optimization
Content filtering
SMTP Proxy

Printing
Follow me printing
Print spooler

Digital Archiving
Record Management
Document Archive
Mail Archiving

Telephony
Base Station Subsystem
Call Logging
Call Management
Call Tracking
PBX
PSTN
Private GSM
SIP trunking
Session Border Controller
Voice over IP

Operating System
Device Drivers
Mobile Device OS
PC OS
Server OS
Thin-client OS

Vulnerability Management
Vulnerability Intelligence
Vulnerability Scanner

LOOK BEYOND

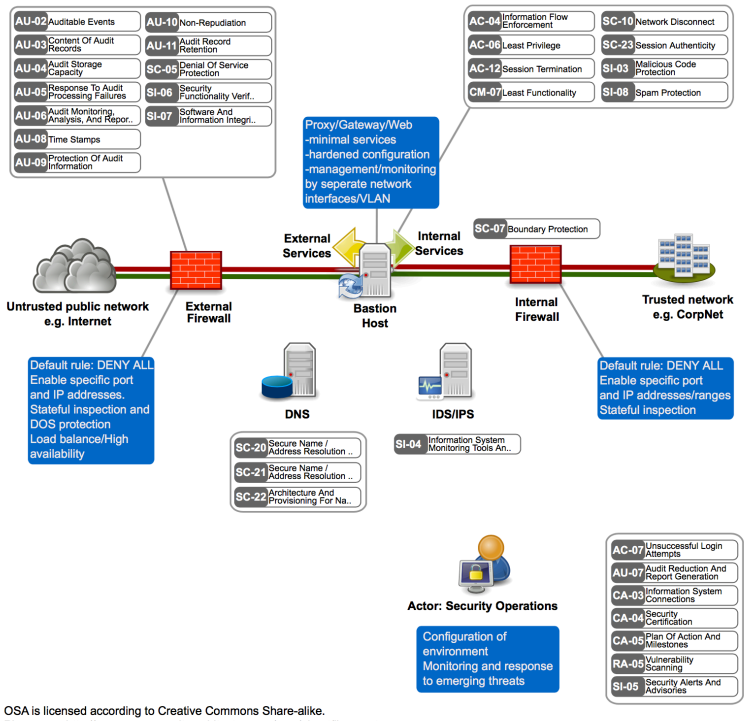
Herbruikbare infrastructuur patronen

- Zijn er voorbeelden
- Zelf ontwikkelen?
- Welke modelleertaal?

Voorbeelden

SP-016: DMZ Module

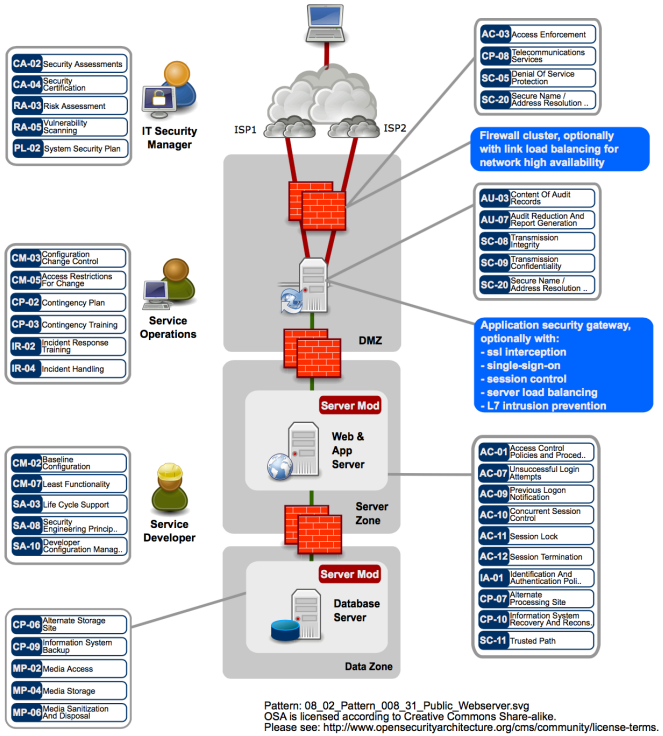
Diagram:



OSA is licensed according to Creative Commons Share-alike.
Please see:http://www.opensecurityarchitecture.org/cms/about/license-terms.

SP-008: Public Web Server Pattern

Diagram:

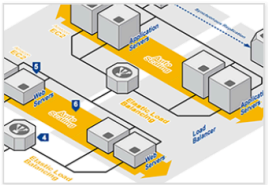


Pattern: 08_02_Pattern_008_31_Public_Webserver.svg
OSA is licensed according to Creative Commons Share-alike.
Please see: http://www.opensecurityarchitecture.org/cms/community/license-terms.

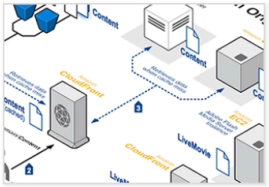
Voorbeelden

AWS Reference Architectures

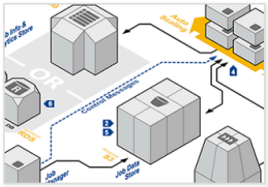
The flexibility of AWS allows you to design your application architectures the way you like. AWS Reference Architecture Datasheets provide you with the architectural guidance you need in order to build an application that takes full advantage of the AWS cloud infrastructure. Each datasheet includes a visual representation of the application architecture and basic description of how each service is used.



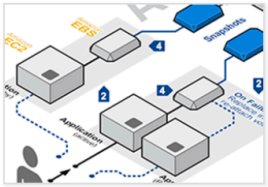
Web Application Hosting
Build highly-scalable and reliable web or mobile-web applications (PDF)



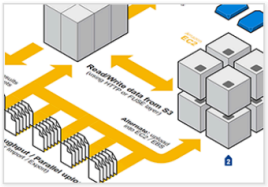
Content and Media Serving
Build highly reliable systems that serve massive amounts of content and media (PDF)



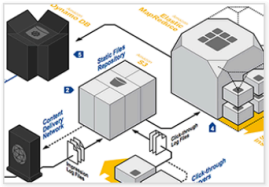
Batch Processing
Build auto-scalable batch processing systems like video processing pipelines (PDF)



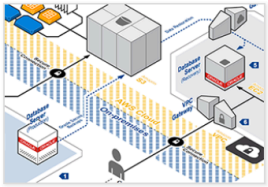
Fault tolerance and High Availability
Build systems that quickly failover to new instances in an event of failure (PDF)



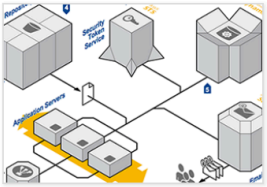
Large Scale Processing and Huge Data sets
Build high-performance computing systems that involve Big Data (PDF)



Ad Serving
Build highly-scalable online ad serving solutions (PDF)



Disaster Recovery for Local Applications
Build cost-effective Disaster Recovery solutions for on-premises applications (PDF)



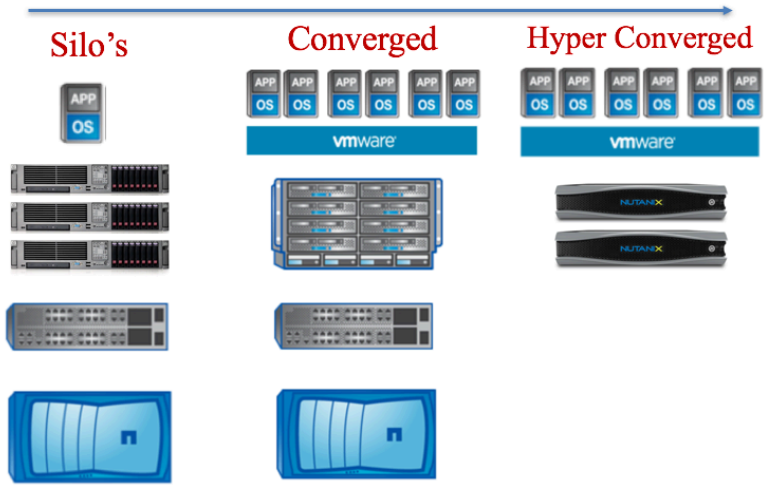
File Synchronization
Build simple file synchronization service (PDF)

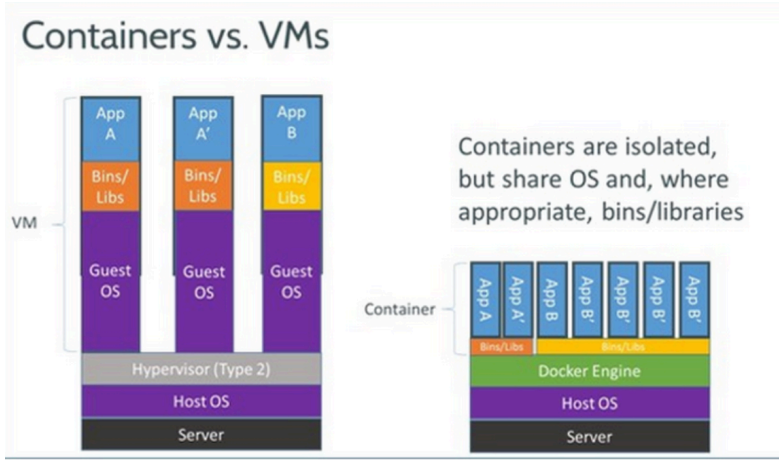
LOOK BEYOND

Wat zelf ontwikkelen

- Concrete afspraken (op basis van al aanwezige standaarden / richtlijnen) uitwerken in best-practices. Bijvoorbeeld.:
  - Beveiligen infra services (SMTP, DNS, et cetera)
  - Zonering (security model)
  - Full TCP proxy / packet filtering
  - OS Hardening
  - Disaster Recovery

Ontwikkelingen





- SDx (alles is/wordt software defined)
- Software defined Datacenter
- Micro-services
- Containers
- Orchestratie van provisoning
- Abstractielaag over technologie
- Management via (REST) API

LOOK BEYOND

Uitdagingen

- Vereiste kennisniveau (van MBO naar HBO+)
- Schaarste op de arbeidsmarkt
- Alles wordt Cloud

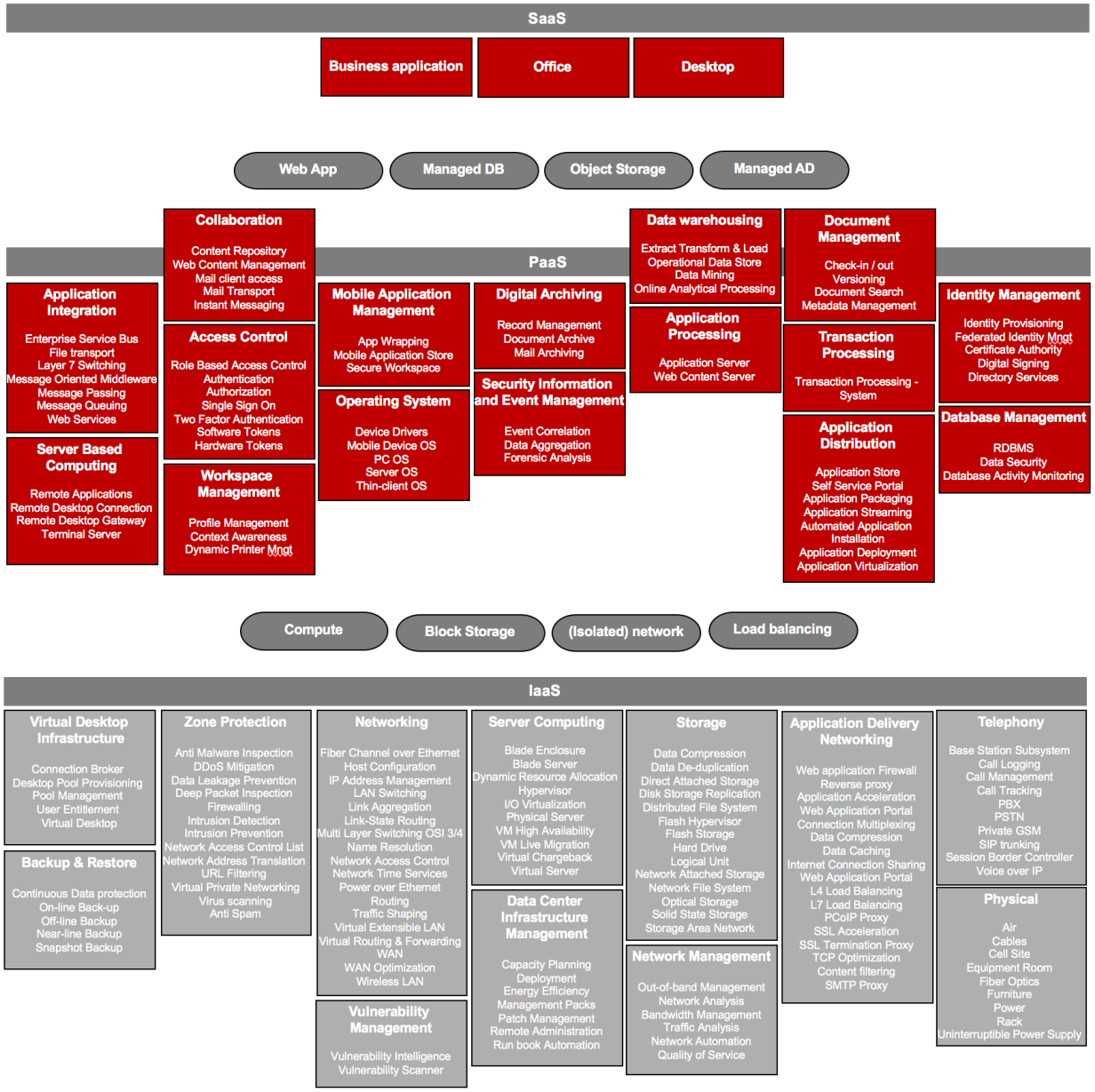
Dus de oplossing is: Infrastructure as a Service (Cloud computing!)

Managed door gemeente

Managed door leverancier

IaaS	PaaS	SaaS
Applications	*Applications*	Applications
Data	*Data*	Data
Runtime	Runtime	Runtime
Middleware	Middleware	Middleware
OS	OS	OS
Virtualization	Virtualization	Virtualization
Compute	Compute	Compute
Storage	Storage	Storage
Networking	Networking	Networking
Housing	Housing	Housing

LOOK BEYOND



Cloud kenmerken :

- Broad network access
- On-demand self-service
- Resource pooling
- Rapid Elasticity
- Measured Service

LOOK BEYOND

Scenario's

- Private (locatie gemeente)
- Community (meerdere gemeenten)
- Private Managed
- Public (multi-tenant)
- Public hyperscale (AWS, Azure, Google)

Uitdagingen IaaS Cloud computing

- Compliancy: Met welke weten, regels en normen moet ik rekening houden?
- ISO 27001/2, VIRBI, Wbp, …maar welke maatregelen horen daar bij?
- Kan ik tegen een cloud leverancier zeggen dat hij aan de BIG moet voldoen?
- Management
  - Optimalisatie (niet meer: het draait dus laat het maar met rust!)
  - Beheer van specialistische security oplossingen (WAF, Firewalls, Full TCP-proxy)
  - Focus op kosten
  - VM sprawl
  - Van ICT-organisatie naar Regie
  - Nadruk op Service level- en contractmanagement

LOOK BEYOND

Veel ruis en meningen

- Maar waarom Rijkswaterstaat en DJI dan wel bij Equinix!?
- En data encryptie dan?

Cloud don'ts voor gemeenten

door: Henri Rauch, 18 september 2013

In het verleden heb ik op deze plaats cloud do's voor gemeenten opgesomd. Die waren gebaseerd op de cloud strategie van de overheid. Regelmatig wordt ik bevraagd over de vraag wat dan don'ts zijn voor gemeenten: zijn er praktijken waar gemeenten zich voorlopig beter verre van houden in het 'woud van de cloud'? Ja, die zijn er zeker: hieronder een eerste opsomming.

Neem geen cloud-diensten af van bedrijven die een vestiging hebben in de VS. Ook indien deze diensten niet inhouden dat de data zich op het Amerikaanse vasteland bevinden kan een dergelijk bedrijf op grond van de Patriot Act gedwongen worden deze data met de Amerikaanse autoriteiten te delen. Nu na de PRISM affaire is inmiddels duidelijk dat dit in de praktijk ook daadwerkelijk gebeurt. Let ook op software van dergelijke firma's die een directe internetkoppeling aanleggen want als de lijn eenmaal open is, is het moeilijk om aan te tonen wat er wel of niet over de lijn loopt.

LOOK BEYOND

Wat kunnen gemeenten samen doen?

- Opzetten community Cloud
- Kennis bundelen:
  - Checklist / best practices bij EA voor IaaS
  - Voorbeeld PvE
  - SLA
  - Exit strategie
  - Contract aspecten
- Training (CCSK van CSA)
- 1 PvE voor alle gemeenten zodat leveranciers hier een oplossing voor kunnen ontwikkelen

LOOK BEYOND

Aanpak Haarlemmermeer?

- Cloud provider is een bedrijf uit de EU. Data blijft in EU.
- ISO 27001 certificering
- Extra eisen security (aanvullend op ISO 27001)
- Kwantificeren beschikbaarheid, RTO, RPO
- Marktonderzoek
- PvE Nadruk op verwachting t.a.v. Services:
  - Meetbaarheid
  - Serviceniveau's
  - Boete bij niet nakomen afspraken

LOOK BEYOND

Vragen?

- srodenhuis@lookbeyond.nl

LOOK BEYOND