

Beheer van Web Services

26 April 2007

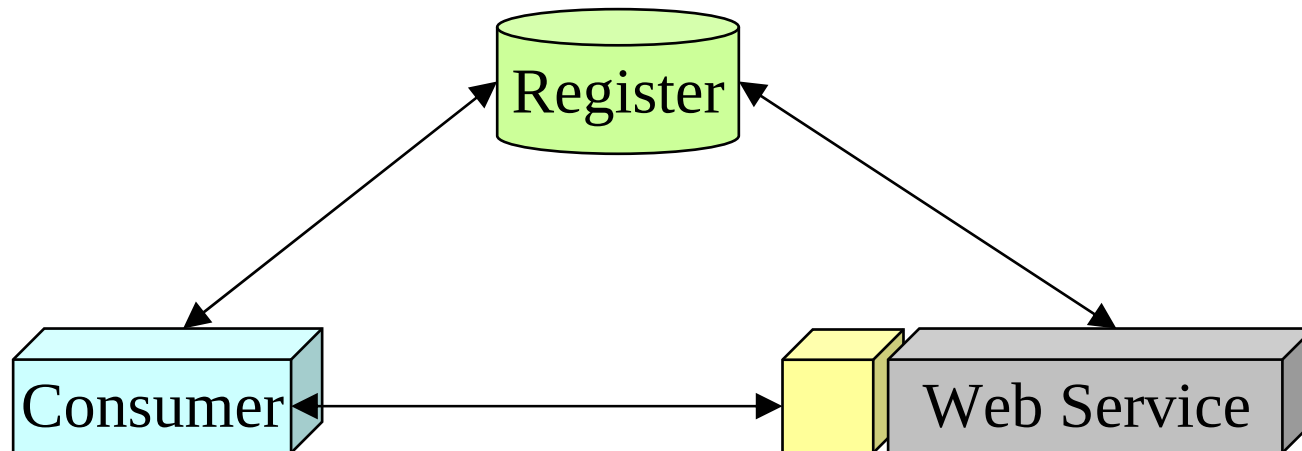
Bert Vanhalst
Sectie Onderzoek

Agenda

1. Inleiding
2. Belang van policies
3. Functionaliteiten
4. Tools
5. Organisatie
6. Best practices
7. Conclusie



Inleiding



- Service interface = contract
 - Op business gericht
 - Scheiding interface en implementatie → WS = black box
 - Als iets wijzigt aan implementatie (maar niet aan interface) zijn consumers niet geïmpacteerd
- Losse koppeling tussen software componenten



Inleiding

- Context
 - Service Oriented Architecture (SOA)
 - SOA gebaseerd op Web Services (WS)
 - Open standaarden: XML, SOAP, WSDL, UDDI
 - Interoperabiliteit tussen verschillende software omgevingen
 - Voorbeeld van een WS: Vierde weg



Inleiding

- Probleemstelling:
 - Welke WS zijn er beschikbaar?
 - Welke toepassing roept welke WS aan?
 - Welke toepassing roept welke versie van welke WS aan?
 - Hoe zijn de WS beveiligd? Kan deze beveiliging eenvoudig aangepast worden?
 - Welke afspraken mbt Quality of Service (QoS) zijn er voor welke WS?
 - In welke mate worden deze afspraken nageleefd?

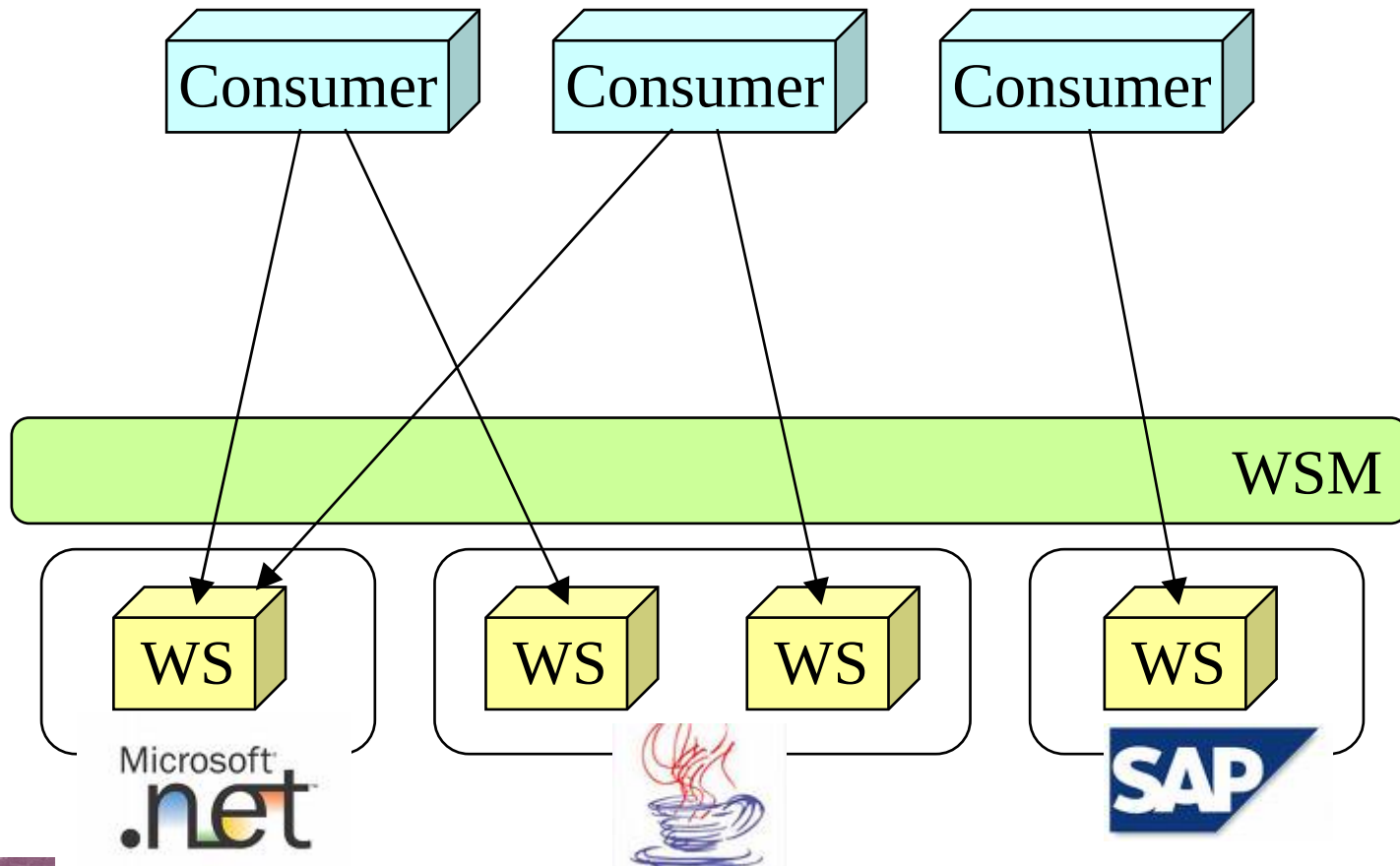


Inleiding

- Nood aan visibiliteit en controle
 - Weten wat er gebeurt
 - Actie kunnen ondernemen om bij te sturen



Inleiding



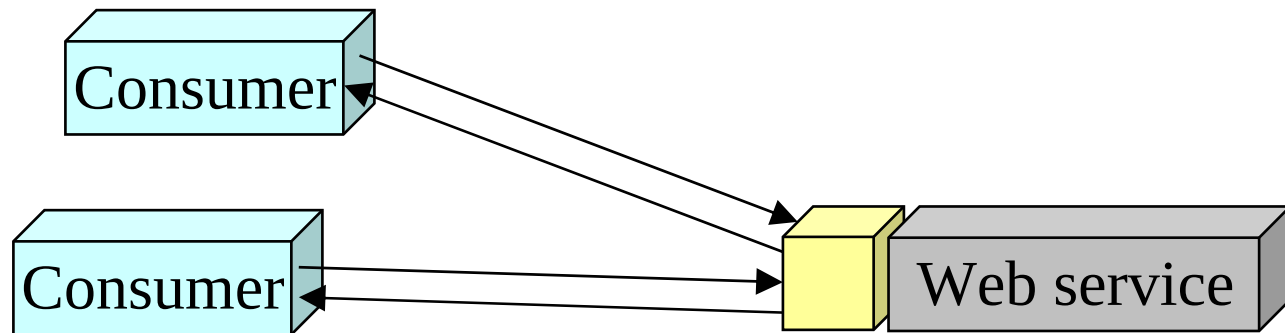
Agenda

1. Inleiding
2. **Belang van policies**
3. Functionaliteiten
4. Tools
5. Organisatie
6. Best practices
7. Conclusie



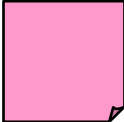
Belang van policies

- WS
 - Interface duidelijk gedefinieerd en gekend (gepubliceerd)
 - Implementatie = black box 
- Scheiding business functionaliteit en beheer-aspecten



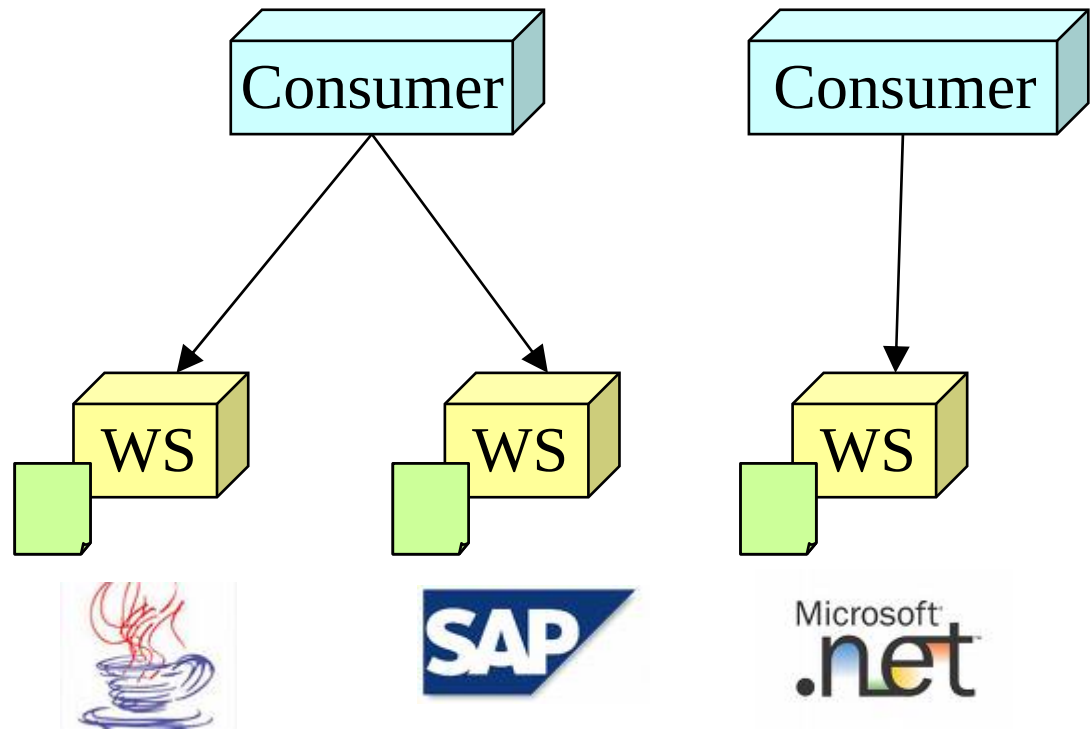
Belang van policies

Huidige security policy:

auth: userid/passwd 

Nieuwe security policy:

auth: certificaat 



Belang van policies

- Beheer-aspecten extern configureerbaar, i.e. los van de WS implementatie
- Voordelen
 - Meer flexibiliteit
 - Meer consistentie
 - Snellere ontwikkeling
- WS-Policy
 - Specificatie voor definitie van policies
 - W3C (candidate recommendation)
 - WS-SecurityPolicy



AmberPoint Services Console - Microsoft Internet Explorer

FileEditViewFavoritesToolsHelp

BackForwardStopRefreshHome

SearchFavoritesHistoryMailPrintEditDiscuss

Addressabout:blankGoLinks

AMBERPOINT

Summary

Services

Containers

Policies

LogoutUser: Admin

E-Menu

Overview

Summary View

Servicesdown | up | all

Containersdown | up | all

Service Configuration

Servicesunmanaged | managed

Register New Service

Life cycle and Discovery

Servicesproduction | developmentnew | changed

Register New Serviceproduction | developmentnew | changedauthentication errors

Management Policies

Securityauthentication | authorizationmessage security | censorshipcredentials | all

Loggingall

Version Transformall

Routingall

Performance and Availability

Service Level ManagerSet URL

Refresh Status Now

Errors and Diagnostic

Exception ManagerSet URL

Management Infrastructure

AmberPoint Servicessphere | all

Agentsall

Containersall

UDDI Repository

User-defined Attributes

Policy Templates

ImportExportNew TemplateNew PolicyDeleteHelp

ShowAll policy templates [add]Go

Name	Type	Subtype	# Policies	Imported	Creator
Simple Authentication	Security	Authentication	1	03/29/05 22:30	Randy
IMS Authentication	Security	Authentication	3	03/29/05 15:30	Randy
LDAP Authentication	Security	Authentication	4	03/29/05 12:30	Jerry
Signature Authentication	Security	Authentication	0	03/29/05 15:30	Randy
SAML Authentication	Security	Authentication	3	03/29/05 6:30	Randy
Operation Classification Authorization	Security	Authorization	2	03/29/05 3:30	Randy
Operation Authorization by Role	Security	Authorization	0	03/29/05 21:30	Randy
Role-based Credential Mapping	Security	Credential Mapping	5	03/29/05 16:30	Jerry
Fixed Credential Mapping	Security	Credential Mapping	8	03/29/05 12:30	Randy
Client-facing Message Security	Security	Message Security	3	03/29/05 3:30	Randy

Operation Classification Authorization by Role

Edit Info

Policy typeSecurityPolicy subtypeAuthorizationVersion1.0

CapabilitiesACL; Role Authorization

CriteriaEndpoint.Protocol = 'HTTP'

DescriptionThis template allows you to map one or more roles to operation classifications. The roles must map to those used in your container or identity management system. The

Agenda

1. Inleiding
2. Belang van policies
3. **Functionaliteiten**
4. Tools
5. Organisatie
6. Best practices
7. Conclusie



Functionaliteiten

- Bijhouden van gebruiksstatistieken (logging)
- Beveiliging
- Versiebeheer
- Transformaties en routing
- Quality of Service (QoS)
- Beheer van Service Level Agreements (SLA's)
- Notificaties / alerts
- Exception handling
- Protocol en transport mediation
- Visualisatie en rapportering



Logging

- Aantal requests per WS of per functie
- Aantal requests per consumer
- Inhoud van berichten
- Antwoordtijden (maximaal, gemiddeld)
- Grootte van de berichten
- Aantal fouten (SOAP faults)

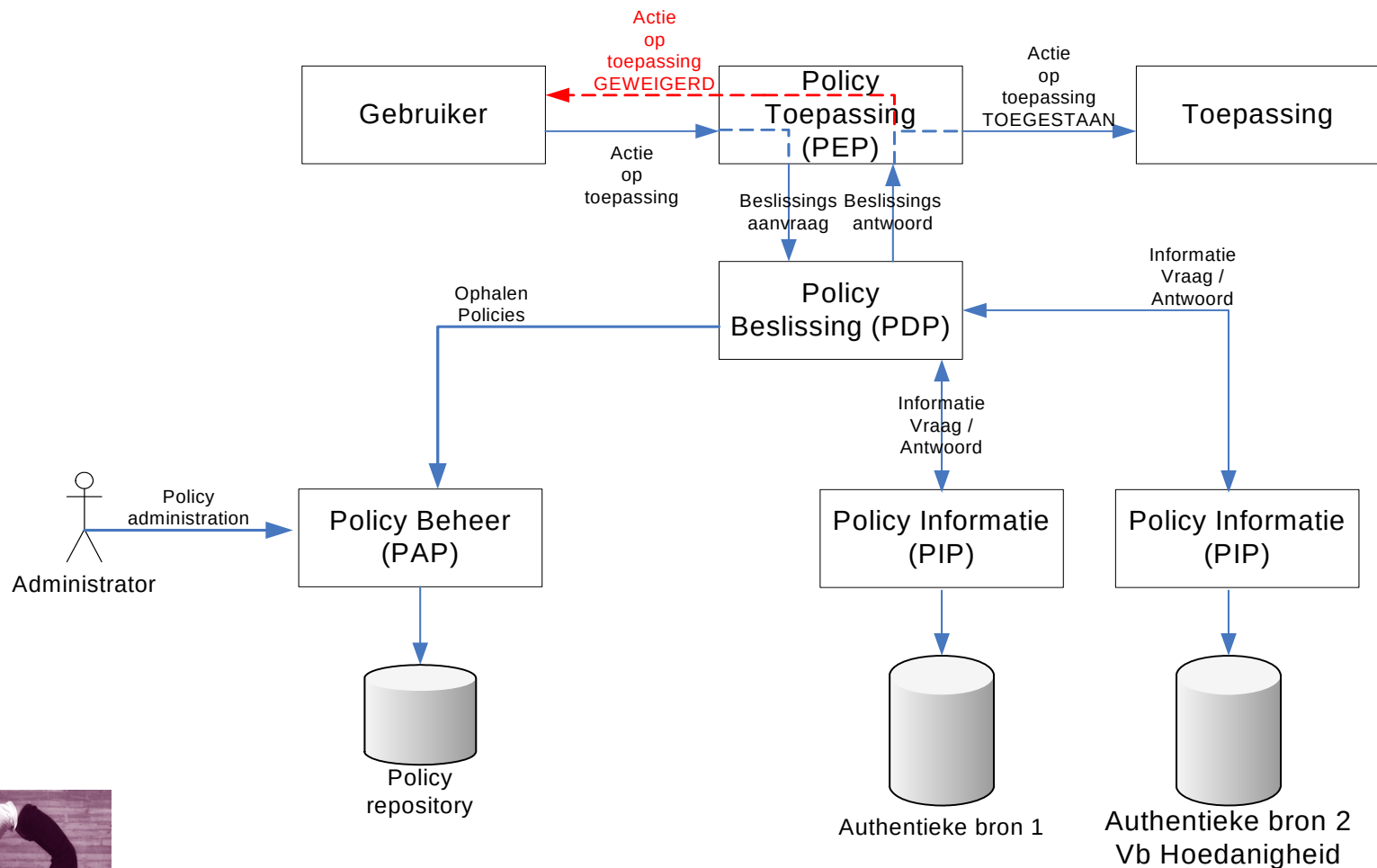


Logging

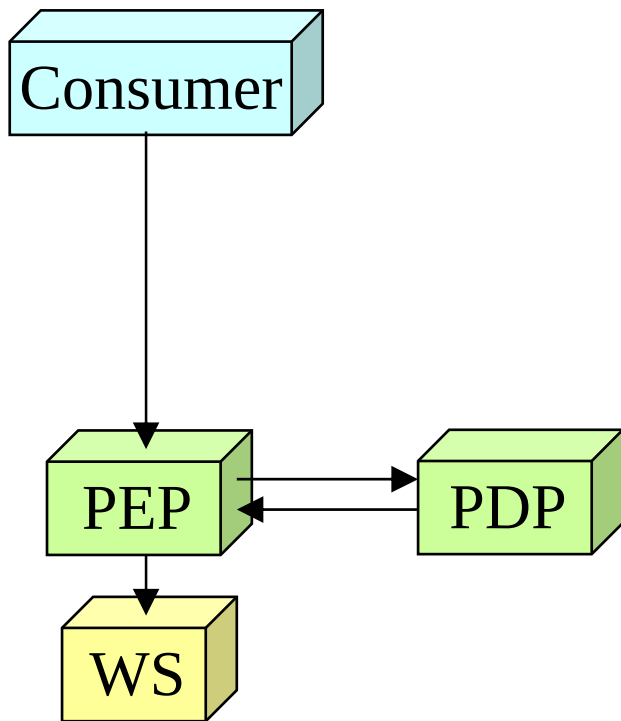
- Logs nuttig voor:
 - Statistieken
 - Analyseren trends / capaciteitsplanning
 - Facturatie
 - Business metrics (BAM)
- Programmatorische exploitatie logs
 - Rechtstreeks via database
 - Via API (WS interface?)



Beveiliging



Beveiliging



- Policy Enforcement Point (PEP)
 - Dwingt policy af
- Policy Decision Point (PDP)
 - Neemt autorisatie-beslissing
- Integratie met PDP via WS en SAML request/response
- Bestaand user management!



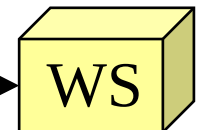
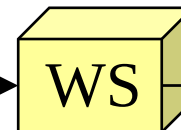
Beveiliging

- Authenticatie, op basis van
 - HTTP username/password
 - SSL X.509 certificaat
 - WS-Security username token
 - WS-Security X.509 token
 - WS-Security SAML token
- Mediation tussen security tokens
 - Vb: WSM voert authenticatie uit op basis van certificaat; WSM stuurt SAML token verder naar endpoint (i.e. de eigenlijk WS)



Beveiliging

- Autorisatie
 - Heeft de consumer toegang tot de WS?
 - Autorisatie-beslissing via intern of extern PDP
- Circle of trust
 - Authenticatie eindgebruiker door consumer
 - 'Trust' tussen WS en consumer
 - Propagatie SAML token als bewijs van authenticatie



Beveiliging

- Confidentialiteit en integriteit
 - SSL / TLS
 - XML Encryption
 - XML Signature
- Encryptie en digitale handtekening mogelijk op niveau van individuele elementen van een bericht
- Opletten met overhead cryptografische bewerkingen !



Beveiliging

- Audit / security logging
 - Wie – welke fysieke persoon?
 - Wat – welke WS, welke functie?
 - Wanneer – timestamp?
 - Hoe – via welke consumer toepassing?



Beveiliging

- Controles
 - Schema validation
 - Zijn berichten conform de WSDL interface?
 - WS-I profiles
 - Zijn berichten conform WS-I profiles?
 - Garanderen interoperabiliteit
 - Basic profile, Security profile (www.ws-i.org)
- Antwoord met SOAP fault

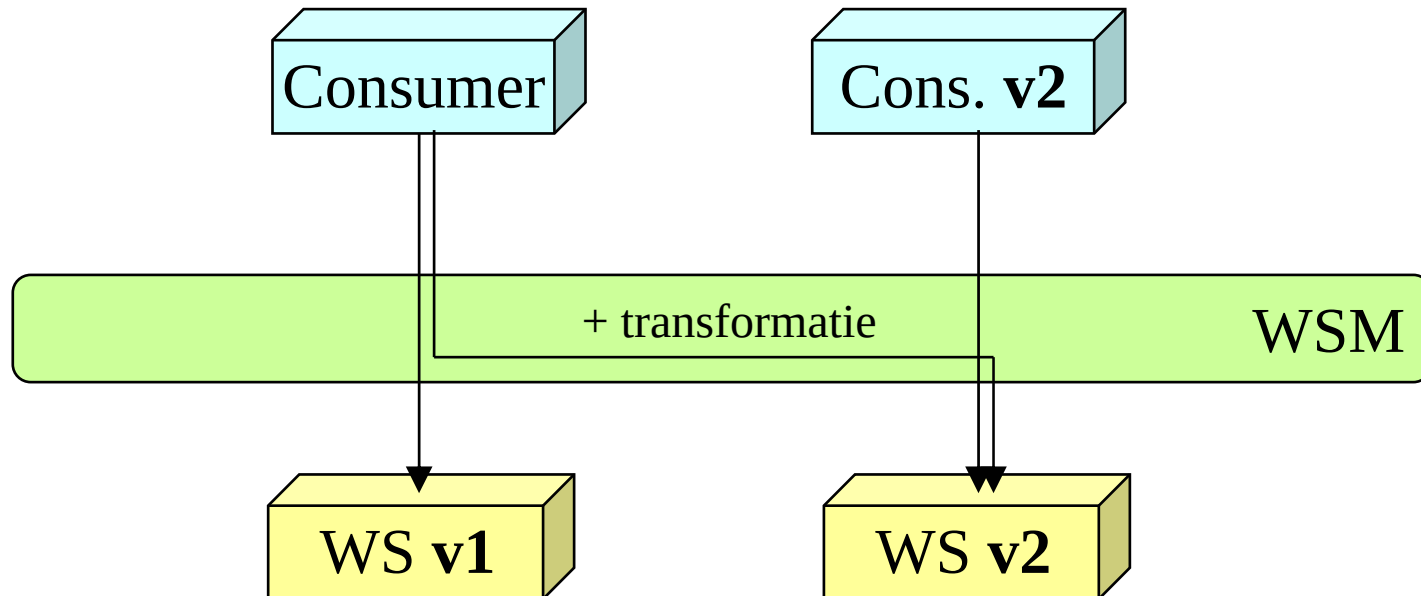


Versiebeheer

- Geval 1: Veranderingen aan de interface zijn backwards compatible
 - Bijkomende functies
 - Gewijzigde implementatie
- Geval 2: Veranderingen aan de interface zijn niet backwards compatible
 - Bijkomende of weggelaten parameters
 - Gewijzigd type van parameter
- Routing en transformaties → geen wijziging aan consumers



Versiebeheer



Transformaties en routing

- Transformaties
 - XSLT & grafische mapping tools
- Routing
 - Op basis van inhoud
 - Vb: op basis van bedrag
 - Op basis van context
 - Vb: op basis van versienummer
 - Vb: op basis van IP
 - Load balancing en fail-over
 - Xpath



Quality of Service (QoS)

- Beschikbaarheid
 - Fail-over
 - Load balancing
- Schaalbaarheid
- Volume controle
 - Vermijden dat een consumer alle resources verbruikt ten koste van andere consumers
 - Opleggen quotum per consumer of groep consumers, bvb. #requests per tijdseenheid



Service Level Agreements (SLA's)

- Goede afspraken nodig mbt de geleverde kwaliteit
- Per WS en per consumer of groep consumers
- Opstellen van KPI's
- Monitoren van SLA compliance
- Mogelijkheid (automatisch) actie te ondernemen indien SLA's dreigen geschonden te worden
 - Vb: voorrang aan 'gold' consumers



Time Range: [Icons]



Monitor Services

Service	Throughput	Faults	ResponseTime
ActivateSubscriberRequest	0	0	---
AddAccount	120	0	16
AddPayment	0	0	---
InquireServiceAreaByZip	120	9	562
OrderEquipment	59	0	25
ReserveSubscriberNumber	120	2	285

[view these services...](#)

Monitor Customers

Customer	Warnings	Failures
Best Buy	0	1
Buy Online	0	0
Cingular Online	0	1
Walmart	0	0
RNS	1	1

[view these customers...](#)

Customer SLAs in Violation or Warning

Currently at	Customer	Period End	Last # Periods
32 ms	Walmart	39 min	■■■■■■■■■■
109 ms	Best Buy	39 min	■■■■■■■■■■

[view these customers...](#)

My Reports

[AddAccount Service Detail](#)

[Service Usage by Customer](#)



Most Recent Alerts

Alerts	Value	Detected
Objective violation	109.0 ms	01-31-2006 02:19 PM
Maximum ResponseTime has violated an agreement		
Objective violation	93.0 ms	01-31-2006 02:15 PM
Maximum ResponseTime has violated an agreement		
Target warning	1090.11 ms	01-31-2006 02:11 PM
ResponseTime is approaching violation of a service target		

[view these alerts...](#)

Notificaties / alerts

- Trigger
- Verschillende niveau's: warning, error
- Integratie
 - Nagios: centrale supervisie
 - Via SNMP



Exception handling

- Oorzaken: technisch of inhoudelijk
 - Time-out in de back-end
 - Verkeerde syntax van berichten
 - Niet toegelaten inhoud van berichten
 - Consumer niet geautoriseerd
- Terugsturen SOAP fault
 - Met duidelijke informatie



Protocol en transport mediation

- Mediation tussen protocolversies
 - SOAP 1.1 en SOAP 1.2
- Mediation tussen transportprotocollen
 - HTTP
 - HTTPS
 - JMS
 - SMTP
 - FTP

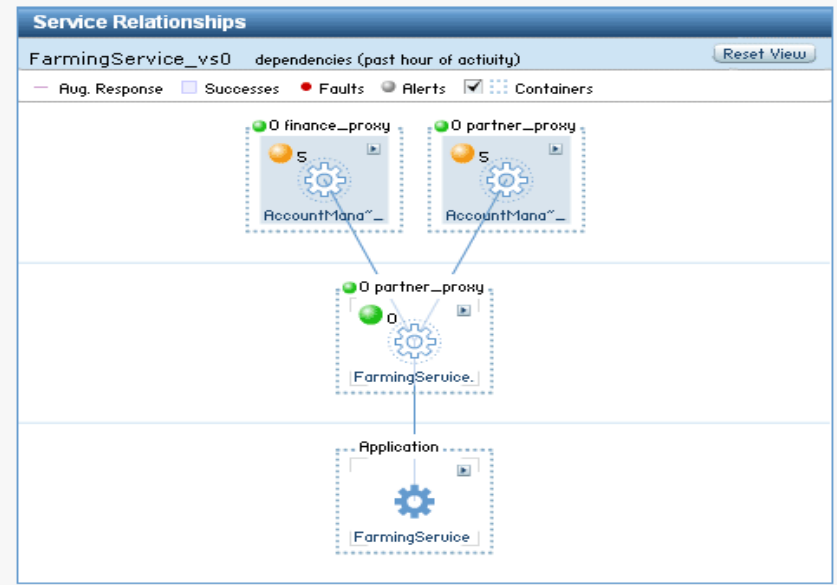
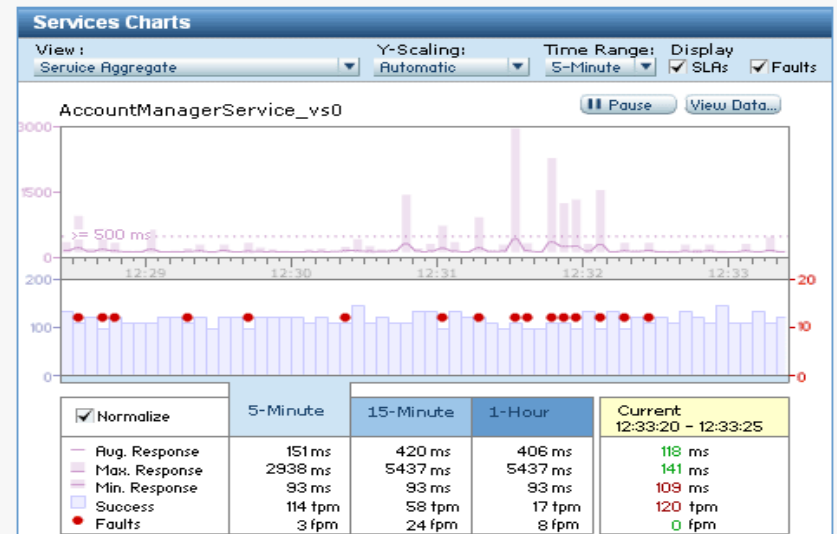


Visualisatie en rapportering

- Verschillende doelgroepen met verschillende rechten
 - Administrator
 - Status infrastructuur
 - Supervisie
 - Status services, alerts
 - SLA beheerders
 - SLA definitie en rapportering
 - Business analisten
 - Gebruiksstatistieken
- Bekomen van (custom) rapporten



Details **Operations**



Service Details

Information

Type: Managed Virtual Service

Name: AccountManagerService_vs0

Description:

State: Major

Alerts: 7

Key: uddi:b5e573f9-d973-11d9-b3b2-ff3c729af946

User Name: dJabaetODvMtPjwPsvBffw==

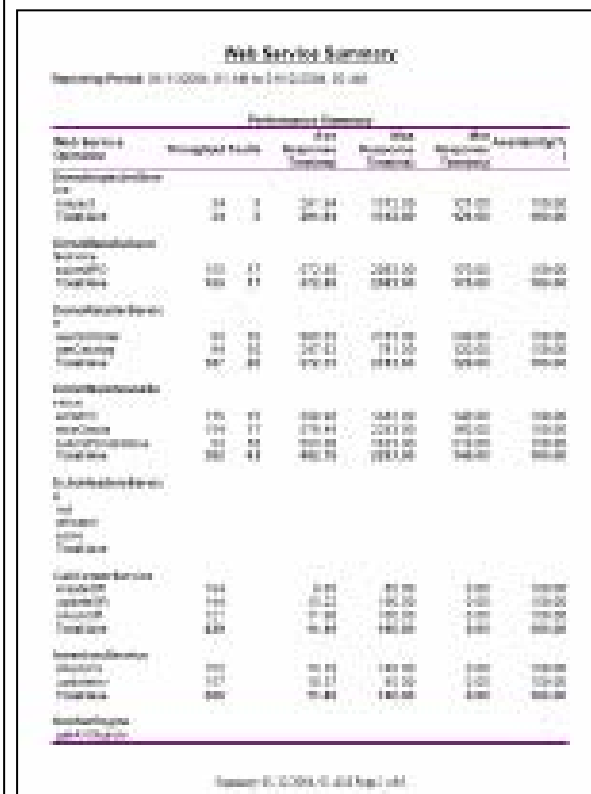
Listeners

- HTTP
- HTTPS
- JMS

Alerts

1616	uddi:b5e573f9-d973-11d9-b3b2-ff3c729af946	06/15/2005 12:31:59
▲	SLA Violation	20000001
○	Poor Response - Response Time (2938) >= 500 milliseconds in 15 min interval	- select -
1417	uddi:b5e573f9-d973-11d9-b3b2-ff3c729af946	06/15/2005 12:16:58
▲	SLA Violation	20000001
○	Poor Response - Response Time (2563) >= 500 milliseconds in 15 min interval	- select -
1079	uddi:b5e573f9-d973-11d9-b3b2-ff3c729af946	06/10/2005 15:04:36
▲	SLA Violation	20000001
○	Poor Response - Response Time (578) >= 500 milliseconds in 15 min interval	- select -
1078	uddi:b5e573f9-d973-11d9-b3b2-ff3c729af946	06/10/2005 15:01:36
▲	SLA Violation	20000001
○	Poor Response - Response Time (531) >= 500 milliseconds in 15 min interval	- select -
1077	uddi:b5e573f9-d973-11d9-b3b2-ff3c729af946	06/10/2005 14:59:36
▲	SLA Violation	20000001
○	Poor Response - Response Time (563) >= 500 milliseconds in 15 min interval	- select -

1-5 of 5



Bijkomende functionaliteiten

- "Zwarte" web services
 - Automatische detectie (vereist 'agent' plugins op hosting platform)
 - Automatische toepassing van een bepaalde policy
- Virtuele web services
 - Weglaten van functies
 - Samenbundelen functies van verschillende WS
 - Nuttig voor beheer oproepen naar externe WS



Bijkomende functionaliteiten

- Afhankelijkheden tussen WS
 - In kaart brengen van oproepen tussen de beheerde WS
 - Nuttig voor root cause analysis in aaneenschakelingen van services
- Functies van systems management software
 - Beheer van J2EE componenten, database connecties
 - Drill-down in technische componenten



AmberPoint Services Console - Microsoft Internet Explorer

FileEditViewFavoritesToolsHelp

BackForwardStopHomeSearchFavoritesRefreshPrintSendToRunFind

Addresshttp://localhost:8080/apasc/portal/html/pages/AwpxPortalHandler.xhtml?~sol=1&~p0=root&~p0:~apsvc=02840D1C-68CF-11D9-B1CF-F509F45GoLinksWind

GoogleDictionary.com

AMBERPOINTSummaryServicesContainers

Log outUser: AmberPoint

E-MenuSelector

ManageEditHelp

Show servicesGo

add

Register

CreditService8080

OrderService

ShippingService8080

WarehouseService

checkAvailability

placeOrder

saveSettings

setOrderServiceUrl

setShippingServiceUrl

AmexService

BonjourMondeService

CreditService8780

HelloWorldService

HolaMundoService

OrderProcessorService

ShippingService

WarehouseService

View Original WSDL

Status: Managed via Plug-in

Discovered: Jan 21 09:08:02

Type: Container Discovered

Last Deployed: Jan 21 09:08:02 by AmberPoint

Version: Unknown

Management Changed: Jan 21 09:17:43 by (ANONYMOUS)

Dependencies

Structure

Service: WarehouseService

Endpoint: WarehouseServiceSOAP

Operation: All Operations

ShippingServiceSO...

WarehouseServic...

OrderServiceSOAP

CreditServiceRouter

CreditServiceSOAP

18

19

19

42

38

20

23

65%

100%

v0.63

Add Dependency

Add To Summary View

EndpointManagedServiceRequests InRequests Out

WarehouseServiceSOAP

Endpoint Info

Yes

WarehouseService

42

38

Done

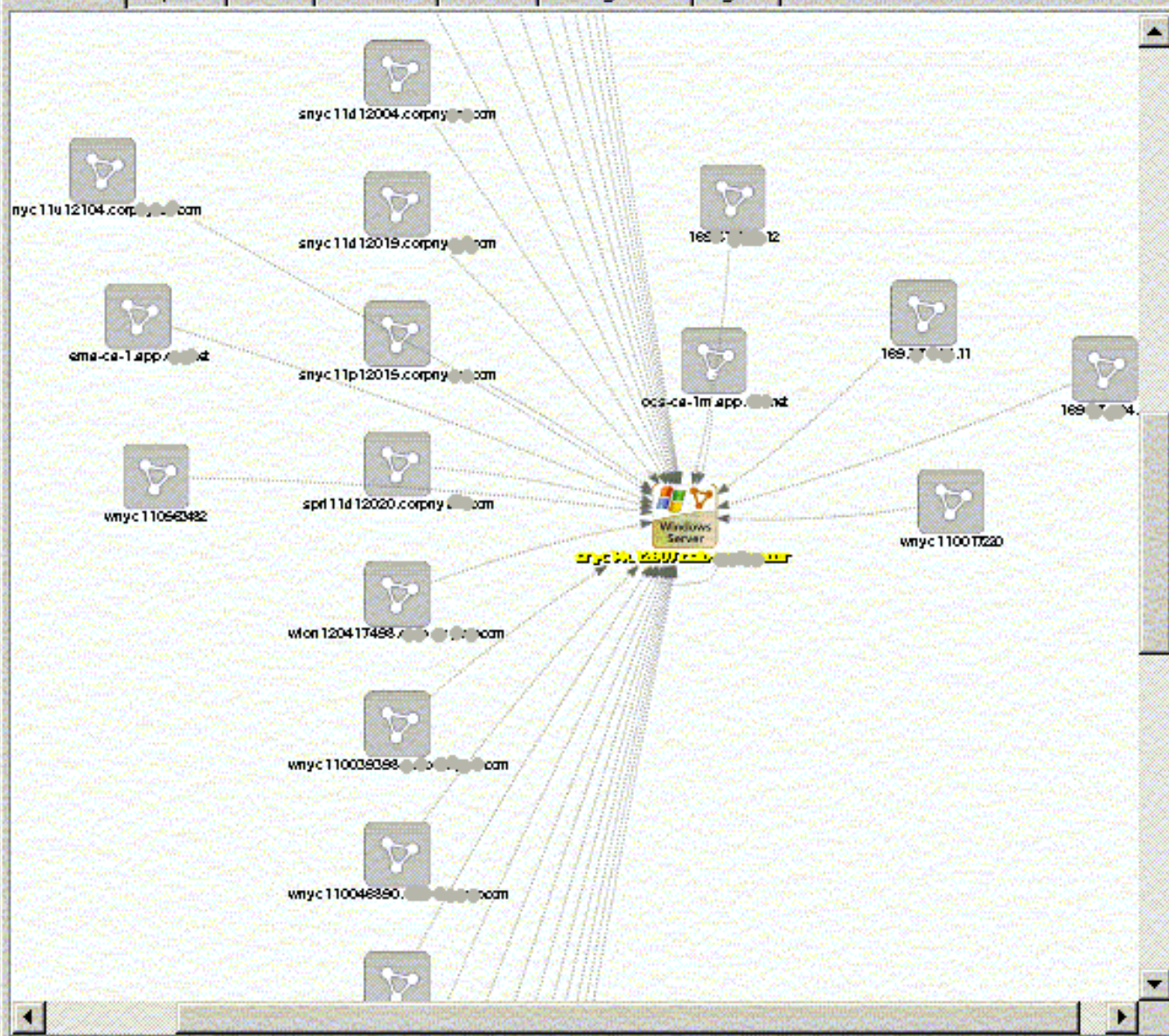
Local intranet

Navigate

Statistics

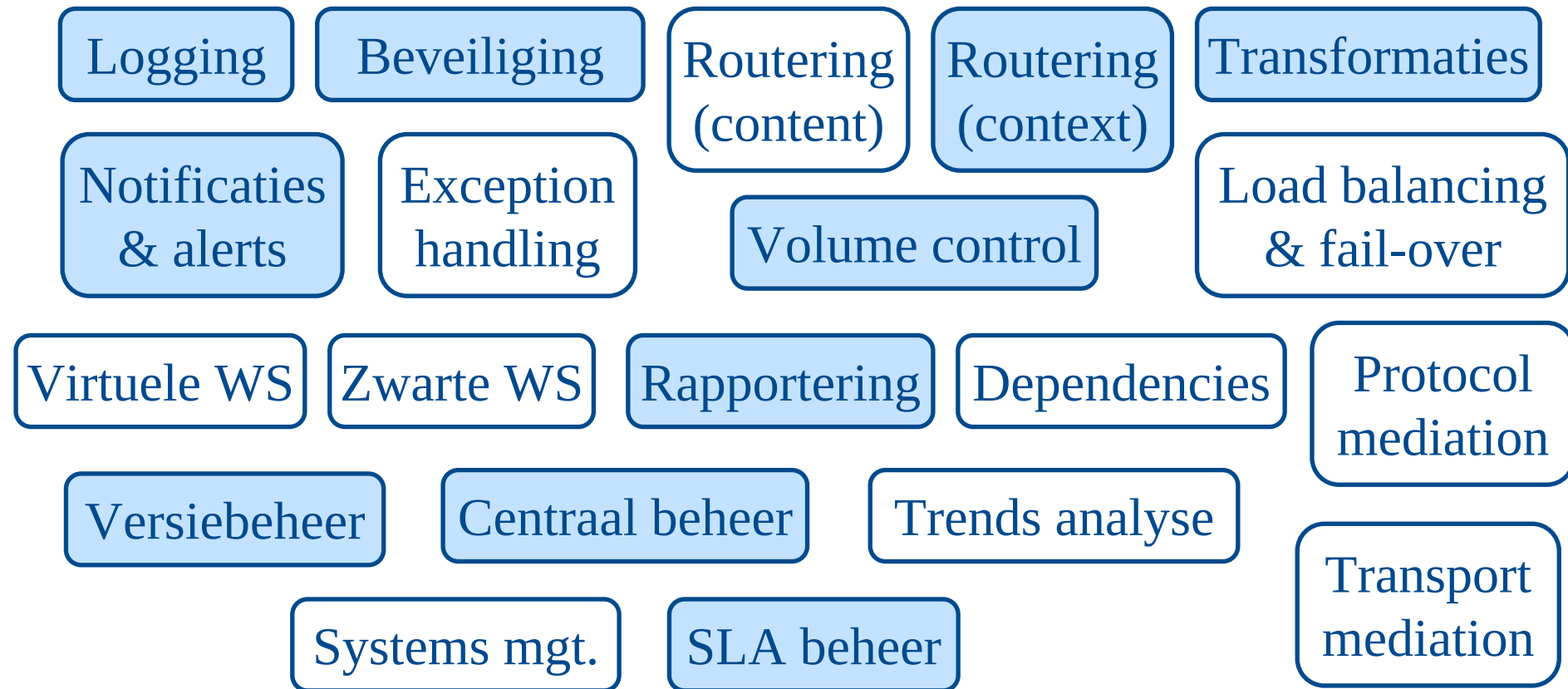
- ema-ca-2.app. net
- ePro - Development
- nys00a-0201. com
- ocs-ca-1m.app. net
- ocs-ca-2m.app. net
- slon12d12100-fid1. co.uk
- slon12d12100-fid2. co.uk
- snyc11d12003.corpn. cor
- snyc11d12004.corpn. cor
- snyc11d12019.corpn. cor
- snyc11p12015.corpn. cor
- snyc11u12104.corpn. cor
- snyc14u12607. c
- spr11d12020. com
- wlon120417498. com
- wnyc110017220
- wnyc110039398. com

Overview Explorer Portal Stabilizers Policies Configuration Agent



Active Stabilizers

Functionaliteiten



Agenda

1. Inleiding
2. Belang van policies
3. Functionaliteiten
4. **Tools**
5. Organisatie
6. Best practices
7. Conclusie

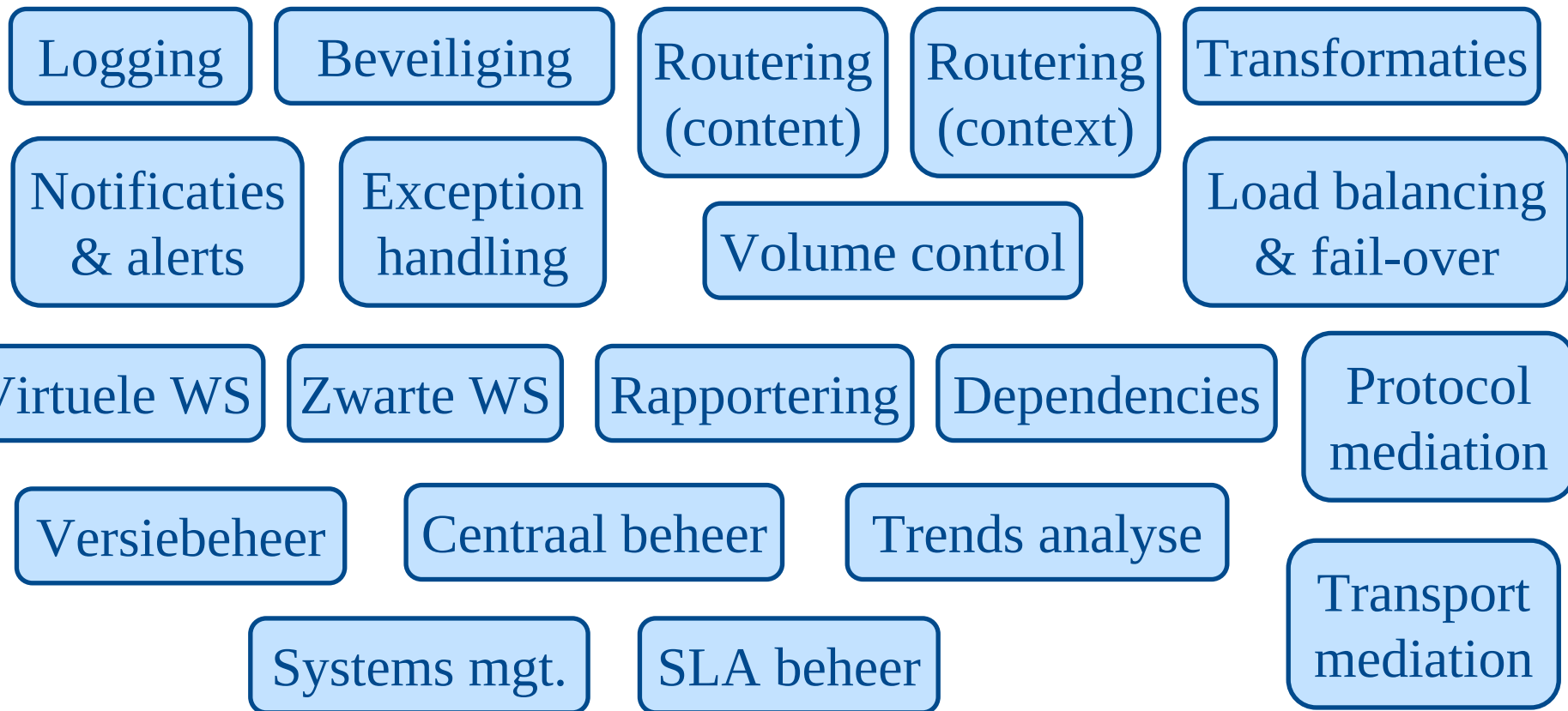


Tools – Overzicht

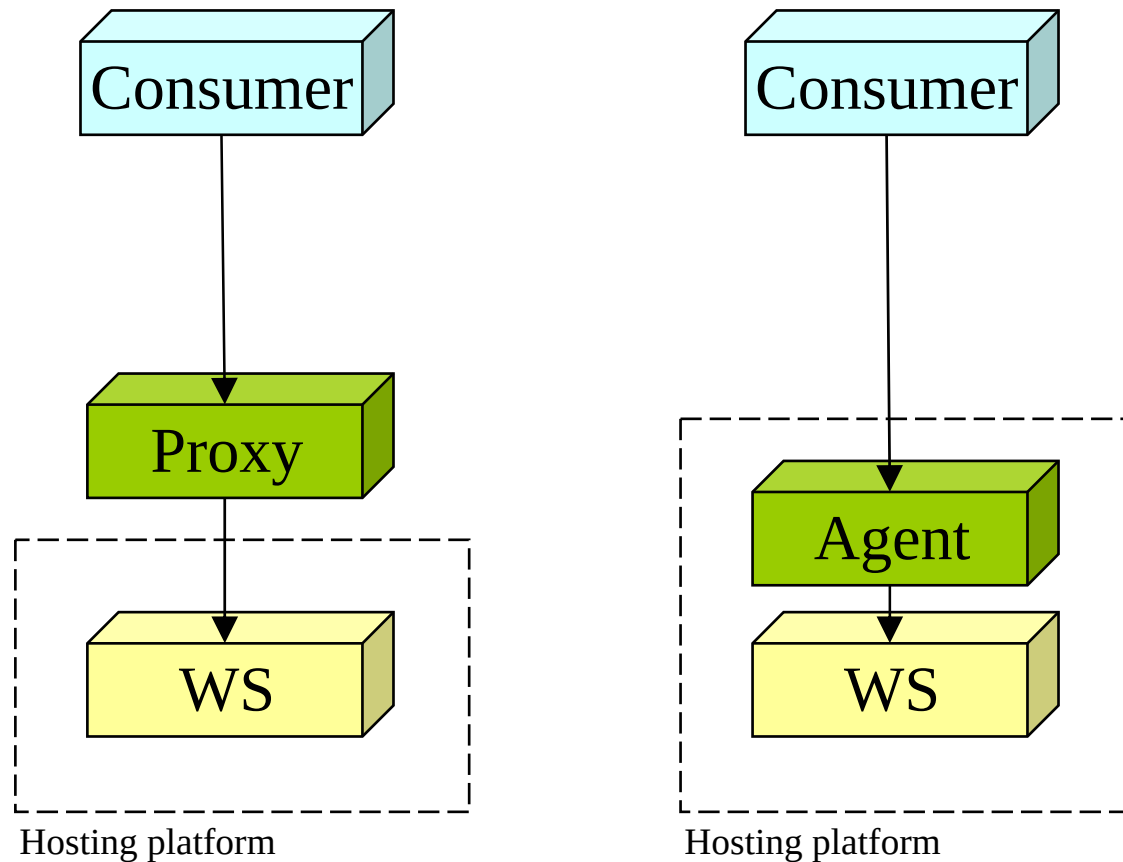
- Web Service Management (WSM) tools
- Registries en repositories
- Enterprise Service Bus (ESB)
- XML appliances



Web Service Management tools

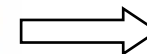
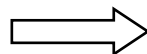
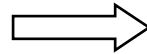
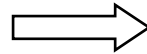


Web Service Management tools



Web Service Management tools

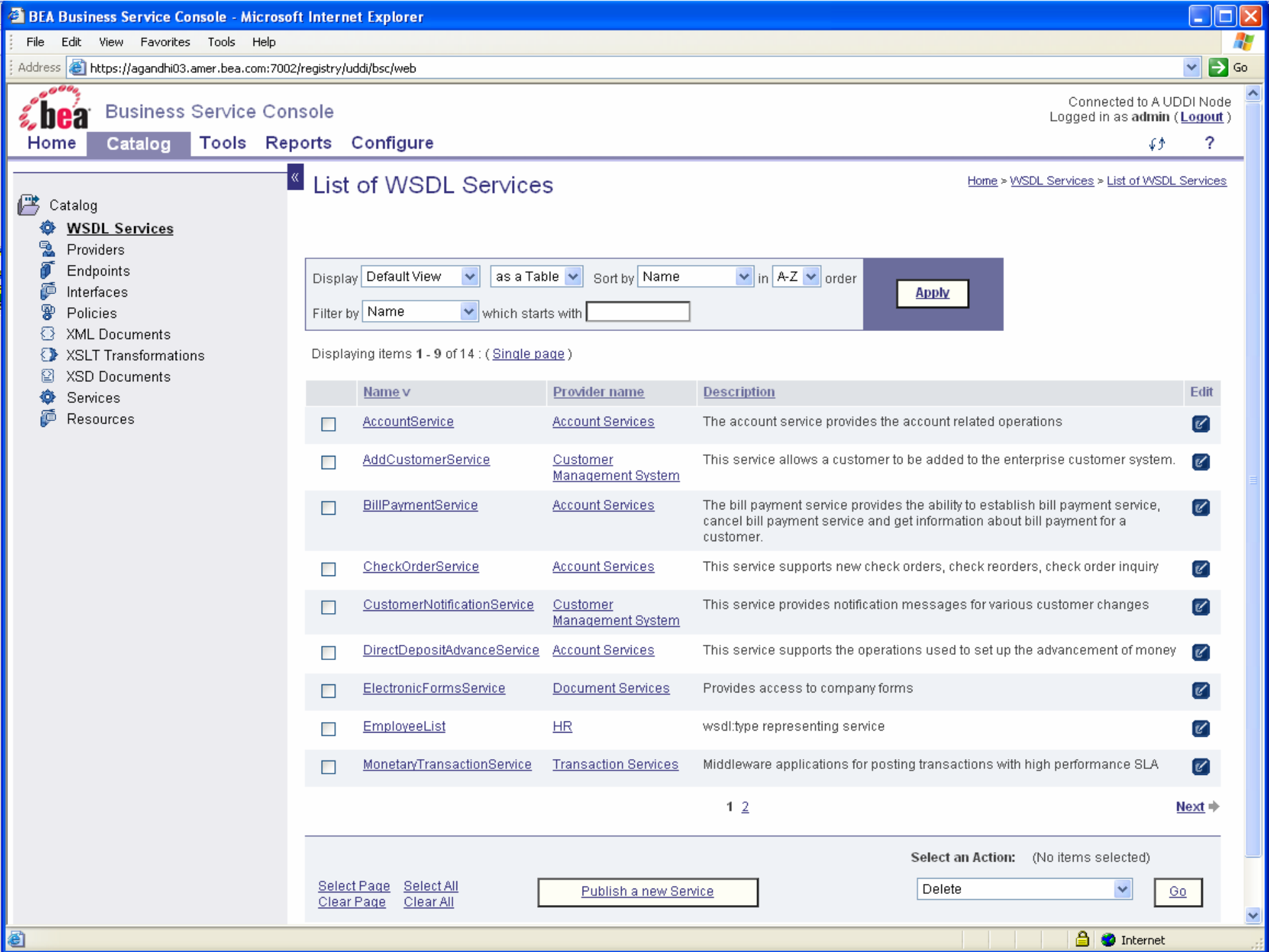
- Leveranciers



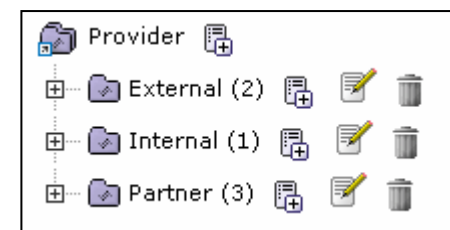
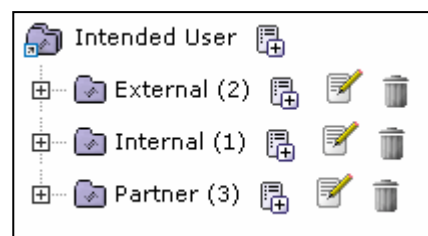
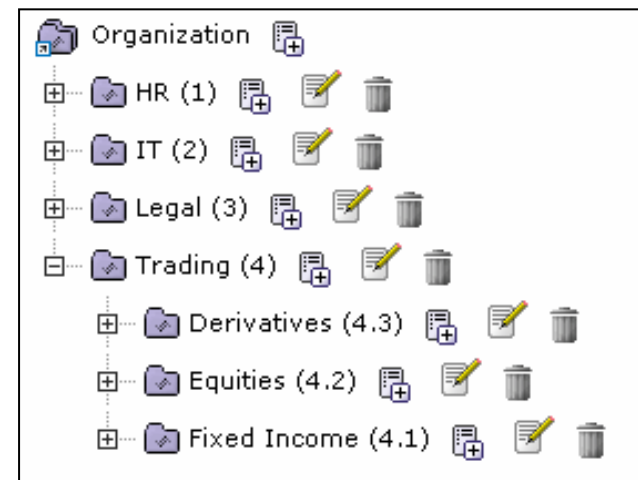
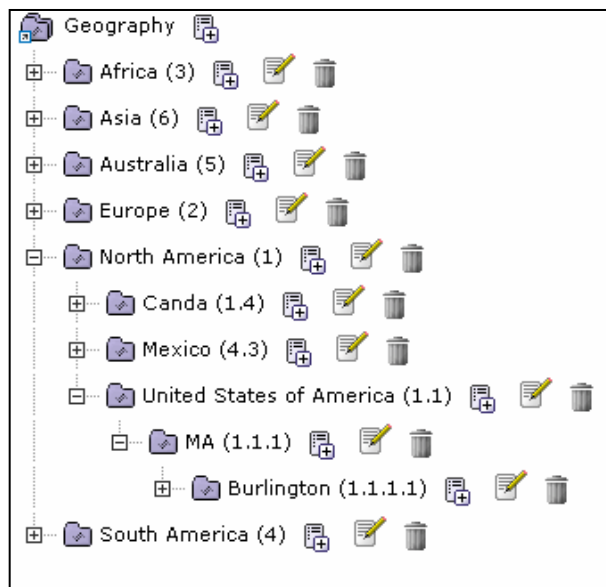
Registries / Repositories

- Functies
 - Designtime: opvragen metadata
 - WSDL interface, contact-info, contracten, policies, enz.
 - Faciliteert hergebruik
 - Schakel met runtime
 - Vb: dynamische binding
- Registry: verwijst naar gegevens
- Repository: bevat gegevens
- Producten kunnen beide functies combineren
- UDDI v3 compliance belangrijk!

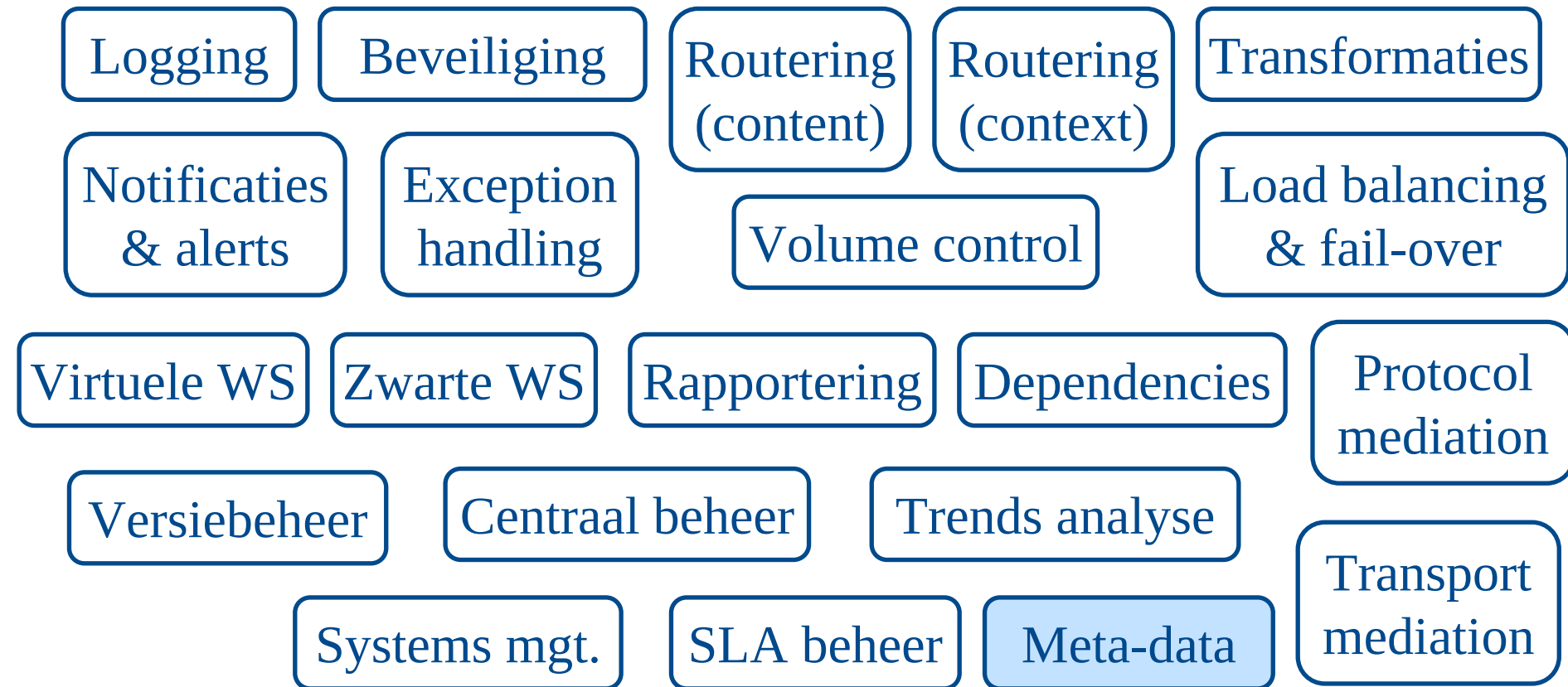




Registries / Repositories

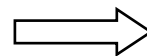
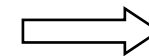
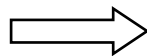
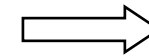
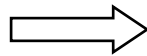


Registries / Repositories

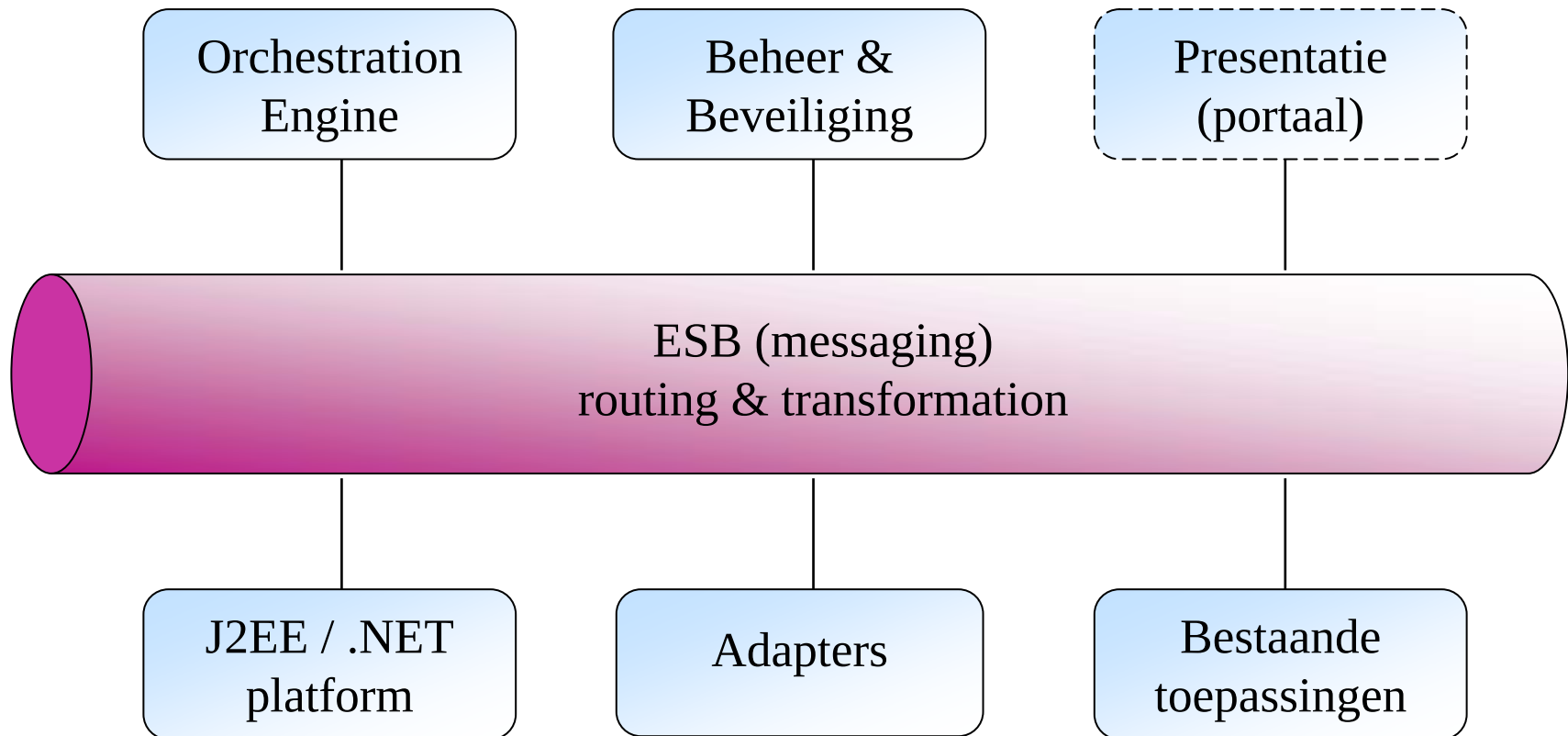


Registries / Repositories

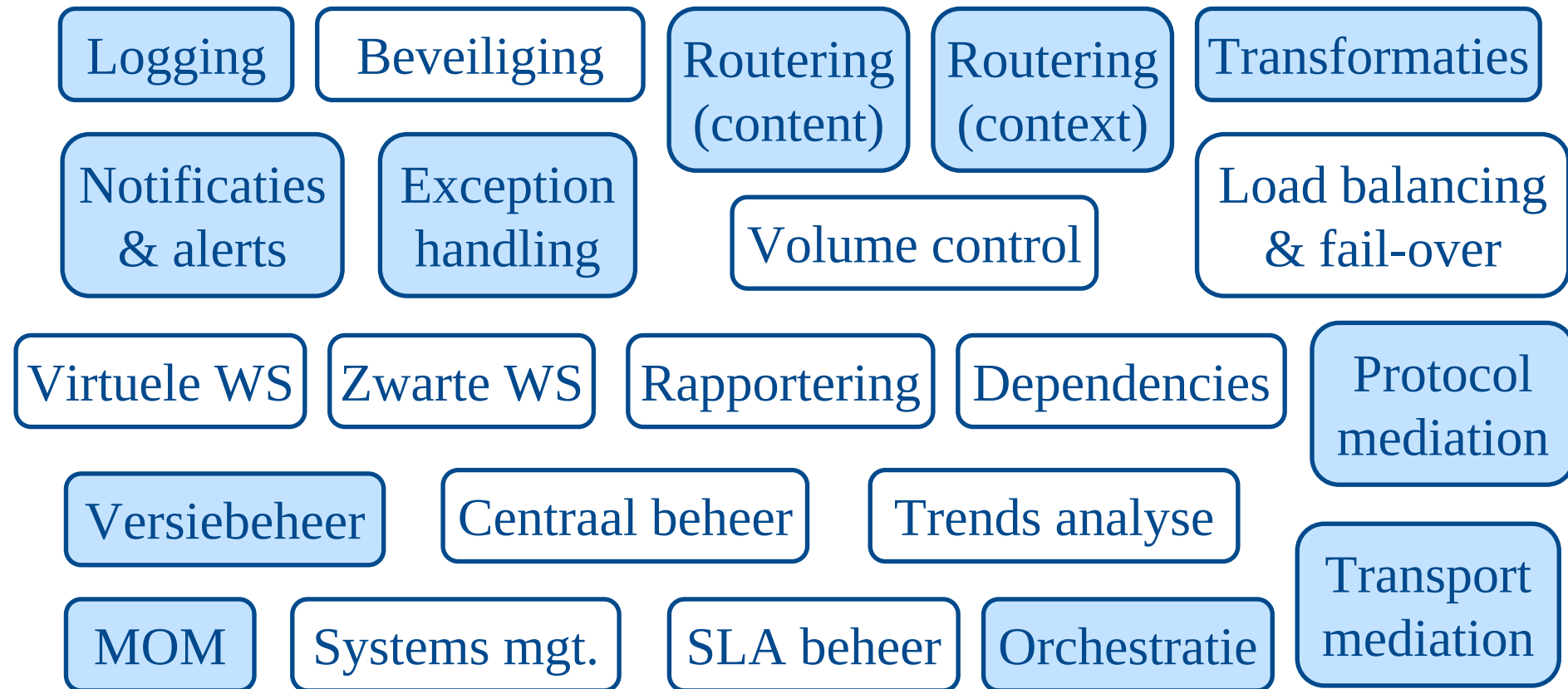
- Leveranciers



Enterprise Service Bus (ESB)



Enterprise Service Bus (ESB)



Enterprise Service Bus (ESB)

- Leveranciers



Open source:



XML appliances

Logging

Beveiliging

Routing
(content)

Routing
(context)

Transformaties

Notificaties
& alerts

Exception
handling

Volume control

Load balancing
& fail-over

Virtuele WS

Zwarte WS

Rapportering

Dependencies

Protocol
mediation

Versiebeheer

Centraal beheer

Trends analyse

Systems mgt.

SLA beheer

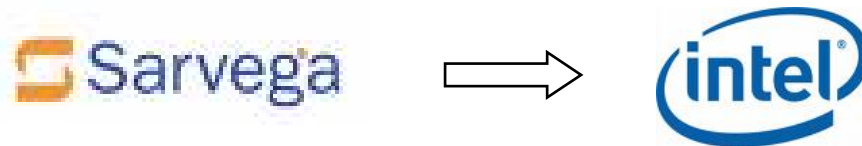
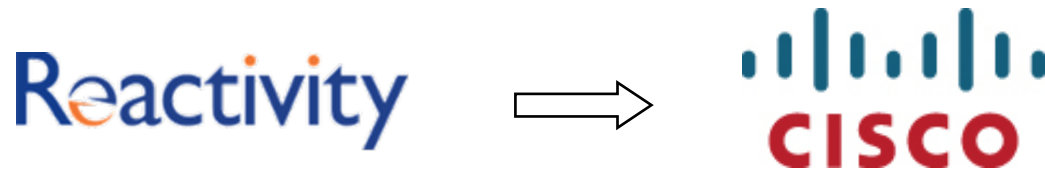
Acceleratie

Transport
mediation



XML appliances

- Leveranciers



Tools - overzicht

	WSM	Reg/Rep	ESB	XMLA
Platform			✓	
Acceleration				✓
Centraal mgmt	✓			
Metadata	±	✓	±	±
MOM			✓	
Mediation	✓		✓	✓
Security	✓		±	✓



Tools – beschouwingen

- Overlap tussen producten
- Geen uniek product voor SOA governance
 - Combinatie nodig van meerdere producten
- Registry = link tussen componenten
- Partnerships zijn belangrijk
 - Gebrek aan standaarden zoals WS-Policy voor communicatie tussen componenten
 - GIF (Governance Interoperability Framework)
 - www.soalink.com – opgestart door Infravio/WebMethods



Agenda

1. Inleiding
2. Belang van policies
3. Functionaliteiten
4. Tools
5. **Organisatie**
6. Best practices
7. Conclusie



Organisatie

- Naast tools ook organisatie nodig en duidelijke afspraken
- Wie bepaalt welke services ontwikkeld worden en met welke prioriteit?
- Wie verantwoordelijk voor een bepaalde WS?
 - Bepalen tempo en interface van nieuwe versies
- Proces voorzien voor afwijkingen en aanpassingen



Agenda

1. Inleiding
2. Belang van policies
3. Functionaliteiten
4. Tools
5. Organisatie
6. **Best practices**
7. Conclusie



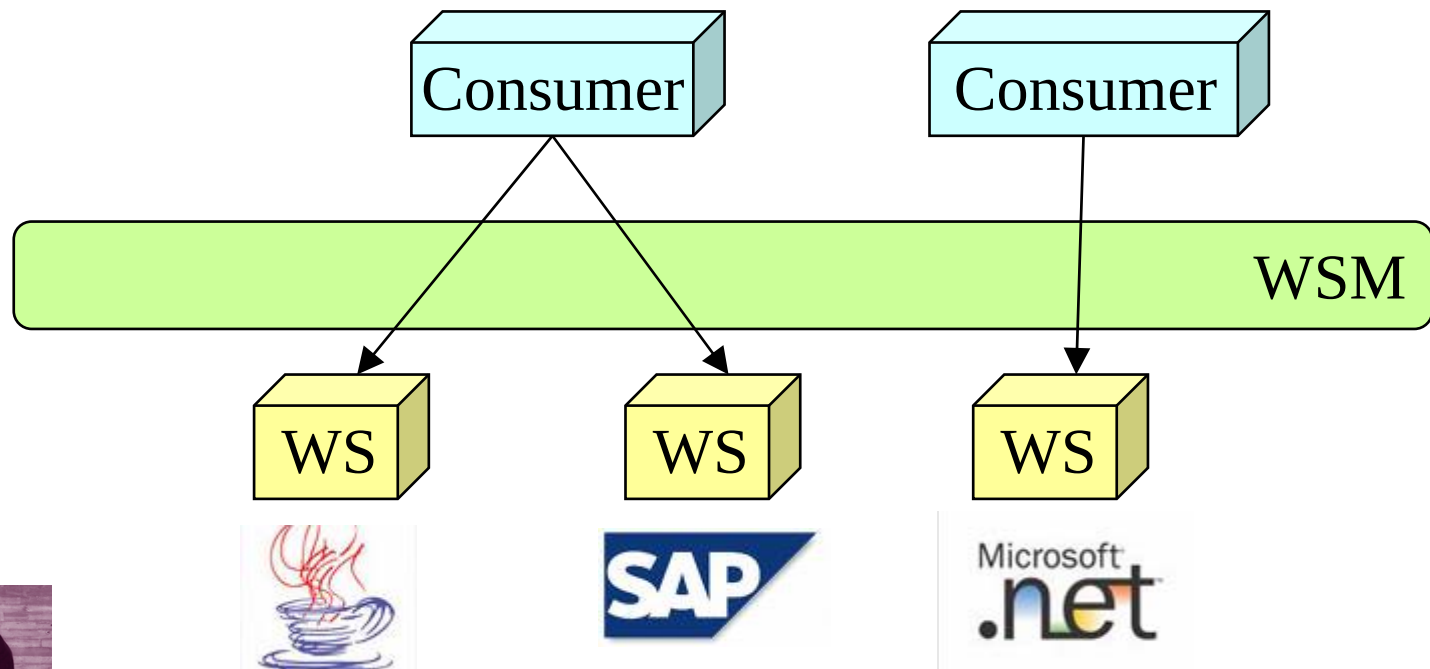
Best practices

- Externaliseer de niet-business functionaliteiten
- Baseer beheer en controle op policies
 - Garantie voor flexibel systeem
- Automatiseer zoveel mogelijk controles
 - Vb: automatische SOAP/WSDL compliance checks
- Besteed aandacht aan standaarden!
 - WS-Policy
 - UDDI



Best practices

- Infrastructuur moet platform-onafhankelijk zijn
 - Vermijd om voor elke WS of elk platform telkens dezelfde beheer-functionaliteit te implementeren



Best practices

- Vermijd onnodige cryptografische bewerkingen (encryptie, digitale handtekening)
 - Performance kost
 - Indien toch nodig, overweeg hardware acceleration (XML appliance)

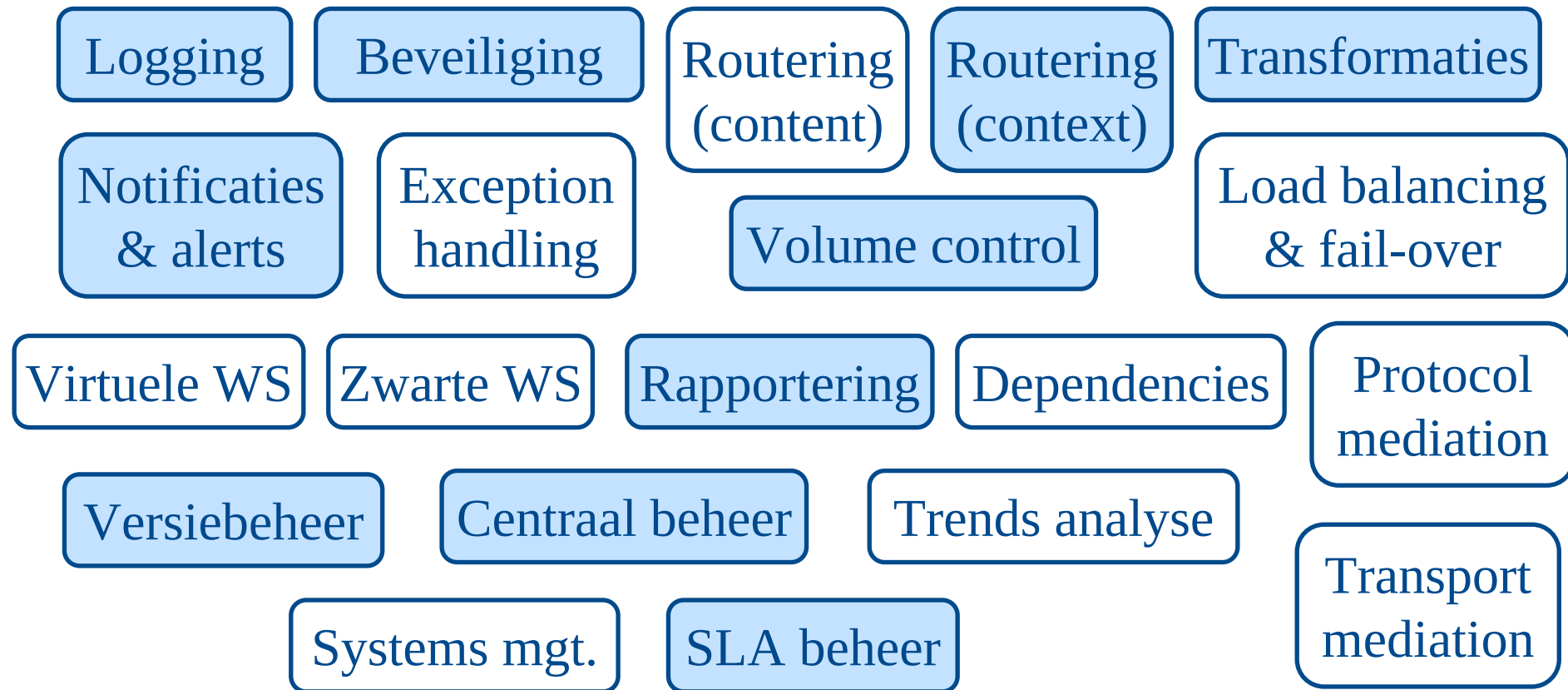


WSM @ Smals

- Lastenboek
 - WSM tool
 - UDDI Register
- Huidige en toekomstige WS gehost door Smals
- Fundament voor SOA



Conclusie



Conclusie

- Degelijk beheer is een must!
- WSM oplossing is nodig
- Fundament voor SOA
- Policies zijn belangrijk!
- Standaarden zijn belangrijk!
- De markt is nog in beweging
 - Maar we kunnen al aan de slag



Bedankt voor uw aandacht!



bert.vanhalst@smals.be



Glossarium

- API: Application Programming Interface
- BAM: Business Activity Monitoring
- Consumer: toepassing die een WS aanroept
- ESB: Enterprise Service Bus
- FTP: File Transfer Protocol
- J2EE: Java 2 Enterprise Edition
- JMS: Java Messaging Service
- PAP: Policy Administration Point
- PDP: Policy Decision Point
- PEP: Policy Enforcement Point
- PIP: Policy Information Point
- QoS: Quality of Service
- SAML: Security Assertion Markup Language



Glossarium

- SLA: Service Level Agreement
- SMTP: Simple Mail Transfer Protocol
- SNMP: Simple Network Management Protocol
- SOA: Service Oriented Architecture
- SOAP: Simple Object Access Protocol
- SSL: Secure Sockets Layer
- TLS: Transport Layer Security
- UDDI: Universal Description, Discovery and Integration
- WS: Web Service
- WSDL: Web Service Description Language
- WSM: Web Service Management
- XSLT: Extensible Stylesheet Language Transformations

