

# **IT Infrastruktur Monitoring mit Microsoft System Center Operations Manager**

Eine praktische Implementierung

Horw 03. März 2010

Reto Vogel, Christian Scherer

## Agenda

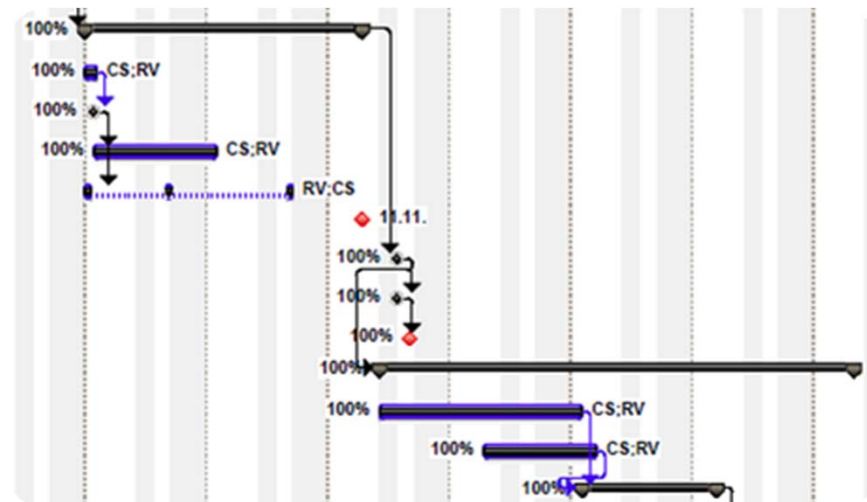
- Warum Monitoring?
- Vorgehen
- Anforderungen
- Implementation
- Fragen

## Wieso Monitoring?

- Ständige, automatisierte Systemüberwachung
  - Verfügbarkeit
  - Auslastung
  - Sicherheit
- Verbesserung der Verfügbarkeit durch proaktive Problemerkennung (und Problembehebung)
- Minimierung von manueller Administrationsaufgaben
- Zentrale Mess- und Logdaten Verwaltung
- Benchmarking, Analyse und Reporting
- Längerfristige Kosteneinsparung

## Vorgehen

- Vorabklärungen zwingend notwendig:
  - Monitored Objects anhand Geräteinventar festlegen
  - Mögliche Messpunkte definieren
  - Funktionale und nicht-funktionale Anforderungen klären
- Produktanalyse
  - Long-List erstellen
  - Produkte durch definierte Anforderungen kategorisieren → Short-List
- Evaluation
- Entscheid und Beschaffung
- Implementation
  - Proof of Concept
  - Konzeption
- Übergabe und Schulung









## Anforderungen

- Überwachung:
  - Serversysteme
    - Hardware
    - Betriebssysteme
    - Dienste
  - Netzwerkkomponenten
  - Anwendungsebene
  - Sonstige Geräte
- Bedienung des Systems
  - Verwaltung für gesamtes Monitoring in einer Konsole
- Sicherheitsanforderungen
  - Rollen- und Benutzergruppen
- Alarmierung
  - Über verschiedene Nachrichtenkanäle






## System Center Operations Manager (SCOM)

- Funktionen und Anforderungen deckungsgleich
- Erweiterbarkeit
- Individualisierung mit sogenannten Management Packs (MPs)
  - Sammlung von Überwachungsregeln mit vordefinierten Grenzwerten und Monitoren sowie Wissensdatenbank mit Informationen und Skripten für Problembehebung
  - Verfügbare Angebote
    - Microsoft eigene MPs für deren Produkte
    - Drittanbieter von MPs (bspw. für Dell Serverhardware)
  - Eigenentwicklungen




 Dell Windows Server (Scalable Edition)	4.0.0.114	Yes	03.02.2010 14:53:53	Dell Server MP v4.0 Scalable edition providing b.
 Dell Windows Server (Detailed Edition)	4.0.0.116	Yes	03.02.2010 14:53:59	Dell Server MP v4.0 Detailed Edition imports ove
 Dell Base Hardware Library	4.0.0.113	Yes	03.02.2010 14:53:48	Dell Base Hardware Library MP v4.0The Dell Bas
 Red Hat Operating System Library	6.1.7000.269	Yes	26.01.2010 11:23:07	Microsoft Red Hat Linux Operating System Libra
 Red Hat Enterprise Linux Server 5 Operating System	6.1.7000.269	Yes	26.01.2010 11:23:10	Microsoft Red Hat Enterprise Linux Server 5 Op
 Linux Operating System Library	6.1.7000.269	Yes	26.01.2010 11:23:06	Microsoft Linux Operating System Library: This f

## System Center Operations Manager (SCOM)

- Zugriff via Webinterface möglich (Konsole, Dashboard)
- Rollenbasiertes Sicherheitskonzept
  - Action Account Profile (für Überwachungsaufgaben durch Agenten)

 Notification Account	Windows account used by notification rules. Use this account's email address as email and instant message '...	06.01.2010 11:48:30
 Print Server Action Account		28.01.2010 11:26:00
 SQL Server Discovery Account	This account is used for all discovery of SQL Server (2000 and 2005) server role components.	28.01.2010 15:12:38
 SQL Server Monitoring Account	This account is used for all monitoring of SQL Server (2000 and 2005) monitoring where querying of SQL is r...	28.01.2010 15:12:38
 Unix Action Account	This account is used for low privilege Unix and Linux access.	26.01.2010 11:23:01

- Benutzerberechtigungen durch Rollen

<b>Profile: Administrator (1)</b>		
 Operations Manager Administrators		The Operations Manager Administrators user role is created at setup time and cannot be deleted. T...
<b>Profile: Advanced Operator (1)</b>		
 Operations Manager Advanced Operators		The Operations Manager Advanced Operators user role is created at setup time, is globally scoped ...
<b>Profile: Author (1)</b>		
 Operations Manager Authors		The Operations Manager Authors user role is created at setup time, is globally scoped and cannot b...

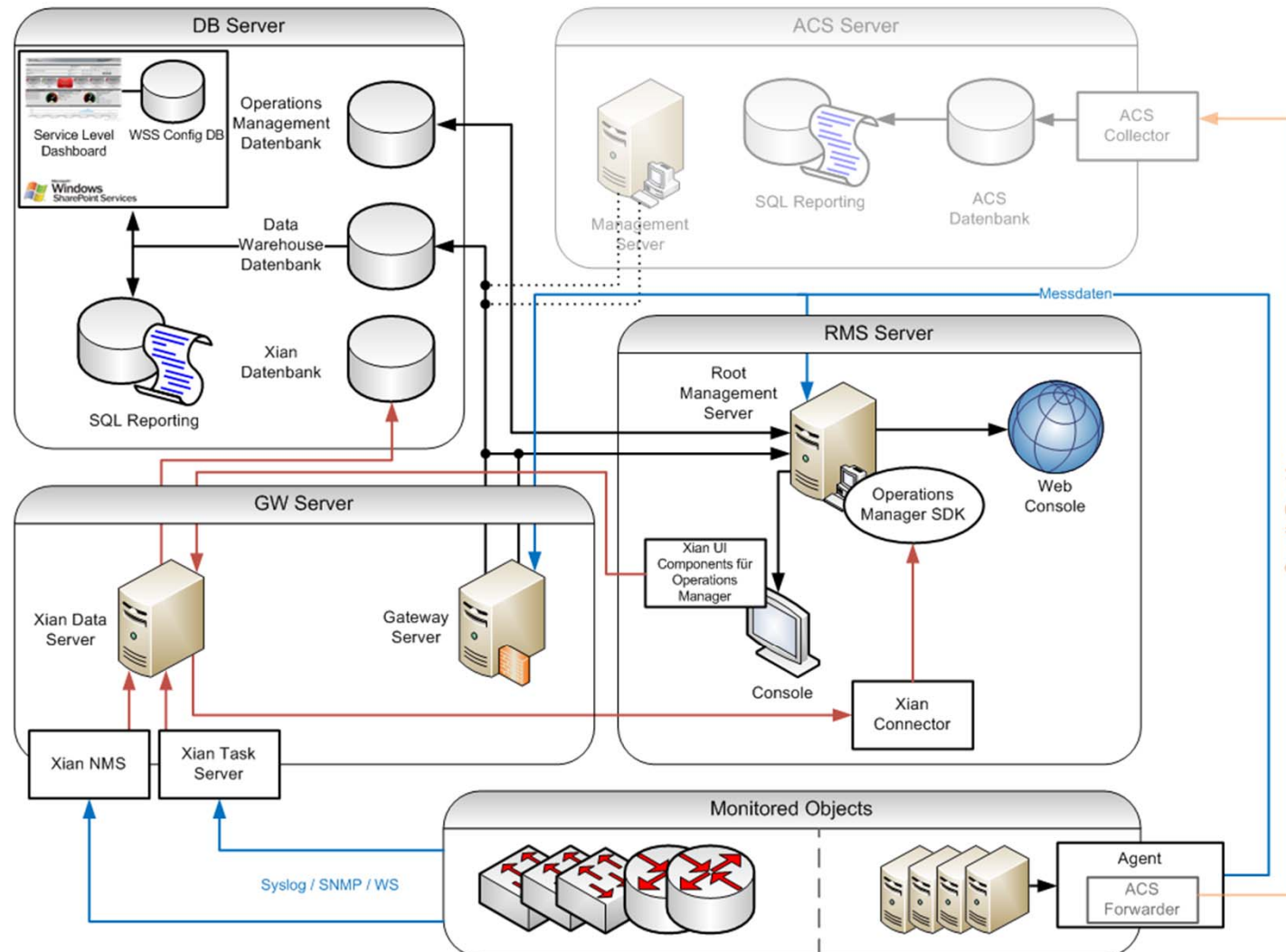
## Jalasoft Xian Network Manager for SCOM 2007 R2

- SCOM primär für Server- und Applikationsüberwachung – keine optimale Überwachung von Netzwerkgeräten möglich (keine vordefinierten Rulesets)
- Fehlende Funktion wird durch den Xian Network Manager von Jalasoft ergänzt
- Dank vorhandenem SDK und Connector, kann Xian problemlos in SCOM integriert werden (Administrative Aufgaben, Messdaten und Reports)
- Obwohl eigentlich zwei Produkte eingesetzt werden, erfolgt die Verwaltung ausschliesslich über die SCOM Konsole



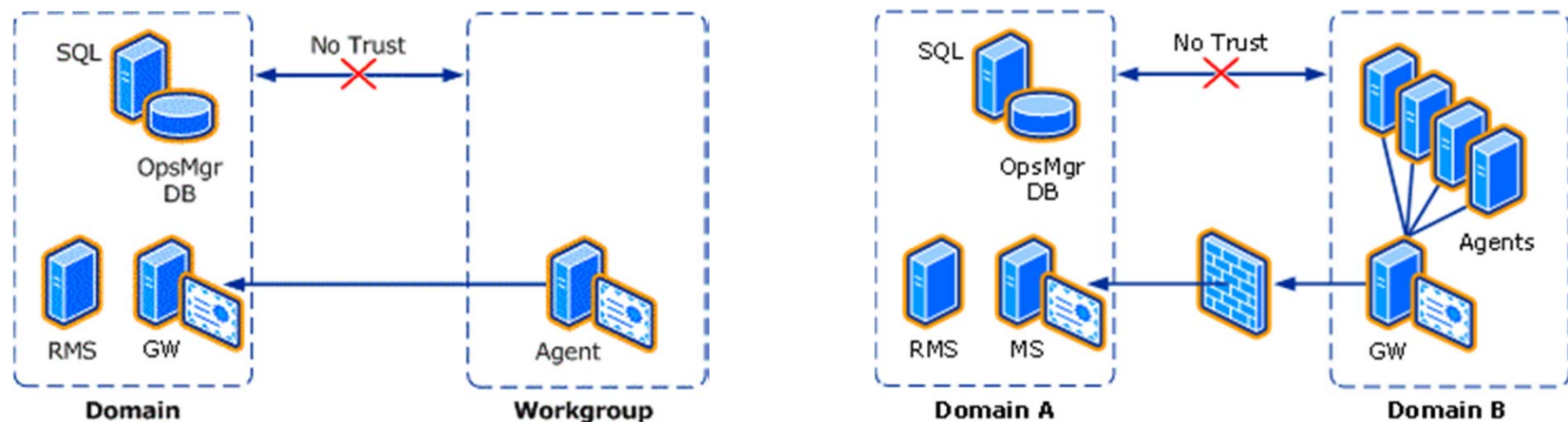


# Systemumgebung



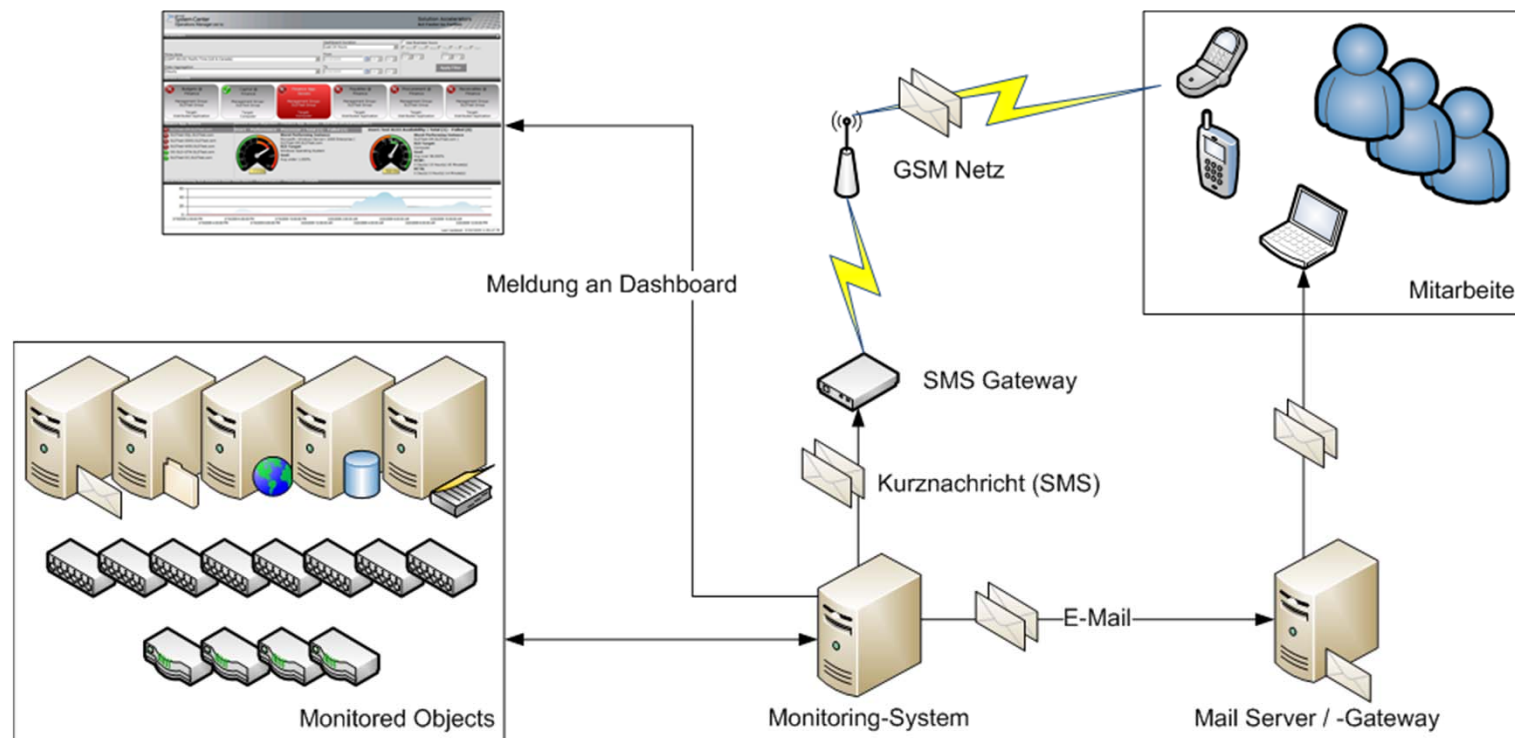
## Sicherheit

- Sämtliche Monitoring Tasks können durch eigene Service Action Accounts ausgeführt werden
- Zuständigkeitsbereiche werden mittels Benutzerrollen / Benutzerrechte definiert
- Kommunikation erfolgt über gesicherte Verbindungen
  - Kerberos als Authentifizierungsprotokoll innerhalb der Vertrauensgrenze
  - Kommunikation zwischen unterschiedlichen Vertrauensgrenzen (ohne Trust) über Zertifikate



## Alarmierung

- Alarmierung nach bspw. 2 Minuten Downtime einer Komponente
  - SMS Nachricht
  - E-Mail Notifikation



# Fragen

