Herzlich Willkommen

bei der Abschlusspräsentation der

Diplomarbeit von

Marcus Eichler

Korrelation von automatisierten Servicekontakten (Events) im Rahmen des Dienstleistungsangebotes Application Service Providing der DATEV im Bereich Leitungsüberwachung und Erstellung eines Prototypen

Aufgabensteller	Prof. Dr. A. Deinzer
Arbeit vorgelegt am	16.02.2004
durchgeführt bei	Fa. DATEV eG, Paumgartnerstraße 6-14 Design & Technik IT-Management
Betreuer	Stefan Nepf Dipl.-Betriebswirt (FH) Michael Schellenberger
Anschrift	Marcus Eichler Neumarkterstr. 34 90559 Burgthann

Teilnehmer

- Prof. Dr. Arnulf Deinzer (FH-Kempten)
- Michael Beer (DATEV)
- Stefan Nepf (DATEV)
- Marcus Eichler (FH-Kempten)

Agenda

1. Motivation
2. Analyse (Leitung)
3. Konzept
4. Implementation
5. Test
6. Resümee

Warum?

„*Ich kann nicht arbeiten*“

Wir helfen unseren Kunden!

Wie?

Fehler erkennen

Fehler beheben

Fehler vermeiden

Was ist nötig?

DATEV

Motivation	Analyse	Konzept	Implementierung	Test	Resümee

Wer Fehler **erkennen**, **beheben** und **vermeiden** will, muss:

- die Systeme des Kunden kennen — ständig
- diese dokumentieren — ständig
- die Systeme so konfigurieren, dass Fehler vermieden werden — ständig
- prüfen, ob die Systeme laufen — ständig
- prüfen, ob die Systeme noch funktionieren — ständig

Manuell NICHT möglich!

(Stand: Januar 2004)

Geschäftsbereich IT-Management

Kanzlei

- 309 betreute Kanzleien

- 1121 administrierte Server

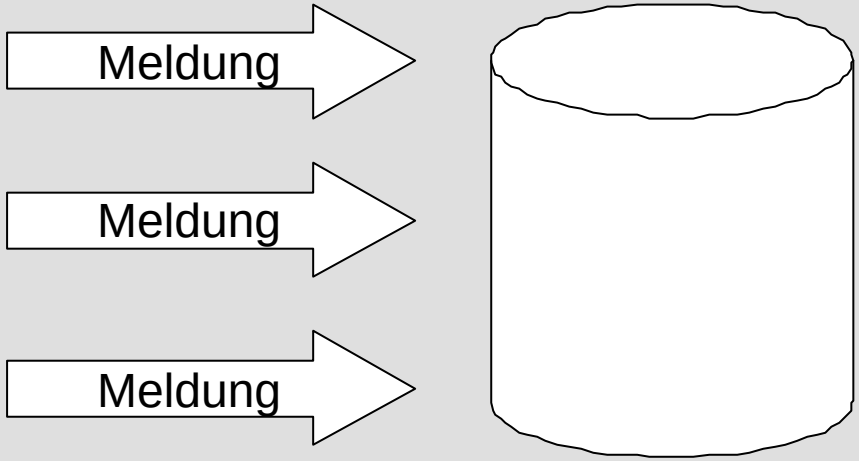
- 3902 verwaltete Clients

Leistungsumfang des IT Management

- Datensicherung
- Virenschutz
- Wartung der Systeme
- Systemmanagement
- Lizenzmanagement
- Administration
- Problemmanagement
- Änderungsmanagement
- Teamservice für produkt-übergreifende Unterstützung
- Hotline

Notwendig: Automatisierung von Serviceprozessen

Problem des automatisierten „Monitorings“



ca. 135.000 Meldungen im Monat

(Stand: Dezember 2003)

Notwendig: Korrelation von automatisierten Servicekontakten

Netzwerkstruktur

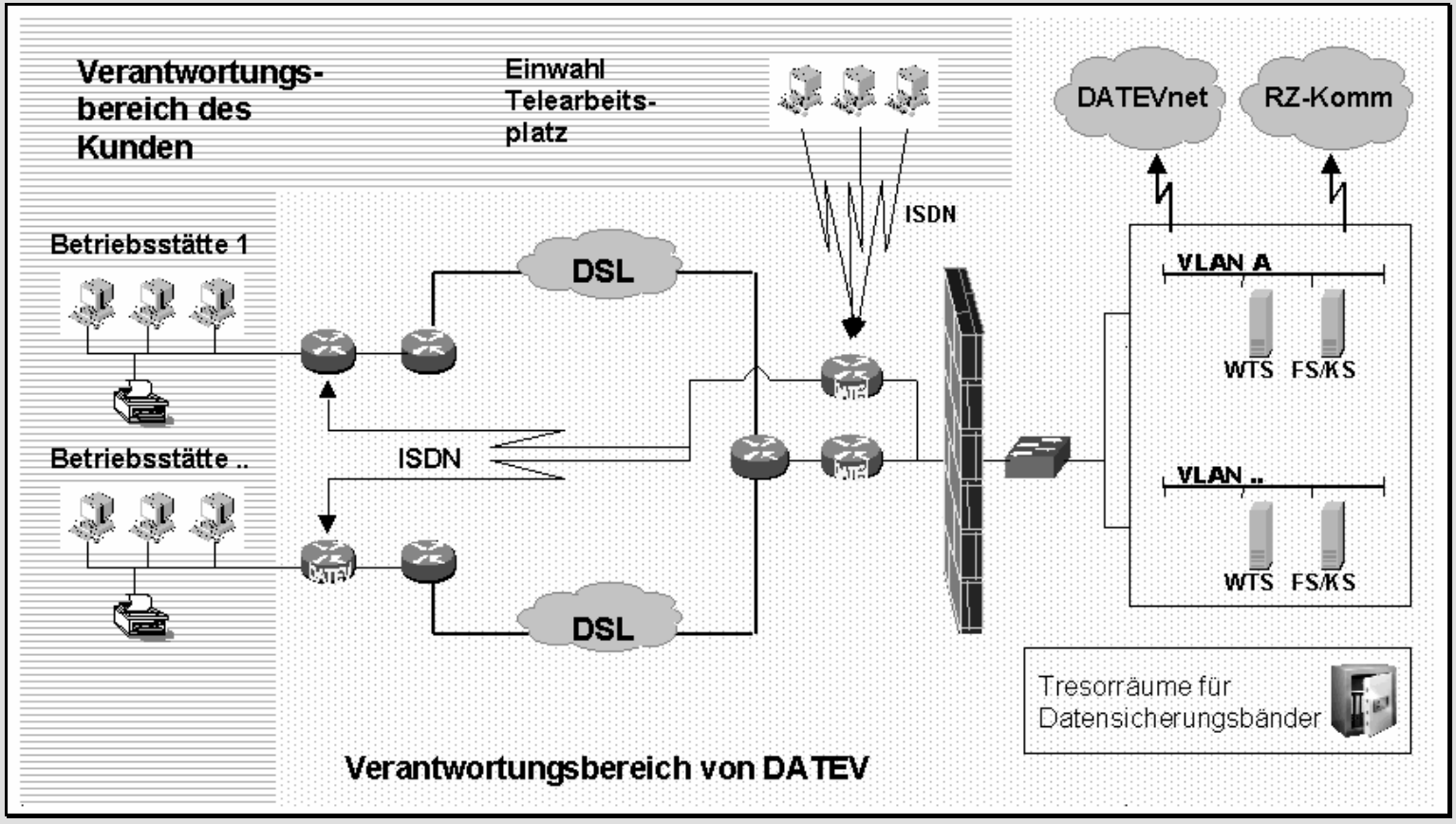


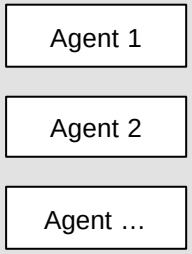
Abbildung : DATEVasp – Die technische Infrastruktur aus den Schulungsunterlagen Doc#: 29643

Ablauf

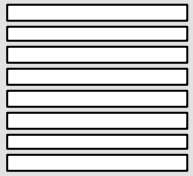
- Automatische Überwachung aller Systeme
- Meldung an eine zentrale Empfangsstation
- Verarbeitung der Meldung

Verarbeitungsprozess

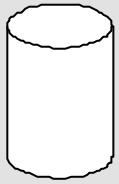
Kanzleisysteme



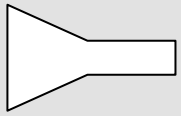
Meldungs-empfänger



Datenbank



Filter / Korrelation



Service Center

Überwachen | **Empfangen** | **Speichern** | **Verdichten** | **Ticket**

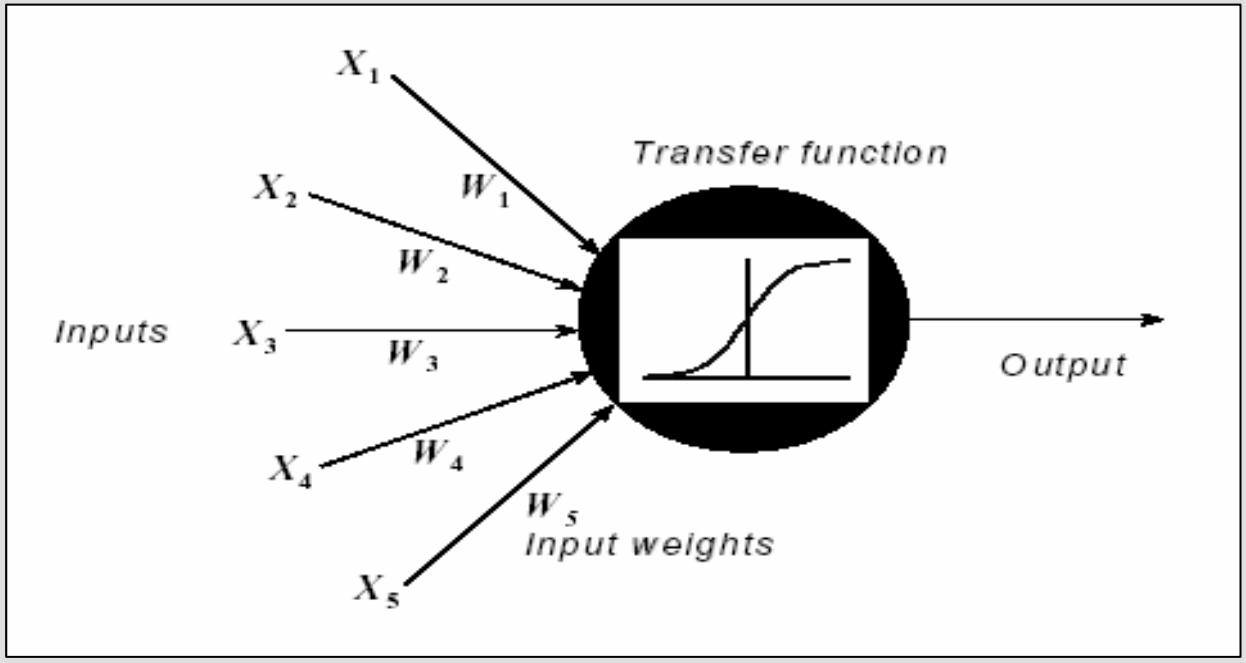
Verschiedene Ansätze

- Rule based Systems
- Model based Systems
- Case based Systems

- Dependency Graph
- Neural Network

Lösungsansatz: Neural Network

Erst bei mehreren Hinweisen auf einen Vorfall wird ein Ticket erzeugt

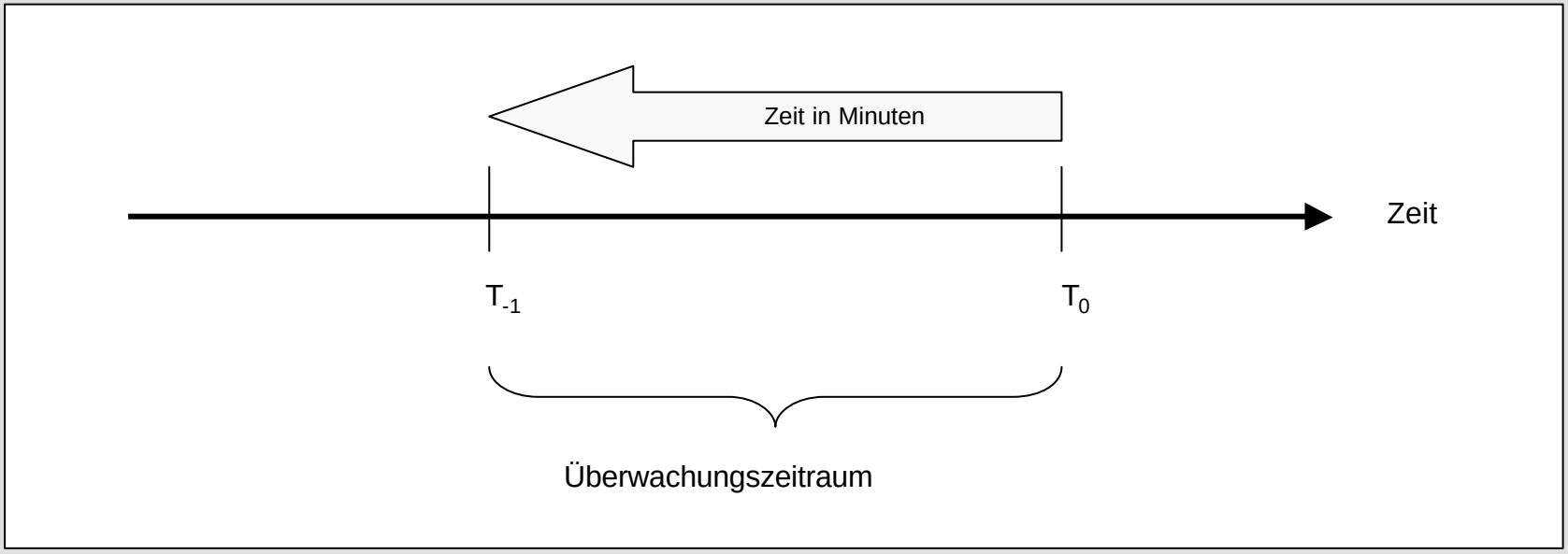


Notwendige Parameter

1. **„NewOID“** ⇨ **Neuron (Knoten)**
2. **„Prozent“** ⇨ **Gewichtung**
3. **„ZeitinMin“** ⇨ **Überwachungszeitraum**
4. **„Bezeichnung“** ⇨ **Information**

Überwachungszeitraum

„ZeitinMin“ = Überwachungszeitraum



Verknüpfung der Meldungen

Neue Meldung

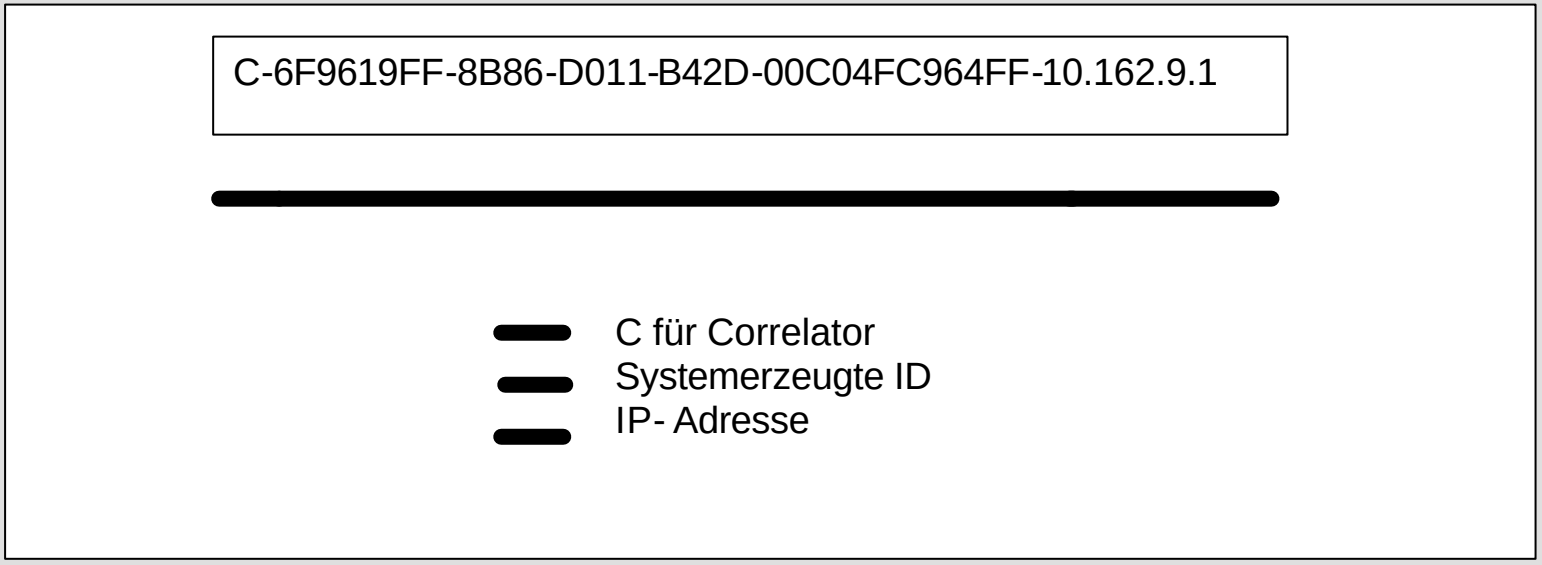
	UUID
Der Korrelator hat Auffälligkeiten in…. entdeckt	C-1234

Kopieren

Eingangssignale

	UUID	ParentUUID
Verlust eines ICMP-Packetes	abcd	C-1234
Datei konnte nicht gelesen werden	efgh	C-1234
Antwortzeit des Routers zu groß	ijkl	C-1234
Verlust eines ICMP-Packetes	mnop	C-1234

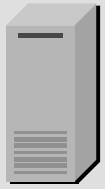
Erzeugung einer UUID



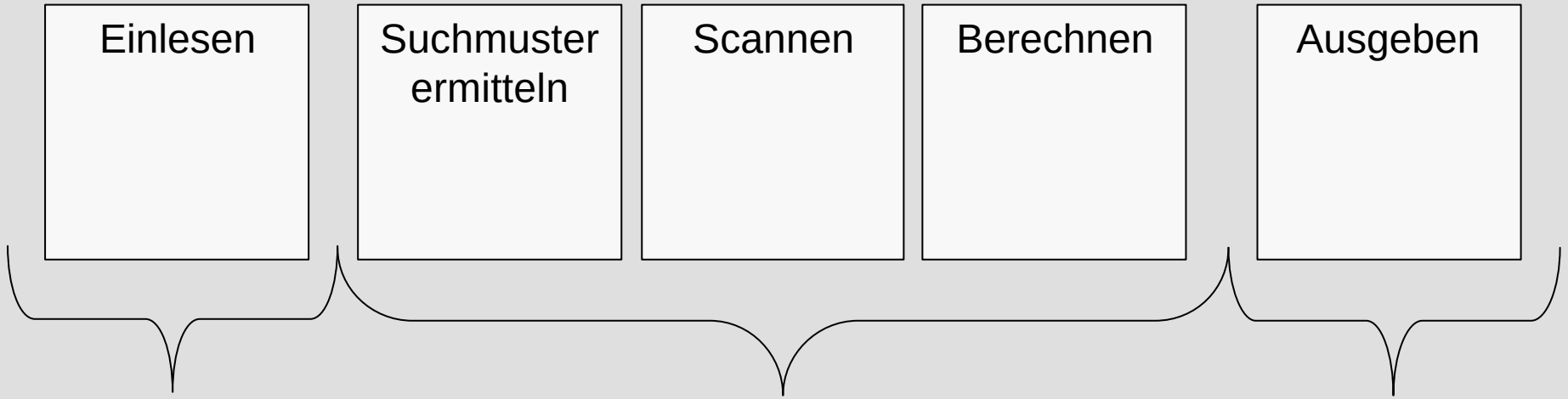
ToDo

1. **Vorbereitungen (Meldung des Agenten eindeutig machen)**
2. **Abfragealgorithmus entwickeln**
3. **Anpassungen am Troubleticketsystem**

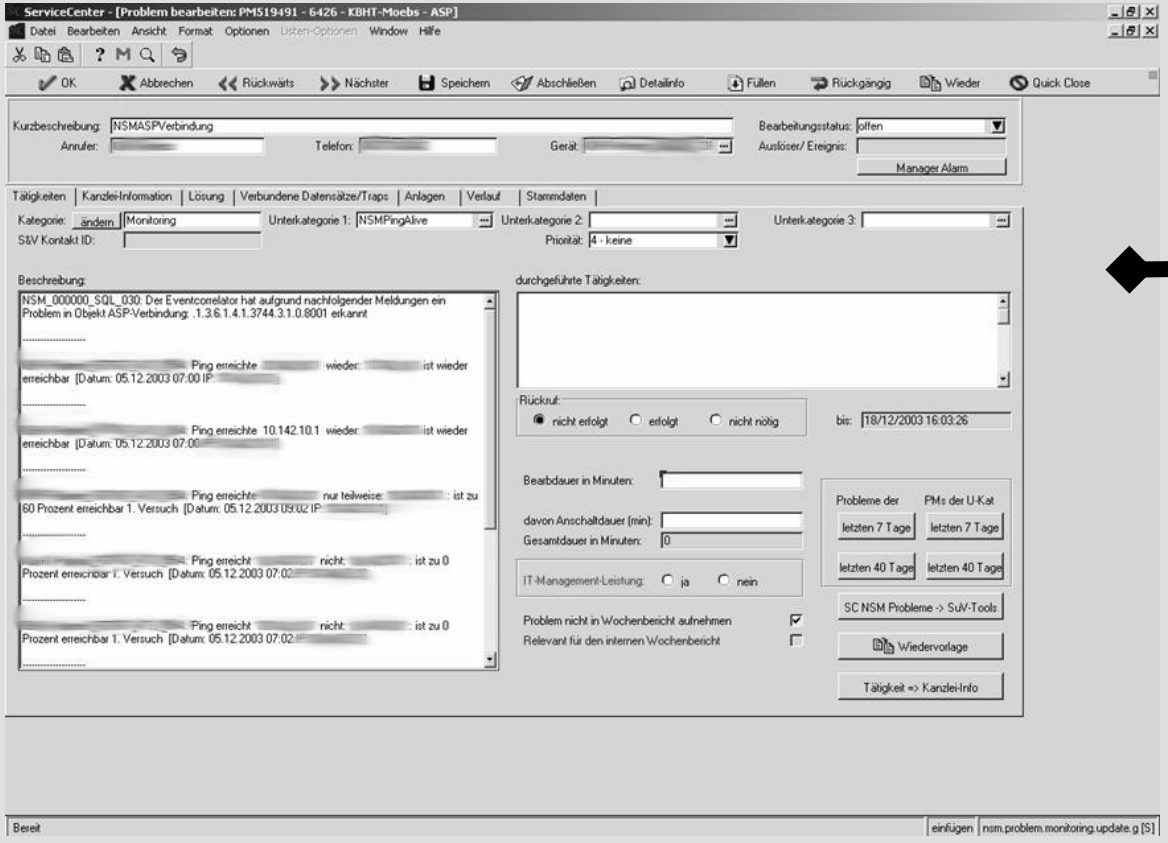
Meldungen eindeutig machen (Beispiel Cricket)

	Vorher	Nachher
	Schwellwert **überschritten** (OID1)	CPU ausgelastet (OID1)
	Schwellwert überschritten (OID1)	Bandbreite überschritten (OID 2)

Abfragealgorithmus entwickeln (gespeicherte Prozedur)



Das Troubleticketsystem anpassen



Array aller UUID´s

UUID1

UUID2

UUID3

…

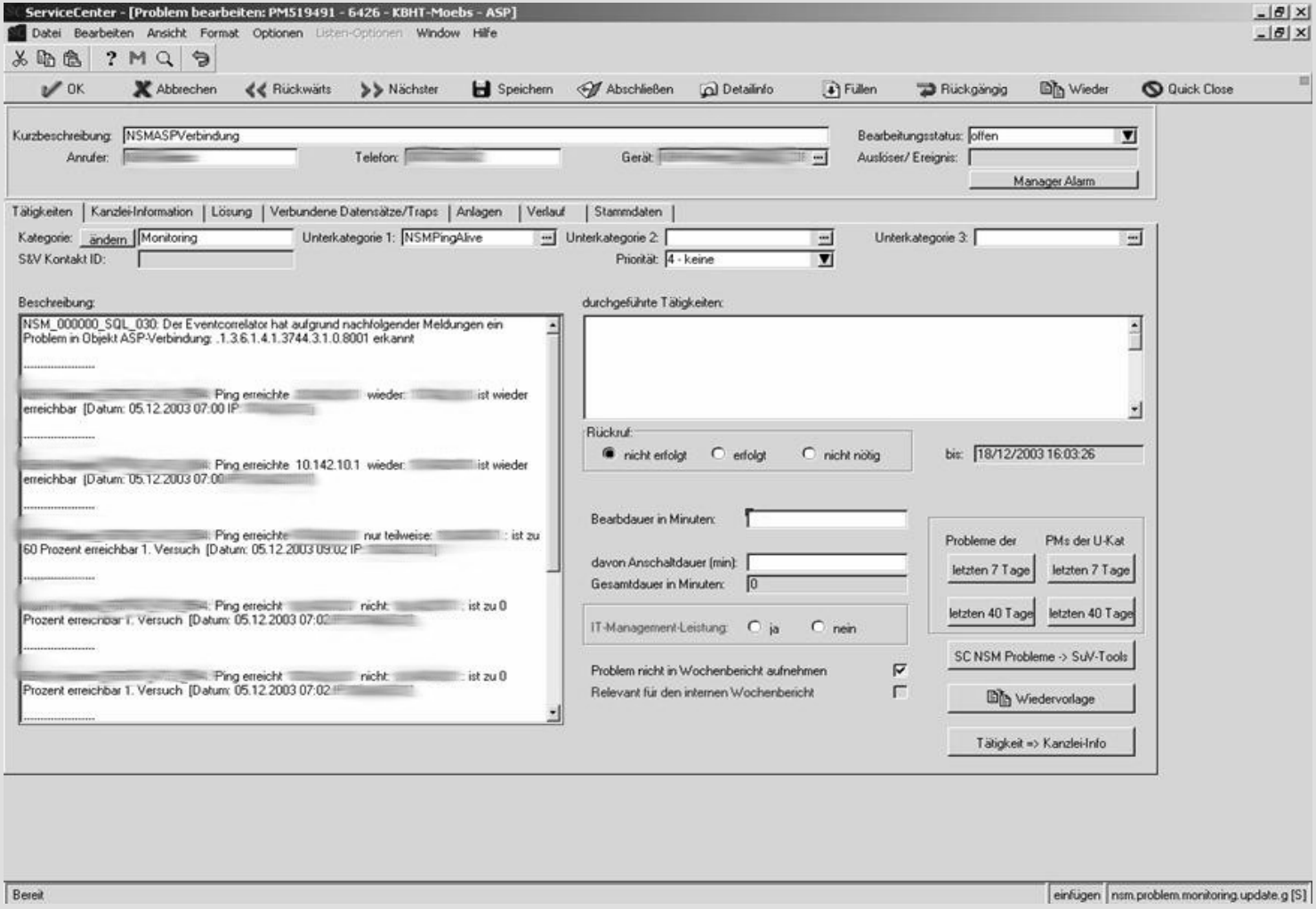
Funktionstest / Stresstest

- **Funktionstest**
  - **Mustererkennung und Verknüpfung**
  - **Weiterleitung der Meldungen**
- **Stresstest**
  - **Erhöhung der Anzahl zu korrelierender Meldungen**
  - **Erhöhung des Überwachungszeitraumes**

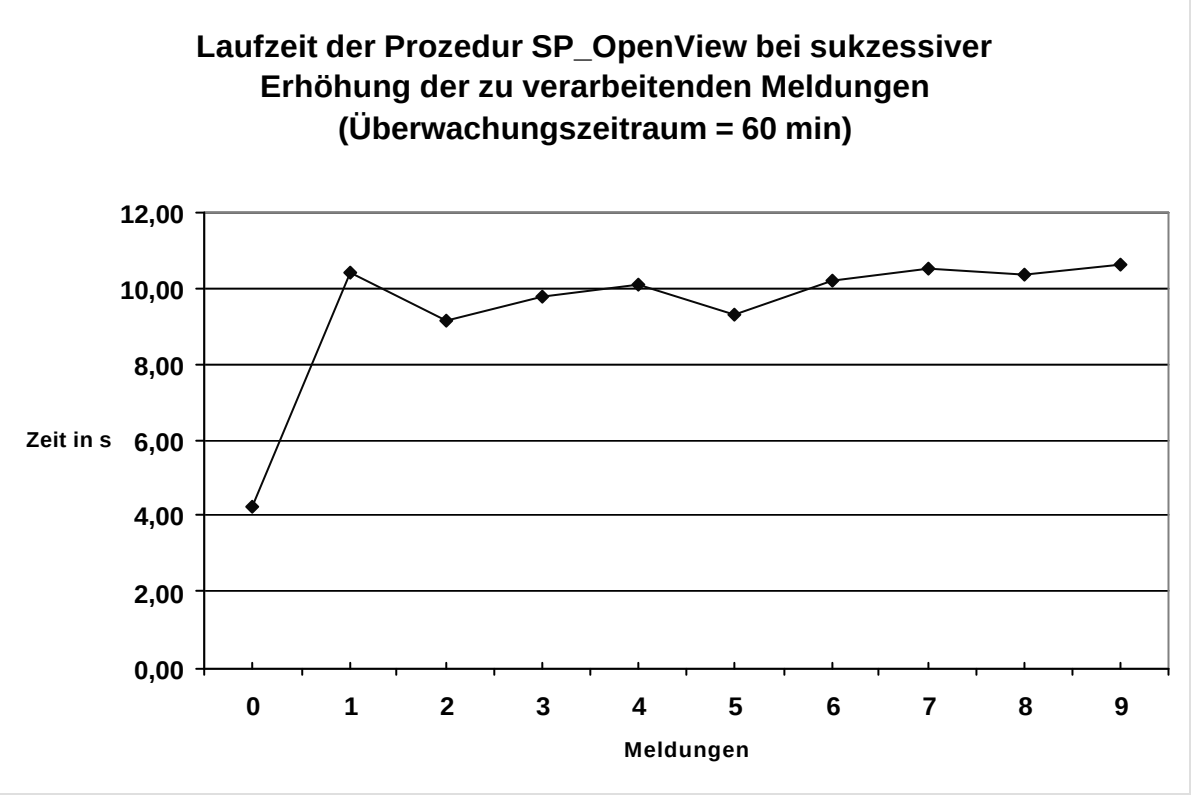
Funktionstest

Durch den Korrelator erstelltes Problemticket

Motivation	Analyse	Konzept	Implementierung	**Test**	Resümee

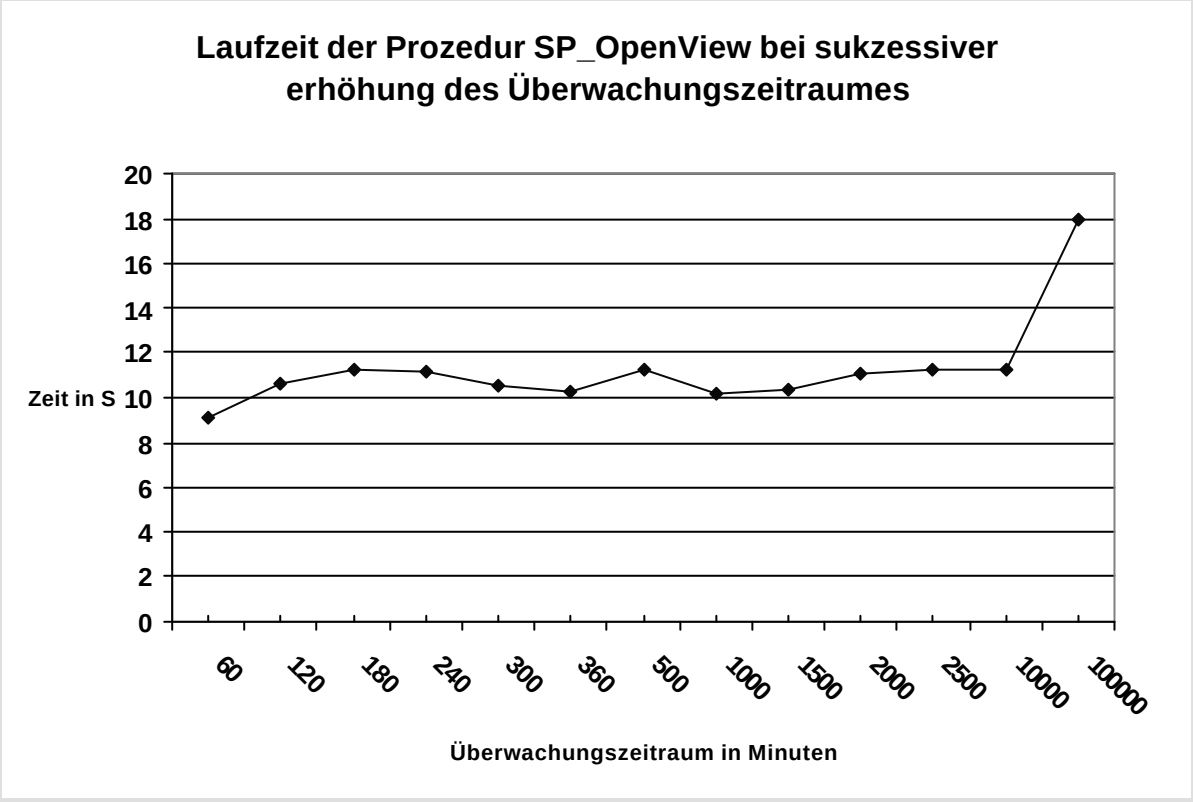


Erhöhung der Anzahl zu korrelierenden Meldungen



Ergebnis: Bei Täglich ca. 3500 Meldungen, reicht Performance aus

Erhöhung des Überwachungszeitraumes



Ergebnis: Korrelationen über mehrere Tage sind möglich

Beispiel (Leitungsüberwachung)

Trapname	**NewOID**	**Zeit/ Min**	**Prozent**	**Bezeichnung**
NSMPingNichtErreichbar	.1.3.6.1.4.1.3744.3.1.11710	60	35	ASP-Verbindung
NSMPingWiederErreichbar	.1.3.6.1.4.1.3744.3.1.11710	60	10	ASP-Verbindung
NSMPingTeilweiseErreichbar	.1.3.6.1.4.1.3744.3.1.11710	60	35	ASP-Verbindung
NSMAliveOKPingTeilweise	.1.3.6.1.4.1.3744.3.1.11710	60	35	ASP-Verbindung
NSMAliveOKPingFehler	.1.3.6.1.4.1.3744.3.1.11710	60	35	ASP-Verbindung
NSMAliveWiederErreichbar	.1.3.6.1.4.1.3744.3.1.11710	60	10	ASP-Verbindung
NSMAliveNichtErreichbar	.1.3.6.1.4.1.3744.3.1.11710	60	100	ASP-Verbindung
NSMAliveNichtErreichbarShare	.1.3.6.1.4.1.3744.3.1.11710	60	100	ASP-Verbindung
NSM_Interface_Ethernet_überschritten	.1.3.6.1.4.1.3744.3.1.11710	60	100	ASP-Verbindung

Resultat in 24 std. → **Korrelationsfaktor hier 18 : 1**

Resümee

- Verringerung der Ticketanzahlen
- Reduzieren des Aufwandes
- Überblick bewahren
- Hinweise behalten (Analyse möglich)

- Fragen?

Vielen Dank für Ihre Aufmerksamkeit

Marcus Eichler