

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

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

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

„Ich kann nicht arbeiten“



Wir helfen unseren Kunden!

Wie?



Motivation	Analyse	Konzept	Implementierung	Test	Resümee
------------	---------	---------	-----------------	------	---------

Fehler erkennen

Fehler beheben

Fehler vermeiden

Was ist nötig?



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!

Motivation	Analyse	Konzept	Implementierung	Test	Resümee
------------	---------	---------	-----------------	------	---------

(Stand: Januar 2004)

Geschäftsbereich IT-Management



Kanzlei

- 309 betreute Kanzleien



- 1121 administrierte Server



- 3902 verwaltete Clients

Leistungsumfang des IT Management



Motivation	Analyse	Konzept	Implementierung	Test	Resümee
------------	---------	---------	-----------------	------	---------

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



Automatisierung von Serviceprozessen

Problem des automatisierten „Monitorings“

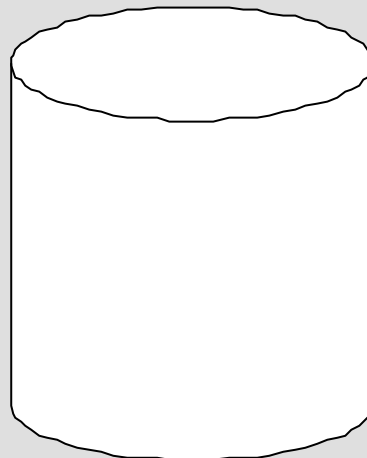


Motivation	Analyse	Konzept	Implementierung	Test	Resümee
------------	---------	---------	-----------------	------	---------

Meldung

Meldung

Meldung



ca. 135.000 Meldungen im Monat
(Stand: Dezember 2003)

Notwendig:

Korrelation von automatisierten Servicekontakten

Netzwerkstruktur



Motivation	Analyse	Konzept	Implementierung	Test	Resümee
------------	---------	---------	-----------------	------	---------

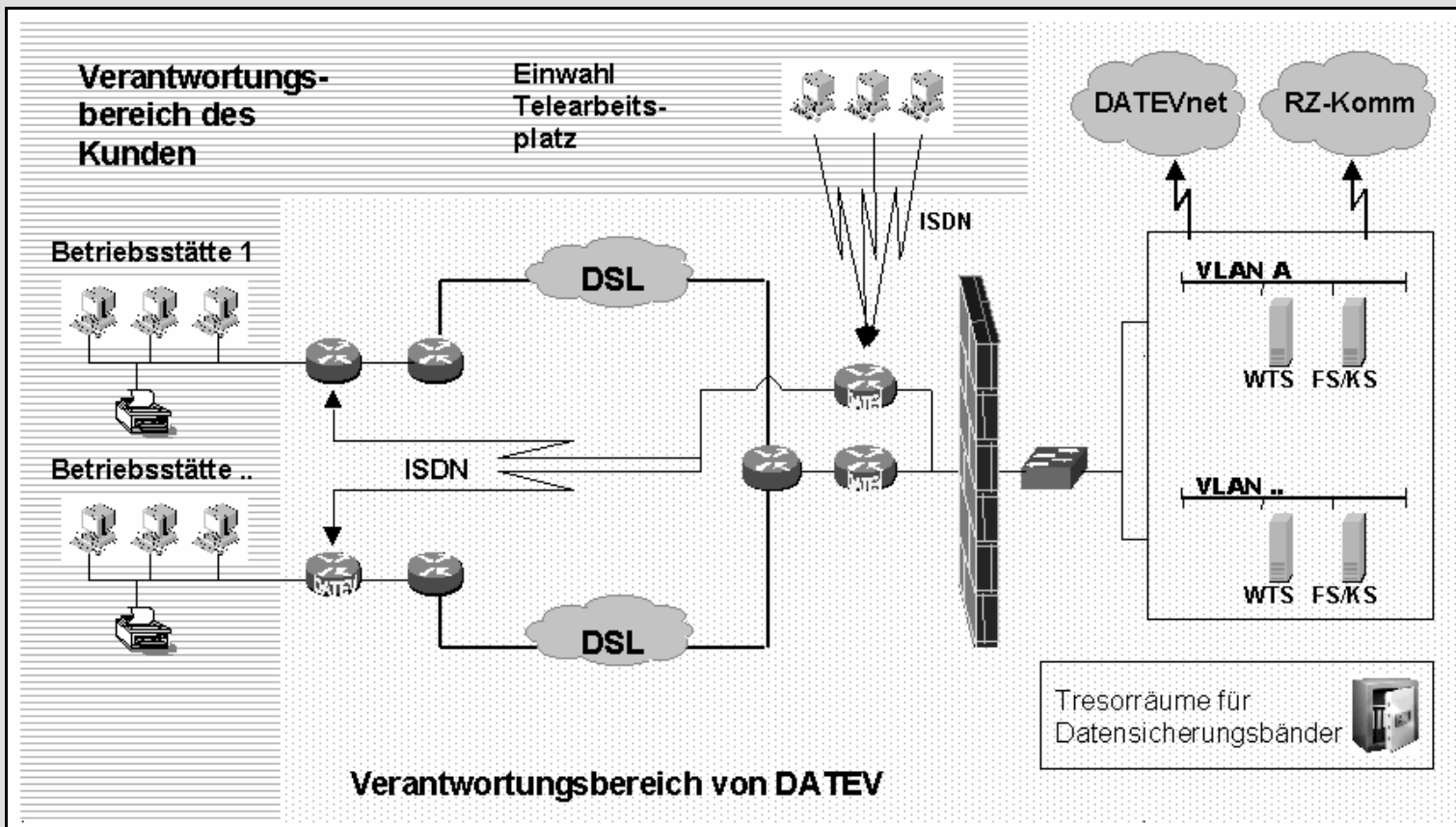


Abbildung : DATEVasp – Die technische Infrastruktur aus den Schulungsunterlagen Doc#: 29643

Motivation	Analyse	Konzept	Implementierung	Test	Resümee
------------	---------	---------	-----------------	------	---------

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

Verarbeitungsprozess



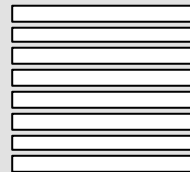
Kanzleisysteme

Agent 1

Agent 2

Agent ...

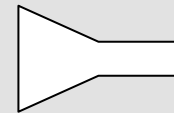
Meldungs-
empfänger



Datenbank



Filter /
Korrelation



Service
Center

Überwachen

Empfangen

Speichern

Verdichten

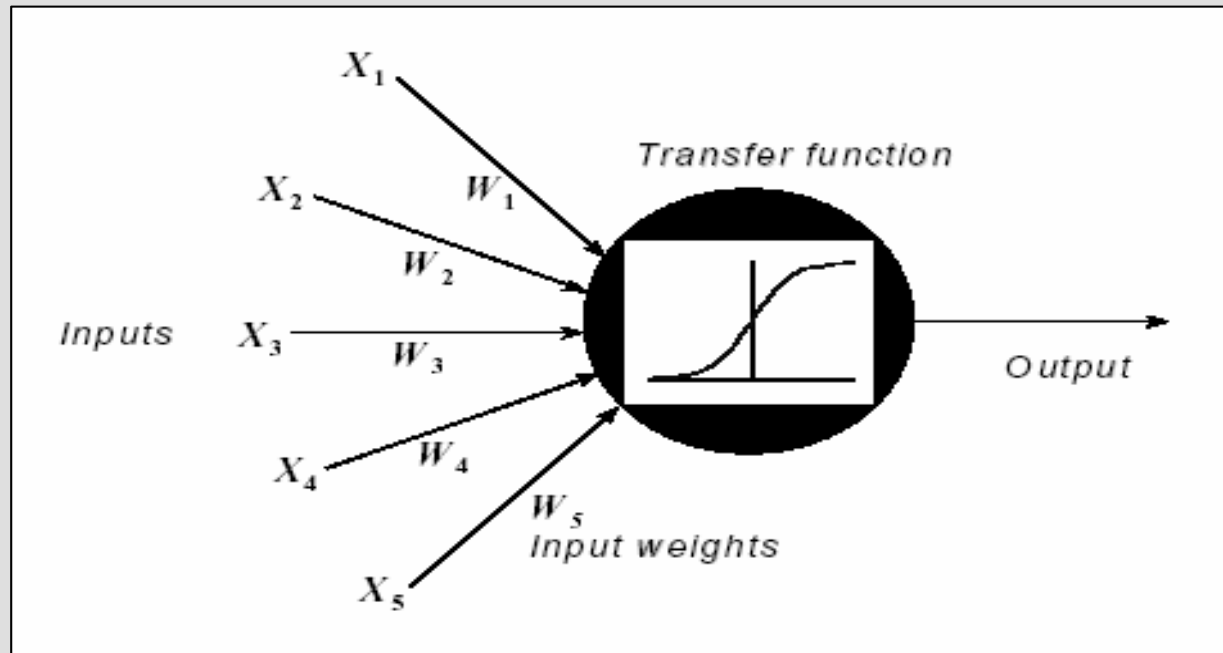
Ticket

Motivation	Analyse	Konzept	Implementierung	Test	Resümee
------------	---------	----------------	-----------------	------	---------

- 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



Motivation	Analyse	Konzept	Implementierung	Test	Resümee
------------	---------	----------------	-----------------	------	---------

1. „NewOID“



Neuron (Knoten)

2. „Prozent“



Gewichtung

3. „ZeitinMin“



Überwachungszeitraum

4. „Bezeichnung“



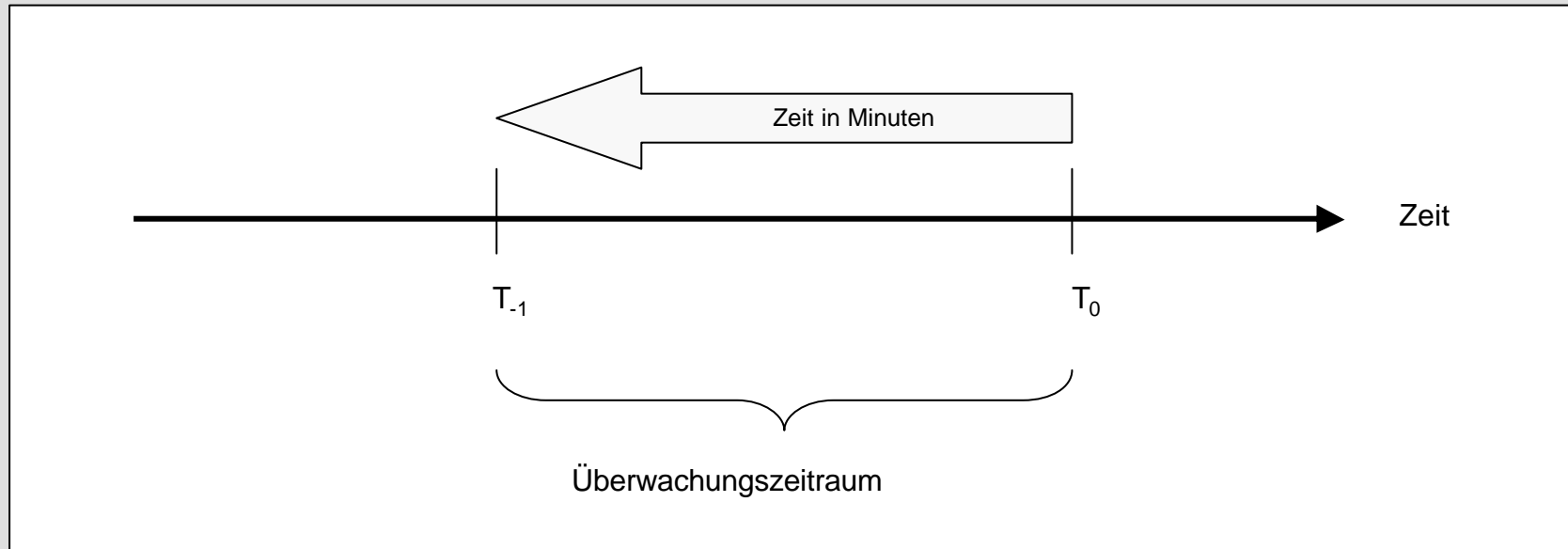
Information

Überwachungszeitraum



Motivation	Analyse	Konzept	Implementierung	Test	Resümee
------------	---------	----------------	-----------------	------	---------

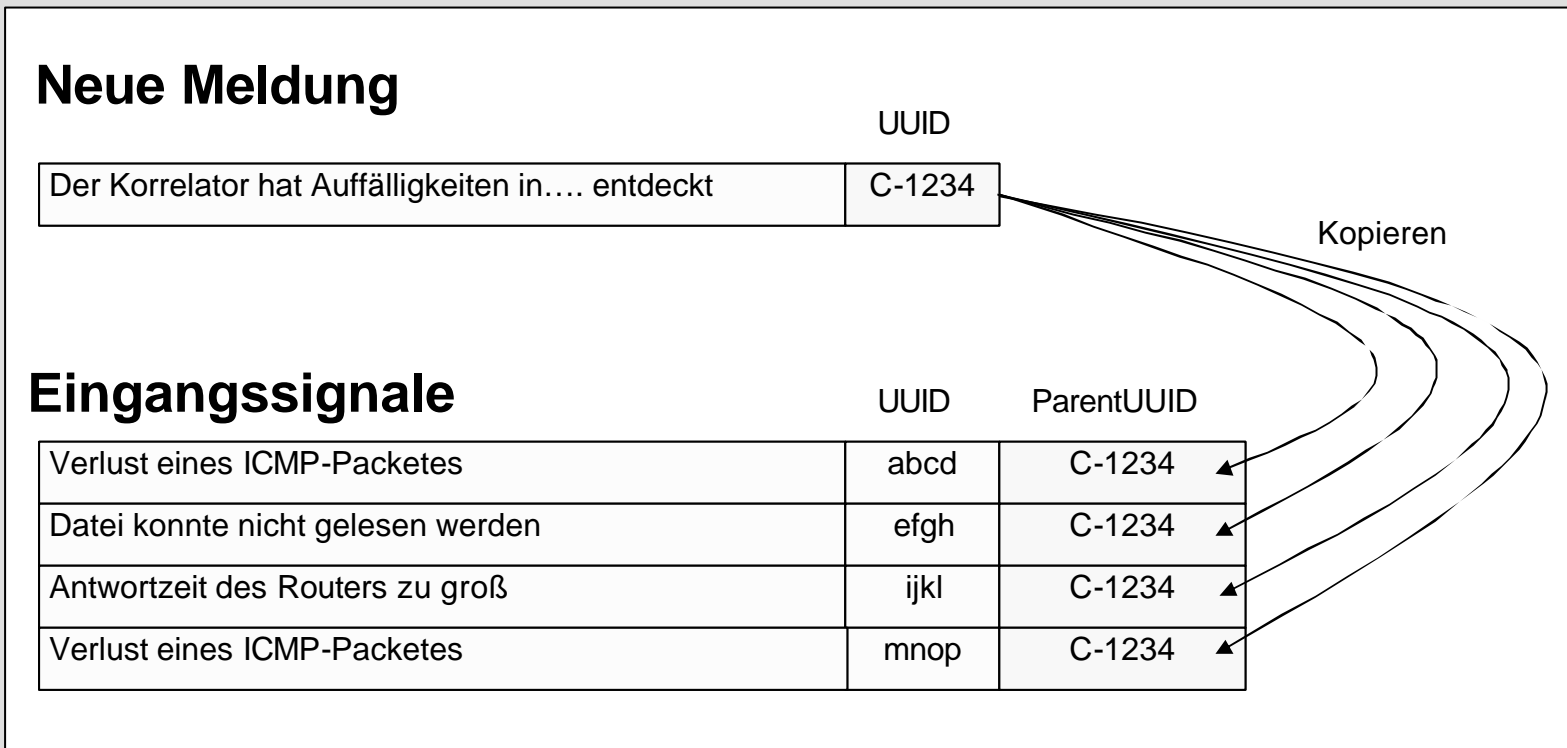
„Zeit in Min“ = Überwachungszeitraum



Verknüpfung der Meldungen



Motivation	Analyse	Konzept	Implementierung	Test	Resümee
------------	---------	----------------	-----------------	------	---------



Erzeugung einer UUID



Motivation	Analyse	Konzept	Implementierung	Test	Resümee
------------	---------	----------------	-----------------	------	---------

C-6F9619FF-8B86-D011-B42D-00C04FC964FF-10.162.9.1



- C für Correlator
- Systemerzeugte ID
- IP- Adresse

Motivation	Analyse	Konzept	Implementierung	Test	Resümee
------------	---------	---------	------------------------	------	---------

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

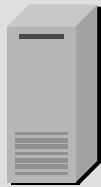
Meldungen eindeutig machen (Beispiel Cricket)



Motivation	Analyse	Konzept	Implementierung	Test	Resümee
------------	---------	---------	-----------------	------	---------

Vorher

Nachher



Schwellwert **überschritten**
(OID1)

CPU ausgelastet
(OID1)



Schwellwert überschritten
(OID1)

Bandbreite überschritten
(OID 2)

Abfragealgorithmus entwickeln (gespeicherte Prozedur)



Motivation	Analyse	Konzept	Implementierung	Test	Resümee
------------	---------	---------	------------------------	------	---------

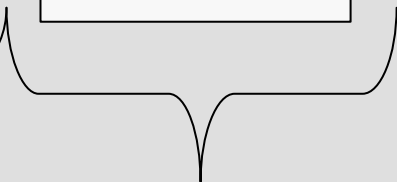
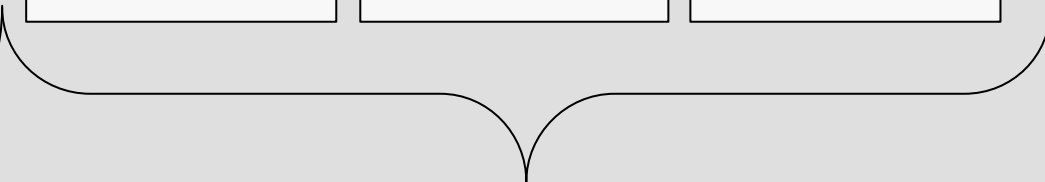
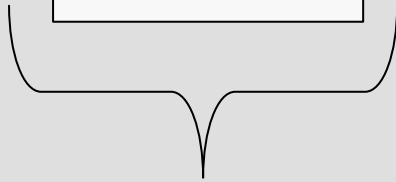
Einlesen

Suchmuster
ermitteln

Scannen

Berechnen

Ausgeben



Eingabe

Verarbeitung

Ausgabe

Das Troubleshootingsystem anpassen



Motivation	Analyse	Konzept	Implementierung	Test	Resümee
------------	---------	---------	------------------------	------	---------

ServiceCenter - [Problem bearbeiten: PMS19491 - 6426 - KBHT-Moebis - ASP]

Kurzbeschreibung: NSMASPV-Verbindung

Anrufer: [redacted] Telefon: [redacted] Gerät: [redacted] Bearbeitungstatus: offen

Auslöser/ Ereignis: Manager Alarm

Tätigkeiten | Kanzlei-Information | Lösung | Verbundene Datensätze/Traps | Anlagen | Verlauf | Stammdaten

Kategorie: ändern | Monitoring | Unterkategorie 1: NSMPingAlive | Unterkategorie 2: | Unterkategorie 3: |

STV Kontakt ID: | Priorität: 4 - keine

Beschreibung:
NSM_000000_SQL_030: Des Eventcorrelator hat aufgrund nachfolgender Meldungen ein Problem in Objekt ASP-Verbindung: .1.3.6.1.4.1.3744.3.1.0.8001 erkannt

durchgeführte Tätigkeiten:

Rückruf:
 nicht erfolgt erfolgt nicht nötig bis: 18/12/2003 16:03:26

Bearbdauer in Minuten: |
davon Anschalldauer (min): |
Gesamtdauer in Minuten: 0

IT-Management-Leistung: ja nein

Problem nicht in Wochenbericht aufnehmen
Relevant für den internen Wochenbericht

Probleme der FMs der U-Kat:
letzten 7 Tage | letzten 7 Tage
letzten 40 Tage | letzten 40 Tage

SC NSM Probleme -> SuV-Tools
Wiedervorlage
Tätigkeit => Kanzlei-Info

Array aller UUID's

- UUID1
- UUID2
- UUID3
- ...

Motivation	Analyse	Konzept	Implementierung	Test	Resümee
------------	---------	---------	-----------------	-------------	---------

- **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
------------	---------	---------	-----------------	-------------	---------

ServiceCenter - [Problem bearbeiten: PM519491 - 6426 - KBHT-Moebis - ASP]

Datei Bearbeiten Ansicht Format Optionen Listen-Optionen Window Hilfe

OK Abbrechen Rückwärts Nächster Speichern Abschließen Detailinfo Füllen Rückgängig Wieder Quick Close

Kurzbeschreibung: NSMASPV-Verbindung Bearbeitungsstatus: offen
Anrufer: Telefon: Gerät: Auslöser/ Ereignis: Manager Alarm

Tätigkeiten Kanzlei-Information Lösung Verbundene Datensätze/Traps Anlagen Verlauf Stammdaten

Kategorie: ändern | Monitoring Unterkategorie 1: NSMPingAlive Unterkategorie 2: Unterkategorie 3:
S&V Kontakt ID: Priorität: 4 - keine

Beschreibung:
NSM_000000_SQL_030: Der Eventkorrelator hat aufgrund nachfolgender Meldungen ein Problem in Objekt ASP-Verbindung: 1.3.6.1.4.1.3744.3.1.0.8001 erkannt
.....
..... Ping erreichte wieder: ist wieder erreichbar [Datum: 05.12.2003 07:00 IP:]
.....
..... Ping erreichte 10.142.10.1 wieder: ist wieder erreichbar [Datum: 05.12.2003 07:00]
.....
..... Ping erreichte nur teilweise: ist zu 60 Prozent erreichbar 1. Versuch [Datum: 05.12.2003 09:02 IP:]
.....
..... Ping erreicht nicht: ist zu 0 Prozent erreichbar 1. Versuch [Datum: 05.12.2003 07:02]
.....
..... Ping erreicht nicht: ist zu 0 Prozent erreichbar 1. Versuch [Datum: 05.12.2003 07:02]

durchgeführte Tätigkeiten:

Rückruf:
 nicht erfolgt erfolgt nicht nötig bis: 18/12/2003 16:03:26

Bearbdauer in Minuten: Probleme der PMs der U-Kat
davon Anschaltdauer (min): letzten 7 Tage letzten 7 Tage
Gesamtdauer in Minuten: 0 letzten 40 Tage letzten 40 Tage

IT-Management-Leistung: ja nein SC NSM Probleme -> SuV-Tools

Problem nicht in Wochenbericht aufnehmen
Relevant für den internen Wochenbericht

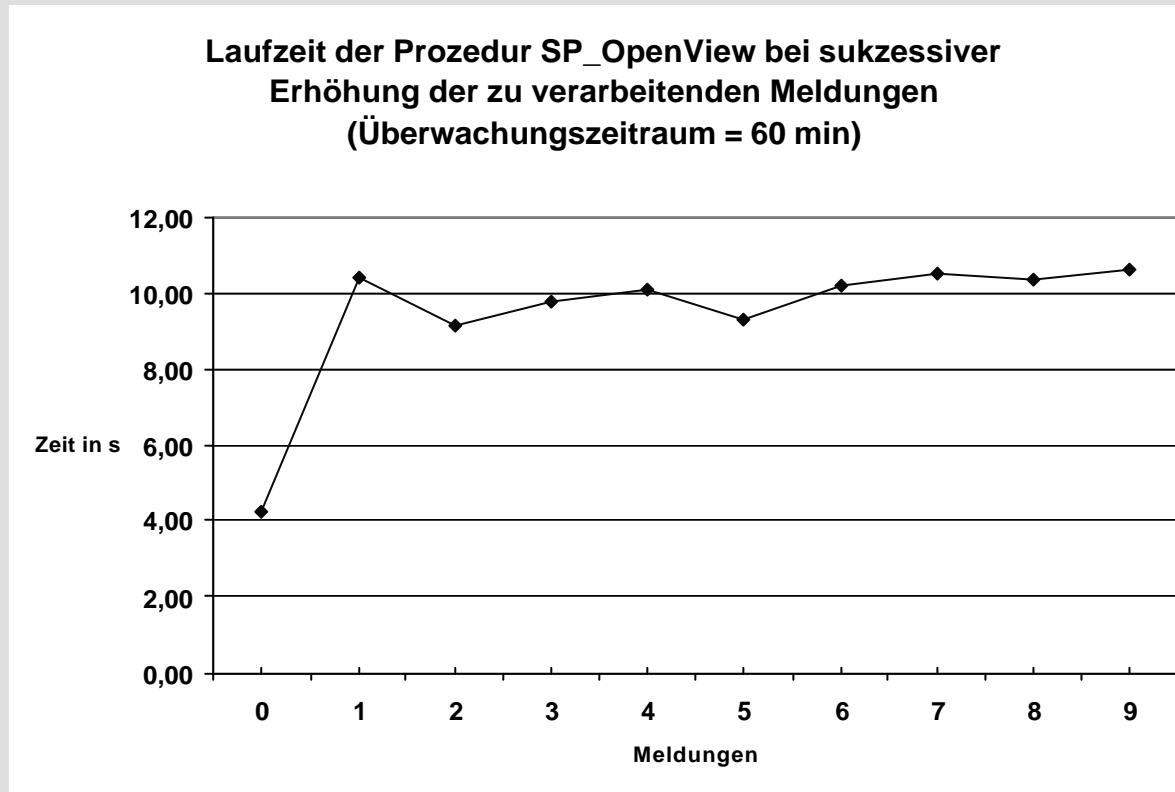
Wiedervorlage
Tätigkeit => Kanzlei-Info

Bereit einfügen nsm.problem.monitoring.update.g [S]

Erhöhung der Anzahl zu korrelierenden Meldungen



Motivation	Analyse	Konzept	Implementierung	Test	Resümee
------------	---------	---------	-----------------	-------------	---------

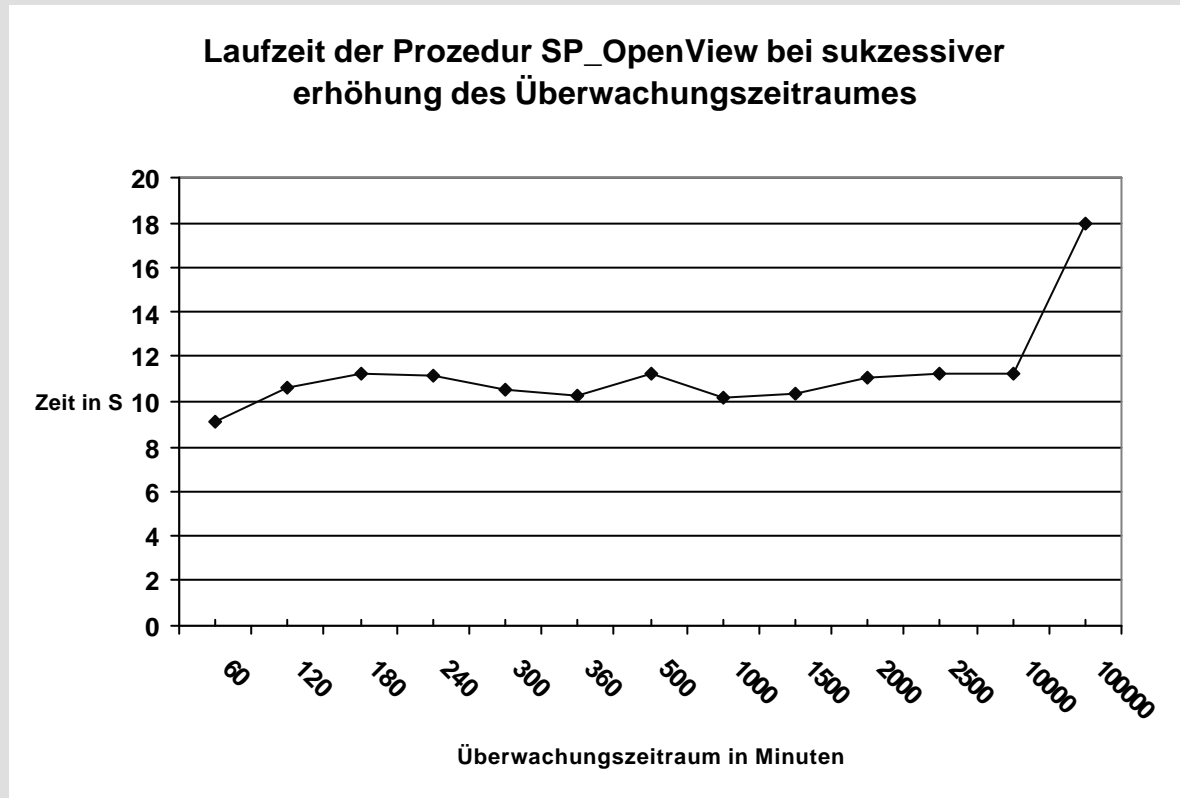


Bei Täglich ca. 3500 Meldungen, reicht Performance aus

Erhöhung des Überwachungszeitraumes



Motivation	Analyse	Konzept	Implementierung	Test	Resümee
------------	---------	---------	-----------------	-------------	---------



Korrelationen über mehrere Tage sind möglich

Beispiel (Leistungsüberwachung)



Motivation	Analyse	Konzept	Implementierung	Test	Resümee
------------	---------	---------	-----------------	-------------	---------

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

Motivation	Analyse	Konzept	Implementierung	Test	Resümee
------------	---------	---------	-----------------	------	----------------

Verringerung der Ticketanzahlen

Reduzieren des Aufwandes

Überblick bewahren

Hinweise behalten (Analyse möglich)

Fragen?



- Fragen?

Vielen Dank für Ihre
Aufmerksamkeit

Marcus Eichler