HOCHSCHULE
MITTWEIDA
UNIVERSITY OF
APPLIED SCIENCES

DIPLOMARBEIT

Herr Ing.
Christoph Voraberger

Konzeption eines Monitoring-systems für ein IT-Unterneh-mensnetzwerk

Mittweida, 2017

Fakultät Computer- und Biowissenschaften

DIPLOMARBEIT

Konzeption eines Monitoring-systems für ein IT Unterneh-mensnetzwerk

Autor:
Herr Ing.

Christoph Voraberger

Studiengang:
Technische Informatik

Seminargruppe:
KT13WIA-F

Erstprüfer:
Prof. Dr.-Ing Olaf Hagenbruch

Zweitprüfer:
Dipl. Ing. (FH) Markus Leuchtenmüller

Einreichung:
Mittweida, 10.07.2017

Verteidigung/Bewertung:
Mittweida, 2017

Faculty: Applied Computer- & Biosciences

DIPLOMA THESIS

Conception of a monitoring-system for an IT corporate network

author:
Mr. Ing.

Christoph Voraberger

course of studies:
Technical Informatics

seminar group:
KT13WIA-F

first examiner:
Prof. Dr.-Ing Olaf Hagenbruch

second examiner:
Dipl. Ing. (FH) Markus Leuchtenmüller

submission:
Mittweida, 10.07.2017

defence/ evaluation:
Mittweida, 2017

Bibliografische Beschreibung:

Voraberger, Christoph:
Konzeption und Einführung eines zentralen IT-Monitoringsystems. - 2017. –
Verzeichnisse: 10 Seiten, Inhalt: 83 Seiten, Anhänge 14 Seiten.
Mittweida, Hochschule Mittweida, Fakultät CB, Diplomarbeit, 2017

Referat:

Diese Arbeit beschäftigt sich mit der Analyse und Evaluierung ausgewählter Tools, im Bereich des IT-Monitorings, sowie der Bewertung der unterschiedlichen Lösungen, unter Berücksichtigung der Anforderungen im Unternehmen. Dazu gehört im Anschluss ebenfalls die Erarbeitung eines Implementierungskonzepts für den Echtbetrieb.

Inhalt

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

API	Application Programming Interface
CAL	Client Access License
CLI	Command Line Interface
CPU	Central Processing Unit
ESX	Elastic Sky X (Markenname von VMWare)
EXE	Executeable
GB	Gigabyte
GSM	Global System for Mobile Communications
GUI	Graphical User Interface
HE	Höheneinheit
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HW	Hardware
IANA	Internet Assignet Numers Authority
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IMAP	Internet Message Access Protocol
IP	Internet Protocol
ITS	Issue Tracking System
IT	Informationstechnologie
KB	Kilobyte
KMU	Klein- und Mittelständisches Unternehmen
KO	Knocked Out
LAN	Local Area Network

MB	Megabyte
MIB	Management Information Base
MKW	Metall- und Kunststoffwerk Weibern
MX	Mail Exchange
NAT	Network Address Translation
OID	Object Identifier
PC	Personal Computer
PHP	Hypertext PreProcessor
POP3	Post Office Protocol Version 3
RAID	Redundant Array of Independant Disks
RJ	Registered Jack
SaaS	Software as a Service
SAN	Storage Area Network
SMS	Short Message Service
SMSC	Short Message Service Centre
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Monitoring Protocol
SOAP	Simple Object Access Protocol
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Sockets Layer
SW	Software
TB	Terabyte
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
USB	Universal Serial Bus
USV	Unterbrechungsfreie Stromversorgung
VBA	Visual Basic für Applications

VBS	Visual Basic for Skripting
VM	Virtual Machine
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
W3C	World Wide Web Consortium
WAN	Wide Area Network
WLAN	Wireless Local Area Network
WMI	Windows Management Instrumentation
XML	Extensible Markup Language

1 Einleitung

Im einleitenden Kapitel werden die Motivation und die Aufgabenstellung dargestellt. Gleichzeitig erfolgen eine kurze Vorstellung des Auftraggebers sowie ein Kapitelüberblick.

1.1 Motivation

Moderne IT-Infrastrukturen werden immer stärker vernetzt und skalieren sehr stark. Dazu sind unterschiedlichste Technologien und Geräte notwendig, welche verschiedensten Konfigurations- und Wartungsaufwand besitzen. Hier einen Überblick zu behalten ist für einen Administrator oder Fachbereichsmitarbeiter kaum möglich. Diese Diplomarbeit soll aufzeigen wie eine heute oft im Einsatz befindliche IT-Infrastruktur zentral überwacht werden kann.

In meiner Tätigkeit als Administrator bin ich oft in der Situation, ein Problem oder einen Fehlerfall zu analysieren. Meist werden die Fehler erst sichtbar, wenn sich diese schon im fortgeschrittenen Stadium befinden. Eine Früherkennung bzw. Frühalarmierung, wenn beispielsweise ein Festplattenspeicher knapp wird oder zu hoher Datenverkehr im Netzwerk herrscht, ist daher heutzutage unverzichtbar.

1.2 Zielsetzung

Diese Diplomarbeit beschreibt den Aufbau eines zentralen IT-Monitorings für ein KMU. Ein derzeit eingesetztes System wird vom Hersteller nicht mehr unterstützt und bietet außerdem nur sehr sporadische Funktionalitäten im Bereich der Liveüberwachung und Visualisierung. Verschiedenste moderne Systeme sind nicht mehr in der aktuellen Software abzubilden, somit ist es notwendig, hier nochmal zurück zum Anfang zu gehen und ein geeignetes Konzept zu erarbeiten.

Ein Schwerpunkt dieser Arbeit ist die Beleuchtung der vorhandenen Überwachungsprotokolle und Alarmierungskonzepte. Zudem sollen verschiedene Analyseverfahren für die Softwareauswahl recherchiert werden.

Anschließend sind geeignete Lösungen zu testen und für den am Ende gewählten Sieger, ist ein auf die Firma MKW zugeschnittenes Konzept zu erarbeiten. Dazu gehört auch die Auswahl einer geeigneten Hardware.

1.3 Auftraggeber

Auftraggeber für diese Diplomarbeit ist die Firma MKW Holding GmbH. Ein Familiengeführtes Industrieunternehmen im oberösterreichischen Weibern, das seit 1960 existiert.

Beschäftigt sind rund 400 Mitarbeiter an 4 Standorten (Österreich, Slowakei, Russland).

Der Schwerpunkt liegt in der Metall- und Kunststoffverarbeitung sowie der Oberflächenbehandlung.

Abbildung 1-1 Kompetenzen MKW (MKW 2017)

1.4 Kapitelübersicht

Nach der Einleitung in diesem Abschnitt (**Kapitel 1**) folgt in **Kapitel 2** die Recherche zum Stand der Technik, wobei hier der Schwerpunkt auf die derzeit eingesetzte Technik, am Markt vorhandene Überwachungsprotokolle sowie Alarmierungskonzepte gesetzt wird.

In **Kapitel 3** wird die Aufgabenstellung auf Basis der Rechercheergebnisse präzisiert und greifbare Ziele definiert.

Kapitel 4 beschäftigt sich mit der Analyse und der Evaluierung bereits vorhandener Softwarelösungen.

In **Kapitel 5** findet sowohl die Hardware- als auch die Softwarekonzeption für die Implementierung des zuvor ausgewählten Siegertools statt.

Kapitel 6 bewertet die erreichten Ergebnisse, welche im Laufe der Arbeit entstanden sind.

Abschließend werden in **Kapitel 7** die Ergebnisse der Diplomarbeit zusammengefasst und ein Ausblick auf zukünftige Möglichkeiten gegeben.

2 Analyse zum Stand der Technik

In diesem Kapitel werden die derzeit eingesetzten Lösungen erklärt und es findet eine Recherche über die bestehenden Techniken des IT-Monitorings statt. Generelle Themen hinsichtlich Überwachungsprotokolle und Alarmierungsmöglichkeiten werden geklärt und ausgearbeitet. Ein weiterer Schwerpunkt liegt auf Bewertungsmodellen für die Auswahl einer geeigneten Softwarelösung.

2.1 Derzeitige Monitoringsituation bei MKW

MKW verwendet derzeit mehrere Lösungen zur Überwachung. Für die Server und die Überprüfung der Geräteerreichbarkeit (mittels Ping) wird ein Tool vom Hersteller GFI, der GFI Network Server Monitor 7.0, verwendet. Dieses hat die rudimentäre Möglichkeit, diverse Parameter wie Festplattenspeicher oder Serverprozesse zu überwachen und schickt im Fehlerfall einen Alarm an die IT-Abteilung. Es gibt keine Auswertemöglichkeit, keinen Verlauf oder die Möglichkeit der Visualisierung. Die Bedienbarkeit ist nicht mehr am aktuellen Stand der Technik und die Funktionalitäten für neue Geräte sind sehr eingeschränkt. Außerdem wurde diese Software vom Hersteller bereits abgekündigt. Es fehlt also die Möglichkeit der Erweiterung, der Verbesserung und des Supports.

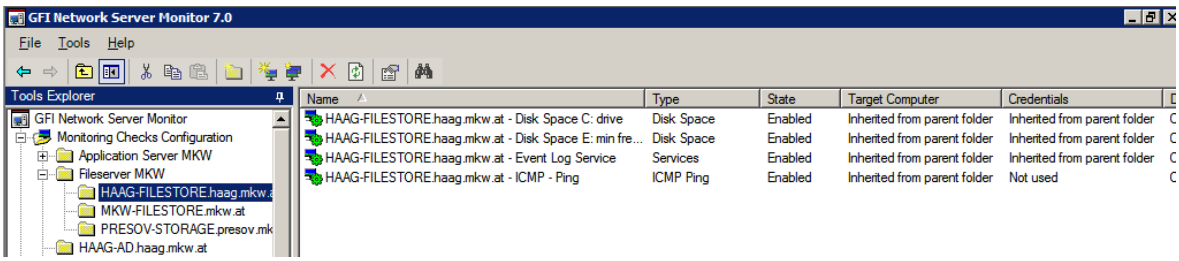


Abbildung 2-2 Ausschnitt GFI Network Service Monitor 7.0

Zusätzlich werden einige netzwerkfähige Geräte direkt über deren Netzwerkschnittstelle überwacht. So kann beispielsweise über die Bedienoberfläche einer USV-Anlage eine Alarmierung per Mail im Fehlerfall eingerichtet werden. Funktioniert diese Netzwerkkarte nicht zuverlässig, werden die Nachrichten nicht erfolgreich übermittelt. Zudem müssen die Einstellungen auf jedem Gerät einzeln vorgenommen werden (Mailserver einrichten, Absenderadresse erstellen, Alarmarten definieren usw.).

Eine weitere Methode ist die manuelle Überwachung durch das IT-Personal. Hier hat sich jeder seine eigenen Prozesse zurechtgelegt, wie und vor allem wie oft er die einzelnen Geräte und Prozesse überwacht. Dies geschieht mittels eines Fernwartungszugriffs auf einen Server oder eine Sichtkontrolle beim Gerät selbst. Diese Wartungsroutinen erkennen Fehler oft erst sehr spät nach deren Auftreten.

2.2 Was ist IT-Monitoring?

Monitoring im Bereich der IT bedeutet Überwachung oder laufende Kontrolle auf korrekte Funktionalität. Es ist ein Begriff, der die Protokollierung und die Erfassung von Prozessen beschreibt. Monitoring ist eine der wichtigsten Aufgaben für einen Systemadministrator.

Es können alle gängigen Computer, Computersysteme sowie Netzwerke überwacht werden, sowohl Hardware als auch Software. Ein solches System zeichnet sich durch geringe Systembelastung aus, obwohl dieses rund um die Uhr, kontinuierlich und gründlich die einzelnen Messpunkte abfragt.

Es kann bereits im frühen Stadium des Fehlers den betreffenden Mitarbeiter verständigen. Über diverse Zugriffsysteme und Fernwartungskonzepte kann der Status der IT-Infrastruktur jederzeit und überall eingesehen werden.

Die klaren Vorteile eines Monitoringsystems sind die Erhöhung der Verfügbarkeit, sowie der Stabilität, 24/7 Überwachung, frühzeitliche Erkennung und Benachrichtigung im Fehlerfall, automatische Visualisierung und Auswertung.[1]

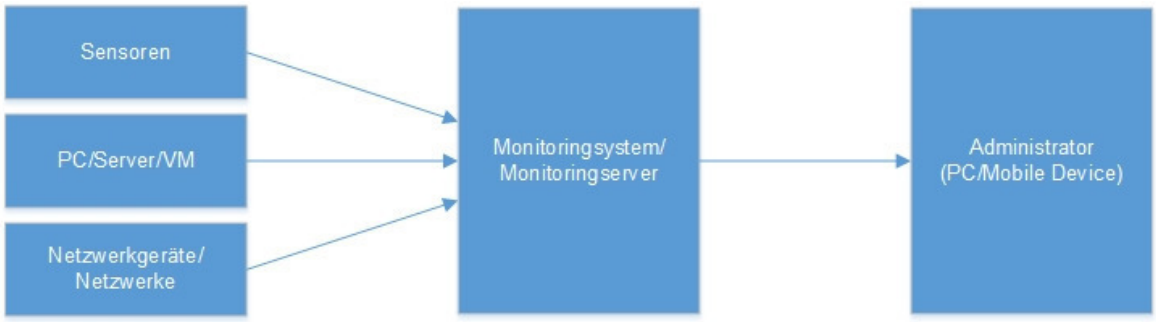


Abbildung 2-3 Funktionsweise IT-Monitoring

Aktives Monitoring

Beim aktiven Monitoring werden aktive Test-Clients im Netz installiert. Von einer zentralen Monitoring Station aus werden aktive Verbindungen zu den Test-Clients aufgebaut und laufend Daten/Pakete übertragen. Dadurch lassen sich End-to-End Verbindungen besser überwachen (VoIP). Signalveränderungen lassen sich beim aktiven Monitoring besser feststellen. Nachteil ist der erhöhte Paketversand im Netz zu reinen Überwachungszwecken.

[1] Vgl. Hagel 2017, Gesamtartikel

Passives Monitoring

Hierbei werden keine zusätzlichen Pakete im Netz gesendet, sondern der Datenverkehr an bestimmten Knotenpunkten einfach mitgehört. Diese Datenströme werden an das Monitoringsystem gespiegelt und anschließend analysiert. Der klare Vorteil ist, dass keine zusätzlichen Netzlasten verursacht werden.[2]

2.3 Überwachungsarten und -protokolle

Zur Überwachung der diversen Hard- und Software gibt es mehrere Möglichkeiten mit denen die Daten abgegriffen werden können. Das kann über standardisierte Protokolle oder durch herstellerspezifische Dienste erfolgen. Auf den folgenden Seiten werden die Grundbegriffe und Funktionsweisen der gängigsten Überwachungsarten geklärt.

2.3.1 Simple Network Monitoring Protokoll (SNMP)

SNMP dient zur Überwachung und zur Konfiguration von Netzwerkgeräten. Es muss auf dem zu überwachenden Gerät aktiviert werden und wird danach über das Netzwerk angesprochen. Das Protokoll ist sehr einfach gehalten und verursacht sehr wenig Datenverkehr. Es ist auch für leistungsschwache Geräte (z.B. Temperatursensoren) geeignet. Das Gerät sendet Infos nach Anfrage einer Managementkonsole über das Netzwerk. Außerdem ist es möglich, automatisierte Nachrichten, sogenannte Traps, im Fehlerfall bzw. bei Zustandsänderung zu senden und diese auszuwerten. Dazu wird ein Request an das zu überwachende Gerät gesendet, dieses antwortet mit einem Response oder einer Trap[3]

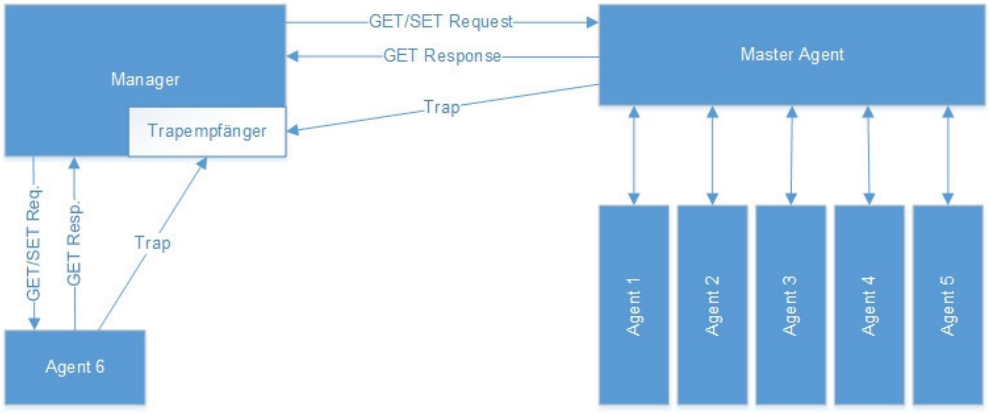


Abbildung 2-4 Funktionsweise SNMP (Wlki-SNMP 2017)

[2] Vgl. Hein 2015, S. 65

[3] Vgl. Dietmüller 2011, S. 3

Der SNMP Agent ist das Netzwerkgerät, das von der zentralen Managementkonsole angesprochen wird. Er stellt die entsprechenden MIB definierten OID Daten bereit. Er muss vor Verwendung dementsprechend aktiviert werden.

Der SNMP Client ist die eigentliche Managementkonsole und ist das Bindeglied zwischen Mensch und Maschine. Er verwaltet die SNMP-Agents und liest die empfangenen Daten aus. Der Client stellt also das eigentliche IT-Monitoringsystem dar.[4]

SNMP glänzt nicht durch Einfachheit in der Einrichtung, jedoch durch den universellen und vielseitigen Einsatz in der Datengewinnung und Auswertung. Vom Prinzip her arbeitet dieses Protokoll als klassisches Client-Server System.[5]

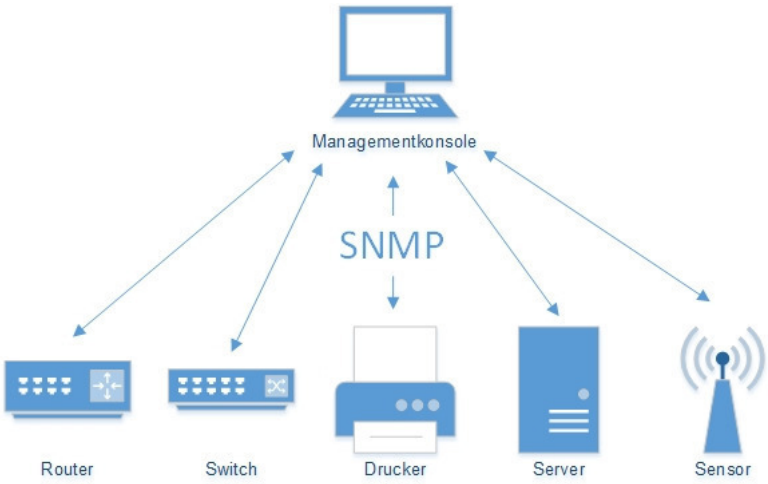


Abbildung 2-5 Überwachungsprinzip SNMP (Dietmüller 2011)

OID/MIB

OID ist ein Zahlenwert, welcher den Wert eines SNMP fähigen Gerätes eindeutig beschreibt. Diese Zahlen sind baumförmig organisiert. Von der Wurzel bis zu einer gewissen Tiefe werden OID's von der IANA verwaltet, ab dann sind die Bezeichnungen meist herstellerspezifisch. OID'S bestehen nur aus den Zahlen (Bsp.: 1-3-6-1-4-….) für den Baum, die Namensauflösung erfolgt erst mittels der MIB.[6]

[4] Vgl. Dietmüller 2011, S. 3–4

[5] Vgl. Wittmann 2015, S. 36

[6] Vgl Dietmüller 2011, S. 4

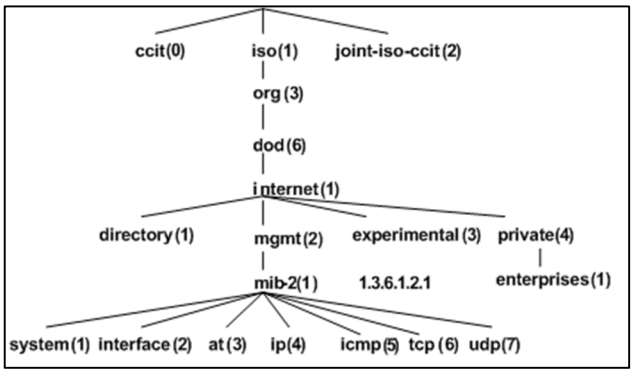


Abbildung 2-6 Baumstruktur OID (H3C 2017)

Die MIB ist die Beschreibung der OID. Darin enthalten ist der Name, Dateityp und die Zugriffsmöglichkeit auf eine OID. MIBs machen den OID Baum lesbar, außerdem wird die MIB von der Managementkonsole benötigt. Gespeichert sind die einzelnen MIB-Elemente in Dateien mit der Endung „mib“. Nach dem Laden der MIB weiß das System, welche Daten von den Geräten abgefragt werden können.[7]

```
-- a collection of objects common to all managed systems.

system   OBJECT IDENTIFIER ::= { mib-2 1 }

sysDescr OBJECT-TYPE
    SYNTAX      DisplayString (SIZE (0..255))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "A textual description of the entity.  This value should
            include the full name and version identification of the
            system's hardware type, software operating-system, and
            networking software."
    ::= { system 1 }

sysObjectID OBJECT-TYPE
```

Abbildung 2-7 Ausschnitt MIB - Abfrage Displaystring (Brisson 2004)

Communitystring

Der Communitystring ist ein einfacher String, der auf den Geräten mit bestimmten Zugriffsberechtigungen verbunden ist. Er ist also vergleichbar mit einem User und kann je nach Version und Ausführung, mit Authentifizierung oder ohne Authentifizierung am Gerät verwendet werden. Dieser String wird bei einer SNMP-Anfrage mitgesendet, um die Berechtigung des Managementsystems dem zu verwaltenden Gerät mitzuteilen. Der Agent kann dadurch entscheiden, ob die Anfrage beantwortet wird oder nicht.[8]

[7] Vgl. Dietmüller 2011, S. 4–5

[8] Vgl. Dietmüller 2011, S. 5

SNMP Version 1

SNMPv1 wurde Ende der 1980er Jahre entwickelt, da eine herstellerspezifische Unabhängigkeit im Netzwerkmanagement erwünscht war. Es wurde sehr rasch als Industriestandard akzeptiert, obwohl diese Version keinerlei Sicherheitsfeatures wie Paketverschlüsselung und Ähnliches liefert. Jedoch ist die Nutzung sehr einfach, da nur ein Communiystring und ein Port definiert werden muss. Version 1 ist aufgrund ihrer Einfachheit und der oftmals nicht notwendigen Sicherheit in einem Intranet sehr häufig im Einsatz. Viele Endgeräte liefern auch nur die Version 1 mit. Der Nachteil ist, dass nur 32 Bit Counter verwendet werden können, das reicht zwar für kleinere Sensoren und Geräte, jedoch nicht für die Überwachung des Datenflusses in einem Gigabit Netzwerk.[9]

SNMPv1 liefert folgende Funktionen:

- **Get:** Fragt bestimmten Datenwert (OID) ab
- **GetNext:** Ruft Datenwert ab, der auf eine bestimmte OID folgt (Datendurchsatz verschiedener Ports)
- **Set:** Setzt einen Datenwert, dazu müssen in der MIB Schreibrechte vergeben sein.
- **Responce:** Ist die Antwort des Agents auf eine Anfrage.
- **Trap:** Normalerweise werden SNMP Daten nur auf Anfrage versendet. Ausnahme sind Traps, diese werden aufgrund eines Ereignisses am Endgerät versendet. Diese müssen zuvor definiert werden (Sensor überschreitet Schwellwert).[10]

SNMP Version 2

Die Version 2 ist der Version 1 sehr ähnlich. Der größte Unterschied ist der Einsatz eines 64 Bit Counters, wodurch auch größere Netze überwachbar werden, da die SNMP Pakete mehr Daten liefern können. Es gibt weiterhin keine Verschlüsselung. Diese Version kann mehrere Werte aus einer OID gleichzeitig auslesen, dies ersetzt die Funktion GetNext. Außerdem wurde versucht, eine gewisse Sicherheit durch Authentifizierungen zu realisieren. Dadurch wurde aber der Administrations- und Konfigurationsaufwand erheblich erhöht und der Nutzen war kaum zu spüren. Daher ist SNMPv2 bis heute kaum im Einsatz.[11] [12]

SNMP Version 3

SNMPv3 ist die aktuellste Version und wird offiziell empfohlen, ist aber von manchen Herstellern nicht unterstützt. Hier wurde erstmals ein durchgängiges Verschlüsselungskonzept

---

[9] Vgl. Wittmann 2015, S. 41–42

[10] Vgl. Dietmüller 2011, S. 5–6

[11] Vgl. Wittmann 2015, S. 41

[12] Vgl. Dietmüller 2011, S. 6

integriert. Es wurde eine Userverwaltung implementiert, die mit oder ohne Authentifizierung Daten abgreifen kann. Der Konfigurationsaufwand ist gegenüber V1 und 2 zwar deutlich höher, der Nutzen aber ebenfalls. Der Nachteil ist die schlechte Einsatzfähigkeit in großen Netzen, da die SSL Verschlüsselung große CPU-Lasten zur Folge hat. Daher hat sich Version 3 gerade in Intranets kaum durchsetzen können und wird hauptsächlich bei WAN Verbindungen genutzt.[13]

SNMPv3 liefert folgende 3 Securitylevels:

- Ohne Authentifikation und ohne Verschlüsselung (NoAuthNoPriv)
- Mit Authentifikation und ohne Verschlüsselung (AuthNoPriv)
- Mit Authentifikation und mit Verschlüsselung (AuthPriv)

2.3.2 WMI

Windows Managemant Instrumentation, kurz WMI, ist eine grundlegende Windows-Verwaltungstechnologie. Mittels WMI können sowohl lokale Computer als auch Remotecomputer verwaltet werden. Es bietet einen einheitlichen Ansatz für die Ausführung täglicher Verwaltungsaufgaben mit Programmier- oder Skriptsprachen.

WMI liefert Informationen zum internen Status von Computersystemen, ähnlich wie die Instrumente im Armaturenbrett von einem Auto. Die Instrumentation in WMI erfolgt durch das Modellieren von Objekten wie Datenträgern, Prozessen oder anderen Objekten in Windows. Diese Systemobjekte werden mithilfe von Klassen (Bsp.: Win32_LogicalDisk) modelliert.

Zu den WMI-Funktionen zählen unter anderem Ereignis-, Remote- und Abfragefunktionen, Sichten, Benutzererweiterungen und Instrumentation.[14]

Um einen Fernzugriff mittels WMI durchzuführen, ist ein Active-Directory Benutzer mit ausreichenden Berechtigungen notwendig. Dieser holt dann vom Gerät die jeweiligen Daten.

Das WMI Protokoll benötigt im Verhältnis zu anderen Überwachungsprotokollen viel Performance, um die Abfragen auszuführen.[15]

---

[13] Vgl. Wittmann 2015, S. 41

[14] Vgl. Microsoft Technet 2017, Abschnitt F1

[15] Vgl. PRTG WMI 2017, Abschnitt "How WMI works"

2.3.3 ICMP

Das Internet Control Message Protocol (ICMP) gehört zum Internet Protokoll (IP), wird aber eigenständig behandelt. Es dient der Übermittlung von Meldungen mittels IP, genauer gesagt sollen Statusinformationen und Fehlermeldungen der Protokolle IP, TCP und UDP übertragen werden.

Die bekanntesten Tools, die unter ICMP fallen, sind „Ping“ und „Trace Route“. Die durch diese Befehle ausgelösten Rückmeldungen können mit einem Netzwerkmonitor analysiert werden.[16]

Ping ist das meistgenutzte Tool, um eine Netzwerkverbindung zu testen. Hierbei werden ICMP-Pakete vom Typ Echo Request an das entfernte Gerät gesendet, dieses sendet bei Erreichbarkeit ein ICMP-Paket vom Typ Echo Reply zurück. Ist das Endgerät nicht erreichbar, so bekommt man eine Fehlermeldung zurück. Somit kann mittels ICMP Ping die Verfügbarkeit diverser Geräte im Netzwerk sehr einfach überprüft werden.[17]

Abbildung 2-8 Ablauf Ping-Befehl

[16] Vgl. ELEK 2017a

[17] Vgl. ELEK 2017b

2.3.4 Netflow

Netflow ist ein Netzwerkprotokoll, welches von der Firma Cisco entwickelt wurde, um Informationen über den Netzwerkverkehr zu sammeln und diesen zu überwachen. Mittels eines NetFlow Collectors und Analyzers können die ein- und ausgehenden Netzwerkdaten eines Netzwerkgerätes ausgewertet werden. Von anderen Herstellern gibt es ähnliche Protokolle wie jflow, s-flow oder Netstream.[18]

Die Daten werden über den IP-Datenstrom vom Switch oder Router per UDP exportiert (Netflow Exporter). Diese Datagramme werden von einem Managementsystem (Netflow Kollektor) gesammelt, gespeichert und verarbeitet.

Die wichtigsten Bestandteile eines Flows sind:

- Sequenznummer
- Zeitstempel
- Bytezähler
- Quell- und Ziel IP-Adressen
- Quell- und Ziel Ports
- Protokolltype

Netflow ist ein passives Messverfahren, d.h. man beeinflusst den Datenverkehr nicht. Durch die Übertragung per UDP wird die Performance des Netzwerks nicht beeinflusst, verlorene Datenpakete können jedoch nicht mehr hergestellt werden. Dies ist speziell bei Flows über eine Internetverbindung oftmals problematisch.[19]

Es gibt bei Netflow die Version 5 sowie die Version 9. Der Unterschied ist der Aufbau des Flows. So sind die Pakete in der Version 5 fix aufgebaut, in Version 9 dynamisch.

Somit kann bei Version 5 immer nur 1 Parameter überwacht und eingerichtet werden, da die Pakete nicht geändert werden können, Version 9 hingegen kann unterschiedlichste Daten übertragen (z.B: CPU Auslastung), muss aber vorab an den Kollektor eine Vorlage schicken wie die nächsten Pakete aufgebaut sind. Man spricht bei NetflowV9 oftmals auch von Flexible Netflow[20]

Für die Konfiguration von Netflow auf dem Netzwerkgerät sind folgende Schritte notwendig:

- Einrichtung Flow Recorder (Definiert, welche Daten gesammelt werden)
- Einrichtung Flow Exporter (Definiert, wohin die Daten exportiert werden)

---

[18] Vgl Solarwinds Netflow, Gesamtartikel

[19] Vgl. Wiki-NF 2017, Gesamtartikel

[20] Vgl. Petterson 2009, Gesamtartikel

- Einrichtung Flow Monitor (Generiert den Flow Monitor für die Interfaces)
- Flow Monitor auf den Interfaces aktivieren

Abschließend muss dem Netflow-Collector (meist Software auf einem Server) mitgeteilt werden, über welche Adresse bzw. welchen UDP Port die Flow-Pakete eintreffen.[21]

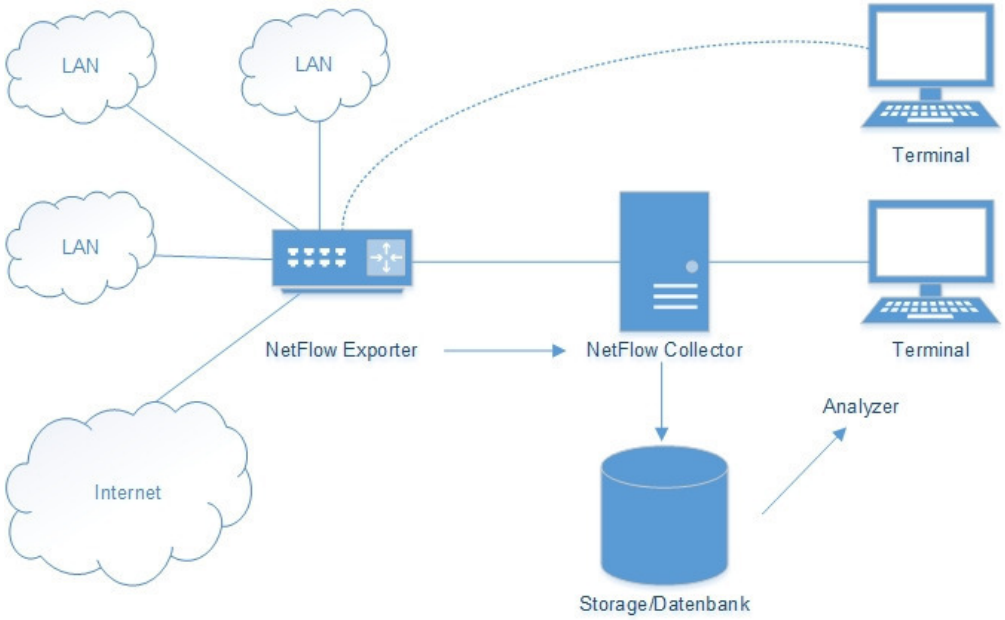


Abbildung 2-9 Funktionsprinzip Netflow (PandoraFMS 2017)

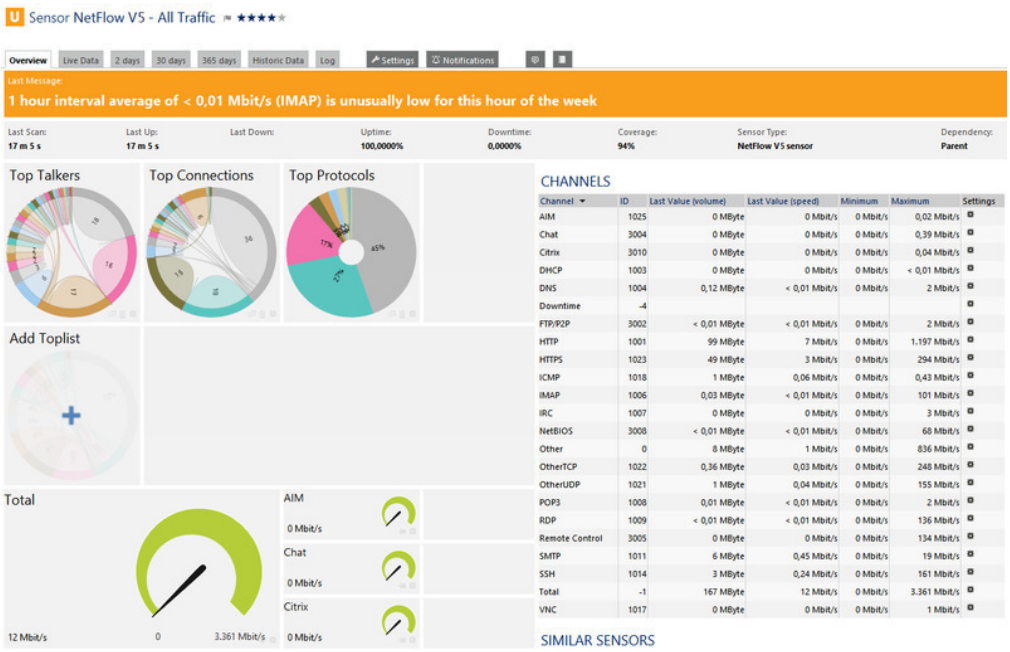


Abbildung 2-10 Netflow Analyse (PRTG Netflow 2017)

[21] Vgl. Solarwinds Netflow Configuration 2017, S. 4–6

2.3.5 Netzwerksniffer

Ein Netzwerksniffer überwacht den Datenfluss im Netzwerk in Echtzeit. Sniffer können sowohl als Hard- und Software gebaut werden. Es werden alle Netzwerkpakete einer gewissen Schnittstelle überwacht und kopiert und können anschließend ausgewertet und gefiltert werden. Neben einzelnen Datenpaketen kann der Inhalt von diesen äußerst genau analysiert werden (Zieladressen, Quelladressen usw.).[22]

Standardmäßig wird die Netzwerkkarte des Rechners auf dem der Sniffer läuft genutzt, aber auch Weiterleitung anderer Schnittstellen auf einen zentralen Punkt (Port Mirroring) ist möglich. Die Last im Netzwerk ist beim Sniffing deutlich höher als bei anderen Verfahren und wird in der Praxis nicht über längere Zeiträume realisiert. Die klassische Anwendung findet man in der Fehleranalyse, also kurzfristig über meist wenige Stunden oder Tage.[23]

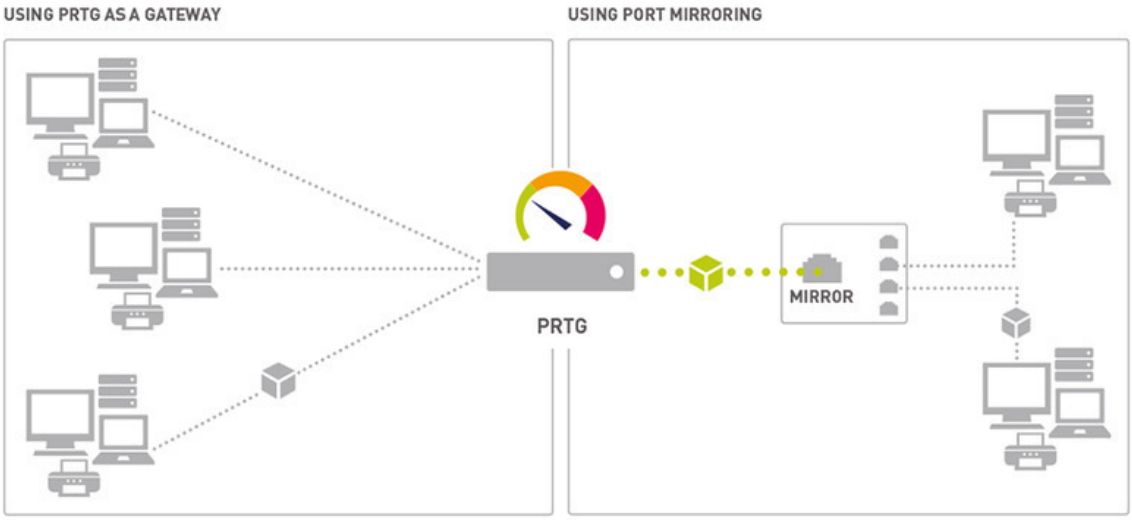


Abbildung 2-11 Sniffing Konzept eines Switchports (PRTG-Sniff 2017)

2.3.6 PowerShell

PowerShell ist ein plattformübergreifendes Framework von Microsoft zur Automatisierung, Konfiguration und Verwaltung von Systemen, bestehend aus einem Kommandozeileninterpreter und einer Skriptsprache.

Das Framework wurde speziell für die Systemverwaltung und –automatisierung entworfen und erlaubt Zugriff auf WMI-Klassen, COM-Objekte und das gesamte .NET-Framework.

---

[22] Vgl. Mitchell 2012, Gesamtartikel

[23] Vgl. PRTG-Sniff 2017, Gesamtartikel

Der Aufbau von PowerShell besitzt folgende Komponenten:

- **PowerShell Engine** ist der Kommandozeileninterpreter, hier werden die Eingaben verarbeitet.
- **PowerShell Host** ist die Benutzerschnittstelle zur Engine. In Windows ist dies eine PowerShell Konsole sowie ein Skripteditor.
- **PowerShell Scripting Language** ist die Sprache, um Skripte für PowerShell zu entwickeln. Diese sind für Automatismen und Datenabfragen notwendig.
- **Cmdlets (=Commandlets)** sind die Befehle in der PowerShell Umgebung. Es handelt sich dabei um sehr kleine spezielle Befehle. Diese können nur in der PowerShell ausgeführt werden. Aufgebaut sind diese mit dem Syntax `Verb-Substantiv` also beispielsweise `Get-Process`, damit werden alle laufenden Prozesse abgefragt und aufgelistet. Mittels Parameter können die Befehle noch verfeinert werden.
- **PowerShellProvider** bieten Zugriff auf Daten und Komponenten, die sonst nicht einfach abrufbar wären.

Eine typische Anwendung der PowerShell im Monitoringbereich ist der Zugriff auf Windowsdienste und –produkte wie Micosoft Exchange Server. Hier können mittels PowerShell Postfächer oder Datensicherungen überwacht werden.[24]

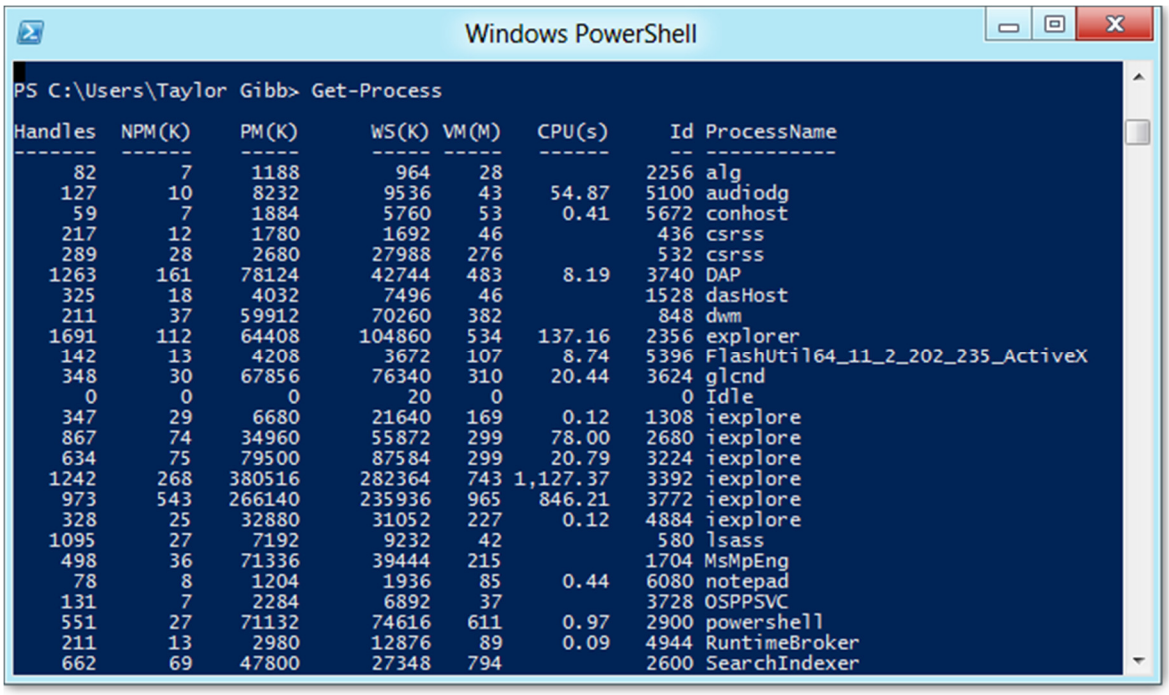


Abbildung 2-12 Powershellansicht Befehl Get-Process (Gibb 2017)

[24] Vgl. Wiki-PS 2017, Gesamtartikel

2.3.7 SOAP

SOAP ist ein Netzwerkprotokoll, mit dessen Hilfe Daten zwischen Systemen ausgetauscht werden können. Es ist ein Industriestandard des W3C.

Es stützt sich auf XML zur Datenrepräsentation und auf Internetprotokolle der Transport- und Anwendungsschicht zur Nachrichtenübertragung (HTTP, TCP).

Das XML-Nachrichtendesign ist bei SOAP genau geregelt, ebenso die Interpretation der Daten. Einsatz findet dieses Protokoll für entfernte Prozeduraufrufe, Nachrichtensystem bzw. zum Datenaustausch. Daten werden in der Praxis meist mittels HTTP gesendet. SOAP wird auch eingesetzt, wenn ein Austausch zwischen sehr verschiedenen Systemen stattfinden soll, wo es zu Kompatibilitätsproblemen kommen könnte (Bsp. Kommunikation ESX-Host mit Monitoringtool).

Eine SOAP Nachricht besteht aus einem Envelopeelement, dieses beinhaltet meist einen Headerteil mit Meta-Informationen und einem Bodyteil, in dem die eigentlichen Nutzdaten untergebracht sind.[25]

2.3.8 SSH

Secure Shell (SSH) bezeichnet sowohl ein Netzwerkprotokoll als auch entsprechende Programme, mit welchen man auf sichere Art verschlüsselte Netzwerkverbindungen auf entfernte Geräte herstellen kann.

Folgende Anwendungsszenarien lassen sich darstellen:

- Secure System Administration (Sichere Systemverwaltung)
- Secure Remote Comand Execution (Sichere Ausführung von Kommandos)
- Secure Subsystem Execution (Sicheres Ausführen von Subsystemen)

Um eine Verbindung zwischen zwei Geräten herzustellen muss eine Authentifizierung stattfinden, diese erfolgt mittels gängigen Verfahren wie Public-Key-Authentifizierung oder Private-Key-Authentifizierung, meist in Verbindung mit einem User, um auch diverse Berechtigungen steuern zu können. Nach der erfolgreichen Anmeldung besteht während der offenen Sitzung eine verschlüsselte Verbindung.

Beim Monitoring wird SSH oft für Linux-Systeme, Netzwerkgeräte oder Virtualisierungsserver verwendet.[26]

---

[25] Vgl. Wiki-Soap 2017, Gesamtartikel

[26] Vgl. Wiki-SSH 2017, Gesamtartikel

2.4 Alarmierungsarten

In jedem System gibt es Fälle, die nicht eintreten sollen bzw. Warnwerte, die eine Auskunft geben, dass Probleme entstehen können. Daher ist es notwendig, im Fehlerfall eine Mitteilung an die betroffenen Personen zu versenden bzw. diese zu alarmieren. Am besten erfolgt diese Benachrichtigung bereits in einem frühen Stadium. Die Art der Alarmierung kann sehr unterschiedlich sein. Oftmals kann eine Alarmierung auch eine Automatisierungsroutine sein, welche den möglicherweise eintretenden Fehlerfall selbst beseitigt. Auf den folgenden Seiten werden die praktikabelsten Alarmierungsmethoden erläutert.

2.4.1 E-Mail

E-Mail ist heutzutage nicht mehr aus dem Alltag wegzudenken. Fast jeder hat zumindest eine eigene Mailadresse und überprüft diese mehrmals täglich. Daher bietet es sich an auch im Alarmierungskonzept auf dieses System zurückzugreifen.

Ein Mailsystem besteht aus folgenden Komponenten:

- Posteingangsserver, der die Nachrichten entgegennimmt und auf die Postfächer verteilt (mittels POP3 oder IMAP)
- Postausgangsserver, an den die gesendeten Nachrichten übergeben werden und der diese weiterleitet (mittels SMTP)
- Mail Client für die Verwaltung der Postfächer[27]

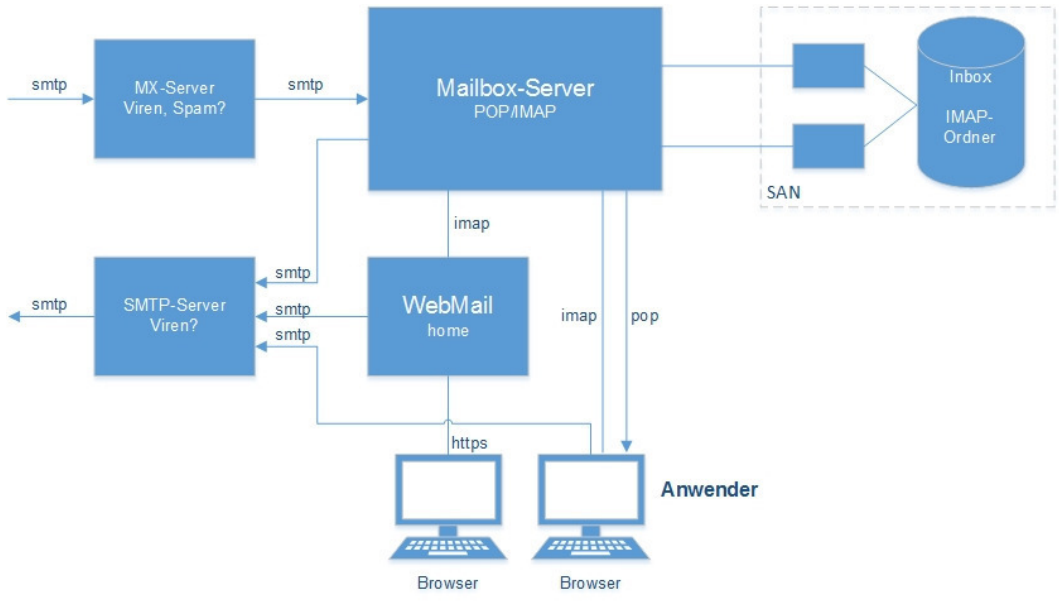


Abbildung 2-13 Funktionsweise Mailserver

[27] Vgl. Universität Bamberg 2017, Gesamtartikel

Für das Monitoring ist hier nur der Postausgangsserver relevant. Sobald ein Fehler vom System erkannt wird, sendet das Monitoringsystem über den SMTP-Server eine Mail an die betroffenen Personen.

2.4.2 SMS

Eine SMS wird in der Geschichte gerne als Zufallsprodukt bezeichnet, weil zur Übertragung Mechanismen verwendet werden, wie sie auch bei der Vermittlung und Übertragung von Telefonanrufen zum Einsatz kommen.

Jeder Mobilfunkanbieter verfügt über ein Short Message Service Center (SMSC), welches die SMS zur Verarbeitung abspeichert. Dort verweilt die SMS, bis die Zustellung erfolgreich war bzw. die Zustellung aufgrund eines unwiderruflichen Fehlers beendet werden muss (Empfänger nicht vorhanden). Für eine erfolgreiche Zustellung wird vom Serviceprovider der Aufenthaltsort der Empfängernummer lokalisiert, der dazugehörige Netzanbieter ermittelt und an dessen System übergeben. Stimmen alle Parameter überein, wird die Nachricht zugestellt.

Eine SMS kann 140 Bytes übertragen (meist Text), das entspricht maximal 160 Zeichen. Längere Nachrichten werden auf mehrere Nachrichten aufgeteilt.[28]

Abbildung 2-14 Vereinfachtes Übertragungsprinzip SMS

2.4.3 Issue-Tracking-System

Ein ITS, oftmals auch Ticketing-System oder Helpdesk-System genannt, ist eine Software, um Empfang, Bestätigung und Bearbeitung von Anfragen zu handhaben. Diese werden manuell vom Kunden erzeugt oder automatisch generiert. Die Anfragen können Anrufe, E-Mails, Faxe, automatisierte Events oder Ahnliches sein. Im Monitoring können automatisiert Fehlermeldungen von Geräten direkt als Bearbeitungsfall ins ITS laufen.

Zu den häufigsten Funktionalitäten eines ITS zählen:

- Erfassung von Störungen und Fehlern
- Verteilung und Zuordnung von Bearbeitern

[28] Vgl. Mrvka 2014, Gesamtartikel

- Überwachung des Bearbeitungsverlaufs
- Garantiertes Einhalten bestimmter Abläufe
- Automatisches Generieren von Tickets durch Alarm-Systeme wie z.B. Netzwerküberwachung

Ein Ticketsystem bietet ein einheitliches und zentrales System für die Bearbeitung von Kundenanfragen, hat jedoch den Nachteil, dass eine Software angeschafft werden muss und die Mitarbeiter eine entsprechende Einschulung benötigen. Bei kleineren Firmen wird eine derartige Investition meist nicht vorgenommen, sondern auf klassischen Mail- und Telefonsupport gesetzt.[29]

2.4.4 Push

Push-Nachrichten finden ihre Anwendung hauptsächlich auf Smartphones und Tablets. Damit ist es möglich, dass Apps bzw. Programme Benachrichtigungen an den Startbildschirm senden. Dazu muss die App nicht geöffnet sein und es werden keine Alarmierungen oder Nachrichten mehr verpasst. Es ist eine Netzwerk- oder Internetverbindung notwendig, damit die Daten vom jeweiligen Server empfangen werden können. Ein Nachteil, durch die ständige Empfangsbereitschaft, ist der erhöhte Stromverbrauch.[30]

Um eine sichere Übertragung zu gewährleisten, setzen viele Hersteller auf bestehende Cloud-Services oder Messaging Dienste wie z.B. jene von Apple, Google oder Amazon. Über dieses kann die Nachricht an die Statuszeile des Endgerätes übertragen werden.[31]

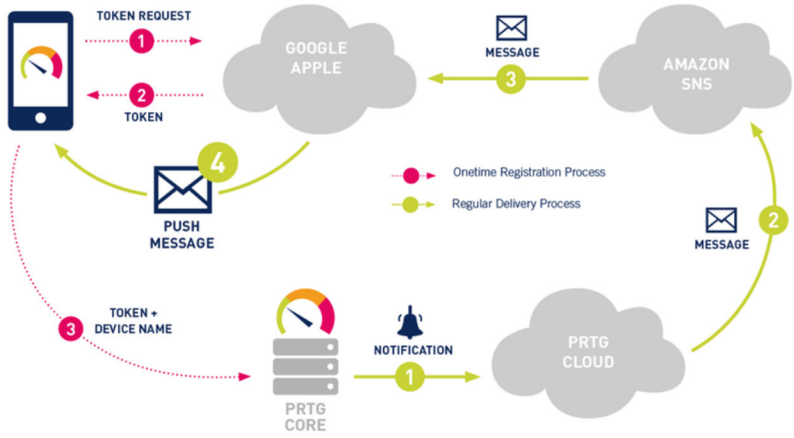


Abbildung 2-15 Push-Übermittlung am Beispiel PRTG (Reder 2015)

[29] Vgl. Wiki-Ticket 2017, Gesamtartikel

[30] Vgl. Flasskamp 2015, Gesamtartikel

[31] Vgl. Reder 2015, Gesamtartikel

2.4.5 Skripting

Mittels Skripting werden meist kleinere Anwendungen oder Anweisungsfolgen realisiert. Eine Besonderheit an Skriptsprachen ist, dass diese nicht in maschinenlesbaren Code übersetzt werden, sondern zur Laufzeit von einem Interpreter ausgeführt werden. Weiters verfügen Skripte über einen gut überschaubaren und leicht lesbaren Quelltext.

Am Beginn der Entwicklung realisierten Skriptsprachen nur interaktive Schnittstellen zur Eingabe von Kommandos an das Betriebssystem (Kommandofolge). Mittlerweile können mit Hilfe von Variablen und eigens definierten Ausdrücken auch eigenständig Codesequenzen realisiert werden. Die wohl bekanntesten Vertreter sind Shellskripte unter Linux/UNIX bzw. Batchdateien im Windows Bereich. Oftmals werden Skripte auch als Funktionserweiterung bestehender Programme eingesetzt. Hier ist wohl an erster Stelle VBA zu nennen. Diese Miniprogramme werden meist als Makros bezeichnet. Mittels Skripting lassen sich viele alltägliche Dinge zeit- oder ereignisgesteuert automatisieren.

Zusätzlich gibt es noch Scripting als selbstständige Programmiersprachen wie z.B. Javascript oder PHP für webbasierte Anwendungen.[32]

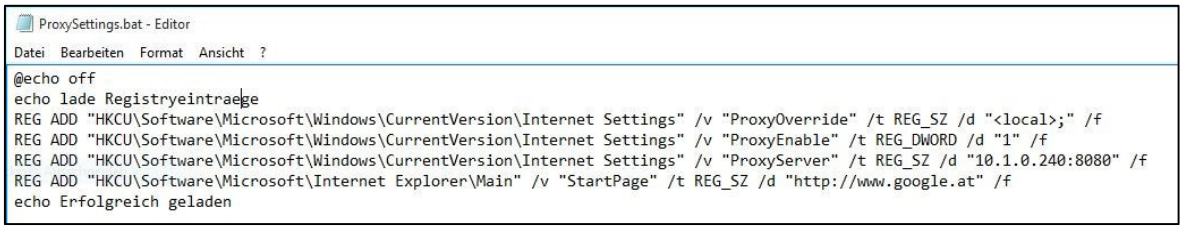


Abbildung 2-16 Batch-Datei zum Ändern von Registrierungseinträgen

2.5 Softwarebewertungsmethoden

Der Markt von fertiger Software ist riesig, auch im Bereich des IT-Monitorings. Es gibt eine Menge an speziell entwickelten Lösungen, wobei jede ihre Stärken und Schwächen hat bzw. jedes Tool für bestimmte Einsatzgebiete auf den Markt gebracht wurde. Um hier das passende Tool zu finden, ist eine Analyse und Bewertung der einzelnen Tools notwendig. Dazu gibt es verschiedene Möglichkeiten und Methoden. Auch bei diesen gibt es große Unterschiede und es muss für die jeweilige Entscheidung das passende Werkzeug gefunden werden.

[32] Vgl. Datacom 2013, Gesamtartikel

2.5.1 Nutzwertanalyse

Die Nutzwertanalyse ist ein Mittel zur Bewertung verschiedener Möglichkeiten und ist sehr universell anwendbar. Nicht nur finanzielle Gesichtspunkte werden hier berücksichtigt sondern meist eine Vielzahl entscheidungsrelevanter Kriterien. Um eine Entscheidung belegbar und bestmöglich begründbar zu machen, sind klare Anforderungen unverzichtbar. Ziel am Ende des Prozesses ist eine aussagekräftige Bewertung der einzelnen Produkte anhand der definierten Kriterien um eine Entscheidung treffen zu können.[33]

Der Vorteil ist die Universalität. Der Nachteil die Subjektivität, da jeder Entscheidungsträger andere Punkte als wichtig erachtet. Hier müssen immer gewisse Kompromisse gefunden werden.[34]

Folgende Teilpunkte muss eine Nutzwertanalyse enthalten (Reihenfolge nicht zwingend aber logisch):

Problemdefinition

Die Problemdefinition ist nicht zwingend Teil der Nutzwertanalyse. Oftmals steht zu Beginn des Projektes bereits das Problem oder der Auftrag fest und die Nutzwertanalyse ist der Weg zur Entscheidung. Wichtig ist eine lückenlose und präzise Formulierung des Arbeitsauftrages, um Missverständnisse während der Ausarbeitung von Beginn an zu vermeiden.

Alternativen auswählen

Hier gilt es, verschiedene Lösungsansätze zu finden und eine Vorauswahl zu treffen. Oft macht es Sinn vorab bereits eine Vorselektion zu treffen, um die Nutzwertanalyse nicht künstlich auszuweiten. Dazu bieten sich andere Werkzeuge besser an. So kann möglicherweise eine Marktanalyse stattfinden, deren Ergebnisliste mittels KO-Kriterien gekürzt wird.

Bewertungskriterien festlegen

Einer der Kernpunkte ist das Festlegen von Kriterien. Anhand des Zieles müssen Anforderungen an die Lösungsalternativen gestellt werden. Man unterscheidet KO-, Muss-, Soll- und Kann-Kriterien. Diese Kriterien sollen in einer Tabelle zusammengefasst werden und dort logische Gruppen gebildet werden, um den Überblick zu behalten.

KO-Kriterien sind diejenigen Kriterien, die unbedingt notwendige Eigenschaften beschreiben. Die Nichterfüllung bedingt den Ausschluss des Betrachtungsgegenstandes. Man kann

---

[33] Vgl. Jansen 2011, S. 3-4

[34] Vgl. Jansen 2011, S. 7–8

hier auch von einem Muss-Kriterium sprechen, das bei Nichterfüllung zu einem KO-Kriterium wird.

Soll-Kriterien sind jene Kriterien, die für das Ziel von hoher Bedeutung sind. Sie sollten möglichst erfüllt werden. Die Nichterfüllung führt nicht zwingend zum KO der Lösungsmöglichkeit.

Kann-Kriterien sind sogenannte „Nice-to-Haves“ bei der Zielerfüllung. Sie beeinflussen die Entscheidung nicht, bringen aber klare Pluspunkte für die Entscheidungsfindung.

Kriterien gewichten

Die vorher definierten Kriterien sind danach zu gewichten. Also soll im Hinblick auf Zielerreichung analysiert werden. Die Gewichtung ist insofern unabdingbar, weil sonst eher unwichtige Kriterien zu viel Einfluss auf das Gesamtergebnis haben. Man gewichtet mit relativen Werten. Das Bewertungsschema kann in Prozent oder einfachen Zahlenwerten ausgedrückt werden. Wie die Gewichtung genau aussieht, muss durch alle Beteiligten gemeinsam beschlossen werden.

Skala erstellen

Für die zu bewertenden Kriterien empfiehlt es sich, eine Skala anzulegen. Hier wird festgehalten, welcher Wert warum zustande gekommen ist, um die Entscheidung transparenter zu gestalten. Außerdem steigert dies die Übersichtlichkeit der gesamten Bewertung und es wird für Dritte nachvollziehbar.

Ermitteln des Nutzwertes der Alternativen

Nun müssen Lösungsvorschläge und Kriterien zusammengebracht und bewertet werden. Die Darstellungsform ist meist eine Tabelle. Für jede Alternative wird der Erfüllungsgrad festgehalten und anhand der Punkteskala ein Zahlenwert vergeben. Am Ende ergibt sich ein Punktewert, der die Höhe des Nutzwertes beschreibt.

Entscheidung

Abschließend kann aufgrund der Zielerfüllungsgrade der Alternativen eine Entscheidung getroffen werden. Dabei ist die Alternative mit dem höchsten Zahlenwert die am besten geeignetste Variante. Durch die direkte Gegenüberstellung während der Nutzwertanalyse, wurde eine belegbare Entscheidungsgrundlage erstellt.[35]

[35] Vgl.Jansen 2011, 4-7;14

2.5.2 Paarvergleich

Beim Paarvergleich werden Varianten paarweise miteinander verglichen, um somit die günstigste Variante zu bestimmen. Variante A wird mit Variante B verglichen und die bessere wird ausgewählt. Diese wird wiederum mit einer Variante C verglichen und der Unterlegene wird ausgeschieden. Dieses Verfahren wird solange durchgeführt, bis eine Siegervariante übrig bleibt. Dadurch wird keine Rangfolge sondern nur ein Gewinner ermittelt. Diese Prozedur kennt man unter dem Namen „King-of-the-Mountain“ Verfahren. Trotz vieler Schwächen findet dieses Verfahren häufig Verwendung in der Praxis, da der Ablauf sehr einfach ist. Voraussetzung ist, dass einheitliche Bewertungskriterien anwendbar sind. Der Entscheidungsprozess an sich ist wenig transparent.[36]

2.5.3 Paarvergleichsmatrix

Mit Hilfe einer Matrix können Varianten systematisch miteinander verglichen werden. Die Matrix ist dabei das Mittel zur Strukturierung, wenn mehrere Varianten gleichzeitig verglichen werden sollen.

Verglichen wird entweder zeilen- oder spaltenweise. Der Bewertungsschlüssel muss zu Beginn festgelegt werden, dieser kann aus Zahlenwerten oder Werten wie „gut“, „neutral“, „schlecht“ bestehen. Bei Zahlenwerten wird eine Summe gebildet, beim anderen Verfahren werden Häufigkeiten gezählt.

Man muss nur eine Hälfte der Matrix ausfüllen, da die zweite Hälfte nur eine gespiegelte Variante der anderen darstellen würde.[37]

Die direkten „Duelle“ zweier gleicher Varianten (z.B. A mit A) werden nicht beurteilt, da dies überflüssig ist und meist ausgegraut dargestellt wird.

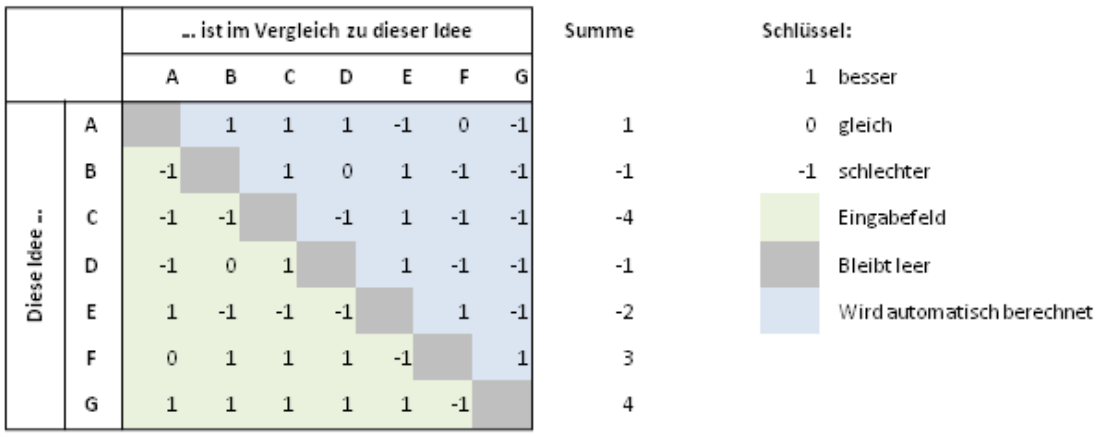
Abschließend werden die Reihensummen gebildet. Daraus entsteht das abschließende Ranking der Varianten.[38]

---

[36] Vgl. Schönwandt 2007, S. 25

[37] Vgl. Schönwandt 2007, S. 26–27

[38] Vgl. Graham, Gesamtartikel



		… ist im Vergleich zu dieser Idee							Summe
		A	B	C	D	E	F	G	
Diese Idee …	A		1	1	1	-1	0	-1	1
	B	-1		1	0	1	-1	-1	-1
	C	-1	-1		-1	1	-1	-1	-4
	D	-1	0	1		1	-1	-1	-1
	E	1	-1	-1	-1		1	-1	-2
	F	0	1	1	1	-1		1	3
	G	1	1	1	1	1	-1		4

Abbildung 2-17 Beispiel Paarvergleichsmatrix (Graham)

2.5.4 Pro und Contra Methode

Die Pro und Contra Methode dient, um einseitigen Sichtweisen vorzubeugen. Sie läuft in zwei Phasen ab und wird durch einen Pro und Contra Katalog strukturiert. Dazu wird eine Tabelle mit zwei Spalten erzeugt, wobei auf einer Seite die Pro-Argumente (Vorteile) und auf der anderen Seite die Contra-Argumente (Nachteile) gesammelt werden. Für jeden Lösungsansatz wird jeweils eine Liste angefertigt. Anschließend werden die Argumente sortiert und gewichtet. Hat man dies für alle Varianten durchgeführt, so können die Vor- und Nachteile verglichen und eine Entscheidung getroffen werden. Im Gegensatz zu anderen Verfahren ist dieses sehr rasch durchführbar, jedoch kommt am Ende nicht immer ein vollständig nachvollziehbares Ergebnis heraus, wodurch es immer wieder zu Unstimmigkeiten und Problemen im Projektverlauf kommen kann. Überwiegen die Vorteile eines Vorschlages gegenüber anderen, d.h. stehen den Vorteilen keine äquivalenten Nachteile gegenüber, ist der Vorschlag wünschenswert. Überwiegen die Nachteile, wird er abgelehnt.[39]

Pro	**Contra**
• deutsche Firmen bereits tätig • Schlüsseltechnologie • Deutsche Firmen erreichen auf diesem Gebiet Weltstandard • Relativ hoher Bedarf	• USA, GB und F führend in diesem Gebiet • Absatz abhängig vom Holzfertighausabsatz • Ständige Weiterentwicklung notwendig

Tabelle 2-1 Beispiel Pro-Contra-Bewertung von Bauelementen (Schönwandt 2007)

[39] Vgl. Schönwandt 2007, S. 28–29

2.5.5 Auswahlliste

Eine Auswahlliste wählt Varianten nach festgelegten, weitgehend allgemeingültigen Auswahlkriterien unter Nutzung eines Formblatts aus.

Eine Auswahlliste gliedert sich in 3 Arbeitsschritte.

Auswahlkriterien festlegen

Das Formblatt wird mit den vordefinierten Auswahlkriterien durchgeführt. Die Kriterien müssen anhand der vorab definierten Anforderungen abgeleitet werden und klar definiert sein. Wichtig ist hier der Grundsatz „Weniger ist mehr“, also der Schwerpunkt soll auf einigen wenigen Kernpunkten liegen.

Varianten beurteilen

Die Varianten werden hinsichtlich der Erfüllung der Auswahlkriterien beurteilt und das Ergebnis mit vordefinierten Schlüsselzeichen gekennzeichnet.

Entscheiden

Ergebnis der Auswahl ist eine eingeschränkte Menge an geeigneten Varianten, die es sich lohnt weiterzuverfolgen. Hier ist immer noch ein Risiko der Fehleinschätzung und der damit resultierenden Falschauswahl möglich.

Mit Hilfe von Auswahllisten lässt sich ein grober Überblick schaffen. Detaillierte Rankings und genaue Werte lassen sich aber nur schwer ableiten.[40]

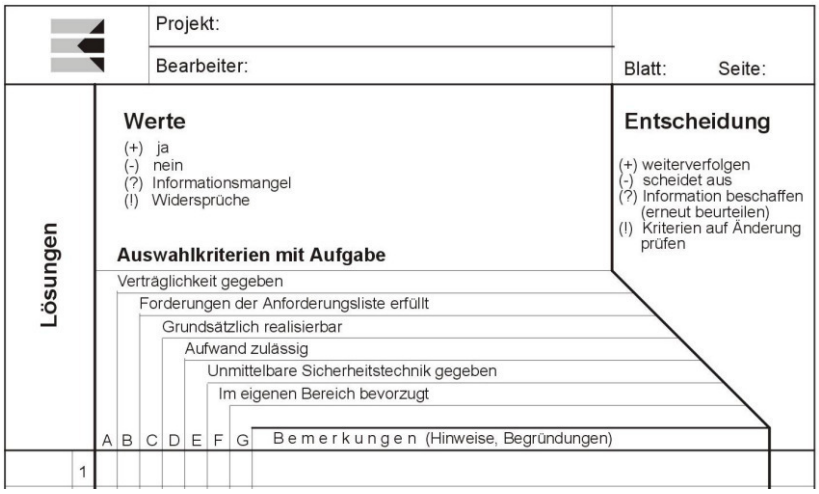


Abbildung 2-18 Beispiel Formblatt Auswahlliste (Meier)

[40] Vgl. Meier, S. 6–8

2.6 Recherchebewertung

Anhand der Rechercheergebnisse zeigt sich, wie vielfältig das Thema Überwachung im IT-Bereich ist. Alleine die Vielzahl der unterschiedlichen Protokolle bietet eine fast unendliche Anzahl an Möglichkeiten, wie die einzelnen Geräte und Bereiche in einem Unternehmen überwacht werden können. Hier sollte der Schwerpunkt aber ganz klar auf SNMP, WMI sowie Netflow gelegt werden, da hier die besten Ergebnisse mit den geringsten Netzlasten erzielt werden können und beinahe jedes Gerät eine dieser Technologien unterstützt.

Bezüglich Alarmierungsmöglichkeiten zeigt sich ganz klar ein Trend zu neuen Techniken, da sich auch hier der Markt in Richtung Cloudlösungen und mobile Verfügbarkeit entwickelt. Hier gilt es abzuwägen, wie sinnvoll solche Varianten in einem Intranetsystem sind und ob es nicht ausreichend ist, auf bewährte Systeme wie Mail und SMS zu setzen und das Ganze mittels Skriptautomatismen zu verfeinern.

Auch im Bereich der Methodik zur Softwareauswahl gibt es sehr viele unterschiedliche Ansätze. Hier gilt es einen gesunden Mittelweg zu finden, um in einem passenden Zeitraum eine Auswahl zu treffen. Dazu eignet sich vermutlich die Variante Nutzwertanalyse mit einer vorgelagerten Marktrecherche, das mit einem KO-Verfahren kombiniert wird, am besten.

Die genauen Details zeigen sich im Laufe der Detailausarbeitung, bzw. wird der Weg durch die am Ende ausgewählte Software auch in gewisser Weise vorgegeben.

Die Vielzahl der Techniken und Lösungen am Markt zeigt einmal mehr, dass die derzeit eingesetzte Vermischung diverser Lösungen klar überholt ist.

3 Präzisierung der Aufgabenstellung

Auf Basis der Recherche zum Stand der Technik wird nun die Aufgabenstellung präzisiert. Dazu werden folgende Anforderungen an die Lösung festgelegt, um den Umfang klarer einzugrenzen:

Die Vielzahl der aktuell sehr unterschiedlichen Monitoringvarianten soll durch ein einziges zentrales Tool abgelöst werden. Die Administration darf nur noch über einen einzelnen Knotenpunkt (Monitoringserver) erfolgen. Auf den zu überwachenden Geräten sind nur die Überwachungstechniken und das Netzwerk einzurichten, nicht jedoch die Alarmierung oder Überwachung selbst.

Für die Überwachung sowie die Fehlerübermittlung der einzelnen Geräte müssen am Markt übliche Techniken (laut Kapitel 2) eingesetzt werden. Programmierarbeiten oder umfangreiche Anpassungen sind strikt zu vermeiden. Es ist also so weit wie möglich, auf standardisierte Funktionalitäten zurückzugreifen.

Für das zukünftige Monitoringtool sind klare Auswahlkriterien zu definieren. Diese sollen einen Vergleich der verschiedenen Produkte ermöglichen. Die einzelnen Kriterien müssen nach Prioritäten klassifiziert werden und einen messbaren Wert aufweisen, welcher zum Ausscheiden des Produktes führt.

Eine Vorauswahl der möglichen Lösungen ist mittels Analyse des Marktes zu treffen (Internet, Literatur, Lieferantengespräche). Dazu müssen die Kernaussagen und -funktionalitäten der einzelnen Produkte erfasst werden. Die Vorauswahl ist durch KO-Kriterien auf möglichst wenige Möglichkeiten einzugrenzen.

Die möglichen Lösungsvarianten müssen in einer Testphase auf Tauglichkeit geprüft werden. Dazu müssen zu Beginn der Softwaretests klare Szenarien, Geräte und Testfälle abgesteckt werden. Der Testplan muss innerhalb eines Tages im jeweiligen Tool konfigurierbar und umsetzbar sein. Eine Auswertung der gesammelten Ergebnisse und Erkenntnisse hat nach einem Testbetrieb von maximal 2 Wochen zu erfolgen. Die Testergebnisse sind verbal und für jedes Produkt extra dokumentiert. Dazu sind die Auswahlkriterien heranzuziehen.

Auf Basis der gesammelten Erkenntnisse der Softwaretests ist eine Bewertung mittels Nutzwertanalyse vorzunehmen. Für die Bewertung sind neben den Testergebnissen auch Herstellerinformationen und eigene Erkenntnisse zu berücksichtigen. Um ein aussagekräftigeres Ergebnis zu bekommen und eine gewisse Objektivität zu gewährleisten, muss eine Gewichtung der Kriterien in die Analyse einfließen.

Das Produkt mit der höchsten Punktzahl muss als Siegertool ausgewählt werden. Persönliche Präferenzen und Meinungen dürfen die Entscheidung nicht beeinflussen und sind vorab bestmöglich in die Nutzwertanalyse zu integrieren.

Der Betrieb eines geeigneten Tools ist aus Performance- und Sicherheitsgründen auf einem physikalischen Server umzusetzen. Virtualisierung ist höchstens für einen redundanten Backupserver zulässig.

Die Auswahl der Hardware muss auf Basis der Unternehmenskriterien (Ausfallssicherheit oder Datensicherheit), sowie der Systemvoraussetzungen des Softwareherstellers erfolgen. Für einen langfristigen Betrieb und die wachsenden Anforderungen der zukünftigen Softwareversionen ist eine ausreichende Kapazität nach oben einzuplanen. In genauen Werten: mindestens 2 zusätzliche CPU Kerne, mindestens doppelter Arbeitsspeicher, mindestens doppelter Festplattenspeicher als vom Hersteller empfohlen.

Die Konzeption der Implementierung ist klar von der Implementierung selbst abzutrennen. Der eigentliche Implementierungsaufwand, der am Ende ausgewählten Software, hat in einem eigenen Projekt im Anschluss an die Diplomarbeit zu erfolgen.

Das Implementierungskonzept muss alle Einstellungen, die im System vorgenommen werden, aufweisen. Dazu gehören die Grundeinstellungen wie Servername, Benachrichtigungsserver, Skripte oder Vererbungsrichtlinien. Zudem sind die geplanten Messpunkte zu definieren und auszuwählen. Zudem muss eine geeignete Strukturierung der einzelnen Standorte, Geräte und Messpunkte festgelegt werden. Im Optimalfall als Baumstruktur, wenn dies von der Software unterstützt wird. Für die Messpunkte sind geeignete Überwachungsprotokolle zu finden und Schwellenwerte festzulegen (= Wann ist der gemessene Wert in Ordnung bzw. wann muss ein Alarm gesendet werden.). Zudem muss festgelegt werden, wie der Alarm der einzelnen Messpunkte an die zuständigen Personen gesendet wird.

Die Software muss die Möglichkeit bieten, die gemessenen Daten zu exportieren, bzw. im Optimalfall selbstständig auszuwerten (vordefinierte Reports).

Die Software muss die Möglichkeit bieten, die Messwerte zu visualisieren und Verläufe graphisch darzustellen.

Die Software ist für die IT-Abteilung über das Internet zugänglich zu machen, um jederzeit auf den Server zugreifen zu können, um die Messpunkte abzulesen.

Für die Einführung eines Tools gibt es seitens der Unternehmensleitung ein vorgeschriebenes Budget von 7000 Euro für Hard- und Software, welches nicht überschritten werden darf.

4 Analyse und Evaluierung ausgewählter Tools

In diesem Kapitel wird eine Marktanalyse für Monitoringtools durchgeführt. Dazu werden zuerst Auswahlkriterien bzw. Anforderungen des Zielsystems definiert. Danach werden die am Markt erhältlichen Tools gelistet und einer Grobbewertung unterzogen, wobei hier bereits eine Aussortierung mittels KO-Kriterien stattfinden muss. Nach einer anschließenden Testphase, der noch zur Auswahl stehenden Produkte, findet eine Nutzwertanalyse mit abschließender Entscheidungsfindung statt.

4.1 Beschreibung der Auswahlkriterien

Die Auswahlkriterien für die Software sollen einen kurzen Titel haben, um sie in den Analysemethoden besser einarbeiten zu können. Den genauen Inhalt kann man den Ausführungen auf den nächsten Seiten entnehmen.

Kosten

Ein wesentlicher Punkt bei der Suche einer passenden Software ist die Finanzierung von dieser. Wir unterscheiden zwischen den Anschaffungskosten, welche einmalig zu Beginn der Implementierung fällig sind und den laufenden Kosten (im IT-Bereich meist als Wartungskosten bekannt), welche periodisch wiederkehren und einem meist den Zugang zu neuen Versionen oder Fehlerbehebungen sowie den Support des Herstellers ermöglichen. Meist wird für ein Projekt ein Budget von der Geschäftsleitung vorgeschrieben, welches nicht überschritten werden darf.

Erstkonfiguration

Für die Erstkonfiguration muss der ausführende Mitarbeiter mehr oder weniger Arbeitszeit investieren. Da diese Zeit oft kostenintensiver für das Unternehmen ist, als die Kosten der Software selbst, ist dieses Kriterium ein wesentlicher Punkt. Je nach Komplexität und Benutzerfreundlichkeit kann die Erstkonfiguration zwischen wenigen Stunden oder Tagen bis hin zu mehreren Wochen dauern. In manchen Fällen benötigt man auch externes Knowhow, was ebenfalls zu hohen Kosten führen kann.

Systemwartung

Nach der Erstkonfiguration sollte das System zufriedenstellend laufen. In der Praxis zeigt sich jedoch, dass immer wieder Änderungen, Anpassungen sowie Erweiterungen notwendig sind. Diese Tätigkeiten fallen unter den Begriff Wartung oder Wartungsaufwand. Auch hier kommt es vor allem auf die Benutzerfreundlichkeit des Systems an, wie viel Aufwand man investieren muss, um die gewünschte Neuanforderung abbilden zu können.

Überwachungsmethoden

Jede Monitoringsoftware hat meist eine Spezialisierung. In diesem Kriterium soll die Flexibilität der Überwachungsmethoden bewertet werden, da jede Gerätetype hier andere Anforderungen aufweist. Für ein klassisches Gesamtmonitoring ganzer IT-Systeme ist ein breites Portfolio an Überwachungsmethoden notwendig. Wenn jedoch nur ein Spezialgebiet oder einzelne Bereiche im Monitoring abgebildet werden sollen, so bietet sich eine Spezialisierung auf genau diese Überwachungsprotokolle an. Soll beispielsweise nur der Netzwerkverkehr überwacht werdenb reicht eine Spezialsoftwareb welche sich mit Netflow beschäftigt.

Cloudanbindung

Das Thema Cloud ist im heutigen Alltag nicht mehr wegzudenken. Daher muss hier die Möglichkeit der Nutzung von Clouddiensten betrachtet werden. Welche Dienste können wie genutzt werden? Beispielsweise kann eine Benachrichtigung bzw. ein Alarm mittels Clouddiensten versendet werden oder die Datenablage und der Datenzugriff über solche Systeme stattfinden. Hier gilt es die Sinnhaftigkeit abzuschätzen, da Clouddienste meist mit Kosten verbunden sind.

Mobilität

Mobilität ist ein weiteres Kernthema der modernen IT. Hier gibt es viele Möglichkeiten wie man ein Tool, online zugänglich machen kann. Ein Entscheidungskriterium ist unter anderem die Verfügbarkeit auf den unterschiedlichen Plattformen wie Android oder iOS, bzw. die klassische Verfügbarkeit über einen Webbrowser. Man muss hier auch bedenken, welche Infos man hier zur Verfügung stellen kann. Oftmals ist dies vom Hersteller so nicht vorgesehen. Eventuell ist auch der Zugang mittels einer gesicherten Verbindung (z.B. VPN) ein möglicher Weg, um Mobilität zu gewährleisten.

Alarmierungsvarianten

Wie vielfältig können Fehler zu den Mitarbeitern gebracht werden? Diese Frage muss man sich bei dieser Anforderung stellen. Auch hier gibt es von den Herstellern unterschiedlichste Ansätze und Realisierungsvarianten. Eine Redundanz ist hier oberstes Gebot. Sollte eine Alarmierungsvariante ausfallen, müssen die Infos im Fehlerfall trotzdem noch zum Mitarbeiter gelangen können. Oftmals liefern die Systeme fertige Mailversandoptionen, manchmal können auch eigene Server angebunden werden.

Automatisierung

Unter gewissen Umständen oder bei gewissen Fehlerbildern muss kein Eingreifen durch den Administrator stattfinden, um den Fehler zu beseitigen. Um eine selbstständige Fehlerbehebung des Systems zu ermöglichen, muss die Software eine automatische Ausführung gewisser Befehle (z.B. Skriptausführung) ermöglichen.

Standortübergreifend

Aufgrund wachsender Infrastrukturen und mehrerer Firmenstandorte, kann nicht immer eine direkte Netzwerkanbindung durch das System stattfinden. Das Monitoringtool muss eine einfache Möglichkeit bieten, auch externe Standorte oder evtl. vereinzelte Systeme bei Kunden oder Lieferanten zu überwachen und den betroffenen Mitarbeitern jederzeit Informationen über diese Geräte liefern können. Am besten ohne einen VPN-Tunnel oder ähnliche Zugangskonzepte einrichten zu müssen.

Bedienbarkeit

Die Konfiguration ist meist nur der Anfang für die Einführung eines Gesamtsystems. Sobald das System läuft, muss es auch einfach bedient werden können. Die Bedienbarkeit muss auch Mitarbeitern ohne Hintergrundkenntnisse des Systems möglich sein. Hier geht es um Datenansicht und Datenauswertung und nicht um Konfigurationsarbeiten. Somit ist eine übersichtliche Benutzeroberfläche, eine gewisse Anpassbarkeit, sowie ein schnelles Zurechtfinden bei der Anwendung, ein wichtiges Kriterium bei der Auswahl einer passenden Softwarelösung. Eine komplizierte Bedienung führt oftmals zum Scheitern, spätestens beim Umschalten auf den Dauerbetrieb, selbst wenn die eigentliche Funktionalität der Software ansonsten bestens geeignet wäre.

Installation

Wie aufwändig ist die Installation der Software bzw. kann diese ohne Hilfe eines externen Consultings durchgeführt werden? Welche Vorbedingungen (z.B. Datenbankserver, Treiber oder Frameworks) müssen für die Installation bereitgestellt werden, damit die Software am Ende problemlos funktioniert. Welches Betriebssystem ist für einen Betrieb des ausgewählten Tools erforderlich. Auch hier gilt es, das Kriterium nicht mit dem Thema Konfiguration zu verwechseln. Kann die Installation auf der vorhandenen Serverstruktur umgesetzt werden Auch das Thema Migration, also die Umsiedelung zu jedem Zeitpunkt auf einen neuen Server und dies ohne größeren Aufwand`, ist hier mit zu betrachten. Können firmenspezifische IT-Vorgaben bzgl. Softwareinstallationen erfüllt werden? (z.B. Alle Services müssen unter Windows funktionieren.)

Hardwarekonzept

Welche Anforderungen hat die Software an die Hardware. Sind bestimmte Komponenten notwendig oder reicht ein Standardsystem? Eine weitere Frage, die man sich in dieser Anforderung stellen muss, ist die Art und Weise, wie die Software betrieben werden kann. Läuft sie nur auf physischen Servern oder ist es auch möglich, virtuelle Maschinen zu verwenden. Auch hier sind die firmenspezifischen Anforderungen an den Server zu berücksichtigen. Diese können z.B. bestimmte Hersteller oder Versorgungskonzepte sein. Ansonsten kann hier das Schnittstellenkonzept (Anbindung an das Netzwerk) oder die Datenträgerverwaltung (RAID-Verbund) ein Thema für die Hardwareauswahl sein.

Redundanz

Redundanz ist wichtig für die Ausfallssicherheit bzw. Hochverfügbarkeit von Systemen. Bietet die Software die Möglichkeit, einen zweiten Server zu betreiben, der im Fehlerfall den Betrieb übernimmt? Die Grundsatzfrage ob Redundanz für das Monitoring tatsächlich notwendig ist, muss im Laufe des Projekts geklärt werden.

Sicherheit

Ein Sicherheitskonzept für IT-Systeme ist heutzutage nicht mehr wegzudenken. Angefangen bei der Zugriffsverwaltung, über Berechtigungen bis hin zu verschlüsselter Übertragung, das Thema Sicherheit in der IT wird sehr groß geschrieben. Da mit einem Monitoring Tool auf verschiedenste Kernsysteme von verschiedenen Abteilungen und deren Mitarbeitern zugegriffen wird, muss es hier bestimmte Einschränkungen geben. Somit ist eine User- oder Gruppenverwaltung, sowie die Anpassung der Zugriffsrechte (Wer sieht was? Oder besser Wer darf Was?) ein Kernthema für das Sicherheitskonzept. Daneben ist die Datensicherung über ein bestehendes Backupsystem des Unternehmens ein wichtiges Sicherheitskriterium.

Lizenzmodell

Für jede Software im kommerziellen Bereich wird eine Lizenzierung benötigt. Hier gibt es von den Herstellern viele unterschiedliche Varianten. Oftmals wird durch kompliziertes Baukastensysteme oder Ähnliches eine Auswahl des passenden Modells für das eigene Vorhaben sehr unübersichtlich und die Transparenz für eine richtige Entscheidung ist nicht mehr wirklich gegeben. Daher ist ein einfach zu überblickendes Lizenzmodell ein wichtiges Auswahlkriterium.

4.2 Klassifizierung der Auswahlkriterien

Die in Punkt 4.1 definierten Auswahlkriterien müssen nun sinnvoll klassifiziert werden. Hier bietet sich eine Gliederung wie bereits beim Thema Nutzwertanalyse an.

Die einzelnen Kriterien werden folgendermaßen eingeteilt:

- Muss-Kriterien
- Soll-Kriterien
- Kann-Kriterien

Bei den Muss-Kriterien ist ein Bereich zu definieren, der nicht überschritten werden darf und somit zu einem KO-Kriterium wird.

Die genaue Generierung der Wertebereiche in den einzelnen Auswahlkriterien erfolgt in einem späteren Schritt, bei der Erstellung einer detaillierten Bewertungsskala.

Kriterium	Klassifizierung	KO-Bewertung wenn
Kosten	Muss-Kriterium	Anschaffungskosten > 7000 Euro, Wartungskosten > 20% des Anschaffungswertes jährlich.
Erstkonfiguration	Muss-Kriterium	< 5 Tage (1 Arbeitswoche)
Systemwartung	Muss-Kriterium	Neugerät umständlich integrierbar. Support Uunzureichend
Überwachungsmethoden	Muss-Kriterium	Eines der Protokolle SNMP, WMI, Netflow, Powershell nicht vorhanden, Spezialisierung auf Gerätetyp
Cloudanbindung	Kann-Kriterium	-
Mobilität	Soll-Kriterium	-
Alarmierungsvarianten	Muss-Kriterium	Alarmierung per Mail und SMS nicht möglich. Alarmierung erfordert immer Firmeninternet
Automatisierung	Soll-Kriterium	-
Standortübergreifend	Kann-Kriterium	-
Bedienbarkeit	Muss-Kriterium	Einschulung der Mitarbeiter nötig
Installation	Muss-Kriterium	Möglichkeit der Virtualisierung nicht möglich, System läuft vollständig in der Cloud. Nur Linux möglich, Agents notwendig

Hardwarekonzept	Muss-Kriterium	Passendes HW-Konzept liegt über 2500 Euro. HW-Konzept kann von der Firma Dell nicht realisiert werden
Redundanz	Kann-Kriterium	-
Sicherheit	Muss-Kriterium	Benutzerprofile, Rechteverwaltung, Passwortschutz nicht möglich
Lizenzmodell	Muss-Kriterium	Unübersichtliches und kompliziertes Lizenzierungsmodell (keine Transparenz)

Tabelle 4-2 Klassifizierung der Kriterien

4.3 Monitoringprodukte

Anhand einer Internetrecherche, Fachartikelrecherche sowie durch die Anfrage bei diversen Lieferanten, wird eine Liste möglicher Kandidaten inklusive einer Kurzbeschreibung erstellt. Diese als Longlist bezeichnete Auswahl wird mittels den zuvor definierten KO-Bewertungen möglichst stark gekürzt. Da der Markt hier fast endlos ist, muss über Eigeneinschätzung und Bewertung der Herstellerangaben möglichst schnell entschieden werden, ob ein Tool für eine genauere Betrachtung infrage kommt oder gleich wieder verworfen wird.

Die Darstellung der Kurzbeschreibungen erfolgt in Form eines Steckbriefes in Tabellenform und beinhaltet die Zeilen: Hersteller, Lizenzmodell, ungefähre Kosten, sowie einige Stichpunkte über das System an sich, welche für die Entscheidungsfindung hilfreich sein könnten. Die Stichpunkte können Funktionsumfang, Einsatzgebiete, eigene Einschätzungen, aber auch allgemeine Eigenschaften sein. Ebenfalls wird jeweils noch ein Screenshot zur Visualisierung beigefügt, um den Ersteindruck der unterschiedlichen Produkte besser zu verdeutlichen. Um den zeitlichen Rahmen hier nicht zu sehr zu beanspruchen, soll sich die Kurzbeschreibung auf einige wichtige Kernpunkte einschränken.

4.3.1 Mögliche Varianten (Longlist)

Wie bereits kurz angesprochen, gibt es noch viel mehr Varianten auf dem Markt. In der Longlist sind jene Tools in alphabethischer Reihenfolge aufgelistet, welche nach einer raschen Eigeneinschätzung möglicherweise zum Einsatz kommen könnten.

Check_MK Enterprise	
Hersteller	Mathias Kettner
Lizenzmodell	Softwaresubscription + Supportcredits
Ungefähre Kosten	Jährliche Kosten von rund 5500 Euro bei Vollausbau inkl. Bronzesupport
Stichpunkte laut Hersteller	Automatische Service-Erkennung, basiert auf Nagios/Linux, hohe Performance, klassische SNMP Überwachung

Tabelle 4-3 Kurzbeschreibung Check_MK Enterprise (Kettner 2017)

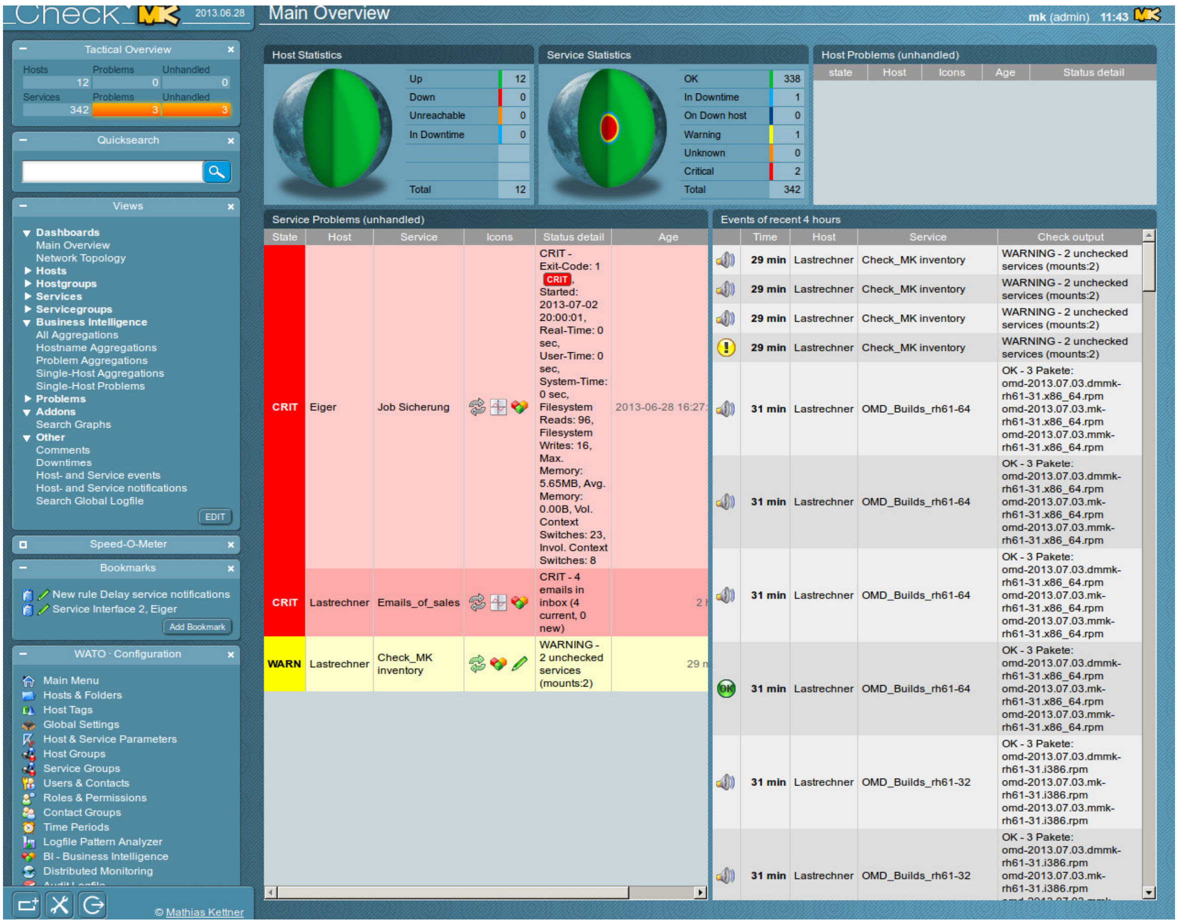


Abbildung 4-19 Screenshot Check_MK Enterprise (Kettner 2017)

GFI Events Manager	
Hersteller	GFI
Lizenzmodell	Je Knoten (=Gerät)
Ungefähre Kosten	5500 Anschaffungskosten, 1500 Wartungsgebühr pro Jahr
Stichpunkte laut Hersteller	Monitoring und Management der gesamten IT-Infrastruktur, umfassende Quellen für Abfragen, Berichterstattung automatisch, einfache Benutzeroberfläche, verteilte Umgebungen möglich

Tabelle 4-4 Kurzbeschreibung GFI Events Manager (GFI 2017)

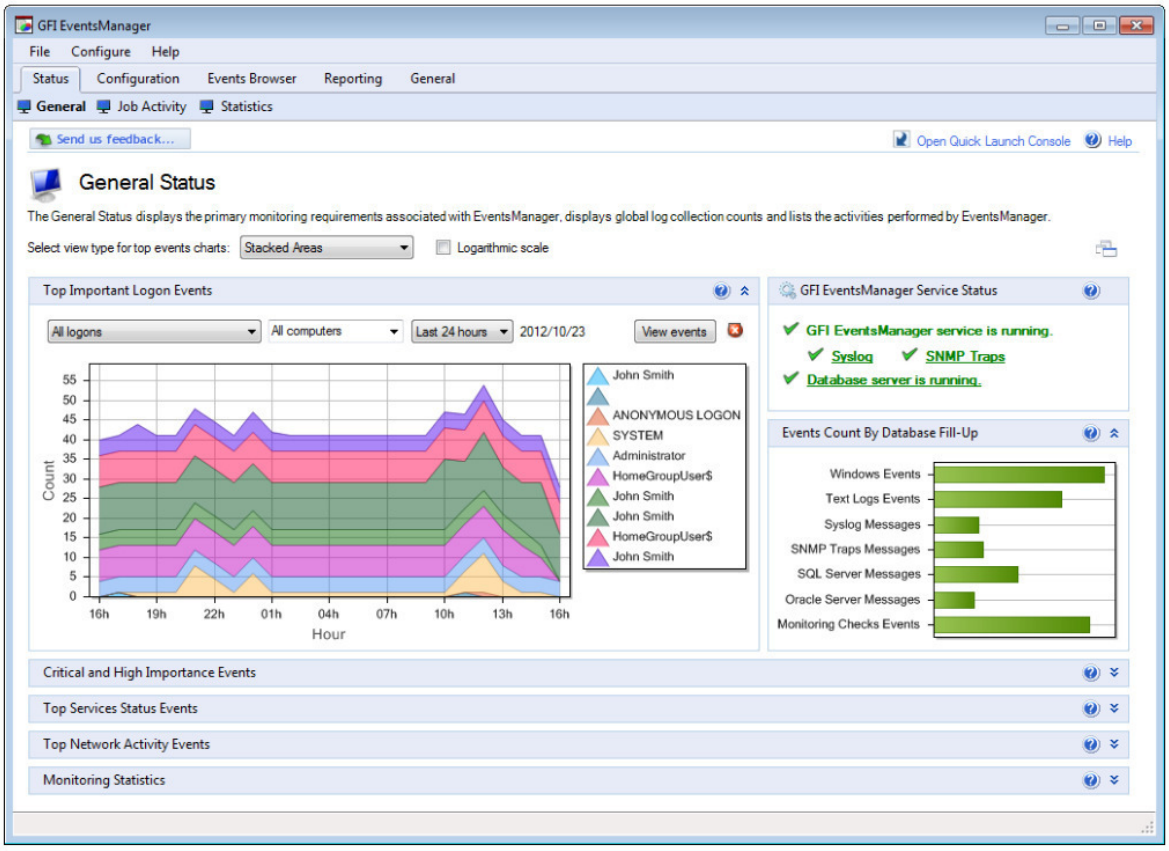


Abbildung 4-20 Screenshot GFI EventsManager (GFI 2017)

Hyperic HQ	
Hersteller	Hyperic
Lizenzmodell	Open Source
Ungefähre Kosten	Keine
Stichpunkte laut Hersteller	Open Source Tool zur Überwachung eines Gesamtsystems, Server-Agent System, basierend auf Java, graphische Oberfläche und Auswertung, Spezialisierung auf Serverüberwachung

Tabelle 4-5 Kurzbeschreibung Hyper HQ (Sacks 2009)

Abbildung 4-21 Screenshot Hyperic HQ (Vardanyan 2011)

ManageEngine OPManger	
Hersteller	ManageEngine
Lizenzmodell	Geräteanzahl
Ungefähre Kosten	995 USD für 25 Devices, für 330 Devices rund 12000 USD
Stichpunkte	Netzwerkmanagement, Servermanagement, Netzwerkdurchsatz Analyse, Konfigurationsmanagement, Datacenter Management, sehr detailliert und umfangreich

Tabelle 4-6 Kurzbeschreibung Manage Engine OPManger (ManageEngine 2017)

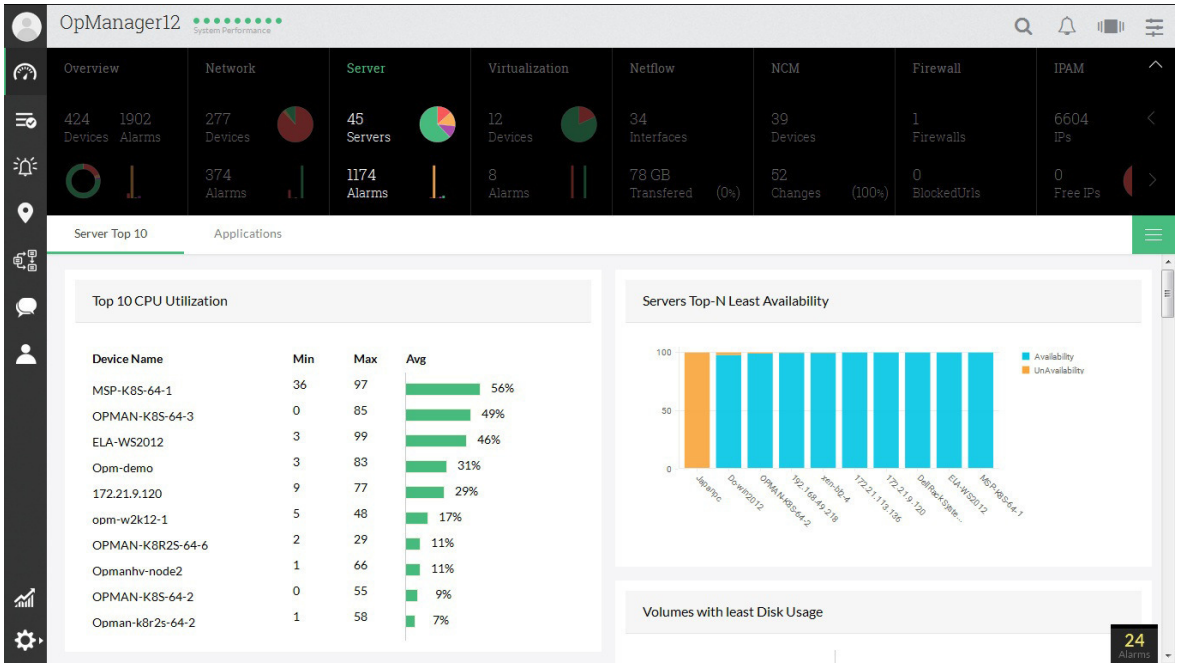


Abbildung 4-22 Screenshot Manage Engine OPManager (ManageEngine 2017)

System Center Operations Manager	
Hersteller	Microsoft
Lizenzmodell	Softwarebasislizenz + User CAL‘s
Ungefähre Kosten	Ab ca. 3500 Euro
Stichpunkte	Sehr umfangreiches Tool mit vielen Umsetzungsmöglichkeiten, sehr mächtig in größeren Umgebungen, mehrtägige Erstkonfiguration, Spezialisierung auf heterogene Server- und Clientlandschaften.

Tabelle 4-7 Kurzbeschreibun System Center Operations Manager (Grote 2015)

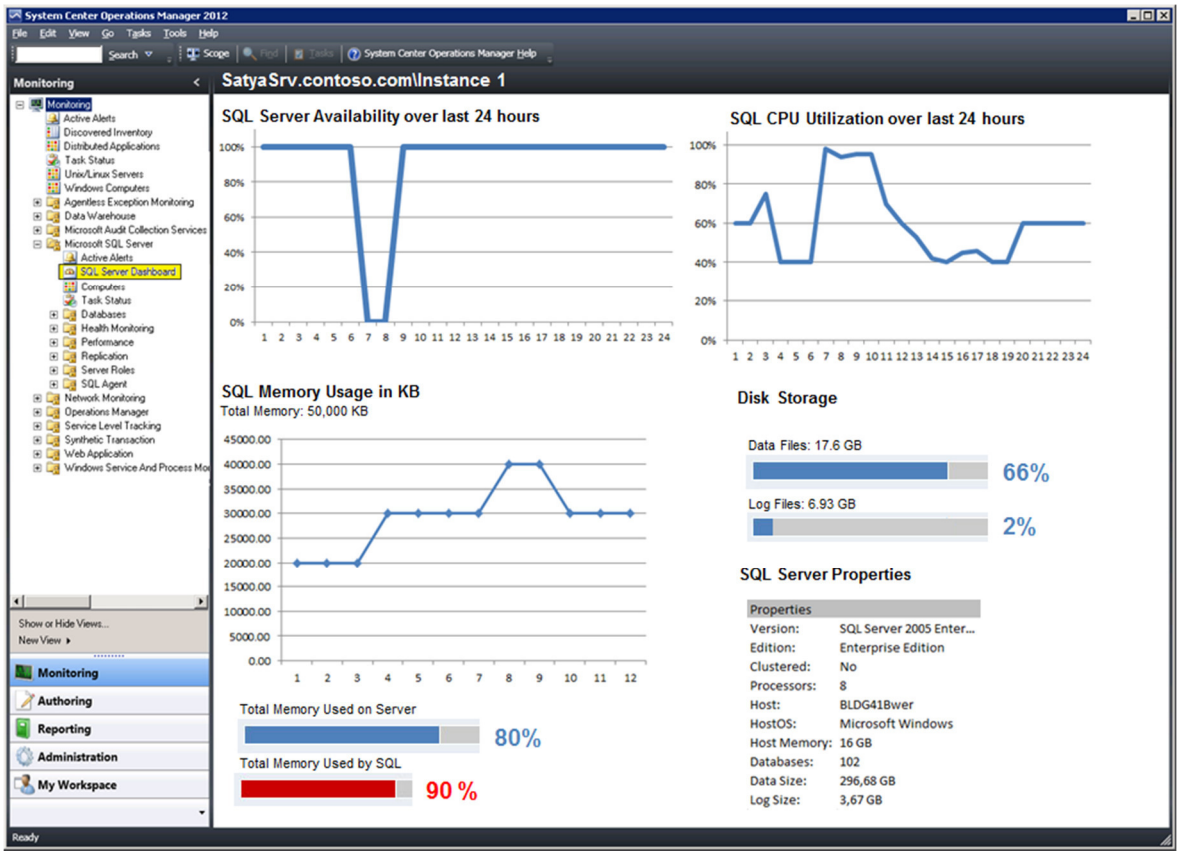


Abbildung 4-23 Screenshot System Center Operations Manager (Souvickroy 2017)

Nagios Core	
Hersteller	Nagios
Lizenzmodell	Freeware
Ungefähre Kosten	Keine für Freeware
Stichpunkte	Bekanntestes Freewaretool im Monitoring-bereich, linuxbasierend, großes KnowHow für Einrichtung erforderlich (mehrwöchiges Einarbeiten), gute Performance, große Community, gute Performance, virtualisier-bar, Premiumfunktionalitäten (Nagios XI) kostenpflichtig.

Tabelle 4-8 Kurzbeschreibung Nagios Core (Nagios 2017)

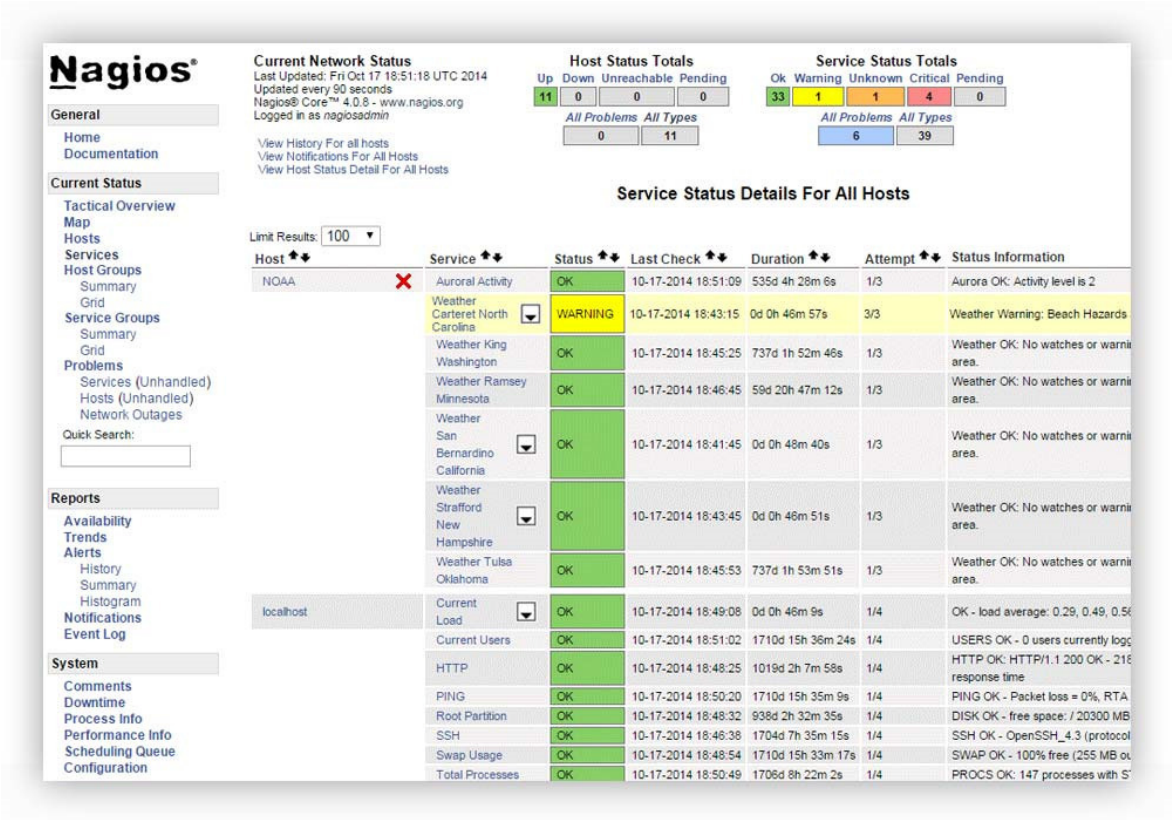


Abbildung 4-24 Screenshot Nagios Core (Nagios 2017)

OpenNMS	
Hersteller	OpenNMS Group
Lizenzmodell	Freeware
Ungefähre Kosten	Keine
Stichpunkte	Einsatz in Gesamtinfrastrukturen, Standardprotokolle integriert, flexibel konfigurierbar, basiert auf Java, Alarmierungsmöglichkeiten eingeschränkt, Erweiterungen umständlich mittels API

Tabelle 4-9 Kurzbeschreibung OpenNMS (OpenNMS 2017)

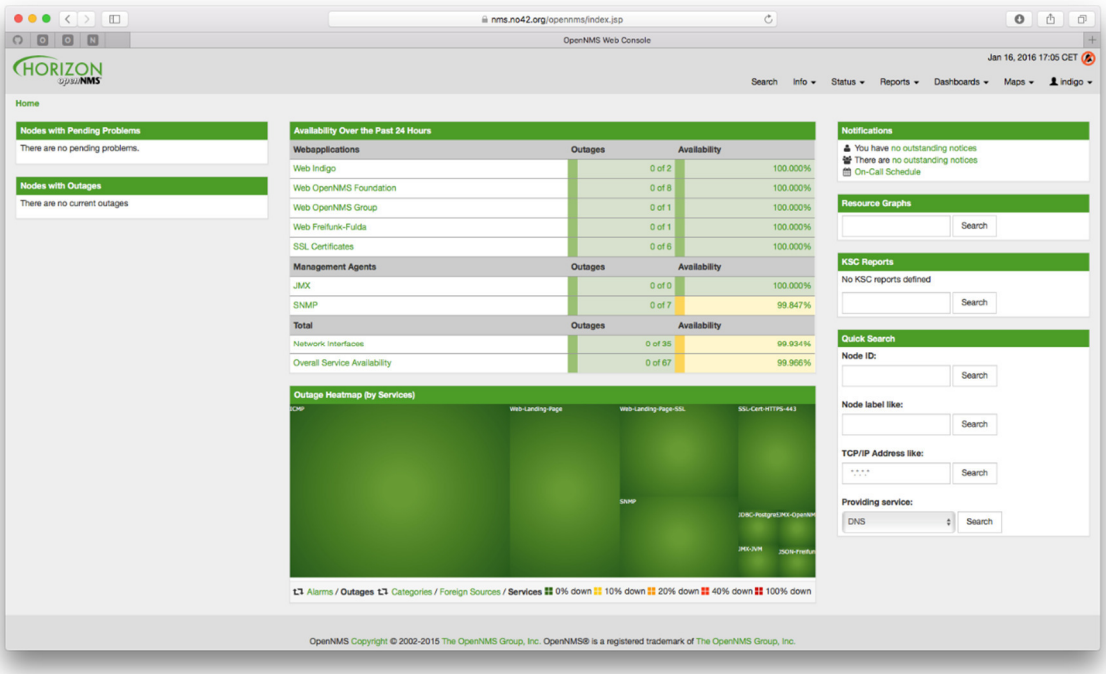


Abbildung 4-25 Screenshot OpenNMS (OpenNMS 2017)

PRTG Network Monitor	
Hersteller	Paessler
Lizenzmodell	Universelle Sensoren
Ungefähre Kosten	1000 Sensoren für rund 3700 Euro inkl. 36 Monate Wartung
Stichpunkte	All-in-One Netzwerküberwachung, Automatische Einrichtung, große Community für Anpassungen, vielseitiger Einsatz

Tabelle 4-10 Kurzbeschreibung PRTG Network Monitor (Paessler 2017)

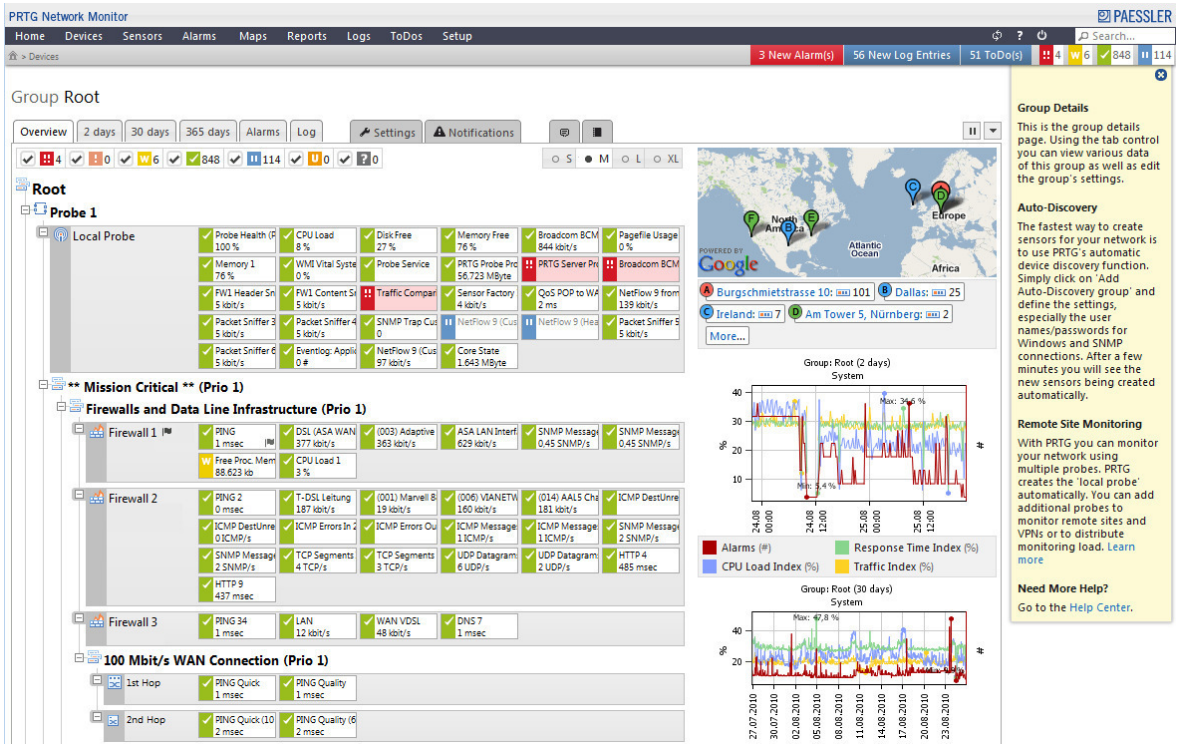


Abbildung 4-26 Screenshot Paessler PRTG

Server Eye	
Hersteller	Servereye
Lizenzmodell	Auch nach mehrmaliger Nachfrage keine Informationen
Ungefähre Kosten	Auch nach mehrmaliger Nachfrage keine Informationen
Stichpunkte	Extern gehostetes Monitoringtool (SaaS), Netzwerk usw., Patchmanagement, Fern-wartung, Managed Antivirus

Tabelle 4-11 Kurzbeschreibung Server Eye (ServerEye 2017)

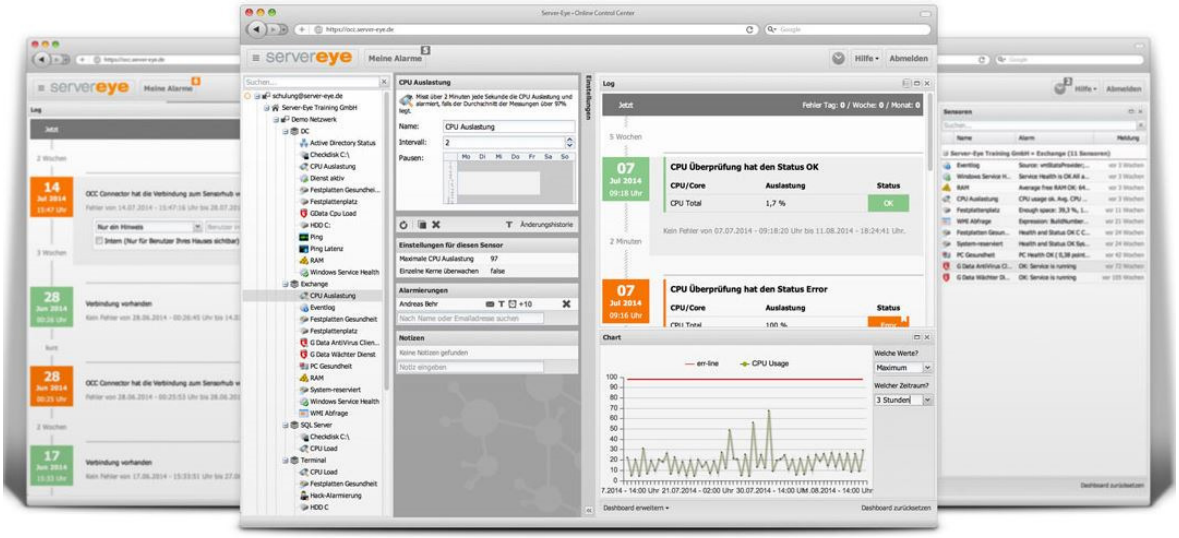


Abbildung 4-27 Screenshot Server Eye (ServerEye 2017)

Solar Winds Netzwerküberwachung	
Hersteller	Solarwinds
Lizenzmodell	Baukastensystem mit diversen Modulen
Ungefähre Kosten	Für Netzwerk und Serverüberwachung rund 6500 Euro
Stichpunkte	Herstellerunabhängige Netzwerküberwachung, automatische Kapazitätsplanung und –prognose, intelligente Alarmierungskonzepte, Bandbreitenanalyse und Auswertung, Baukastensystem eher unübersichtlich, genaue Details für Serverüberwachung nur mit Testversion eruierbar.

Tabelle 4-12 Kurzbeschreibung Solar Winds Netzwerküberwachung (Solarwinds 2017)

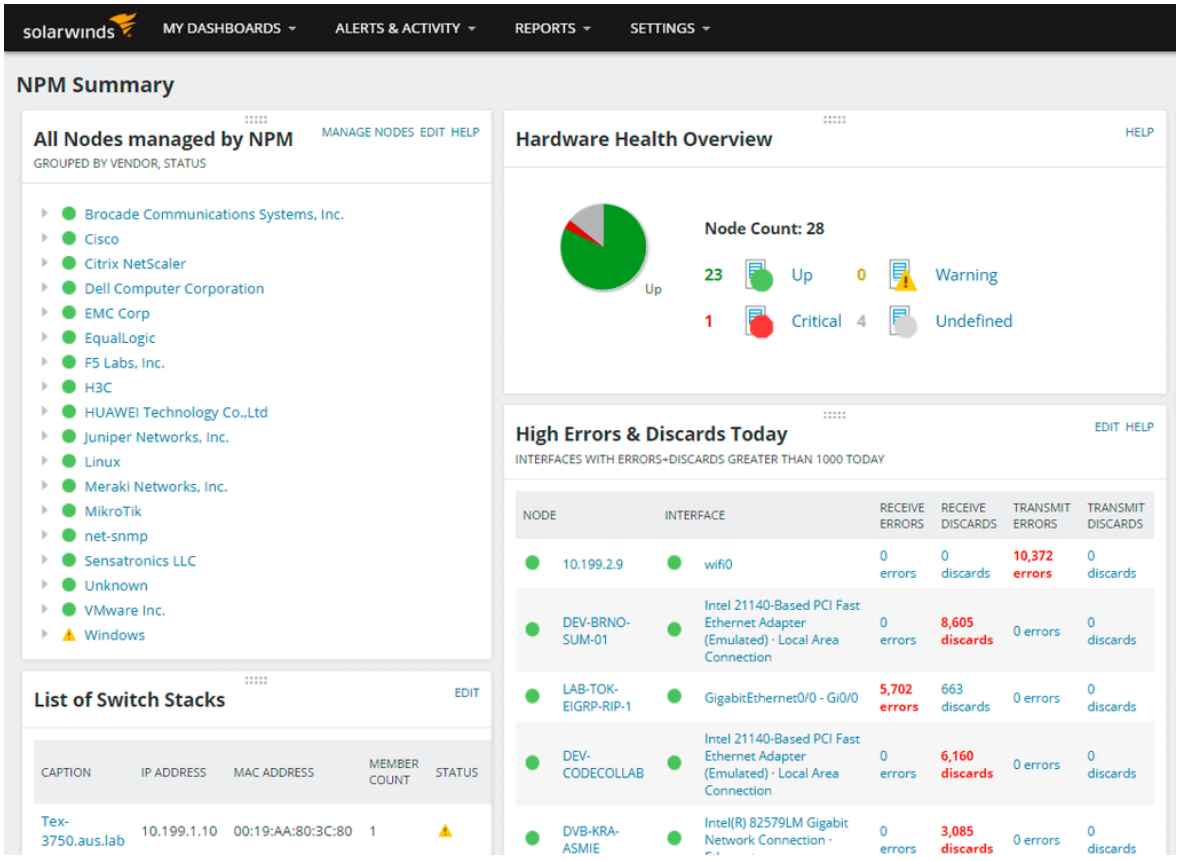


Abbildung 4-28 Screenshot Solar Winds Netzwerküberwachung (Solarwinds 2017)

vRealize Hypertic	
Hersteller	vmWare
Lizenzmodell	Anzahl an überwachten Maschinen
Ungefähre Kosten	360 USD pro überwachter Maschine
Stichpunkte	Infrastruktur und Betriebssystem Monitoring, gutes Reporting, spezialisiert auf Virtuelle Umgebungen und Produkte der Firma vmWare, über API erweiterbar, Alarmierung direkt über vmWare Services

Tabelle 4-13 Kurzbeschreibung vRealize Hypertic (vmWare 2017)

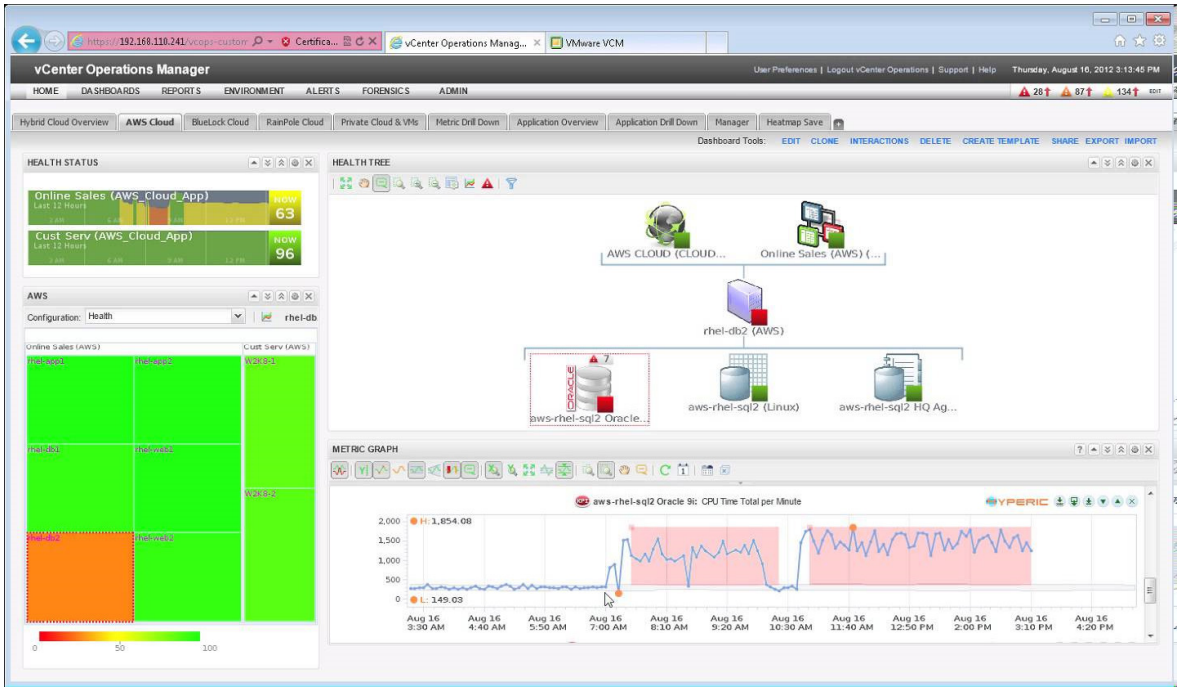


Abbildung 4-29 Screenshot vRealize Hypertic (vmWare 2017)

WhatsUp Gold	
Hersteller	Ipswitch
Lizenzmodell	Punktesystem
Ungefähre Kosten	6700 Euro für 300 Punkte inkl. 12 Monate Wartung
Stichpunkte	All-in-One Monitoring, Fehlerbehebung, automatischer Netzwerkplan, Visualisierung kritischer Bereiche, Bandbreitenanalyse

Tabelle 4-14 Kurzbeschreibung WhatsUp Gold (Ipswitch 2017)

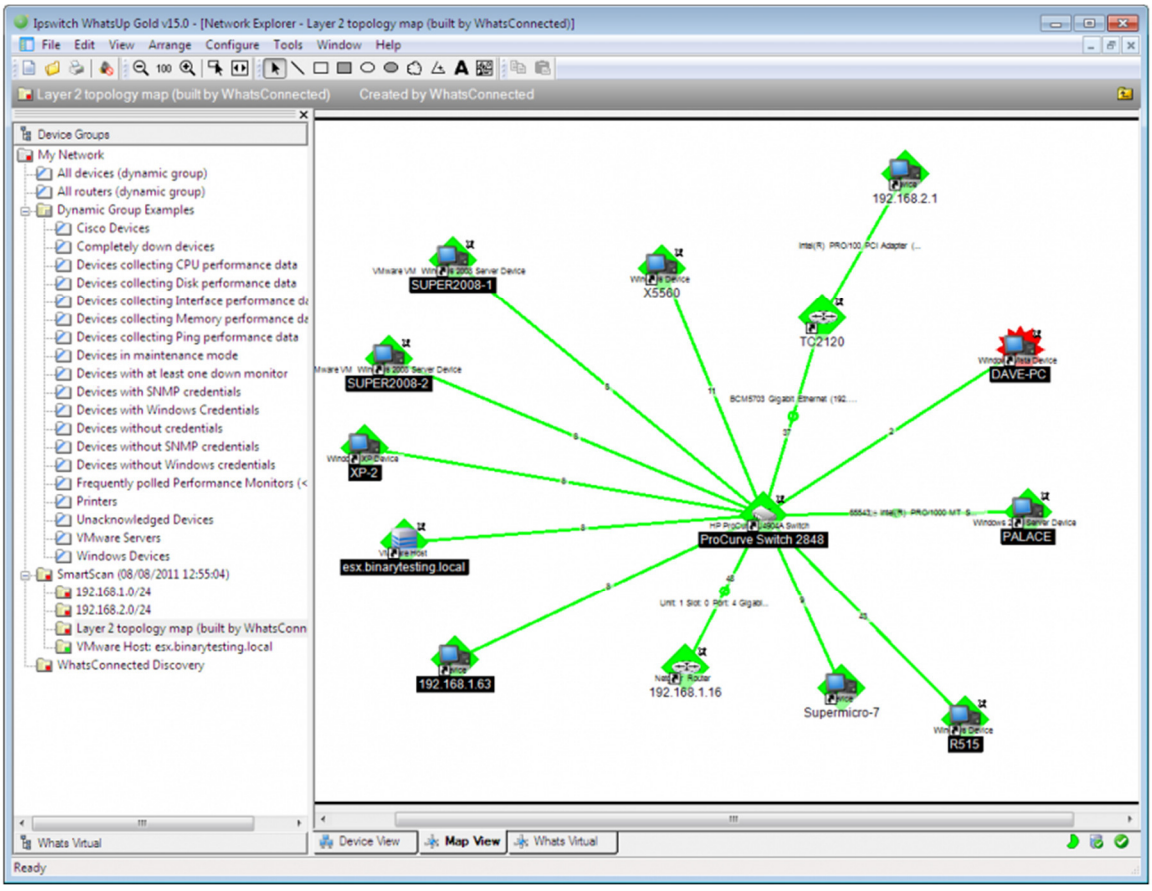


Abbildung 4-30 Screenshot WhatsUp Gold (Ipswitch 2017)

Wireshark	
Hersteller	Wireshark-Community
Lizenzmodell	Freeware
Ungefähre Kosten	Keine
Stichpunkte	Netzwerksniffer, Protokollierung aller eingehenden Netzwerkpakete an einem Punkt, Filtermöglichkeiten, Spezialsoftware für Netzwerkverkehr

Tabelle 4-15 Kurzbeschreibung Wireshark (Wireshark 2017)

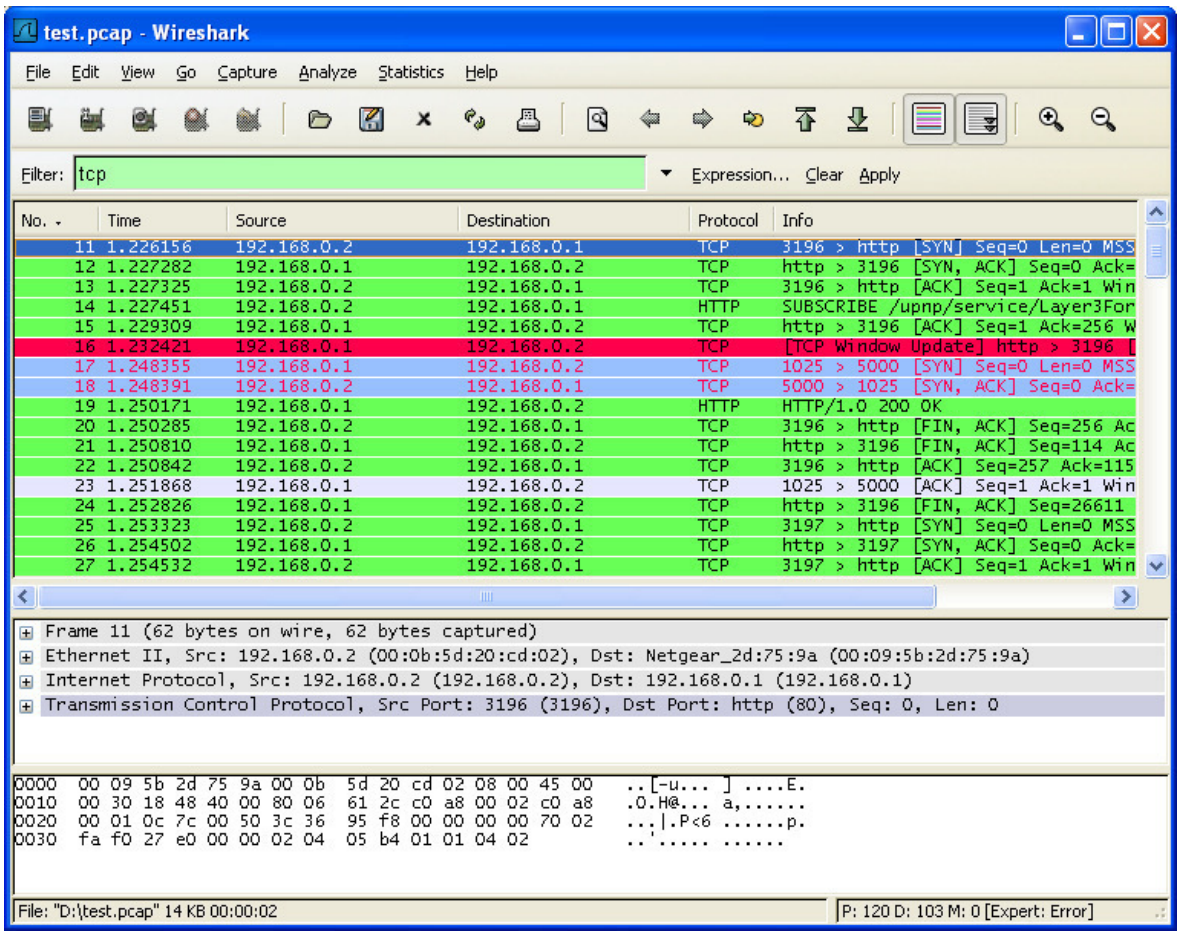


Abbildung 4-31 Screenshot Wireshark (Wireshark 2017)

Zabbix	
Hersteller	Zabbix by Alexei Vladishev
Lizenzmodell	Freeware
Ungefähre Kosten	Keine
Stichpunkte	OpenSource Monitoring, Server-Agent System, ICMP, SNMP, WMI ohne Agent möglich, webbasiertes Interface, service-basierte Serverinstallation, linuxbasierend

Tabelle 4-16 Kurzbeschreibung Zabbix (Wiki Zabbix 2017)

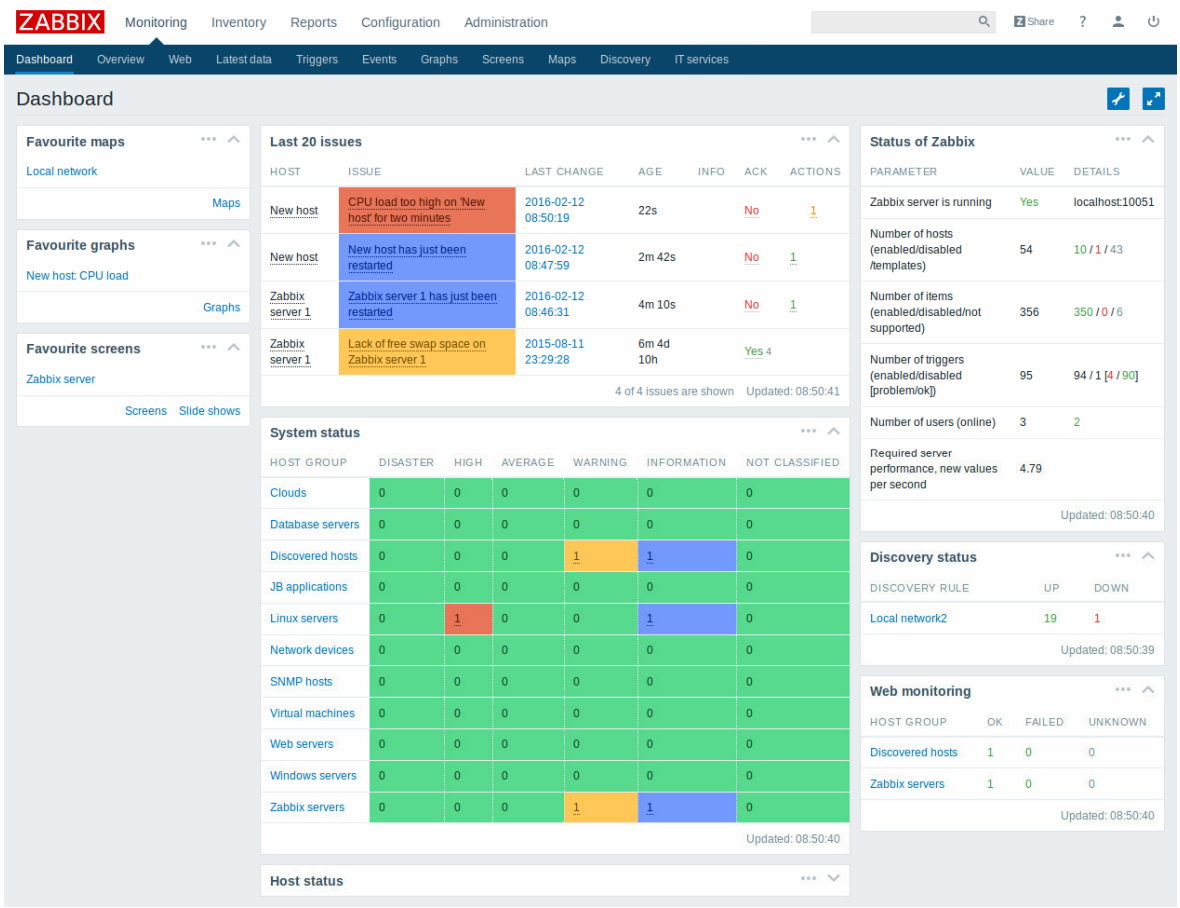


Abbildung 4-32 Screenshot Zabbix (Wiki Zabbix 2017)

4.3.2 Eingrenzung der Varianten

Mittels der definierten KO Kriterien soll die Longlist bestmöglich gekürzt werden, sodass am Ende nur mehr wenige Varianten in die Entscheidungsrunde weiterkommen. Als Darstellungsform für diese Schnellanalyse bietet sich die Form einer Tabelle an.

Produkt	KO-Kriterium
Check_MK	Wartungskosten zu hoch, umständliche Einrichtung
GFI Events Manager	Vorerst keine KO-Kriterien
Hyperic HQ	Agent auf jedem Gerät notwendig, Spezialisierung auf Serverüberwachung
ManageEngine OP Manager	Anschaffungskosten zu hoch, umständliche Bedienbarkeit
System Center Operations Manager	Spezialisiert auf Serverstrukturen, kompliziertes Lizenzmodell
Nagios	Basiert auf Linux, sehr lange Einrichtungszeit, lange Einarbeitungszeit, Premiumfuntion teuer
OpenNMS	Eingeschränkte Alarmierungsmöglichkeiten, umständliche Anpassungen mittels API
PRTG Network Monitor	Vorerst keine KO-Kriterien
Server Eye	Extern gehostet (SaaS), Herstellerkommunikation mangelhaft
SolarWinds Netzwerküberwachung	Vorerst keine KO-Kriterien

vRealize Hypertic	Spezialisierung auf virtuelle Maschinen auf einem vmWare-System
WhatsUP Gold	Vorerst keine KO-Kriterien
Wireshark	Kann nur Netzwerkpakete überwachen
Zabbix	Server-Agent System für detailliertes Monitoring notwendig

Tabelle 4-17 Bewertung der Longlist mittels KO-Kriterien

Somit kommen folgende Produkte am Ende des Bewertungsprozesses in die finale Auswahlrunde und werden genauer getestet:

- GFI Events Manager
- PRTG Network Monitor
- Solar Winds Netzwerküberwachung
- WhatsUp Gold

4.4 Testphase

Die vier ausgewählten Tools werden nun mittels einer Testlizenz über einen Zeitraum von mehreren Wochen überprüft. Dazu werden mit jeder Software, die gleichen zuvor definierten Geräte und Szenarien testweise überwacht. Anschließend werden die Testergebnisse dokumentiert und die Softwarefunktionalitäten und -eigenschaften noch genauer vorgestellt.

4.4.1 Definition der Testszenarien

Für die Tests sollen von jeder Software dieselben Geräte überwacht werden. Die Messpunkte müssen hier alle möglichen Eventualitäten und Spezialbereiche umfassen, um diese anschließend im Echtsystem dementsprechend zu skalieren.

Gruppierung der Messwerte nach Gerätegruppen

Nachfolgend werden die Gerätegruppen, welche von der Software überwacht werden müssen, definiert, sowie die zu erhebenden Messwerte allgemein definiert. Diese müssen vom System unbedingt abgebildet bzw. erfasst werden können, um eine flächendeckende Überwachung zu ermöglichen. Hierbei werden noch keine genauen Geräte festgelegt.

Abbildung 4-33 Schema Gerätegruppen

Detailspezifikation der Testgeräte

Die vorab definierten Gruppen werden nun konkreten Geräten zugeordnet. Wichtig ist, dass jeder definierte Messpunkt 1x auf einem Gerät überwacht wird. Die gewählte Darstellungsform ist hierbei ein Strukturbaum, da hier die beste Übersichtlichkeit erreicht wird. Es wird auch bedacht, dass unterschiedliche Standorte überwacht werden sollen. Auch an den externen Standorten (ausgehend von der Firmenzentrale) muss jeweils mindestens 1 Gerät überwacht werden.

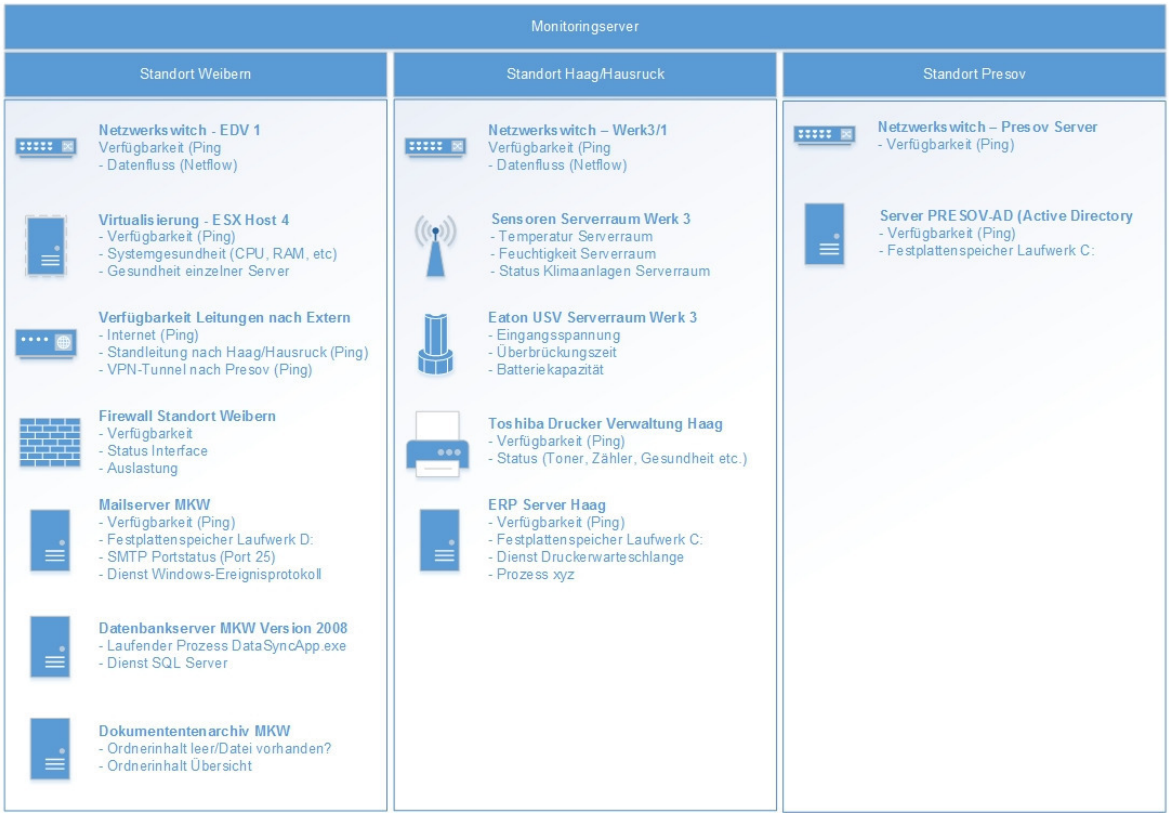


Abbildung 4-34 Schema Teststruktur

4.4.2 Testdurchführung

Für die Testdurchführung werden die Evaluierungslizenzen auf einem Testsystem installiert. Danach wird versucht, die zuvor definierten Testszenarien in der Software einzurichten. Nach der Einrichtung werden über einen Zeitraum von maximal 2 Wochen die Tools betrieben und die jeweiligen Messwerte erfasst. Zwischendurch werden immer wieder Fehler provoziert, um die Alarmierung bzw. die Systemgenauigkeit sowie die Stabilität zu testen. Der gesamte Testbetrieb soll die einzelnen Anforderungsbereiche berücksichtigen und miteinbeziehen. Eventuell auftretende KO-Kriterien, welche in der Erstanalyse nicht erkannt wurden, führen nun nicht mehr zum sofortigen Ausscheidenm sondern fließen in die anschließende Analyse ein und führen zu einer schlechteren Beurteilung in diesem Bereich. Die gesammelten Infos und Erfahrungen aus der Testphase werden anschließend dokumentiert und durch Herstellerinformationen bzw. Daten aus Lieferantengesprächen ergänzt. Alle gesammelten Informationen fließen in die anschließende Entscheidungsfindung einm bzw. bilden die Basis für die Beurteilung mittels Nutzwertanalyse. Für eine übersichtlichere Dokumentation werden die Überschriften der Einzelkriterien herangezogen. Dadurch bekommt man einen guten Überblick über die Software. Abschließend wird ein Fazit gezogen, in welchem nochmals die wichtigsten Eigenschaften oder auch Nicht-Eigenschaften zusammengefasst werden.

GFI Events Manager

Kosten

Die Kosten für GFI Eventsmanager betragen 5500 Euro für 100 Geräte. Die Kosten sind also absolut im Rahmen.

Erstkonfiguration

Das System überwach,t wie der Name schon sagt, hauptsächlich Events und Logfiles der Server und Clients. Das System ist vollständig auf Englisch. Dies macht das Zurechtfinden auf der Oberfläche zunächst etwas schwieriger. Generell ist die Konfiguration sehr umständlich und eine Step-by-Step Anleitung führt ebenfalls nicht sofort zum gewünschten Ziel. Bereits hier zeigt sich, dass die Stärke nicht unbedingt auf dem Überwachen von aktuellen Zuständen liegt, sondern eher auf der Datensammlung und deren periodischer Auswertung. Auch das Alarmierungssystem ist sehr rudimentär vorhanden. Alles in allem ist eine mehrtägige Einarbeitung notwendig und es konnten danach nicht alle gewünschten Messwerte erfasst werden. Ein klarer Pluspunkt ist die Erstellung von diversen Profilen und der dazugehörigen Vererbung. Somit müssen Messpunkte wie die Verfügbarkeit mittels Ping nur einmal definiert werden und können dann an die jeweiligen Geräte vererbt werden.

Systemwartung

Die Systemwartung ist nach erfolgreicher Erstkonfiguration relativ einfach. Geräte können bei vorhandener Lizenz rasch hinzugefügt werden. Durch zuvor erstellte Profile lassen sich anschließend sehr rasch erste Werte erfassen. Updates können sehr einfach durchgeführt werden, hier bietet der Hersteller einen automatischen Dienst an, welcher die Versionen abgleicht und gegebenenfalls die neue installiert. Die Ausfallszeit beträgt nur wenige Minuten

Überwachungsmethoden

Das System bietet klassische Methoden wie WMI oder ICMP, welche auch sehr schnell einzurichten sind. SNMP ist nur sehr oberflächlich implementiert und beschränkt sich auf einen manuellen Messpunkt, welcher generiert werden muss. Eine Integration von MIB-Files ist nicht möglich. Ebenfalls lassen sich Netzwerkbandbreiten nicht zufriedenstellend überwachen, denn Netflow wird nicht unterstützt.

Cloudanbindung

Eine Anbindung an Clouddienste ist nicht möglich.

Mobilität

Mobile Abfragen können nur über Umwege realisiert werden. Eine mobile Anwendung oder Ähnliches existiert nicht.

Alarmierungsvarianten

Die Alarmierung kann mittels Email, SMS oder Push Nachricht auf einzelne Clients passieren. Die Einrichtung dafür ist sehr schnell durchführbar. Eine Ausnahme ist SMS, hier muss über Umwege ein Provider eingerichtet werden, welcher die SMS versenden kann. Die Alarmierung erfolgt dann automatisch, sobald ein Sensor den zuvor definierten Fehlerstatus erreicht.

Automatisierung

Automatismen wie Skriptläufe oder Ähnliches können realisiert werden.

Standortübergreifend

Standortübergreifende Überwachung kann nicht direkt von der Software bewerkstelligt werden, sondern muss über Umwege (VPN) erfolgen.

Bedienbarkeit

Die Oberfläche bietet einige wenige Hauptkategorien und ist nach einer Einarbeitungszeit gut verständlich. Jedoch gibt es bereits sehr viele vorgefertigte Gruppen und Auswertungen, worunter die Übersichtlichkeit leidet. Hier müssen zu Beginn viele Vereinfachungen vorgenommen werden. Danach bietet die Oberfläche einen Statusmonitor und farbliche Unterscheidungen, um den jeweiligen Status der Messwerte betrachten zu können.

Installation

Die Installation der Software ist sehr einfach. Alle benötigten Komponenten wie Datenbankdienste und vorbereitende Installationen werden direkt mitinstalliert. Es sind keine aufwändigen Einstellungen vorzunehmen und die Installation ist sehr rasch abgeschlossen und GFI Eventsmanager ist danach sofort einsatzbereit.

Hardwarekonzept

Das Hardwarekonzept ermöglicht sowohl eine virtuelle als auch eine physikalische Umgebung. Die einzelnen Hardwareanforderungen wie Prozessor oder Arbeitsspeicher liegen im absoluten Branchenstandard.

Redundanz

Ein redundanter Betrieb ist seitens GFI nicht vorgesehen.

Sicherheit

Der Zugriff erfolgt direkt auf dem Server. Ein Client kann mittels Userverwaltung geschützt werden. Berechtigungen können eingerichtet werden, aber nur in einer sehr einfachen Form.

Lizenzmodell

Die Lizenzierung dieses Tools erfolgt nach der Anzahl der Geräte, die in die Überwachung einbezogen werden. Es ist alles sehr transparent und übersichtlich.

Fazit

Der GFI Eventsmanager ist das direkte Nachfolgeprodukt zum derzeit bei MKW eingesetzten Überwachungstool. Leider ist die Einrichtung gegenüber dem Vorgänger deutlich komplexer und umständlicher und die neuen Funktionalitäten wie die Logfileüberwachung oder Reporterstellung bringen nicht den gewünschten Mehrwert. Zudem sind einige gewünschte Features gar nicht oder nur unvollständig umsetzbar.[41]

PRTG Network Monitor

Kosten

Die Kosten für 1000 Messpunkte (Sensoren) belaufen sich auf rund 3500 Euro inkl. 3 Jahre Support. Man geht von einem Sensorbedarf von rund 10 Messpunkten je Gerät aus.

Erstkonfiguration

Für die Erstkonfiguration gibt es mehrere Möglichkeiten. Einerseits bietet das System einen automatischen Netzwerk Scan an und fügt damit alle gefundenen Geräte und deren mögliche Sensoren ein. Die dabei entstehende Flut an Sensoren übersteigt die tatsächliche Notwendigkeit. Eine weitere Methode ist das einmalige Hinzufügen einer Gerätegruppe, um diese anschließend als Vorlage abzulegen und jederzeit darauf zurückzugreifen. Bei Abweichungen der Geräte können jedoch manchmal Sensoren nicht korrekt angelegt werden. Daher wird meist die manuelle Methode gewählt. Hierbei kann der Administrator die Einrichtung am besten steuern. Es werden die Grundparameter bzw. die Zugangsdaten global eingerichtet. Danach wird ein Übersichtsgerüst (Bsp. Gerätegruppen, Standorte o.ä.) eingerichtet und danach die Geräte mit deren Sensoren hinzugefügt und konfiguriert. Für ein Unternehmen mit rund 100 zu überwachenden Geräten geht der Hersteller von maximal 2 Tagen Einrichtungszeit bis zum Echtbetrieb aus.

Systemwartung

Die Wartung und Erweiterung ist sehr einfach und intuitiv und erfordert nur einige wenige Klicks, da die wichtigsten Einstellungen von der globalen Gruppe vererbt werden.

---

[41] Vgl. GFI 2017, Herstellerwebseite

Überwachungsmethoden

PRTG bietet alle erdenklichen Überwachungsmethoden. Ein besonderer Fokus liegt auf SNMP, hier können MIB Files importiert werden und es gibt sehr viele vorgefertigte Sensoren. Ein weiterer Fokus liegt auf der einfachen Anbindung von Netflow, zur Switchüberwachung. Protokolle wie WMI oder ICMP sind ebenfalls im Standardumfang enthalten.

Cloudanbindung

Clouddienste können problemlos angebunden werden (z.B. Amazon Cloud). Weiters werden auch eigene Cloudfunktionalitäten angeboten.

Mobilität

Aufgrund der Möglichkeit, die Bedienung mittels Webzugang zu realisieren, ist auch ein Zugriff von extern mittels Firewall realisierbar. Eine APP für iOS und Android ist ebenfalls im Standardumfang enthalten.

Alarmierungsvarianten

Für die Alarmierung werden neben der klassischen Mailalarmierung auch SNMP, Push, Programmaufruf, Netzwerknachricht usw. angeboten. Mittels diverser Anpassungen und Automatismen können viele der Methoden kombiniert werden.

Automatisierung

Automatismen wie Skriptläufe können realisiert werden. Getestet wurde eine Löschroutine, aber auch der SMS Versand oder die akustische Alarmierung ist mittels Programmaufrufen realisierbar.

Standortübergreifend

Mittels VPN kann jederzeit ein weiterer Standort hinzugefügt werden. Die Besonderheit bei PRTG ist jedoch die Remote Probe. Diese ermöglicht, mittels eines Clients, die Überwachung von externen Geräten über das Internet. Dazu muss nur der notwendige Port für das Internet freigegeben werden und somit der Server über das Internet erreichbar sein. Zusätzlich gibt es noch sogenannte Mobile Probes. Diese laufen auf Androidgeräten und bieten die Möglichkeit, die Umgebung zu überwachen. Somit kann z.B. die WLAN-Stärke erfasst werden.

Bedienbarkeit

Die Bedienbarkeit mittels Windowsclient oder Webanwendung, also auch mit der App am Smartphone, ist sehr einfach und intuitiv. Mittels Gruppierungen und diverser Ansichten können die einzelnen Geräte sehr einfach monitorisiert werden. Die Datenauswertung ist ebenfalls sehr einfach in die Software integriert (Datenexport über Kontextmenü).

Installation

Die Installation ist in wenigen Minuten erledigt. Es sind keine Vorinstallationen wie Datenbanksysteme oder Frameworks notwendig. Innerhalb von rund 10 Minuten ist die Software für die Erstkonfiguration bereit.

Hardwarekonzept

Das Hardwarekonzept ermöglicht sowohl eine virtuelle als auch eine physikalische Umgebung. Für den Betrieb werden keine erhöhten Anforderungen benötigt.

Redundanz

Eine Redundanz ist mittels eines Failoverclusters vom Hersteller berücksichtigt, benötigt aber zusätzliche Hardwarekapazitäten.

Sicherheit

Die Software lässt sich nur mittels berechtigter User bedienen. Ebenfalls notwendig sind Berechtigungsgruppen, um die Administration der Zugangsrechte zu vereinfachen. Dieses Modell zieht sich danach in der gesamten Software durch. So können bestimmte Abteilungen nur ihre Geräte einsehen oder es erfolgt eine Alarmierung nur an bestimmte Personengruppen.

Lizenzmodell

Die Lizenzierung erfolgt mittels Sensoren. Jeder Sensor ist ein Messpunkt und liefert bestimmte Ergebnisse. So kann ein Sensor beispielsweise einen Switchport, die CPU-Auslastung oder den Festplattenstatus überwachen. Diese Methode ermöglicht einen sehr einfachen Überblick über die Auslastung der Lizenz.

Fazit

Wie der Hersteller angibt, handelt es sich bei PRTG um ein Allroundmonitoring für KMUs. Es gibt keine genaue Spezialisierung, aber es können für alle Bereiche erforderliche Daten erfasst werden. Die Einrichtung und Bedienung stellte sich als sehr einfach heraus, die Auswertemöglichkeiten und das Alarmierungskonzept sind sehr ausführlich integriert. Es gibt nur eine Version der Software, diese kann je nach Firmengröße skaliert werden. Der Funktionsumfang ist dabei aber immer gleich. Außerdem gibt es sehr viele Workarounds und HowTo-Anleitungen vom Hersteller und der sehr großen Community. Das ist dem Zustand geschuldet, dass die ersten 100 Sensoren kostenfrei sind.[42]

[42] Vgl. Paessler 2017, Herstellerwebseite

Solar Winds Netzwerküberwachung

Kosten

Die Kosten für Solarwinds belaufen sich auf rund 8000 Euro für die Module Netzwerk, Server sowie Netflow. Dadurch liegt die Software im oberen Preissegment und wurde in der Erstanalyse etwas unterschätzt, aufgrund der im Internet ersichtlichen Mindestpreise.

Erstkonfiguration

Für die Erstkonfiguration sind zuerst die Grundeinstellungen vorzunehmen. Danach gibt es die Möglichkeiten verschiedener Suchfunktionen im Netzwerk, um alle erforderlichen Geräte in die Software zu integrieren (Netzwerkbereich, einzelne Adressen, Active Directory). Anschließend kann eingerichtet werden, über welches Protokoll ein Monitoring durchgeführt werden soll. Alle Grundinformationen werden dann automatisiert angezeigt. Anschließend können noch spezielle Werte wie Interfaces, Prozesse und sowie die Alarmierungen eingerichtet werden. Eine wichtige Funktion sind Templates, welche den Überwachungsumfang einzelner Geräte bzw. Gerätegruppen eingrenzen und wiederverwendbar machen. Man hat hier also relativ schnell erste Ergebnisse. Die Detaileinrichtung nimmt jedoch aufgrund der vielen Informationen und Möglichkeiten mehrere Tage in Anspruch. Man braucht relativ lange, um sich in die mächtigen Funktionalitäten einzuarbeiten.

Systemwartung

Das Thema Systemwartung ist wie bei allen Produkten sehr einfach gehalten. Sobald einmal alles eingerichtet ist, lässt sich die Software sehr einfach erweitern. Updates werden direkt über die Herstellerwebsite geladen und installiert.

Überwachungsmethoden

Es werden alle Überwachungsmethoden in den unterschiedlichen Modulen angeboten. Man muss sich diese beim Kauf zusammensuchen, um danach den vollen Funktionsumfang zu gewährleisten.

Cloudanbindung

Eine Cloudanbindung direkt über die Software ist nicht angedacht. Jedoch können Clouds mittels einem eigenen PRTG-Baustein überwacht werden.

Mobilität

Da die Bedienung der Software über einen webbasierten Client erfolgt, kann dieser nach der Freischaltung über externe Geräte aufgerufen werden. Alternativ kann man den Server mittels VPN Verbindung erreichen.

Alarmierungsvarianten

Die Alarmierung kann je Gerät definiert werden. Alarme werden erstellt und dann dementsprechend zugeordnet. Dazu muss zuerst der Fehlerfall definiert werden, um anschließend eine Aktion auszuführen. Hier kann man Programme ausführen, Geräte automatisch neustarten, vordefinierte Tasks generieren oder klassisch Mails, SMS oder Push-Nachrichten versenden.

Automatisierung

Die Automatisierungsmöglichkeiten bei Solarwinds sind sehr stark integriert. Es werden z.B. einige Tasks für virtuelle Maschinen (Neustart, Programme beenden etc.) automatisch mitgeliefert. Zudem können Skripte und Programme (EXE, Batch, VBS) über einen Trigger gestartet werden oder Befehle mittels eigener Schnittstelle programmiert werden. Dazu ist jedoch einiges an Erfahrung mit der Software notwendig.

Standortübergreifend

Ein standortübergreifender Betrieb ist über gängige Methoden wie VPN möglich. Eine eigene Funktionalität wird nicht angeboten.

Bedienbarkeit

Um die Software zufriedenstellend bedienen zu können, bedarf es einer längeren Einarbeitungszeit. Die grundlegenden Übersichten sind sehr einfach über das Hauptmenü erreichbar, jedoch sind die einzelnen Messpunkte, Überwachungsmethoden und Dashboards sehr verschachtelt. Generell lässt sich sagen, dass Solarwinds extrem viele Funktionen liefert, die zwar praktisch sind, jedoch deshalb eine übersichtliche und vor allem einfache Bedienung nicht möglich ist. Durch Visualisierung und Reporting können zwar sehr einfach Ergebnisse dargestellt werden. Dies erfordert jedoch viel Fingerspitzengefühl, um auch wirklich nur die notwendigen Daten anzuzeigen.

Installation

Die Installation erweist sich also nicht so einfach wie bei anderen Systemen. Es müssen einige Vorbedingungen eingehalten werden und es gibt Einschränkungen beim Betriebssystem. (Nur Windows-Server ist möglich). Nachdem diese Bedingungen erfüllt waren, konnte die Software installiert werden. Dazu muss jeder Baustein/Modul gesondert installiert werden. Der zeitliche Aufwand wird somit stark erhöht. Außerdem ist die Installation auf Windows Server Betriebssysteme eingeschränkt, Testsysteme können also nicht einfach auf dem eigenen PC installiert werden.

Hardwarekonzept

Hier gibt es keinerlei Einschränkungen. Es ist Standardhardware vorgeschrieben und die Installation kann sowohl virtuell aber auch physisch erfolgen.

Redundanz

Eine Redundanz ist vom Hersteller nicht vorgesehen.

Sicherheit

Die sicherheitsrelevanten Themen wie Zugriff oder Anpassungen können über Userberechtigungen gesteuert werden. Um Daten einzusehen, ist ein Login über die Weboberfläche notwendig.

Lizenzmodell

Die Lizenzierung erfolgt nach dem Baukastenprinzip. Je nach Funktionsumfang müssen unterschiedliche Module angeschafft werden. Für MKW sind 3 Module sinnvoll (Netzwerkmonitor, FlowMonitor, Servermonitor). Für jedes Modul gibt es eine eigene Lizenzierung. So wird für das Netzwerk die Anzahl der zu überwachenden Interfaces herangezogen, bei der Serverüberwachung benötigt man sogenannte Komponenten (z.B. Prozess, Dienst) für die Lizenzierung. Dieses System bietet einem zwar eine maßgeschneiderte Lösung, wird aber sehr schnell intransparent und man verliert die Kostenübersicht.

Fazit

Die Monitoringsoftware von Solarwinds bietet eine große Anzahl an Möglichkeiten der Konfiguration und Überwachung. Das Tool ist sehr mächtig und kann unendlich skaliert werden, wodurch sich auch sehr große Netzwerke abbilden lassen. Jedoch entstehen sehr schnell Probleme, aufgrund der Unübersichtlichkeit der vielen verschiedenen Ansichten. Nach einer umfangreichen Systemdemonstration und diversen Gesprächen durch den Lieferanten konnten die offenen Punkte und Fragen geklärt werden. Die Software bietet einen Funktionsumfang, welcher für MKW teilweise irrelevant ist (Bsp.: automatische Konfigurationsänderungen, Programmierschnittstelle).[43]

WhatsUp Gold

Kosten

Die Kosten für 300 Punkte betragen rund 6700 Euro. Darin enthalten sind alle für MKW notwendigen Überwachungsmethoden.

[43] Vgl.Solarwinds 2017, Herstellerwebsite

Erstkonfiguration

Nach erfolgreicher Installation kann man sofort über das Webinterface einsteigen. Danach erfolgt ein Netzwerkscan über einen bestimmten Adressbereich. Anschließend werden die notwendigen Geräte ausgewählt und das Monitoring gestartet. Danach werden die jeweiligen Messpunkte konfiguriert. Ein Layout bzw. eine Karte der überwachten Geräte wird automatisch erstellt. Um jedoch detaillierte Einstellungen wie Alarme oder Ähnliches vornehmen zu können bedarf es einer ziemlich zeitintensiven Einarbeitung, da das Tool sehr umfangreich und mächtig ist und auch viele Features liefert, die nicht zwingend notwendig sind. Eine intuitive Konfiguration ist hier nicht möglich. Es müssen diverse Medien wie Bedienungsanleitungen oder Konfigurationsvideos zu Rate gezogen werden, um eine einigermaßen sinnvolle Einrichtung zu gewährleisten.

Systemwartung

Die Systemwartung ist, nachdem man das Konzept verstanden hat, sehr einfach. Geräte können durch einen Netzwerkscan sehr einfach zum Server hinzugefügt werden. Updates lassen sich direkt über das Programm steuern.

Überwachungsmethoden

WhatsUp Gold bietet alle notwendigen Überwachungsmethoden. Die Anpassbarkeit und Skalierung ist jedoch eingeschränkt. MIB-Files können für die SNMP-Überwachung integriert werden. Netflow und WMI wird durch einen Userzugang ermöglicht.

Cloudanbindung

Clouddienste können problemlos angebunden werden (z.B. Amazon Cloud). Weiters werden auch eigene Cloudfunktionalitäten angeboten.

Mobilität

Eine App wird aktuell noch nicht angeboten, ist laut Lieferanten jedoch in einem der nächsten Updates im Jahr 2017 enthalten. Derzeit gibt es nur die Möglichkeit, mittels VPN auf den Server zu gelangen, bzw. den Server mittels Portweiterleitung im Internet zur Verfügung zu stellen.

Alarmierungsvarianten

WhatsUp bietet eine lange Liste an Alarmierungsmöglichkeiten. Neben Mail und SMS gibt es auch die akustische Alarmierung oder die Benachrichtigung über Skripte. Die Einrichtung erfolgt zentral und wird danach dementsprechend auf die jeweiligen Geräte verteilt oder vererbt.

Automatisierung

Automatismen können durch Skriptsprachen und die Ausführung externer Programme (EXE-Ausführung) realisiert werden.

Standortübergreifend

Die Software liefert keine direkte Möglichkeit, standortübergreifend zu agieren. Die Möglichkeit muss mittels VPN-Tunnel oder einer ähnlichen Technik umgesetzt werden.

Bedienbarkeit

Eine Bedienung der Software erfolgt über den sehr ansprechenden Webclient. Leider ist die Reaktion hier etwas träge. Durch eine Vielzahl an Features, welche WhatsUp liefert, wird die Bedienoberfläche sehr schnell unübersichtlich. Zur Administration gibt es zusätzlich einen Administratorclient auf dem Server. Die einzelnen Schaltflächen werden in 4 Hauptkategorien (z.B. Erkennen, Überwachen usw.) unterteilt.

Installation

Die Installation erfolgt mittels Assistenten. Alle notwendigen Vorbedingungen werden mitgeliefert und in einem ersten Schritt installiert (SQL Express Datenbank). Der weitere Ablauf erfolgt sehr einfach und unspektakulär. Nach 10 Minuten kann WhatsUp Gold ausgeführt werden.

Hardwarekonzept

Hier gibt es keinerlei Einschränkungen. Die Hardware wird nicht sonderlich beansprucht und eine Installation ist auf physischen als auch virtuellen Geräten möglich.

Redundanz

Eine redundante Ausführung ist in den Herstellerangaben nicht vorgesehen.

Sicherheit

Für den sicheren Einstieg gibt es eine Userverwaltung mit Beschränkungen. Dadurch können die Zugriffe und die Dateneinsicht genau geregelt werden.

Lizenzmodell

Das Lizenzmodell basiert auf einem Punktesystem. Hierbei wird für jedes Gerät 1 Punkt verbraucht. Für spezielle Anforderungen, wie den Netzwerkdurchfluss werden z.B. 10 Punkte benötigt. Zudem gibt es insgesamt 4 Grundpakete der Software, welche sich durch den Funktionsumfang unterscheiden. Für den Anforderungsfall der Firma MKW würde eine WhatsUp Gold Totalview Lizenz benötigt werden.

Fazit

Laut Hersteller eignet sich WhatsUp als Allroundtool für die Überwachung einer gesamten IT-Infrastruktur. Neben der sehr intelligent gelösten Visualisierung mittels Netzwerkplan, hat die Software ihre Stärke im Funktionsumfang und dem einfachen Lizenzmodell. Die Community ist jedoch eher klein und Abweichungen von der Norm (Schnittstellen, Anpassbarkeit) sind vom Hersteller eingeschränkt. Weiters wurde zu wenig auf den Trend der Mobilität geachtet. Der Einsatz eignet sich nach den Erkenntnissen aus dem Testlauf für alle Größen von Firmen, da eine gute Skalierbarkeit und eine einfache Lizenzierung gegeben ist.[44]

4.5 Nutzwertanalyse

Die durch Recherchearbeit und Testsystem erhobenen Daten fließen nun in die nächste Bewertungsrunde ein. Diese wird in Form einer Nutzwertanalyse durchgeführt und soll am Ende einen Sieger hervorbringen.

Um die Nutzwertanalyse zufriedenstellend zu generieren, wurden im Laufe der Diplomarbeit bereits einige Vorbereitungen erledigt. So gibt es bereits die Problemdefinition bzw. Zielstellung und die zu bewertenden Alternativen bzw. Varianten. Ebenfalls wurden schon Bewertungskriterien festgelegt, welche gegebenenfalls noch genauer unterteilt werden müssen. Ausständig sind noch die Erstellung einer geeigneten Bewertungsskala sowie die Gewichtung der einzelnen Kriterien und die abschließende Ermittlung des Nutzwertes, also der Durchführung der Analyse.

Zum Abschluss folgt anhand der errechneten Nutzwerte die Entscheidungsfindung aus dem Portfolio der 4 Softwarefavoriten.

4.5.1 Erstellung der Bewertungsskala

Für die Bewertung der einzelnen Kriterien dient eine Skala mit Zahlenwerten. Um eine zu hohe Komplexität zu vermeiden, werden 3 Punktwerte definiert (0, 5 und 10 Punkte). Ist das Kriterium eine ja/nein Entscheidung, so können auch nur die Punktwerte 0 und 10 zur Auswahl stehen. Für die Punktevergabe wird eine Kernfrage gestellt. Mittels dieser Frage wird der Punktewert ermittelt. Wann welche Bewertung zum Tragen kommt, wird in der folgenden Tabelle für jedes Kriterium definiert.

[44] Vgl. Ipswitch 2017, Herstellerwebsite

Kriterium	Kernfrage	Punktwert		
		0	**5**	**10**
Kosten	Anschaffungskosten + Wartung für 1 Jahr?	>6000€	1000€-6000€	<1000€
Erstkonfiguration	Dauer der Erstkonfiguration?	>10 Tage	5-10 Tage	<5 Tage
Systemwartung	Wie ist die Aufwand für Wartung, für Anpassungen?	hoch	mittel	gering
Überwachungsmethoden	Alle Protokolle im System implementiert?	nein	1-2 fehlen	ja
Cloudanbindung	Clouddienste im System integriert?	nein	teilweise	ja
Mobilität	Mobile Erreichbarkeit möglich (App, Webzugang,…)?	nein	über Umwege (z.B. VPN)	ja
Alarmierungsvarianten	Alarmierung möglich mittels Mail, SMS, Skripting?	nein	ja, aber umständlich	ja
Automatisierung	Können automatisierte Vorgänge implementiert werden?	nein	über API	ja
Standortübergreifend	Standortübergreifender Betrieb direkt möglich?	nein	über Umwege (z.B. VPN)	ja
Bedienbarkeit	Komplexität der Oberfläche?	kompliziert	machbar	einfach

Installation	Wie verläuft der Installationsaufwand?	umständlich	annehmbar	einfach
Hardwarekonzept	Wie hardwareintensiv ist die Software?	intensiv	akzeptabel	gering
Redundanz	Redundanzkonzepte möglich?	nein	teilweise	ja
Sicherheit	Benutzer und Rechteverwaltung für den Zugang?	nein	teilweise	ja
Lizenzmodell	Transparenz des Lizenzmodells?	kompliziert	Erklärung notwendig	einfach

Tabelle 4-18 Bewertungsskala für Nutzwertanalyse

4.5.2 Gewichtung der Kriterien

Da es Kriterien gibt, welche für die Entscheidung eine höhere Bedeutung haben als andere, muss eine Gewichtung der Einzelkriterien stattfinden. Für die 15 Einzelkriterien müssen Prozentsätze definiert werden. Mittels dieser kann anschließend der Punktewert umgerechnet werden. Die Summe der 15 Gewichtungen muss am Ende 100% betragen. Die Festlegung erfolgt durch Eigeneinschätzung bzw. Abklärung mit den beteiligten Personen.

Die Einteilung der genauen Gewichtungswerte wird in der folgenden Tabelle dargestellt.

Kriterium	Gewichtungswert
Kosten	15%
Erstkonfiguration	10%
Systemwartung	5%
Überwachungsmethoden	15%

Cloudanbindung	2%
Mobilität	4%
Alarmierungsvarianten	10%
Automatisierung	5%
Standortübergreifend	2%
Bedienbarkeit	10%
Installation	5%
Hardwarekonzept	5%
Redundanz	2%
Sicherheit	5%
Lizenzmodell	5%

Tabelle 4-19 Gewichtungswerte für Nutzwertanalyse

4.5.3 Durchführung der Analyse

Zur Durchführung der Nutzwertanalyse werden die bisherigen Vorarbeiten zusammengefügt. In den Spalten stehen die Alternativen und in den Zeilen die Bewertungskriterien. Anhand der Testergebnisse, sowie Eigeneinschätzung und Herstellerangaben werden nun die Punktewerte laut Bewertungsskala vergeben. Durch Multiplikation des erhobenen Punktewerts mit der jeweiligen Gewichtung des Einzelkriteriums, ergibt sich die verrechenbare Bewertung. Die Summe aller Beurteilungspunkte ergibt abschließend den Nutzwert der einzelnen Alternativen. Der maximale Nutzwert wäre theoretisch 10 Punkte.

Die genaue Durchführung der Nutzwertanalyse findet sich im Anhang, Teil 1. Nachfolgend nur die verkleinerte Darstellung sowie die Dokumentation des Endergebnisses.

		GFI		PRTG		SolarWinds		WhatsUP		Maximum	
Kriterium	Gewichtung	Wert	verrechnet	Wert	verrechnet	Wert	verrechnet	Wert	verrechnet	Wert	verrechnet
Kosten	15%	5	0,75	10	1,5	5	0,75	5	0,75	10	1,5
Erstkonfiguration	10%	10	1	5	0,5	10	1	10	1	10	1
Systemwartung	5%	5	0,25	5	0,25	5	0,25	5	0,25	10	0,5
Überwachungsmethoden	15%	5	0,75	10	1,5	5	0,75	10	1,5	10	1,5
Cloudanbindung	2%	0	0	5	0,1	0	0	0	0	10	0,2
Mobilität	4%	0	0	10	0,4	0	0	5	0,2	10	0,4
Alarmierungsvarianten	10%	10	1	10	1	10	1	10	1	10	1
Automatisierung	5%	5	0,25	10	0,5	5	0,25	5	0,25	10	0,5
Standortübergreifend	2%	5	0,1	10	0,2	5	0,1	5	0,1	10	0,2
Bedienbarkeit	10%	10	1	5	0,5	10	1	10	1	10	1
Installation	5%	5	0,25	10	0,5	5	0,25	5	0,25	10	0,5
Hardwarekonzept	5%	10	0,5	10	0,5	10	0,5	10	0,5	10	0,5
Redundanz	2%	5	0,1	5	0,1	5	0,1	5	0,1	10	0,2
Sicherheit	5%	0	0	10	0,5	5	0,25	10	0,5	10	0,5
Lizenzmodell	5%	10	0,5	5	0,25	0	0	5	0,25	10	0,5
	100%		6,45		8,3		6,2		7,65		10

Abbildung 4-35 Verkleinerte Darstellung Nutzwertanalyse

Die Nutzwerte der 4 Varianten ergeben nach der Berechnung folgende Werte:

Produkt	Nutzwert	Platzierung
GFI EventsManager	6,45 Punkte	Platz 3
PRTG Network Monitor	8,3 Punkte	**Platz 1**
SolarWinds Netzwerküberwachung	6,2 Punkte	Platz 4
WhatsUP Gold	7,65 Punkte	Platz 2

Tabelle 4-20 Ergebnis Nutzwertanalyse

4.5.4 Bewertung der Analyse

Die Nutzwertanalyse zeigt, dass alle Produkte klar ihre Stärken und Schwächen aufweisen. Da hier ein Monitoringtool für ein sehr breites Einsatzgebiet gesucht wurde und durch die Vorauswahl nur mehr solche in die Entscheidungsfindung einflossen, sind die Nutzwerte alle sehr hoch angesiedelt. Die Funktionalitäten wurden beinahe alle erfüllt, den Unterschied machten hauptsächlich Bereiche wie Usability oder Konfigurationsverhalten. Am Ende gibt es jedoch eine klare Reihenfolge. Auf dieser Basis kann nun eine klare Entscheidung getroffen werden.

4.6 Toolauswahl

Die Auswahl fällt aufgrund der Nutzwertanalyse auf den „PRTG Network Monitor“ von „Paessler“. Aufgrund vieler Argumente wie der einfachen Konfiguration, der Anpassbarkeit oder dem großen Funktionsumfang, konnte hier der höchste Nutzwert erzielt werden. Bereits in der Testphase zeigte sich, wie schnell sich hier sichtbare Ergebnisse realisieren lassen.

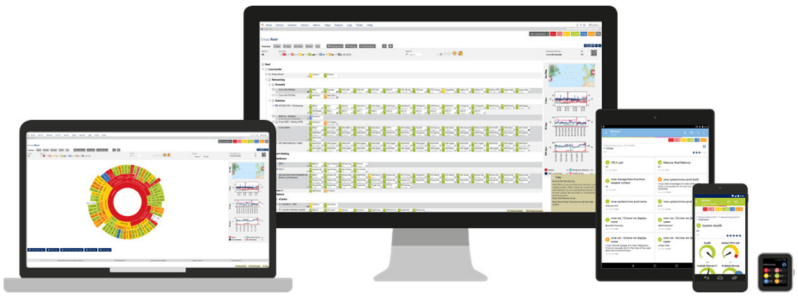


Abbildung 4-36 Produktbild PRTG Network Monitor (Paessler 2017)

5 Erarbeitung eines Implementierungskonzepts

Im Kapitel 5 geht es um die konkrete Realisierung und Implementierung der Gewinnersoftware. Dazu gehört einerseits ein passendes Hardwarekonzept, um einen erfolgreichen Betrieb sicherzustellen. Außerdem muss eine Konzeption zur Softwarekonfiguration stattfinden, um die Anforderungen wie Übersichtlichkeit oder Bedienbarkeit perfekt realisieren zu können.

5.1 Hardwarekonzeption

Um eine Software bestmöglich zu betreiben, bedarf es eines geeigneten Hardwarekonzepts. Um die passende Hardware zu finden, müssen die Herstellervorgaben erfüllt werden. Zudem ist es notwendig, Firmeneigene Regeln und Anforderungen in die Konzeptionierung mit einfließen zu lassen. Abschließend muss noch an die Skalierbarkeit gedacht werden, um wachsende Strukturen abbilden zu können.

5.1.1 Systemvoraussetzungen

Ausgehend von rund 100 zu überwachenden Geräten, geht der Hersteller von PRTG Network Monitor von einer Lizenz mit 1000 Sensoren aus. Die dafür empfohlene Hardware ist ein Prozessor mit 2 Cores und 3 GB RAM sowie ein Festplattenspeicher mit mindestens 250 GB. Virtualisierung in dieser Größenordnung ist möglich, ebenfalls die Realisierung eines PRTG-Clusters, also der redundanten Ausführung der PRTG-Installation. Für alle weiteren Skalierungsstufen sind dementsprechend mehr Ressourcen notwendig. Empfohlen wird die Installation ganz klar auf einem physikalischen Server, da Performance und Ausfallssicherheit deutlich besser sind.

5.1.2 Anforderungen MKW

Seitens Auftraggeber gibt es auch klare Anforderungen an die Hardware, die weniger mit den Leistungsmerkmalen, als vielmehr mit Sicherheitsmerkmalen und Standardisierung zu tun haben. Auch zukunftsrelevante Themen fließen hier mit ein.

Redundante Stromversorgung

Die Stromversorgung eines Servers erfolgt prinzipiell mit der Absicherung durch eine USV-Anlage, um bei Stromausfällen weiterhin den Betrieb für gewisse Zeit zu gewährleisten. Da auch diese Notstromversorgungen versagen können, ist es notwendig, den Server 2x an das Stromnetz anzubinden. Ein Anschluss erfolgt an das normale Stromnetz ohne USV-Absicherung, ein weiterer Anschluss erfolgt direkt an die Notstromversorgung. Somit läuft

bei einem Stromausfall der Server über die USV, sollte diese versagen, bleibt noch der Anschluss am normalen Stromnetz, um den Server zu betreiben. Ein Restrisiko bleibt natürlich, wenn sowohl USV und Stromnetz versagen. In diesem Fall ist aber ein genereller Betrieb der IT-Anlagen nicht mehr möglich und das Monitoring ist sinnlos.

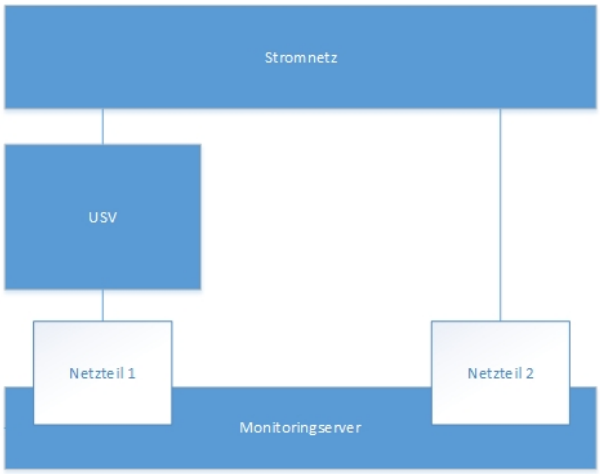


Abbildung 5-37 Konzept redundante Stromversorgung

Redundante Alarmierungsmöglichkeit

Für die Alarmierung per Mail ist eine Internetverbindung notwendig. Falls diese eine Störung hat, können keine Mails versendet werden. Daher ist es notwendig, eine unabhängige Internetleitung (z.B. mittels GSM) einzusetzen. Mit dieser können beispielsweise SMS versendet werden. Auch hier gilt wie bei der Stromversorgung: Ein Restrisiko für den Fall, dass beide Leitungen ausfallen bleibt bestehen.

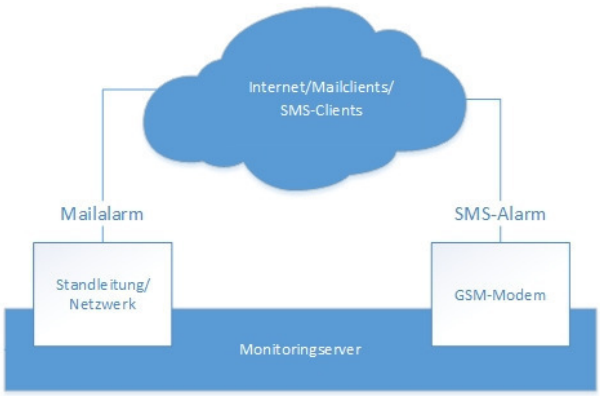


Abbildung 5-38 Konzept redundante Alarmierungsmöglichkeit

Redundante Netzwerkanschlüsse

Für die Anbindung an die Netzwerkinfrastruktur bei MKW ist ein RJ45 Anschluss notwendig. Dieser ermöglicht den Zugang zu allen relevanten Netzwerkdiensten und verbindet den Server mit den Geräten, welche von PRTG überwacht werden sollen. Auch hier muss eine

Ausfallssicherheit gewährleistet werden. Realisiert wird dies mittels eines zweiten Netzwerkanschlusses. Die beiden physischen Anschlüsse können mittels eines speziellen Herstellertreibers zu einem virtuellen Anschluss, einem sogenannten Team, zusammengefasst werden. Jeder Anschluss wird an einem anderen Switch angeschlossen. Dadurch können zum einen höhere Bandbreiten übertragen werden. Zudem kann beim Ausfall einer Schnittstelle oder beim Ausfall eines Switches auf den zweiten Anschluss zurückgegriffen werden.

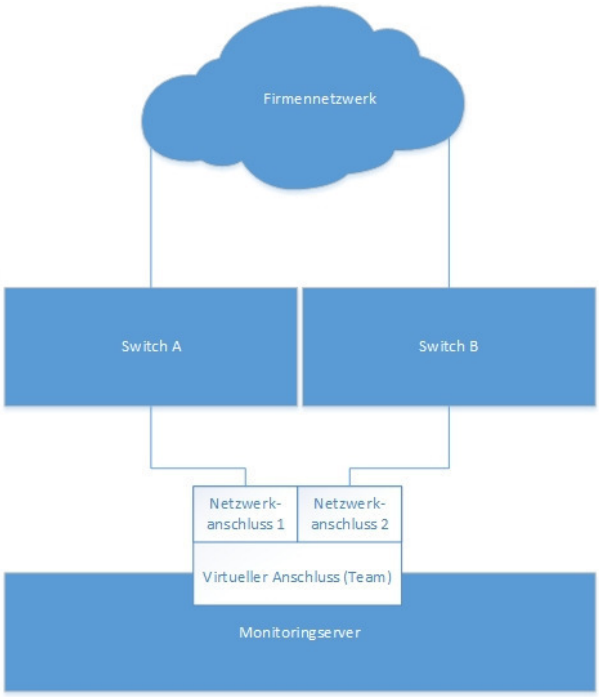


Abbildung 5-39 Konzept redundante Netzwerkanschlüsse

RAID Verbund

Für die Datensicherheit am Server ist ein geeignetes Datenhaltungskonzept erforderlich. Dazu eignet sich ein Festplattenverbund mit einer Ausfallssicherheit für eine oder mehrere Festplatten besonders gut. Hier gibt es verschiedenste Varianten der Realisierung. So gibt es zum einen die Variante RAID 1 (Mirroring), wobei hier auf 2 Platten immer alle Daten parallel auf jeder Festplatte gehalten werden. Diese Variante ist mit hohen Kosten verbunden und nicht unbedingt die sicherste Variante. Die zweite Variante ist ein RAID 5 Verbund (Block Striping mit verteilter Parität), hierbei werden die Daten nicht gespiegelt, sondern eine Kontrollsumme berechnet, die auf eine der vorhandenen Festplatten geschrieben wird. Beim Ausfall einer Festplatte werden die fehlenden Informationen aus der Kontrollsumme berechnet. Der Vorteil ist eine größere nutzbare Festplattenkapazität sowie geringe Kosten. Eine Weiterentwicklung von RAID 5 ist RAID 6 (Block Striping mit verteilter Parität auf 2

Platten), hierbei können nicht nur 1 sondern 2 Festplatten ausfallen und der Betrieb ist weiterhin gewährleistet. Hier wird die Prüfsumme wie bei RAID 5 berechnet und dann auf 2 Platten geschrieben.[45]

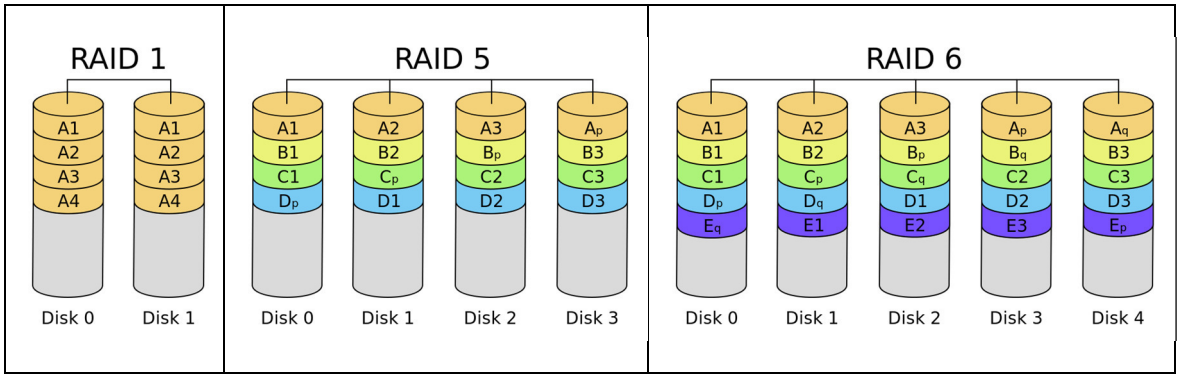


Abbildung 5-40 Vergleich RAID Systeme (Wiki-Raid 2017)

Für den PRTG Server bietet sich die Variante RAID 6 an. Dadurch können die Monitoringdaten über einen langen Zeitraum protokolliert werden, ohne an die Kapazitätsgrenzen zu stoßen.

Lieferant

Die Firma MKW arbeitet seit Jahren mit der Firma Dell als Komplettausstatter im Server/Client Bereich zusammen. Daher muss auch dieser Server von Dell geliefert werden. Hier bietet sich ein Server der PowerEdge-Serie an.

Rackeinbau

Der vorhandene Serverraum besteht derzeit aus 5 Racks für den Einbau von 19 Zoll Geräten. Die Hardware muss ebenfalls diese Eigenschaften aufweisen, um einen Einbau mit möglichst kleinem Platzbedarf zu ermöglichen. Der Höhenbedarf soll 1 HE nicht überschreiten.

Kabelmanagement

Um am Server Wartungsarbeiten vornehmen zu können und ein Kabelgewirr zu vermeiden, ist der Einsatz eines Kabelmanagements, welches für Dellserver passend ist, erforderlich. Die Umsetzung erfolgt mittels ausziehbarer Serverschienen in Verbindung mit einem Kabel Arm zur Kabelführung.

[45] Vgl. Stor IT Back 2010, Gesamtartikel

Abbildung 5-41 Dell Kabelarm (Dell 2017)

5.1.3 Hardwareauswahl

Aufgrund der zuvor genannten Anforderungen wurde mit der Firma Dell folgender Server ausgewählt:

Dell Rackserver Poweredge 330 1HE mit

- 4 Stück SATA Festplatten mit 1 TB in einem RAID 6 Verbund
- Intel Xeon E3-1220 v5 Prozessor mit 4 Cores zu je 3 GHz und 8 MB Cache
- 16GB Arbeitsspeicher
- 2 Netzwerkanschlüsse mit einer Geschwindigkeit von je 1 Gbit
- 2 Netzteile zu je 350 Watt
- Betriebssystem Windows Server 2012 R2 Standard Edition

Abbildung 5-42 Beispiel Vorderansicht/Rückansicht Poweredge 330 (Dell 2017)

Zusätzlich kommt ein USB-Datenmodem für den SMS-Versand zum Einsatz. Hier wird auf ein vorhandenes USB-GSM-Modul der Type Huawei E272 zurückgegriffen.

5.2 Softwarekonzeption

Um die Software strukturiert zu konfigurieren, muss ein passendes Konzept erstellt werden. Dies dient als Basis, um die Software möglichst effizient in den Echtbetrieb übernehmen zu können.

5.2.1 Grundeinstellungen

Nach der Installation auf der entsprechenden Hardware müssen zuerst die wichtigsten Einstellungen vorgenommen werden. Dazu gehören die Zugänge zu den Geräten (Windowsanmeldung, SNMP Communitystring, SOAP Zugang, usw.), die User und Personengruppen bzw. Abteilungen welche Zugriff benötigen, die Benachrichtigungsvarianten, die Versandrichtlinien und der dazugehörige technische Hintergrund (Mailserver, SMS Gateway, Batchskripte usw.), Portfreigaben für Webinterface und externe Erreichbarkeit (Firewallkonfiguration), Abfrageintervalle sowie Lizenzeinstellungen.

Diese Einstellungen werden für die oberste Ebene eingerichtet (PRTG-Serverebene bzw. Mainprobe) und auf die gesamte Gerätestruktur nach unten vererbt. Sollten einzelne Geräte oder Gerätegruppen andere Einstellungen benötigen, so können die Vererbungsrichtlinien unterbrochen werden.

5.2.2 Strukturierung

Anschließend muss eine geeignete Strukturierung gefunden werden, um die entsprechenden Geräte rasch zu finden und aussagekräftige Ergebnisse zu bekommen. Die dabei entstehende Baumstruktur umfasst folgende Ebenen:

- Standorte (Weibern, Haag am Hausruck, Presov)
    - Gerätegruppen (Server, Netzwerk, Drucker, Firewall, USV, Sensoren, Virtualisierung, Sonstige)
        - Gerät (Geräte je Gruppe)
            - Sensor (Messwerte je Gerät)

Die detaillierte Auflistung der einzelnen Geräte bzw. die geplante Struktur wird unter Anlage, Teil 3 behandelt.

5.2.3 Sensoren

Nach der Generierung der Gerätestruktur müssen die jeweiligen Sensoren je Gerät spezifiziert werden. Dazu muss jedes Gerät gesondert betrachtet werden, um ein geeignetes Überwachungskonzept zu erhalten. Die genaue Auflistung, welche Messwerte auf den verschiedenen Geräten erfasst werden, wird in Anlage Teil 3 in der Strukturplanung angeführt.

Nachfolgend werden die wichtigsten Sensoren dargestellt, welche für den Betrieb benötigt werden.

ICMP Ping

Mittels Ping wird laut definiertem Zeitintervall periodisch die Erreichbarkeit des Gerätes überwacht.

SNMP Cisco Systemzustand

Mittels SNMP werden Zustände auf Ciscogeräten erfasst wie z.B. Temperatur, Prozessorlast oder RAM-Auslastung.

SNMP Bibliothek

Über diesen Sensor können herstellerspezifische Bibliotheken aus MIB-Files eingelesen werden. Benötigt wird dies beispielsweise für USV-Geräte, um die Batteriekapazität oder die Eingangsspannung zu erfassen.

SNMP benutzerdefiniert

Über benutzerdefinierte Sensoren können, sofern bekannt, die OID Codes einzelner Hersteller abgefragt werden. MKW verwendet dies für die Abfrage von Temperatursensoren, Feuchtigkeitssensoren oder diverse Statusabfragen bei Firewalls.

SNMP Dell PowerEdge Systemzustand

Dieser Sensor ermöglicht das Erfassen von Werten eines Dell PowerEdge Servers. Beispiele sind die Festplattengesundheit, Temperaturstatus usw.

SNMP NetAPP Sensoren

Mittels vorgefertigten Sensoren lassen sich diverse Gesundheitswerte einer Netapp-Storage erfassen (z.B. Auslastung der Platten).

SNMP Drucker

Der allgemeine Druckersensor erfasst Werte wie Tonerstände, Zählerstände oder geöffnete Klappen am Gerät.

SNMP QNAP Sensoren

Diese Sensorvariante ermöglicht die Überwachung von QNAP-Geräten (=Netzwerkspeicher/NAS). Hierbei ist besonders der Festplattenstatus interessant.

WMI Datenträger

Einer der Hauptsensoren im Serverbereich erfasst die Auslastung auf den einzelnen Festplattenpartitionen.

WMI Dienst/Prozess

Hierbei wird periodisch geprüft, ob ein Windows Dienst/Prozess läuft oder nicht.

WMI Datei/Ordner

Der Sensor überprüft, ob Dateien vorhanden sind oder nicht (je nach Anforderung), zählt beispielsweise Dateien in Ordnern oder gibt das Alter der jüngsten/ältesten Datei aus.

WMI SQL-/Exchange-Server

Er überwacht den Status eines SQL- oder Exchange-Servers. (Dienste, Systemgesundheit, usw.)

WMI SMTP

Hier wird geprüft ob SMTP auf einem Mailserver zufriedenstellend funktioniert.

NetFlow v9

Der Netflowsensor erfasst alle Datenflüsse eines definierten Netzwerkgeräts mittels UDP. Dabei dient der Server als Netflow Empfänger für alle Geräte und kann gegebenenfalls mittels Parameter separiert werden. Der Sensor bietet die Möglichkeit, die Top-Verbindungen oder Top-Verbindungsprotokolle darzustellen und Überlastungen zu erkennen.

PowerShell Exchange Sensoren

Mittels Powershell Abfragen können einzelne Postfächer, die Maildatenbank oder der Sicherungslauf überprüft werden.

SOAP VMWare Sensoren

Mittels SOAP Zugang kann die Gesundheit oder der Status der ESX-Hosts und die darauf laufenden VM’s monitorisiert werden.

Zusätzlich zur Einrichtung müssen Grenzwerte definiert werden, ab wann ein Sensor eine Warnung bzw. einen Fehler ausgibt. Auf Basis dessen können dann Alarmierungen hinterlegt werden. Diese Grenzwerte müssen sehr individuell für jedes Gerät betrachtet werden. So gibt es beispielsweise Server, wo 1 GB Festplattenspeicher ausreichend ist, bei anderen wird es bereits bei einem Unterschreiten von 10 GB kritisch. Bei anderen Sensoren, welche z.B. die Verfügbarkeit mittels Ping überwachen, reichen auch binäre Werte, sprich erreichbar oder nicht erreichbar.

5.2.4 Alarmierungskonzept

Um im Fehlerfall auch eine zeitgerechte Information zu erhalten, bedarf es eines durchdachten Alarmierungskonzepts. Der Schwerpunkt liegt im Bereich des Mailings. Im Fehlerfall müssen bei allen Messwerten E-Mails versendet werden. Dies soll über den firmeneigenen Mailserver mittels SNMP geschehen. Die Empfängerlisten müssen den jeweiligen Sensoren angepasst werden. Es gibt Sensoren, wo die gesamte IT-Mannschaft benachrichtigt werden muss, andere Fehlerinformationen benötigen nur einzelne Personen oder andere Abteilungen.

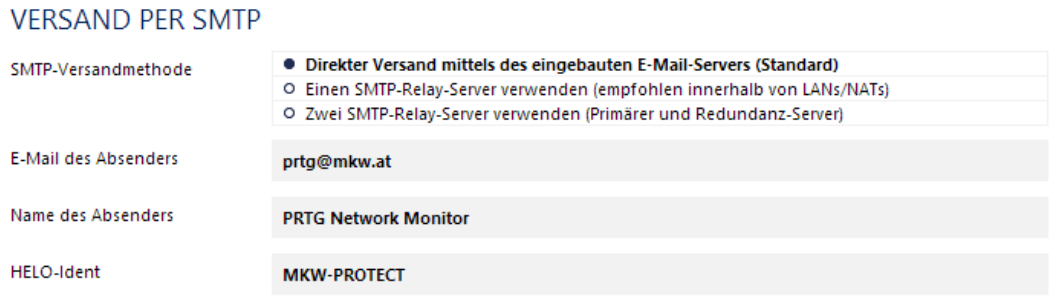


Abbildung 5-43 Einrichtung Mailversand in PRTG (Paessler 2017)

Die Alarmierung per SMS soll für alle Ping-Sensoren zur Verfügbarkeitsüberprüfung erfolgen. Alarmiert werden hier immer dieselben Personen. SMS-Benachrichtigungen dienen als Sicherheitsstufe, sollte die Mail-Alarmierung nicht wie gewünscht funktionieren.

Als Gateway für den SMS-Versand dient, das in der Hardwarekonzeptionierung erwähnte GSM-Modem. Dieses wird mittels USB-Anschluss mit dem Monitoringserver verbunden. Für die Verbindung wird das gratis Dienstprogramm „MWConn“ verwendet. Hier gibt es von PRTG einen Workaround, um dieses einzurichten. Im Fehlerfall wird ein Textfile über ein aufzurufendes Batchskript generiert, welches dann mittels „MWConn“ an die definierten Empfänger versendet wird. Diese Methode bietet einen autonomen Versand, welcher nicht von der Standardinternetleitung des Unternehmens abhängig ist. Somit ist die geforderte Redundanz ausreichend erfüllt.

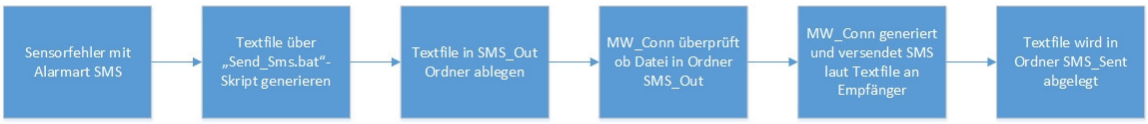


Abbildung 5-44 Ablauf SMS-Versand mit PRTG und MWConn (PRTG-SMS 2017)

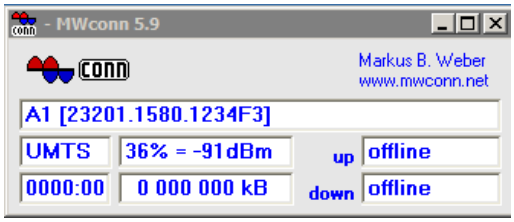


Abbildung 5-45 Ansicht MWConn (Weber 2016)

Weitere Alarmierungsvarianten machen nach Erkenntnissen, welche in der Testphase festgestellt wurden, wenig Sinn.

Die genaue Zuordnung, welcher Sensor wann und wie einen Alarm sendet, wird in Anlage Teil 3 im Detail dargestellt.

5.2.5 Externe Verfügbarkeit

Um PRTG auch außerhalb des Unternehmens zu nutzen, muss der Server über das Internet verfügbar sein. Dazu muss dieser über die Firmenfirewall freigeschaltet werden. Die dabei gängige Methode ist eine Portweiterleitung Zudem ist nur der entsprechende Port, welcher in PRTG definiert wird, freizugeben

Die dafür notwendigen Regeln werden auf der Firmenfirewall eingerichtet. Danach ist der Server über das Internet erreichbar, aber weiterhin ausreichend vor Fremdzugriffen geschützt.

5.2.6 Reporting und Visualisierung

PRTG liefert bereits sehr viele Standardfunktionen zur Visualisierung und Auswertung. Jeder Sensor bietet Statusdiagramme der letzten Stunde/Tage/Wochen/Jahr oder „Tachoansichten“ über den derzeit aktuellen Messwert.

Weiters gibt es historische Daten, welche im 15 Minuten Takt gespeichert werden. Diese können ins Excel Format oder andere gängige Textformate exportiert und ausgewertet werden. Auch direkt in PRTG können HTML-Reports betrachtet werden.

In der Weboberfläche und im Windowsclient können verschiedene Übersichten/Dashboards eingerichtet werden, um eine Gesamtansicht aller Sensoren zu erhalten. Diese können als einfache Liste oder Blockdiagramm, aber auch als Tortengrafik oder Landkarte dargestellt werden.

Zusätzlich lassen sich alle Sensoren als individuelle Karten, sogenannte Maps darstellen. Diese können vom Administrator per „Drag-and-Drop“ erstellt werden. Damit sind Userspezifische Dashboards möglich.

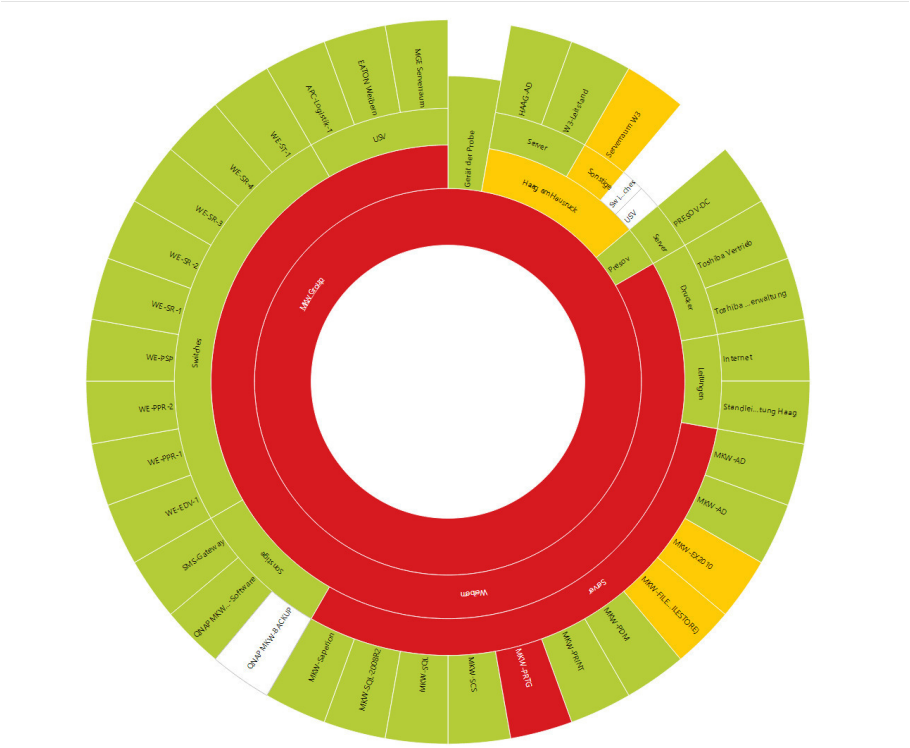


Abbildung 5-46 Dashboard Variante PRTG (Paessler 2017)

Weiters ist in jeder Ansicht von PRTG, immer eine kleine Summenübersicht alle Sensoren mit deren Satus ersichtlich. Somit sieht man, wie viele Sensoren im Status Fehler (rot) sind, welche Warnwerte aufweisen (gelb) oder welche OK sind (grün). Zusätzliche Statusmöglichkeiten sind ungewöhnliche Sensoren (orange), welche plötzlich zwar korrekte Werte aufweisen, diese aber von der sonstigen Norm abweichen. Außerdem können Sensoren pausiert (blau) werden, dies kommt oft bei Wartungsarbeiten einzelner Geräte zur Anwendung.

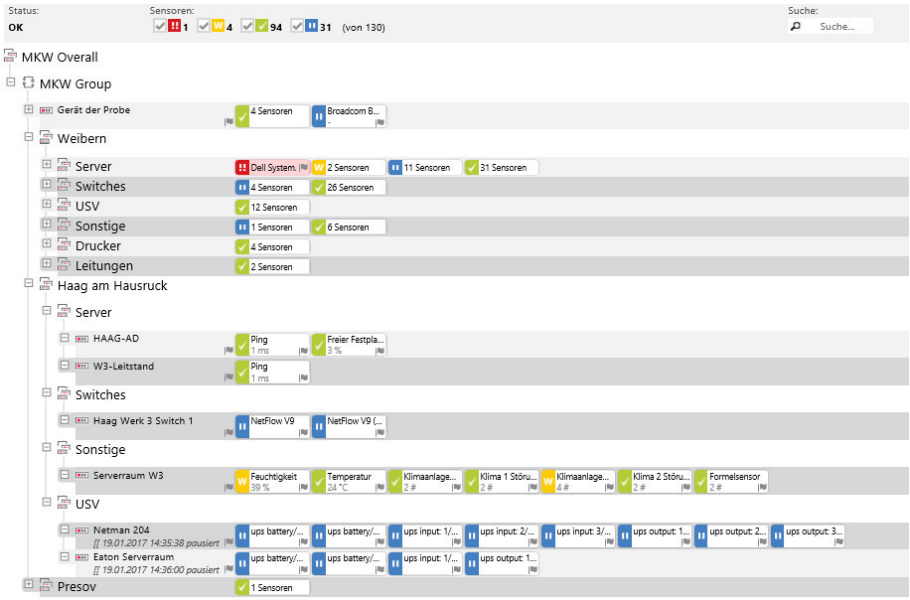


Abbildung 5-47 Übersicht Sensorstatus gesamt (Paessler 2017)

5.2.7 Automatisierung

Richtig mächtig ist die Möglichkeit der Automatisierung. Hier gibt es fast keine Grenzen, da von PRTG Skripte automatisiert ausgeführt werden können.

Läuft beispielsweise ein Ordner voll, da eine bestimmte Dateianzahl erreicht wurde, so läuft PRTG in einen Fehler und führt dadurch eine Batchdatei aus, welche den Ordner leert. Danach ist der Sensor wieder im Status OK. Realisiert werden diese Skriptausführungen mittels der PRTG-Benachrichtigungsfunktion. Genau betrachtet, ist eine Skriptausführung also eine Sonderform der Alarmierung.

Der Sensor „WMI Prozess“ bzw. „WMI Dienst“ kann im Fehlerfall versuchen Prozesse/Dienste automatisiert neu zu starten. Erst wenn dies nicht erfolgreich war, geht der Sensor in den Fehlerstatus und man muss manuell eingreifen.

Weitere Möglichkeiten der Automatisierung wurden getestet (Stichwort: Automatisierter Neustart von Servern), wurde aber für zu riskant erachtet und somit verworfen.

Im Rahmen der Möglichkeiten eines Batchskripts können jederzeit Erweiterungen in der Automatisierung vorgenommen werden. Auch die Möglichkeit diverser Dienstprogramme im „.exe“ Dateiformat ist gegeben, wurde aber aus Sicherheitsgründen vorerst noch nicht im System getestet.

6 Bewertung der erreichten Ergebnisse

Anhand der in Punkt 3 definierten Zieldefinitionen lassen sich die Ergebnisse dieser Diplomarbeit wie folgt bewerten:

Eine der wichtigsten Erkenntnisse im Laufe dieser Arbeit war, dass zwar jedes Gerät Daten mittels der am Markt befindlichen Methoden an ein zentrales System liefern kann, diese sind aber nicht immer gut verwertbar. Für eine detaillierte Fehleranalyse muss anschließend das Gerät direkt begutachtet werden und der Fehler dort behoben werden. Somit lassen sich zwar die Fehler wie geplant zentral auf einem einzigen System abbilden, für einen tieferen Blick sind aber weiterhin die Benutzeroberflächen der Geräte direkt heranzuziehen.

Das Festlegen geeigneter Auswahlkriterien, welche sich für alle möglichen Produkte decken, ist nur sehr schwer machbar. Es ist sehr viel Objektivität und sehr viel Kompromissbereitschaft notwendig. Nur aufgrund tatsächlicher Fakten ist eine Auswahl nicht sinnvoll und auch kaum machbar. Jeder Beteiligte hat auf unterschiedlichste Teilbereiche Wert gelegt. Um dem entgegenzuwirken, wurde mittels Gewichtung der einzelnen Anforderungsbereiche gearbeitet, um trotzdem auf ein verwertbares Ergebnis zu kommen.

Damit die Auswahlkriterien für die diversen Tools universell eingesetzt werden konnten, mussten diese sehr allgemein gehalten werden. Dadurch konnte eine einheitliche Bewertung durchgeführt werden. Bei manchen Tools lässt dies aber einen gewissen persönlichen Interpretationsspielraum, speziell bei der Beurteilung mit KO-Kriterien konnten nicht immer klare Beurteilungen vorgenommen werden. Da aber bei den meisten Varianten nicht nur ein einzelnes KO-Kriterium zum Tragen kam, konnte die Anzahl der Varianten mit der eingesetzten Methodik sehr gut vereinfacht werden.

In der Testphase zeigten sich bereits bei der Installation diverse Unterschiede. Bei der Konfiguration konnten die Testszenarien nicht überall vollständig umgesetzt werden, bzw. waren dazu umfangreiche Anpassungen nötig. Die 2 wöchigen Tests brachten sehr gut auswertbare Ergebnisse in Bezug auf die notwendigen Funktionen und Kriterien. Jede Software hat klare Stärken und Schwächen und es gab diverse Präferenzen für jedes einzelne Tool. Diese persönlichen Meinungen und die Ergebnisse lassen eine objektive Bewertung nur sehr schwer zu. Dieser Umstand wurde mit der Gewichtung der Kriterien sehr gut kompensiert. Die Nutzwertanalyse brachte überraschenderweise nicht das klare Ergebnis für ein einzelnes Tool. Dies liegt an der Tatsache, dass durch die Vorauswahl nur mehr geeignete Varianten in der engeren Auswahl waren.

Die Entscheidung für den PRTG Network Monitor von Paessler war trotzdem eindeutig, da die gewünschten Funktionalitäten sowie die erforderliche Akzeptanz, aber auch die Skalierbarkeit für die Zukunft damit am besten abgedeckt werden können. Aber auch hier mussten diverse Kompromisse eingegangen werden.

Die Hardwarekonzeption konnte mittels der firmeneigenen Regeln sehr rasch zufriedenstellend abgeschlossen werden. Zudem wurden vom Hersteller keine speziellen Hardwarekonfigurationen gefordert. Das Faktum, dass diese Servertype bereits mehrfach im Unternehmen im Einsatz ist, machte die Entscheidung für dieses Produkt noch leichter. Mittels eines 5-jährigen Wartungsvertrags ist auch die langfristige Laufzeit der Hardware sichergestellt und der Betrieb der Software gesichert.

Die abschließende Konzeption der Softwareimplementierung erwies sich als sehr zeitintensiv. Grund dafür war die Erstellung des detaillierten Strukturplans, da hier jedes Gerät einzeln analysiert werden musste. Dieser ist jedoch eine sehr wichtige Basis, wenn im Anschluss an die Diplomarbeit die Implementierung erfolgt. Hier kann mittels Strukturplan sehr rasch der geforderte Strukturbaum erstellt werden und mittels Vererbung der Zugangsberechtigungen bzw. der globalen Einstellungen (Abtastintervall, Benachrichtigungen) ein lauffähiges Echtsystem konfiguriert werden, ohne immer wieder zu unterbrechen, um die Geräte zu analysieren.

Die externe Verfügbarkeit ermöglicht eine Überprüfung der Geräte von überall. Auch Anpassungen und Erweiterungen sind über die Weboberfläche jederzeit möglich. Das entstehende Sicherheitsrisiko durch die Verfügbarkeit über das Internet, lässt sich durch gezielte Portfreigaben auf ein Minimum reduzieren und wird durch den entstehenden Mehrwert in Kauf genommen.

Der Datenexport ist möglich, muss aber sehr umständlich eingerichtet werden. Dies ist einer der Schwachpunkte von PRTG. Da hier aber nicht ständig neue Reports eingerichtet werden müssen, ist dieser Umstand nicht als kritisch zu betrachten.

Die Visualisierungsmöglichkeit mittels frei definierbarer Maps bzw. Dashboards ist ein sehr gutes Feature, um die Daten graphisch auswerten zu können und auf den ersten Blick Veränderungen der Sensoren zu erkennen.

Das Budget war für viele der Tools ein absolutes KO-Kriterium, da man für ein reines Tool zur Überwachung möglichst wenig Geld ausgeben will. Ein Freewaretool ist, aufgrund der hohen Konfigurationszeiten und des oftmals fehlenden Supports, nicht für eine schnelle Realisierung geeignet, da der Mitarbeiteraufwand die Anschaffung eines kommerziellen Systems klar übersteigt. Am Ende konnte mit PRTG Network Monitor in Verbindung mit einem Dell Server eine Lösung gefunden werden, die mit rund 5500 Euro innerhalb des zu Beginn vereinbarten Budgets von maximal 7000 Euro liegt.

7 Zusammenfassung und Ausblick

Durch die umfangreiche Marktanalyse konnten relativ schnell geeignete Kandidaten für das geplante Vorhaben gefunden werden. Auch zeigte sich, wie groß der Markt in diesem Bereich bereits ist und wieviel bereits standardisiert ist.

Mittels Tests, Gesprächen, Demonstrationen und Analysen der einzelnen Tools, konnte man einen guten Einblick in die diversen Möglichkeiten bekommen. Mehr als ein Überblick war im Zuge der Arbeit bei vielen Produkten nicht möglich, da die Menge an Möglichkeiten einfach zu groß ist.

Durch das abschließend erstellte Implementierungskonzept kann das Monitoring jederzeit in den Echtbetrieb übergehen und somit böse Überraschungen im Arbeitsalltag durch frühzeitige Benachrichtigungen stark eingedämmt werden.

Auch an Wochenenden, Feiertagen oder in der Nacht kann zukünftig, mittels des externen Zugangs sowie der Alarmierung per Mail und SMS, immer die Gesundheit der einzelnen Geräte im Auge behalten werden.

Da man sich für ein kommerzielles Produkt entschied, wird für die Implementierung nur mehr sehr wenig Zeit in Anspruch genommen. Die Kosten bleiben trotzdem im definierten Rahmen.

Der nächste Schritt ist, wie bereits erwähnt, der Übergang in den Echtbetrieb. Dieser wird sehr zeitnah erfolgen, um die Verbesserungen für den Arbeitsalltag so schnell wie möglich nutzen zu können.

Weitere Themen sind der Ausbau diverser Automatismen, um Fehler selbstständig zu beheben (Dienstneustart, Programmausführung usw.).

Bisher läuft nur ein Server, sollte dieser ein Problem haben, funktioniert der gesamte Monitoringdienst nicht mehr. Angedacht ist eine virtuelle Maschine, wodurch ein Failovercluster aus zwei Servern entsteht.

Geplant ist in weiterer Folge auch ein zentrales Dashboard im IT-Büro, dieses soll allen Mitarbeitern zu jeder Zeit einen Überblick über die gesamte Systemgesundheit geben.

Literaturverzeichnis

Brisson, Florent (2004): SNMP Objects and mib tree. Online verfügbar unter http://www.loriotpro.com/Products/On-line_Documentation_V5/LoriotProDoc_EN/C3-Introduction_to_Network_Supervision/C3-F6_Main_%20SNMP_Objects_EN.htm, zuletzt aktualisiert am 08.03.2011, zuletzt geprüft am 06.04.2017.

Datacom (Hg.) (2013): Skriptsprache :: script language :: ITWissen.info. Online verfügbar unter http://www.itwissen.info/Skriptsprache-script-language.html, zuletzt geprüft am 10.04.2017.

Dell (2017): Dell Österreich. Online verfügbar unter http://www.dell.at/, zuletzt geprüft am 15.05.2017.

Dietmüller, Peter (2011): Dietmüller. Online verfügbar unter http://www.dietmueller.at/download/05_SNMP.pdf, zuletzt aktualisiert am 30.11.2011, zuletzt geprüft am 04.02.2017.

ELEK (2017a): ICMP - Internet Control Message Protocol. Elektronik Kompendium. Online verfügbar unter http://www.elektronik-kompendium.de/sites/net/0901011.htm, zuletzt geprüft am 06.04.2017.

ELEK (2017b): Ping - Paket Internet Groper / pathping. Elektronik Kompendium. Online verfügbar unter http://www.elektronik-kompendium.de/sites/net/0901031.htm, zuletzt geprüft am 06.04.2017.

Flasskamp, Maik (2015): Was ist eine Push-Benachrichtigung? Einfach erklärt. Online verfügbar unter http://praxistipps.chip.de/was-ist-eine-push-benachrichtigung-einfach-erklaert_42231, zuletzt geprüft am 10.04.2017.

GFI (2017): Verwaltung und Überwachung von Log-Daten. Online verfügbar unter http://www.gfisoftware.de/products-and-solutions/network-security-solutions/gfi-eventsmanager, zuletzt geprüft am 17.04.2017.

Gibb, Taylor (2017): 5 Cmdlets to Get You Started with PowerShell. Online verfügbar unter https://www.howtogeek.com/114344/5-cmdlets-to-get-you-started-with-powershell/, zuletzt geprüft am 07.04.2017.

Graham, Horton: Ideenbewertung mit der Paarvergleichsmatrix « Zephram. Online verfügbar unter http://www.zephram.de/blog/ideenbewertung/ideenbewertung-paarvergleichsmatrix/, zuletzt geprüft am 10.04.2017.

Grote, Marc (2015): Vielschichtiger Superheld. Architektur des Sysem Center 2012 R2 Operations Manager. In: *IT-Administrator* 2015 (Sonderheft 2/2015), S. 77–83.

H3C (2017): Technology White Paper - Product & Technology - H3C. Online verfügbar unter http://www.h3c.com.hk/Products___Technology/Technology/System_Management/Technology_White_Paper/200805/606347_57_0.htm, zuletzt aktualisiert am 16.03.2017, zuletzt geprüft am 06.04.2017.

Hagel (2017): Monitoring von IT-Systemen - eine Übersicht. Hagel IT Services. Online verfügbar unter https://www.hagel-it.de/it-sicherheit/monitoring-von-it-systemen-eine-uebersicht.html, zuletzt geprüft am 06.04.2017.

Hein, Mathias (2015): Streckenposten. Monitoring in LAN und WAN. In: *IT-Administrator* 2015 (Sonderheft 2/2015), S. 64–67.

Ipswitch (2017): WhatsUp Gold Netzwerk-Monitoring. Online verfügbar unter https://de.ipswitch.com/anwendungs-und-netzwerk-monitoring/whatsup-gold, zuletzt geprüft am 12.04.2017.

Jansen, Sven (2011): Nutzwertanalyse im Projektmanagement: Grin Verlag.

Kettner, Mathias (2017): Check_MK. Online verfügbar unter https://mathias-kettner.de/check_mk.html, zuletzt aktualisiert am 11.04.2017, zuletzt geprüft am 12.04.2017.

ManageEngine (2017): Network Monitoring Software by ManageEngine OpManager. Online verfügbar unter https://www.manageengine.com/network-monitoring/, zuletzt aktualisiert am 28.03.2017, zuletzt geprüft am 17.04.2017.

Meier, Prof.Dr. Markus: Auswählen und Bewerten. ETH Zürich. Online verfügbar unter http://e-collection.library.ethz.ch/eserv/eth:25112/eth-25112-01.pdf, zuletzt geprüft am 10.04.2017.

Microsoft Technet (2017): Übersicht über die Windows-Verwaltungsinstrumentation (Windows Management Instrumentation, WMI). Online verfügbar unter https://technet.microsoft.com/de-de/library/dn265977(v=ws.11).aspx, zuletzt aktualisiert am 04.02.2017, zuletzt geprüft am 04.02.2017.

Mitchell, Bradley (2012): What is a network sniffer and how does it work? Online verfügbar unter https://www.lifewire.com/definition-of-sniffer-817996, zuletzt geprüft am 07.04.2017.

MKW (2017): MKW Website. Online verfügbar unter http://www.mkw.at/, zuletzt geprüft am 06.04.2017.

Mrvka, Martin (2014): Wie funktioniert eine SMS. Online verfügbar unter https://websms.at/blog/websms-technische-infos/1179-wie-funktioniert-eine-sms, zuletzt geprüft am 07.04.2017.

Nagios (2017): Nagios - Network, Server and Log Monitoring Software. Online verfügbar unter https://www.nagios.com/, zuletzt geprüft am 17.04.2017.

OpenNMS (2017): OpenNMS - Product Base. Online verfügbar unter https://www.opennms.org/en, zuletzt geprüft am 17.04.2017.

Paessler (2017): PRTG Network Monitor - umfassende Netzwerkmonitoring-Software. Online verfügbar unter https://www.de.paessler.com/prtg, zuletzt aktualisiert am 12.04.2017, zuletzt geprüft am 12.04.2017.

PandoraFMS (2017): Documentation Netflow PandoraFMS. Online verfügbar unter http://wiki.pandorafms.com/index.php?title=Pandora:Documentation_en:Netflow, zuletzt aktualisiert am 23.03.2017, zuletzt geprüft am 06.04.2017.

Petterson, Michael (2009): NetFlow v9 vs. NetFlow v5: What are the differences? Online verfügbar unter https://www.plixer.com/blog/netflow/netflow-v9-vs-netflow-v5/, zuletzt aktualisiert am 05.04.2017, zuletzt geprüft am 06.04.2017.

PRTG Netflow (2017): NetFlow-Analyse- & Monitoring-Tool - PRTG. Online verfügbar unter https://www.de.paessler.com/netflow_monitoring, zuletzt aktualisiert am 06.04.2017, zuletzt geprüft am 06.04.2017.

PRTG WMI (2017): PRTG Manual: Monitoring via WMI. Online verfügbar unter https://www.paessler.com/manuals/prtg/wmi_monitoring, zuletzt aktualisiert am 06.04.2017, zuletzt geprüft am 06.04.2017.

PRTG-SMS (2017): Sending out PRTG SMS Notifications in 8 easy steps. Online verfügbar unter https://www.de.paessler.com/blog/sending-out-prtg-sms-gsm-modem-mwconn, zuletzt geprüft am 29.05.2017.

PRTG-Sniff (2017): Bandbreiten-Monitoring mit PRTG Network Monitor mittels Packet Sniffing. Online verfügbar unter https://www.de.paessler.com/packet_sniffing, zuletzt geprüft am 07.04.2017.

Reder, Bernd (2015): Paessler RTG mit kostenloser Push-Benachrichtigung | WindowsPro. Online verfügbar unter https://www.windowspro.de/news/network-monitoring-paessler-rtg-kostenloser-push-benachrichtigung/02312.html, zuletzt geprüft am 10.04.2017.

Sacks, Matthew (2009): App Watch » Linux Magazine. Online verfügbar unter http://www.linux-magazine.com/Issues/2009/102/Hyperic-HQ, zuletzt geprüft am 17.04.2017.

Schönwandt, Walter Prof. Dr. Ing. (2007): Methoden zur Beurteilung von Varianten. Universität Stuttgart. Online verfügbar unter http://www.igp.uni-stuttgart.de/publika/pdf/methoden.pdf, zuletzt aktualisiert am 2007, zuletzt geprüft am 15.03.2017.

ServerEye (2017): Funktionen der Server-Eye IT Monitoring Software. Online verfügbar unter https://www.server-eye.de/funktionen/, zuletzt aktualisiert am 16.04.2017, zuletzt geprüft am 17.04.2017.

Solarwinds (2017): IT-Verwaltungssoftware und Überwachungstools | SolarWinds. Online verfügbar unter http://www.solarwinds.com/de/, zuletzt geprüft am 17.04.2017.

Solarwinds Netflow: What is NetFlow by SolarWinds. Online verfügbar unter http://www.solarwinds.com/de/what-is-netflow, zuletzt geprüft am 04.02.2017.

Solarwinds Netflow Configuration (2017): How-To Configure NetFlow v5 & v9 on Cisco® Routers. Online verfügbar unter https://web.swcdn.net/creative/pdf/techtips/configure_netflow_on_cisco_routers.pdf, zuletzt geprüft am 06.04.2017.

Souvickroy (Hg.) (2017): Installing SCOM 2016 TP4 step by step | souvickroy on WordPress.com. Online verfügbar unter https://souvickroy.wordpress.com/2015/11/29/installing-scom-2016-tp4-step-by-step/, zuletzt geprüft am 17.04.2017.

Stor IT Back (2010): RAID / RAID-Level - Performance und Verfügbarkeit. Online verfügbar unter https://www.storitback.de/service/raidlevel.html, zuletzt geprüft am 15.05.2017.

Universität Bamberg (2017): Funktionsweise von E-Mail-Systemen. Online verfügbar unter https://www.uni-bamberg.de/rz/dienstleistungen/mail/weitere-informationen-zu-e-mail/funktionsweise-von-e-mail-systemen/, zuletzt geprüft am 07.04.2017.

Vardanyan, Mikayel (2011): 11 Top Server Management & Monitoring Software. Online verfügbar unter http://www.monitis.com/blog/11-top-server-management-monitoring-software/, zuletzt geprüft am 17.04.2017.

vmWare (2017): vRealize Hyperic - VMware Products. Online verfügbar unter http://www.vmware.com/products/vrealize-hyperic.html, zuletzt aktualisiert am 24.03.2017, zuletzt geprüft am 17.04.2017.

Weber, Markus B. (2016): MWconn. Online verfügbar unter http://mwconn.net/info.html, zuletzt aktualisiert am 26.04.2016, zuletzt geprüft am 29.05.2017.

Wiki Zabbix (2017): Zabbix. Online verfügbar unter https://de.wikipedia.org/w/index.php?oldid=160650677, zuletzt aktualisiert am 14.04.2017, zuletzt geprüft am 17.04.2017.

Wiki-NF (2017): Netflow. Wikipedia. Online verfügbar unter https://de.wikipedia.org/w/index.php?oldid=160824375, zuletzt aktualisiert am 14.01.2017, zuletzt geprüft am 04.02.2017.

Wiki-PS (2017): PowerShell. Wikipedia. Online verfügbar unter https://de.wikipedia.org/w/index.php?oldid=162283023, zuletzt aktualisiert am 03.02.2017, zuletzt geprüft am 04.02.2017.

Wiki-Raid (2017): RAID. Online verfügbar unter https://de.wikipedia.org/w/index.php?oldid=165375119, zuletzt aktualisiert am 10.05.2017, zuletzt geprüft am 15.05.2017.

WIki-SNMP (2017): Simple Network Management Protocol. Wikipedia. Online verfügbar unter https://de.wikipedia.org/w/index.php?oldid=160645490, zuletzt aktualisiert am 19.01.2017, zuletzt geprüft am 04.02.2017.

Wiki-Soap (2017): SOAP. Hg. v. Wikipedia. Online verfügbar unter https://de.wikipedia.org/w/index.php?oldid=161834228, zuletzt aktualisiert am 22.03.2017, zuletzt geprüft am 06.04.2017.

Wiki-SSH (2017): Secure Shell. Hg. v. Wikipedia. Online verfügbar unter https://de.wikipedia.org/w/index.php?oldid=162745856, zuletzt aktualisiert am 20.03.2017, zuletzt geprüft am 07.04.2017.

Wiki-Ticket (2017): Issue-Tracking-System. Hg. v. Wikipedia. Online verfügbar unter https://de.wikipedia.org/w/index.php?oldid=160771016, zuletzt aktualisiert am 25.03.2017, zuletzt geprüft am 10.04.2017.

Wireshark (2017): Wireshark · Go Deep. Online verfügbar unter https://www.wireshark.org/, zuletzt aktualisiert am 06.03.2017, zuletzt geprüft am 12.04.2017.

Wittmann, Martina (2015): Netzwerküberwachung mit SNMP. In: *IT-Administrator* 2015 (Sonderheft 2/2015), S. 36–42.

Anlagen

Anlagen, Teil 1

Nutzwertanalyse als Detailansicht

		GFI		PRTG		SolarWinds		WhatsUP		Maximum	
Kriterium	**Gewichtung**	**Wert**	**verrechnet**	**Wert**	**verrechnet**	**Wert**	**verrechnet**	**Wert**	**verrechnet**	**Wert**	**verrechnet**
Kosten	15%	5	0,75	10	1,5	5	0,75	5	0,75	10	1,5
Erstkonfiguration	10%	10	1	5	0,5	10	1	10	1	10	1
Systemwartung	5%	5	0,25	5	0,25	5	0,25	5	0,25	10	0,5
Überwachungsmethoden	15%	5	0,75	10	1,5	5	0,75	10	1,5	10	1,5
Cloudanbindung	2%	0	0	5	0,1	0	0	0	0	10	0,2
Mobilität	4%	0	0	10	0,4	0	0	5	0,2	10	0,4
Alarmierungsvarianten	10%	10	1	10	1	10	1	10	1	10	1
Automatisierung	5%	5	0,25	10	0,5	5	0,25	5	0,25	10	0,5
Standortübergreifend	2%	5	0,1	10	0,2	5	0,1	5	0,1	10	0,2
Bedienbarkeit	10%	10	1	5	0,5	10	1	10	1	10	1
Installation	5%	5	0,25	10	0,5	5	0,25	5	0,25	10	0,5
Hardwarekonzept	5%	10	0,5	10	0,5	10	0,5	10	0,5	10	0,5
Redundanz	2%	5	0,1	5	0,1	5	0,1	5	0,1	10	0,2
Sicherheit	5%	0	0	10	0,5	5	0,25	10	0,5	10	0,5
Lizenzmodell	5%	10	0,5	5	0,25	0	0	5	0,25	10	0,5
	100%		6,45		8,3		6,2		7,65		10

Anlagen, Teil 2

Übersicht Protokollzugriffe, Userverwaltung, Usergruppen

Protokollzugriffe			
Protokoll	**User**	**Rechte**	**Info**
SNMPv1	public	Zugriff auf SNMPv1 Geräte	SNMP-Port: 161
SNMPv2c	public	Zugriff auf SNMPv2c Geräte	SNMP-Port: 161
SNMPv3	writeuser	Zugriff auf SNMPv3 Geräte	SNMP-Port: 161
WMI	prtg	Administrator für Windows	Domäne: mkw.at, Zugang für WMI Sensoren
SOAP	vm-admin	Administrator für vmWare	Domäne: mkw.at
Powershell	prtg	Administrator für Windows	Gleich wie bei WMI Sensoren

Benutzergruppen	
Gruppe	**Rechte**
IT-Abteilung	Lesen,Schreiben, Ändern aller Sensoren
Haustechnik	Lesen von Abteilungsrelevanten Sensoren (Temperaturen usw.)
Viewer	Lesen bestimmter Sensoren für einen groben Überblick

Benutzer			
User	**Username**	**Rolle**	**Gruppe**
Christoph Voraberger	christoph	Administrator	IT-Abteilung
Roland Krausgruber	kroli	Administrator	IT-Abteilung
Rene Gebetsroither	rene	Administrator	IT-Abteilung
Laura Humer	laura	Administrator	IT-Abteilung
Patrick Mair	patrick	Benutzer	Haustechnik
Christian Obermayr	obermayr	Benutzer	Haustechnik
Viewer	viewer	Benutzer	Viewer

Anlagen, Teil 3

Strukturplanung Sensorkonfiguration in PRTG

Standort	Gruppe	Gerät	Sensor	Fehlergrenzwert	Alarmierungsart	Alarm an
Weibern	Server	MKW-AD (Active Directory)	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung
			Festplattenspeicher (WMI)	<4GB	Mail	IT-Abteilung
			Dienst DHCP Server (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			DNS Port 53 (WMI Port)	Port nicht erreichbar	Mail	IT-Abteilung
			Dienst DNS Server (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Dienst NTDS (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Dienst Event Log (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
		MKW-EX2010 (Mail)	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung
			Festplattenspeicher C: und D: (WMI)	C: < 7GB; D:<15GB	Mail	IT-Abteilung
			Dienst Event Log (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			SMTP Port 25 (WMI)	Port nicht erreichbar	Mail	IT-Abteilung
			Dienst Microsofr Exchange Inforamtionsserver (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Exchange Datenbank (Powershell)	nicht verbunden	Mail	IT-Abteilung
		MKW-INFOR-DB (Datenbank ERP)	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung
			Festplattenspeicher C: und D: (WMI)	C: < 5GB; D:<15GB	Mail	IT-Abteilung
			Dienst SQLServer KU (WMI)	Dienst läuft nicht	Mail	IT-Abteilung
			Dienst SQL Server Reporting Services (WMI)	Dienst läuft nicht	Mail	IT-Abteilung
			Dienst SQLServer-Agent KU (WMI)	Dienst läuft nicht	Mail	IT-Abteilung
		MKW-INFOR-AP (Anwendung ERP)	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung
			Festplattenspeicher C: und D: (WMI)	C: < 5GB; D:<10GB	Mail	IT-Abteilung
			Dienst inforCE_KU (WMI)	Dienst läuft nicht	Mail	IT-Abteilung
			Dienst inforCE_Main_72 (WMI)	Dienst läuft nicht	Mail	IT-Abteilung
			Dienst inforLicenseServer_KU (WMI)	Dienst läuft nicht	Mail	IT-Abteilung
			Dienst inforCE_OD (WMI)	Dienst läuft nicht	Mail	IT-Abteilung
			Dienst inforCE_TEst (WMI)	Dienst läuft nicht	Mail	IT-Abteilung
			Dienst inforLicenseServer_OD (WMI)	Dienst läuft nicht	Mail	IT-Abteilung
			Dienst inforLicenseServer_Test (WMI)	Dienst läuft nicht	Mail	IT-Abteilung
		MKW-BMD (Buchhaltung)	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung
			Festplattenspeicher C: und D: (WMI)	C: < 5GB; D:<10GB	Mail	IT-Abteilung
			Dienst BMD-Server (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Dienst Event Log (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Dienst BMDNtcsSvc (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Dienst BMDSrv: BMD Netspeed (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
		MKW-BMD-NTCS (Buchhaltung Neu)	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung
			Festplattenspeicher C: und D: (WMI)	C: < 5GB; D:<10GB	Mail	IT-Abteilung
			Dienst Event Log (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Dienst NTCSSvr (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
		MKW-Filestore (Datenablage)	Verfügbarkeit (Ping)	Dienst läuft nicht	Mail	IT-Abteilung
			Festplattenspeicher C,D,E,F und G (WMI)	C:< 5GB; D:<10GB;E:<10GB;F:<10GB;G:<10GB	Mail	IT-Abteilung
			Dienst Event Log (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Dienst Dfs (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Dienst DFSR (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
		MKW-Print (Drucker)	Verfügbarkeit (Ping)	Dienst läuft nicht	Mail	IT-Abteilung
			Festplattenspeicher C: (WMI)	C:< 10GB	Mail	IT-Abteilung
			Dienst Event Log (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Dienst Druckerwarteschlange (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Dienst Seagull License Server (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Dienst EFMS Server (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung

Standort	Gruppe	Gerät	Sensor	Fehlergrenzwert	Alarmierungsart	Alarm an
Weibern	Server	MKW-Saperion (Belegarchivierung)	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung
			Festplattenspeicher C: und D: (WMI)	C: < 5GB; D:<50GB	Mail	IT-Abteilung
			Fehlgeschalgene Mailimporte (WMI Ordner)	Datei in Ordner nicht importierbar	Mail	Christoph
			Anzahl importierte Mails (WMI Ordner)	Älteste Datei 180 Tage (Ordnerinhalt) löschen)	Mail	Christoph
			Saperion Java Core Server (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Falsche Mailanhänge(WMI Ordner)	Datei in Ordner Faslche Attechments	Mail	Christoph
		MKW-SQL-2008R2 (Datenbanken)	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung
			Festplattenspeicher C: und D: (WMI)	C: < 1,5GB; D:<4GB	Mail	IT-Abteilung
			Dienst Event Log (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Dienst SQL Server (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Dienst SQL Server Browser (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Dienst SQL Server Agent (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Prozess Artikel Viewer Sync (WMI Prozess)	Prozess fehlerhaft	Mail	IT-Abteilung
			Prozess VAD Sync (WMI Prozess)	Prozess fehlerhaft	Mail	IT-Abteilung
			Dienst WHComTaskService01 (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Dienst WHControlService (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Dienst WHGuardian (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			SQL Server Instanz	rein informativ	-	-
		MKW-SQL (Datenbanken)	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung
			Festplattenspeicher C: und D: (WMI)	C: < 0,5GB; D:<15GB	Mail	IT-Abteilung
			Dienst Event Log (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Dienst SQL Server (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Dienst SQL Server Browser (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Dienst SQL Server Integration Services (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Datei Infor_to_ABB_Errorlog.txt vorhanden? (WMI Datei)	Datei vorhanden	Mail	IT-Abteilung
			SQL Server Instanz	rein informativ	-	-
		MKW-Terminal (Anwendungen)	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung
			Festplattenspeicher C: (WMI)	C: < 10GB	Mail	IT-Abteilung
			Dienst Event Log (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Dienst DameWare Server (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
		MKW-PDM (Konstruktionsdaten)	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung
			Festplattenspeicher C: und D: (WMI)	C: < 10GB; D:<100GB	Mail	IT-Abteilung
			Dienst Event Log (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Dienst SolidWorks License Manager (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Dienst Solidworks PDM Archivserver (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Dienst Solid Works PDM Datenbankserver (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung

Standort	Gruppe	Gerät	Sensor	Fehlergrenzwert	Alarmierungsart	Alarm an
Weibern	Server	MKW-EDI-Echt (EDI Anbindung)	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung
			Festplattenspeicher C: (WMI)	C: < 10GB	Mail	IT-Abteilung
			Dienst Event Log (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Dienst Lobster Integration Server (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
		MKW-EDIFACT (EDI-Anbindung)	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung
			Festplattenspeicher C: (WMI)	C: < 10GB	Mail	IT-Abteilung
			Dienst Event Log (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Ordnergröße Inernorm ORDERS05 Job (WMI Ordner)	>650KB	Mail	IT-Abteilung
			Prozess XML Edifact Converterf.exe (WMI Prozess)	Prozess fehlerhaft	Mail	IT-Abteilung
		MKW-SCS (SystemCenter)	Verfügbarkeit (Ping)	Dienst läuft nicht	Mail	IT-Abteilung
			Festplattenspeicher C,D,S und W (WMI)	C:< 10GB; D:<10GB;S:<10GB;W:<10GB	Mail	IT-Abteilung
			Dienst Event Log (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Dienst Update Services (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
		MKW-Intranet (Intranetserver)	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung
			Festplattenspeicher C: (WMI)	C: < 10GB	Mail	IT-Abteilung
			Dienst Event Log (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Dienst IIS-Verwaltungsdienst (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
		MKW-BI (Datenauswertungen)	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung
			Festplattenspeicher C: (WMI)	C: < 5GB	Mail	IT-Abteilung
			Dienst Event Log (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Prozess qvs.exe (WMI Prozess)	Prozess fehlerhaft	Mail	IT-Abteilung
			CPU-Auslastung (WMI)	>=80%	Mail	IT-Abteilung
		MKW-Backup (Backup AD)	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung
			Festplattenspeicher C: (WMI)	C: < 5GB	Mail	IT-Abteilung
			Dienst Event Log (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Systemgesundheit (SNMP)	laut Sensorstandard	Mail	IT-Abteilung
			Dienst DHCP Server (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Dienst DNS Server (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Dienst ekey bit service (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Dienst TeleData-CallData Import (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Dienst TeleData-Service Controller (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Festplattenstatus (SNMP)	laut Sensorstandard	Mail	IT-Abteilung
		MKW-Protect (div. Anwendungen)	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung
			Festplattenspeicher C: (WMI)	C: < 5GB	Mail	IT-Abteilung
			Dienst Event Log (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Systemgesundheit (SNMP)	laut Sensorstandard	Mail	IT-Abteilung
			Prozess Outlook.exe (WMI Prozess)	Prozess fehlerhaft	Mail	IT-Abteilung
			Prozess Datapump_agent.exe.exe (WMI Prozess)	Prozess fehlerhaft	Mail	IT-Abteilung
			Prozess Netmanager.exe (WMI Prozess)	Prozess fehlerhaft	Mail	IT-Abteilung
			Festplattenstatus (SNMP)	laut Sensorstandard	Mail	IT-Abteilung

Standort	Gruppe	Gerät	Sensor	Fehlergrenzwert	Alarmierungsart	Alarm an
Weibern	Server	MKW-DWHouse (Datawarehouse)	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung
			Festplattenspeicher C: und D: (WMI)	C: < 5GB; D:<50GB	Mail	IT-Abteilung
			Dienst Event Log (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Systemgesundheit (SNMP)	laut Sensorstandard	Mail	IT-Abteilung
			Dienst SQL Server (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Dienst SQL Server Browser (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Dienst SQL Server Agent (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Dienst IDL Application Server (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Dienst IDL Workplaxe Server Cache (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Dienst IDL Workplace Server Event (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Dienst IDL Workplace Server Job (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Dienst IDL Workplace Server Scheduled Job (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Dienst IDL Workplace Server Semantic Logging(WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			SQL Server Instanz	rein informativ	-	-
			Festplattenstatus (SNMP)	laut Sensorstandard	Mail	IT-Abteilung
		MKW-PRTG (Monitoring)	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung
			Festplattenspeicher C: (WMI)	C: < 50GB	Mail	IT-Abteilung
			Dienst Event Log (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Systemgesundheit (SNMP)	laut Sensorstandard	Mail	IT-Abteilung
			Festplattenstatus (SNMP)	laut Sensorstandard	Mail	IT-Abteilung
		MKW-AS-Weibern (Backup)	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung

Standort	Gruppe	Gerät	Sensor	Fehlergrenzwert	Alarmierungsart	Alarm an
Weibern	Netzwerkgeräte	Switch Serverraum 1	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung
			Temperatur (SNMP)	>65°C	Mail	IT-Abteilung
			CPU-Auslastung (SNMP)	>80%	Mail	IT-Abteilung
		Switch Serverraum 2	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung
			Temperatur (SNMP	>65°C	Mail	IT-Abteilung
			CPU-Auslastung (SNMP)	>80%	Mail	IT-Abteilung
		Switch Serverraum 3	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung
			Temperatur (SNMP	>65°C	Mail	IT-Abteilung
			CPU-Auslastung (SNMP)	>80%	Mail	IT-Abteilung
			Netflow v9	vorerst rein informativ	-	-
		Switch Serverraum 4	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung
			Temperatur (SNMP	>65°C	Mail	IT-Abteilung
			CPU-Auslastung (SNMP)	>80%	Mail	IT-Abteilung
		Switch EDV 1	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung
			Temperatur (SNMP	>65°C	Mail	IT-Abteilung
			CPU-Auslastung (SNMP)	>80%	Mail	IT-Abteilung
			Netflow v9	vorerst rein informativ	-	-
		Switch EDV 2	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung
			Temperatur (SNMP	>65°C	Mail	IT-Abteilung
			CPU-Auslastung (SNMP)	>80%	Mail	IT-Abteilung
		Switch Draht 1	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung
			Temperatur (SNMP	>65°C	Mail	IT-Abteilung
			CPU-Auslastung (SNMP)	>80%	Mail	IT-Abteilung
		Switch Draht 2	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung
			Temperatur (SNMP	>65°C	Mail	IT-Abteilung
			CPU-Auslastung (SNMP)	>80%	Mail	IT-Abteilung
			Netflow v9	vorerst rein informativ	-	-
		Switch PSP 1	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung
			Temperatur (SNMP	>65°C	Mail	IT-Abteilung
			CPU-Auslastung (SNMP)	>80%	Mail	IT-Abteilung
		Switch PPR 1	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung
			Temperatur (SNMP	>65°C	Mail	IT-Abteilung
			CPU-Auslastung (SNMP)	>80%	Mail	IT-Abteilung
			Netflow v9	vorerst rein informativ	-	-
		Switch PPR 2	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung
			Temperatur (SNMP	>65°C	Mail	IT-Abteilung
			CPU-Auslastung (SNMP)	>80%	Mail	IT-Abteilung
		Switch Stöcklhaus 1	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung
			Temperatur (SNMP	>65°C	Mail	IT-Abteilung
			CPU-Auslastung (SNMP)	>80%	Mail	IT-Abteilung
			Netflow v9	vorerst rein informativ	-	-

Standort	Gruppe	Gerät	Sensor	Fehlergrenzwert	Alarmierungsart	Alarm an
Weibern	Drucker	Vermittlung	Druckerübersicht (SNMP)	laut Sensorvoreinstellung	Mail	Christoph
		Technik	Druckerübersicht (SNMP)	laut Sensorvoreinstellung	Mail	Christoph
		Verwaltung	Druckerübersicht (SNMP)	laut Sensorvoreinstellung	Mail	Christoph
		Draht Arbeitsvorbereitung Mono	Druckerübersicht (SNMP)	laut Sensorvoreinstellung	Mail	Christoph
		Draht Arbeitsvorbereitung Color	Druckerübersicht (SNMP)	laut Sensorvoreinstellung	Mail	Christoph
		Logistik	Druckerübersicht (SNMP)	laut Sensorvoreinstellung	Mail	Christoph
		Verkauf	Druckerübersicht (SNMP)	laut Sensorvoreinstellung	Mail	Christoph
		Werkzeugbau	Druckerübersicht (SNMP)	laut Sensorvoreinstellung	Mail	Christoph
		Draht Logistik	Druckerübersicht (SNMP)	laut Sensorvoreinstellung	Mail	Christoph
		Drahtfertigung	Druckerübersicht (SNMP)	laut Sensorvoreinstellung	Mail	Christoph
		Presserei Leitung	Druckerübersicht (SNMP)	laut Sensorvoreinstellung	Mail	Christoph
		Presserei Produktion	Druckerübersicht (SNMP)	laut Sensorvoreinstellung	Mail	Christoph
		Buchhaltung	Druckerübersicht (SNMP)	laut Sensorvoreinstellung	Mail	Christoph
		Konstruktion Sanitär	Druckerübersicht (SNMP)	laut Sensorvoreinstellung	Mail	Christoph
		Spritzguss	Druckerübersicht (SNMP)	laut Sensorvoreinstellung	Mail	Christoph
	Firewall	MKW-Firewall				
			Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung
			Uptime	rein informativ	-	-
			Systemzeit	rein informativ	-	-
			Load Durchschnitt 15 Minuten	rein informativ	-	-
			verwendeter RAM	rein informativ	-	-
			Anzahl Schnittstellen	rein informativ	-	-
			Interface Status IF1	down	Mail	IT-Abteilung
			Interface Status IF2	down	Mail	IT-Abteilung
			Interface Status IF3	down	Mail	IT-Abteilung
			Interface Status IF4	down	Mail	IT-Abteilung
	USV	Eaton Serverraum	Batteriekapazität (SNMP)	<60%	Mail	IT-Abteilung
			Überbrückungszeit (SNMP)	<60 Minuten	Mail	IT-Abteilung
			Eingangsspannung (SNMP)	<200 Volt	Mail	IT-Abteilung
			Auslastung (SNMP)	>75%	Mail	IT-Abteilung
		Eaton Stöcklhaus	Batteriekapazität (SNMP)	<60%	Mail	IT-Abteilung
			Überbrückungszeit (SNMP)	<60 Minuten	Mail	IT-Abteilung
			Eingangsspannung (SNMP)	<200 Volt	Mail	IT-Abteilung
			Auslastung (SNMP)	>75%	Mail	IT-Abteilung
		MGE Serverraum	Batteriekapazität (SNMP)	<60%	Mail	IT-Abteilung
			Überbrückungszeit (SNMP)	<60 Minuten	Mail	IT-Abteilung
			Eingangsspannung (SNMP)	<200 Volt	Mail	IT-Abteilung
			Auslastung (SNMP)	>75%	Mail	IT-Abteilung
		APC Logistik 1	Batteriekapazität (SNMP)	<60%	Mail	IT-Abteilung
			Überbrückungszeit (SNMP)	<60 Minuten	Mail	IT-Abteilung
			Eingangsspannung (SNMP)	<200 Volt	Mail	IT-Abteilung
			Auslastung (SNMP)	>75%	Mail	IT-Abteilung
		APC Logistik 2	Batteriekapazität (SNMP)	<60%	Mail	IT-Abteilung
			Überbrückungszeit (SNMP)	<60 Minuten	Mail	IT-Abteilung
			Eingangsspannung (SNMP)	<200 Volt	Mail	IT-Abteilung
			Auslastung (SNMP)	>75%	Mail	IT-Abteilung

Standort	Gruppe	Gerät	Sensor	Fehlergrenzwert	Alarmierungsart	Alarm an
Weibern	Sensoren	Temperatur Serverraum	Temperaturwert (SNMP	<15°C bzw. >30°C	Mail	IT-Abteilung
		Feuchtigkeit Serrverraum	Feuchtigkeitswert (SNMP)	<20% bzw. >60%	Mail	IT-Abteilung
	Virtualisierung	ESX-Host 1	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung
			Hardwarestatus VM	laut Sensorvoreinstellung	Mail	Christoph
		ESX-Host 2	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung
			Hardwarestatus VM	laut Sensorvoreinstellung	Mail	Christoph
		ESX-Host 3	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung
			Hardwarestatus VM	laut Sensorvoreinstellung	Mail	Christoph
		Netapp	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung
			Freier Speicher	laut Sensorvoreinstellung	Mail	Christoph
			Freier Speicher	laut Sensorvoreinstellung	Mail	Christoph
		Glasfaserswitch 1	Verfügbarkeit (Ping)	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS
	Leitungen	Internet (8.8.8.8)	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung
		Standleitung Haag (10.4.0.1)	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung
		Standleitung Presov (10.3.0.240)	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung
		Standleitung Rene (10.10.0.200)	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	Rene
	Sonstige	QNAP Software	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung
			Status Festplatte 1 (SNMP)	nicht OK	Mail	IT-Abteilung
			Status Festplatte 2 (SNMP)	nicht OK	Mail	IT-Abteilung
			Systemstatus (SNMP)	vorerst rein informativ	-	-
		QNAP-Backup	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung
			Status Festplatte 1 (SNMP)	nicht OK	Mail	IT-Abteilung
			Status Festplatte 2 (SNMP)	nicht OK	Mail	IT-Abteilung
			Status Festplatte 3 (SNMP)	nicht OK	Mail	IT-Abteilung
			Status Festplatte 4 (SNMP)	nicht OK	Mail	IT-Abteilung
			Systemstatus (SNMP)	vorerst rein informativ	-	-
		SMS Gateway	Anzahl gesendete SMS (WMI Ordner)	>100 Dateien (dann leeren)	Mail, Skript	Christoph
			Aktivität (WMI Prozess)	Prozess löuft nicht	Mail	IT-Abteilung

Standort	Gruppe	Gerät	Sensor	Fehlergrenzwert	Alarmierungsart	Alarm an
Haag am Hausruck	Server	HAAG-AD (Active Directory)	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung
			Festplattenspeicher C: und D: (WMI)	C: < 1GB; D:<10GB	Mail	IT-Abteilung
			Dienst Event Log (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Systemgesundheit (SNMP)	laut Sensorstandard	Mail	IT-Abteilung
			Festplattenstatus (SNMP)	laut Sensorstandard	Mail	IT-Abteilung
			Dienst DHCP Server (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			DNS Port 53 (WMI Port)	Port nicht erreichbar	Mail	IT-Abteilung
			Dienst DNS Server (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Dienst NTDS (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
		HAAG-Filestore (Dateiablage)	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung
			Festplattenspeicher C:,D: und E: (WMI)	C: < 5GB; D:<15GB; E:<10GB	Mail	IT-Abteilung
			Dienst Event Log (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Systemgesundheit (SNMP)	laut Sensorstandard	Mail	IT-Abteilung
			Festplattenstatus (SNMP)	laut Sensorstandard	Mail	IT-Abteilung
			Dienst Codemeter Runtime Service (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
		HAAG-Kasto (Lagersoftware)	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung
			Festplattenspeicher C:,D: und E: (WMI)	C: < 5GB; D:<10GB; E:<5GB	Mail	IT-Abteilung
			Dienst Event Log (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Systemgesundheit (SNMP)	laut Sensorstandard	Mail	IT-Abteilung
			Festplattenstatus (SNMP)	laut Sensorstandard	Mail	IT-Abteilung
			Dienst Kastolvr (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Dienst OracleServiceLVR (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Dienst OracleXETNSListener (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
		HAAG-ERP (ERP Server)	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung
			Festplattenspeicher C: und D: (WMI)	C: < 1GB; D:<10GB	Mail	IT-Abteilung
			Systemgesundheit (SNMP)	Dienst läuft nicht	Mail	IT-Abteilung
			Dienst Event Log (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Prozess uniRTE.exe (WMI Prozess)	Prozess fehlerhaft	Mail	IT-Abteilung
			Dienst Druckerwarteschlange (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Dienst maxx PDFMailer Network Sharing (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Dienst SQL Server (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Dienst SQL Integration Services (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Dienst SQL Server Agent (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			SQL Server Instanz	rein informativ	-	-
			Festplattenstatus (SNMP)	laut Sensorstandard	Mail	IT-Abteilung
		MKW-BESCH-W3 (Beschichtungsleitstand)	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung
			Festplattenspeicher C: (WMI)	C: < 10GB	Mail	IT-Abteilung
			Dienst Event Log (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Systemgesundheit (SNMP)	laut Sensorstandard	Mail	IT-Abteilung
			Festplattenstatus (SNMP)	laut Sensorstandard	Mail	IT-Abteilung
		MKW-AS-Haag (Backup)	Verfügbarkeit (Ping)			

Standort	Gruppe	Gerät	Sensor	Fehlergrenzwert	Alarmierungsart	Alarm an
Haag am Hausruck	Netzwerkgeräte	Werk 3 Switch Serverraum 1	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung
			Temperatur (SNMP	>65°C	Mail	IT-Abteilung
			CPU-Auslastung (SNMP)	>80%	Mail	IT-Abteilung
			Netflow v9	vorerst rein informativ	-	-
		Werk 3 Switch Serverraum 2	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung
			Temperatur (SNMP	>65°C	Mail	IT-Abteilung
			CPU-Auslastung (SNMP)	>80%	Mail	IT-Abteilung
			Netflow v9	vorerst rein informativ	-	-
		Werk 2 Switch Verwaltung 1	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung
			Temperatur (SNMP	>65°C	Mail	IT-Abteilung
			CPU-Auslastung (SNMP)	>80%	Mail	IT-Abteilung
			Netflow v9	vorerst rein informativ	-	-
		Werk 2 Switch Verwaltung 2	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung
			Temperatur (SNMP	>65°C	Mail	IT-Abteilung
			CPU-Auslastung (SNMP)	>80%	Mail	IT-Abteilung
		Werk 2 Switch Beschichtung	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung
			Temperatur (SNMP	>65°C	Mail	IT-Abteilung
			CPU-Auslastung (SNMP)	>80%	Mail	IT-Abteilung
		Werk 2 Switch Beschichtung Vertikal	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung
			Temperatur (SNMP)	>65°C	Mail	IT-Abteilung
			CPU-Auslastung (SNMP)	>80%	Mail	IT-Abteilung
		Werk 2 Switch Aluverarbeitung	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung
			Temperatur (SNMP)	>65°C	Mail	IT-Abteilung
			CPU-Auslastung (SNMP)	>80%	Mail	IT-Abteilung
		Werk 2 Switch Aufhänger	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung
			Temperatur (SNMP)	>65°C	Mail	IT-Abteilung
			CPU-Auslastung (SNMP)	>80%	Mail	IT-Abteilung
	Drucker	Werk 3 Logistik	Druckerübersicht (SNMP)	laut Sensorvoreinstellung	Mail	Christoph
		Werk 3 Produktionsleitung	Druckerübersicht (SNMP)	laut Sensorvoreinstellung	Mail	Christoph
		Werk 2 Produktuinsleitung	Druckerübersicht (SNMP)	laut Sensorvoreinstellung	Mail	Christoph
		Werk 2 Kasto	Druckerübersicht (SNMP)	laut Sensorvoreinstellung	Mail	Christoph
		Werk 2 Staplerbüro	Druckerübersicht (SNMP)	laut Sensorvoreinstellung	Mail	Christoph
		Werk 2 Verwaltung	Druckerübersicht (SNMP)	laut Sensorvoreinstellung	Mail	Christoph
		Werk 2 Beschichtung	Druckerübersicht (SNMP)	laut Sensorvoreinstellung	Mail	Christoph
		Werk 2 PUG	Druckerübersicht (SNMP)	laut Sensorvoreinstellung	Mail	Christoph
		Werk 2 PUV	Druckerübersicht (SNMP)	laut Sensorvoreinstellung	Mail	Christoph
		Werk 2 HD	Druckerübersicht (SNMP)	laut Sensorvoreinstellung	Mail	Christoph
		Werk 2 Folierer	Druckerübersicht (SNMP)	laut Sensorvoreinstellung	Mail	Christoph
		Werk 2 Produktionsbüro	Druckerübersicht (SNMP)	laut Sensorvoreinstellung	Mail	Christoph
		Werk 2 Alu	Druckerübersicht (SNMP)	laut Sensorvoreinstellung	Mail	Christoph
		Werk 2 Aufhänger PUV	Druckerübersicht (SNMP)	laut Sensorvoreinstellung	Mail	Christoph

Standort	Gruppe	Gerät	Sensor	Fehlergrenzwert	Alarmierungsart	Alarm an
Haag am Hausruck	USV	Werk 2 USV	Batteriekapazität (SNMP)	<60%	Mail	IT-Abteilung
			Überbrückungszeit (SNMP)	<60 Minuten	Mail	IT-Abteilung
			Eingangsspannung (SNMP)	<200 Volt	Mail	IT-Abteilung
			Auslastung (SNMP)	>75%	Mail	IT-Abteilung
		Werk 3 USV Serverraum	Batteriekapazität (SNMP)	<60%	Mail	IT-Abteilung
			Überbrückungszeit (SNMP)	<60 Minuten	Mail	IT-Abteilung
			Eingangsspannung (SNMP)	<200 Volt	Mail	IT-Abteilung
			Auslastung (SNMP)	>75%	Mail	IT-Abteilung
		Werk 3 Eaton	Batteriekapazität (SNMP)	<60%	Mail	IT-Abteilung
			Überbrückungszeit (SNMP)	<60 Minuten	Mail	IT-Abteilung
			Eingangsspannung (SNMP)	<200 Volt	Mail	IT-Abteilung
			Auslastung (SNMP)	>75%	Mail	IT-Abteilung
	Sensoren	Temperatur Serverraum	Temperaturwert (SNMP)	<15°C bzw. >30°C	Mail	IT-Abteilung
		Feuchtigkeit Serrverraum	Feuchtigkeitswert (SNMP)	<20% bzw. >60%	Mail	IT-Abteilung
		Klimaanlage 1	Störung (SNMP)	Wert=4	Mail	IT-Abteilung
			Betrieb (SNMP)	rein informativ (nur Warnung)	-	-
		Klimaanlage 2	Störung (SNMP)	Wert=4	Mail	IT-Abteilung
			Betrieb (SNMP)	rein informativ (nur Warnung)	-	-

Standort	Gruppe	Gerät	Sensor	Fehlergrenzwert	Alarmierungsart	Alarm an
Presov	Server	PREOSV-DC (Active Directory)	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung
			Festplattenspeicher C: und D: (WMI)	C: < 5GB; D:<10GB	Mail	IT-Abteilung
			Dienst Event Log (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Systemgesundheit (SNMP)	laut Sensorstandard	Mail	IT-Abteilung
			Festplattenstatus (SNMP)	laut Sensorstandard	Mail	IT-Abteilung
			Dienst DHCP Server (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			DNS Port 53 (WMI Port)	Port nicht erreichbar	Mail	IT-Abteilung
			Dienst DNS Server (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Dienst NTDS (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Dienst Druckerwarteschlange (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
		PRESOV-Storage (Dateiablage)	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung
			Festplattenspeicher C: und D: (WMI)	C: < 5GB; D:<15GB	Mail	IT-Abteilung
			Dienst Event Log (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Systemgesundheit (SNMP)	laut Sensorstandard	Mail	IT-Abteilung
			Festplattenstatus (SNMP)	laut Sensorstandard	Mail	IT-Abteilung
		PRESOV-BMD (Buchhaltung)	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung
			Festplattenspeicher C: (WMI)	C: < 5GB	Mail	IT-Abteilung
			Dienst Event Log (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Systemgesundheit (SNMP)	laut Sensorstandard	Mail	IT-Abteilung
			Festplattenstatus (SNMP)	laut Sensorstandard	Mail	IT-Abteilung
			Dienst BMDNtcsSvc (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Dienst BMDSrv: BMD Netspeed (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
		PRESOV-Exchange (Mail)	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung
			Festplattenspeicher C:, D: und E: (WMI)	C: < 5GB; D:<15GB; E:<1GB	Mail	IT-Abteilung
			Dienst Event Log (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Systemgesundheit (SNMP)	laut Sensorstandard	Mail	IT-Abteilung
			Festplattenstatus (SNMP)	laut Sensorstandard	Mail	IT-Abteilung
			SMTP Port 25 (WMI)	Port nicht erreichbar	Mail	IT-Abteilung
			Dienst Microsoft Exchange Inforamtionsserver (WMI Dienst)	Dienst läuft nicht	Mail	IT-Abteilung
			Exchange Datenbank (Powershell)	nicht verbunden	Mail	IT-Abteilung
	Firewall	MKW-Firewall	Verfügbarkeit (Ping)	nicht erfolgreich	Mail, SMS	IT-Abteilung

Selbstständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Literatur und Hilfsmittel angefertigt habe.

Stellen, die wörtlich oder sinngemäß aus Quellen entnommen wurden, sind als solche kenntlich gemacht.

Diese Arbeit wurde in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt.

Gaspoltshofen, den 10.07.2017

Ing. Christoph Voraberger