USU

White Paper

Und läuft und läuft und läuft – Automatisiertes Systems Management

Inhalt

Einleitung

Jeder kennt den Werbe-Slogan, der untrennbar mit dem Käfer verbunden ist: Er läuft und läuft und läuft. Unter der Haube garantierte in den 50er und 60er Jahren ein quasi „hochverfügbarer, ausfallsicherer“ Motor, dass das Fahrziel erreicht wurde Wirt-schaftsmotor unserer Zeit ist eine hochverfügbare, ausfallsichere IT. Und auch sie muss laufen. Ohne Störung. Jederzeit 24 × 7. Weltweit. Denn die darauf ausgerichteten wertschöpfenden Prozesse von Unternehmen dürfen nicht ins Stocken geraten. Dafür sorgt mit dem Systems Management eine Kern-Disziplin der IT, die seit Jahrzehnten ihresgleichen überwacht. System Management hat immer Konjunktur, wandelt sich aber im Zuge der immer heterogener und komplexer werdenden Infrastruktur bis hin zur automatisierten Überwachung von IoT-Devices, KI-gestützte Bewertungs-Cluster für Events oder Container-Monitoring.

Das vorliegende White Paper beschreibt im Einzelnen die Praxishürden, mit denen IT-Organisationen heute konfrontiert sind, Voraussetzungen und Anforderungen an eine „ideale“ Lösung sowie eine praxiserprobte Vorgehensweise zur Umsetzung. Neue Trends wie Systems Management für Cloud- bzw. Container-Applikationen oder IoT-Devices werden ebenso dargestellt wie wichtige Nachbardisziplinen, z. B. Capacity Monitoring bzw. Alarm Management, um durchgehende, weitestgehend automatisierte Überwachungsprozesse zu gewährleisten.

Warum ist Systems Management elementar?

Systems Management ist System- und damit Geschäftskritisch.

Durch die Reduktion der Prozess-Kosten, minimierte Ausfallzeiten oder geringere Ticketlaufzeiten gelingt eine Amortisation der Aufwände erfahrungsgemäß innerhalb von 18 Monaten.

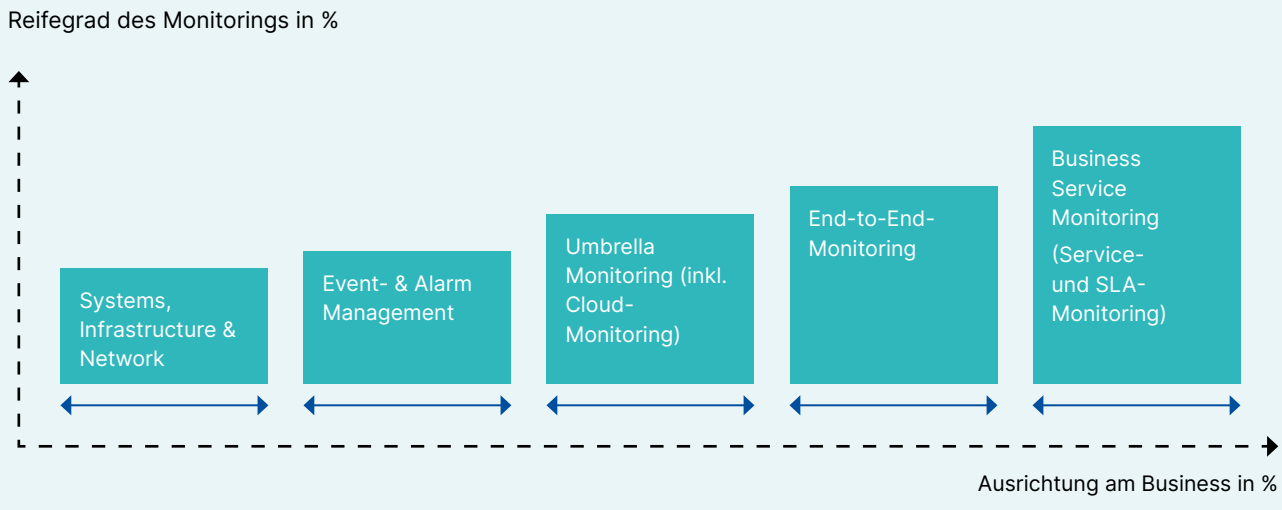
Eine effektive Systemverwaltung bzw. -steuerung war im Zeitalter überschaubarer physikalischer IT-Ressourcen vergleichsweise einfach und auch ohne Automatisierung gut zu realisieren. Angesichts einer heterogenen IT-Landschaft, vielfältiger Applikationen und virtueller Server bzw. Netzwerke ist dieses Ziel deutlich anspruchsvoller zu bewerkstelligen.

Ein modernes Systems Management unterstützt dabei, die gegenseitigen Beziehungen und Abhängigkeiten so zu definieren, dass ein effektives Zusammenwirken von Systemen und Anwendungen gewährleistet wird und über grafische Dashboards jederzeit relevante Event-Daten transparent verfügbar sind. Mit diesem Konzept können IT-Administratoren Automatisierungen einführen, mit deren Hilfe einfache Probleme schnell gelöst und bei Bedarf Fachleute alarmiert werden.

Darüber hinaus können sie Ressourcen verfolgen, kritische Situationen vorhersagen und vermeiden, kleinere Probleme schnell erkennen und beheben sowie nach schwerwiegenden Fehlern eine effektive Wiederherstellung durchführen. Die Implementierung einer zentralen und proaktiven Lösung rechnet sich.

Ein effektives Systems Management ist nicht zuletzt die Basis, um bei fortgeschrittenem Reifegrad ein ausgefeiltes Business Service Management zu realisieren.

Abb. 1: Reifegrad des Monitoring – Systems Management als Basis



Wichtige Aspekte bei der Umsetzung eines Systems Managements

Ausgangslage

In der Regel haben Unternehmen entweder eine Reihe von Produkt-bezogenen Monitoring-Lösungen, die parallel, aber isoliert voneinander Daten liefern, oder eine ältere Systems Management-Anwendung, die vom Hersteller nicht mehr weiterentwickelt wird. Auch freie Software, bei der individuelle Anpassungen, Pflege oder sonstige benötigte Services nur schwer erhältlich oder unverhältnismäßig teuer sind, können Gründe sein, eine neue zentrale Lösung zu implementieren, die physikalische, virtuelle und Cloud-Welten beherrscht.

Die Größe und Komplexität der IT-Infrastruktur variiert dabei erheblich. Die untere Grenze bilden etwa 200 Server, aber auch die Überwachung von über 30.000 Servern muss gewährleistet werden. Einer der wichtigsten Treiber ist zudem das Thema Automation, um den Betrieb und die Prozesskosten entsprechend zu reduzieren. Das setzt auch die Integration in die komplette Monitoring-Service-Kette voraus, also die nahtlose Anbindung an Nachbardisziplinen wie Capacity, Alarm Management oder Ticketing.

Abb. 2: Schwellwert-Übersicht

Kundenkommunikation als Erfolgsfaktor

Kunden sind in der Regel die Fachabteilungen innerhalb der IT, also z. B. das Datenbank- oder SAP-Team etc. Denn sie benötigen zielgerichtete aktuelle Daten, um den Betrieb, beispielsweise für Windows- oder Unix-Anwendungen, optimal sicherzustellen. Aus der Fachperspektive ist ein übergeordnetes Monitoring häufig nicht nötig – man hat ja sein individuelles Überwachungssystem. Und es gibt zudem häufig Ängste vor einer zu großen Transparenz. In der Praxis führt die Konstellation parallel laufender Inselsysteme allerdings dazu, dass sich die Ursachenfindung von Störungen in der Regel schwieriger und zeitraubender gestaltet, wenn man nicht weiß, ob der Fehler eher im Datenbank- oder Netzwerkbereich zu suchen ist. Die Störungsbehebung verzögert sich, da die einzelnen System-Administratoren zunächst ihre eigenen Ansichten überprüfen. Ein strukturierter, exakt definierter Prozess ist daher erfolgskritisch. Dazu gehört z. B. auch die Definition der Schwellwerte, z. B., dass bei einer CPU-Auslastung von 90 Prozent ein „Warning“ erfolgt und ab 95 Prozent ein Alarm.

Für die Definition der Schwellwerte sind im Detail die Fachabteilungen der IT verantwortlich. Ebenfalls muss mit ihnen die Diskussion geführt werden, welche Überwachungstiefe sinnvoll ist.

Diese variiert von Unternehmen zu Unternehmen teilweise deutlich. Um beispielsweise mögliche DoS (Denial of Service)-Attacken abzuwehren, muss man diverse einschlägige Prozessparameter in der Applikation aufwändig überwachen. Andere Organisationen benötigen dagegen lediglich ein oberflächliches Basis-Monitoring mit längeren Messungszyklen ihrer physikalischen Server.

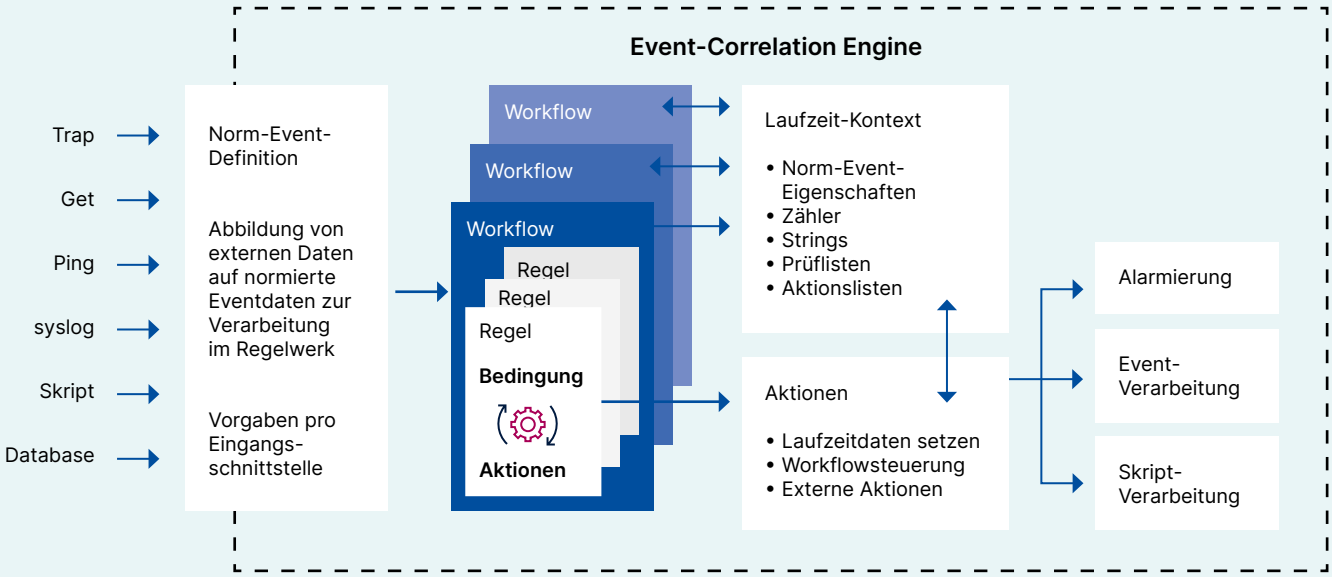
Für ein effektives Systems Management ist der aktive Dialog mit den IT-Fachabteilungen ein Erfolgs-Schlüssel. Es hat sich bewährt, diese aktiv in den Auswahlprozess mit einzubeziehen, deren Anforderungen aufzunehmen, die Mehrwerte für deren tägliche Arbeit darzustellen und auch die Umsetzung im Team zusammen durchzuführen.

Das Erstellen der Eventstruktur und die Verarbeitung der Events sind elementare orbereitungsschritte: Welche Quelle wird für die Eventstruktur genutzt, welche Informationen werden aus Meldungen herausgefiltert, wie sehen die Regeln aus, um Mehrfach-Events bzw. wichtige oder unwichtige Vorfälle zu erkennen etc.

Projektmeilensteine

Ein Kick-off-Meeting behandelt zu Beginn die grundsätzlichen Fragen zu den Projektzielen, zur Organisation, den Aufgaben und Rollen bzw. dem Projektrahmen, wie sie bereits oben teilweise skizziert wurden. Die sich anschließende Konzeptionsphase analysiert zunächst vor allem die bestehende Systemlandschaft. Dabei wird beispielsweise definiert, welche Systeme direkt überwacht werden sollen und wie die einzelnen Komponenten zu überwachen sind. Bezüglich der Schnittstellen wird z. B. festgelegt, welche Informationen die Zuliefersysteme senden und wie das Meldungsformat bzw. der Inhalt aussehen soll.

Abb. 3: Integration der EventKorrelation



Das oben bereits angesprochene Ziel der Automatisierung gilt es zunächst einmal für die Inventarisierung von Servern, virtuellen Systemen sowie Netzwerk-Komponenten umzusetzen. Ist im Unternehmen noch keine CMDB vorhanden, werden die Konfigurationselemente im Systems Management-Tool selbst integriert, verwaltet und in Relationen zu einander gesetzt. Eine umfangreiche Automation des Regelwerks ist erforderlich. Diese Informationen sollten zusätzlich für ein eventuell in der Zukunft anstehendes CMDB-Projekt exportiert und zur initialen Befüllung genutzt werden können.

Dutzende von Plugins, z. B. für die RAM-, Logfile- oder CPU-Kontrolle, sorgen für diese Standardüberwachung, können aber im Bedarfsfall leicht auf individuelle Kundenwünsche angepasst werden.

Zur automatischen „Betankung", also Konfiguration, werden eine Reihe vordefinierter „Best practice-Templates" eingesetzt. In der Praxis sind dies oftmals deutlich mehr als hundert. Diese gewährleisten die Überwachung mit den relevanten Parametern oftmals innerhalb von Sekunden.

Im Zuge der Umsetzung hat es sich außerdem bewährt, die Teilnehmer und Nutzer bereits frühzeitig am neuen System zu schulen und damit die realen Möglichkeiten des Systems kennenzulernen. Die Hilfe zur Selbsthilfe kann ein wichtiges Konzept sein und führt dazu, dass die Administratoren des Kunden das System autark weiterentwickeln können.

Best Practice-Templates – Auszug für Applikations-Monitoring

- Webserver
- Web Application Server
- Java-Überwachung
- E-Mail-Server
- Datenbank-Server
- Virtualisierungs-Management
- Microsoft-Server-Produkte
- Basis-Server-Dienste
- Authentifizierung

Neue Herausforderungen: Cloud, Container, KI

Galt es vor Jahren noch, einfache Client-Server-Strukturen zu überwachen, stellt vor allem das Konzept der Cloud heute das effektive Systemmanagement moderner hybrider IT-Umgebungen vor neue Herausforderungen. Die Anbindung von Cloud-Anwendungen in den Monitoring-Zyklus mit Hilfe von Cloud-Connectoren muss anhand der richtigen Parameter automatisiert und rasch erfolgen. Hierbei unterstützen Best-Practice-Templates mit den spezifischen Überwachungsmetriken, so dass neue Cloud-Komponenten innerhalb kürzester Zeit überwacht werden können. Eine weitere Schwierigkeit besteht in der Überwachung agiler Workloads, wenn grundlegende Infrastruktur-Komponenten wie Rechenleistung, Storage oder Netzwerkkapazitäten dynamisch skalieren. Ein entsprechendes System muss in der Lage sein, kurzfristig und automatisiert z. B. 30 neue Webserver zu überwachen.[1]

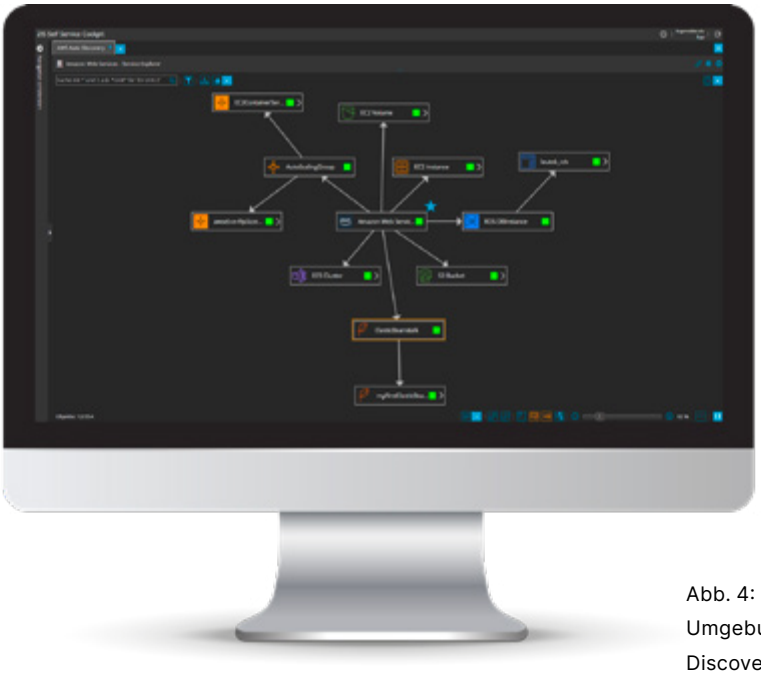


Abb. 4: Beispiel einer Kubernetes Umgebung mit automatischem Discovery

Docker-Monitoring ist eine der wesentlichen Anforderungen für die effiziente Überwachung einer „containerisierten Welt“. Mit Containeranwendungen, Microservices und dynamischen Infrastrukturen investieren Unternehmen in ihre Effektivität. Dieser Ansatz hat sehr viele Vorteile, in einer Microservices-Architektur kann es aber auch eine besondere Herausforderung darstellen, die genaue Ursache von Fehlern oder Leistungsengpässen zu ermitteln. Microservices sind in der Regel in Containern verpackt. Daher müssen Unternehmen Monitoring-Metriken nicht nur auf der VM-Ebene, sondern auch auf der Containerebene sammeln. Dies kann beispielsweise mit der Kubernetes-Technologie erfolgen, die Statistiken zu CPU, Arbeitsspeicher, Dateisystem und Netzwerkressourcen jedes Containers sammelt.[2]

[1] Vgl. U. Ostler, 6 große Trends im IT-Monitoring, https://www.datacenter-insider.de/6-grosse-trends-im-it-monitoring-a-638100/
[2] Vgl. P. Münch / C. Puppe, Docker-Container und -Hosts überwachen, iX 5/2017, S. 78 ff.

Künstliche Intelligenz steckt im Monitoring noch in den Kinderschuhen. Aber angesichts riesiger Datenvolumina im IoT-Zeitalter wächst der Bedarf, z. B. für die Analyse und Korrelation von großen Logfiles. Ziel ist es, sich anbahnende Störungen möglichst bereits per Früherkennung zu bemerken und zu beheben.[3] Klassische Monitoring-Ansätze auf Basis von Mittel- und Schwellwerten müssen dafür verfeinert werden. Ein Beispiel ist die automatische Schwellwertfindung und Extrapolation. Eine Systems Management-Lösung würde hierfür historische Daten zur Festlegung von Schwellwerten auswerten, diese zyklisch und dynamisch anpassen oder über Machine-Learning-Funktionen den Input von Fachleuten für die automatische Erkennung von Anomalien verwenden. Ein weiteres Einsatzszenario ist die komfortable Analyse auf Basis von Timeline-Korrelationen. Funktionen hierfür erkennen Event- und Metrikmuster anhand historischer Daten und unterstützen durch eine grafische Darstellung der Datenströme oder der Häufigkeiten und Zusammenhänge von Events auf Service- bzw. Applikations-Ebene.

Was eine ideale Lösung leisten sollte

Voraussetzung für ein effizient funktionierendes Systems Management ist die Integrationsfähigkeit des Systems, auch zu weiteren Teildisziplinen wie z. B. Capacity Management, so dass die komplette Prozesskette abgedeckt ist. Vielfältige Schnittstellen bilden die Basis und stellen den Sammelpunkt für unterschiedlichste Daten dar. Die Anwendung liefert Systemadministratoren und IT-Verantwortlichen in Echtzeit alle Daten, um physikalische und virtuelle Ressourcen sowie Cloud-Applikationen und damit eine hybride, heterogene Infrastruktur optimal überwachen zu können. Die zu messenden Parameter sind vielfältig, z. B. Temperatur, Lüfterdrehzahl, Speicherbelegung, Speicherverfügbarkeit etc. Ausgewertet wird das gesamte Spektrum physikalischer, prozessualer und anwendungsbezogener Daten, die über mandantenfähige Dashboards aggregiert und zentral dargestellt werden können. Zusätzliche Alarmierungsfunktionen sorgen im Störungsfall für eine automatisierte Fehlerbehebung.

Abb. 5: Überblick: Automatische „Betankung“ & Überwachung der Server-Systeme mit „Best Practice-Templates“ durch die Systems Management-Plattform

[3] Cf. S. Greiner, Das Monitoring lernt selbst. KI in Überwachungsszenarien, https://www.heise.de/developer/artikel/Das-Monitoring-lernt-selbst-KI-in-Ueberwachungsszenarien-4029666.html

Typische Praxis-Anforderungen

Best-Practices für proaktive Überwachung

- Sämtliche IT-Ressourcen (Server, Netzwerk, Applikationen) werden durch vordefinierte praxiserprobte Templates und Plug-Ins sehr rasch und standardmäßig überwacht

Leistungsfähige Event-Korrelation

- Logische Gewichtung und Verknüpfung von Daten zu aussagekräftigen Zuständen für die Bewertung, Korrelation und Aggregation von Ereignissen aus den unterschiedlichsten Systemen

Automation

- Rascher Produktivstart & geringer Betriebsaufwand
- Automatisiertes Update der Assets / Incident-/ Change-/ Knowledge Base-Koppelung gemäß ITIL®-Standard/ Restart-Möglichkeit von Prozessen etc.
- Automatisches Patch-Management etc.

Umfangreiche & schnelle Analysemöglichkeiten

- Einfache individuelle Self-Service-Analysen
- Ad-hoc Zoom-In bis ins Detail
- Simulation von Wartungsszenarien

Rollenbasierte Dashboards

- Mandanten-fähige, Web-fähige und verständliche Cockpit-Sichten für Operating, Help-Desk, Management, Kunden…
- Individuelle Self-Service-Dashboards
- Flexibel erweiterbar (z. B. Performancedaten verknüpfbar) und teil- bzw. speicherbar

Integriertes Alarm- & Lösungsmanagement

- Alarmpläne, Alarmgruppen, Eskalationsmanagement, Alarmkalender, Alarmregionen
- Diverse Kanäle: SMS, E-Mail, VOIP, App etc.
- Ticket und Change-Informationen
- Handlungsanweisungen durch Kopplung mit Lösungsdatenbank

Service & Support

- Updatefähigkeit des Systems
- Autarke kundenseitige Weiterentwicklung wird unterstützt
- Qualitätssicherung von Templates bzw. Plug-Ins

In der Praxis liegt der Aufwand bei der händischen Implementierung und Pflege von Open Source-Lösungen oftmals beim Doppelten bis Dreifachen gegenüber professionellen proprietären Standard-Tools, die eine automatisierte Implementierung und einen automatisierten Betrieb erlauben.

Auf den ersten Blick gibt es eine ganze Reihe von Open-Source-Monitoring-Lösungen, die eine Vielzahl von Features haben und unterschiedlichste Bereiche abdecken. Betrachtet man jedoch die Erfahrungen mit dem Handling und den Gesamt- und Folgekosten in komplexeren IT-Umgebungen, schwinden die Vorteile der zunächst vergleichsweise günstig erscheinenden Lösungen.

Integrations- und Mandantenfähigkeit, umfangreiche Eventkorrelation, Benutzer-Rollen-Konzepte und Revisionssicherheit sind weitere Aspekte, bei denen Open-Source-Tools an ihre Grenzen stoßen. Auch der After-Sales-Service ist eine wichtige Komponente – denn nach der Implementierung ist vor der Implementierung.

Mehrwert Alarmierung

Alarm-Funktionen sind ein wichtiger Teil des Systems Management. Viele Unternehmen verfügen über mehrere Alarmierungs-Tools, die – oft isoliert voneinander – nur für bestimmte Infrastrukturkomponenten zuständig sind. Ein zentrales und integriertes Alarmmanagement ist daher ein wesentlicher Erfolgsfaktor, um im Ernstfall eine schnelle und zielgerichtete Problembehebung zu gewährleisten. Eskalationsmechanismen, das Follow-the-Sun-Prinzip zur Optimierung der weltweiten Bereitschaftskosten oder einheitliche Handlungsanweisungen in einer intelligenten Lösungsdatenbank sind nur einige wichtige Funktionen. Im Einzelnen bietet ein State-of-The-Art-System zur Alarmierung folgende Möglichkeiten:

- Mandantenfähige Dashboards für eine zentrale Sicht auf alle aktiven Alarme
- Priorisierung der Alarme durch verschiedene Severities
- Alarm-Reduktion durch frei konfigurierbare Alarmfilter zur Erstellung von anwenderspezifischen Views
- Unterdrückung gleichartiger Alarme innerhalb definierbarer Zeiträume
- Maßgeschneiderte Alarmierung der jeweils zuständigen Bereitschaft durch Kombination von unterschiedlichen Alarmmedien (Voice Call mit Text to Speech, SMS, E-Mail, GSM, Voice over IP, App etc), abhängig von Uhrzeit und Dringlichkeit
- Gleichzeitige Übertragung von Alarmen an einen Empfänger oder an Gruppen, abhängig vom Alarm
- Absicherung der Alarmierung durch Eskalationsstufen innerhalb einer Bereitschaft, indem in definierbaren zeitlichen Abständen mehrere Personen alarmiert werden, sofern der Alarm nicht quittiert wird
- Hinterlegung von Alarmplänen
- Moderne Web-Oberfläche für eine einfache und schnelle Bereitschaftsplanung

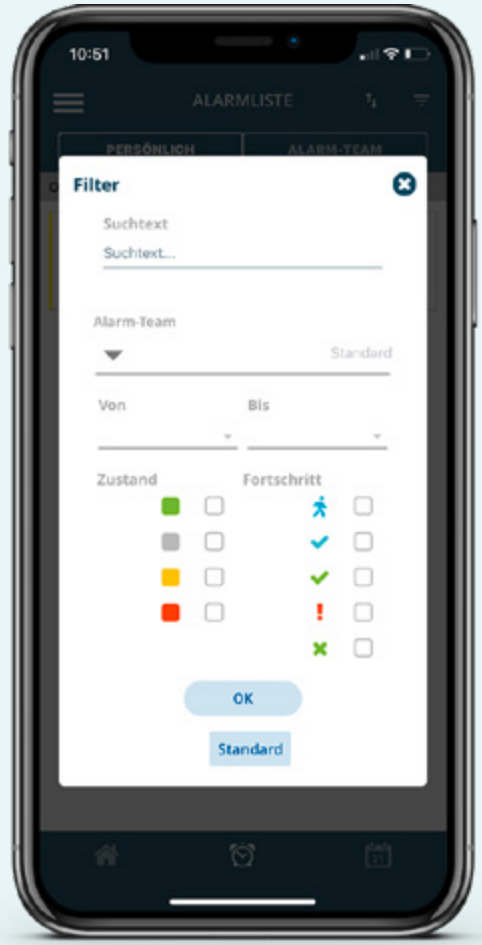


Abb. 6: Alarmierung via App

Mehrwert Capacity Management

Über das reine Systems Management hinaus stellt das Capacity oder Performance Monitoring sicher, dass die vorgehaltenen IT-Kapazitäten den aktuellen und künftigen Anforderungen gerecht werden. Ein integrierter „Überwachungsschirm“ über alle Performancedaten ermöglicht deren Zusammenführung und Verdichtung in einer einheitlichen Struktur und Sichtweise. Einerseits lassen sich die Kapazitäten bestimmter, für Services, Systeme und Applikationen benötigter Ressourcen bzw. Komponenten messen, andererseits erlauben automatisierte Datenanalysen und das Einbeziehen von Vergangenheits-Werten die Priorisierung, Optimierung und Planung von Kapazitäten auf Basis von Prognosen und Trends. Übersichtliche Dashboards für verschiedene Rollen, z. B. Service Owner, Fachabteilungen, Leitstände oder Management, liefern die jeweils benötigte Information auf einen Blick. Und bei drohenden Kapazitätsengpässen oder sonstigen konkreten Problemen greift das Alarmmanagement. So hält man die Balance zwischen Wirtschaftlichkeit und Leistungsfähigkeit – auch beim bedarfsgerechten Einkauf von externen Kapazitäten.

Abb. 7: Dashboard-Übersicht über zentrale Performance-Daten

Fazit

Ein zentrales Systems Management arbeitet zwar hinter den „Systemkulissen“, ist aber dennoch „System-relevant“, denn es sorgt dafür, dass die Geschäfts-kritische IT läuft. Hochverfügbar und ausfallsicher. Allerdings zwingt die Überwachung neuer Technologien bzw. Trends wie Cloud, Container oder Mobile bzw. IoT-Devices Organisationen dazu, ihre IT-Monitoring-Strategien neu auszurichten. Der digitale Wandel in den Unternehmen erfordert zunehmend eine neue Generation von Systems Management-Lösungen, welche in der Lage sind, die komplexen und heterogenen Infrastrukturen flexibel, aktiv und weitestgehend automatisiert zu überwachen.

Neben der Technik ist die Projektbegleitung von Spezialisten erfolgskritisch, um eine praxisnahe Umsetzung und den Know-how Transfer für eine zukünftig eigenständige Administration zu gewährleisten. Der aktive Dialog mit den Fachabteilungen der IT ist ein zentraler Erfolgsfaktor, um Schwellwerte praxistauglich zu definieren und ein leistungsfähiges Event-Korrelations-Konzept zu erarbeiten. Wenn Mensch und Maschine gut harmonieren, amortisieren sich die Gesamtaufwände für Systems Management innerhalb sehr kurzer Zeit – denn die Betriebs- und Systembetreuungskosten sinken, und das Risiko von Systemausfällen und Compliance-Verletzungen wird minimiert.

Der Autor

Steffen Kircher ist seit 2005 bei der USU. Als PreSales Consultant im Bereich Vertrieb berät er Interessenten und Kunden mit technischem Know How und seiner langjährigen Erfahrung. Er kennt die Lösung USU IT Monitoring wie kaum ein anderer.

Über USU

USU setzt mit seinen Softwarelösungen für IT & Customer Service Management Maßstäbe für eine bessere Servicewelt. Im deutschsprachigen Raum ist USU einer der führenden Hersteller von IT-Monitoring-Lösungen.

Das Leistungsspektrum im Bereich IT Monitoring umfasst die gesamte Entwicklung und Implementierung der Monitoring-Lösung, den Know-how-Transfer in die jeweiligen IT-Abteilungen sowie Support und Wartung der Software. Aufgrund der langjährigen Erfahrung ist USU in der Lage, individuelle Kundenanforderungen zu berücksichtigen und maßgefertigte Lösungen anzubieten.