USU

E-Book

Von Daten zu Entscheidungen

Wie das Event Management in der IT-Strategie zum Erfolgsfaktor wird

Einleitung

In der heutigen schnelllebigen digitalen Welt ist es für eine ganzheitliche Überwachung der IT-Infrastruktur und der darauf laufenden IT- und Business-Services unverzichtbar, auf eine Vielfalt an modernen Informationsquellen zurückzugreifen.

Jede dieser Quellen generiert eine Fülle von Daten, die Veränderungen in der Infrastruktur als Events abbilden. Im täglichen IT-Betrieb generiert sich ein kontinuierlicher Strom von Ereignissen (Events), die effektiv nur durch ein automatisiertes Event Management-System analysiert und gehandhabt werden können.

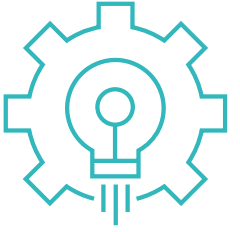
Das Ziel ist es, im Datenstrom echte Warnsignale frühzeitig und zuverlässig zu erkennen und somit durch proaktive, korrigierende Maßnahmen Probleme im IT-Betrieb zu verhindern.

Herzstück Correlation Engine

Die Event Correlation Engine, ist der zentrale Bestandteil des Event Managements und für das Erkennen von echten Warnsignalen zuständig.

Über verschiedene Schnittstellen werden zunächst Infrastruktur-Events aus existierenden Quellen wie Infrastruktur-Monitoring-Software, Systems-Management-Lösungen, Applikations-Logs und Netzwerk-Komponenten gesammelt. Um einen effizienten Abgleich und eine gründliche Überprüfung dieser Events zu ermöglichen, erfolgt als erster Schritt deren Standardisierung.

Eine weitere entscheidende Informationsquelle stellt die Configuration Management Database (CMDB) dar. Diese beinhaltet detaillierte Informationen über die Service-Topologie, also die Struktur und technischen Abhängigkeiten der an einem Business Service beteiligten technischen Komponenten. Darüber hinaus enthält die CMDB die für einen Business Service relevanten Service Level Agreements (SLAs), die wichtige Leistungsparameter wie Verfügbarkeit und Antwortzeiten definieren. Von Bedeutung ist auch der Change-Kalender, der Auskunft über geplante Wartungszeiträume für die verschiedenen Services und Komponenten gibt.



Event Correlation – Das Herzstück des USU Event Managements

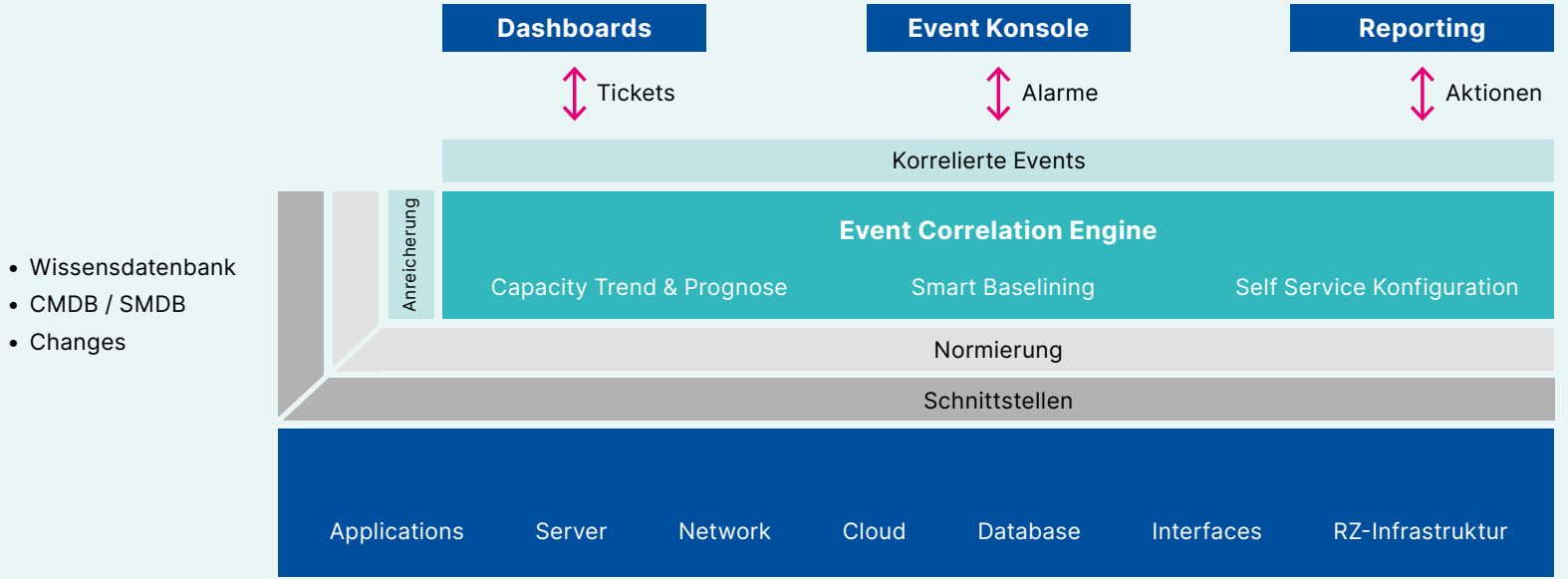


Abb. 1: Event Management

Entscheidungssicherheit in komplexen IT-Umgebungen

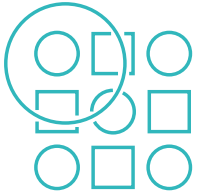
Da sämtliche Informationen über den Zustand der IT in einer standardisierten und damit nutzbaren Form in die Engine einfließen und zugleich alle Bewertungskriterien und Workflows vorhanden sind, kann sie Events zuverlässig korrelieren. Das geschieht, indem die Engine Zusammenhänge zwischen verschiedenen Events identifiziert, diese mit bestehendem Wissen abgleicht und beispielsweise das Überschreiten von definierten Schwellwerten erkennt.

Darüber hinaus verarbeitet die Engine kontinuierlich die eingehenden Daten, wodurch sie stetig verbesserte Ergebnisse liefert: Nahezu alle drohenden Störungen werden erkannt und es werden gezielt jene Maßnahmen ergriffen, die sowohl notwendig als auch angemessen sind. Diese grundlegende Funktion allein beschleunigt die Abläufe im IT-Service-Management erheblich und entlastet gleichzeitig die Ressourcen der Mitarbeitenden.

Es gibt keine starren Regeln

Die Event Correlation Engine wertet die standardisierten Infrastruktur-Events in Echtzeit aus. Dabei erkennt sie verschiedene Arten von Korrelationen, darunter Typ, Zeit und Topologie. Sie verfügt über eine umfassende Palette von Analysetools und kennt sowohl physische als auch logische Topologien bis hin zur Geräteebene.

Weisen Events eines Typs in einem kurzen Zeitintervall identische Anomalien auf, betrachtet die Engine diese als auffällig. Ebenso wird auffälliges Verhalten erkannt, wenn Events eine topologische Verbindung aufweisen: Fallen sowohl ein Switch als auch ein Service, der über diesen Server läuft, aus und hat der Server keine Netzwerkverbindung, identifiziert das System diese Events als eine einzige Störung.



Die Reaktion der Event Correlation Engine hängt von einer Vielzahl von Faktoren ab

- Ein Alarm wird erst ausgelöst, wenn eine Auffälligkeit in einer bestimmten Häufigkeit auftritt.
- Ist lediglich einer von mehreren Netzwerk-Routern außer Betrieb, wird die Störung in der Regel weniger dringlich behandelt.
- Fällt ein Business Service aus, richtet sich die Reaktion nach den Service Level Agreements (SLAs): Wenn eine Anwendung innerhalb der garantierten Zeiten nicht erreichbar ist, fordert das System eine schnelle Reaktion.

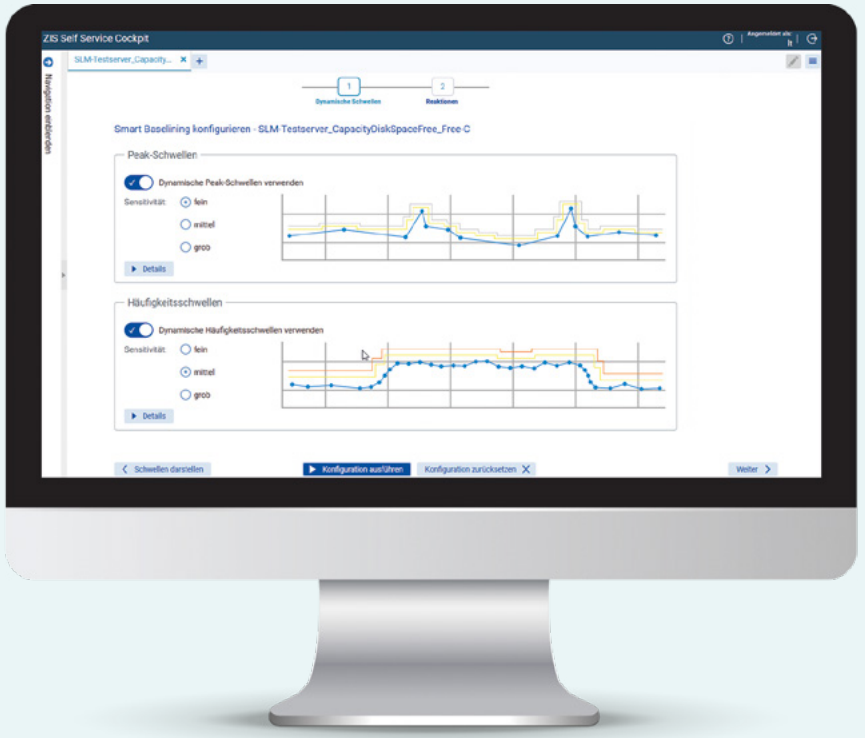
Die Correlation Engine wird im Laufe der Zeit immer besser, indem sie gelernte Event-Korrelationen und Reaktionen anwendet und ihre Art der Reaktion auf Event-Korrelationen kontinuierlich anpasst. In komplexen und dynamischen IT-Landschaften ist diese Vorgehensweise besser geeignet als die Verwendung eines starren Regelkatalogs, der die Realität in IT- und Fachabteilungen nur begrenzt und punktuell erfasst.

Capacity-Trend-Alarme

Die Engine ist in der Lage, Kapazitäten und deren Auslastung präzise zu prognostizieren und somit frühzeitig Warnungen auszugeben sowie Engpässe vorausschauend zu identifizieren. Dazu greift die Engine auf Messdaten von Services und Systemen zurück und erstellt eine ganzheitliche Übersicht über die benötigten Ressourcen und Komponenten. Sollten die bestehenden IT-Kapazitäten nicht ausreichen, können automatisierte Workflows zur Skalierung der Infrastruktur aktiviert werden. Durch automatisierte Datenanalysen und die Analyse von historischen Daten wird es außerdem ermöglicht, Kapazitäten auf Grundlage von Prognosen und Trends zu planen, zu priorisieren und zu optimieren.

USU Capacity Management

USU Smart Baselining



Smart Baselining

In der Vergangenheit war das IT- und Service-Monitoring auf starre Schwellenwerte angewiesen. Heutzutage passen sich diese Schwellenwerte dank KI-gesteuerter Technologien in Kombination mit Observability dynamisch an. Die Event Correlation Engine lernt, wie verschiedene Anwendungen auf Lastspitzen reagieren und was als normaler Verlauf gilt. Dadurch werden manuelle Konfigurationen überflüssig werden. Selbst die generelle Festlegung von Schwellenwerten, Regeln und Standardwerten ist nicht mehr zwingend erforderlich. Aktuelle Schätzungen zeigen, dass die automatische Anpassung von Schwellenwerten in Verbindung mit Observability die Anzahl der Alarme um bis zu 90 Prozent reduzieren kann, wobei aussagekräftige Anomalien in weniger als einer Minute erkannt werden.

Self Service Cockpit

Die Informationen, die von der Correlation Engine bereitgestellt werden, sind nicht ausschließlich im Alarmfall relevant. Wenn ein Service Owner Informationen über den aktuellen Zustand seines Business Services benötigt, kann er dies eigenständig über ein Self Service Cockpit tun, ohne auf die Expertise eines Monitoring-Spezialisten angewiesen zu sein.

Erfolgsfaktor: KI in Kombination mit Observability

Diese Anwendungen repräsentieren einen grundlegenden Paradigmenwechsel. Events werden nicht länger mit vorgegebenen Regeln und Normen abgeglichen, sondern tragen selbst dazu bei, die Kriterien zu definieren, an denen sie gemessen werden. So entsteht ein dynamisches Monitoring, das den immer komplexer werdenden IT-Landschaften gerecht wird. Diese Herangehensweise ermöglicht es, den Aufwand im IT Service Management zu reduzieren und zugleich die Ausfallsicherheit zu maximieren. Durch den Einsatz intelligenter Korrelationen, unterstützt durch Observability, setzt KI dem Event-Rauschen und der damit verbundenen Alarmmüdigkeit wirksam ein Ende. Obwohl KI-basierte Event-Korrelation noch in den Anfängen steht und ihr volles Potenzial noch nicht ausgeschöpft ist, ist es ratsam, frühzeitig Erfahrungen mit diesen neuen Technologien in Verbindung mit Observability zu sammeln, um langfristig die Aufwände im IT Service Management nachhaltig zu reduzieren.

Vorteile einer zentralen Event- und Service-Korrelation

Konsolidierte Alarme und Tickets

Durch die Filterung von Events durch die Correlation Engine werden die Mitarbeitenden nur über den relevanten Teil informiert, bei dem ihr Eingreifen erforderlich ist. Dabei erfolgt für jeden Störfall nur eine einzige Benachrichtigung, unabhängig von der Anzahl der in die Korrelation eingeflossenen Events. Tickets werden lediglich einmal erstellt, selbst wenn der Handlungsbedarf in verschiedenen Kontexten besteht, und sie werden automatisch nach Priorität sortiert. Diese Vorgehensweise führt zu einer erheblichen Entlastung des IT-Service-Desks.

Der Gesamtzustand im Überblick

Ein wesentlicher Vorteil der Event-Korrelation besteht darin, dass sie den Gesamtzustand der IT in einer einheitlichen Struktur und Sichtweise darstellt (siehe Abbildung 2). Durch Dashboards und Event-Konsolen, die speziell für verschiedene Rollen wie Service Owner, Fachabteilungen, Leitstände und das Management entwickelt wurden, erhalten die Beteiligten die benötigten Informationen auf einen Blick. Dies ermöglicht den Mitarbeitenden, Engpässe frühzeitig zu identifizieren und zusätzliche Kapazitäten bedarfsgerecht und wirtschaftlich zu beschaffen, ohne auf das integrierte Alarm- und Ticketmanagement angewiesen zu sein. Darüber hinaus haben sie die Möglichkeit, Berichte auf Grundlage der korrelierten Events zu erstellen, etwa zu der Performance bestimmter Services oder der Auslastung vorgehaltener Ressourcen.

Wirtschaftlicher IT-Betrieb

Eine zentrale Event- und Service-Korrelation erhöht die Wirtschaftlichkeit des IT-Betriebs:

- Da die Aufwände im IT Service Management, werden weniger Ressourcen für einen sicheren IT-Betrieb benötigt.
- Die Auswertungen der Event-Korrelationen decken Optimierungspotenziale im IT-Betrieb auf. Die Effizienz steigt.
- Die Mitarbeitenden greifen für Reportings und Performance-Analysen auf die konsolidierten Darstellungen aus der Event Correlation Engine zu. Das steigert die Produktivität.
- Die Mean Time To Repair (MTTR) sinkt und damit auch die Dauer von Ausfällen, die den Umsatz senken, wie etwa Downtimes von Webshops.

Fazit

Menschen nutzen Fehler, um daraus zu lernen. Mit KI gelingt das der IT ebenfalls. Korrelierte Events zeigen Optimierungspotenzial auf und verfeinern die Planung von Kapazitäten. Eine deutlich verringerte Anzahl an Tickets und Alarmen schafft darüber hinaus Freiräume im IT Service Management, um Prozesse und Komponenten zu verbessern. Es lohnt sich daher, das Servicemanagement mit einem Next Generation Monitoring auf eine neue Ebene zu heben.

Über USU

USU ist Deutschlands Nr. 1 für IT-Monitoring-Lösungen. Das umfangreiches Leistungsspektrum im Bereich IT Monitoring erstreckt sich über die gesamte Entwicklung und Implementierung von Monitoring-Lösungen, den Know-how-Transfer in die jeweiligen IT-Abteilungen sowie den erstklassigen Support und die zuverlässige Wartung der Software. Mit einer unübertroffenen Expertise und einer langjährigen Erfolgsgeschichte ist die USU in der Lage, auch individuelle Kundenanforderungen zu berücksichtigen und maßgeschneiderte Lösungen anzubieten.

Kontaktieren Sie uns, um mehr über das **Event Management** zu erfahren.

Melisa Mujic
ITM Community Developer USU Solution IT Monitoring

Jetzt einen Termin vereinbaren.