



IT-MONITORING MITTELS ADAPTIVER SCHWELLWERTE / SMART BASELINING

Beim Monitoring komplexer IT-Infrastruktur werden viele Messgrößen erfasst und ausgewertet. Die Überwachung geschieht dabei meist mittels statischer Schwellwerte. Ein Über- oder Unterschreiten führt automatisch zur Benachrichtigung der zuständigen Administratoren, die dann in einer nachfolgenden Analyse feststellen, ob tatsächlich ein Problem vorliegt, das abstellende Maßnahmen erfordert. Mithilfe des regelmäßigen Monitorings mittels dynamischer Schwellwertanpassung können echte Störungen frühzeitig erkannt und behoben werden.

FÜR FOLGENDE HERAUSFORDERUNGEN

- Zielgerichtete Alarmierung
- Schnellere Reaktionen auf Anomalitäten
- Vermeidung von Fehlalarmen
- Höhere Service-Verfügbarkeit und weniger SLA-Verletzungen

DER ANWENDUNGSFALL

Der erste Punkt beim Monitoring ist die kontinuierliche Erfassung und Speicherung vielfältiger Messdaten (zum Beispiel Performance-daten, Daten aus Log-Einträgen, Speicherauslastung, CPU-Verbrauch, Festplattenkapazität und so weiter).

Des Weiteren werden für ein umfassendes Monitoring, neben der Visualisierung, fixe Schwellwerte definiert, um die IT-Infrastruktur effektiver überwachen zu können. Die richtige Festlegung der Schwellwerte ist hierbei von großer Bedeutung.

Werden diese Schwellwerte zu weit gefasst, bleiben möglicherweise Probleme unerkannt, die später eine Verletzung des Service Level Agreements (SLA) oder einen Serviceausfall verursachen können. Werden dagegen die Schwellwerte zu eng gesetzt, führt dies zu vielen Alarmen beziehungsweise zu manuellen Analysen, bei denen häufig festgestellt wird, dass gar keine Probleme vorliegen.

DIE LÖSUNG IM DETAIL

Die Entwicklung eines statistischen Modells zur Anomalie-Erkennung mittels dynamischer Schwellwerte greift hier diese Problematik der festen Schwellwerte direkt an.

Die Messdaten werden auch hier kontinuierlich erfasst und in einem weiteren Schritt aufbereitet und gespeichert. Hierbei werden fehlerhafte oder unvollständige Messreihen verworfen.

In dem statistischen Modell werden dann die Daten in einem rollierenden Zeitfenster mit Messungen aus der Vergangenheit verglichen. Nur bei Mustern, die in der Vergangenheit mit einer Problemsituation korrelierten, wird ein Alarm ausgelöst. Dies führt zu optimierten, verbesserten Alarmen.

Das Training der Mustererkennung findet hierbei auf Basis historischer Daten fortlaufend statt.

STATUS IM PROJEKT

Das Modell befindet sich in der Entwicklung und wird später kommerziell verfügbar sein.

VORAUSSETZUNGEN

- Der Service erfordert ein trainiertes Modell, hierfür müssen historische Daten existieren.
- Es ist kein Spezialwissen über den zu erfassenden Messwert notwendig.

VERFÜGBARKEIT

Auf Anfrage.



SPEZIFIKATION

	Inputdaten	Preprocessing	Datenspeicher	Algorithmen	Interfaces
High-Level-Beschreibung	E2E-Messungen, Messung der Server- und Netzwerk-Performance, Daten aus Log-Einträgen, Speicher, CPU-Verbrauch, Festplattenkapazität	Sanity Check	NAS-Speicher, Datenbanken	Anomalie-Erkennung	Monitoring / Dashboard / Alarme
Konfigurierbarkeit	Auswahl der Messgrößen			Trainingszeitraum, Empfindlichkeit	Plot-Auswahl bzw. Darstellung des Dashboards
Technische Umsetzung	Messungen vor Ort	Python, Docker Container	Filesystem, DBs, Docker Container	Python, Docker Container	REST-API
Spezifisches Beispiel aus dem Schnellboot	Die Messdaten werden kontinuierlich erfasst	Die Daten werden aufbereitet, Verwerfen fehlerhafter oder unvollständiger Messreihen	Das Training der Mustererkennung auf Basis historischer Daten findet fortlaufend statt	Rollierende Zeitfenster werden mit Messungen aus der Vergangenheit verglichen. Nur bei Mustern, die in der Vergangenheit mit einer Problemsituation korrelierten, wird ein Alarm ausgelöst.	Möglichkeit des regelmäßigen Monitorings mittels dynamischer Schwellwertanpassung, somit können echte Störungen frühzeitig erkannt werden

