New
Also Available
in English

Autonome IT Dienstleistungen

Ein kurzer Überblick über den aktuellen Stand der Technik

Volume 3, Nr. 6

Februar 2022

Michael Leyer Universität Rostock

Florian Bär Accenture GmbH

Layout & Design: Christopher Rothhardt

White Paper Serie des Lehrstuhls ABWL: Service Operations
Volume 3

In den letzten Jahren hat sich die Art und Weise, wie Unternehmen IT-Dienste betreiben, stark verändert. Immer mehr Unternehmen haben das Paradigma von Entwicklung und Betrieb (DevOps) übernommen. Damit haben sie den Automatisierungsgrad bei der Serviceintegration und -bereitstellung erhöht, z.B. durch die Implementierung von CICD-Pipelines (Continuous Integration and Continuous Delivery) und die Nutzung von IaC-Technologien (Infrastructure as Code). In dieser Hinsicht ist das Site Reliability Engineering (SRE) eine spezifische Umsetzung von DevOps. Es handelt sich dabei um eine Reihe von Grundsätzen und Praktiken, die auf dem Software-Engineering beruhen und auf den IT-Servicebetrieb angewendet werden können. Ein Schlüsselprinzip von SRE ist die Automatisierung und Beseitigung aller sich wiederholenden Aufgaben im Zusammenhang mit dem Betrieb eines IT-Dienstes. Diese Automatisierung ist wichtig, denn jede Steigerung der Nutzung eines IT-Dienstes führt auch zu einem Anstieg der manuellen Arbeitsbelastung. Das Endziel dieser Automatisierung ist daher die Realisierung eines autonomen Betriebs von IT-Diensten, d.h. die Software ersetzt vollständig die menschliche Arbeit in der Durchführung von IT-Diensten.

TECHNOLOGIEN UND ALGORITHMEN FÜR DIE AUTOMATISIERUNG

BEOBACHTBARKEIT UND ÜBERWACHUNG

Beobachtbarkeit bezieht sich auf die Fähigkeit, auf der Grundlage der externen Ausgaben eines IT-Dienstes Rückschlüsse auf dessen internes Verhalten zu ziehen. Ein IT-Dienst ist beobachtbar, wenn er Metriken (z. B. Fehlerraten und Anfragen pro Sekunde) und Protokolle


Photo created by DCSstudio / Freepik

(z. B. Ergebnisse bestimmter Aktionen in einem IT-Dienst) nach außen hin offenlegt. Diese Offenlegung muss im Code des IT-Dienstes durch die Anwendung von Observability-Technologien und Frameworks wie Prometheus, OpenTelemetry und Beats sichergestellt werden.

Unter Überwachung (Monitoring) versteht man das Sammeln und Analysieren von Metriken und Protokollen, die von einer Reihe an IT-Diensten ausgegeben werden, um das aktuelle Verhalten und unerwünschte Änderungen dieser IT-Dienste feststellen zu können. Ein wichtiger Leistungsindikator (Key Performance Indicator, KPI) für die Überwachungstätigkeit ist, wie vom SRE vorgeschlagen, die mittlere Zeit bis zur Entdeckung solcher Ausfälle (MTTD). Ein wichtiges Ziel für den IT-Betrieb ist es, die MTTD für alle IT-Dienste zu minimieren, idealerweise bevor die Kunden dies bemerken.

Heutzutage gibt es mehrere Überwachungstechnologien, die verschiedene Algorithmen des maschinellen Lernens implementieren, um Ausfälle in IT-Diensten auf der Grundlage der Analyse von Metriken und Protokollen zu erkennen. Beispiele für diese Technologien sind Splunk (mit seinem Machine Learning Toolkit),

CloudWatch (mit seiner Funktion zur Erkennung von Anomalien) und Elastic Stack (mit seinen maschinellen Lernfunktionen). Die Technologien ermöglichen die Verwendung einer Reihe von unüberwachten Algorithmen des maschinellen Lernens zur Erkennung von Anomalien oder Ausreißern in kontinuierlich erfassten Daten. Zu diesen Algorithmen gehören abstandsbasierte Algorithmen (wie k-nearest neighbor und k-means) und dichtebasierte Algorithmen (wie random cut forests (RCF) und local outlier factor). Durch die Anwendung derartiger Algorithmen wird das normale Verhalten eines IT-Dienstes erlernt. Jede Abweichung davon wird hingegen als Anomalie betrachtet, über die das IT-Betriebspersonal informiert wird.

FEHLERANALYSE

Wird ein Fehler in einem IT-Dienst festgestellt, muss er zunächst analysiert werden, bevor er behoben werden kann. Die Zeit, die für die Fehleranalyse aufgewendet wird, trägt zur durchschnittlichen Behebungszeit (MTTR) des Fehlers bei. Gemäß dem SRE besteht eine Priorität für den IT-Betrieb darin, die MTTR für alle IT-Dienste zu minimieren, um eine hohe Zuverlässigkeit zu gewährleisten.

Die Fehleranalyse bezieht sich auf die Identifizierung und Analyse der Grundursache eines Fehlers in einem IT-Dienst. Heute gibt es verschiedene Technologien, die Algorithmen anwenden, um solche Ursachenanalysen zu ergänzen. Beispielhafte Technologien dafür sind Elastic Observability (mit seinen Funktionen zur Überwachung der Anwendungsleistung (APM)), Dynatrace (mit seiner künstlichen Intelligenz (KI) Davis), LogicMonitor und Sophie (die KI von Loom Systems). Diese Technologien verwenden Servicetopologien und Maps, um die Beziehungen zwischen allen IT-Services und den damit verbundenen Configuration Items (CIs), die von IT Operations verwaltet werden, zu bestimmen. Für einige spezifische IT-Infrastrukturen, wie z.B. Kubernetes-Cluster, werden diese Service-Typologien oft automatisch auf der Grundlage von vordefinierten


Photo created by pressfoto / Freepik

Meta-Modellen ermittelt, die sofort einsatzbereit sind. Einige Technologien können die Service-Typologien automatisch erkennen, indem sie Text-Mining-Algorithmen auf die Zeilen in den gesammelten Log-Dateien anwenden. Andere Technologien ermöglichen es den Benutzern, die Entitätstypen und ihre Beziehungen für ihre benutzerdefinierten Anwendungen manuell zu definieren. Sobald die Servicetopologien entdeckt sind, können erkannte Ausfälle auf der Grundlage der entdeckten Beziehungen und Zeitstempel zum ursächlichen IT-Service oder CI zurückverfolgt werden, indem die Service Map durchlaufen wird.

Um die Fehleranalyse weiter zu verbessern, werden einige der Technologien auch in bestehende Wissensdatenbanken mit bekannten Fehlern und Lösungsvorschlägen integriert. Die Lösungsvorschläge werden dem Benutzer angezeigt, wenn die Algorithmen bestimmte Zeilen in den gesammelten Protokolldateien entdecken, die mit den in den integrierten Wissensdatenbanken gespeicherten bekannten Fehlern übereinstimmen.


Photo created by creativeart / Freepik

AUSLIEFERUNG UND KONFIGURATION

Um einen Fehler zu beheben und den IT-Dienst wieder in den Normalzustand zu versetzen, muss eine Abfolge von Aktionen durchgeführt werden, die auf der identifizierten und analysierten Grundursache basieren. Diese Aktionssequenzen werden häufig in Form von Runbooks von IT Operations beschrieben. In Runbooks werden die erforderlichen Aktionen in der Regel auf einer sehr technischen Ebene beschrieben, d. h. es werden die genauen Befehle definiert, die ausgeführt werden müssen. Die Runbooks dienen dabei als Anleitung für die SREs. Um die MTTR zu reduzieren, müssen die erstellten Runbooks automatisiert werden.

Es gibt viele Technologien zur Automatisierung von Runbooks. Beispielhafte Technologien sind Ansible, Puppet, Chef, Terraform und Pulumi. Während einige dieser Technologien den Schwerpunkt auf die Automatisierung der Konfiguration von IT-Diensten legen, konzentrieren sich andere Technologien auf die Automatisierung der Einrichtung von IT-Infrastrukturen. Die genannten Technologien haben jedoch eines gemeinsam: Die Spezifikation der Runbooks muss ausschließlich durch Code erfolgen. Daher werden diese Technologien oft unter dem Begriff Configuration as Code (CaC) oder IaC-Technologien zusammengefasst. Obwohl es diese Technologien sehr einfach machen, einzelne Runbooks zu automatisieren, erfordert es manuellen Aufwand, die Abhängigkeiten zwischen einer Reihe von Runbooks zu definieren und zu warten (z. B. mit Ansible Galaxy). Diese Abhängigkeiten müssen jedoch den IT-Automatisierungstechnologien bekannt sein, gemäß dem imperativen Programmierpara-digma, dass eine Reihe von Runbooks in

Photo by Possessed Photography /Unsplash

einer sequentiellen Reihenfolge auszuführen ist. Derzeit wird am Lehrstuhl für Service Operations der Universität Rostock an der Entwicklung eines Agenten geforscht, der die Abhängigkeiten zwischen Runbooks erlernt.

SICHERHEIT

IT-Dienste müssen auf sichere Weise betrieben werden. Es gibt mehrere Tools, die die Erkennung und Behebung von Sicherheitsproblemen in IT-Diensten automatisieren, wie Prisma Cloud und die Aqua Platform.

Prisma Cloud nutzt Algorithmen des maschinellen Lernens zur Erkennung von Anomalien. Dadurch ist das Tool in der Lage, automatisch ungewöhnliches Netzwerk-, Cloud-Ressourcen- und Benutzerverhalten auf der Grundlage von Daten zu erkennen, die über Cloud Application Programming Interfaces (APIs) gesammelt wurden. Die erkannten Anomalien können auf der Grundlage von vordefinierten Cloud-Befehlszeilenschnittstellen (CLI) automatisch behoben werden.

Die Aqua Platform wendet ebenfalls Algorithmen des maschinellen Lernens an, um das Verhalten von containerisierten IT-Diensten automatisch zu erlernen. Auf der Grundlage des erlernten Verhaltens eines containerisierten IT-Dienstes erstellt sie ein Image-Profil, indem sie die von den IT-Diensten genutzten und benötigten Funktionen wie Systemaufrufe und Netzwerkkommunikation in eine Whitelist aufnimmt. Dieses Whitelisting ermöglicht es, die Angriffsfläche des containerisierten IT-Dienstes zu minimieren.

AUSBLICK

Heutzutage gibt es viele intelligente Technologien, um die Erkennung von Fehlern in IT-Diensten zu automatisieren. Die Analyse dieser erkannten Fehler kann jedoch mit den vorhandenen Technologien nur ergänzt, nicht aber automatisiert werden. Um die Ursache eines Fehlers zu beheben, können Technologien eingesetzt werden, um die erforderlichen Runbooks zu automatisieren. Die Spezifikation und Pflege der Abhängigkeiten zwischen diesen Runbooks ist jedoch noch immer eine manuelle Aufgabe. Allerdings lässt sich die Absicherung von IT-Diensten, die in der Cloud oder in Kubernetes-Clustern betrieben werden, in hohem Maße automatisieren.

Insgesamt lässt sich sagen, dass zwar einzelne Bereiche des IT-Betriebs in hohem Maße automatisiert werden können, es aber nur eine geringe Automatisierung über die verschiedenen IT-Betriebsbereiche hinweg und keine End-to-End-Sicht gibt. Bis zu einem wirklich autonomen IT-Servicebetrieb ist es also noch ein weiter Weg.

KONTAKTDATEN

Prof. Dr. Michael Leyer
Lehrstuhl ABWL: Service Operations

Wirtschafts- und Sozialwissenschaftliche Fakultät

Adjunct Professor, School of Management,
Queensland University of Technology,
Brisbane, Australien

Direktor Center für Accounting and Auditing
Direktor Institut für Bankrecht und Bankwirtschaft an der Universität Rostock

Email michael.leyer@uni-rostock.de