FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Fachhochschule Aachen
Campus Köln

Fachbereich 9: Medizintechnik und Technomathematik
Studiengang: Angewandte Mathematik und Informatik

Logging, Tracing & Monitoring - Verfahren zur Überwachung von Anwendungen

Bachelorarbeit

von

Natalie Fritzen

Prüfer:	Prof. Dr. rer. nat. Karola Merkel
Zweitprüfer:	Sebastian Otto
Matrikelnummer:	3240219

Niederkassel-Rheidt, den 10. Juni 2022

Sperrvermerk

Die nachfolgende Bachelorarbeit enthält vertrauliche Daten und Informationen der AXA Konzern AG. Veröffentlichung, Vervielfältigung oder die Weitergabe des Inhalts der Arbeit im Gesamten oder in Teilen sowie das Anfertigen von Kopien oder Abschriften (auch in digitaler Form) sind grundsätzlich untersagt. Ausnahmen bedürfen der schriftlichen Genehmigung der AXA Konzern AG. Die Bachelorarbeit ist nur den Korrektoren sowie den Mitgliedern des Prüfungsausschusses zugänglich zu machen.

Eidesstattliche Erklärung

Ich versichere hiermit, dass ich die vorliegende Bachelorarbeit mit dem Thema

> *Logging, Tracing & Monitoring - Verfahren zur Überwachung von Anwendungen*

selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe, wobei ich alle wörtlichen und sinngemäßen Zitate als solche gekennzeichnet habe. Die Arbeit wurde bisher keiner anderen Prüfungsbehörde vorgelegt und auch nicht veröffentlicht.

Niederkassel-Rheidt, den 10. Juni 2022

Natalie Fritzen

Abstrakt

Inhaltsverzeichnis

1 Einleitung

2 Definitionen von Logging, Tracing & Monitoring

2.1 Logging

Das automatische Protokollieren von Ereignissen wird als Logging bezeichnet. Hierbei sind Ereignisse Fehlermeldungen, Systemnachrichten, Statusmeldungen, etc. Die Daten, die protokolliert werden, werden in eine Log-Datei geschrieben. Diese speichert die Ereignisse mit Zeitstempel und meist chronologisch ab. Außerdem werden die einzelnen Logs mit einem Loglevel versehen, um dem Nutzer das Protokoll besser auswerten kann. Es gibt sechs verschiedene Loglevel. Das schwerwiegendste Level heißt „Fatal“, hierbei spiegeln die Logs wider, dass die Applikation in einem katastrophalen Zustand ist und eingegriffen werden muss. Falls dieses Level auftritt, sollte sofort eingegriffen werden, um die Applikation wieder verfügbar zu machen. Das zweite Loglevel nennt sich „Error“, hierbei läuft die Applikation weiter, ist aber auf einen Fehler getroffen. Der Administrator sollte die Anwendung so früh wie möglich untersuchen und den Fehler beheben. Das nächste Level für Logs ist „Warning“. Die Applikation ist in einem Zustand, der nicht üblich ist. Dieser sollte analysiert werden, um wieder in den Normalzustand zu gelangen. Da die Anwendung läuft, hat die Fehlerbehebung nicht die höchste Priorität, sollte trotzdem zeitnah erledigt werden. Als viertes Loglevel wird „Information“ bezeichnet. Dieses Level wird in der produktiven Umgebung genutzt, um Interessantes im Produktionssystem nachvollziehen zu können. In Testumgebungen wird das Loglevel „Debug“ genutzt, um weitere Informationen auswerten zu können. Das letzte Loglevel wird „Verbose“ genannt, hierbei werden alle Details einer Anwendung dokumentiert. Das Log-Management kümmert sich um die langfristige Speicherung, sodass

die Daten über lange Zeit nachvollziehbar sind. Hierbei sollten die Logs an einer zentralen Stelle gespeichert werden, wie zum Beispiel einer Datenbank. Die Logs können kurzfristig auch in der Konsole ausgegeben werden, können jedoch nicht langzeitig ausgewertet. Lokale Speicherung der Logs in Dateien erschweren das Auswerten. Event-Management stellt Funktionen bereit, um diese Daten auswerten zu können. Zusammengefasst Log- und Event-Management sammeln die Log-Daten, speichern sie, sodass die Daten genutzt werden können, um Probleme zu identifizieren, Prozesse nachzuvollziehen, Systemleistung optimieren oder Cyberangriffe und andere Sicherheitsvorfälle zu erkennen und abzuwehren.
Logs helfen dabei Sicherheitsvorfälle zu identifizieren. Falls gegen Richtlinien verstoßen wird, fallen diese in den Logs durch die Überwachung auf. In den Protokollen werden Informationen festgehalten, um Probleme und ungewöhnliches Verhalten nachvollziehen zu können. Manche Logs sind durch den Gesetzgeber verpflichtend, um Ereignisse nachverfolgen zu können. Transaktionen im Bankumfeld sind verpflichtend aufzuzeichnen, um die Nachvollziehbarkeit dieser Aktionen sicherzustellen. Im Gesundheitswesen ist Logging gesetzlich gefordert, um Compliance-Richtlinien zu erfüllen. Unter anderem gibt es die Datenschutzgrundverordnung, um die Daten richtig zu verarbeiten.
Durch künstliche Intelligenz oder maschinelles Lernen können große Datenmengen automatisiert organisiert und ausgewertet werden. Logging sollte innerhalb einer Anwendung einheitlich verwendet werden. [1–3]

2.2 Tracing

Direkte.[4, 5]

2.3 Monitoring

Status aller Komponenten.[6–8]

3 Verfahren

3.1 Standards aus verschiedenen Sprachen

3.2 Logging

3.3 Tracing

3.4 Monitoring

3.5 Weiterentwicklungen

3.6 Performance

4 Nutzen im Projekt

4.1 Aktuelle Nutzung

4.2 Verbesserungen

5 Zusammenfassung und Ausblick

Literatur

[1] S. Luber und A. Donner. *Was ist Logging/(event-)Log-Management?* 23. Nov. 2021. URL: https://www.ip-insider.de/was-ist-logging-event-log-management-a-1074430/ (besucht am 09. 06. 2022).

[2] F. Bader. *Fehlerhandling und Logging - Wie macht man das eigentlich richtig?* 13. Sep. 2019. URL: https://www.aitgmbh.de/blog/entwicklung/fehlerhandling-und-logging-wie-macht-man-das-eigentlich-richtig/ (besucht am 09. 06. 2022).

[3] *Logging Cheat Sheet.* URL: https://cheatsheetseries.owasp.org/cheatsheets/Logging_Cheat_Sheet.html (besucht am 09. 06. 2022).

[4] C. Kappel. *Logging vs Tracing.* 19. Mai 2022. URL: https://www.adesso.de/de/news/blog/logging-vs-tracing-2.jsp (besucht am 09. 06. 2022).

[5] M. Kahl. *Tracing vs. Tracking – Mikro vs. Makro: Digitale Corona Lösungen.* URL: https://monstar-lab.com/de/expertinsights/digitale-corona-loesungen/ (besucht am 09. 06. 2022).

[6] *Was ist Monitoring?* 20. Nov. 2020. URL: https://www.cloudradar.io/blog/was-ist-monitoring (besucht am 09. 06. 2022).

[7] *Professionelles IT-Monitoring für einen reibungslosen IT-Betrieb.* URL: https://www.wbs-it.de/loesungen/monitoring (besucht am 09. 06. 2022).

[8] S. Collet. *Monitoring: Definition und was IT-Monitoring leistet.* URL: https://www.crossmedia-it.com/it-monitoring-managed-service-provider/ (besucht am 09. 06. 2022).