



Raphael Jöhl



Nico Vinzens

Studenten	Raphael Jöhl, Nico Vinzens
Examinator	Prof. Beat Stettler
Themengebiet	Networks, Security & Cloud Infrastructure

Automatisiertes Troubleshooting

OATS - Open Source Automated Troubleshooting System



Logo

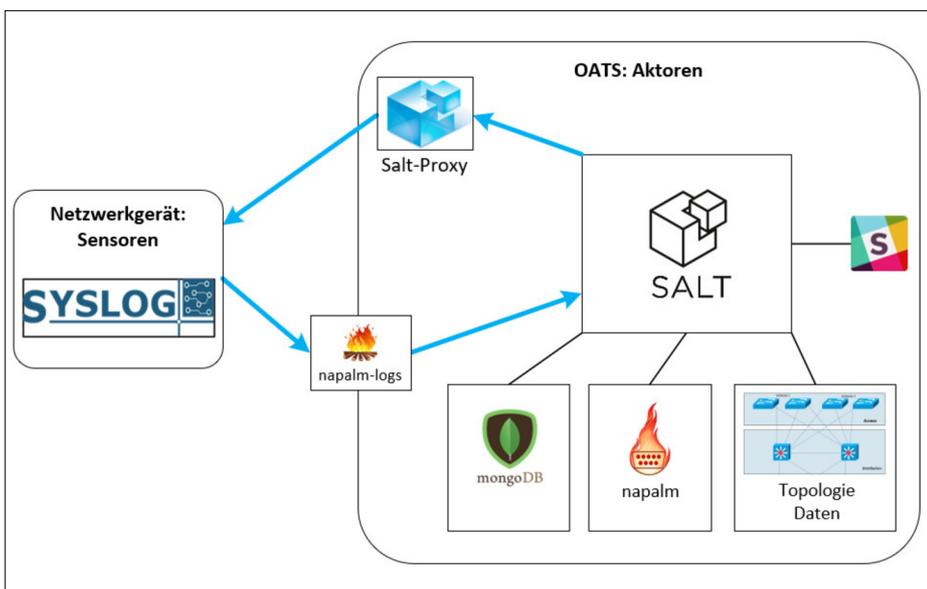
Aufgabenstellung: Das Troubleshooting von Problemen in Netzwerken ist heutzutage zum grössten Teil immer noch manuelle Arbeit. Der Netzwerk Engineer sammelt dabei Informationen indem er den Zustand der Verbindungen überprüft oder die Konfiguration der Geräte durchforstet. Dieses altmodische Paradigma soll durch ein System ersetzt werden, welches dank dem Konzept von «Event Driven Automation» das Troubleshooting automatisieren kann.

Vorgehen / Technologien: Zu diesem Zweck wurden in einer Analysephase Tools identifiziert, die ein solches System ermöglichen. Das Hauptaugenmerk lag dabei darauf, dass die Tools untereinander kompatibel sind und so viel vom Netzwerk wie möglich abstrahieren, sodass kein «Screen-Scraping» mehr nötig ist. Die Tools erfüllen folgende Funktionen: Das Erkennen von Problemen im Netzwerk (Syslog), das Sammeln von Daten zu einem bestehenden Problem (napalm, napalm-logs), das Auslösen eines Workflows, der auf den aktuellen Problemfall zugeschnitten ist (Salt) und das Überprüfen der im Workflow durchgeführten Massnahmen (napalm). Zudem soll zu jedem Problemfall ein Log erstellt und in einer Datenbank (mongoDB) abgespeichert werden. War der Workflow nicht erfolgreich, so wird ein Techniker benachrichtigt (über Slack), der das Problem manuell lösen muss. Die Hauptarbeit dieser Studienarbeit bestand darin, das Gerüst aufzubauen welches all diese Tools zu einem sinnvollen Ganzen verbindet.

Fazit: Das Resultat der Arbeit ist OATS (Open Source Automated Troubleshooting System), welches die Kommunikation zwischen den Tools ermöglicht und über Python-Skripts verschiedene Workflows abbildet, welche in der Lage sind Netzwerkprobleme automatisch zu beheben. OATS wird auch Gegenstand einer weiterführenden Bachelorarbeit sein, welche das automatisierte Troubleshooting noch weiter ausbauen wird. So wäre es zum Beispiel interessant, die benutzten Tools direkt weiter zu entwickeln.

TOOL	ZWECK
Syslog	Sensor für Netzwerkprobleme, löst Events aus
Napalm-logs	Daten aus Syslog-Events extrahieren
Salt	Auf Events mit Troubleshooting-Workflows reagieren
Salt-proxy	Proxy für Netzwerkgeräte
Slack	Chats-Ops
Napalm	Library für Netzwerkzugriffe
mongoDB	Datenspeicherung
Topologie Daten	Daten über das zugrundeliegende Netzwerk

Die Tools und ihre Einsatzzwecke



Architektur der verwendeten Tools