

Maximilian Arthofer, Manuel Ranzmeir

Container basiertes System zur Auswertung von DNS Daten

Betreuer: Prof. DI Robin Laage

To create several network related statistics, all DNS queries running via a DNS cache are recorded and saved in the form of log-files. These logs are then parsed and evaluated using a PHP script. The results are then displayed on a web page.

Since it can take a long time to process a log file (depending on the size of the network), this task was parallelized. That way it's possible to recalculate archived log files, while the system also processes the newly captured ones.

During the initial installation and configuration steps, the focus was on automating all of these steps. For this purpose, we created various scripts. For displaying the results on the website, the data stored in the database is used to create suitable statistics. The data on the website should always be up to date. The generated results should not only be presented in text form, but also in the form of diagrams.

Aufgabenstellung:

- Beschleunigung von Analyseprozessen durch Parallelisierung
 - Umwandeln des PHP-Analyseprogrammes in einen Docker-Container
 - Verwaltung, Parallelisierung und Automatisierung der Docker-Container durch ein Orchestration System
- Erstellung einer Statistik aus den Analysedaten
- Erstellung einer Webseite zur Darstellung der Statistik
- Weitestgehend automatisiert (auch außerhalb des Orchestration System)
- Skripts zur einfachen Installation der Systemkomponenten
- Zusatz: Setup und Einbindung eines DNS-Cache

