THETA

The Higher Education Technology Agenda

Awesome ELK: Solving (some of) The University of Queensland's IT issues with real-time log analysis

With the continuous volume growth of data and ever increasing number and types of security threats, there has never been a greater need to provide IT analysis tools. The authors will present one solution that offers a collective view into large volumes of data and allows both managerial and technical staff the ability to make quick, supported decisions.

As a regular occurrence, we now use terms such as "terabytes" at home and "petabytes" in the enterprise but soon this will be "exabytes" and "zettabytes". With an estimated growth of 4300% in annually generated data by 2020 and vendors and the IT press constantly focused on the need to collect and analyse new types of data, what should we do? First and foremost, let's not ignore the data that our systems have been generating for years. Currently, systems logs are generally "stored and discarded" but there is great potential for analysis and decision making from what we used to assume was information "in case of a fault". Bringing together log information from multiple servers and services, processing the data and then visualising the results, it is easier to see trends and events that many of us were unaware of previously. Trends such as whom, when and from where people access services, threats such as brute force attacks and distributed denial of service attacks are all easily detected by the solution described in this presentation. Analysis of this "ever present" data offers real value to every organisation.

The University of Queensland has recently developed a proof of concept around the open source ELK stack to answer some of the questions and solve some of the issues mentioned above. The ELK stack consists of Elasticsearch, Logstash & Kibana and provides a zero-cost software option to a well-known alternative. Mixing this together with technologies such as Docker to provide rapid provisioning and a well-defined process to categorise data, the solution has yielded great results from day one. Within a few days of powering up the solution, a slow rate brute force attack on student account passwords was identified and closed down. This, as well as many other insightful discoveries will be presented as part of

the presentation.

David Stockdale, Aidan Rowe, Brian Sullivan and Roy Duncan
University of Queensland