The ELK stack as a solution for IaaS-to-application log monitoring and post-mortem service failure analysis

pasquale.maiorano4@unibo.it, marco.cilloni2@unibo.it

ABSTRACT

Nowadays the spread of microservices architecture lead to a huge complexity in terms of monitoring and when is necessary post-mortem fault analysis.
Monitoring systems do an important part in fault prevention, and post-mortem fault analysis in order to identify which component has caused the failure, but in order to check if there were dangling transactions also log analysis will be helpful. Unfortunately, in case of huge failure, these logs could not be available anymore or are corrupted.
In order to avoid this kind of problem, a log concentrator like ELK (Elasticsearch, Logstash, Kibana) stack must be used. A Logstash agent must be installed on each node in order to have system logs, and, at the application level, the logger must be configured in order to write logs on the log stack.
A log strategy also must be decided and implemented in order to exploit the capacity of Elastic search to act as NoSQL data storage with tagged data.
Nowadays the spread of microservices architecture lead to a huge complexity in terms of monitoring and when is necessary post-mortem fault analysis.

Monitoring systems do an important part in fault prevention, and post-mortem fault analysis in order to identify which component has caused the failure, but in order to check if there were dangling transactions also log analysis will be helpful. Unfortunately, in case of huge failure, these logs could not be available anymore or are corrupted.

In order to avoid this kind of problem, a log concentrator like ELK (Elasticsearch, Logstash, Kibana) stack must be used. A Logstash agent must be installed on each node in order to have system logs, and, at the application level, the logger must be configured in order to write logs on the log stack.

A log strategy also must be decided and implemented in order to exploit the capacity of Elastic search to act as NoSQL data storage with tagged data.
The objectives of this work are:

- Deployment of ELK stack on Openstack
- Deployment of logstash agent from IaaS level to application level
- Implementation of a simple application which logs all activities using logstash
- Definition of a logging strategy for the above application
- Definition of a plan in order to detect on Elasticsearch if there are some possible data corruption