Contribution ID: **46** Type: **not specified**

A solution for secure use of Kibana and ElasticSearch in multi-user environment

Thursday, March 9, 2017 4:20 PM (20 minutes)

In order to check health, activities, or resource usage of IT service, monitoring is indispensable. A combination of Kibana and ElasticSearch is used for monitoring in many places such as KEK, CC-IN2P3, CERN, and also non-HEP communities. Kibana provides a web interface for rich visualization and ElasticSearch is a scalable distributed search engine. However, these tools do not support authentication and authorization features by default. There is no problem in the case of single-user environment. On the other hand, in the case of single Kibana and ElasticSearch services shared among many users, any user who can access Kibana can retrieve other's information from ElasticSearch. In multi-user environment, in order to protect own data from others or share part of data among a group, fine-grained access control is necessary.

The CERN cloud service group provides cloud utilization dashboard to each user by ElasticSearch and Kibana. The group has been deployed a homemade ElasticSearch plugin to restrict data access based on a user authenticated by the CERN Single Sign On system. It enables each user to have a separated Kibana dashboard for cloud usage and cannot access to others. Based on the solution, we propose an alternative one which enables user/group based ElasticSearch access control and Kibana dashboards separation. It is more flexible and can be applied to not only the cloud service but also other various situations. We confirmed our solution works fine in CC-IN2P3. And a pre-production platform for CC-IN2P3 is under construction.

We will describe our solution for the secure use of Kibana and ElasticSearch including integration of Kerberos authentication, development of a Kibana plugin which allows Kibana dashboards to be separated based on user/group, and contribution to Search Guard which is an ElasticSearch plugin enabling user/group based access control. We will also describe the effect on performance from using Search Guard.

Primary author: TAKASE, Wataru (KEK)

Co-authors: SASAKI, Takashi (KEK); Dr NAKAMURA, Tomoaki (KEK); WATASE, Yoshiyuki (KEK)

Presenter: TAKASE, Wataru (KEK)

Session Classification: Netwok, Scurity, Infrastructure &Operations IV

Track Classification: Networking, Security, Infrastructure & Operations