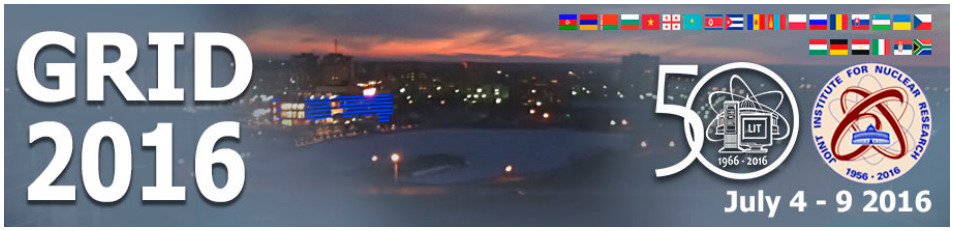

Contribution ID: **30** Type: **Plenary reports**

Grid Site Monitoring and Log Processing using ELK

Thursday, 7 July 2016 08:00 (20 minutes)

Typical WLCG Tier-2 centres use several hundreds of servers with different services. Manual checks of all log files is impossible and various smart solutions for monitoring and log file analysis are used. We describe used procedures in the Computing Centre of the Institute of Physics in Prague, which hosts Tier-2 centre for ALICE and ATLAS experiments and provides resources
for several other projects.

Nagios is used as a basic monitoring tool set. Our custom plug-in aggregates warning and standard error messages and sends them summarised 3 times per day to
administrators via email. Errors on critical components are sent immediately via email and Short Message System to predefined phone numbers. Nagios is complemented by Munin and Ganglia for better status overview of each server and
the whole infrastructure.

ELK stack is the most recent part of our monitoring set up.
All log files from all production servers are shipped for processing by Logstash and then are
stored in Elastic Search. We will describe used hardware, roles of each machine in the ELK cluster, technological challenges, obstacles and our cluster set up and its tuning. Typical examples of searches and graphical outputs will be presented.

Primary author: Mr MIKULA, Alexandr (Institute of Physics of the Czech Academy of Sciences)

Presenter: Mr MIKULA, Alexandr (Institute of Physics of the Czech Academy of Sciences)

Session Classification: Plenary reports

Track Classification: 10. Databases, Distributed Storage systems, Big data Analytics