Contribution ID: **24** Type: **not specified**

Training on security system logging and auditing

Monday, 16 September 2013 14:00 (1h 30m)

Description of Work

Centralized log management is not deployed on all the sites and institutions in EGI. We want to present guides about how a central logging server can be established to collect information from various services. Since the amount of data collected is quite high, it is often not possible to process the data using conventional tools, like grep or custom usual scripts in Perl, etc. Therefore, we would also like to present experiences with efficient processing of large volumes of logs, which make it possible to work with the logs in a way which has not been possible up to now.

Wider Impact of this Work

Centralized management of logs produced by computer systems is an important piece of operations. Having log records collected at a single point
simplifies handling of various incidents since the operator has all the
information collected centrally. The logs also contain other important information that may reveal misconfiguration of services etc.

However, a central log repository is just the first step. In order to be able to utilize the information logged, it is also necessary to process the information and be able to extract relevant data.

In this session we will emphasize the need for a centralized log management and utilizing tools for processing of logs.
We also want to stimulate further discussions in this area among NGIs.

Session, double-session

one session

Printable Summary

Various components of operating systems as well as grid middleware typically produce a lot of information about their operations. The logs contain important details and are invaluable source of information that is important to reveal misconfigurations, etc. Logs also play very important role during investigation of security incidents since they make it possible to track down activites of users and applications.

In the sessions we will present best practices about how logs can be collected and what tools are needed to establish a central logging instance. We will also present current works focusing on efficient log management.

We will try to collect people from other NGIs that have experience in this area to share during the sessions.

The expected audience of the session is the site administrators and security officers.

Primary authors: KOURIL, Daniel (CESNET); BODO, Radoslav (CESNET)

Presenters: KOURIL, Daniel (CESNET); BODO, Radoslav (CESNET)

Session Classification: Training on security system logging and auditing