Contribution ID: **110** Type: **Training/Tutorial**

EGI-CSIRT, Improving Security in a Cloud Environment

Monday, 19 May 2014 15:00 (3 hours)

Managing security in a cloud environment is a challenge. The focus in this session is on security monitoring technologies and how to use them in a cloud environment.

In order to help assess VM images from a security point of view we suggest couple of checks and tools that can be done. The intended audience is either the cloud provider administrator, VM endorser, or VM operator, mostly running Linux-based OS. We will demonstrate how an VM can be checked to detect vulnerable packages installed on VM filesystem and will show how these checks could be
persistently installed in the image.

It is also important to have a centralized log management available, therefore we discuss possibilities how to store these logs from within the VM, either run-time or at least offline.

There are also couple of other rather simple precautions that can foster security of a node on the public Internet, e.g. to disable password-based authentication, preventing from common directory and/or brute-force attacks. We will also discuss these possibilities and demonstrate how they can be enforced.

Another central problem in distributed computing environments is to efficiently suspend identities found in activities misusing the infrastructure. In this session we will show how a central user suspension framework is deployed in the European Grid Infrastructure.

Wider impact and conclusions

Implementing basic security features in a cloud environment.

Description of work

Extension of EGI Security Monitoring tools for usage in a cloud environment.

Primary authors: KOURIL, Daniel (CESNET); NIXON, Leif (LIU); Dr GABRIEL, Sven (FOM)

Presenters: KOURIL, Daniel (CESNET); NIXON, Leif (LIU); Dr GABRIEL, Sven (FOM)

Session Classification: Advancing security in federated clouds