Enabling Grids for E-science in Europe

www.eu-egee.org

SSC Status and Issues

Pal Anderssen (CERN)
Riccardo Brunetti (INFN Torino SA1)

EGEE is a project funded by the European Union under contract IST-2003-508833

Goal of the Security Service Challenges

- *The goal of the LCG/EGEE Security Service Challenges, is to investigate whether sufficient information is available to be able conduct an audit trace as part of an incident response, and to ensure that appropriate communications channels are available.*
- **Stages of the SSC**
  - The SSCs are executed in two stages:
    - Security Challenge targeting the principal site of each of the LCG/EGEE Regional Operation Centers (ROC);
    - Security Challenge targeting the individual sites in each ROC;
- **Roles**
- There are two principal roles in the execution of the SSCs:
  - The Test Operator (TOP), who submits the challenging job, issues the alert, escalates the alert as required and checks the response.
  - The Security Contact of the target site, who receives and acknowledges the alert, makes the necessary investigation and submits the response back to TOP

Previous SSCs

- The first SSC_1 (“Find the user and the UI!”) was executed in january-february 2006.
  - The proposed challenge was to identify submitting user and UI for a given job.
- The second SSC_2 (“Find the storage operations!”) was executed in april-june 2007
  - The challenge was to identify a group of 7 storage operations which involved the target site Storage Element.
- The third SSC_3 is on going.
  - The challenge is to identify a submitted job, to find the relevant programs, to kill the job and to ban the user who submitted it.

In all the challenges it was decided to raise the alert about 24 hours after the submission and to consider 72 hours as an overall time-out for the solution.

The alerts are sent using the GGUS ticketing system and, eventually, each ROC can keep the ticket and turn it to its own support system.

SSC_3: Stop that job!

Enabling Grids for E-science in Europe

- The challenge proposed for the SSC_3 is the following:
  - A job is submitted by the TOP, using an EGEE RB, to the site.
  - The job stays on the WN for a given amount of time (basically sleeping)
  - The security contact, together with the site administrator, are requested to find the job, to kill it and to ban the submitting user.
- It was decided to start with a test phase, challenging a limited number of ROCs/Sites in order to watch for possible issues and improvements before involving every sites.
- The first phase challenged the ROC_IT regional center and showed an important issue (also for future SSCs) that is now blocking the show

SSC_3: ROC_IT report

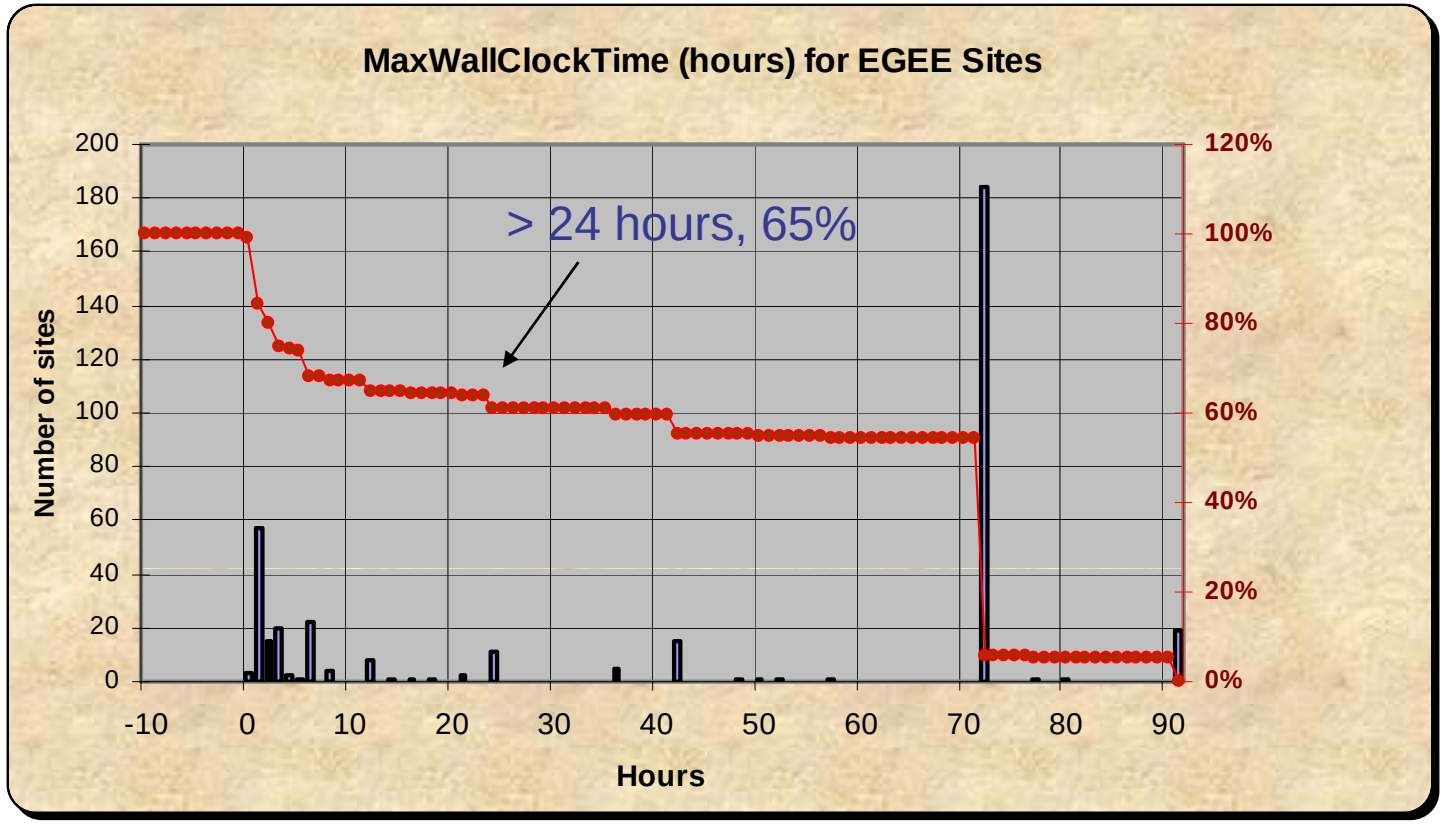
- The challenge was executed on september 13 targeting the INFN-T1 site.
  - 2007-09-13_06:31:01 edg-job-submit
  - 2007-09-13_09:35 GGUS ticket raised
  - 2007-09-13_09:53 TPM assigned the ticket to Security Management
  - 2007-09-13_10:10 Ticket redirected to ROC_IT support system by the Italian security contact
  - 2007-09-13_13:20:54 Job status changes to 'done (failed)'; Job terminates
  - 2007-09-13_13:48:01 TOP tries to resubmit a job. The submission fails
  - 2007-09-13_14:22 The site administrator updated and closed the ticket saying that the job was killed and the user was banned.
  - 2007-09-13_17:07:34 One of the processes apparently continued the execution (may be it was not killed?)
  - 2007-09-16_06:32:37 The survived process gave a last report and exited.

SSC_3: main issue

- In order to figure out what is going on, the job must be running at the site
- Unfortunately, many sites only give a short maximum wall clock time for the dteam queues
- The job is likely going to be killed by the batch system before the system administrator even receives the alert.
- If the job is ruled out, all that you can do is to investigate for detached processes and eventually kill them, but you can’t argue whether they are part of the challenge or not. Thus the “auditing” motivations of the SSC is somehow lost.

Max WallClockTime in EGEE Sites

- The distribution of the maximum allowed wall clock time in EGEE sites for the dteam VO can be found by querying the IS.



SSC_3 proposed workarounds

- The solutions to this issue which have been proposed so far are:
  - The TOPs subscribe to a different VO (for example an LHC VO) which has a longer queue time.
    - Not very good (in my opinion) since this breaks the concept of VO as a group of persons with given common goals, rules and mandates.
  - We ask a member of a different VO to be TOP for this challenge.
    - Which VO steps forward to volunteer?
  - We create a new VO with a “Security” mandate
    - Cons: We would have another “management” VO (we already have dteam and ops)
    - Pros: We would have a dedicated VO that might be used (with specific rules and agreements) also for other perhaps more “intrusive” tests (pen-tests ecc...)
  - We ask the sysadmins to change (peraphs for a limited time) the settings of the dteam-allowed queues, in order to have as much available sites as possible
    - After all, the dteam VO was made right for monitoring and management purposes at the project level.

Main qestion:

- Is the present DTEAM VO appropriate for the SSCs ?
- Does it have the appropriate privileges/environment ?

- Suggestions, questions?