Security Monitoring

Romain Wartel

EGEE 4 Conference, Pisa

www.eu-egee.org

1. Policy issues and interaction with JSPG

2. Monitoring infrastructure

3. Metrics monitoring

- *What documents do we need to write in order to perform security monitoring?*

- *What authorizations do we need? Who can deliver it?*

- *Can we enforce monitoring everywhere it is necessary?*

- *How will the information be displayed?*

- *How will authentication of trusted people be managed?*

- *How could that fit in existing non-monitoring infrastructure?*

- *How can we implement this?*

- *What are the core elements of the grid that need to be monitored?*

- *How can we retrieve appropriate information from these elements?*

- *How intrusive will this be?*
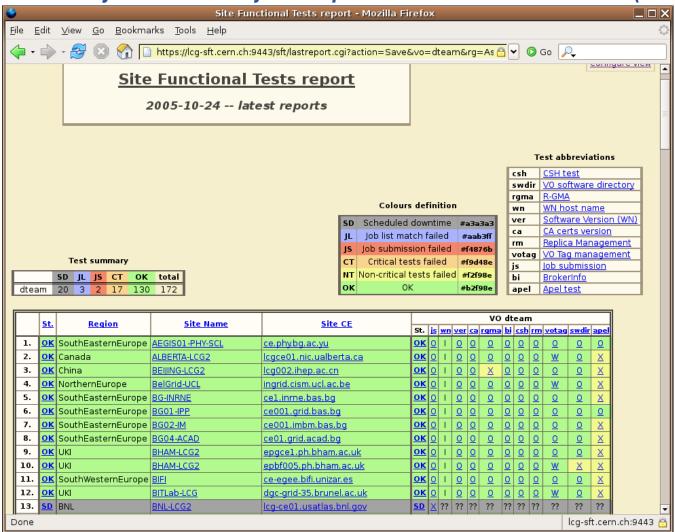
- *How can we implement this?*

Two main approaches:

- *Mandatory tests model*
  - *tests are grid jobs, with no specific privileges*
  - *tests are submitted to all the CEs, no exception*
  - *General results (failed, passed, warning) are public*
  - *Detailed results are only available to a group of authenticated people*

- *Subscription model*
  - *tests are optional, sites have to ask for it*
  - *CEs passing the tests receive an extra "security label"*
  - *tests might sometimes require privileged access*
  - *Detailed results are only available to a group of authenticated people*

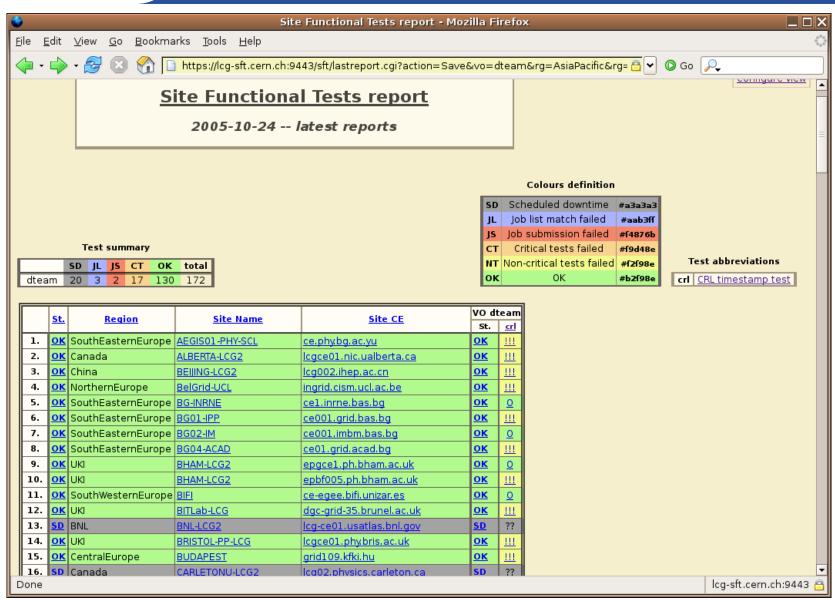- *Ideally, mandatory tests should just be part of Site Functional Tests (SFTs):*

- *A first "security extension" called sft-crl has been developed for SFTs*

- *Piotr Nyczyk has added a secure area on the Site Functional Tests report page*

- *sft-crl is checking the timestamps of the CRL, for each valid certificate:*

  – *A warning is issued if the CRL is more that 9 hours old, but less than 3 days.*

  – *An alert is issued if no CRL is found, or if it is older than 3 days.*

- *The goal is too highlight outdated CRLs or certificates with no CRL*

- *General results are published on the main SFT report page (public access)*

- *Detailed results are available to authorized people only*
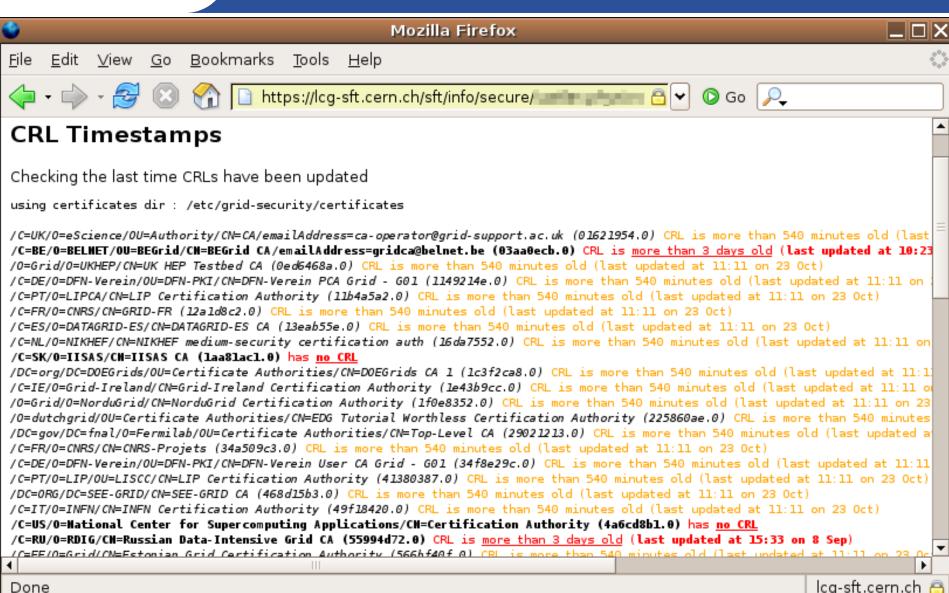
- *Surprise: 106 sites on 172 failed!*
- *Main causes: bugs in edg-fetch-crl, bad configuration, no mechanism to get CRLs*

- *Security extensions are useful*

- *Developing the tool was very easy (thanks to Piotr's secure area)*

- *Sites' configuration need to be more tested*

- *Some work still need to be done:*

  - *To authenticate people from the GOCDB*

  - *To have some more sft security extensions*

  - *Possibly to be able to launch sft tests on the CEs, not only on the WNs.*

In order to provide an efficient security monitoring on the Grid:

- *Some critical elements of the Grid requires dedicated monitoring (RBs, etc.)*

- *Some tests could require privileged access to gather information (for ex: from the log files)*

However:

- *None of this can be done via SFTs*

- *It would be difficult to "force" sites to install such monitoring tools (lots of policy issues)*

Therefore a subscription based model is being adopted.

Current issues to be discussed:

- *What other SFT extension would be useful?*

- *How could we implement a mechanism to check patching status of Grid nodes?*

- *How to have sites to "buy" our subscription based model?*

- *Which parameters should be monitored on the core Grid elements?*

- *It is extremely useful*

- *It should be part of next security service challenge*

- *How do we do this?*

Two proposals:

- *Having a grid job that would:*
  - *Get the list of installed RPM and Linux distribution*
  - *Report it to one or more central service*
  - *The central server(s) will compare this list with the latest list of the vendor*
  - *Security patches will be highlighted from the list (how?)*

- *Having a program, install by local sysadmins that would:*
  - *Launch a command to retrieve the list of pending updates (a la Yumit)*
  - *Report the list to one or more central service*
  - *Security patches will be highlighted from the list (how?)*