

-- MaiteBarroso - 19 Sep 2008

“The mission of the Worldwide LHC Computing Grid (LCG) project is to build and maintain a data storage and analysis infrastructure for the entire high energy physics community that will use the LHC”

People involved

The 3 CODs:

David Bouvet (IN2P3); Kai Neuffer (PIC); Vera Hansper (NDGF)

The people talking to the media on demand:

Pablo Saiz

Flavia Donno

Romain Wartel

Nicholas Thackray

Maria Alandes

Oliver Keeble

John Shade

You need to register to obtain entrance badges, you can do it here:

<http://indico.cern.ch/conferenceDisplay.py?confId=39020> please contact Maria Dimou for the password and write that you will participate in the grid operations demo.

Schedule for the day

The busy times when the journalists will approach the demos are during the breaks: - 9-10 am: registration - 12.40-14.00: lunch - 15:30-15:45: coffee break We should have a good coverage at those times. It is good if all of you could be there in the first slot, and then distribute between you the rest of the day.

Some additional info to remember:

- Rehearsal in the Globe on Mon Sep 29th 14-17 hrs (for those at CERN)

- Sandwich and media briefing offered in the Globe on Wed Oct 1st 12:30 hrs followed by a second rehearsal 14-17 hrs (for those at CERN).

- Lunch is offered on Oct 3rd but please have it **early** (12 o'clockish) to be free for demos when the visitors eat (standing up).

All this is also explained in: <https://twiki.cern.ch/twiki/bin/view/LCG/Oct3rdGridFestDemos#Provided>

As most of us are attending the EGEE08 conference, we will have no time for preparations next week. Let's meet (those of you at CERN) on Monday Sep 29th at 14.00 in the Globe entrance, so we can have a look at the place. After, we'll come back to B28 and discuss the demos, so we can fully profit of the next rehearsal slot on Wednesday. I would highly encourage all of you to follow the briefing offered in the Globe on Wed Oct 1st 12:30 hrs.

Demo setup

- Operations control desk : 2 tables where 3 grid operators will be sitting with laptops, back to the public, with 5-6 standard screens (17'-19'). It would be good to have switches in the table for 5-6 machines, or ports.

- Rtm, Google earth map with tour of T1s: 2 towers with big screens (min 30') in the front, at both sides of the tables. We will put there 2 posters with the GridFest and T1s logos

TO-DO list

Things that are left to do/bring after today's rehearsal:

- 3 screens (similar, as big as possible)
- 3 "something" to put the screens higher (James)
- Keyboard + mouse for RTM big screen
- 3 people shifts for the different times of the day
- Posters: Tiers plus data flow

Preparation:

- Message we want to give
- Prepare story connecting all the tools and starting with RTM (volunteer?)
- Everybody to read Flavia's and Romain's FAQ (at the wiki)
- We meet tomorrow to prepare, with a question/answer brainstorming. 2 pm in 28-R-6. Cristy will join us at 3 (I attach a set of questions she has prepared)
- 5 laptops with certificates to do the rehearsal on Wednesday (at least one of them RTM-enabled!)
- Prepare what to say about each of the tools:
 - ◆ RTM
 - ◆ SLS (<http://sls.cern.ch/sls/service.php?id=WorldwideLCG>)
 - ◆ Gridview: <http://gridview001.cern.ch/GVTEST/lcg-inaug.php>
 - ◆ Gridmap: <http://gridmap.cern.ch/gm/g1.html>
 - ◆ Atlas dashboard for transfers
 - ◇ <http://dashb-atlas-data.cern.ch/dashboard/request.py/site>
 - ◆ accounting: http://www3.egee.cesga.es/gridsite/accounting/CESGA/tier1_view.html
 - ◆ Dashboard Job Monitoring:
 - ◇ Used by 4 LHC experiments + biomed community in The Netherlands
 - ◇ Combine information from different sources (grid status, application...) and present it in a coherent way
 - ◇ Top level view, and possibility to drill down
 - ◇ Output in different formats,
 - ◇ <http://dashb-cms-job.cern.ch/dashboard/request.py/jobsummary>
 - ◇ Example: CPU used by the 4 exp in September is equivalent to the cpu used by a single computer during 1400 years

General WLCG FAQ

<https://twiki.cern.ch/twiki/bin/view/LCG/FAQ>

The key messages from Wolfgang:

- we are ready, passing from development into an operational phase
- yes there is a delay in the data, but we expect the flood for 2009 will be as expected so our plans don't change much. Life goes on despite the technical incident which should be played down
- Hacking questions - blown up by the press. Security is taken very seriously and we have all measures in place to react to incidents.
- Important to show we are happy, it's the beginning of the future and we have a lot of confidence that it works.

Useful "dealing with the media" slides:

- EGEE08 media presentation [↗](#)

Grid security FAQ

Please write here the questions for which you would like some help answering about grid security. Answering a question may require combining several of the proposed responses below.

- **1. How does the project deal with grid security issues? Could somebody attack grid services?**

The EGEE/LCG project includes several security groups (<http://www.eu-egee.org/security>), to deal with the various aspects of security: infrastructure and middleware, policies, operations.

The infrastructure and middleware security groups include security architects from many grid participants and aim at designing, developing and maintaining the grid security services and components of the infrastructure.

The policy group prepares and maintains security policies, which grid participants (including users, VO and sites) must follow.

The security operations group provides an operational response to security threats against the EGEE infrastructure. It focuses mainly on computer security incidents handling, by providing reporting channels, pan-regional coordination and support. It also deals with security monitoring on the grid and provides best practices and advice to grid system administrators.

- **2. What are the main risks?**

The security risks linked to the operations of a large grid are very similar to the risks of any other large/powerful computing infrastructure: they may attract attackers who may want to also use these resources. The main difference is that the grid spans over multiple administrative domains, which is why security operations are completely distributed (and coordination follows a pyramidal structure).

- **3. Did you already had a security incident?**

There are about 5-10 incidents (mostly compromised SSH accounts) per year involving grid sites (although the grid has not yet been used as an infection vector), which are dealt as part of normal grid security operations. The important point is that grid operations were/are not affected.

- **4. How serious can a grid security incident be? How do you deal with security attacks?**

The priorities during security incidents are three-fold: containing the incident to prevent further possible attacks against or from the grid, ensuring the integrity of the services/data, and ensuring the impact on grid operations is minimal.

The grid security operations team is well-prepared to deal with security incidents, has worked many possible scenarios and is continuously training via security drills. The objective of the drills is to check incident reporting channels and security procedures are working as expected, and to ensure an adequate response to security threats with a minimal impact on grid operations.

During real security incidents, documented security procedures are followed, which include ensuring the security incident is fully contained, performing thorough investigations to understand the exact cause of the incident, restoring the access the affected resource(s) if needed, and updating service documentation and procedures to prevent recurrence as necessary. During the entire process, continuous communication between the involved participants (including service managers, experts, users, VO) is maintained in order to ensure an

effective information flow.

- **5. Could'nt you design the grid so that it is secure enough to ensure there is NO security incident? How can you explain that some resources may become compromised?**

Running a computing service is similar to running a motorway service: No matter how good/safe/secure the infrastructure is, it is not possible to shadow each user/driver, thus to guarantee there will be no incident. However the important point is that should an incident occur, great precautions are immediately taken to limit its damage, to maintain the integrity of the service for the other users and to prevent re-occurrence.

- **6. I heard/read about that CMS website that was compromised?**

This has nothing to do with grids. See

<http://cern.ch/it-support-servicestatus/IncidentArchive/080915-CMSMON.htm>

Tools

GridMap

-- JohnShade - 30 Sep 2008

<http://gridmap.cern.ch/gm/gridmap1.html> (modified colour-coding) <http://gridmap.cern.ch/gm/g1.html> (optimised for 800 x 600 screens)

Developed by EDS in the context of CERN's collaboration with industry (OpenLab project). GridMap is a new approach to visualizing complex monitoring data of the Grid. It provides:

- an easy-to-understand interface with intuitive colour-coding
- top-level view with drill-down capabilities for quick, action-oriented oversight and insight

Sites or services of the Grid are represented by rectangles of different size and colour allowing two dimensions of data (e.g. size & status) to be visualized simultaneously. Monitoring data can be visualized from different VO and geographical perspectives. Both current and historical views are available.

[Technical detail: grouping can be by region or tier, rectangles correspond to sites, and are sized according to number of CPUs or number of jobs running. Drill-down into region by clicking on title; clicking on site rectangle opens corresponding SAM page (current view) or GridView page (historical view). Light Red means site is down, Light Green=degraded (problems with one or more services), Green=OK. White rectangles are displayed if site doesn't support selected VO; avoid this by selecting "ops" VO.]

- [The_Worldwide_LHC_Computing_Grid_at_a_glance.pdf](#): The Worldwide LHC Computing Grid at a glance

Dashboard

-- JuliaAndreeva - 02 Oct 2008

[Entry page](#)

Developed mainly at CERN IT Department in close collaboration with LHC experiments and developers of other LCG monitoring systems. Considerable contributions from the institutes in Taiwan, Russia, France and England. Covers complete range of the computing activities of the LHC experiments on the Grid; job processing, data transfre and site commissioning. Transparent monitoring across various Grid Infrastructures

(LCG,OSG, NDGF). Mainly focussed on the needs of the customers (LHC experiments). Widely used by the experiments for their everyday work. Provides both high level and very detailed view. Possibility to drill down in case problem is indicated, as deep as particular reason of failure (job, transfer , service test) retrieved from the log file. Good example is Dashboard for Data transfer for ATLAS.

What we can show there: Example of the ATLAS Data Transfer Dashboard[?]. In the 4 plots on the upper part of the page there are graphs showing throughput, amount of transferred data (in unites of GBytes and Files) done in one time bin, number of errors. In the table below one can see the status of group of sites (ATLAS cloud) which are 'attached' to a given Tier1. The status of the group is indicated by the colour. Pink colour indicates problems. Clicking on the name of the group, one gets the detailed status of transfer for all storage elements belonging to the sites of the group. Clicking on the problematic line, one gets detailed information about failures

This topic: LCG > WlwgOperations

Topic revision: r19 - 2008-10-02 - MaiteBarroso



Copyright &© 2008-2022 by the contributing authors. All material on this collaboration platform is the property of the contributing authors.

or Ideas, requests, problems regarding TWiki? use Discourse or Send feedback