Enabling Grids for E-sciencE

Security Service Challenges

Operational Security Coordination Team

OSCT-3 , Edinburgh

19/20 June 2007

Information Society

www.eu-egee.org

ASIA PACIFIC

Jinny Chien

(Edited by Pål S. Anderssen, CERN)

Sites within the AsiaPacific ROC challenged April 2007

	Site	Admitted	Response	Score
1	**Australia-UNIMELB-LCG2**	√	√	🟢 feedback
2	**GOG-Singapore**	-	-	⚫ **job not admitted**
3	**HK-HKU-CC-01**	√	√	🟢 feedback
4	**IN-DAE-VECC-01**	√	-	🔴
5	**INDIACMS-TIFR**	-	-	⚫ **job not admitted**
6	**JP-KEK-CRC-01**	-	-	⚫ **job not admitted**
7	**JP-KEK-CRC-02**	√	√	🟢
8	**KR-KISTI-GCRT-01**	√	√	🟢 feedback
9	**LCG-KNU**	√	√	🟢
10	**NCP-LCG2**	√	√	🟢 feedback

(continued)

Sites within the AsiaPacific ROC challenged April 2007 (2)

	Site	Admitted		Response	Score
11	**PAKGRID-LCG2**	√	√	🟢	
12	**Taiwan-IPAS-LCG2**	√	√	🟢	
13	**Taiwan-NCUCC-LCG2**	√	√	🟢	feedback
14	**TOKYO-LCG2**	√	√	🟢	feedback
15	**TW-FTT**	-	-	⚫	
16	**TW-NTCU-HPC-01**	√	√	🟢	feedback
17	**TW-NIU-EECS-01**	√	√	🟢	
18	**TW-NCUHEP**	√	-	🔴	
		78%	**67%**		**39%**

SSC_2 Stage_2 debriefing feedback from APROC

- **Was it useful for you?**
  - It demonstrated the issues related to a security incident;
  - It helped to understand how to respond pragmatically to a request for audit;
  - It was a practical exercise for them to trace the related jobs.

- **Was it too easy? Too difficult?**
  - Generally, the SSC-2 was not difficult to respond to;
  - Sites with experience from SSC_1 were at an advantage.

- **How much resources were involved on your site?**
  - One or two professionals, during one to a few hours.

(continued)

SSC_2 Stage_2 debriefing feedback from APROC

- **How could we improve? What should be done differently?**
  - Responding participants asked for affirmation that their responses were complete and correct;
  - A step-by-step guide for the resolution would be appreciated;
  - A different sequence would be useful in later challenges.

[

APROC has created a Web page which explains the resources that were useful for responding to the challenge –

http://lists.grid.sinica.edu.tw/apwiki/Security_Service_Challenge

]

SSC_2 Stage_2 debriefing feedback from APROC

- **Off-site RB created an extra hurdle -**
  - Only APROC Site managers had access to the RB;
  - A GOCDB lookup gave contact information;
  - The Security contact needed to liaise with the contact at the RB.

- **New Sites needed -**
  - Operational guidance;
  - Reference information about the SSC;
  - Some guidance from APROC helping them to complete the challenge.

CENTRAL EUROPE

Daniel Kouril, CESNET

SSC_2 timeline

- **3rd June morning**
  - the challenge jobs submitted
  - 16 sites from CE challenged
    - almost all production sites in CE
    - only one SE per sited used
    - CLI not GUI used
    - results from the jobs collected
- **4th June afternoon**
  - GGUS tickets submitted
  - quickly got assigned to the CE_ROC US and site supporters

SSC_2 timeline

- **4th – 6th June**
  - results from most sites arrived
    - four sites didn‘t sent answer
  - the fastest reply received after 3,5 hours after assignement
  - slow propagation from CE ticketing system
    - reply from one site not propagated at all
- **7th June – now**
  - reminders sent to the four sites
  - discussions with the sites
  - new challenge will be sent when the channels have been stabilized

CERN

Pål S. Anderssen

CERN - IT

Sites within the CERN ROC challenged Jan/Feb 2007

	Site	Admitted	Responded	Score
1	**ALBERTA-LCG2**	√	√	🟡 **no UI**
2	**BEIJING-LCG2**	√	√	🔴 **no UI, no file operations**
3	**CERN-PROD**	√	√	🟢 **default log info.**
4	**BNL-LCG2**	√	√	🔴 **no UI, no file operations**
5	**SFU-LCG2**	√	-	🔴 **no response**
6	**TORONTO-LCG2**	√	√	🔴 **no UI, premature flush of logs**
7	**TRIUMF-LCG2**	√	√	🟠 **no UI**
8	**UIOWA-LCG2**	-	-	⚫ **job not admitted (Site later withdrew from the Grid)**
9	**Umontreal-LCG2**	√	-	🔴 **no response**
10	**USCMS-FNAL-WC1**	-	-	⚫ **job not admitted**
11	**VICTORIA-LCG2**	√	√	🟠 **no UI**

A few selected issues from the CERN ROC in Stage 2

- **Access to logs -**
  - Several Sites reported difficulties obtaining information from off-Site RB;
  - Could be the reason why more than half of the Sites missed the UI question.

- **Contents of logs –**
  - No Site had enabled sufficient logging to identify all 7 storage operations;
  - Fairly deep knowledge about the elements of the storage systems appears to be needed in order to relate the SSC_2 storage operations to the entries in the logs.

- **Log retention –**
  - One site rotated the logs prematurely;
  - Are the requirements for log retention sufficiently clear?

- **Sites with limited SSC experience -**
  - TOP was often solicited for guidance in the resolution process;
    - However, the CERN TOP tried to avoid this role-conflict
  - Is there a need for incident resolution training in general? Or perhaps only SSC training?

SSC More Information

- **Detail information about the individual Sites:**

  Available in the GGUS tickets

- **There is more on the LCG/EGEE TWiki pages:**
  https://twiki.cern.ch/twiki/bin/view/LCG/LCGSecurityChallenge

France

Rolf Rumler

(IN2P3)

SSC2 France

- **Since some time already there are manpower problems for France to work correctly in the OSCT**
- **New people have started very recently**
  - B. Delaunay and B. Boutherin, involved in computers security but no experience with the grid!
- **Doing SSC2 is their first activity and is now ongoing**
  - Decision to launch SSC2 two weeks ago,
  - First actions where to get a valid grid certificate and register to dteam…

SSC2 France status

- SSC2 launched on Thursday 14th, GGUS tickets submitted on Friday 15th
- 6 IN2P3's sites where challenged

IN2P3-GRIF	Paris	asked for script to extract DPM logs
IN2P3-LPC	Clermont	solved on Monday (except UI)
IN2P3-LAPP	Annecy	solved on Friday
IN2P3-IRES	Strasbourg	solved on Monday
IN2P3-IPNL	Lyon	solved on Monday
IN2P3-Subatech	Nantes	solved on Friday

- 3 IN2P3 sites where not challenged
  - IN2P3-CC was already challenged with SSC1
  - IN2P3-CPPM has no Storage Element
  - IN2P3-LPSC is not already validated
- Tests where not exhaustive
  - GRIF is more than on institute
  - Auvergrid is larger than LPC
- Non IN2P3 sites where not challenged
  - CGG-LCG2 (CGGVeritas)
  - CINES (CINES)
  - IPSL-IPGP-LCG2

All French sites from ROCdb

- **IN2P3-LPC (IN2P3-LPC, Clermont-Ferrand, France)**
  - AUVERGRID (IN2P3-LPC, Clermont-Ferrand, France)
- **CGG-LCG2 (CGGVeritas)**
- **CINES (CINES)**
- **GRIF (Grille de Recherche d'Ile de France (GRIF))**
  - IN2P3-LPNHE (Laboratoire de Physique Nucléaire et de Hautes Energies)
- **IN2P3-CC (IN2P3, Lyon, France)**
- **IN2P3-CPPM (Centre de Physique des Particules de Marseille)**
- **IN2P3-IPNL (Institut de Physique Nucl\x{00E9}aire de Lyon)**
- **IN2P3-IRES (IRES, Strasbourg, France)**
- **IN2P3-LAPP (Laboratoire d Annecy-le-Vieux de Physique des Particules)**
- **IN2P3-LPSC (IN2P3, Grenoble, France)**
- **IN2P3-SUBATECH (IN2P3,Nantes,France)**
- **IPSL-IPGP-LCG2 (IPSL-IPGP-LCG2)**

Germany and Switzerland

Italy

Riccardo Brunetti

31 Sites tested

3 not able to execute the job (./.storacc: error while loading shared libraries: liblcg_util.so: cannot open shared object file: No such file or directory)

5 did not respond/execute the challenge

22 executed the challenge

1 on going

- 19 sites identified lcg-cr + lcg-rep
- 6 sites identified lcg-cr + lcg-rep + UI
- 3 sites identified lcg-cr + lcg-rep + UI + lcg-del (all of them with dcache/dpm SE)
- 1 site identified lcg-cr + lcg-rep + lcg-cp (the only one with local SE as source for copy)
- 1 site only identified the file (no operation)
- 2 sites only identified the user (lcas-lcmaps.log)
- 1 site said he lost the log files

Comments

- The challenge was more difficult than the previous (less experience on Storage Elements)
- Some concerns about the fact that some operation could not be traceable (ex. a classic SE does not log the dele operation, at least with the default config.)
- Procedure too complicate: launch the test, send mail, open ticket on ggus, (wait for TPM??) reassign the ticket …..
- General minor participation of sites with respect to SSC_1 (brought to the attention of ROC managers)

North Europe

Russia

South East Europe

Eddie Aronovich

Additional points that were

- Most of the sites in the region challenged
- Test sites were challenged too !
- The runnings on Jan and tickets sent 3 month – a week later !
- Challenge was partially repeated on Apr

Conclusions

- Most sites performed the SSC O.K.
- Most of the sites had no logs after almost 3 month !!!
- Some security contacts asked help
- Test sites are not aware of security issues (This might be out big pb.)

Ideas for next SSC

- **Procedures !**
  - Resource abuse – check that site identifies it and knows what to do
  - Logs from backup
- **Penetration tests for sites and compare it with local assumptions**

South West Europe

SSC 2 - Result

- **Run it over six sites of SWE**
  - 40 % tested of the sites
- **Using GCUS and RTIR**
  - GCUS for opening the ticket
  - RTIR for handling the incident in SWE region
- **First answer less than 3 hours**
  - Some sites were confused
    - “Do we have to answer?”
    - “Why?”
- **Total resolution 3 days average**
  - Reminders sent to 70% of the sites
  - Summer working time delayed the answers
- **100% success**

SSC 2 - Results

- **General feelings from the sites**
  - Not too difficult
  - Good test for checking incidents
  - Good for getting acknowledge and documentation
- **Resource implied in**
  - Two person, Security Officer and a member of the site
- **Quite realistic questions for getting the information**
- **For next round cross-sites test**
  - Having to coordinate several site to get the information

Regional Feedback

UK/I