

*FEEDBACK PRESENTED AT
THE ROC MANAGERS MEETING ON NOVEMBER 21st 2006*

ROC ISSUES FROM COD-11

NEEDS- Resources for failover - SPOF into COD tools-
SHOULD BE REMINDED ON THE AGENDA OF NEXT MEETING --- COD IT team

=====

We need some feedback from the ROC Managers regarding these resources request for failover procedures –please contact alessandro.cavalli@cnaif.infn.it, who centralizes the offers.

=> RB - Rafal Lichwala

For SAM Admin's Page we need WMS server accepting OPS VO test jobs for ALL the EGEE sites (Production, PPS, certified and non-certified). Currently, there is only one such WMS server used by SAM Admin's Page in INFN CNAF (2xXeon-2.4Ghz, 2048MB ram, 2x40GB hd). RAM and CPU could be increased to cope with future load. There is a proposal **TO BE CONFIRMED** to extend WMS server currently used for regular/official SAM test job submissions in CERN, to use it by SAM Admin's Page and to set up a third at INFN CNAF.

=> SAM failover - David Collados

At present at CERN, each of two machines in load balancing has: 4 GB RAM, 2 HD mirrored of 256 GB each, Dual core CPU (3.3 GHZ or more, not sure). Oracle 10g is used on separate HA cluster, Oracle 10g Express Edition (which is free) is being used in other SAM server portals instead (for other Grid projects). Oracle expertise and DB maintenance is needed.

ROC AGENDA-POLICY RECOMMENDATIONS-
SHOULD REMINDED ON THE AGENDA OF NEXT ROC MEETING---COD DECH team

=====

=> A SA1 expert or somebody else who is not a COD should not open a ticket against a site/ROC. When in doubt they should contact either the site's ROC the COD SU.

=> Policy procedures are mainly dealt within the ROC managers meetings only.

=> A site manager should update their info directly in the GOC or through their ROC manager and not contact the COD.

=> Draft of the Operational Manual Procedure to check:

https://twiki.cern.ch/twiki/bin/view/EGEE/EGEEOperationalProceduresDraft#1_SA1_Operational_Procedures_Man.

FOR YOUR INFO - COD PROCEDURES UPDATES

=====

Now 10 teams are working COD duty one out of five weeks. The transition period is over and Lead and Backup teams will work half of the workload on a given week starting early 2007.

⇒ The update of old and new version manual is handled in a wiki and minor modifications are entered by the editorial committee. There should be a handling of stamped version in the very next future. Proposals for COD format and use cases are to be collected through this wiki and a couple of phone conference calls.

⇒ Current procedure URL is the following:
<https://twiki.cern.ch/twiki/bin/view/EGEE/EGEEOperationalProcedures>.

⇒ The draft one is:
https://twiki.cern.ch/twiki/bin/view/EGEE/EGEEOperationalProceduresDraft#1_SA1_Operational_Procedures_Man.

*FEEDBACK PRESENTED AT
THE ROC MANAGERS MEETING ON NOVEMBER 21st 2006*

- ⇒ COD and OSCT-DC procedure presented at last ROC managers meetings is in place into the operation manual and the COD teams are aware that they have to contact their OSCT-DC early in their shift.
- ⇒ COD SU mandate in GGUS has changed, it will not be used to contact grid experts as third level SU are now in place. COD SU should be used to contact the COD team to announce some specific problems about core services so COD can create manual alarms. It will be also a catch-all way to reach the COD mailing list and to forward generic operations feedback and suggestions.
- ⇒ Dashboard and alarms handling by COD. There is a typical classification system under study for COD Activity efficiency. Now that the dashboard has been updated to work on the SAM tests and alarms, it reflects a huge amount of workload that has resulted in a new organization starting in 2007 about the sharing of the workload and in the prioritization of the handling of tickets by COD people.
Basically, a number of criteria has been set up to reckon the prioritization of the failure handling and to take this into account in the display - (It will not be based on the site's size only).

The 4 different criteria that will allow defining alarm priority are **

A– Type of Node: we are dealing with a Central Core Service or Site level Service or not.

B– Number of related alarms masked by the top-one.

C– Current status of the alarm.

D– Site size (in CPUs) allowed to site services.

** Below is some more info on the A to D classification.

A - Node Type

We consider central services are the most important to keep online. Among Core Services, there are some that are "top-level" which should be the most important. Site services that could impact many nodes (sBDII, RGMA) are more important than simple nodes:

Group 1: BDII, RB, WMS, VOMS, LFC

Group2: FTS, SRM, My Proxy

Group3: sBdII, RGMA

Group4: CE, gliteCE, SE

e.g. an alarm raised for a node in group 2 will always have a higher priority than an alarm raised for a node in group 3.

B - A single isolated alarm should be less urgent than an alarm with numerous related alarms behind because it means there are many problems implied by this one.

C - The bigger the error is, the most urgent the alarm is.

– An alarm raised for a test with a "CRITICAL" status should have a higher priority than an alarm raised for a test with a "ERROR" status. If the problem disappeared, alarms become less urgent.

– Alarms that have been triggered by a failing test which is now "OK" should have a low priority (because somehow the problem is not here anymore and the node is working).

– Alarms that have been triggered by a failing test which is now "MAINT" should have a low priority (because this means the problem is being taken care of, and the site is offline on purpose).

D - (For site level services only) A problem on a big site has a higher priority than a problem on a small site.