Minutes COD F2F meeting 8/9-11-2012
Present: Marcin, Tadeusz, Magda, Ernst, Luuk and Ron.

RT tickets
4569: The probe for local monitoring if information has been sent is already there. It just need to be made an operations test. There is a need for a probe that checks the central nagios to see if data has been received.
Action: NGI_PL will propose to turn local nagios probe into operations test. NGI_NL will discuss with Emir the possibilities for a central probe.

4572: COD can be present on jabber but there will be no guaranties about response times. About the COD OLA, this only applies to GGUS tickets.
Action: NL will sent around draft response and put this as resolution in the ticket.

4574: COD agrees to chair this working group if there is a sufficiently large quorum of NGIs that are willing to put effort into this. There is a need for control over the submitted probes and the relevant community supporting the s/w component needs to be involved to review the probes. Maybe the DMSU can be involved in this.
Action: Put response above into ticket. NGI_PL will take this.

4573: COD will not moderate this forum but will participate in it. If questions come along where people require support, COD will direct people to the right support unit.
Action: NGI_NL will update the RT ticket

4564: See “test infrastructures” below

4566, 4567: See “middleware upgrade campaign” below

4568:
Action: NGI_NL will ask Emir and update the ticket

4571: See “Status of the activity” below

Status of the activity
Ron gives presentation about current status of the activity. The outcome is that the follow-up by GGUS tickets has no beneficial effect for the “unknown”, “A/R” and “RPI” and it has had an effect on the top-bdii A/R but that has leveled off.

The idea is to become more of a support unit instead of just being an executioner (OLA enforcer) for badly performing RODs/NGIs. The suggestion is to stop the followup by GGUS tickets and to acquire and analyse that data and derived patterns and trend from it to identify structural badly performing NGIs/RODs and not respond to incedents as was the case with the GGUS tickets. There is agreement on the idea and this needs to be written into a plan and be proposed. The problem that is identified here is that we lack to tools to easily get the necessary data and analyse it. The suggestion is to ask for a programmatic interface for the ops portal and ACE.

An other issue is that OLA violations are not propagated to a managerial level within the NGI. EGI should come up with a proposal on how to solve such an issue. One idea would be to ask poor performing NGIs to dial in on the OMB phone conf and give some explanations about their performance. Enabling individual thresholds for NGIs need to be discussed with COO and we will come up with a proposal.
Action: Send a proposal to COO
Action: Ask COO for observing trends and patterns over time and OLA violations. NGI_NL will do this.

Test infrastructures

Ron explains the status of the discussion between COD and the GOCdb developers. Initially one resource could belong to only one site and one site could only belong to one target infrastructure. Moreover, resources that belong to multiple sites can be grouped together in a service group. This is a virtual site that is not target infrastructure aware. There are a number of issues with this approach.

1. Resources shared by different target infrastructures (projects) wind up in such a service group which can make the service group overcrowded.
2. When different projects want to have different instances of the GOCdb and share resources at the same time, then downtimes need to be declared in multiple GOCdb instances.

The GOCdb developers came up with a very nice solution where sites are scoped to have different target infrastructures and resources that can be scoped to have multiple target infrastructures as defined by their parent site. The proposal has the following advantages:

1. No more downtimes in multiple GOCdbs
2. Site.Production_status is no longer needed as well as flags like “visible to EGI”, “monitored”, “production” which makes things a lot simpler.

In all target infrastructures sites can have the status “certified”, “uncertified”, “suspended”, “candidate”, “closed”. These statuses may mean different things to different target infrastructures. For example, “certified” in the “EGI Production” target infrastructure means exposed to operational tools, monitored, alarms in dashboards, A/R computation and possible suspension, while in the “EGI Test” target infrastructure it only means “monitored by nagios”. This is up for the project behind the target infrastructure to decide. This proposal from the GOCdb developers opens a lot of interesting possibilities of which a number is outlined by the presentation which may be found at:
https://indico.egi.eu/indico/getFile.py/access?resId=1&materialId=slides&confId=1243

There is still a discussion going on between COD and GOCdb developers about the Site.Production_status flag which the GOCdb developers want to retain. Another thing is that in order for the above proposal to work, a different GIIS URL (sitebdii) should be defined per scope of a site in order to enable resource BDII to publish their results to the sitebdii of the same scope. The current situation is that COD has proposed a phone conf with the GOCdb developers.

Malgorzata has on behalf of EGI.eu joined the meeting on test infrastructures. She agreed with the proposal, had no questions and would present this to COO.

Middleware upgrade campaign
The opinion is that this should be taken care off by the usual operations policies. This would mean that this is a task for RODs. COD comes up with the following proposal:

1. EGI Management determines which service needs to be upgraded
2. Probes should be developed, tested and delivered. After the start of the campaign there will be no more services, probes or other modifications anymore. Here the start of the campaign is defined as the moment that tickets are opened to NGIs.
3. COD opens tickets to NGIs 1.5 months before the end of support for security updates., requiring:
    a. To open tickets to sites from the security dashboard requiring a status and plan within two weeks regarding the upgrade. Status and plan have to be suplied in a predefined format. These tickets will be generated at least one month before end of support for security updates. For the retirement of EMI1 this means end of March. Site can close the tickets stating that the upgrade has been done or they finished the decommissioning of the service. Or provide upgrade plan in predefined format. If the later is the case the ticket should not be closed.
    b. RODs have to provide report when support for security updates end. Ticket should remain open until site suspended or has upgraded.
4. COD prepares final handover report for CSIRT. Close ticket to NGIs.

COD wants to discuss this in the November OMB. COD will consult RODs before the OMB by a phone conf and will discuss the nagios probe working group as well.

Handovers
Since there is not much need anymore to put information in handovers, from now on handover are just being used to mark the end of a shift. There is agreement to issue empty handover unless there is something important to report.

NGI_ZA
COD will ask COO to roll back the actions done in the certification of the NGI_ZA and close the GGUS ticket.

Future of COD
Need more visibility in OMB
More close relations with RODs to make clear to NGIs that COD is a useful body.
Organise a slot at the EGI CF13 in Manchester.