**Operations Management Board (OMB)**

|  |  |
| --- | --- |
| **Meeting:** | Operations Management Board |
| **Date and Time:** | 24 January 2012  |
| **Venue:** | Face to face meeting, Amsterdam, NL |
| **Agenda:** | https://www.egi.eu/indico/conferenceDisplay.py?confId=618 |

Participants 2

ACTION REVIEWS 2

Introduction 4

Submission of QR6 5

FOR APPROVAL: Resource Provider OLA 5

FOR APPROVAL: addition of metric org.bdii.Freshness to profile WLCG\_CREAM\_LCGCE\_CRITICAL 6

top-BDII NGI monthly A/R statistics 6

Report from EMI all hands meeting 7

Proposal for GOCDB configuration of NGI services 7

AOB 7

# Participants

|  |  |  |  |
| --- | --- | --- | --- |
| Name and Surname | Abbr. | Organisation | Membership[[1]](#footnote-1) |
| Andres Aeschlimann  |  | Switch, NGI\_CH | member |
| Emrah Akkoyun |  | TUBITAK, NGI\_TR | Deputy Member |
| Torsten Antoni |  | KIT, NGI\_DE | TSA1.6, JRA1 |
| Goncalo Borges |  | LIP, IberGrid | Member |
| Riccardo Brunetti |  | INFN/NGI\_IT | Deputy Member |
| Daniele Cesini |  | INFN | JRA AM |
| Hélène Cordier |  | NGI\_FRANCE | Member |
| Linda Cornwall |  | STFC, SVG | Invited participant |
| Mario David  |  | LIP, Ibergrid | Member, TSA1.3 |
| Claire Devereux  |  | STFC, UKI | Member |
| Tiziana Ferrari  |  | EGI.eu | Chairman |
| Sven Gabriel |  | NIKHEF/SA1.2 | Invited participant |
| John Gordon |  | STFC, UKI | Member |
| Vera Hansper  |  | CSC/NDGF, NGI\_NDGF | Member, TSA1.8 |
| Emir Imamagic |  | SRCE, NGI\_HR | Member, TSA1.3, TSA1.4 |
| Kostas Koumantaros  |  | GRNET | Member |
| Malgorzata Krakowian |  | ACC CYFRONET, NGI\_PL | Member, TSA1.7 COD |
| Ludek Matyska |  | CESNET/NGI\_CZ | Member |
| Mats Nylen |  | NGI\_SE | Member |
| Ernst Pijper |  | SARA/NGI\_NL | TSA1.7 COD |
| Marcin Radecki (EVO) |  | CYFRONET, NGI\_PL | Member, TSA1.7 |
| Mario Reale |  | GARR, NGI\_IT | TSA1.7, network support |
| Miroslav Ruda |  | NGI\_CZ | Member |
| Peter Solagna |  | EGI.eu | Minutes |
| Ulf Tigerstedt |  | CSC | TSA1.8 |
| Ron Trompert |  | SARA, NGI\_NL | Member, TSA1.7 |
| Alessandro Usai |  | SWITCH/NGI\_CH | Deputy Member |
| Paolo Veronesi |  | INFN, NGI\_IT | Member |
| Anders Waananen (EVO) |  | UCPH, Denmark | Member |
| Pavel Weber |  | KIT/NGI\_DE | Member |

Some participants were connected through skype and phone bridges.

# ACTION REVIEWS

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Action Owner** | **Content** | **Status** |
|  |
|  |  |  |  |
| **Actions from the 24 January 2012 OMB meeting** |
| **18.01** | T. Ferrari/M. David | To collect information from EMI about which products will be released by Debian by EMI 🡪 EMI release manager contacted on the 20th of Feb. Tasks are being tracked by EMI at<https://savannah.cern.ch/search/?type_of_search=task&words=debian&only_group_id=734&offset=1&max_rows=25#results> | IN PROGRESS |
| **18.02** | M. David | In order to distribute EA resources evenly, to provide statistics for the 1 year of EMI and IGE to assess the products which are released more frequently (<https://rt.egi.eu/rt/Ticket/Display.html?id=3458>) | OPEN |
| **18.03** | L. Cornwall | To communicate SVG assessment plans for 2012 to the OMB | OPEN |
| **18.04** | E. Imamagic | To assess deployment of NGI SAM failover configuration (<https://rt.egi.eu/rt/Ticket/Display.html?id=3457>) | OPEN |
| **18.05** | E. Imamagic | To distribute documentation on how to trouble shoot the message broker network (<https://rt.egi.eu/rt/Ticket/Display.html?id=3459>) | OPEN |
| **18.06** | K. Kanellopoulos | To provide an overview page with all catch all services provided (<https://rt.egi.eu/rt/Ticket/Display.html?id=3460>) | OPEN |
| **Actions from the 20 December OMB meeting** |
| **17.01** | T. Ferrari | To ensure that M. Ma participate to the works of the WLCG Security TEG 🡪 Mail sent on the 21st of December 🡪 participation to all groups ensured | CLOSED |
| **17.02** | NGIs | To participate to the two EGI surveys on NGI operational services, and EGI.eu operations Global Services by the 19th of January | CLOSED |
| **17.04** | T. Ferrari/P. Solagna | To contact NGIs who are in favour of changing their GOCDB configuration of critical services and implement changes during Jan/Feb and to support the other NGIs in computing their A/R statistics by extracting data from the SAM PI | IN PROGRESS |
| **17.05** | T. Ferrari | To review the naming scheme of EGI profiles when POEM will be in production 🡪 this action will be completed after the first release of POEM | OPEN |
| **17.06** | P. Solagna | To rerun a WLCG\_CREAM\* and ROC\_CRITICAL profile comparison for December 2011. 🡪 a rerun of comparison was run and results distributed to the OMB | CLOSED |
| **17.07** | COD | To reassess the UNKNOWN test percentage in March 2012  | OPEN |
| **Actions from the 28 November OMB meeting** |
| **16.02** | M. Ma | To consult with technology providers and VOs with the aim of updating the EGEE notice about maximum proxy lifetime. | OPEN |
| **16.06** | J. Walsh | To submit a RT requirement of change of the MPI probe 🡪 e-mail discussion in progress related to ticket <https://ggus.eu/ws/ticket_info.php?ticket=76755> and to the correct setting of PolicyMaxWallClockTime and PolicyMaxObtainableCPUTime. 🡪 revision of MPI probes in part of the agenda of the MPI Virtual Team | CLOSED |
| **16.07** | All NGIs | To submit new middleware requirements for ARC/gLite/GLOBUS/UNICORE by January 15 2012. All NGIs are requested to contact their site administrators to involve them in this process 🡪 requirements were submitted and reviewed at the Jan OMB meeting. The requirements accepted by EMI are listed at:https://savannah.cern.ch/task/?group=emi-req | CLOSED |
| **Actions from the 19 September OMB meeting** |
| **14.03** | M. Ma | To assess the current communication channels EGI 🡨🡪 OSG in case of incidents and critical vulnerabilities involving both parties. 🡪 A workflow is needed to share security tickets and discussion is needed to find a ticketing system that satisfy EGI CSIRT and OSG requirements. 🡪 20/12/2011: discussion with OSG at the Jan 2012 OMB 🡪 OSG participation to the OMB was postponed to March | IN PROGRESS |
| **Actions from the 21 June OMB meeting** |
| **12.09** | T. Ferrari | To assign wiki documents ready for revision to the respective reviewers | OPEN |
| **Actions from Oct 2010 OMB meeting** |
| **Action 3.** | TF | to update as necessary the procedure to retire middleware components (<https://edms.cern.ch/document/985325>). <https://rt.egi.eu/rt/Ticket/Display.html?id=347>  | OPEN |
| Note: Actions from previous meetings are closed. |

# Introduction

Tiziana Ferrari/EGI.eu

The PY2 EGI-InSPIRE project review all NGI council members will be invited to attend. The first part of the review agenda will be dedicated to the discussion of strategy plans. The EGI-InSPIRE review will be preceded by a Council meeting. All members of security teams (EGI CSIRT, SVG, SPG etc.) are invited to attend the review in order to address the comments raised during the first review for SA1.

For other information items see the on-line introduction information.

# EGI Operations Roadmap 2012

Task leaders present their proposal for their respective task.

## SA1.2 Security

S. Gabriel/L. Cornwall

### Software vulnerability group

L. Corwall presents status and plans of SVG. T. Ferrari. How does SVG plan to cope with the deployment of heterogeneous grid software stacks? How is the effort and expertise procured?

SVG is not focused on gLite. Assessment of ARC and UNICORE is in the plans. It is however true that full assessment of a product can require a few weeks of manpower. A checklist to be used to assess different middlewares will be provided.

T. Ferrari. Plans should reflect priorities of the NGIs in terms of deployed software. **It would be good that SVG assessment plans are communicated to the OMB (Action, L. Corwall).**

### EGI CSIRT

The ssc5 framework needs some extensions. It will be used to run a challenge at an NGI level with the collaboration of a national VO (the NGI run is locally coordinated by the NGI). The NGI run should be piloted by at least one NGI. The next EGI run – SSC6 – will require the collaboration of another international VO (the previous run relied on the collaboration of ATLAS). SSC6 will focus on the interaction between teams (VO and CSIRT) rather than involving sites.

The RC certification procedure needs to be adapted to assess some security necessary conditions to be met by a site before moving to certified status

A new version of Pakiti is expected to be released. A proposal for a site-wide security monitoring will be distributed to the OMB for comments. The problem to be addressed is the security monitoring of all WNs of a site (which should replace the current monitoring limited to a subset of the WNs). The script required to be run on WNs is very lightweight and does not require root privileges.

NGI\_IT is managing the security training activities, providing materials, etc. T. Ferrari. Training material should be published on the EGI training market place[[2]](#footnote-2).

Risk assessment activities should be run regularly, for example every 18 months. This is agreed by the SVG representative, Linda, coordinating the risk assessment activities of EGI which will take place in Spring 2012.

## SA1.3 Staged Rollout and Interoperation

M. David presents the plans for the software provisioning (staged rollout) activities in preparation to the EMI release 2.0 and IGE releases.

With EMI 2.0 a subset of EMI products will be released for Debian, and the existing resources for early adoption will have to be reallocated. T. Ferrari: priorities will have to be defined according to the interest of the NGIs.

**Action (M. David). To collect feedback on products to be released for Debian and to collect information about interest in deploying these**.

SA1.3 will work in collaboration with OSG and various VOs in order to perform software interoperability testing using test instances of VO services.

T. Ferrari: we need to discuss how to make sure that A/R statistics of a RC are not affected in case of failure due to an EA task. One of the options discussed was the possibility to consider a production service in Early Adoption as in downtime. This is particularly useful for stateful services who cannot easily removed from a pool of service instances 🡪 Item to be added to the SA1.3 roadmap

M. David. Clear instructions on how to roll back a buggy service would ease the Early Adoption activity.

H. Cordier: what is the minimum number of components to be staged rollout by a NGI? T. Ferrari. There is no limit, participation should be driven by interest of participating sites (some products are released more frequently than others).

**Action (M. David). In order to distribute EA resources evenly, to provide statistics for the 1 year of EMI and IGE to assess the products which are released more frequently**.

T. Ferrari. Does the SR process need to be further simplification? It will probably require revision if products will be increasingly distributed in EPEL (as according to the EMI plans).

P. Veronesi. Sufficient time needs to be allowed (e.g. recent EA of MPI). M. David. Time constrains in some (sporadic) cases cannot be avoided to meet the SA2 code freeze deadline.

J. Gordon. Why isn’t VOMS/Oracle and FTS included in UMD? T. Ferrari. CERN was formally approached to participate to staged rollout of these components, but CERN did not commit to that. CERN is the natural partner for SR of FTS as testing is coordinated by WLCG. VOMS/Oracle is only adopted by CERN.

K. Koumantaros. It is important that deployment/known issues are documented in the UMD release notes, this is a community effort for improving documentation to site administrators. This information complements the release notes coming from the technology providers.

## SA1.3 Interoperations

E. Imamagic

Most of the current interoperations activities are in good shape, in particular the integration of desktop grid software (in collaboration with EDGI). New activities that will start in the coming months will concern grid software for using HTC and HPC resources in parallel (in collaboration with MAPPER).

A list of metrics for UNICORE and GLOBUS needs to be populated to enable notification in the operations portal. After this step, a list of metrics for Availability computation will need to be defined.

Also, a list of tests for certification of GLOBUS and UNICORE sites needs to be defined.

## SA1.4 Tools

E. Imamagic

NGI SAM instances can be deployed in failover configuration, even if this is currently possible locally (no geographical failover is currently possible) and no automatic switching between instances is possible – it requires manual intervention. This feature was released with SAM Update 13.

Action (E. Imamagic). To assess deployment of NGI SAM failover configuration.

H. Cordier. Is this also applicable to VO SAM? D. Cesini: this topic will be addressed at the next OTAG.

GOCDB failover is still not active-active. Generally speaking, during 2012 all EGI.eu central tool instances should have a failover configuration in place. In case of failure, notification through ALARM tickets (or similar mechanism) to trigger prompt intervention should be considered. T. Ferrari. Please add this action to the plan.

Messaging: various aspects of this infrastructure need improvement, including: reliability and availability of the messaging system through the usage of virtual destinations (ActiveMQ 5.5), enhanced scalability (to reduce the number of connections to the broker network that are left behind pending), and the implementation of a test network to try new software releases. The difference between “camel routes” and “virtual destinations” is in how data is consumed. With camel routes a message is recorded until it is consumed and then deleted, while with topics a message is published to a consumer without keeping record. A time to live of 3 days is adopted by default.

Almost all these changes will be implemented in Q1 of the second project year. The security implementation is expected to be completed in QR4. The infrastructure is ready to use authenticated connections but the following steps have to be followed: (1) Identify and register the clients, (2) Setup credentials for each client, (3) Modify client configurations to use authenticated access.

T. Ferrari. **More information/documentation on debugging of the message broker is needed when propagation of messages needs to be checked (Action, E. Imamagic).** In addition, NGIs have requested access to information on load/traffic of messages, and the possibility to inspect log files (this requirement can be satisfied if documentation on how to debug messaging is available).

E. Imamagic. Accounting of the broker network is needed but currently not planned.

## SA1.5 Accounting

J. Gordon

The first milestone is about the usage of Secure STOMP Massager to receive summary records from infrastructures. The Secure Stomp Messenger (SSM) is the messaging system used by APEL to transmit messages. It is written in Python and uses the STOMP protocol.

The SSM was designed as a way of using python and STOMP to securely and reliably send messages from APEL clients to the APEL server. It is designed to use the EGI broker network (see https://wiki.egi.eu/wiki/Message\_brokers), but should be compatible with any stomp broker. It is not tied to any other APEL components, so could be used elsewhere. Key features:

* any file can be sent as a message
* messages are encrypted in transit, using IGTF X509 certificates
* all messages are acknowledged by the receiving SSM, so both sides know if a message has been sent
* the same program can act as a sending or receiving SSM, or both, SSM compliance is required both at the client and at the server side
* a receiving SSM must run as a daemon process; a sending SSM can run as a daemon process or can run once, sending all its messages, and quit.

EMI clients will have dependencies on SSM and SSM will have to be distributed and packaged. An APEL client with SSM backend is expected after EMI 2.0. Example code already exists. SSM does not need to be included in the client code, the clients need to write files in a specific directory where SSM software will poll files to create messages.

T. Ferrari: Are Italy and ARC sites already testing them? J. Gordon. Some tests have been conducted. However, NDGF and Sweden are using SGAS and status of development of SGAS is currently unclear due to people leaving. However, tests are needed for other NGIs using ARC without SGAS (e.g. NGI\_CH).

The production roadmap for the repository is basically the same as the clients.

T. Ferrari. Another requirement to be considered is the implementation of NGI views providing information on usage of NGI resources by users with certificates released by other CAs, and vice versa the usage of resources from other NGIs by users with certificates released by a given CA (as according to the requirements defined by the “NGI usage report” virtual team

(<https://wiki.egi.eu/wiki/VT_Inter_NGI_Usage_Report>). These views are requested by several national funding agencies. Currently most NGIs are publishing user DNs so aggregations are possible centrally. The only exceptions are NGI\_IT (that does not publish this information for legacy reasons, but is willing to extend the national accounting system based on DGAS to publish user DNs in the summarized records), and NIKHEF, who has concerns about the security level of messaging. The recent upgrade of the messaging network should now address all concerns. P. Veronesi. Certificates released by the Terena CA include a country code.

Pilot jobs can introduce inaccuracy in the views. glexec is used for traceability, but not for accounting purposes. T. Ferrari: topic for discussion at the accounting Task Force

 (https://wiki.egi.eu/wiki/TCB:Accounting\_Task\_Force).

H. Cordier requires better coordination with virtual teams whose areas overlap with operations.

J. Gordon. EMI is not committed to provide storage accounting until EMI-3.

T. Ferrari: what about local jobs accounting and accounting of parallel/multicore jobs? These requirements will be assessed at the OMB for discussion in the task force. See:

* Accounting of parallel and multi-core jobs <https://rt.egi.eu/rt/Ticket/Display.html?id=3328>
* Support for local jobs in the accounting system https://rt.egi.eu/rt/Ticket/Display.html?id=3327

APEL is evolving to receive accounting records from UNICORE/GLOBUS (ongoing). For ARC direct publishing into the central DB is foreseen. For EDGI (desktop grids) the topic is being investigated.

## SA1.6 Helpdesk

T. Antoni

Report generator is fully ready for the end of the year, but the first version will be released for 2012-Q2.

J. Gordon: alternative workflows would be needed for tickets whose sites stay in the NGI (to minimize notification of tickets assigned to sites). T. Antoni. From a GGUS point of view the responsible SU is still the NGI. For a per-site workflow, a national helpdesk interfaced to GGUS needs to be deployed.

An application widget will be developed to embed a GGUS interface into application portals.

S. Gabriel. A fine grained access control is needed to support security tickets.

T. Ferrari. The implementation of a HA configuration needs higher priority to meet WLCG requirements. Good Nagios probes are also needed to text workflows involving GGUS and NGI helpdesks (if possible). The complexity of this implementation needs to be assessed.

## SA1.7 Support

R. Trompert

Network support. There’s increasing need of end-to-end monitoring tools according to WLCG. Some collaboration should be established for the deployment and support of PerfsonarMDM. A Perfsonar MDM training event is scheduled in Berlin (20-22 March, <https://www.terena.org/events/details.php?event_id=2221>). Test sites for the implementation of a IPv6 testbed will be recorded in the production GOCDB instance (local scope needs to be used so that they do not appear as being part of EGI).

T. Ferrari. TPM effort and activities should be reviewed. We need to understand if TPM effort can be focused on 1st line ticket solving, or this is infeasible with the current level of funding.

Grid oversight activities should concentrate on technical support for the solution of difficult tickets rather than focusing on the timeline. NGI and sites need to be aware that COD can provide technical support and should ask COD if this is needed.

## SA1.8 Availability, core services and documentation

K. Koumantaros (see slides)

The EGI.eu OLA is a document that defines the expected performance for all EGI technical (global) services. In order to have a working reporting system, a monitoring infrastructure and an availability reporting tool are needed.

The catch-all services need to be better documented and publicized.

As to Availability/Reliability reporting, an extension of the existing reporting framework is needed to produce NGI and EGI.eu availability reports. This action will be discussed with the operations portal product team.

**Action (K. Kanellopoulos) To provide an overview page with all catch all services provided**.

No plans about the coordination of documentation were provided to the task leader.

# NGI plans and requirements

T. Ferrari presents the main proposed main actions for SA1 during 2012:

* Security risk assessment and consolidation of security tools
* Middleware upgrade campaign and decommissioning of obsolete services
	+ Phasing out of gLite 3.1/3.2 and definition of related procedures
* Extended staged rollout
* Upgrade plan to GLUE 2.0, GLUE 2.0 EGI profile, GLUE information validation
* Complete OLA framework
* Monitoring and A/R reporting of EGI.eu and NGI services
* Consolidation of NGI services
* Consolidation of NGI integration activities
	+ ARC, GLOBUS, UNICORE, desktop grids, QCG (starting)
* Migration of accounting infrastructure to SSM
* IPv6/network monitoring in collaboration with WLCG

T. Ferrari presents the output of the NGI int. task survey, including information on the main activities planned by NGIs during 2012 and the feedback received about the global services.

M. David: phasing out glite: a support program from NGIs operations needs to be defined. gLite could be still deployed after end of support in case of no critical vulnerability and if still supported by NGIs.

# Review and sustainability of operations services (EGI.eu and NGI)

T. Ferrari presents the output of the NGI survey on sustainability of NGI operations after EGI-InSPIRE.

Input from the survey is discussed and summarized in a set of slides for presentation at the subsequent sustainability workshop.

See slides at:

<https://www.egi.eu/indico/contributionDisplay.py?sessionId=6&contribId=12&confId=709>).

# New middleware requirements

P. Solagna

The status of previously submitted requirements is presented.

All new requirements submitted during January are reviewed. The requirements that are accepted together with the approved priority are documented at:

<https://wiki.egi.eu/wiki/OMB_Requirements>

All requirements will be passed on to EMI and IGE for evaluation during the TCB meeting in February.

# EGI Risk Assessment

L. Cornwall presents the plan for risk assessment in EGI (D4.4). In EGEE 100 threats were assessed.

WLCG is currently running a risk assessment as well and only 12 risks were identified.

EGI assessment could cover up to 50 (an in-between level of granularity will be probably chosen), the exact number of threats is still to be defined.

# Revision of GOCDB roles

P. Solagna

A proposal for the revision of the tree of GOCDB roles and the related authorization is presented. The new roles are proposed to update the name of some roles, to add new roles and to make changes to the actions each role grants the user. These changes will affect both the front end portal and information made available through our programmatic interface.

The full proposal is described at: <https://wiki.egi.eu/wiki/GOCDB/Release4/Development/NewRoles>

H. Cordier asks about the difference in duties between a site operations manager and a security officer.

T. Ferrari: The security officer is responsible of the day by day operations of the site security. The site operations manager is responsible of approving security policies making sure these are endorsed by the site. This responsibility is defined in the RC OLA. The security office is defined in the security glossary:

Grid Security Officer: A named individual responsible for operational security of the Grid

Grid Security Operations: The team providing the operational security capability for the Grid

The OMB approves the proposal. NGI\_FR will comment on the differences of these roles and provide comments via e-mail.

Discussion on the proposed changes in the RC OLA and RP OLA will take place via e-mail.

The discussion on the site decommissioning procedure will be also discussed via e-mail.

Next meeting: 28 Feb (via EVO)

1. Member, Observer, in Attendance [↑](#footnote-ref-1)
2. <http://www.egi.eu/user-support/training_marketplace/> [↑](#footnote-ref-2)