# EGI.eu Core services performance report

# May - October 2014

## Table of Contents



## EGI.eu Core Services/Activities

EGI.eu core services and activities have been identified by the EGI Council as critical for the sustainability of the EGI infrastructure, and they are partially funded by the EGI members' fees. The EGI.eu core services and activities provided by EGI.eu partners were assigned through a bid in 2013. With all partners EGI.eu Operational Level Agreement [1] has been agreed and signed covering each of the EGI.eu core service and activities separately. The documents define aspects such as: scope, service hours, service components, support, service level targets, limitations and constrains, communication, reporting and escalation, additional responsibilities, customer responsibilities and review process.

As part of the reporting process EGI.eu partners are obligated to provide every 6 month performance report covering such aspects as: general overview of performance, performance against Service Targets, issues arising in the period, measures planned and foreseen activities and changes.

This document provides a summary from received reports [2] for period May – October 2014.

# Performance report summary

## 1.1 Message Broker Network

**Short description**

Consortium: GRNET, SRCE

The message broker network is a fundamental part of the operations infrastructure ensuring message exchange for monitoring, the operations dashboard and accounting. As such it is a critical infrastructure component whose continuity and high availability configuration must be ensured. The Message Broker Network is part of the EGI Core Infrastructure Platform which is needed to support the running of tools used for the daily operations of EGI.

**Report summary**

The service availability was above the target of 95% availability for all the months in the period, all the months but one above 99%.

Message brokers had two main issues during the reporting period, described as well in the Central SAM report. These issues did not affect the overall availability of the service but caused data loss.

The first issue has started as a problem on the consumer side (Central SAM) and caused a chain effect that reduced the messaging functionalities for more than one week.

In the next period, the team plans one development to improve the reliability of messages transport, define ACL to control which clients will be able to consume messages from specific queues.

## 1.2 Operations Portal

**Short description**

Consortium: CNRS

The Operations Portal provides VO management functions and other capabilities which support the daily operations of EGI. It is a central portal for the operations community that offers a bundle of different capabilities, such as the broadcast tool, VO management facilities, a security dashboard and an operations dashboard that is used to display information about failing monitoring probes and to open tickets to the Resource Centres affected. The dashboard also supports the central grid oversight activities. It is fully interfaced with the EGI Helpdesk and the monitoring system through messaging. It is a critical component as it is used by all EGI Operations Centres to provide support to the respective Resource Centres. The Operations Portal provides tools supporting the daily running of operations of the entire infrastructure: grid oversight, security operations, VO management, broadcast, availability reporting.

**Report summary**

The availability target was not reached for month 2. The main reason is two major interventions on the IN2P3 Computing Center, one on the web cluster and the second on the whole infrastructure. The team is working closely with the IN2P3 Computing Center staff to limit the maintenance activity and their impact.

Except the regular releases and the scheduled maintenance of the infrastructure we don’t see major issues to follow the current OLA. This year the team has made major upgrades and refactoring of the application

and the associated components and technologies. These changes will help for the future developments and maintenance of the portal. The team will continue to work closely with EGI.eu Operations team to ensure that the user's needs are satisfied.

## 1.3 Accounting Repository

**Short description**

Consortium: STFC

The Accounting Repository stores user accounting records from various services offered by EGI. It is part of the EGI Core Infrastructure Platform, which supports the daily operations of EGI. The EGI Accounting Infrastructure is distributed. At a central level it includes the repositories for the persistent storage of usage records. The central databases are populated through individual usage records published by the Resource Centres, or through the publication of summarised usage records. The Accounting Infrastructure is essential in a service-oriented business model to record usage information.

**Report summary**

The performance of the activity is stable and well in the scope of the agreed level targets.

The support load was unexpectedly high due to the lateness of sites migrating from EMI2 APEL to EMI3. Many NGIs did not provide support for their sites and the APEL team had to help them. The Poodle security exposure exposed a problem with the version of SSL used by APEL to talk with the Message Brokers. A misconfigured site managed to pull accounting messages from the message brokers so they did not reach APEL.

A new release of SSM which does not use SSLv3 will be released in December. The security on the APEL queues in the message broker is being changed to prevent a rogue site causing problems. The messages were retrieved. There will be a major scheduled database change in the next few months once all sites have migrated to EMI3.

## 1.4 Accounting and Metric Portal

**Short description**

Consortium: CESGA

The Accounting Portal provides data accounting views for users, VO Managers, NGI operations and the general public. The Accounting Portal is part of the EGI Core Infrastructure Platform which supports the daily operations of EGI. The EGI Accounting Infrastructure is distributed. At a central level it includes the repositories for the persistent storage of usage records. The central databases are populated through individual usage records published by the Resource Centres, or through the publication of summarised usage records. The Accounting Infrastructure is essential in a service-oriented business model to record usage information.

The Metrics Portal aggregates metrics from the EGI Infrastructure from activity leaders and NGI managers in order to quantify and track the infrastructure evolution.

**Report summary**

Accounting portal availability was lower than the target during May, July and August 2014. During these months a hardware failure caused several mandatory migrations of virtual machines in the cluster, making

the service unavailable during the migration. The lowest availability has been 91% in July. The problem has been solved and the service Availability in the last two months has been 100%.

All the tickets but two has been responded according to the OLA.

## 1.5 SAM central services

**Short description**

Consortium: GRNET, SRCE, CNRS

SAM Central Service is part of the EGI Core Infrastructure Platform which supports the daily operations of EGI. Central systems are needed for accessing and archiving infrastructure monitoring results of the services provided at many levels (Resource Centres, NGIs and EGI.EU), for the generation of service level reports, and for the central monitoring of EGI.eu operational tools and other central monitoring needs.

**Report summary**

During this period the service exceeded all service targets, achieving 100% availability every month. Two incidents occurred, but they had no impact to the overall service performance, although some service availability data was lost.

In May the service experienced a loss of data due to a set of chained failures involving also the message brokers' network. The incident caused large amounts of "unknown" service availability during the first half of the month Normal operations have been resumed on May 12th. To mitigate the issue CRNS devoted more resources to the SAM database, but it required time to consume messages at the same time, and some data was loss.

The second incident was caused by an unavailability of one of the messaging brokers. The large majority of clients properly used the other instances, but some sites reported errors in the 4 days after the incident. One of the triggers of the issue is the worker node testing framework that will be decommissioned in the next SAM update.

## 1.6 Monitoring central services

**Short description**

Consortium: GRNET, SRCE

Monitoring Central Services is supporting monitoring of activities to be conducted centrally, like monitoring of e.g. UserDN publishing in accounting records, GLUE information validation, software versions of deployed middleware, security incidents and weaknesses and EGI.eu technical services. Central Monitoring Services is part of the EGI Core Infrastructure Platform, which supports the daily operations of EGI

**Report summary**

The performance of the activity is stable and met the agreed level targets.

Services were delivered according to the OLA and were extended with new tests and old tests were decommissioned according to EGI.eu requirements. There were no issues during the report period. During next period it is planned to upgrade all services to the SAM Update-23. In addition, once the upgrade to SAM Update-23 is complete, testing of transition to the ARGO Monitoring Engine will be performed

## 1.7 Security monitoring and related support tools

**Short description**

Consortium: CESNET

Security monitoring and related support tools are part of the EGI Core Infrastructure Platform which supports the daily security operations of EGI. EGI is an interconnected federation where a single vulnerable place may have a huge impact on the whole infrastructure. In order to recognise the risks and to address potential vulnerabilities in a timely manner, the EGI Security Monitoring provides an oversight of the infrastructure from the security standpoint. Also, sites connected to EGI differ significantly in the level of security and detecting weaknesses exposed by the sites allows the EGI security operations to contact the sites before the issue leads to an incident. Information produced by security monitoring is also important during assessment of new risks and vulnerabilities since it enables to identify the scope and impact of a potential security incident.

**Report summary**

Over the reported period the Pakiti service was provided for EGI. The instance was moved to a new virtual server based on a new major version of the operating system. The transition was planned as transparent and therefore no downtime was declared for the process. The Pakiti service was used to track critical vulnerabilities detected by the EGI CSIRT, including the Bash vulnerabilities known as Shellshock. Discussions started with wLCG and Cern developers about the possibility to join effort to develop a single solution for monitoring of system packages. Other coordination effort includes introduction of a new system to process monitoring results to security Nagios and Dashboard, which will decrease the number of reported false positives.

The service is used on regular basis by the EGI CSIRT and sites and minor issues are provided when necessary. However, there was no issue raised during the reported period, which would impact the performance of the task.

We plan to continue to work with wLCG teams working on package monitoring, which may induce additional changes in the deployment and/or utilization of the Pakiti service.

## 1.8 Service registry (GOCDB)

**Short description**

Consortium: STFC

Service Registry (GOCDB) is a central registry to record information about different entities such as the Operations Centres, the Resource Centres, service endpoints and the contact information and roles of people responsible for operations at different levels. GOCDB is a source of information for many other operational tools, such as the broadcast tool, the Aggregated Topology Provider, the Accounting Portal, etc. GOCDB is part of the EGI Core Infrastructure Platform, which supports the daily operations of EGI.

**Report summary**

The GOCDB service performed well during the period with no major issues or unscheduled outages.

Failover testing revealed an expected behaviour of the DNS switching mechanism for the Gocdb failover procedure; If the failover is engaged and the DNS is switched, different sites across Europe will experience service outages of unknown periods of time (1~2 hrs). This is due to the caching nature of DNS which can take an undetermined period of time to update all upstream caching DNS servers. The Gocdb OLA states that outages caused due to DNS issues are not a violation.

The Gocdb roadmap and planned developments should not affect the OLA for the next period, which include Pay For Use (P4U) developments and Authentication extensions.

## 1.9 Catchall services

**Short description**

Consortium: GRNET

Catch-All services are auxiliary services needed by the Core Infrastructure Platform and by various operational activities of EGI. Auxiliary services and activities are needed for the good running of Infrastructure Services. Examples of such services are VOMS service and VO membership management for infrastructural VOs (DTEAM, OPS), the provisioning of middleware services needed by the monitoring infrastructure (e.g. top-BDII and WMS), and catch-all services for emerging user communities.

**Report summary**

The availability and reliability of the catch-all services is stable and met the agreed level targets.

dteam VO is an important component of the federation, and for this reason the VOMS is replicated across two geographically separated regions. VOMS has been available constantly for the whole reporting period. The VOMS supports one other VO beside the dteam VO, as a catch-all service. During the reporting period a bug affected the HA configuration of the voms, and caused the interruption of one of the services, these short interruptions never prevented the functioning of the dteam VO. Problem has been investigated and a patch is under deployment.

Catch-all CA has renewed the root-CA certificate during the reporting period and it is releasing SHA-2 signed certificates. During the period there were 8 personal certificates and 11 server certificates issued by the CA.

The catch-all certification top-bdii has been used by six sites under certification during the reporting period, and has been available fulfilling the 99% target requested by EGI for core services.

WMS and LFC served several VOs.

In the next months an upgrade of the certification portal and dteam VOMS are planned.

## 1.10 Operations support

**Short description**

Consortium: CYFRONET

Operations support is auxiliary service needed by the Core Infrastructure Platform and by various operational activities of EGI. Auxiliary activities are needed for the good running of Infrastructure Services. Examples of such are activities for service level management, service level reporting, service management in general and central technical.

**Report summary**

The performance of the activity is stable and well in the scope of the agreed level targets.

Due to Operations Dashboard version 3 release as a ROD support action the team prepared training materials covering operational procedures and their handling in new Operations Dashboard and organized a ROD training. ROD wiki pages have been reviewed and updated. The team also support Operations Portal in terms of consultancy for new Operations Dashboard features. As part of technical support to the EGI.eu the team performed different types of campaigns with sites (e.g. EMI-2 decommissioning, new VOMS services for LHC and OPS VO to be configured at sites, Argus, FedCloud). The team handled introduction of new NGIs into EGI (IDGF, AfricaArabia, NGI_CHINA) and adding new operations tests. Operation support started work towards new broadcast policy to decrease number of separate messages sent to EGI community and participate in works on upgrading procedures.

The team operate the RA process in e-Grant. In total we handled 8 requests; however we had a lot of communications with the customers clarifying their needs, explaining EGI environment and instructing them through the RA process.

As a result the team was consequently improving user-side documentation, raised issues and feature requests to the e-Grant developers and communicating with Resource Providers to organize pool creation process. Operations Support also participated in the development of Resource Allocation process by extending it to FedCloud resources.

Operations Support team has been attending a number of meetings: Operations Management Board, FedCloud Task Force, FedCloud User Support, Pay-For-Use.

There were no issues such as OLA violations or problems in performance which affected the service. However, it is worth to mention it was agreed with EGI.eu operations on closer collaboration through weekly meetings.

In the next period the Operations Support team plans to perform the regular tasks agreed by the OLA related to Central technical support, Resource Allocation and Coordination as well as new regular tasks or activities which may be agreed during weekly teleconferences depending on the expertise and load at Operations Support team.

## 1.11 Security coordination

**Short description**

Consortium: STFC, FOM, SNIC

Central coordination of the security activities ensures that policies, operational security, and maintenance are compatible amongst all partners, improving integrity and availability and lowering access barriers for use of the infrastructure.

**Report summary**

In terms of targets in response time, there were 8 tickets in the reporting period not achieving the target of medium support set for the support unit. These overdue tickets were about expired CRLs from Certification Authorities and the response time has been delayed waiting for an answer from the CA managers.

During the reporting period EGI CSIRT has been certified for the TERENA Trusted Introducer framework.

IRTF (Incident Response Team) handled 10 new security incidents and issued and handled 10 advisories. SVG (software Vulnerability Group) handled 21 new vulnerabilities and issued 10 advisories. Several high-publicity vulnerabilities had to be tracked and handled, including Heartbleed, Shellshock and POODLE, all resulting in a lot of work. A total of 170 new tickets were submitted to EGI RT-IR in the reporting period and were handled by the EGI CSIRT and SVG.

Policy coordination concentrated on activity in Federated Identity Management, in particular with IGTF, FIM4R.

Work on evolving our security operations for Clouds has started but progress has been limited by the higher number of important vulnerabilities emerged during the reporting period. Cloud Technology provider questionnaire: 1st version has been tried out and it will be improved in the next months. Cloud Resource Provider Questionnaire: filled in by all sites and analysed, some sites have issues that need to be followed up.

The reported highlighted two main issues: the reduced volunteer contributions to the CSIRT/SVG groups, and the need of security education of the users and service providers of the CLoud platform. The first issue reduced the capability of the team to deal with low priority issues, since the effort was redirected to the critical ones.

Two new members joined the SVG group, recently, and this will mitigate both the two main issues.

The Security Policy Activities suffered as well of the increased effort devoted to vulnerabilities and incidents, and it is planned to start more regular in early 2015.

## 1.12 Acceptance criteria

**Short description**

Consortium: IberGrid

The Acceptance Criteria are the functional and non-functional requirements that a product must fulfil to be released in UMD, these include generic requirement applicable to every product, and specific requirements applicable to the capabilities supported by a component.

**Report summary**

The current set of quality requirements (Release 7) has proven to be valid for the current set of products in UMD: no new definitions or updates to the criteria have been included.

Four new products -Squid, CVMFS, MyProxy and QCG Broker EGI IS provider- have been successfully validated with those criteria and there is an ongoing analysis in order to see if new definitions can be built upon the existing ones to better assess them.

The verification of acceptance criteria for this period has covered the products of UMD-3.7.0, UMD-3.8.0, UMD-3.8.1 and UMD-3.9.0. A total of 18 UMD Release Candidates (RC) tests were made before each release, and 106 products were verified with no rejections found.

In this regard the tool used to detect issues in the repository dependencies have been improved to minimize the UMD repository key installation.

## 1.13 Collaboration tools/IT support

**Short description**

Consortium: CESNET

Collaborations tools are services needed by the EGI back-office and supporting EGI collaboration.

**Report summary**

The performance of the activity is stable and well in the scope of the agreed level targets.

IT support received over 250 requests requests during the reporting period. All of them were resolved in timely manner.

No significant issues have arisen during the reporting period. In addition to the regular operations stemming from the OLA agreement, the Collaboration Tools SU was asked to deploy the Limesurvey survey software tool[1]. The tool was deployed as EGI Survey (https://survey.egi.eu/) and integrated with EGI Single Sing On (SSO) system. Collaboration Tools SU was also asked to help with deployment of Eduroam for the EGI.eu employees. We have contributed to this effort by setting up and operating an Authentication, Authorization, and Accounting (AAA) management RADIUS server and integrating it with EGI SSO.

## 1.14 Staged Rollout

**Short description**

Consortium: IberGrid

The Staged Rollout is an activity by which certified updates of the supported middleware are first tested by Early Adopter (EA) sites before being made available to all sites through the production repositories. This procedure permits to test an update in a production environment that exposes the product to more heterogeneous use cases than the certification and verification phase. This allows the discovery of potential issues and potentially to add mitigation information to the UMD release notes. Early Adopters teams receive support, for questions related to the Stage Rollout process and for emergency releases.

**Report summary**

Staged rollout contributed to the testing of the components for four UMD releases during the reporting period. Staged rollout coordination include also the process of importing new components in the UMD framework. During this quarter there were a total of two regular releases for UMD components and one emergency update.

In total 24 products and sub-components were deployed and tested, and a total of 45 reports were collected and analysed to integrate the UMD release notes.

The Stage rollout team produced contributions for the EGI Operations Meeting, URT meetings and also represented the UMD activities in the WLCG Middleware readiness group.

No tickets were submitted through the helpdesk to the SR coordination, in the reporting period.

## 1.15 Software provisioning infrastructure

**Short description**

Consortium: GRNET, CESGA

The software-provisioning infrastructure provides the technical tools to support the UMD release process from pulling packages from the developers' repositories to the build of a release.

**Report summary**

Software provisioning infrastructure met and exceeded the availability targets.

During this period the Software Provisioning infrastructure service has been available 24/7 and there was not any relevant issue thus it met its performance target. Maintenance tasks involved security updates and regular operations task such logkeeping and system updates.

CESGA maintained the machines for the verification testbed keeping their OS and digital certificates updated and also preparing new machines for running new tests.

For the next period the team is evaluating the possibility to add support for the UMD-composer to produce UMD Preview in order to allow access to cutting edge products before they pass the workflow. For the verification testbed, the team is currently evaluating a platform based on Jenkins with jclouds plugin in order to have a cloud-based solution to orchestrate the creation/deletion of the required infrastructure for the product under verification, including the automatic installation and configuration of the service.

## 1.16 Incident management helpdesk

**Short description**

Consortium: KIT

Incident Management (Helpdesk) is the central helpdesk provides a single interface for support. The central system is interfaced to a variety of other ticketing systems at the NGI level in order to allow a bi-directional

exchange of tickets. GGUS is part of the EGI Collaboration Platform and is needed to support users and infrastructure operators.

**Report summary**

The performance of the activity is stable and well in the scope of the agreed level targets.

During the monthly releases maintenance work was done and the system was enhanced with some additional features. New support units were introduced for meeting EGI and other needs (e.g. NGI_CHINA, NGI_INDIA, Perun, DIRAC, e-Grant RA Tool, EGI Federated Cloud support units, EGI Catch-all Services, EGI UMD Quality Assurance, EGI Staged Rollout, EGI Collaboration Tools).

Some obsolete support units have been removed (e.g. NGI_AL, various VOs).

The GGUS web servers have been integrated in a load balancing system. Both web servers are now running in parallel. This increases the system reliability.

For enabling the calculation of response times for NGIs work flows have been adapted. A bi-weekly report to EGI Operations team on unresponsive NGIs and sites was established.

## 1.17 1st and 2nd level support

**Short description**

Consortium: IberGrid, CESNET

First level support is responsible for ticket triage and assignment. This activity is also responsible for the coordination with teams responsible for 2nd level and 3rd level support.

Software-related tickets that reach the second level support are analysed and if necessary are forwarded to 3rd line support units only when there are clear indications of a defect (in software, documentation, etc.).

**Report summary**

The performance of the activity is stable and well in the scope of the agreed level targets.

The CESNET and IBERGIRD partnership has successfully established procedures to provide support services and cover all relevant areas orphaned by the dissolution of the previous partnership. The mode of operation has been mostly carried over.

Contrary to the original bid, 1st level support is not provided solely by IBERGIRD, but rather CESNET and IBERGRID alternate on a weekly basis. Since there was little formally described procedure provided by the previous 1st level support owner (INFN), 1st level support by both partners had to follow a natural learning curve, resulting in occasional ticket routing issues in the early months. This seems to have been resolved with learning and with the creation of an internal ticket routing knowledge base / documentation.

There were no serious issues encountered during the period in question. There were occasionally issues wherein GGUS FAQs have been found lacking, and routing was initially unclear to the 1st level supporter on shift, and had to be discussed within the support consortium, resulting in the target response time to be slightly exceeded.

During next period support activities will continue “as tickets arrive.” No changes in procedure or team composition are expected.

# References

[1] EGI.eu OLA agreements: https://documents.egi.eu/document/2170

[2] Performance Reports May - October 2014 https://documents.egi.eu/document/2362