EGI.eu Core services performance report
November 2014 - April 2015

Contents

EGI.eu Core Services/Activities

As part of the EGI Core activity reporting process EGI.eu partners are obligated to provide every 6 month performance report, defined in EGI.eu Operational Level Agreement[1], 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 November 2014 – April 2015.

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

Main activities

- Normal maintenance of the message brokers

OLA Performances report

- The combined availability of the distributed brokers have been above the targets during the monitored period

Issues

- A misconfigured APEL client consumed accounting data
    - ACL implemented to mitigate this issue
- A misconfiguration at CERN caused one broker to be unresponsive. The clients with automatic failover configuration were not affected, clients without failover capabilities were affected
    - Still under investigation with the support of CERN

Plans

- Deploy the ACL features in production

---

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

[2] https://documents.egi.eu/document/2517

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

Main activities

- Portal release, upgrade of the system
- Improved release process/testing

OLA Performances report

- The targets for both availability and support have been exceeded during the monitored period

Plans

- Regular deployment in production of the developments done within EGI-Engage, or within the core activity funds, and maintenance of the services

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

Main activities

- finalized transition to EMI-3 probes in all EGI sites
- releases of the APEL software
- Interface with the Accounting portal for the new data

OLA Performances report

- Availability and reliability: always over 99%
- Support response time: below target only in November
  - The breach has been caused by an erroneous re-assignment of the ticket from another support unit

Issues

- The following issues caused data loss:
  - Misconfigured site, acting as repository
  - Crash caused by another site misconfiguration
- Data was re-published by affected sites, or is being republished

Plans

- Review accounting monitoring tests
- Migrate EMI-2 data in the new repository
- Support for multicore accounting in production

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

Main activities

- Maintenance and support through helpdesk tickets

OLA Performances report

- Availability targets met for all the months but March, due to a failure during a week end

Issues

- Failures during week-end

Plans

- Installation of apache watchdog service

- Study feasibility of a redundant deployment

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

Main activities

- SAM Update-23 has been released and deployed
- Support

OLA Performances report

- Both the targets for service availability and support were met and exceeded during the monitored period

Plans

- Deployment of ARGO service in production
- Test feasibility for monitoring with central Nagios'es

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

Main activities

- Upgrade of the SAM instances to SAM-23
- Changes in the monitoring probes

OLA Performances report

- The service was available 100% of the time during the monitored period.

Plans

- Normal maintenance of the services

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

Main activities

- Provisioning of the Pakiti service
- Implementation of new probes for vulnerability test
- Development of the clients
- Development in the security dashboard

OLA Performances report

- The services and the support met and exceeded the targets during the monitored period

Plans

- No changes in the service, besides regular maintenance (new vulnerabilities support)

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

Main activities

- Operation of the service

- Two new releases of GOCDB
    - Multiple endpoints support, federated identities support

OLA Performances report

- Availability targets were achieved during the monitored period
- Support targets were achieved all the months but in March where one very urgent ticket was handled in 1.25 days, caused by unavailability of staff

Issues

- Unavailability of staff during holiday periods
    - One additional staff member is following operational support for GOCDB from April
- Deployment of federated identity support was affected by some issues
    - Not directly affecting production features

Plans

- Planned Database migration

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

Main activities

- Dteam VO: administration of the VOMSes, upgrade of VOMS software
- CA: One new RA established, re-key of one RA. 3 new personal certificates and 6 new server certificates
- Normal administration of the other catch-all services

OLA Performances report

- All the catch all services were above the availability targets during the monitored period

Plans

- Deployment of a web portal for the catch-all CA
- Routine system administration of the services

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

Main activities

- Updating manuals on wiki
- Carrying out upgrade campaigns
- Handling procedures
- Coordination of advisory boards for the ops tools supporting the operations procedures
- Resource allocation process

OLA Performances report

- Targets for support have been achieved during the monitored period

Plans

- Integrate the resource allocation process with the technical outreach activities

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

Main activities

- IRTF handled 5 new security incidents, completed work on 11 old security incidents and issued 4 advisories.
- SVG handled 25 new vulnerabilities and issued 10 advisories. Four of the advisories were assessed as "Critical" risk.
- Policy coordination with IGTF, SIRTIFI, SCI. Evolution of Cloud security
- IGTF Trust anchor regular releases

OLA Performances report

- The support was provided according to the targets during the monitored period

Issues

- Big number of vulnerabilities handled compared to previous periods

- o Revision of the SVG issue handling procedure
- Lack of participation to security groups
  - o Involve cloud providers, for example

Plans

- Involve more resource providers in the activities, as well as other infrastructures such as PRACE and EUDAT.
- New security risk assessment

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

Main activities

- Quality verification of UMD products (28 products)
- One product rejected
- Started the deployment of an automatic verification framework

OLA Performances report

- Producing new document was not necessary because set of requirement has not changed. Quality criteria were valid for previous period.
  - o Service level target will be revised

Issues

- Security issue found in product was not properly followed up
- Improve communication with security bodies of EGI

Plans

- Implement the automatic verification for all the UMD products
- Start the QA process for the Engage JRA2 software

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

Main activities

- Provisioning of the EGI collaboration tools: wiki, document DB, website, ect…

OLA Performances report

- Availability and reliability always over 90%
- Support targets achieved

Plans

- Continue the provisioning according to the requirements

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

Main activities

- Support for three UMD releases
- Total of 78 product releases, tested by 38 staged rollout deployments

OLA Performances report

- No violation of the OLA targets

Issues

- Lack of EAs

Plans

- Review Staged rollout framework in the light of lack of EAs

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

Main activities

- Maintenance of the software provisioning infrastructure
- Maintenance of the verification testbed for UMD QA

OLA Performances report

- The services exceeded the targets of availability during the monitored period
- The support targets were met all the months but in January, with a response time of 6 days for a ticket. Slightly over

Plans

- Add support for EL7 repositories and Ubuntu and implement the UMD-4 major release for September 2015

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

Main activities

- Support of the helpdesk tool
- Creation/decommission of support units
- Follow up with non-progressing tickets

OLA Performances report

- The service has exceeded the availability targets during the monitored period

Plans

- Development of GGUS, as reported in the release plans[3]

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.

---

[3] https://wiki.egi.eu/wiki/GGUS:Release_Schedule

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

Main activities

- Tickets support and redirection to 3rd level support when necessary

OLA Performances report

- There were deviations from the targets for the ticket assignment in four months and one month for top priority tickets handling by 2nd level support

Issues

- The delays in the assignment have been caused by "test tickets", which in practice should not have been considered in the calculations, mostly
- The delay in handling the top priority ticket by 2nd level support was caused by unavailability of the supported for a large part of the day
    - The support team implemented replacement procedures also for non-full day leaves

Plans

- Improvements in the ticket routing guidelines