



www.egi.eu

@EGI_eInfra

EGI Operations and Responsibilities of an NGI

Matthew Viljoen and Alessandro Paolini

EGI Foundation



The work of the EGI Foundation
is partly funded by the European Commission
under H2020 Framework Programme

- Brief introduction to EGI and the NGIs
- The Teams
- Operations and Procedures
 - *Operations Centres and Resources Centres*
 - *Decommissioning and Suspension*
 - *Monitoring and Performance*
 - *Escalation*
 - *VOs, Software and Security*
- Core Services Overview
- EGI Foundation Responsibilities
- Expectations of an NGI
- Perspective of an NGI (João Pina, IBERGRID)

EGI: Federation of National Infrastructures

- Established in 2010
 - EGI Foundation: Coordinator (based in Amsterdam, Science Park)
 - NGIs: National e-infrastructures (22 country + CERN)
- Membership fees sustain the federation; Projects to advance our services (e.g. EOSC-hub, EGI-ACE)
- EGI = Compute, Storage, Data, Training, Consultancy services
- Gateway to the **European Open Science Cloud (EOSC)**



- Partnerships with peer e-Infrastructures and research communities and industry
- Provision of core services, distributed access, support and expertise provision.
- Also training, SLA brokering; technology scouting and access to project funding opportunities

- **Central Operations and Coordination**



Matthew Viljoen
Service Delivery & IS
Lead



Baptiste Grenier
Information Security
(IS) Manager



Valeria Ardizzone
Service Delivery Officer



Alessandro Paolini
Service Delivery Officer



Cătălin Condurache
Service Delivery Officer



Benjamin Jacobs
Systems Administrator

- **Distributed Operations**

Resource Centre admins/ops teams coordinating at national/regional level. Some ~3000 service endpoints, 225 cloud/htc resource centres and 30 operations centres

- **Specialized Teams**

Computer Security Incident Response Team (CSIRT), Security Policy management, Technical support, Ticket management, Staged Rollout coordination, Accounting & Monitoring staff

Operations Activities

- Service delivery in reliable/trusted way
- Requirements gathering
- Definition + maintenance of OLAs
- Service monitoring
- User accounting
- Service Request & Incident Response
- Service/Software Validation, Verification & Distribution
- Documentation & Expertise Retention
- Authentication & Authorization Infrastructure (AAI)
- Evaluation of Security Threats
- External Liaison
- **NEW:** Collaboration Tools (wiki, confluence, jira, indico, mailing lists, SSO etc.)

- https://wiki.egi.eu/wiki/Operations_Procedures
- **Operations Centre creation (and decommission)**
 - actions and relative steps to be undertaken for integrating an Operations Centre/NGI into the EGI Infrastructure.
 - registration in the configuration database
 - operations and security contacts
 - Support unit in the helpdesk system
 - accept the **Resource Infrastructure Provider OLA**
- **Resource Centre Registration and Certification**
 - **Resource Centre OLA** and the infrastructure policies
 - registration in the configuration database
 - contacts
 - services
 - Certification and **security checks**

- **Resource Centre and Production Server Decommissioning**
 - Good practices between a Resource Centre and its users when the resource centre or a production service are being decommissioned
 - provide decommissioning timeline
 - Logs retention policy (90 days)
- **Decommissioning of unsupported software**
 - timeline and constraint to remove software that is being reached end of life
- **Resource Center suspension**
 - under-performing (RCs OLA violations)
 - software declared unsupported
 - Security incident or failing a critical security procedure
 - can be recertified when the problems are solved

- **Quality verification of monthly availability and reliability statistics**
 - How to notify OLAs violations
 - How to handle with justifications provided by sites
- **Adding new probes to ARGO**
 - each request evaluated by EGI Operations
 - required the OMB approval
- **Managing the A/R profile**
 - collection of tests used to compute the A/R of RCs and services
 - changes approved by OMB

- **EGI Infrastructure Oversight Escalation**
 - Critical part of operations in terms of sites' problems detection, identification and solving
 - The main goal is to track the problem follow-up process as a whole and keep the process consistent from the time of detection until the time when the ultimate solution is reached
 - Two parts:
 - Escalation for operational problem at site
 - Escalation for operational problem with unsupported MW at site

- **VO registration and de-registration procedures**
 - how to fill in the request and information to provide
 - VO ID Card on the Operations Portal
 - criteria to approve the request
 - timeline and ordered steps to decommission a VO
- **Integration of new technology/middleware in the infrastructure**
 - Security, monitoring, support, accounting, documentation
- **Managing new releases of EGI Core Services**
 - 2 weeks testing in pre-production before updating the production instances
- **Security:**
 - vulnerabilities discovery, announcement, and handling
 - security incidents handling

- [Accounting Portal](#) and Repository
 - compute, cloud, and storage usage records
 - accounting records collected through APEL
- [Application DB](#) (AppDB)
 - provides information on virtual appliances and application software available in the EGI Infrastructure.
 - integrated with the EGI FedCloud
- [ARGO Messaging Service](#)
 - used by Accounting, AppDB, Monitoring, and FedCloud services
- [ARGO Monitoring Service](#)
 - monitoring the status of the EGI infrastructure
 - A/R reports
- Collaboration tools
 - EGI.eu website, SSO and DNS; indigo, wiki, jira, confluence, rt, mailman
- [EGI Workload](#) (Dirac)
 - cluster of instances to allow the users to submit computational tasks to HTC and Cloud services

- [Helpdesk - GGUS](#)
 - central point for users support
 - register incidents and service requests
- Helpdesk - Human support
 - 1st and 2nd level support
 - tickets triage, first analysis and assignment
 - analysis of configuration and deployment issues and on suspected software defects
 - suggestions of workarounds, creation of a Known Error DB
- [Marketplace Services](#)
 - EGI Service Portfolio
- Online CA - [RCauth](#)
 - release of temporary X509 certificates
 - token translation
 - Integrated with EGI Check-in
- [Operations Portal](#)
 - Operations and security dashboard, VO management facilities, broadcast tool, Service Order Management Back Office (SOMBO), VAPOR (information system)

- Security coordination and security tools
 - Security policies and procedures
 - middleware risk assessment
 - security incidents, vulnerabilities handling
 - security monitoring
- [Configuration Database - GOCDB](#)
 - infrastructure topology source
- Services for the AAI
 - AAI platform - [EGI Check-in](#)
 - Attribute management ([PERUN](#))
 - VOMS catch-all server
- [Unified \(and Cloud\) Middleware Distribution - UMD and CMD](#)
 - infrastructure supporting the UMD release process
 - quality assurance, staged rollout
 - middleware release

- Service Bidding process
 - periodic calls to find providers for certain capabilities, for the delivery of key Activities and Services
 - opened for EGI Participants
 - services partially funded by EGI Foundation
- OLA for the delivery of the Core Services
- EGI Core services performance reports
 - to verify the agreed quality of service
 - issues occurred and relative mitigations/solutions
 - main results achieved
 - plans for the next reporting period

- EGI Infrastructure oversight
 - monitor the overall status of services, resource centres, and NGIs
 - measure the fulfilment of agreed service level targets
 - problems follow-up
 - technical support to NGI Operators, Resource Centre administrators, and user communities

- Coordination of activities with the Operations Management Board and the User Community Board
 - procedures and policies
 - new technologies
 - technical roadmap of EGI Core Services and requirements gathering

- Coordination of regional activities
- Support to users and resource centres
 - provide help in resolutions to operational incidents and problems
 - escalating these to higher-level teams in case of need for specialized support
- Manage the Resource Centre OLA with respective Resource Centres
 - the services provided by respective Resource Centres are in compliance with the OLA
 - report violations
 - enforcement of the related procedures and policies
- proactively check the status of the Resource Centres, and monitor the progress of open tickets
- Security
 - interface between EGI Central Security and Incident Response Team and the Resource Centre Security officers
 - overview the security incidents and vulnerability issues occurred to their sites
- Be a member of Operations Management Board
 - attend OMB and other operations meeting when needed
- Ensure the accuracy of the information in GOCDDB

EGI: Advanced Computing for Research

Thank you
for your attention.

Questions?



The work of the EGI Foundation
is partly funded by the European Commission
under H2020 Framework Programme

This work by the EGI Foundation
is licensed under a Creative Commons
Attribution 4.0 International License.



www.egi.eu
[@EGI_elnfra](https://twitter.com/EGI_elnfra)