

**EGI-Engage**

Report on the evolution of the EGI Operations Infrastructure

D5.1

|  |  |
| --- | --- |
| **Date** | 25 February 2016 |
| **Activity** | SA1 |
| **Lead Partner** | EGI.eu |
| **Document Status** | DRAFT |
| **Document Link** | https://documents.egi.eu/document/2670 |

Abstract

This documents presents the current status of the EGI Operations infrastructure, focusing on the evolution of services and processes that has been implemented in the first year of the EGI-Engage project. This deliverable gives an overview of the deployed services that are provided to users and members of the federation, the amount of resources available, and the activities that support service provisioning.

The roadmap for evolving the current set of services is presented as well, linked with the other EGI-Engage activities.

**COPYRIGHT NOTICE**



This work by Parties of the EGI-Engage Consortium is licensed under a Creative Commons Attribution 4.0 International License (http://creativecommons.org/licenses/by/4.0/). The EGI-Engage project is co-funded by the European Union Horizon 2020 programme under grant number 654142.

**DELIVERY SLIP**

|  |  |  |  |
| --- | --- | --- | --- |
|  | ***Name*** | ***Partner/Activity*** | ***Date*** |
| **From:** |  |  |  |
| **Moderated by:** |  |  |  |
| **Reviewed by** |  |  |  |
| **Approved by:** |  |  |  |

**DOCUMENT LOG**

|  |  |  |  |
| --- | --- | --- | --- |
| ***Issue*** | ***Date*** | ***Comment*** | ***Author/Partner*** |
| **v.1** |  |  |  |
| **...** |  |  |  |
| **...** |  |  |  |
| **v.n** |  |  |  |

**TERMINOLOGY**

A complete project glossary is provided at the following page: <http://www.egi.eu/about/glossary/>

**Contents**

1 Introduction 5

2 The EGI Production infrastructure 6

2.1 Resources distribution and available capacity 6

2.2 The HTC services 6

2.3 The Cloud services 6

2.4 Capacity consumption 6

2.5 Service level availability performances 6

3 Evolution in the operational coordination 7

3.1 Evolution of the operational procedures and processes 7

3.2 The EGI core activities 7

3.3 The UMD software provisioning 7

4 The evolution of the security operations 8

4.1 Security policies 8

4.2 Security procedures 8

4.3 Security risks assessment 8

5 Roadmap for the EGI production infrastructure 9

6 Figures and captions 10

6.1 Pictures 10

6.2 Tables 10

Appendix I. Appendix example 12

**Executive summary**

EGI production infrastructure is evolving, both in terms of services provided and in terms of supporting procedures and tools, to support the evolving needs of the researchers.

Both the available resources (+23%) and the usage of the capacity (+20%) has increased during 2015. Although the number of sites has reduced, the affected sites were generally small sites, with little human and hardware resources, and that allowed the overall capacity of the infrastructure to increase. EGI Operations are dealing with NGIs with effort issues trying to better support them in their work with limited resources.

The overall quality of the service provided by EGI is good, availability and reliability are in line with the previous years. The central services supporting the federation have been provided with no deviations, also considering the very high quality targets defined for these core tools.

The usage of the infrastructure has increased of 20% in 2015, in terms of CPU time. The Virtual Organizations supporting the LHC remain by far the bigger users, as the total of the non LHC VOs consume about the same amount of the third LHC-VO alone. Never the less the non-LHC relative VOs CPU usage increased of ~40% compared to 2014.

The usage of the federated cloud has not exponentially increased, partially due to the different usage patterns of the communities who has started using it, which is not computing intensive. The increase in the interest in the federated cloud can be measured also by the increase in the VOs registering their virtual machine images in federated cloud, and the total number of virtual machine images registered in the federated cloud.

The EGI production infrastructure roadmap is moving along several paths. The first is strengthening the existing production services, enhancing the user experience in particular for the relatively new services of the federated cloud. While the individual cloud providers are often solid, the federation layer is still fragile, and this is causing a non uniform use experience for the cloud users. The production services need to evolve, with more reliable and consistent federation capabilities that can ensure high productivity for the users and low overhead for the service providers.

The services offered will be extended through EGI-Engage and the collaboration with other projects and with the EGI Marketplace with inputs from the user communities and other service providers. EGI will ensure the quality of the service provided, integrating these services with the operations framework.

# Introduction

The EGI infrastructure builds on more than 10 years of design, development, and production deployment of geographically distributed data analysis services. The production infrastructure federates hundreds of resource centres, to serve thousands of users organised in hundreds of research communities. This document provides an overview of the production infrastructure, in terms of capacity and usage by the communities, and the activities that enable the federation.

Section 2 provides an overview of the status of the production infrastructure, the resources accessed by users, in terms of geographical distribution, deployed capacity and resource consumption, both for high throughput computing and cloud. The data and metrics provided by this section has been gathered from the EGI operational tools, such as the accounting[[1]](#footnote-1) and the monitoring[[2]](#footnote-2) services, and the trends in the last year, or several years, are analysed.

Section 3 focuses on the operational coordination and the operational framework that support the EGI federation, the processes, procedures and the central services that integrate the services operated by the resource centres and the operations centres to ensure the uniformity and quality of the service provisioning to EGI users. The section describes the evolution in the operational procedures, security coordination, service management and software quality assurance. The new services evaluated for production deployment need to be validated versus the operational processes and policies, and this process triggers – when needed- the evolution of the operational tools and the extension of the federation framework.

Section 4, describes the roadmap for the evolution of the EGI Operations in the coming months, with an overview of the new services, or the new access modes to existing services, that will have to be integrated in the production infrastructures.

The federation of cloud services, in production for more than one year, has continued. The capacity has expanded by integrating new sites, and the capabilities offered to the users have been extended, through the extension of standard interfaces and the integration of additional APIs including some native cloud management framework interfaces. The work done to improve the support for cloud services affected all the levels of the EGI operation, and it has been described in all the following sections.

# The EGI Production infrastructure

The **European Grid Infrastructure (EGI)** is a federation of resource infrastructure providers. The resource infrastructure providers manage and operate (directly or indirectly) all the operational services needed to enable the federation at national (or regional) level, for the Resource Centres and their user community. They are also responsible for the maintenance, coordination and integration of the resource centres that provides the resources accessed by the end. The Resource infrastructure Providers liaise locally with the Resource Centre Operations Managers, and represent the Resource Centres.

The EGI resource infrastructure providers are:

* **Council-members resource providers**: National Grid Initiatives (NGIs) and European Intergovernmental Research Organizations (EIROs), who are represented in the EGI Council and directly contribute to the sustainability of EGI.
* **Integrated resource providers**: International organizations who contribute resources and have a collaboration agreement with EGI through a Memorandum of Understanding:
  + Asia Pacific Region (including resources from Australia, China, India, Iran, Japan, Malaysia, New Zealand, Pakistan, Philippines, South Korea, Taiwan, Thailand, Vietnam)
  + "Africa Arabia" (including resources from South Africa, Egypt, Morocco, Tanzania, Kenya, Nigeria, Algeria, Senegal, Ethiopia, Tunisia, Ghana)
  + Ukrainian National Grid (UNG)
  + Latin America (including resources from Brazil, Chile, Mexico)
  + IHEP (China)
  + Canada

At the moment of writing, EGI has strong collaboration activities to enable interoperability for common users with three **Collaborating infrastructures**:

* + Open Science Grid (USA)
  + C-DAC (India)
  + ComputeCanada

In February 2016 EGI comprises resources provided across 58 countries and 2 European Intergovernmental Research Institute (CERN and EMBL), of which 39 are EGI council members. From an operational point of view there is no difference between the integrated resources and the EGI council members sites, all these sites are federated in EGI, and must fulfil the EGI policies and procedures, and support the EGI users.

The collaborating infrastructrues are infrastructures with which EGI has some interoperations agreements, and common user communities, but do not share the EGI operational infrastructure.

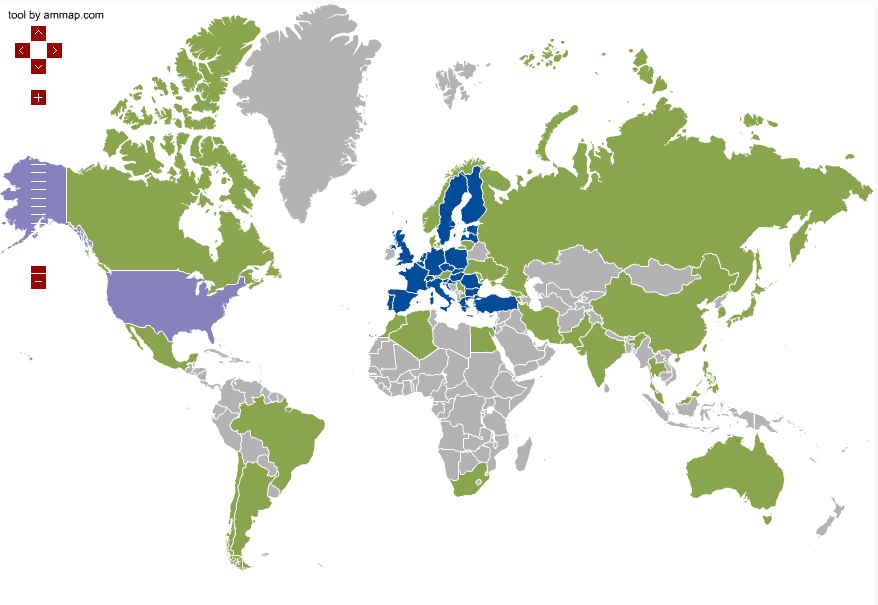


Figure Map of the European Grid Infrastructure. EGI council members in blue, integrated RPs in green, collaborating RP in purple

During the first year of the project the number of resource providers remain almost constant, only the Cyprus NGI has been decommissioned for sustainability reasons.

Only few NGIs raised issues in terms of the available effort to support national operations, and these few cases have been evaluated in collaboration with the EGI.eu operational coordination team, and all beside the decommission mentioned above have been solved, by prioritizing the NGI’s activities in order to continue to fulfil EGI policies and efficiently support the users. The work done with these NGIs also produced inputs for the operational procedures with suggestions to improve their efficiency and better support NGIs with limited effort.

## Resources distribution and available capacity

The National Grid Initiatives (NGIs) are organisations set up to manage the resources provided in their countries by the resource centres to the European Grid Infrastructure (EGI). They represent the country's single point of contact for EGI as well as to liaise with government, research communities and resource centres as regards ICT services for e-science.

Each NGI operations are supported by an Operations Centre, defined as a centre offering operations services on behalf of the Resource infrastructure Provider [GLO], and it can serve multiple RPs. Examples of these services are supporting the sites in the certification process, deploying the monitor services at NGI level or information system, and liaise with EGI during the software upgrade campaigns.

EGI currently comprises 27 national operations centres and 7 federated operations centres encompassing multiple NGIs (Table 1). The federated centres in Europe NGI\_IBERGRID, NGI\_NL and NGI\_IT, each containing two countries, are the result of a collaboration agreement that is expected to continue in the next PYs. In contrast, integrated federated centres in Asia Pacific and Latin America encompass a large number of countries, where the amount of sites per country do not justify the creation of a national operations centre, but suggests an international collaboration. The creation of new national grid initiatives in those regions will depend on their expansion plans and on national policies.

In Table 1 it is shown the resource centres number per country and per operation centre.

Table Number of certified Resource centres per NGI and per country

|  |  |  |
| --- | --- | --- |
| **Operations Centre** | **Country (RCs Number)** | **Resource Centres** |
| AfricaArabia | Algeria (1), Egypt (1), Morocco (2), South Africa (5) | 9 |
| AsiaPacific | Australia (1), China (1), India (2), Iran (1), Japan (2), Malaysia (3), Pakistan (2), South Korea (4), Taiwan (6), Thailand (4) | 26 |
| CERN | Switzerland | 1 |
| IDGF[[3]](#footnote-3) | Hungary | 1 |
| NGI\_AEGIS | Serbia | 6 |
| NGI\_ARMGRID | Armenia | 1 |
| NGI\_BG | Bulgaria | 2 |
| NGI\_CH | Switzerland | 6 |
| NGI\_CHINA | China | 2 |
| NGI\_CZ | Czech Republic | 6 |
| NGI\_DE | Germany | 19 |
| NGI\_FI | Finland | 10 |
| NGI\_FRANCE | France | 17 |
| NGI\_GE | Georgia | 1 |
| NGI\_GRNET | Greece | 16 |
| NGI\_HR | Croatia | 4 |
| NGI\_HU | Hungary | 3 |
| NGI\_IBERGRID | Portugal (5), Spain (18) | 23 |
| NGI\_IL | Israel | 5 |
| NGI\_IT | Austria (2), Italy (45) | 47 |
| NGI\_MARGI | FYROM | 2 |
| NGI\_MD | Moldova | 2 |
| NGI\_NDGF | Denmark (1), Estonia (2), Finland (11), Latvia (2), Lithuania (1), Norway (1), Sweden (2) | 20 |
| NGI\_NL | Belgium (3), Netherlands (15) | 18 |
| NGI\_PL | Poland | 13 |
| NGI\_RO | Romania | 10 |
| NGI\_SI | Slovenia | 2 |
| NGI\_SK | Slovakia | 8 |
| NGI\_TR | Turkey | 3 |
| NGI\_UA | Ukraine | 15 |
| NGI\_UK | United Kingdom | 24 |
| ROC\_Canada | Canada | 8 |
| ROC\_LA | Brazil (3), Chile (3), Mexico (3) | 9 |
| Russia | Russia | 9 |
| **Total OCs: 34** | **Total Countries: 53** | **Total RCs: 335** |

Table Number of certified EGI Resource Centres (February 2016) compared to December 2014.

|  |  |  |
| --- | --- | --- |
| **Resource Centres** | **Number of RCs (February 2016)** | **Number of RCs (December 2014)** |
| EGI-InSPIRE Partners and NGI Council Members | 289 | 310 |
| From non-European EGI-InSPIRE Partners | 24 | 23 |
| From integrated Infrastructures (AfricaArabia, Canada, China, Latin America) | 46 | 42 |
| **Total** | **335** | **352** |

As shown in Table 2, the total number of certified RCs in February 2016 amounts to 335, of which: 289 are contributed by European NGIs/EIROs that are Council members and 46 by integrated RPs namely: AfricaArabia, Canada, China and Latin America.

CERN is an EIRO that comprises one resource centre.

Of the 289 RCs mentioned above, 26 are contributed by Asia Pacific NGIs.

A Resource Centre is the smallest resource administration domain in an e-Infrastructure. It can be either localised or geographically distributed. It provides a minimum set of local or remote IT Services compliant to well-defined IT Capabilities necessary to make resources accessible to Users. Access is granted by exposing common interfaces to Users [GLO].

In December 2014 the total number of certified RCs was 352: this decrease may be explained by the fact that the missing sites were RCs with a low amounts of resources, both in terms of hardware and personnel, and for them it was difficult maintaining a level of service in accordance to the EGI operational level agreement[[4]](#footnote-4), so they have been suspended when the issues they are facing require more time to be solved, than it was allowed. Currently 39 RCs are in the status of suspended on GOCDB, some of them are already in the process of being re-certified. The suspension of a resource centre is needed to ensure that the services that users expect to be production ensure the level of quality required to be used productively.

We usually distinguish between two categories of services: the HTC services and the CLOUD ones. There are also some RCs that provide both kind of services, so they are counted in both the categories (Table 3).

In the following sections they will be analysed separately.

Table Number of HTC and CLOUD resource centre (February 2016)

|  |  |
| --- | --- |
| Number of HTC resource centres | 314 |
| Number of CLOUD resource centres | 21 |
| Number of HTC/CLOUD resource centres (included in the numbers above) | 7 |

## The HTC services

The HTC services offered by a resource centre can be grouped in two categories:

* Grid compute: allows users to run computational tasks on high quality IT resources, accessible via a standard interface and supporting authentication/authorization based on a membership within a virtual organization.
* Grid storage: allows files to be stored in and retrieved from high quality IT resources, accessible via a standard interface and supporting authentication/authorization based on a membership within a virtual organization.

In according to the OLA [RCOLA], each site may provide one or both of this kind of services.

The GRID compute platforms supported in EGI are: ARC, CREAM, UNICORE and GLOBUS.

Since the UNICORE and GLOBUS resources are not published in the information system, for them we can provide only the number of the certified instances registered in the GOC-DB.

The total grid compute capability is shown in the Table 4

Table EGI grid compute capacity (February 2016)

|  |  |  |
| --- | --- | --- |
|  | **Logical cores** | **HEP-SPEC 06** |
| 2014 (December) | 527248 | 4211709,28 |
| 2016 (February) | 651748 | 5841854,648 |
| Year increment | 23.61% | 38,71% |

At the end of 2014 the total amount of logical cores was 433,957, so there was an increment of more than 23%. Nevertheless the total number of RCs is slightly decreased (Table 2), the certified ones grew in size in terms of resources, increasing the total capacity of the infrastructure. As shown in Figure 1, where the logical cores and Hep-spec06[[5]](#footnote-5) power distribution is shown in as well.

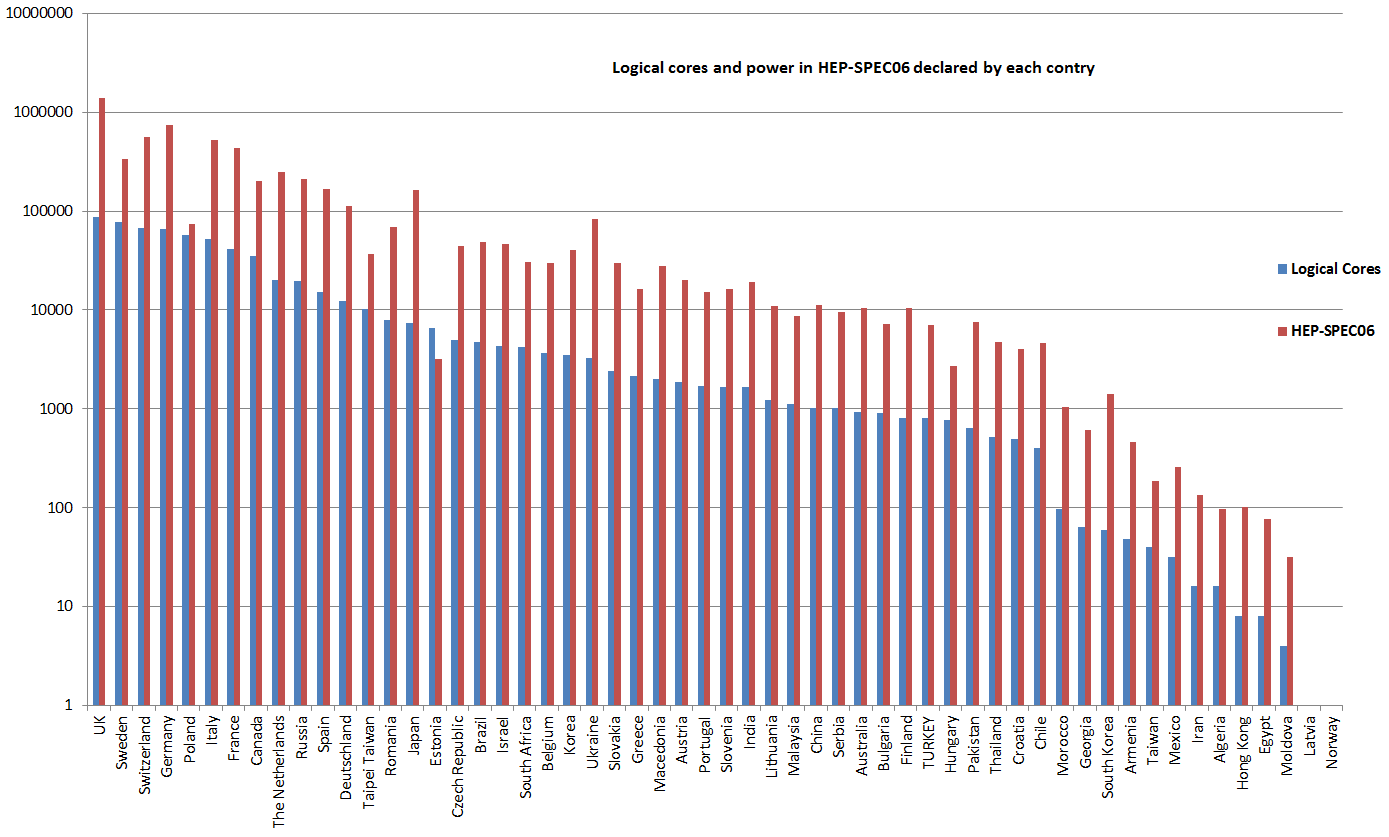


Figure , Logical cores and hep-spec power provided by each country.

Figure 2 shows the distribution of computing element types across the NGIs.

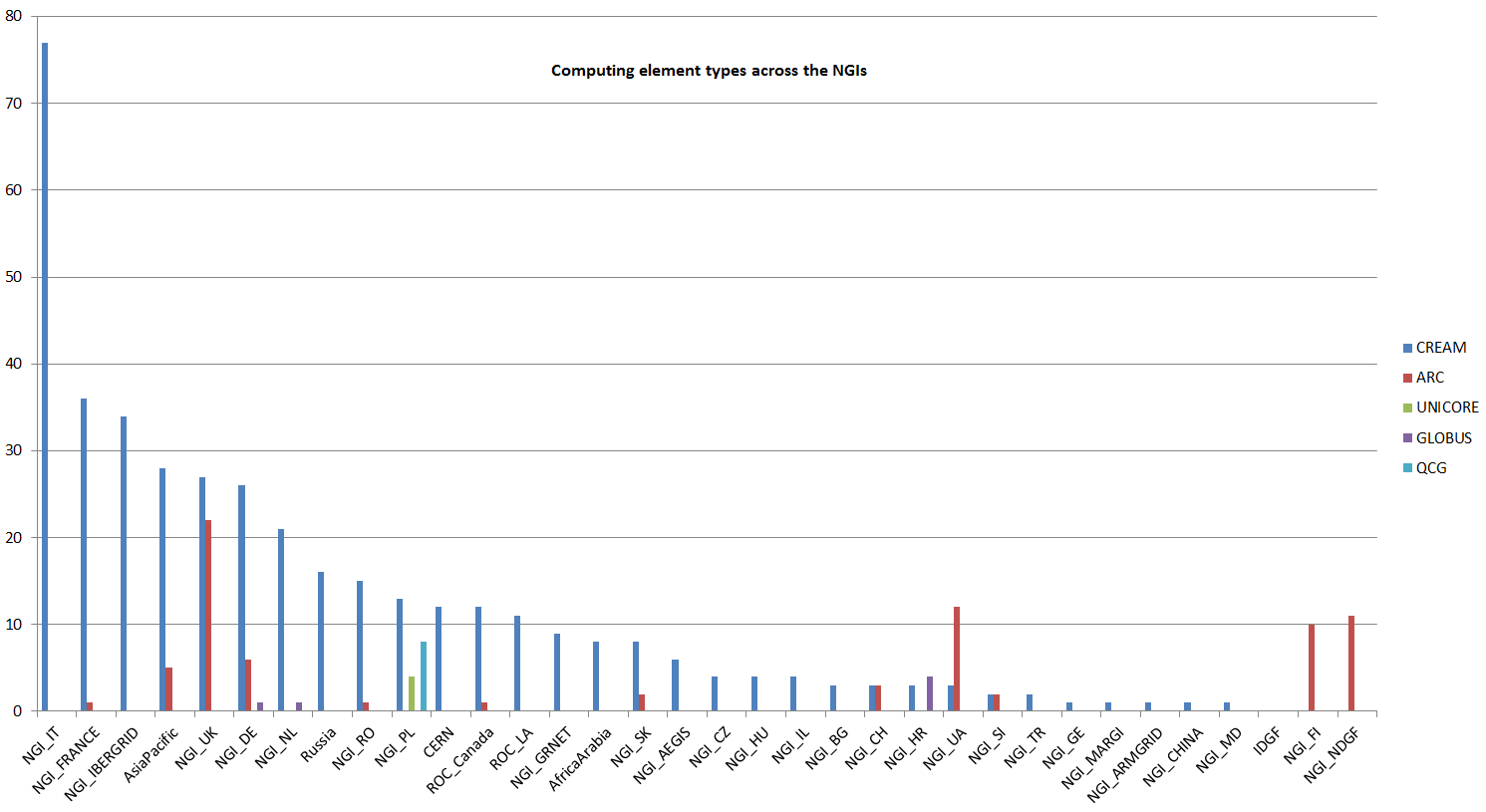


Figure computing elements distribution across the NGIs

The EGI infrastructure provides also compute resources for parallel jobs. The number of resource centres that support MPI jobs are 54 as results in February 2016 (Figure 4), or rather 67 computing elements in total. In 2014 there were 76 RCs supporting MPI: as explained above, even if the number of resource centre is decreased, there was an increment in term of compute capacity of the MPI-enabled infrastructure.

The information about MPI capabilities are not only published by services to the Information Discovery Service, but they are also registered into the EGI service registration facility (GOCDB). A more accurate mechanism to estimate the MPI support in the infrastructure is available. In addition, during 2015 a new accounting publisher was deployed that is capable of reporting accounting information of multi-core jobs. Accounting information of MPI jobs will be a more accurate indicator of the amount of parallel computing workload supported by EGI and have being published increasingly by sites during 2015.

Figure Number of RCs supporting MPI jobs (February 2016, source: GOC-DB)

Three main services are available in EGI as grid storage solutions: DPM, dCache and STORM.

The total amount of storage certified instances is 313, which correspond to a total disk capacity of about 311.7 Pb. In April 2014 the total disk capacity reported by GSTAT was 250 Pb, so there was an increase of 24.68%. Instead the total tape capacity (also called nearline storage), which is mainly provided by CERN and WLCG Tier-1 RCs amounts to 239.8 Pb. In April 2014 the corresponding value was 168.8 Pb, so the increment was 42.06%.

The distribution of disk storage resources among the EGI operations centres is shown in Figure 5, which shows that the disk capacity is concentrated across five NGIs:NGI\_IT, NGI\_UK, NGI\_DE, NGI\_IBERGRID and AsiaPacific in descending order. This may be explained by the fact that they are the larger NGIs, they have a WLCG Tier-1 and several WLCH Tier-2 RCs that offer a lot of resources.

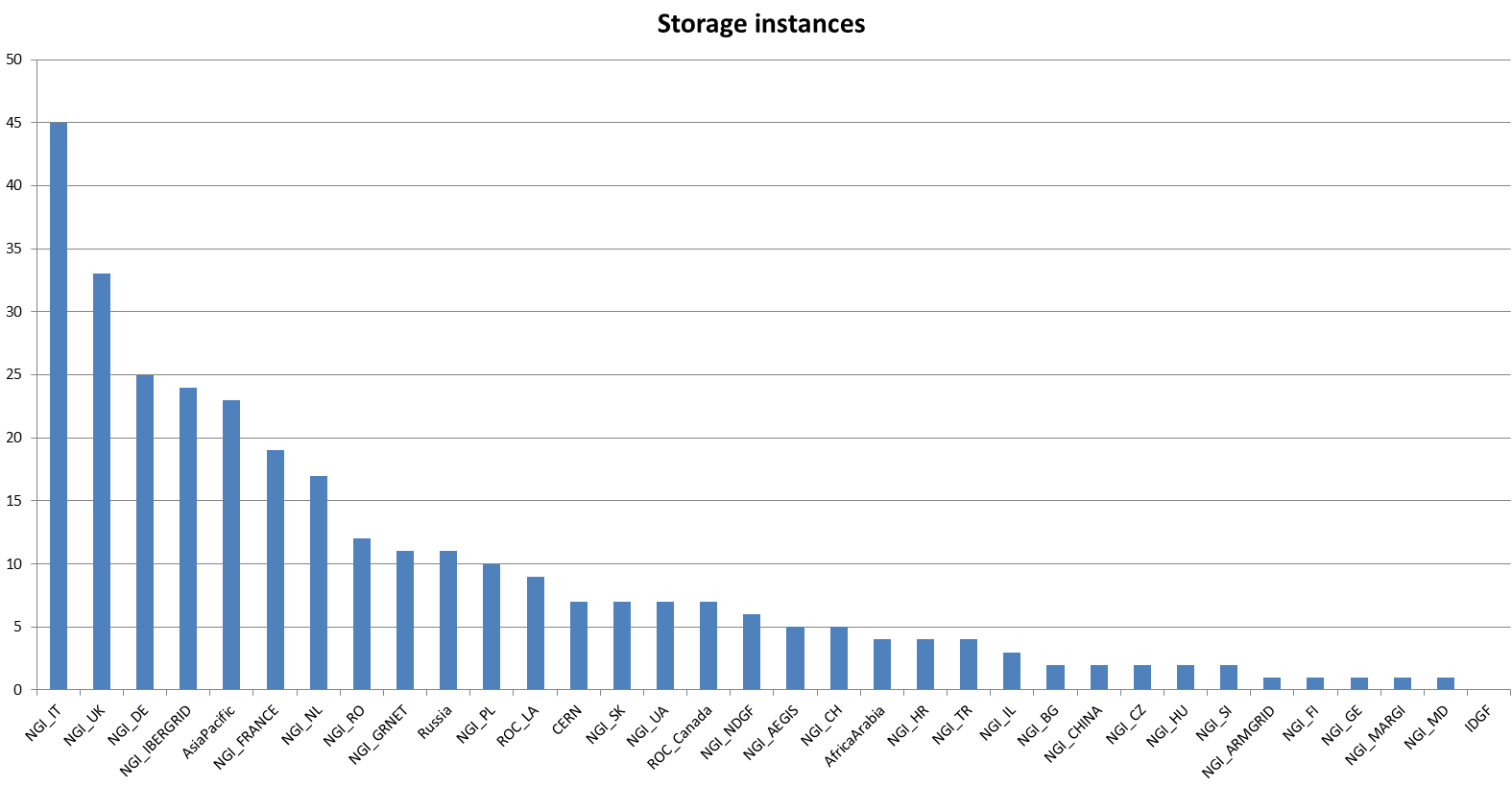
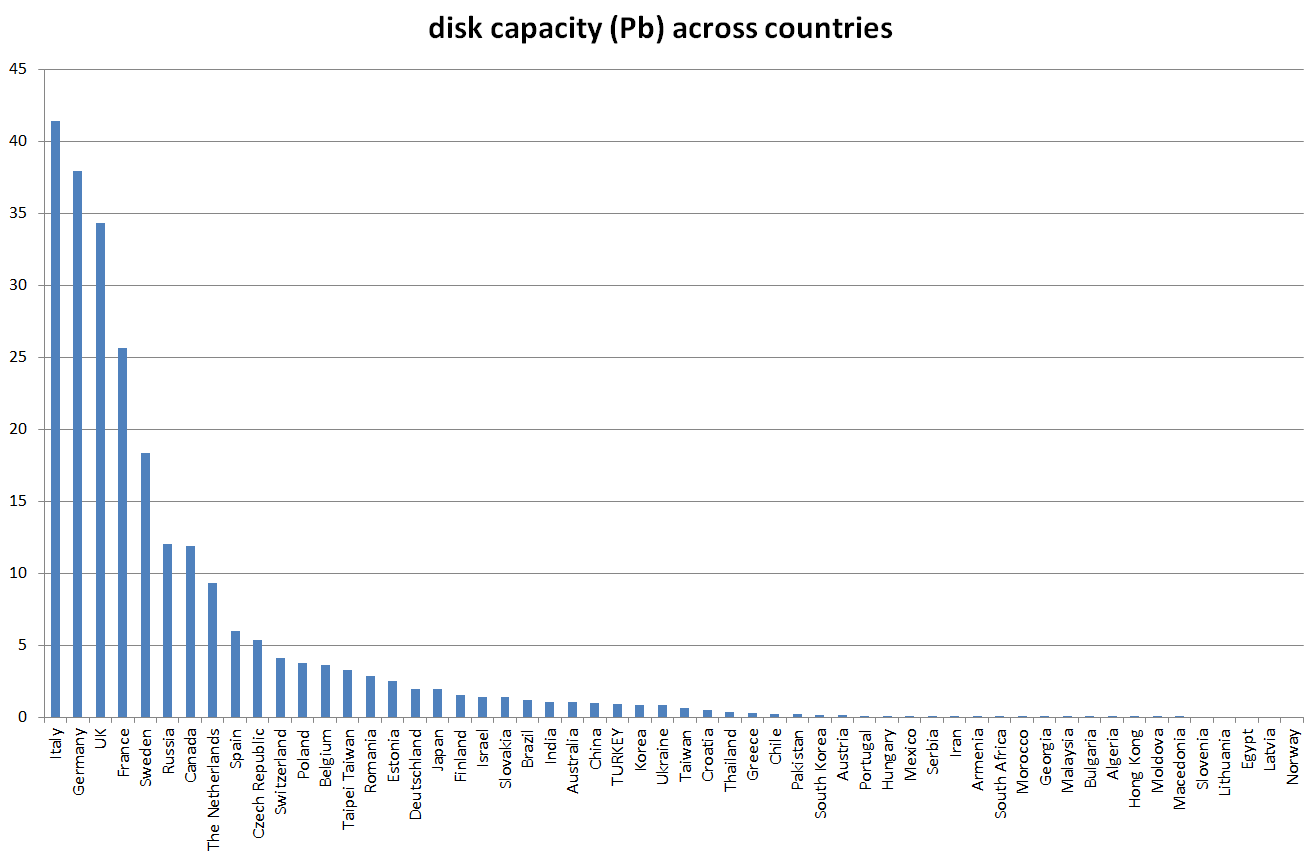


Figure certified storage elements across the NGIs (February 2016, source: GOC-DB)



Figure

Figure

Disk capacity distribution across the NGIs (source: GSTAT)

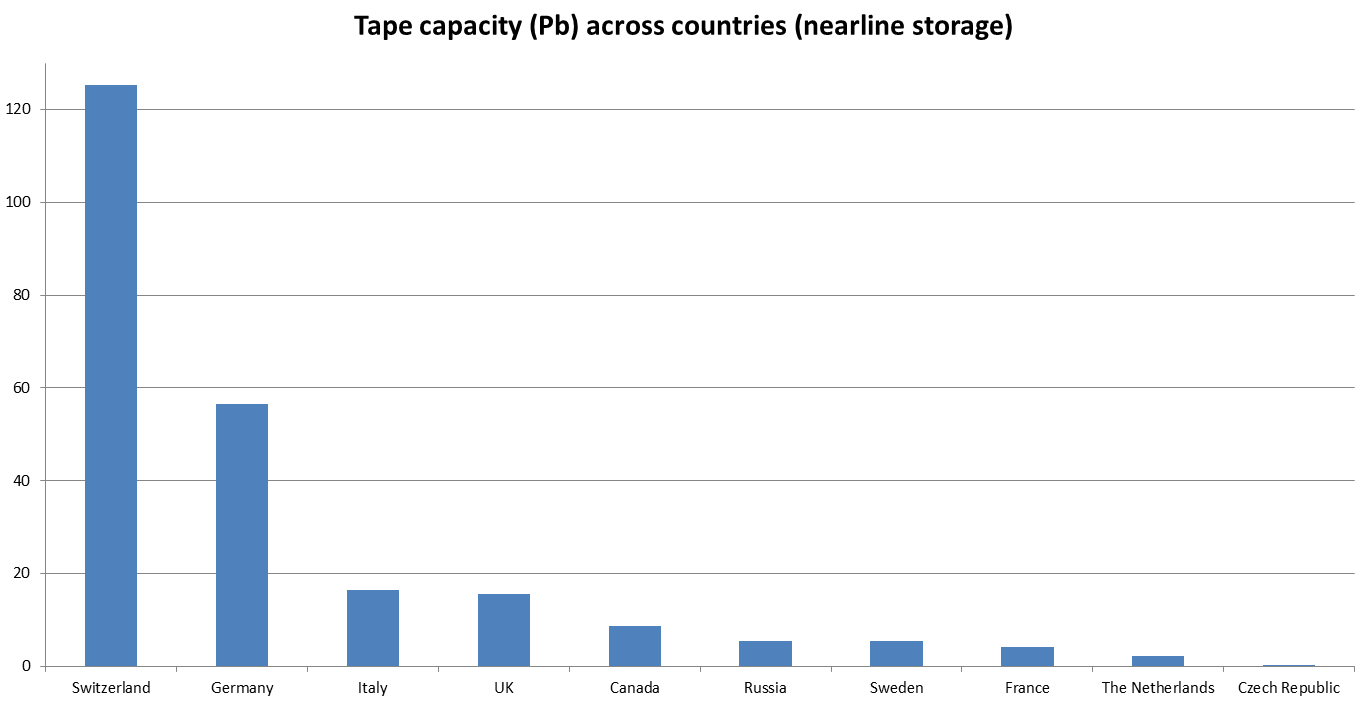


Figure Tape capacity (online storage) distribution across the NGIs (source: GSTAT)

## Cloud services

The EGI Federated Cloud is part of EGI production infrastructure, a seamless grid of academic private clouds and virtualised resources, built around open standards and focusing on the requirements of the scientific community. It is **in production** since mid May 2014.

The Federated Cloud is targeted at researchers and research communities that need to access digital resources on a flexible environment, using common standards to support their data- and computing intensive experiments.

Several resource centres joined to the Federated Cloud since its beginning: currently (beginning of February 2016) 21 RCs are part of the cloud infrastructure (Table 5) and other sites, undergone to the certification procedure (https://wiki.egi.eu/wiki/PROC09), will join soon (Table 6). From Table 5 we can see how the Federated cloud activity is led, in terms of resource provisioning, by IBERGRID, NGI\_IT, NGI\_SK and NGI\_DE.

A CLOUD resource centre provides to the community at least one kind of these facilities:

* Cloud compute: an Infrastructure-as-a-Service (IaaS) for the scientific community. The service allows scientists to allocate virtual servers on demand, with customizable set of hardware, network and storage resources.
* Cloud storage: is an Infrastructure-as-a-Service for the scientific community. It allows end-users and service providers to store files, images and other generic objects that can be accessed from any device with integrated basic processing capabilities.

Resource centres are free to use any Cloud Management Framework with the requirement that the CMF exposes interfaces compliant to the FedCloud standards[[6]](#footnote-6).

Common CMF used are OpenStack and OpenNebula, but also Synnefo is supported in the federation. The common interfaces provided to access the virtualized resources are Open Cloud Computing Interface (OCCI) and Cloud Data Management Interface (CDMI).

Table Federated CLOUD resource centres

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Resource Centre** | **NGI** | **Number of cores declared** | **Amount of disk space declared** | **Cloud Management Framework** |
| 100IT | NGI UK | 120 | 16 Tb | OpenStack |
| BIFI | NGI IBERGRID | 720 | 36 Tb | OpenStack |
| CESGA | NGI IBERGRID | 448 | 6 Tb | OpenStack |
| CESNET-MetaCloud | NGI CZ | 416 | 56 Tb | OpenNebula |
| CETA-GRID | NGI IBERGRID | 184 | 5 Tb | OpenStack |
| CYFRONET-CLOUD | NGI PL | 200 | 20 Tb | OpenStack |
| FZJ | NGI DE | 216 | 50 Tb | OpenStack |
| GoeGrid | NGI DE | 192 | 40 Tb | OpenNebula |
| HG-09-Okeanos-Cloud | NGI GRNET | 70 | 1 Tb | Synnefo |
| IFCA-LCG2 | NGI IBERGRID | 2288 |  | OpenNebula |
| IISAS-FedCloud | NGI SK | 176 | 50 Tb | OpenStack |
| IISAS-GPUCloud | NGI SK | 96 | 6 Tb | OpenStack |
| IN2P3-IRES | NGI FRANCE | 192 | 5 Tb | OpenStack |
| INFN-CATANIA-NEBULA | NGI IT | 16 | 5 Tb | OpenNebula |
| INFN-CATANIA-STACK | NGI IT | 16 | 16 Tb | OpenStack |
| INFN-PADOVA-STACK | NGI IT | 144 | 5 Tb | OpenStack |
| MK-04-FINKICLOUD | NGI MK | 100 | 1 Tb | OpenNebula |
| NCG-INGRID-PT | NGI IBERGRID | 80 | 3 Tb | OpenStack |
| PRISMA-INFN-BARI | NGI IT | 300 | 50 Tb | OpenStack |
| TR-FC1-ULAKBIM | NGI TR | 336 | 40 Tb | OpenStack |
| UPV-GRyCAP | NGI IBERGRID | 128 | 5 Tb | OpenNebula |
| **Total declared** |  | **6438** | **416 Tb** |  |

Table Resource centres in the certification phase

|  |
| --- |
| **RCs under integration process in the Federated Cloud** |
| RECAS-BARI: new name of PRISMA-INFN-BARI |
| SCAI: moving its resources from HTC to CLOUD |

In a distributed, federated Cloud infrastructure, users will often face the situation of efficiently managing and distributing their VM Images across multiple resource providers. Users need a catalogue of Virtual Machine images (VMIs) that are usable on the IaaS cloud provider sites and encapsulate those software configurations that are useful and relevant for the given community. (Typically pre-configured scientific models and algorithms). To maximise usability of VMIs across cloud sites the images should be in a format that’s supported at every federation member site (Or at least can be converted to such formats). Users also need a system that automatically replicates VMIs from the VMI catalogue to the federation member sites, keeps them updated or removes them when not needed anymore. Automated replication can ensure consistency of capabilities across sites and it is being coupled with a VMI vetting process to ensure that only properly working, and relevant VMIs are replicated to the cloud sites of the community.

The EGI AppDB service has been extended to a Virtual Appliance Marketplace which are virtual machine images designed to run on a virtualization platform, that provide a software solution out-of-the-box, ready to be used with minimal or no set-up needed within the EGI Federated Cloud infrastructure.

AppDB's Virtual Appliance Marketplace provides the ground for managing and publishing versioned repositories of virtual appliances, in a way that integrates with the existing HEPiX [VMCaster](https://github.com/hepix-virtualisation/vmcaster) / [VMCatcher](https://github.com/hepix-virtualisation/vmcatcher)[[7]](#footnote-7) framework, currently in use by the EGI.

Research Communities ultimately create and update VM Images stored the Research Community, publish a VM Image list using AppDB. Federated Clouds Resource Provider use these lists to make the VMI available for instantiation at site level for the VOs there supported, this process is automated through VMCaster/VMCatcher.

The CLOUD resource information published in the BDII are following the GLUE2 schema, and EGI Federated Cloud is working within the GLUE2 WG in OGF to further extend the schema (the so-called 2.1) to represent Cloud Computing, Storage and in the future Platform and Software services. The proposed extensions are currently under discussion in the WG.

All cloud services are registered in GOCDB and are monitored with a cloud-specific instance of SAM-NAGIOS: the monitoring service is an instance of the SAM production distribution, with in addition a set of cloud-specific probes. It is on going the process of the activation of a central monitoring instance based on ARGO framework, phasing out all the SAM regional instances.

## Capacity consumption

EGI accounting information are gathered and stored centrally and accessible through the accounting portal[[8]](#footnote-8). Accounting information is aggregated by Operations Centre, whose list is obtained from GOCDB.

Table Compute resource usage in the last three years

|  |  |  |  |
| --- | --- | --- | --- |
|  | **2015** | **2014** | **2013** |
| **Total normalized CPU wall clock time consumed (Billion HEP-SPEC 06 hours)** | 20.56 | 16.27 | 14.62 |
| **Total number of jobs (Million)** | 584.9 | 535 | 522.8 |
| **Average number of jobs per day (Million)** | 1.60 | 1.47 | 1.43 |

The overall quantity of computing resources used in 2015 amounts to 20.56 Billion HEP-SPEC 06 Hours as shown in Table 7, with an increment of 26% from 2014 (the increment in the 2014 compared to 2013 was 11%). The total number of jobs executed on the infrastructure is 584.9 Million, which corresponds to an average of 1.60 Million job/day.

The increase of the wall clock time registered in 2015 (20%) higher than the increased number of jobs (~10%) may be explained by the submission of multi-core jobs that consume more resources than the single core ones. During the 2015 the number of multi core/parallel jobs has increased.

It is reported in Figure 7 and in Figure 8 the monthly trends about the HEP-SPEC06 hours usage and the number of jobs of the last 3 years respectively. The less increasing trend of the number of jobs can be explained by the increasing popularity of parallel jobs, which use more resources than jobs running on a single job slot. CPU time has increased constantly.

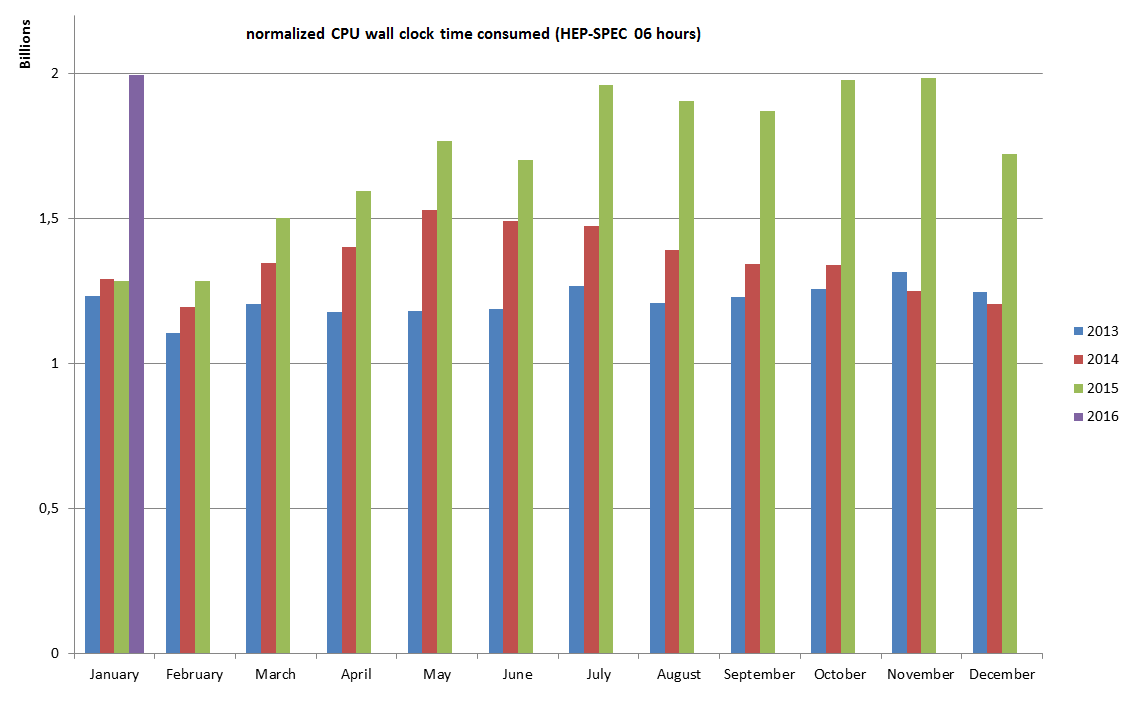


Figure HEP-SPEC 06 Hours monthly usage of the last three years (source: accounting portal).

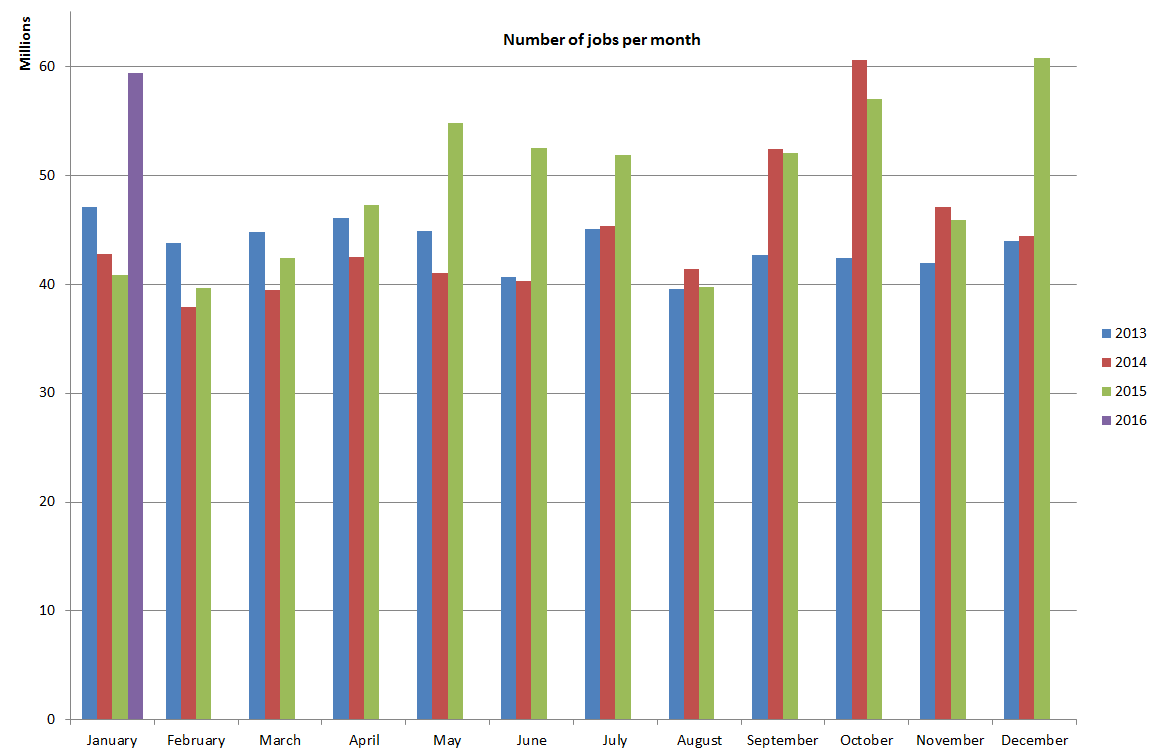


Figure Number of jobs per month of the last three years (source: accounting portal)

The diagrams in Figure 9 and in Figure 10 shows the total number of jobs per VO and per Operations Centre respectively, in the period between January 2015 and January 2016.

The usage expressed in HEP-SPEC 06 Hours of CPU wall time across the various resource infrastructures of EGI is plotted in Figure 11, where infrastructures are grouped by operations centre. The diagram also shows the distribution between the four LHC VOs atlas, cms, alice and lhcb (red bars) and the other VOs (blue bars).

The most used infrastructure by the several disciplines (in decreasing order): NGI\_DE, NGI\_UK, NGI\_IT, NGI\_FRANCE and CERN. Usage distribution naturally reflects availability of installed capacity (Section 2.2), however the level of multidisciplinary support varies considerably across the infrastructures. Figure 12 plots the distribution of used HEP-SPEC 06 CPU wall clock hours of non-HEP user communities. NGI\_IT is the infrastructure with the largest absolute amount of resources used by non-LHC communities with almost 626 Million CPU wall time hours, followed by NGI\_DE, NGI\_FRANCE, NGI\_UK and NGI\_TR.

The Figure 13 shows how support of LHC VOs and high energy physics is dominant in large resource infrastructures, while other disciplines dominate in various countries in Eastern-South Europe. The smallest NGIs in terms of number of sites usually support only few VOs, making some NGIs almost discipline-specific. Instead the larger NGIs that include also important RCs and more regional scientific communities, have the possibility to provide resources to more kind of users.

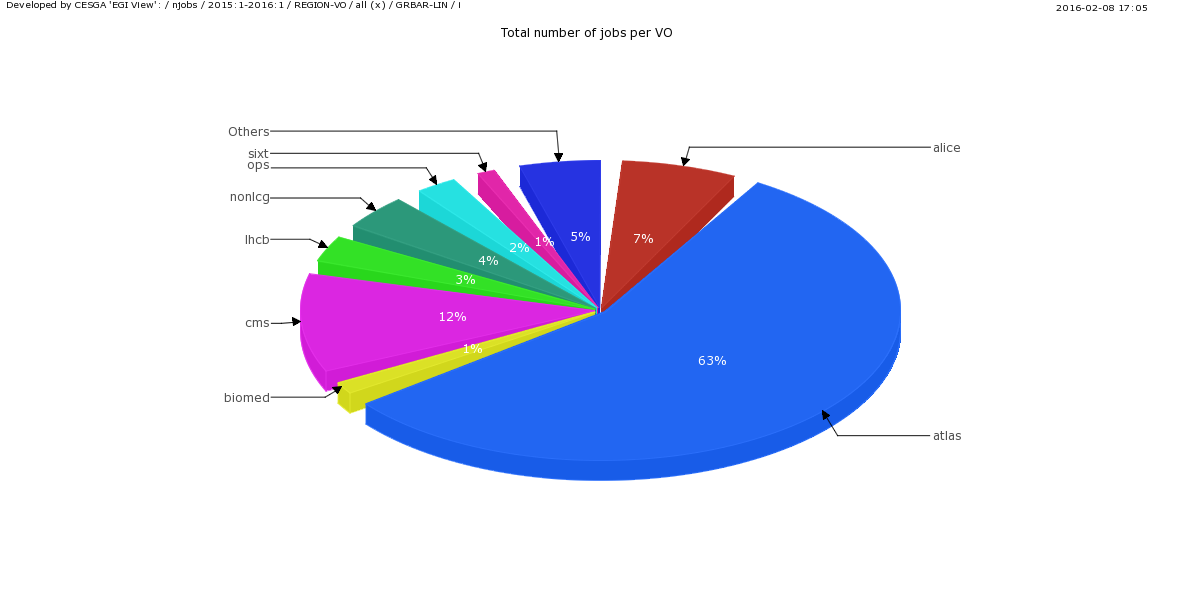


Figure Total number of jobs per VO (Jan 2015 - Jan 2016, source: Accounting Portal)

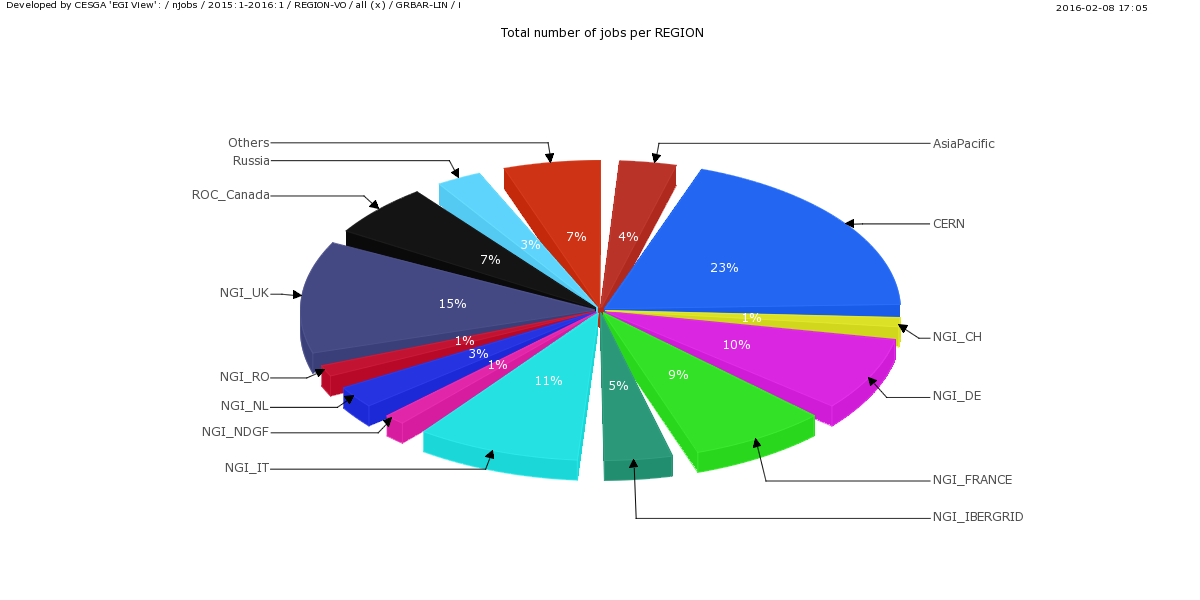


Figure Total number of jobs per NGI/EIRO (Jan 2015 - Jan 2016, source Accounting Portal)

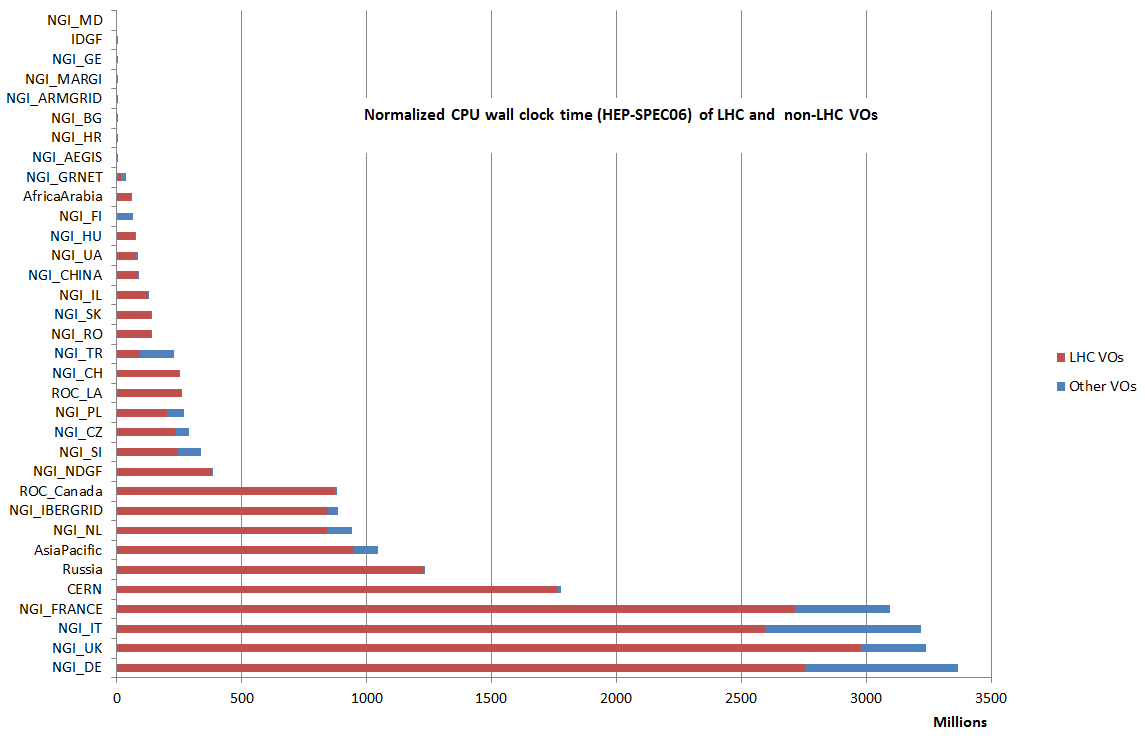


Figure HEP-SPEC 06 Hours from January 2015 to January 2016 (source: accounting portal). LHC VOs usage is displayed in red while the aggregated usage of the rest of VOs is in blue

Figure Distribution across EGI Operations Centres of aggregated usage of non-LHC VOs (CPU wall clock time in HEP-SPEC 06 hours) from January 2015 to January 2016 (source: accounting portal).

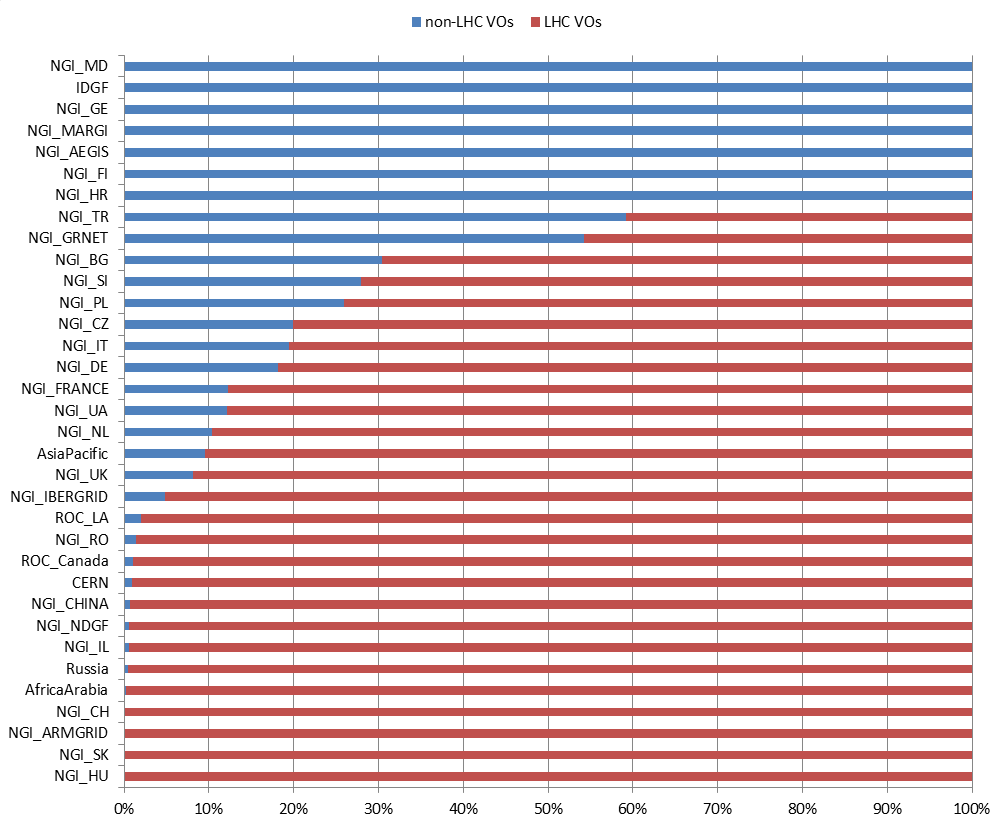


Figure Distribution of resource usage (%) across HEP and non-HEP VOs from January 2015 to January 2016 (source: accounting portal).

As mentioned before, during 2015 it was implemented the accounting of multicore jobs: the not-normalized CPU time consumed by this kind of jobs is reported inFigure 11,while in Figure 12 there is a comparison of used resources between the single and multi-core jobs.

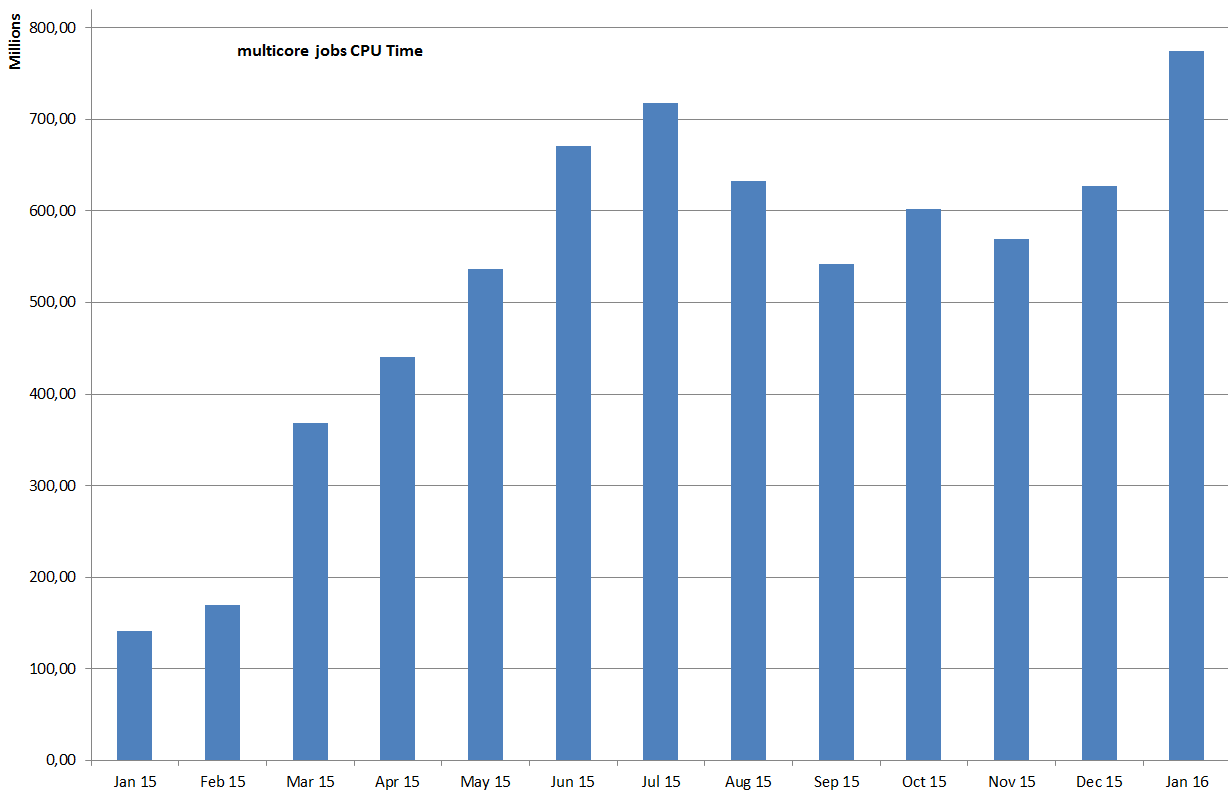


Figure SUM Normalised Elapsed Time \* number of processors

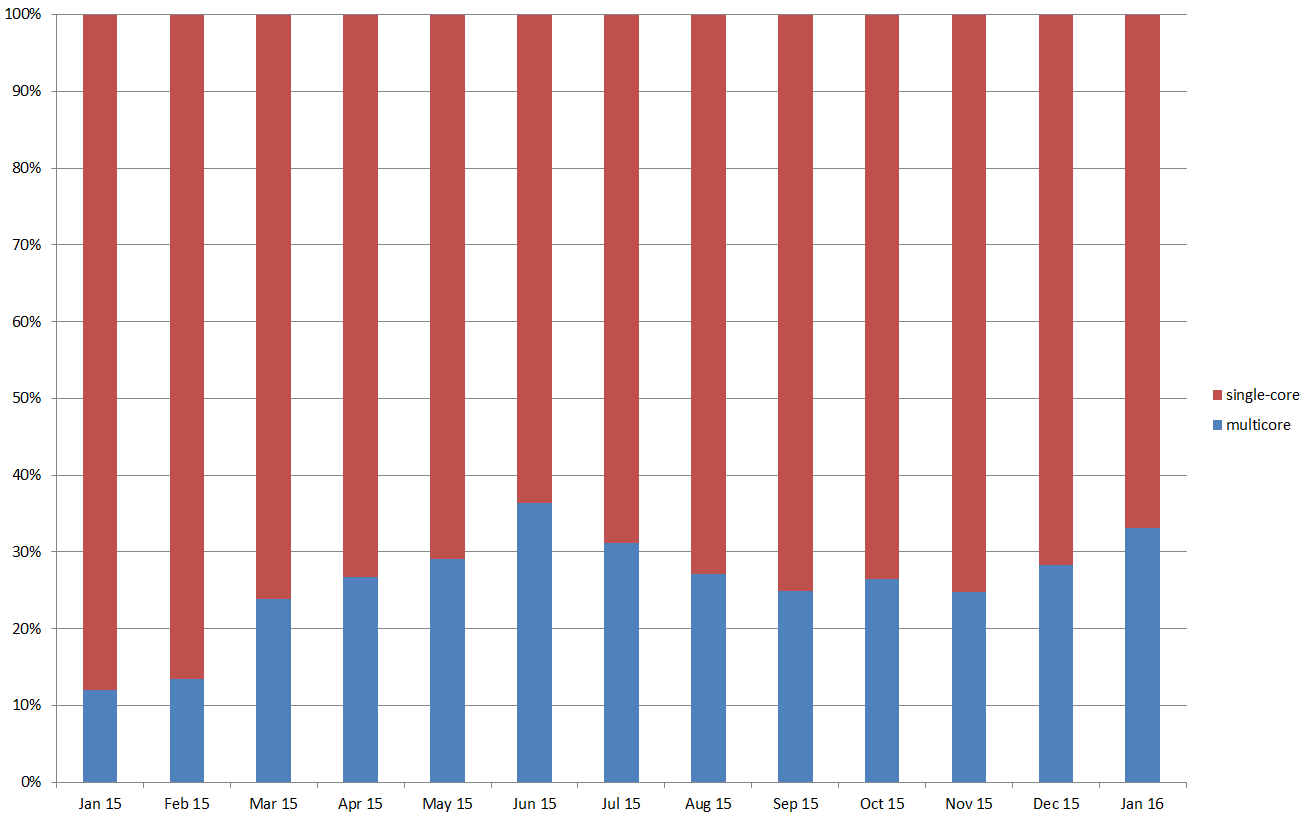


Figure resource percentage utilization of single and multi-core jobs.

The number of virtual machines instantiated since January 2015 is shown in Figure 12, instead in Figure 13 it is displayed the percentage SUM CPU time spent in the Federated CLOUD.

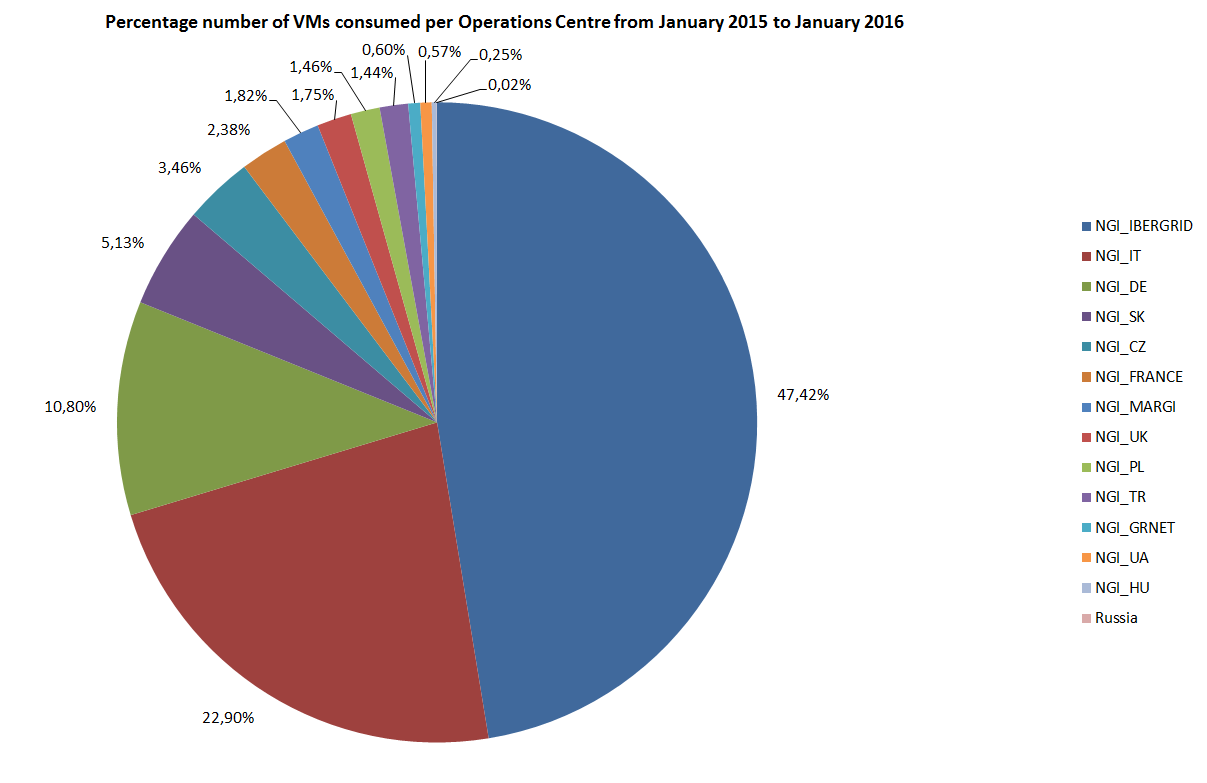


Figure VMs instantiated in the Federated CLOUD per Operations Centre from January 2015 to January 2016 (source: accounting portal)

|  |  |
| --- | --- |
| **Cloud usage during 2015** | |
| Total # of VMs instantiated | 557,836 |
| Total CPU time consumed (CPU hours) | 1924000 |

Table Overall usage of the federated cloud resources between Jan 2015 and Jan 2016

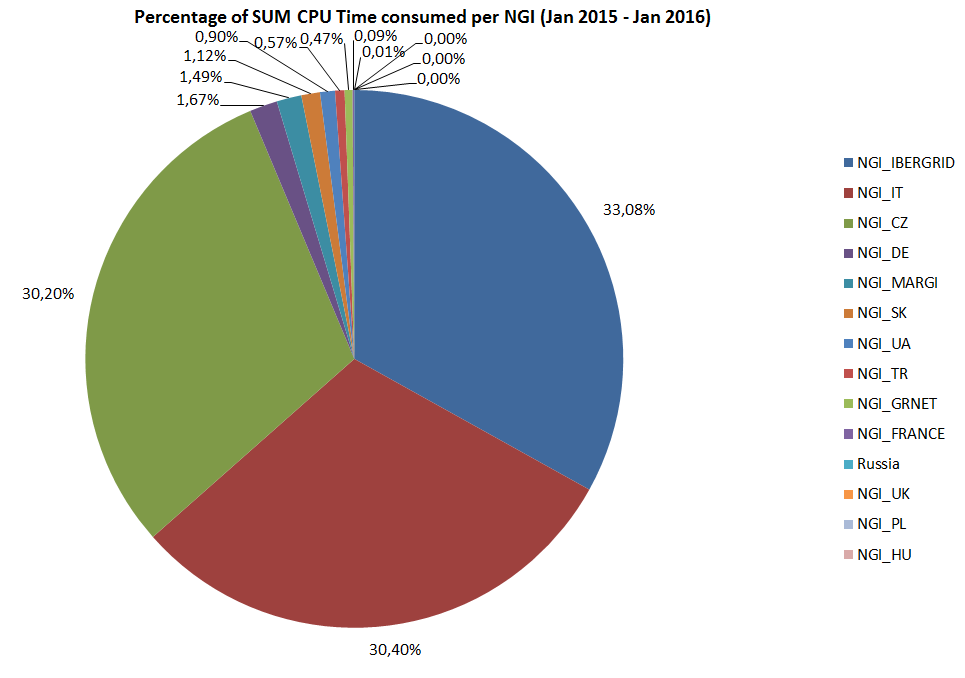


Figure Percentage of SUM CPU Time consumed through cloud services per NGI from January 2015 to January 2016 (source: accounting portal).

## Disciplines, Virtual organizations and users

This section provides information about the evolution of the user community (users registered in VOs) in some of the main scientific disciplines currently identified by EGI at the infrastructure level, namely: Engineering and Technology, Medical and Health Sciences, Natural Sciences, Agricultural Sciences, Social Sciences, Humanities, Support Activities and Others[[9]](#footnote-9).

The overall number of international and national VOs registered in the Operations Portal[[10]](#footnote-10) at the beginning of February 2016 amounts to 233.

The use of gateways to provide users with a native user-friendly environment to the infrastructure services is increasing. Quite often user portals provide users with the capability of using institutional credentials to authenticate themselves, these credentials are then mapped to robot certificates (often owned by the VO managers). By doing so it is not necessary for an user the request of a personal X.509 certificates and the registration to a VO: this contributes to increase the user friendliness of the platforms. Use of robot certificates is internally accounted for by the portals in compliance to the VO Portal policy. In February 2016 the number of robot certificates embedded in user gateways is 157; robot certificates are used by 51 VOs in total. Almost 11,000 users can potentially use scientific gateways; this is increased by the number of registered users to active VOs, which amounts to be 46246 in February 2016.

The increase in the number of Robot Certificates indicates that users, in particular new user and communities, are looking for alternative authentication mechanisms different from the X.509 certificates. This is also signal for EGI to explore different authentication technologies in the future, or to work on a better integration of robot certificates with the production infrastructure.

The diagram in Figure 16 shows the trend in use of robot certificates and VOs since November 2011.

Figure Use of robot certificates and related VO in EGI since EGI-InSPIRE PY1.

### VOs and user distribution across scientific fields

The distribution of VOs per discipline is illustrated in Figure 17

Figure Distribution of number VOs per discipline (February 2016, source: Operations Portal).

The largest discipline in terms of number of registered users is Natural Sciences (65.98%): it is remarkably larger than the other ones because it includes 153 VOs (more than the half of the total VOs). Then there is the Support Activities discipline (9.09%), followed by Medical and Health Science (6,46%) and by Engineering and Technology (6.32%). The complete users distribution is shown in the Figure 18

Figure Users distribution per discipline (February 2016, source: Operations Portal)

### Resource utilization per disciplines

In Table 8 and in Figure 11 it is reported the resources usage in 2015 by the 10 most used disciplines compared with the one in 2014: the larger disciplines augmented the usage in 2015.

The monthly 2015 resources usage in HEP-SPEC hours by High Energy Physics disciplines is shown in Figure 12, while in Figure 13 it is reported the resources utilization of Natural Sciences disciplines (excluded Physical Sciences) for the last two years.

Table Comparison between normalised CPU time utilization in 2015 and in 2014 by 10 most used disciplines: percentage increment or decrement (source: accounting portal), ordered by utilization.

|  |  |
| --- | --- |
| **DISCIPLINE** | **Norm. CPU time 2015**  **compared to 2014** |
| Physics | 28,93% |
| High Energy Physics | 31,72% |
| Particle Physics | 27,96% |
| Nuclear Physics | 43,06% |
| Space Science | 12,33% |
| Astrophysics | 12,33% |
| Astronomy | 9,20% |
| Neurosciences | -38,34% |
| Medical imaging | -38,45% |
| Comput. chemistry | -30,94% |

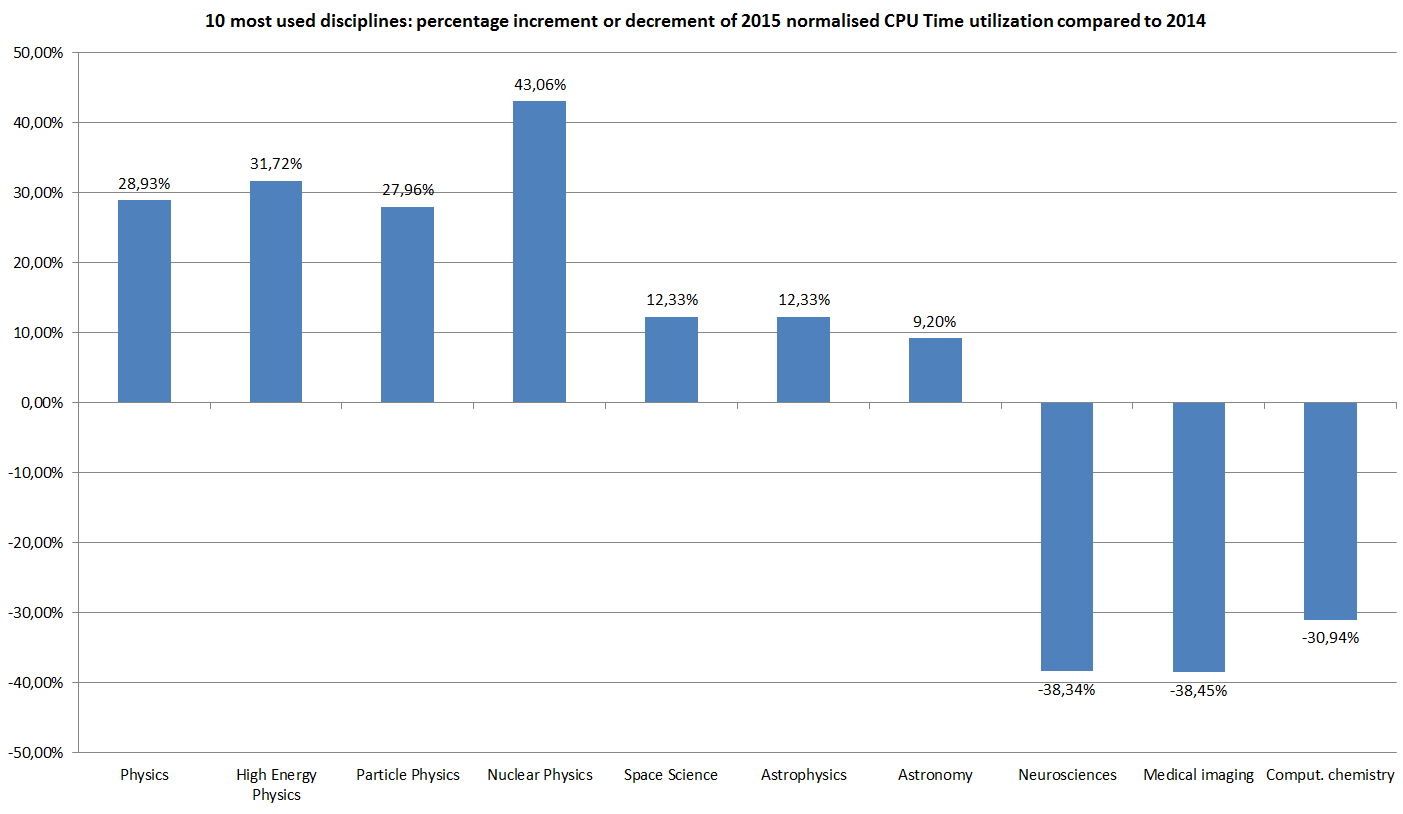


Figure 2015 increment or decrement of normalised CPU time utilization compared to 2014 by 10 most used disciplines

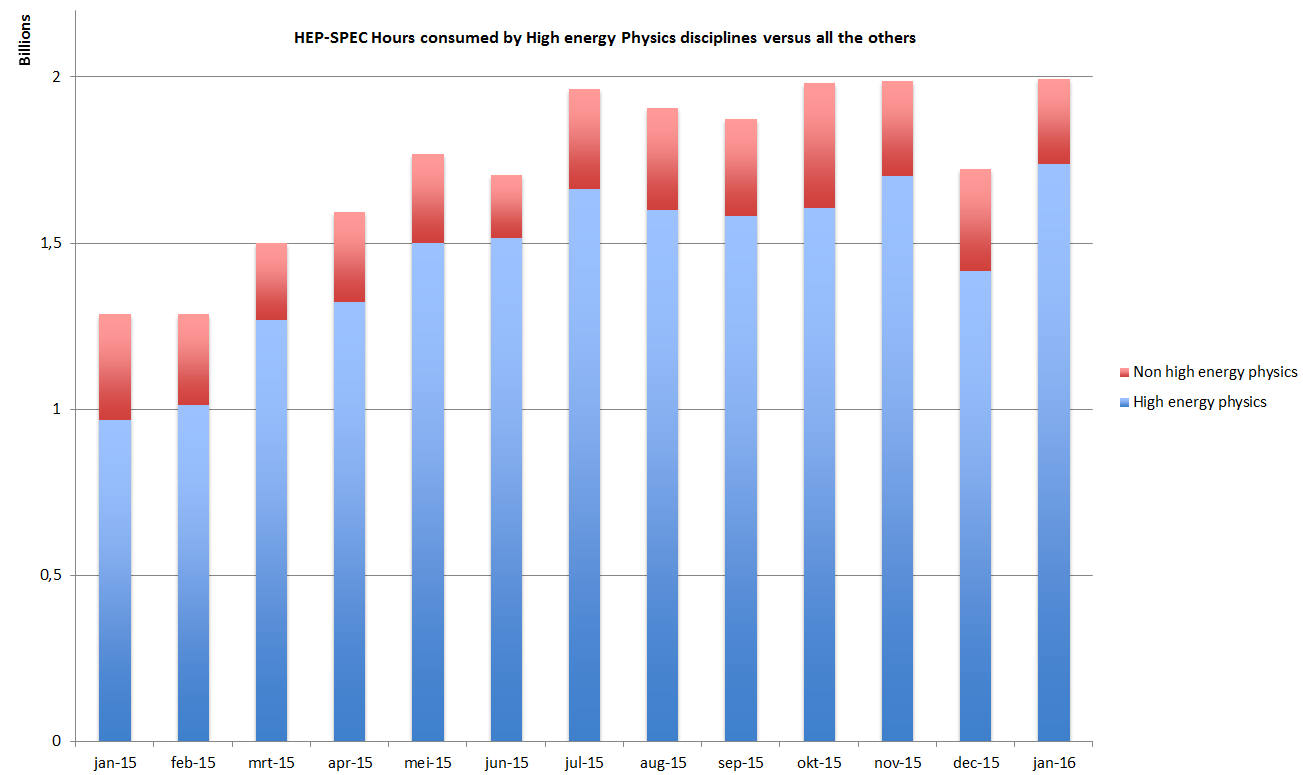


Figure High energy Physics usage compared with all the other disciplines.

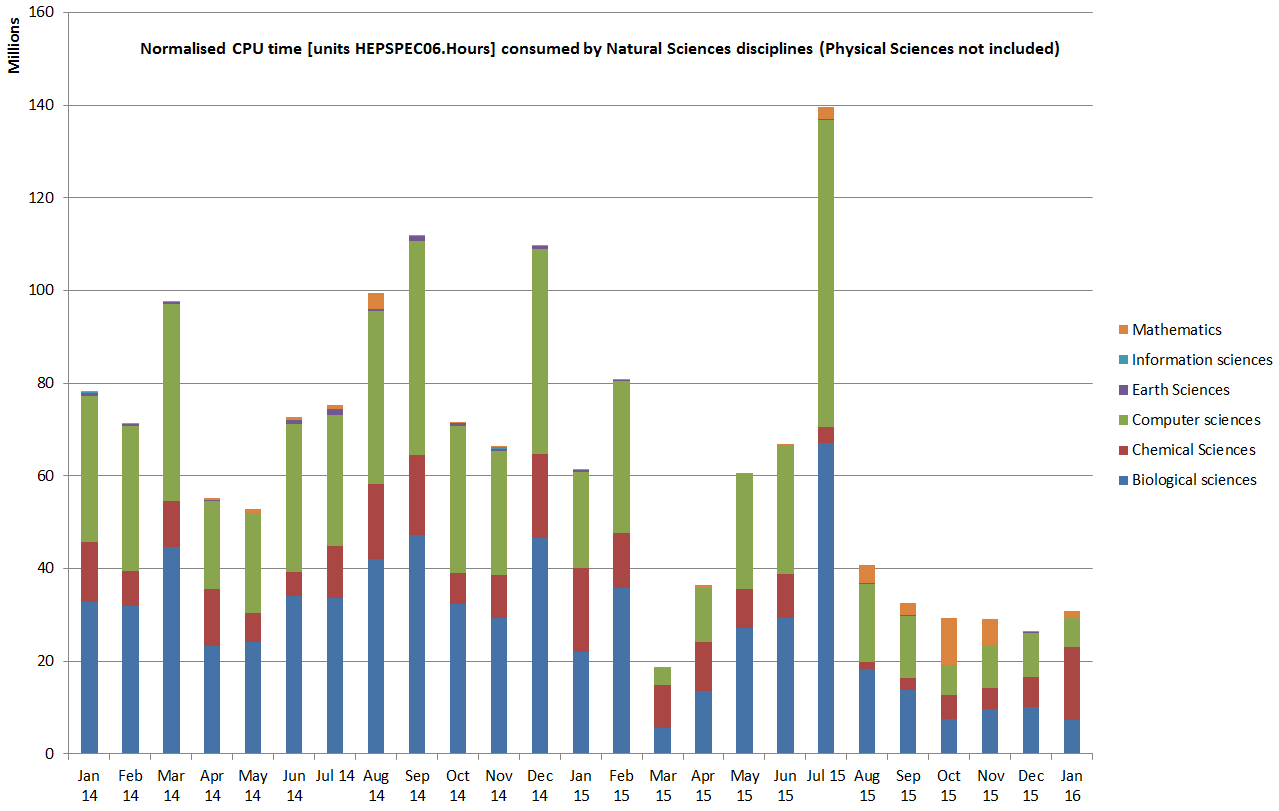


Figure Natural Sciences disciplines resources usage (Physical Sciences excluded).

## Service level availability performances

Services are monitored at three different levels:

* Resource Centre Services;
* Resource infrastructure Provider Services
* EGI.eu Services.

For each category a different set of service level and targets are defined and periodically reviewed (see the chapter 3 for details). For each set of service levels various reporting systems are available, and are detailed in the following section. The service levels and targets – summarized in (capitolo 3), are formally defined in the RC Operational Level Agreement [RCOLA], in the RP Operational Level Agreement [RPOLA] and EGI.eu Operational Level Agreement.

### RCs availability and reliability

The quality of grid services deployed by Resource Centres is being measured since 2008 with availability and reliability metrics, computed from the results of periodic tests performed at all certified centres through the Service Availability Monitoring framework (SAM) [SAM]. Availability and reliability metrics were defined to quantitatively express the level of functionality delivered by grid services to end-users with the ultimate goal of identifying areas of the infrastructure needing improvement.

The capability of closely reflecting the experience of the end-user depends on the tests performed. The EGI monthly availability and reliability reports are based on tests (run using the OPS VO), which are sufficiently generic to allow a comparison across all Resource Centres of the infrastructure.

Availability of a service (or a site, depending on the level of aggregation) represents the percentage of time that the services (or sites) were up and running ([uptime / total time] \* 100), while Reliability is the percentage of time that the services (or sites) were supposed to be up and running, excluding scheduled downtime for maintenance and other purposes ([uptime / (total time – scheduled down time)] \* 100) [AVL].

Certified Resource Centres guarantee 80% availability and 85% reliability for their services. The minimum availability and reliability values accepted for a Resource Centre are defined in Operational Level Agreements established with EGI.eu.

Increasing the overall performance delivered to users has been an on-going effort since the introduction of service level management.

The trend of the overall EGI RC availability and reliability is shown in Figure 19 and in Figure 20

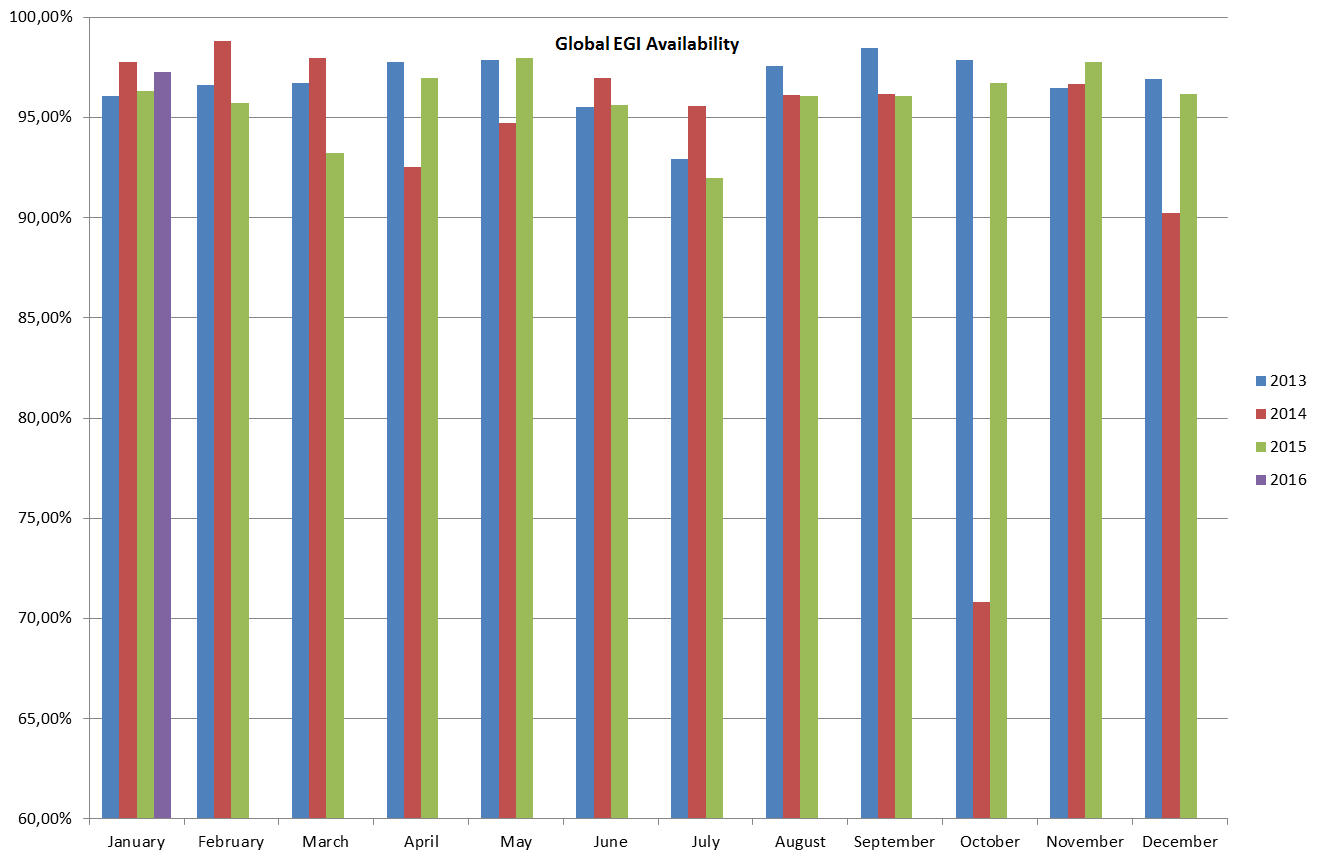


Figure Monthly Availability of resource centres averaged across EGI.

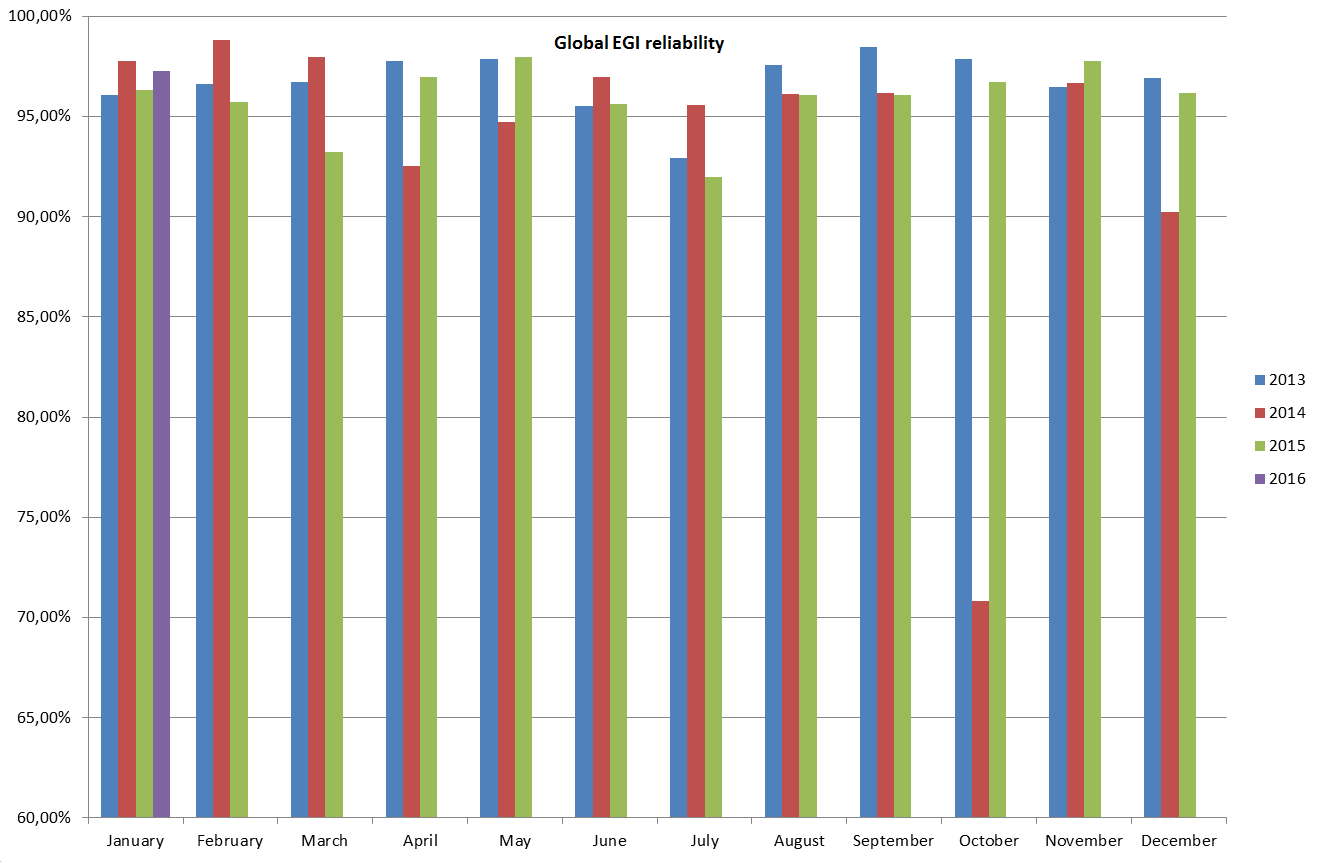


Figure Monthly Reliability of resource centres averaged across EGI, for the last three years.

The overall average availability of the EGI production infrastructure have been above 95% for almost all the months of 2015. Although it has not improved significantly from the previous year, average 95% of availability is a good result considering that the highly distributed nature of the infrastructure allows users to use another site if one is not available. Moreover availability is also strictly considering all the site’s services, and – for example – if a user is using only the computing services may not be affected by an outage of the storage services.

Figure Monthly availability and reliability trends of Federated CLOUD.

Figure 17 shows the availability and reliability trends for the cloud RCs: differently from the values computed for the EGI Production Infrustructure, they are not weighted on the size of RCs, so that small RCs influence the global trends in the same way than the bigger ones; besides the occurrence of problems in small RCs is higher than in the larger ones, so this explains why the average availability and reliability figures of Federated CLOUD are lower than the EGI ones.

. As already written, the Federated Cloud Infrastructure started in mid-May 2014. The reports were produced separately from the EGI production infrastructure ones because the Federated Cloud was a test environment during the first part of its life, but in the second half of 2015 there was a general improvement of the quality of the service provided. By now the federated CLOUD reached such a level of maturity to be included in the global EGI availability and reliability computation. It was proposed in the January 2016 OMB to apply to the CLOUD RCs the same follow-up procedures valid for the HTC RCs, and this is expected to become valid starting from June 2016.

# Evolution in the operations coordination

The operations of the EGI production infrastructure develop at different levels:

* Infrastructure level operations: coordinated by EGI.eu
* National level operations: operated by the NGI Operations Centres (NOC)
* Site level operations: operated by the site staff

This sections focuses on the operations at infrastructure level, which components are:

* Operational procedures and processes
* Core services
* Software provisioning and distribution

## Evolution of the operational procedures and processes

Documents are produced by EGI Operations to establish coherent and repeatable procedures for the partners of EGI. While manuals are technical documents that provide guidelines focused on a specific task, procedures are step-by-step descriptions of processes requiring actions from several partners. The purpose of a procedure is to define a workflow. Procedures are approved by the OMB and periodically reviewed. Appliable areas for procedures are:

* Ticket management
* Operations Center Management
* Resource Centre Management
* Availability and monitoring
* Security Incident Handling
* Vulnerability Issue Handling ed Questions”)

In the first year of the project, the evolution of the operational procedures have mainly focused to the cloud services, both in terms the definition of new procedures and processes and on the integration and harmonization with the pre-existing operational infrastructure.

The documents listed below represent new documents or old documents revised during the last year. They are collected under the EGI Operations Documentation <https://wiki.egi.eu/wiki/Documentation> , under which the whole list of documents can be browsed (23 Procedures, 12 Manuals, 18 HOWTOs, 10 "Frequently Asked Questions”).

|  |  |  |
| --- | --- | --- |
| Title | New or Updated | Description |
| Setting up Cloud Resource Centre <https://wiki.egi.eu/wiki/MAN10> | Updated | It provides very detailed instructions to set up a Resource Centre from the beginning, with references to the diverse technologies available in the EGI Federated Cloud. Contributions come from both developers of the tools and the RC admins themselves. The steps to set up a cloud RC in the EGI Federated Cloud is now well known and straightforward. |
| Per-User Sub-Proxy <https://wiki.egi.eu/wiki/MAN12> | New | This manual shows how to set up a per-user sub-proxy (PUSP), which allows identification of the individual users under a common robot certificate. This new feature, defined and developed in the Federated Cloud context, allows a web portal to map a group of users (i.e. VO users) creating a proxy credential from the robot credential. This is fundamental to enable *science gateways*. |
| Quality verification of monthly availability and reliability statistics <https://wiki.egi.eu/wiki/PROC04> | Updated | The document describes the process of how to handle justification for poor monthly performance, with the goal of maintaining a given level of quality for the overall EGI infrastructure.  The main update to this procedure is represented by a new step in the procedure for communicating with underperforming sites. In case the NGI does not respond to the GGUS ticket in 10 working days, a direct email is sent to the NGI for comments, improving reliability of the communication with the NGI in case of issues through the GGUS ticket, especially with NGIs that are experiencing a frequent personnel turn-over or temporary manpower issues. |
| Support for CVMFS replication across the EGI Infrastructure <https://wiki.egi.eu/wiki/PROC22> | New | The procedure describes the process of creating a repository within the EGI CVMFS infrastructure for an EGI VO. This has been entirely defined and tested in the EGI Engage context. |
| Production tools release and deployment process <https://wiki.egi.eu/wiki/PROC23> | New (still drafted) | The procedure describes the process of release and deployment in EGI production infrastructure for Production tools. |

## The EGI core activities

The EGI core activities are fundamental, as they represent the glue that puts together Resource Centres and user communities (Virtual Organizations) implementing the policies between the different partners of EGI. As a consequence, it is very important that they maintain very high levels of availability and reliability.

The EGI core activities didn’t experience big changes in the last year, testifying the stability and maturity of the infrastructure. The only new core activity is AppDB, the EGI Applications Database, that is a central service that provides a way to distribute the virtual machine images in the cloud sites that are part of the Federated Cloud.

This section provides a summary of the EGI operations service level targets formally agreed between resource providers, and periodically reported on a monthly basis.

|  |  |  |
| --- | --- | --- |
| Name | Description | Documentation or service URL |
| Message Broker Network | 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. |  |
| Operations Portal | 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. | <http://operations-portal.egi.eu/> |
| Accounting Repository | 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. | <http://accounting.egi.eu/egi.php> |
| Accounting and Metric Portal | 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. | <http://accounting.egi.eu/egi.php> |
| SAM central services | The 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.  The system is currenty going to be moved from the old distributed MyEGI to the new (central) ARGO infrastructure. | <http://argo.egi.eu/>  <https://wiki.egi.eu/wiki/SAM_Instances> |
| Monitoring central services | 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. |  |
| Security monitoring and related support tools | 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. | <https://wiki.egi.eu/wiki/EGI_CSIRT:SMG> |
| Service registry (GOCDB) | 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. | <http://goc.egi.eu/> |
| Catchall services | 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), the provisioning of middleware services needed by the monitoring infrastructure (e.g. top-BDII and WMS), and catch-all services for emerging user communities. | <https://wiki.egi.eu/wiki/Catch_All_Grid_Core_Services> |
| Operations support | 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. |  |
| Security coordination | 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. |  |
| Acceptance criteria | 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. |  |
| Collaboration tools/IT support | Collaborations tools are services needed by the EGI back-office and supporting EGI collaboration. | <https://wiki.egi.eu/wiki/EGI_Collaboration_tools> |
| Staged Rollout | 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. |  |
| Software provisioning infrastructure | 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. | <https://wiki.egi.eu/wiki/EGI_Software_Component_Delivery> |
| Incident management helpdesk | 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. | <http://helpdesk.egi.eu/> |
| 1st and 2nd level support (core platform, community platform) | 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 of 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.). |  |
| AppDB | The EGI Applications Database (AppDB) is a central service that stores and provides to the public, information about software solutions in the form of native software products and/or virtual appliances, the programmers and the scientists who are involved, and publications derived from the registered solutions. | <https://appdb.egi.eu/> |
| e-Grant | e-GRANT is a tool supporting Resource Allocation process. It allows researchers to request an amount of compute and storage resources, or FedCloud resources, for a given amount of time. e-GRANT handles all activities involved in RA Process which leads to SLA signing. | <https://e-grant.egi.eu/slaneg/auth> |

The provision of the core activities, has been constant and – with minor deviation – in the boundaries set by dedicated OLA signed by the service providers.

## The UMD software provisioning

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. The main goals of the overall Software Provisioning process are:

* Distributing the software provided by the Technical Providers (i.e. development teams) through a central repository
* Verify that the software fulfils a given set of Quality Criteria
* Deploy the software into the infrastructure in a controlled way, so that a software is installed on sites only if it has been tested in a real production context (Early Adoption).

The UMD Software Provisioning activity is made of several components:

* **Software Provisioning Process**, made of 3 subprocesses
  + **Software Delivery**, when Technology Providers (i.e. the development/product teams) submit new software releases; this is made by email or GGUS ticket. Software delivery is performed using one of the three different user interfaces available, i.e. a web form, e-mailing and a web service interface, that create tickets including all the necessary information about the software delivered in order to be processed. GGUS forwards the tickets to RT creating one RT ticket per Product per Platform and Architecture (PPA)
  + **Software Assessment**, consisting in
    - **Quality Assurance**, which assures that the software fulfils the Quality Criteria to be released in UMD; these include generic requirements applicable to every product, and specific requirements applicable to the capabilities supported by a component. During the last year, a new version of the Quality Criteria has been produced: <http://egi-qc.github.io/>
    - **Staged Rollout**, which is a procedure 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 the addition of corresponding mitigation information to the UMD release notes
  + **Reporting**, which is about informing TPs about the outcome of the Software Provisioning Process
* **UMD Release Process**, collecting tested Products per Platform and Architecture (PPAs) into UMD Releases.

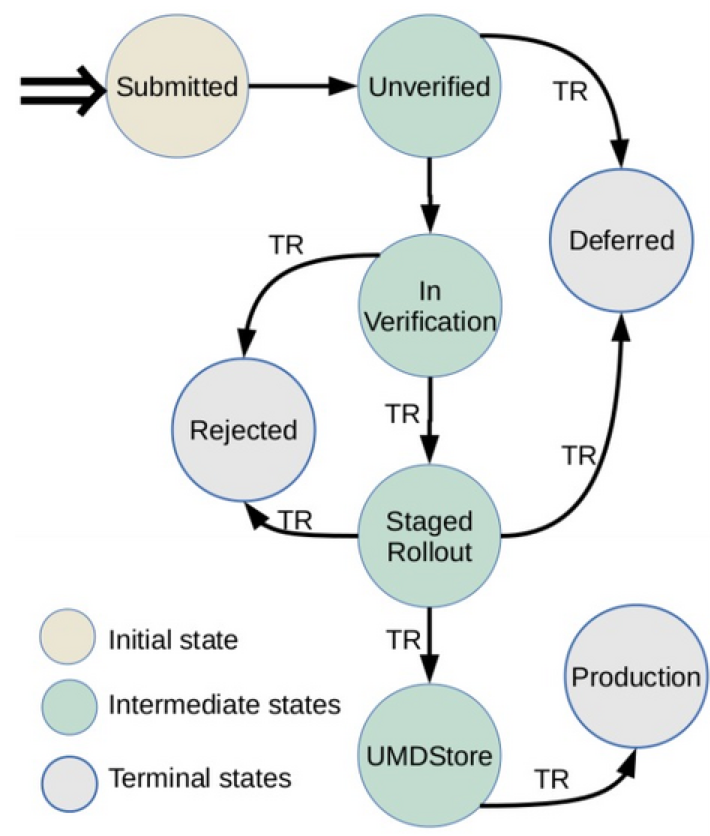


Figure - Status of products through the Software Provisioning Process

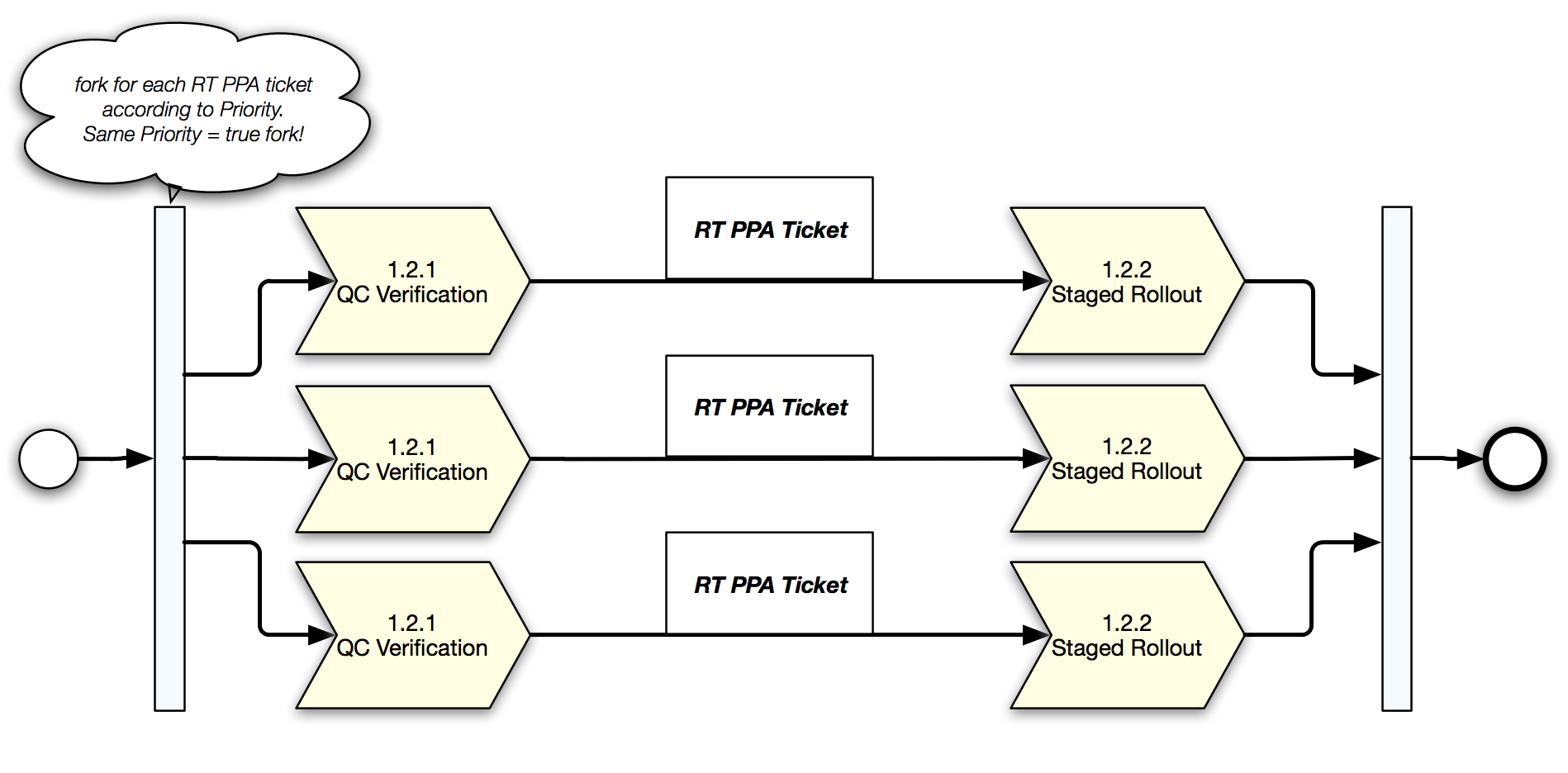


Figure - Software assessment

The Software Provisioning infrastructure is composed by several components. The most important are:

* **RT** (Request Tracker) tracks the status of the product in the software provisioning process, for a given release of a given product;
* **Repository Back-End** automates the movement of packages between repositories, validating the individual product releases submissions
* **Composer**, a web-based interface for bundling versioned software products that have successfully passed the UMD verification process, into a robust UMD release ready to be deployed
* **Web frontend** publishing the information about UMD releases
* **Repositories** to be maintained for every operating system and major release supported; they are:
  + **Untested**: contains the packages to be installed during the verification
  + **Testing**: contains the packages to be installed during staged rollout
  + **Base**: contains the packages released in the first major release
  + **Update**: contains the packages released in the update releases
  + **Release Candidate**: it is generated before a UMD release, to simulate the production repositories after the UMD release under preparation. This is used to test the installability of the newly released components, as well as the products already in production.

The Software Provisioning infrastructure supports multiple operating system (EL-based, Debian-based) and major releases. At the moment, the UMD4 structure provides support to CentOS7, SL6, and Ubuntu.

The infrastructure provides also a *“Preview” repository* where products are quickly released without verification; this is not an official UMD repository, but it follows the same procedures and has the same features.

The UMD Release Team (URT) has been working during the last year on releasing the middleware distribution according to the criteria of the Software Provisioning Process developed in the EGI context.

The documentation and the procedures used by the URT have been modified to improve the performances and the reliability of the whole process. In particular, a new guide has been written to make the whole process more transparent, provide tracking of the packages and feedback during the followed steps; this guide also gives a view of the provisioning procedure as a process compatible with FitSM standards. Moreover, several optimizations to the release workflow allow now to make the release time more predictable (about 2 months) and more reliable (no products out of the UMD radar).

At the moment, EGI is supporting two different major releases of UMD:

* **UMD3**, providing two EL-based platforms (Scientific Linux 5 and Scientific Linux 6) and Debian;
* **UMD4**, providing two EL-based platforms (CentOS7, Scientific Linux 6) and Ubuntu

The choice of the new platforms for UMD4 has been driven by:

* Almost full backward compatibility with previous releases (CentOS with SL, Ubuntu with Debian)
* Explicit preference of the Resource Centres in using CentOS/Ubuntu instead of SL/Debian (survey presented on May 2015).

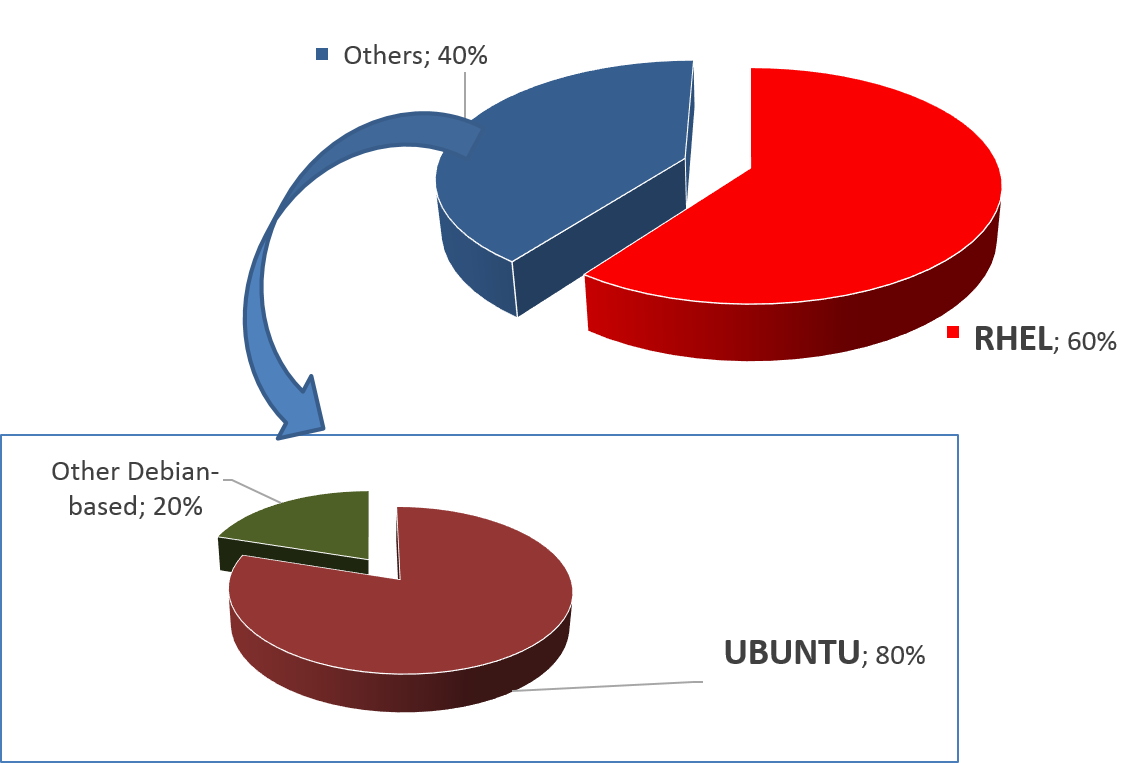


Figure - FedCloud RCs use CentOS and Ubuntu

A new release of the UMD has been released in January 2016 (UMD 4.0.0). The first release focuses on the adoption of CentOS7. The UMD4 release will soon host also the products developed in the EGI Federated Cloud context (Cloud Management Framework) for Ubuntu 14.04 LTS.. Considering that SL5 is under the decommissioning phase (deadline is April 2015), and the SL6 porting from UMD3 to UMD4 is currently ongoing, the decommissioning of UMD3 can be planned in favour of UMD4.

During 2015 there have been 9 releases of UMD3, 4 of which are minor releases and 5 revisions or fixes.

|  |  |
| --- | --- |
| **Capability** | **Product/Technology** |
| Compute, Job Execution, Job Scheduling | CREAM, Globus GRAM5, QCG-Computing, UNICORE TSI, UNICORE/X, ARC, WMS |
| Accounting | APEL |
| Attribute authority | VOMS Server, UNICORE XUUDB |
| Authentication | Globus GSI, UNICORE-Gateway |
| Authorization | ARGUS-PAP |
| Client tools | GFAL2 utils, VOMS clients |
| Credential management | MyProxy, ProxyRenewal |
| Data access | DAVIX |
| File Access, File Transfer, Storage Management | StoRM, dpm-xroot, XRootD, CVMFS, dCache, DPM/LFC, Frontier SQUID, Globus GRIDFTP, XROOTD |
| File Transfer Scheduling | FTS3 |
| Information Discovery | Globus InfoProviderService, UNICORE Registry |
| Other | BLAH, CGSI-gSOAP, CREAM TORQUE module, CREAM GE module, DMLITE, GFAL2, GFAL2-python, SRM-ifce, classads-libs, edg-mkgridmap, fetch-crl, ARC Nagios probes |

Figure – Products updated in UMD3 during 2015

### User software distribution

While UMD aims at distributing the “middleware” to the Resource Centres, other ways are necessary to distribute user applications: in these cases the life cycle management of the application must be decoupled from the operating system and the middleware as much as possible.

CVMFS (CERNVM File System) fits perfectly to the case: it is a network file system based on HTTP and optimized to deliver experiment software in a fast, scalable, and reliable way. Files and file metadata are downloaded on demand and locally cached, without interfering with the base system.

Several VOs are asking for migrating to CVMFS to distribute their software. EGI has formalized a procedure to drive the Virtual Organizations through setting up CVMFS for their software in the EGI infrastructure, making the software automatically available at the Resource Centres by means of the preinstalled CVMFS clients.

Effort has been spent to ensure interoperability between the CVMFS services provided by EGI and OSG: as anticipated, a procedure (https://wiki.egi.eu/wiki/PROC20) has been set, and recently refined, to ensure that VOs managing the CVMFS area are supported by Resource Centres in both OSG and EGI.

### Virtual Appliance distribution and VA Endorsement

The AppDB acts basically as a catalogue of virtual appliances (VA): for each VA, it maintains a set of metadata, among which a description, an identifier, and the URL of the VA itself, which is not stored on the AppDB itself. Versioning of the VAs is supported as well. After publishing a new appliance, or a new version of an existing appliance, everybody is able to download the instance.

The VO manager manages a “VO image list”; he can add a VA to his VO image list. Then the members of a VO can run the images of their VO image lists on the Resource Centres supporting their VO; this means that the VO manager decides which images can be run on the EGI Federated Cloud by the VO members simply listing the allowed images in the VO image list. This is the reason why the act of adding a VA to a Vo image list is called **endorsement**: the VO manager, on his responsibility, states that the image is “trusted” and can be used in the context of his VO.

The images available in AppDB can be classified in two types:

* EGI images, which are general purpose images, based on broadly used OSes
* VO-specific image, which are VO specific images, available to a specific VO and customized for specific purposes

Procedures are available that can assure that a given virtual appliance published in AppDB, under control of a given VO manager/endorser, is well-configured, secure and up-to-date. A checklist has been drafted to schedule and execute the maintenance of the appliances; the work done so far is available on wiki: <https://wiki.egi.eu/wiki/Virtual_Machine_Image_Endorsement>

In order to make the VAs of a specific VO list available at the Resource Centres supporting the VO, two tools are used: vmcatcher[[11]](#footnote-11) and vmcaster. In particular, vmcaster is a tool for managing and updating published virtual machines image lists on the AppDB side. The vmcatcher is the corresponding counterpart on the Resource Centre side: for each supported VO, it downloads the corresponding image list, and synchronizes locally a fresh copy of each image; if the list is updated, the vmcatcher takes care of reflecting the modifications locally (adding new images, deleting old images, overwriting old versions with new ones). In fact, this allows the endorser of the images to decide which images should be available at the Resource Centres in a very simple way and centrally.

These two graphs provide a general positive trend in the total number of Virtual Appliances and Software Appliances stored by Virtual Organizations, especially in the last 6 months.

The number of VOs publishing appliances on AppDB has doubled in the last year with a linear trend.

Taking into consideration only the VOs publishing appliances, the average number of appliances published by a single VO looks increased as well (+25% for both software and virtual appliances in 6 months).

## IT service management

During first year of the project, WP5 has been working towards improvement of EGI service delivery and quality of its services.

One action is to start implementing the ITIL/ISO20k based standard FitSM. FitSM is a free and lightweight standards family aimed at facilitating service management in IT service provision, including federated scenarios. The main goals of FitSM are:

* Create a clear, pragmatic, lightweight and achievable standard that allows for effective IT service management (ITSM).
* Offer a version of ITSM that can cope with federated environments, which often lack the hierarchy and level of control seen in other situations.
* Provide a baseline level of ITSM than can act to support ‘management interoperability’ in federated environments where disparate or competing organisations must cooperate to manage services.

A significant work has been done on clear definition of services which are provided through EGI Production infrastructure together with EGI.eu newly created Board – Service and Solution Board. As a result of the work an EGI Service Portfolio has been created and lists following services as in production:

|  |  |
| --- | --- |
| **Service Category** | **Name** |
| Compute | Cloud Compute |
| Cloud Container Compute |
| High-Throughput Compute |
| Storage | File Storage |
| Archive Storage |
| Data Management | File Transfer |
| Software and Service Platforms | Configuration Database |
| Accounting |
| Service Monitoring |
| Helpdesk |
| Attribute Management |
| Training Infrastructure |
| Validated Software and Repository |
| Operations Tools |
| Collaboration and Community Management Tools |

EGI is working with a number of communities (DRIHM, BILS[[12]](#footnote-12), Terradue, Mobrain, Pancancer, Life Science Grid Community, iMARINE, EXTRAS project, Human Brain project and Nanotechnology) to establish a Service Level Agreement (SLA) with resource providers. SLAs are not legal contracts but, as agreements, they outline the clear intentions to collaborate and support research. To support this work a process of SLA negotiation has been defined and followed to ensure effectiveness and repetitiveness of this activity.

Once an SLA is agreed, EGI continues to support the effort between the resource providers to enable the research community on the promised resources as well as future monitoring.

The base for SLA negotiations with research communities are Resource Center (RC)[[13]](#footnote-13) and Resource infrastructure Provider (RP)[[14]](#footnote-14) Operational Level Agreements established in 2014. Both documents ensure that resource providers are properly integrated with EGI Infrastructure and provide minimum required availability and reliability of resources.

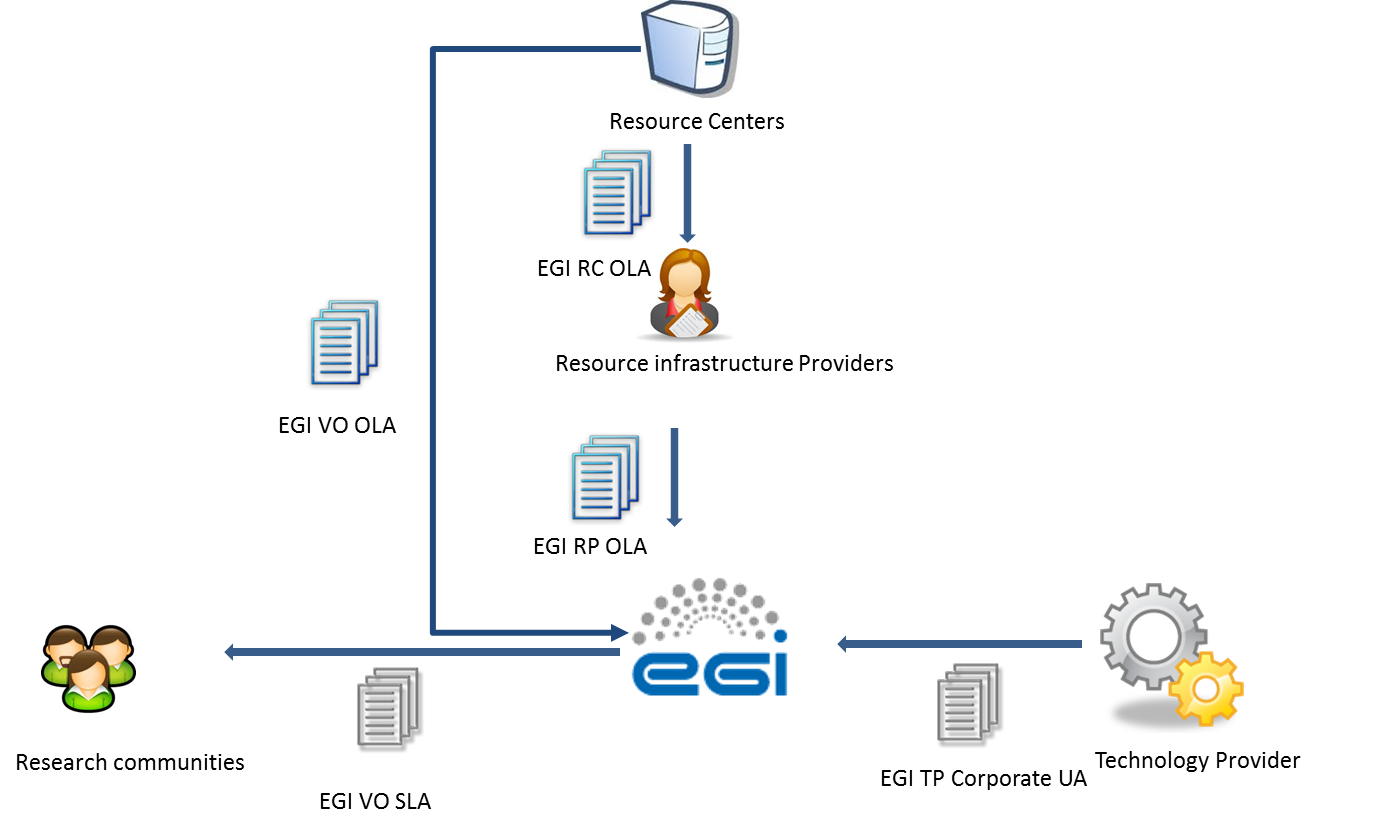


Figure EGI OLA and SLA scheme

Figure 7 shows the SLA/OLA framework. EGI centrally agrees the SLA with the research communities, liaising with the NGIs/EIROs and the resources centres The outputs of this internal negotiation are the VO-specific OLAs who are extending the RC OLA and RP OLA, these documents support the VO SLA, ensuring that the targets of this last agreement are fulfilled by the service providers.

Another area the project has been improving is suppliers and customer relationship management where suppliers and customers for each service have been identified and unified approach has been defined to manage performance, satisfaction and complains.

To support production tools release and deployment process a new procedure[[15]](#footnote-15) is in preparation which aims to define steps which needs to be performed before new release of services under Software and Service Platforms category can be introduced into production infrastructure. Thanks to this procedure it will be ensured that each release is properly tested and documented, and will not impact the Infrastructure in negative way.

In next year EGI will work towards implementation of remaining processes defined in FitSM[[16]](#footnote-16) standard:

* Service Reporting Management
  + Defining all service reports and ensure they are produced according to specifications in a timely manner to support decision-making.
* Service Availability & Continuity Management
  + Ensuring sufficient service availability to meet agreed requirements and adequate service continuity in case of exceptional situations
* Capacity Management
  + Ensuring sufficient capacities are provided to meet agreed service capacity and performance requirements.
* Information Security Management
  + Managing information security effectively through all activities performed to deliver and manage services, so that the confidentiality, integrity and accessibility of relevant information assets are preserved
* Problem Management
  + Defining way to investigate the root causes of (recurring) incidents in order to avoid future recurrence of incidents by resolving the underlying problem, or to ensure workarounds / temporary fixes are available
* Configuration Management
  + Defining way to provide and maintain information about all services and their relationships and dependencies
* Change Management
  + Ensuring changes to the services are planned, approved, implemented and reviewed in a controlled manner to avoid adverse impact of changes to services or the customers receiving services

# The evolution of the security operations

Security operations, policies, procedures and best practices, have all had to evolve to meet the requirements of new trust models, new developments and new usage scenarios in EGI-Engage. As usual, developments in policies and procedures have been driven by risk assessment of the security requirements and trust models of the new EGI services, including the use of Federated Identity Management, the EGI Federated Cloud service and the Long Tail of Science service.

In this section we present this evolution and plans for further changes in the next year.

## Security policies

A meeting of the EGI Security Policy Group at the start of EGI-Engage considered which security policies were most in need of revision to address the new EGI-Engage services. It was decided that the "Grid Acceptable Use Policy" and "The Security Policy for the Endorsement and Operation of Virtual Machine Images" [ENDSP] should be addressed by EGI-Engage in its first year. This work has been done in parallel with the production of new policies for the Long Tail of Science service (LToS) and a draft new general policy addressing Data Protection issues. All of this policy work helps provide appropriate managerial controls on the operation of new services developed in EGI-Engage, thereby mitigating the related security risks.

The new AUP, now called "Acceptable Use Policy and Conditions of Use" [AUP], has been generalised to include all EGI service offerings (Grids, Clouds, LToS, etc.). At the same time wording was changed to require appropriate acknowledgement of use iof resources and support in publications. The policy on VM Endorsement has been modified to better fit the policy and trust issues in the EGI Federated Cloud service. The new policy may be found at [Ref: https://documents.egi.eu/document/2729].

A large number of users and communities would benefit from expanded use of credentials based on Federated Authentication (“FedAuth”) for accessing services instead of employing personal certificates either installed in browsers or used to create proxy certificates. Secure use of FedAuth on the infrastructure relies on two capabilities:

a) A translation of FedAuth credentials to a form understood by the services, and b) some agreed mechanism to retain the current credential assurance levels and confidence in identity vetting. In this context, it is important to realize that user communities may be structured in different ways, and that, depending on the internal structure, coherence, and level of organization of the user community, it may or may not be able to provide user traceability, assurance, or identity vetting. Of the many user communities supported by EGI, only a small sub-set is so stringently organized as to be able to independently perform high-assurance identity vetting. In other cases (in particular in the context of the specific provisions for the Long Tail of Science), EGI centrally takes a responsibility of providing higher-assurance identity and traceability information independent of the user community. In the majority of cases, the communities actually rely on external identity vetting information in enrolling their members.

Only for highly organized communities, and for those cases where EGI independently provides assurance, FedAuth can be leveraged early since only minimal information (a persistent non-reassigned identifier) is needed from the identity providers in the FedAuth infrastructure. For those cases, and for the first concrete implementation of a prototype around the ‘Federated Identity Management for Research’ (FIM4R) pilots, the WLCG WebFTS use case, a co-existence model and policy needs to be in place in order to support both these highly structured as well as the more dynamic communities on the same infrastructure. To advance the development of a coordinated trust policy that will in the future be able to more dynamically accommodate differentiated trust models, WLCG in collaboration with EGI has developed a co-existence model and evolution for a sustained implementation. This model was developed with support from ENGAGE and is documented in the evolving document “Considerations on the coexistence of controlled and flexible community models” [DIFFTRUST].

Also the “Long Tail of Science” specific policy leverages differentiated and redistributed responsibilities. Here the policy distributed specific elements of the end-to-end risk assessment to the registrars within the EGI community, the centralized “User Management Portal” of the EGI LToS service, and the participating resource centres, aiming to contain any residual risks exposed through the LToS service towards other, non-participating resource centres and NGIs. The policy aims to enable a low-barrier Service to be offered to a wide range of research users in Europe and their collaborators world-wide, by any Resource Centre organisation that elects to do so. In offering such LToS Services, the Resource Centre shall not negatively affect the security or change the security risk of any other Resource Centre or any other part of the e-Infrastructure. In particular, security incidents originating in the LToS Service should not impact the IT Infrastructure in ways that are incompatible with the operational model of other, more tightly controlled, parts of the infrastructure. This document also provides guidelines on the implementation of security procedures and controls to facilitate offering of the Service by Resource Centres and Science Gateways.

The Guidelines [LTOSSP] also contain normative information on how to implement the Policy.

A version of the new AUP specific to LToS has also been produced and adopted [LTOSAUP].

Future work on security policies during year 2 of the project will be aimed at making other policies more applicable to the new EGI-Engage use cases. This will include a revision of the top-level overall Security Policy document and a revision of the Virtual Organisation Membership Management Policy to apply to the wider range of user communities now being addressed in EGI-Engage.

## Security procedures

In order to provide efficient Operational Security in evolving infrastructures the security procedures constantly have to be developed further.

The technological aspect of the procedure development aims to exploit new possibilities in incident response required by the newly integrated technologies. In addition the new players (e.g. cloud resource providers) have to be integrated into the overall incident response  concept. This activity is reflected  in the  *EGI CSIRT Security Incident Handling Procedure[[17]](#footnote-17)*. This procedure was presented to OMB for approval.

To maintain a properly patched infrastructure and make sure that CRITICAL Vulnerabilities are handled adequately by all involved entities the *EGI-CSIRT Critical Vulnerability Handling* procedure[[18]](#footnote-18) was further developed. This procedure is currently in draft, here the  new developed supporting policies (e.g. [ENDSP], see above)  need to be approved.

In addition to the procedure development, also security monitoring and incident response tool development will be addressed in project year 2. The aim here is to be able to monitor and enforce the policies developed here and to preserve the central user management capabilities  as for the extended set of services provided by EGI. The EGI Software Vulnerability group vulnerability issue handling procedure has been revised and approved by the EGI Operations Management board.

Previously during EGI-InSPIRE the main focus of the EGI issue handling was on the Grid Middleware distributed in the EGI UMD, and additionally to assist EGI CSIRT in the risk assessment of other software vulnerabilities, mainly in the Linux operating system. Technology is changing, in particular related to the emergence of the EGI Federated cloud. A much wider variety of software is in use such as Cloud enabling software, software within VMs, VMs themselves, VO specific software. SVG cannot control what software is in use. Some of this software is commercial; produced by large or small companies or organisations. Some is produced by EGI partners. Some software is released in the EGI UMD by resource providers with which EGI has a service level agreement, some such as operational tools for EGI infrastructure is released by the EGI team, as well as VOs which take their software from a much wider variety of sources. This means we needed to revise the way we minimize risk arising from software vulnerabilities to the EGI infrastructure.

The advisory template has also been revised, taking account of comments from various site administrators, including so that the basic information and what is required of sites is displayed in the e-mail preview page and to make it more mobile friendly.

It has been found that various Virtual Organisations and user groups have been developing or using software which is not as secure as we would like, or configured in a way that is not secure or compliant with policy. Also this wider variety of software means the SVG cannot be experts on much of the software deployed in the EGI infrastructure. For this reason we included a Software security Checklist to help those who are developing or selecting software avoid some of the most common problems. This has been made available on the EGI Wiki[[19]](#footnote-19)

For technology on which the EGI federated cloud heavily relies, a Technology Provider questionnaire was produced to ensure that the technology is reasonably secure and suitable for use in the EGI infrastructure. The idea is that this questionnaire is filled in for any technology which is deployed on the EGI infrastructure, and on which EGI relies. This provides some assurance that at least at the time this questionnaire is filled in, it does not contradict EGI security policy. It is not a full security analysis of the software.  This questionnaire may be filled in by the developers, which is the case for software being developed for use on our infrastructure. Or it may be filled in by someone who is selecting a technology, or who has expertise in that technology in EGI.  
  
A version of the Technology provider questionnaire was approved at the EGI Operations management board in September 2015.

## Security risks assessment

EGI Security Threat Risk assessment with focus on the EGI Federated cloud and the changing EGI environment is being carried out and is near completion. A similar approach to that in 2012 is being carried out. First a team of people to carry out the work was established, this included people from CSIRT, the SVG, the EGI Federated cloud, SPG, and others. Then a draft set of threats was produced, starting from the list from 2012 but adding new ones both from general experience since then and those associated with Virtualization and the Federated Cloud. These threats were divided into various categories, and members of the team were asked to take one or two categories each and improve on them, and provide a description of or update the current situation. Then the team were invited to comment, add others. A list of 103 threats was produced, in 18 different categories. Then all members of the team were invited to provide their opinion on the 'likelihood' and 'Impact' of each threat, according to certain guidelines. In all 10 members of the team returned a spreadsheet with their opinion of likelihood and impact, and the average risk was computed from this. At present, the report is being prepared, including suggestions for mitigation of some of the highest risk threats, and is due shortly.

# Roadmap for the EGI production infrastructure

The roadmap for the EGI Operations is developing in two directions:

* Consolidating the current production services, increasing their performances, and their reliability, with the final goal of improving the user experience.
* Integrating in the production infrastructure the new platforms and services that are produced by the EGI-Engage project, and other activities related to EGI.

These two main themes are described in detail in the next sub-sections.

## Consolidating current production services

The production services of EGI must continue to evolve with the goal to improve the user experience. All services are periodically assessed to understand where there are issues degrading the quality of service perceived by our users. The HTC services, considering the longer experience, have reached a good maturity level, with a considerably decreasing number of issues also helped by the fact that the middleware software is not being updated frequently, with major changes.

The federated cloud services are in production for less than two years at the moment of writing, and although in constant improvement the quality of the service provided to the user is not very uniform, and can vary much depending on the service provider used at the moment.

This is caused primarily to the following main reasons:

* Non complete documentation for the service providers
* Non complete coverage of all the capabilities by monitoring
* Lack of integration with the cloud management system of the federated cloud extensions
* Lack of proper software and release management of the “plugins” developed by EGI for the cloud management system

This is how these issues will be tackled.

**Documentation.**

At the moment the documentation is fairly complete, what is partially missing is a top-down structure, that would lead the cloud sites from the first approach to EGI through the integration and certification process. In particular documentation should highlight the different deployment scenarios in order to help the cloud provider in choosing the best architecture to federate with EGI. A restructure of the documentation is being carried out at the moment of writing.

**Monitoring**

The automatic monitoring of the services is covering the basic functionalities of the services, for example virtual machine instantiation and removal. The user experience can though be affected by a number of other factors. One example is the availability of the virtual machine images, or advanced contextualization features, that are needed by the user use cases, which distribution at the moment are not monitored.

The current plan is to start a detailed assessment of the status of the sites in the federated, through manual testing actually replicating the work of the users, at least touching most of the functionalities expected by users. This will achieve two results: sites with issues will be asked to fix their issues, and recurring issues will generate monitoring probes that are closer to user behaviour.

**Integration testing with the cloud management system and software packaging.**

At the moment, to federate private cloud, EGI is developing and maintaining a set of extensions to the community based cloud management system (e.g. Open Stack and open Nebula). Maintaining these components means, keep the compatibility with the new version of the cloud management system, and make the EGI development available to the site managers who needs to install them.

The integration tests with new CMS are currently implemented with some of the components, for example the OCCI integration with OpenStack is tested by the developers as soon as a new version of OpenStack is pre-released by the OS collaboration, but other components are not validated with the new releases of the main CMS, not with a reliable and repeatable process at least. This will have to improve with dedicated testbed resources, and automated testing procedures to validate new developments on both sides (EGI and the CMS).

Good testing of new releases will be the main building block for a proper distribution of the releases to the EGI sites. The distribution in UMD, or equivalent process, of the federated cloud components will force the developers to achieve: proper packaging and testing, clear documentation, plus a trusted single entry point for the download of the federating software.

Besides the federated cloud, another improvement deployed in the coming months is a centralized monitoring, that will free the NGIs from the burden of deploying a dedicated Nagios instances to submit probes to their sites, by deploying a centralized group of Nagios services that can support the whole infrastructure. This will reduce the maintenance cost of the Nagios services, and at the same time it will make much more flexible the monitoring system, which will not require a deployment campaign of a new version to add new probes or similar changes that now require NGIs intervention.

## Integrating new services in production

New services, to be technically integrated in EGI must fulfil some prerequisites:

* Technical support for the EGI AAI infrastructure
* Support for the EGI Accounting infrastructure, if relevant
* Monitoring probes to be integrated with the EGI monitoring infrastructure
* Fulfilment of EGI security policies

In some cases, it is acceptable to have a roadmap for the development of the requirements above, if the services need to be quickly integrated and made available to the users. Service provider must sign an OLA with EGI, where the targets for the service are defined.

Besides technical integration, EGI must ensure that the quality of the software supporting the services is production-ready. This is implemented by ensuring the software support by the developers, through an underpinning agreement, as described in section 3.4 and through the software quality assurance process described in section 3.3.

In EGI-Engage a number of services are being developed. Many Competence centres (CC) will integrate high-level discipline specific services targeting the represented communities. These services, or part of them, will be technically integrated and offered as EGI services to a wider community. This is one of the changes foreseen for the EGI production infrastructure, the users will not only access the resources, through services providing plain computing or storage, but will use also platforms that, underpinned by EGI resources, will provide high level services.

The new platforms can be of different level of abstraction, from a PaaS to a Virtual Research Environment, operated by EGI partners, or by the VOs.

To support these new platforms, EGI Operations must focus the effort in different directions, for example to develop the security policies and processes to assess the policy compliancy of the new technologies and access paradigms, and to properly react to any security issue that could involve the new platform, as it is done for every EGI service.

At the moment the operational infrastructure is hierarchically organized in NGIs/EIROS and resource centres. Every service is provided by a resource centre, and every resource centre is connected to an NGI. If EGI integrates services offered by other entities, e.g. communities or external providers, the hierarchical structure will have to be extended to include in the operational framework other entities providing services part of the EGI portfolio.

While the technical implementation of monitoring should not change from any development done for the current services, the reporting, how the monitoring results are used, will have to change. Currently any deviation in performance is handled by the NGI and by the site staff, but adding on top of these services a platform operated by – let say – a VO introduces a new level of complexity. Availability of the platform can be monitored and reported, to the entity operating the service, as well as the supporting resources, can be monitored and reported to the resource centres operating the resources.

The development of the EGI Marketplace will push the boundaries of the scenario described above. On top of what the CCs will integrate in EGI, through the marketplace a number of new services will be added. While at the moment of writing the structure and the policies behind the marketplace are not yet defined, we can anticipate that the services accessible through the Marketplace will be very diverse, for example in the form of virtual appliances and datasets. As every service provided by EGI, Operations will have to work with the providers in order to understand how service availability can be monitored, reported, and how targets should be set, and ultimately upon which events EGI Operations can remove a service from production, preventing users to access it. Moreover, at least a subset of the services in the marketplace will have to be monitored and the status information be made available to the users who want to access the them.

The evolution of the AAI infrastructure, under the JRA1 work package, is one of the topics of EGI-Engage with the biggest impact on operations. At all levels. The most important impact is the new capabilities offered to the users, who will be able to use their institutional credentials to access EGI, and this will affect all the layers of the production infrastructure. Once the AAI layer will be enabled for federated authentication the current EGI services must implement the support for the new authentication services.

Ultimately, AAI layer is composed by a number of components that need to be rolled in production, and integrated in the set of core services provided by EGI to our stakeholders. The deployment of these production instances must be planned, and appropriate resources be allocated, but also the components must be monitored and supported by appropriate OLAs and policies to be production-ready.

The other big change that is being introduced by EGI-Engage is the Open Data Platform. Similarly to other new services, the outputs of the JRA2 work package will have to be integrated in the operations framework. But beside the operational details, the new set of services of the open data platform will be a big shift in the EGI service provisioning, adding to the current one, compute-centric, a new data-centric resource provisioning. Users will be able to use EGI as a data infrastructure, and use computing associated to data. These features will be supported by appropriate monitoring and accounting, and offered through the marketplace.

Some of the current and the new services will be also offered through the long tail of science, as described in [D5.2], which is an access mode to get basic services, and limited resources, without the overhead of setting up a virtual organization, or ask for a grant of resources. The long tail of science access mode can be also considered a tool to offer a “try before you buy” mode, that could consequently evolve in a long-term collaboration with a community.

Ultimately EGI production infrastructure will hopefully incorporate also the outputs of other activities with a strong collaboration with EGI, such as the INDIGO DataCloud project, which will release both infrastructure/service providers oriented developments and PaaS and SaaS for the user communities.

# References

GLO, EGI Glossary: <https://wiki.egi.eu/wiki/Glossary>

RCOLA RC Operations Level Agreement: <https://documents.egi.eu/document/31>

AUP Acceptable Use Policy <https://documents.egi.eu/document/2623>

ENDSP: <https://documents.egi.eu/document/771>

DIFFTRUST: <https://documents.egi.eu/document/2745>

LTOSSP: <https://documents.egi.eu/document/2734>

LTOSAUP: <https://documents.egi.eu/document/2635>

GLO: https://wiki.egi.eu/wiki/Glossary

1. Accounting portal: http://accounting.egi.eu [↑](#footnote-ref-1)
2. ARGO monitoring service: http://argo.egi.eu [↑](#footnote-ref-2)
3. At the moment of writing the desktop grid operations centre is on hold, since the leading institution asked for decommissioning but the procedure has not been closed yet. [↑](#footnote-ref-3)
4. <https://documents.egi.eu/document/31> [↑](#footnote-ref-4)
5. https://w3.hepix.org/benchmarks/doku.php [↑](#footnote-ref-5)
6. https://wiki.egi.eu/wiki/Federated\_Cloud\_Architecture [↑](#footnote-ref-6)
7. https://github.com/hepix-virtualisation/vmcaster [↑](#footnote-ref-7)
8. <http://accounting.egi.eu/egi.php> [↑](#footnote-ref-8)
9. “Others” is a category of user communities that do not belong to the other disciplines that are part of the current classification. The scientific discipline classification of EGI is being reviewed. [↑](#footnote-ref-9)
10. https://wiki.egi.eu/wiki/Scientific\_Disciplines [↑](#footnote-ref-10)
11. Documentation about vmcatcher/caster: <https://github.com/hepix-virtualisation/vmcatcher>

    <https://github.com/hepix-virtualisation/vmcaster> [↑](#footnote-ref-11)
12. EGI BILS VO SLA and OLAs <https://documents.egi.eu/public/ShowDocument?docid=2701> [↑](#footnote-ref-12)
13. <https://documents.egi.eu/public/ShowDocument?docid=31> [↑](#footnote-ref-13)
14. <https://documents.egi.eu/public/ShowDocument?docid=463> [↑](#footnote-ref-14)
15. <https://wiki.egi.eu/wiki/PROC23> [↑](#footnote-ref-15)
16. <http://fitsm.eu/> [↑](#footnote-ref-16)
17. : <https://wiki.egi.eu/wiki/SEC01> [↑](#footnote-ref-17)
18. [ref: <https://wiki.egi.eu/wiki/SEC03>] [↑](#footnote-ref-18)
19. <https://wiki.egi.eu/wiki/SVG:Software_Security_Checklist> [↑](#footnote-ref-19)